

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

**FRAUDE AL SENADO DE  
MICHIGAN POR EMPLEADO  
FANTASMA  
ANÁLISIS DE CASO: USA VS. BERTRAM JOHNSON, Jr.  
Caso Número: 2: 17-cr-20233**

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

MARZO, 2019

PREPARADO POR  
Vanessa De Jesús Díaz

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

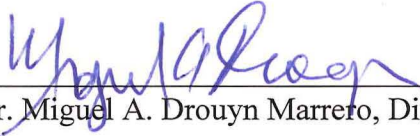
**FRAUDE AL SENADO DE  
MICHIGAN POR EMPLEADO  
FANTASMA  
ANÁLISIS DE CASO: USA VS. BERTRAM JOHNSON, Jr.  
Caso Número: 2: 17-cr-20233**

Preparado por  
Vanessa De Jesús Díaz

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

Marzo, 2019

Aprobado por:

  
\_\_\_\_\_  
Dr. Miguel A. Drouyn Marrero, Director

## Tabla de Contenido

<b>Sección 1: Introducción y Trasfondo</b> .....	1
Introducción .....	1
Descripción del caso .....	2
Trasfondo .....	3
Descripción de los hechos.....	4
Acusaciones, cargos y penalidades .....	6
<b>Sección 2: Revisión de Literatura</b> .....	7
Introducción .....	7
Fraudes Involucrados .....	8
Leyes Aplicables .....	19
Casos Relacionados .....	20
Herramientas de Investigación.....	23
<b>Sección 3: Simulación</b> .....	27
Introducción .....	27
<b>Sección 4: Informe del Caso</b> .....	30
Resumen Ejecutivo .....	30
Objetivo.....	30
Alcance del Trabajo .....	31
Datos del Caso .....	31

Descripción de los Dispositivos Utilizados .....	32
Resumen de Hallazgos .....	34
Cadena de Custodia.....	37
Procedimiento .....	40
Conclusión .....	49
<b>Sección 5: Discusión del Caso .....</b>	<b>50</b>
<b>Sección 6: Auditoría y Prevención.....</b>	<b>52</b>
Introducción .....	52
Resumen de Hallazgos .....	53
Recomendaciones .....	58
Opinión de Auditoría .....	59
<b>Sección 7: Conclusión .....</b>	<b>60</b>
<b>Sección 8: Referencias .....</b>	<b>62</b>

## Tabla de Figuras

Figura 1: Fraudes ocupacionales más comunes en agencias gubernamentales .....	14
Figura 2: Cómo castigan las agencias gubernamentales a perpetradores de fraude .....	14
Figura 3: Controles antifraude más comunes en agencias gubernamentales .....	15
Figura 4: Cómo se detecta inicialmente el fraude en agencias gubernamentales .....	15
Figura 5: Frecuencia de desembolsos fraudulentos .....	16
Figura 6: Promedio de pérdida de desembolsos fraudulentos.. .....	16
Figura 7: Esquema de un ghost employee (Wells, J. 2013).....	17
Figura 8: Esquema de horas y salarios falsificados (Wells, J. 2013).....	18
Figura 9: Esquema de Fraude .....	28
Figura 10: Imagen de la información de la computadora utilizada para este examen .....	32
Figura 11: Imagen de la pantalla de la computadora forense .....	33
Figura 12: Imagen del USB Drive que se analizará.....	33
Figura 13: Imagen recuperada en Forensic Toolkit de Formulario del “PAF”.....	34
Figura 14: Imagen “PAF” .....	35
Figura 15: Imagen recuperada en Forensic Toolkit de Formulario de Depósito directo ..	35
Figura 16: Imagen formulario de depósito directo .....	36
Figura 17: Imagen recuperada en Forensic Toolkit del timesheet .....	36
Figura 18: Imagen Timesheet .....	37
Figura 19: Imagen pantalla máquina virtual e inicio de FTK Imager.....	40
Figura 20: Selección del tipo de fuente de evidencia .....	41
Figura 21: Selección de la unidad de origen.....	41

Figura 22: Selección del tipo de imagen.....	42
Figura 23: Información del elemento de evidencia.....	42
Figura 24: Selección de carpeta para guardar imagen .....	43
Figura 25: Selección de ubicación donde se guardará imagen .....	43
Figura 26: Creación de imagen .....	44
Figura 27: Resultado de los Hash Values del archivo creado.....	44
Figura 28: Resumen de la imagen creada .....	45
Figura 29: Verificación de Hashes y datos del archivo creado.....	45
Figura 30: Seleccionar tipo de fuente de evidencia .....	46
Figura 31: Evidencia para análisis .....	47
Figura 32: Transferencia de los 3 documentos encontrados .....	47
Figura 33: Transferencia de Hashes de los documentos encontrados.....	48
Figura 34: Evaluación del archivo del caso .....	48
Figura 35: Datos contenidos en el expediente .....	49

## **Sección 1: Introducción y Trasfondo**

### **Introducción**

Según Antilavado de Dinero (2017), la corrupción y el fraude paralizan el desarrollo económico de cualquier lugar y van en deterioro de la justicia social, causando perjuicios graves a la economía y en muchos casos facilita las operaciones de la delincuencia organizada.

Corrupción es considerada como un conjunto de conductas delictivas que defraudan los recursos públicos del Estado, y por lo general son cometidos por funcionarios públicos. Surge del mal uso del poder cuando se utiliza para obtener beneficios privados, pero también puede incluir miembros de la familia o amigos.

Esta conducta, cometida por acción o por omisión por una o varias personas, entiéndase, empleados, directivos o terceros, corrompe y corroe las instituciones públicas y las entidades privadas, con igual grado de responsabilidad, ya que es tan corrupto el que solicita y recibe como el que propone y da. La corrupción en el sector público afecta la administración y los recursos públicos y la corrupción privada afectan el patrimonio económico de los particulares. Sin embargo, los delitos públicos, de forma general, son el fraude, la conclusión, el delito, el acontecimiento indebido de contratos estatales, el tráfico de influencias, la circulación de influencias, el enriquecimiento ilícito, la utilización indebida de información y el soborno (Iberdrola, 2018).

A continuación, se expone el caso del ex senador estatal Bertram Johnson, Jr., de 44 años, de Highland Park, Michigan, el cual fue acusado por cargos de conspiración y robo a un programa financiado con fondos federales pertenecientes al estado ingresando un empleado fantasma en su nómina (Morelaw.com, 2018).

**Descripción del caso**

**Número de caso:** 2: 17-cr-20233

**Caso:** United States of America vs. Bertram Johnson, Jr.

**Asunto:** Conspiración y robo de un programa financiado con fondos federales

**Partes en el caso:**

Acusado (autor):

- Bertram Johnson, JR.

Entidades relacionadas (víctimas):

- Estado de Michigan

Agentes Investigadores:

- Jeffery E. Peterson, Agente Especial Interino, División de Detroit del FBI
- Manny J. Muriel, Agente Especial del Servicio de Impuestos Internos, Investigación Criminal de Detroit

Abogados y Fiscales:

- Daniel L. Lemisch, Fiscal Interino de los Estados Unidos, Distrito de Michigan
- Michael Buckley, Fiscal Auxiliar de los Estados Unidos, Jefe Adjunto, Unidad de Corrupción Pública, Distrito de Michigan
- Frances Lee Carlson, Fiscal Auxiliar de los Estados Unidos, Unidad de Corrupción Pública, Distrito de Michigan
- John Shea, Abogado del acusado, Tribunal Federal del Distrito Este de Michigan



Juez:

- Matthew F. Leitman, Tribunal de Distrito de los Estados Unidos para el Distrito Este de Michigan (Condado de Wayne)

## **Trasfondo**

Este trabajo de investigación está enfocado al fraude por medio del ingreso de un empleado fantasma para la apropiación ilegal de un programa financiado con fondos federales. Según Ballotpedia.org (2018), el acusado en este caso es Bertram Johnson, Jr., ex miembro demócrata del Senado del Estado de Michigan, por el Distrito 2 desde el año 2011 hasta 2018. Johnson renunció a su cargo el 2 de marzo de 2018, después de declararse culpable de robo. El 11 de abril de 2017, Johnson fue acusado por un gran jurado federal por cargos de conspiración y robo. Johnson supuestamente contrató a un empleado fantasma, que no trabajaba, para pagar una deuda personal. Johnson expresó interés en una candidatura al Congreso en 2014, pero finalmente se postuló y ganó la reelección al senado estatal. Johnson sirvió dos términos en la Cámara de Representantes de Michigan, representando al Distrito 5 desde 2007 hasta 2011.

Johnson se graduó de la Universidad de Detroit Jesuit High School y Academia. Estudió Criminología y Administración de Seguridad en la Universidad de Detroit Mercy. Su experiencia profesional incluye trabajar como gerente de oficina en el bufete de abogados de su familia y como Jefe de Personal del Representante Estatal Bill McConico.

El acusado Bertram Johnson Jr., tomó prestado más de \$10,000 en octubre de 2013 de un conspirador anónimo y más tarde contrató a esa persona a su nómina para pagar la deuda. El empleado fantasma recibió un pago de \$23,134 y trabajó desde marzo de 2014 hasta enero de

2015 como organizador comunitario. Si es declarado culpable, Johnson podría cumplir hasta cinco años en el cargo de conspiración y hasta 10 años en el cargo de robo.

El 18 de abril de 2017, Johnson se declaró inocente de los cargos. Fue liberado con una fianza de \$10,000. Johnson declinó comentar sobre los cargos luego de su comparecencia. El abogado de Johnson, Cyril Hall, dijo a los reporteros que lo negaban todo y estarían preparados para litigar la controversia. El 11 de julio de 2017, Cyril Hall, el abogado de Johnson, se retiró del caso. John Sea se convirtió en el abogado designado por el tribunal de Johnson el 13 de julio.

El 27 de septiembre de 2017, un juez federal retrasó el juicio de Johnson hasta el 12 de marzo de 2018. Se esperaba que comenzara el 23 de octubre de 2017. Johnson renunció a su puesto el 2 de marzo de 2018, después de declararse culpable de robo.

### **Descripción de los hechos**

Según el *Indicment* del caso United States of America vs. Bertram Johnson, Jr. (2017,11 abril), se indicó que el Estado de Michigan es una agencia gubernamental que recibió en exceso de \$10,000 bajo uno o más programas federales que involucran subsidios, contratos, préstamos, garantías, seguros y otras formas de asistencia federal por períodos de un año. Como senador estatal, el acusado Johnson tenía la autoridad de seleccionar y contratar empleados para su plantilla senatorial.

Como senador estatal, el acusado Johnson, era responsable de presentar y hacer que se presentaran como correctas y verdaderas, las hojas de tiempo de su plantilla de empleados para reflejar sus horas trabajadas por quincena. Cada vez que el demandado Johnson presentaba las hojas de asistencia de sus empleados, autorizaba a que se pagaran con fondos que se encontraban bajo custodia y control del estado de Michigan.

El término *ghost employee*, tal como se usa en la Acusación, significa un empleado, que se pagó por hora por el estado de Michigan, para realizar trabajos para la oficina del acusado, el senador Bertram Johnson, JR., y quien en realidad no hizo ningún trabajo. Todo este esquema se hizo con el propósito de que el acusado pudiera obtener los salarios por hora que fueron pagados. En octubre de 2013, el acusado Johnson se acercó a *Cooperating Witness-1* (CW-1) y solicitó un préstamo personal en efectivo de \$10,000.

El 21 de octubre de 2013 o alrededor de esa fecha, CW-1, otorgó al acusado Johnson un préstamo de \$10,000 en efectivo. Entre el 21 de octubre de 2013 y marzo de 2014, CW-1, solicitó en repetidas ocasiones el pago de su préstamo personal al acusado Johnson, pero él no pagó a CW-1. En marzo de 2014, el acusado Johnson le dijo a CW-1 que podía reembolsar el préstamo de \$10,000 colocando a CW-1 en la nómina de su personal senatorial del Estado de Michigan y CW-1 aceptó el acuerdo.

El 27 de marzo de 2014 o alrededor de esa fecha, el acusado Johnson contrató oficialmente a CW-1 como parte de su personal senatorial del Estado de Michigan utilizando el nombre de *Community Liaison*, efectivo el 28 de marzo de 2014, se completó y firmó el *Michigan State Senate Personnel Action Form (PAF)*, y luego presentándolo a la Secretaria de Hacienda del Senado. En el *PAF*, el acusado Johnson indicó que CW-1 trabajaría por 30 horas a la semana a una tarifa de \$22.00 por hora. Desde aproximadamente el 28 de marzo de 2014 hasta aproximadamente el 2 de enero de 2015, CW-1 recibió pagos quincenales para un total aproximado de \$23,133.89 del estado de Michigan como parte del personal senatorial del acusado Johnson cuando en realidad CW-1 era un *ghost employee*.

En o alrededor del 7 de enero de 2015, el acusado Johnson firmó y presentó al *PAF*, la terminación oficial de *CW-1* como empleado de su personal senatorial, citando el motivo como “renuncia voluntaria” efectivo el 2 de enero de 2015.

### **Acusaciones, cargos y penalidades**

El ex senador estatal fue condenado por cargos de conspiración (18 U.S.C § 371) y robo de un programa financiado con fondos federales (18 U.S.C § 666).

Fue sentenciado a 90 días en prisión, seguidos de dos años de libertad supervisada con 90 días de confinamiento en el hogar y 480 horas de servicio comunitario, y más de \$23,000 en restitución, después de haberse declarado culpable de conspiración para cometer robo de un programa financiado con fondos federales, anunció el fiscal Matthew Schneider.

## Sección 2: Revisión de Literatura

### Introducción

Según Diario Financiero (2013), los esquemas de fraude corporativo interno están divididos en tres grandes ramas: Apropiación de Activos, Declaraciones Fraudulentas y Corrupción. Entre los primeros, una familia de fraude frecuente son los esquemas de nómina de sueldo, o *payroll*. En los esquemas de *payroll*, el perpetrador falsifica o altera información en la nómina de pagos, provocando que la empresa, inadvertidamente, pague sueldos ficticios o duplicados, que finalmente van a parar a manos del defraudador o un cómplice.

Típicas modalidades de fraude por *payroll* son el pago a “empleados fantasmas”, la falsificación de carga de horarios, y los esquemas de pago de comisiones. “Empleado fantasma” se refiere a empleados que figuran en la nómina de *payroll*, aunque en los hechos no hay tal empleado trabajando para la compañía; la empresa, sin embargo, le paga al “fantasma” que en algunos casos, se trata de personas completamente ficticias; entre otros, de personas reales cuya identidad está siendo utilizada por el defraudador. Para operar exitosamente un esquema de “empleado fantasma”, deben ocurrir 4 cosas:

- Incorporar al “fantasma” en la nómina de pagos
- Mantener actualizados los registros sobre horarios y salarios falsificados del “fantasma”
- Que la empresa gire un cheque o deposite al respectivo pago
- Que el pago sea direccionado hacia el perpetrador o un colaborador

Se trata de un fraude interno relativamente simple de llevar a cabo con éxito, por aquellas personas cuyos cargos, poderes o funciones les permiten ya sea formalmente, o por hechos, incorporar nuevos trabajadores en la nómina de pago, o remover a aquellos cuyo vínculo laboral ha terminado.

La mitigación de este esquema de fraude convoca tanto controles preventivos como detectivos, que hoy están sumamente descritos, y permiten detectar tempranamente con una alta eficacia la ocurrencia del fraude y los involucrados, lo cual a su turno genera una espiral virtuosa de disuasión de dichos fraudes dentro de la empresa, al aumentar la probabilidad de captura y con ello la percepción de riesgo y dificultad de elementos del componente “oportunidad”, uno de los tres vértices del triángulo del fraude.

### **Fraudes Involucrados**

Según [Auditoool.org](http://Auditoool.org) (2014), el fraude es perpetrado por una persona que sabe que el mismo podría resultar en algún beneficio no autorizado tanto para sí personalmente, para la organización o terceros, y que puede ser perpetrado por personas que estén dentro o fuera de la organización. Algunos esquemas de fraude comunes incluyen:

- Malversación de activos que involucra el robo de efectivo o activos (suministros, inventarios, equipos e información) de la organización. En muchos casos, el perpetrador intenta ocultar el robo, usualmente incorporando ajustes en los registros.
- El *skimming* que se produce cuando el efectivo de una organización es robado antes de ser registrado en los libros y registros de la organización. Por ejemplo, un empleado acepta el pago de un cliente, pero no lo registra.

- El fraude por reembolso de gastos se produce cuando a un empleado se le paga por gastos ficticios o inflados. Por ejemplo, un empleado presenta un informe de gastos fraudulento y reclama reembolso por viajes personales, alimentos inexistentes, kilometraje extra, etc.
- El fraude del rol de pagos que ocurre cuando quien comete el fraude hace que la organización emita un pago para luego de presentar reclamos falsos por compensación. Por ejemplo, un empleado reclama trabajo durante horas extras en las que no ha trabajado o un empleado añade empleados fantasmas al rol de pago y recibe el respectivo cheque de pago.
- El fraude de estados financieros involucra la inclusión de información falsa como parte de los estados financieros, por lo general sobreestimando los activos o ingresos o subestimando pasivos y gastos. El fraude de estados financieros es generalmente perpetrado por los gerentes de una organización quienes buscan afianzar la imagen económica de la misma. Miembros de la gerencia podrían beneficiarse directamente del fraude al vender acciones, recibir bonos de desempeño, o al utilizar el reporte falso para ocultar otro fraude.
- El fraude de desembolso se produce cuando una persona hace que la organización emita un pago por bienes o servicios ficticios, facturas infladas, o facturas por compras personales. Por ejemplo, un empleado puede crear una compañía fachada (*Shell Company*) y luego facturas empleados por servicios inexistentes. Otros ejemplos incluyen reclamos de salud fraudulentos (facturación por servicios no prestados, facturación fraccionada en lugar de una facturación completa), reclamos por seguros de desembolso por parte de gente que está trabajando o pensión o reclamos al seguro social correspondientes a personas que han muerto.

- La presentación de información falsa involucra la inclusión de información adulterada, usualmente para quienes están fuera de la organización. Más frecuentemente estos fraudes involucran estados financieros fraudulentos, aunque también puede ocurrir que se falsifique la información utilizada como medición de desempeño.
- Corrupción es el mal uso del poder confiado, para lucro personal. La corrupción incluye soborno y demás usos impropios del poder. La corrupción constituye con frecuencia un fraude fuera de libros, significando esto que exista escasa evidencia disponible de los estados financieros para que el delito se ha cometido. Los empleados corruptos no tienen que cambiar fraudulentamente los estados financieros para encubrir sus delitos, simplemente reciben pagos en efectivo bajo la mesa. En la mayoría de los casos, estos delitos son descubiertos a través de indicios o quejas provenientes de terceros, con frecuencia a través de una línea de denuncias de fraude. La corrupción frecuentemente involucra la función de compras. Cualquier empleado autorizado a gastar el dinero de la organización es un posible candidato a estar involucrado en actos de corrupción.
- El soborno es el ofrecimiento, suministro, aceptación, o solicitud de cualquier cosa de valor para influir en el resultado. Los sobornos pueden ser ofrecidos a empleados clave o gerentes tales como agentes de compra quienes cuentan con discreción para adjudicar compra a vendedores. En el caso típico, un agente de compras acepta beneficios para favorecer a un vendedor externo en la compra de bienes o servicios. La otra cara de ofrecer o recibir cualquier cosa de valor que se exige como condición para la adjudicación de negocios es denominada extorsión económica. Otro ejemplo constituye un funcionario de préstamos corrupto quien demanda prebendas a cambio de que se



apruebe un préstamo. Quienes pagan los sobornos tienden a ser vendedores que trabajan bajo comisión o intermediarios para vendedores externos.

- Un conflicto de interés se da cuando un empleado, gerente o ejecutivo de una organización tiene un interés personal y económico no divulgado dentro de una transacción que perjudica a la organización o a los intereses de sus accionistas.
- Una desviación es el acto de desviar una transacción potencialmente rentable, que normalmente generaría utilidades para la organización, hacia un empleado o hacia una tercera parte externa.
- El uso no autorizado o ilegal o el robo de información confidencial y de propiedad de la organización para beneficiar equivocadamente a alguien.
- Actividad entre partes relacionadas constituye una situación en donde una de las partes recibe de la otra relacionada algún beneficio que no se obtendría en una transacción de negocios normal y justa
- La evasión de impuestos constituye un reporte intencional de información falsa en una declaración de impuestos con el fin de disminuir los impuestos que se adeuden.

Los esquemas de nómina son otra forma de desembolsos fraudulentos y se basan típicamente en tarjetas de tiempo o registros de nómina. En este caso se detalla como el acusado Bertram Johnson Jr., entregó hojas de asistencias falsas lo que causó que la Oficina del Senado de Michigan pagara el salario del *ghost employee* por el periodo del 28 marzo de 2014 hasta el 2 de enero de 2015.

Se pueden definir como fraudes ocupacionales a los esquemas de nómina en los cuales, una persona que trabaja en una organización hace que esa misma organización, emita un pago al realizar reclamos falsos. Existen tres categorías principales de fraude de nómina:

- Esquemas de empleados fantasmas
- Esquemas de falsificación de horas y sueldo
- Esquema de comisiones

El primer paso en un esquema de *ghost employee* es entrarlo a la nómina. En algunas empresas, la contratación se realiza a través de otra Oficina Central en donde se encuentra el Departamento de Personal; entre otros, su función es administrar el personal de la organización. Independientemente de cómo sea la contratación de nuevos empleados, la persona que tiene el rol o la autoridad de agregar nuevos empleados, se encuentra en la mejor posición de agregar *ghost employee*. Fue la autoridad del ex senador Johnson que tenía en la contratación y la supervisión de los empleados que le permitieron perpetrar este fraude.

En un correcto escenario, todos los nombres que figuran en la nómina de una organización, deben ser verificados en contra de registros de personal y registros de ponches para asegurarse de que las personas que reciben cheques de pago trabajen para la empresa, pero, en este caso que investigamos, analizamos y auditamos, no ocurrió así. La falta de separación de funciones y la ausencia de revisión, le facilitaron la tarea del acusado de agregar un empleado ficticio en el sistema de nómina.

La segunda cosa que debe ocurrir para que un cheque de pago se emita a un *ghost employee*, para aquellos en que los empleados cobren por hora, es la recopilación y cálculo de la información de tiempo trabajado. El perpetrador debe proporcionar un registro de asistencia que

muestre cuántas horas ha trabajado el empleado ficticio durante el periodo de pago más reciente. Esta información, junto con la información del salario que se encuentra contenida en los archivos de personal o de nómina, se utiliza para llevar a cabo el cálculo del cheque fraudulento.

Un empleado fantasma, por definición, no trabaja para la compañía víctima por lo que la aprobación deberá ser obtenida de manera fraudulenta. Refiriéndonos a este caso, el propio ex senador creó el *ghost employee*, completó las hojas de asistencias y aprobó las mismas para luego enviarlas al área de nómina para que se emitiera el pago.

El tercer paso en el esquema de fraude es la emisión del cheque de pago. Una vez que la falsificación haya ocurrido, el perpetrador no toma un papel activo en la emisión del cheque. En la mayoría de los casos, el autor no tiene la autoridad para distribuir el cheque de pago y por esto debe asegurarse de que el empleador víctima envíe los cheques a un lugar en donde pueda tener acceso (Wells, J. 2013).

En este caso, como el empleado ficticio fue agregado al registro de personal y de nómina, la distribución de su pago resultó uno más fácil ya que su cuenta bancaria fue configurada para recibir los mismos por depósito directo.

En las figuras que se presentan a continuación, se presentan en porcentajes; los distintos tipos de esquemas de fraude ocupacional que son más comunes en las agencias gubernamentales, las medidas que toman los patronos para castigar el fraude, los controles más comunes que se utilizan, como detectan inicialmente la comisión de estos actos fraudulentos y la frecuencia de los desembolsos fraudulentos por módulos, el promedio de pérdidas de los desembolsos fraudulentos y los esquemas que se llevan a cabo para un *ghost employee* y el que corresponde a horas y salarios falsificados:

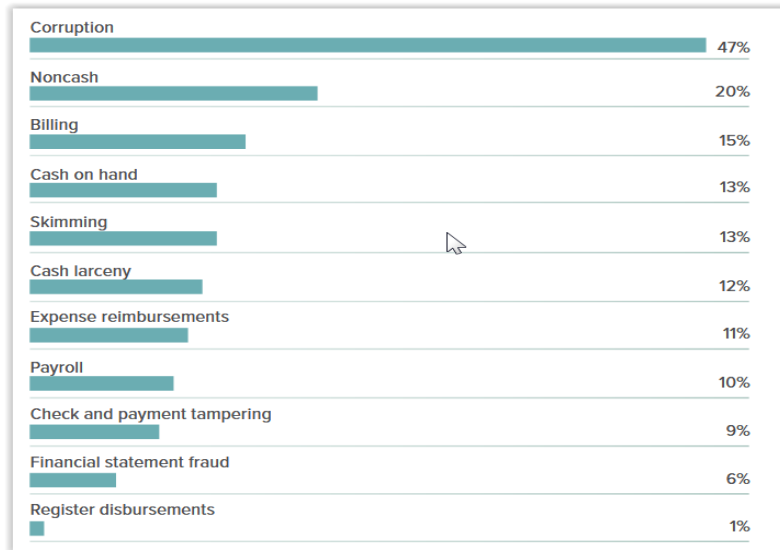


Figura 1: Fraudes ocupacionales más comunes en agencias gubernamentales (ACFE, 2018a)

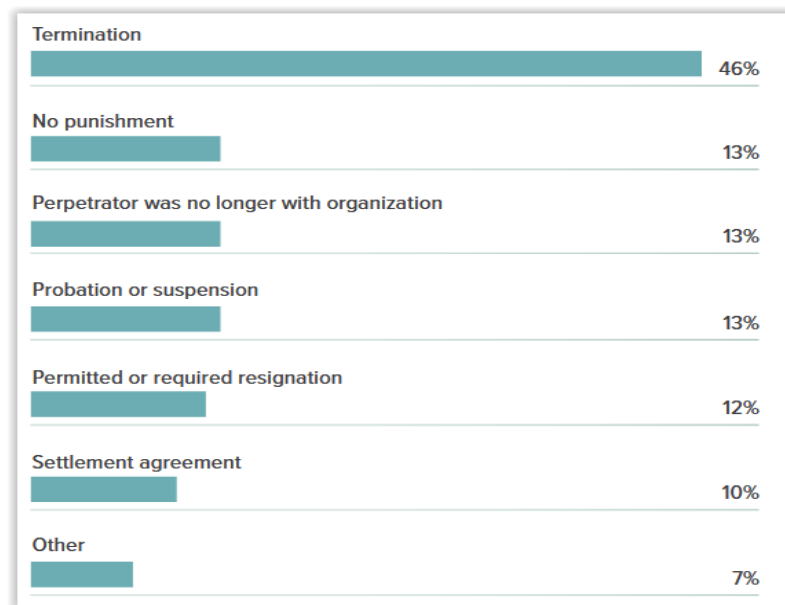


Figura 2: Cómo castigan las agencias gubernamentales a perpetradores de fraude (ACFE, 2018a)

Control	Percent of cases
Code of conduct	86%
External audit of financial statements	84%
Internal audit department	79%
External audit of internal controls over financial reporting	71%
Employee support programs	68%
Management certification of financial statements	68%
Hotline	66%
Management review	58%
Anti-fraud policy	50%
Independent audit committee	49%
Fraud training for employees	48%
Fraud training for managers/executives	47%
Formal fraud risk assessments	35%
Dedicated fraud department, function, or team	34%
Surprise audits	28%
Proactive data monitoring/analysis	27%
Job rotation/mandatory vacation	16%
Rewards for whistleblowers	12%

Figura 3: Controles antifraude más comunes en agencias gubernamentales (ACFE, 2018a)

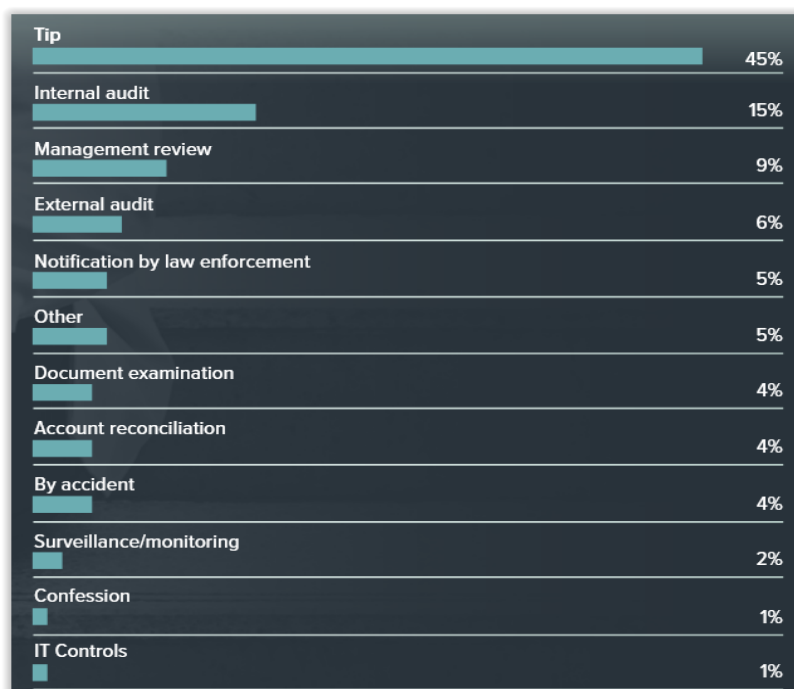


Figura 4: Cómo se detecta inicialmente el fraude en agencias gubernamentales (ACFE, 2018a)

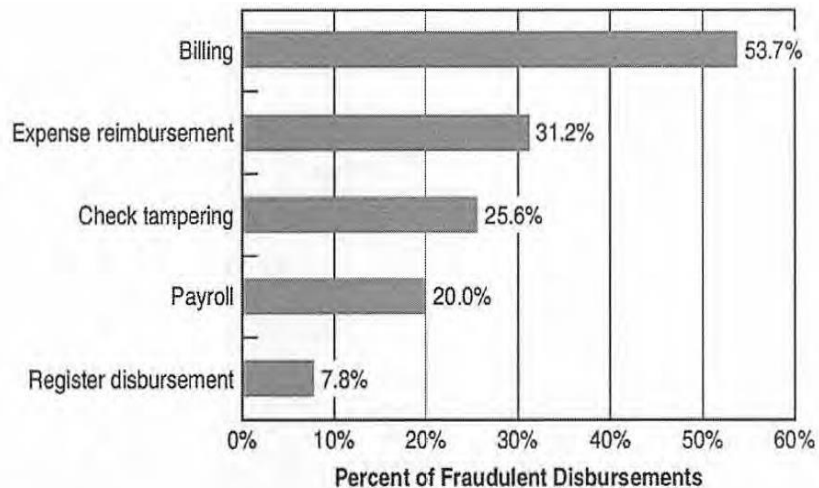


Figura 5: Frecuencia de desembolsos fraudulentos (Encuesta de Fraude Global 2011)

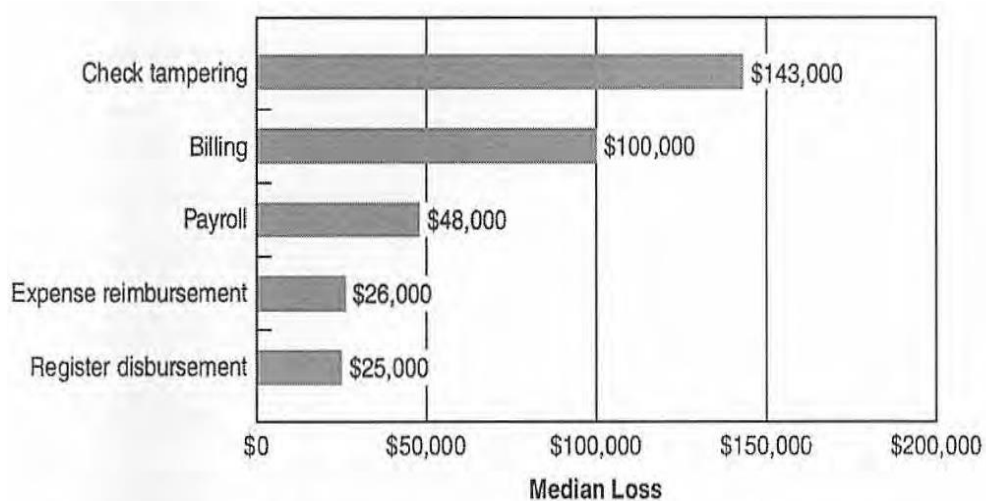


Figura 6: Promedio de pérdida de desembolsos fraudulentos (Encuesta de Fraude Global 2011)

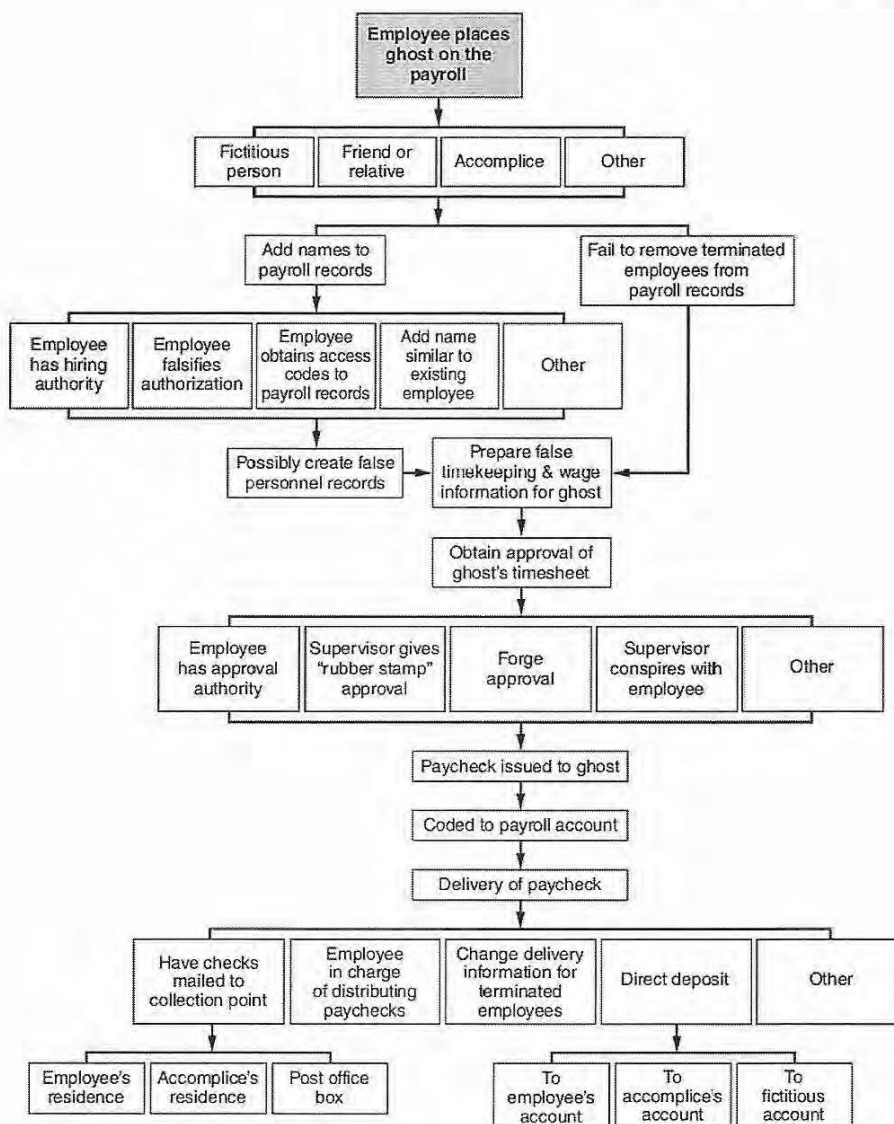


Figura 7: Esquema de un ghost employee (Wells, J. 2013)

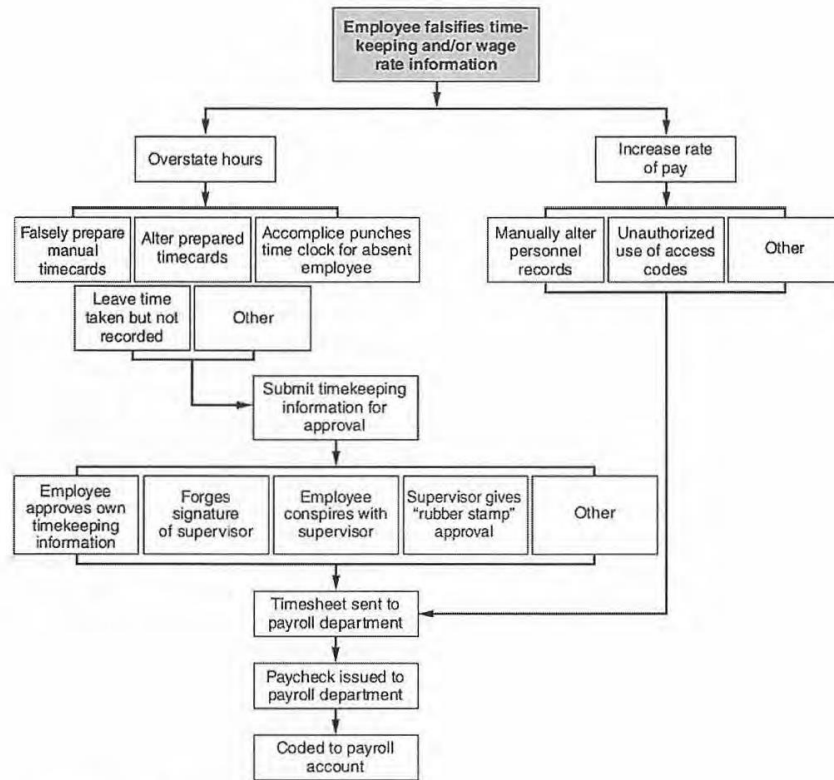


Figura 8: Esquema de horas y salarios falsificados (Wells, J. 2013)



## **Leyes Aplicables**

Las leyes aplicables al esquema de fraude cometido por el ex senador Bertram Johnson, Jr., son las siguientes:

Según la Ley *Conspiracy to Defraud the United States* (2015). (18 U.S.C § 371).

Entiéndase si dos o más personas conspiran para cometer cualquier ofensa con el propósito de defraudar o actuar en contra de los Estados Unidos, o cualquiera de sus agencias de cualquier manera y una o más de esas personas hacen cualquier acto para realizar el objeto de la conspiración, cada uno será multado bajo este título o encarcelado no más de cinco años, o ambos. Multa máxima de \$10,000.

Según la Ley *Theft or bribery concerning programs receiving Federal funds* (2015) (18 U.S.C § 666). Cualquier persona que sea un agente de una organización, o del gobierno federal, estatal, local, o cualquier agencia de la misma y malversa, roba u obtiene mediante fraude o de otra manera sin autoridad, cualquier persona que no sea el propietario legítimo o intencionalmente aplica el uso incorrecto de la propiedad que se valora en \$5,000 o más y es propiedad de, o está bajo el cuidado, custodia o control de dicha organización, gobierno o agencia; o solicite de manera corrupta el beneficio de cualquier persona, con la intención de ser influenciado o recompensado en relación con cualquier negocio, transacción o serie de transacciones de dicha organización, gobierno o agencia que involucre cualquier cosa de valor de \$5,000 o más; u otorga, ofrece o acepta de manera corrupta cualquier cosa de valor para cualquier persona con la intención de influir o recompensar a un agente de una organización o de un gobierno federal, estatal o local, o cualquier agencia del mismo, en relación con cualquier negocio, transacción, o

una serie de transacciones de dicha organización , gobierno, o agencia que involucre algo de valor de \$5,000 o más; será multado bajo este título, encarcelado no más de 10 años o ambos. Esto aplica a toda organización, gobierno a agencia que reciba por periodos de un año, beneficios en exceso de \$10,000 bajo un programa federal que involucra una subvención, contrato, subsidio, préstamo, garantía, seguro, u otra forma de asistencia federal.

### **Casos Relacionados**

#### **Pueblo de Puerto Rico vs. Germaine Cruz Correa (Tribunal de Primera Instancia del Centro Judicial de San Juan):**

Según publicado por el Departamento de Justicia del Gobierno de Puerto Rico (2018, 20 de junio), se radicaron 63 cargos contra una exempleada de una compañía por fraude, apropiación ilegal, apropiación ilegal de identidad y por presentar ante el Departamento de Hacienda planillas de contribución sobre ingresos falsas y fraudulentas.

De la investigación se desprende que la entonces empleada de Auto Grupo, Germaine Cruz Correa, se desempeñaba como Oficial de Nómina en el Departamento de Recursos Humanos y entre el 11 de noviembre de 2013 y el 17 de junio de 2016, creo un expediente falso de tres empleados fantasmas con los que logró desviar fondos a sus cuentas bancarias.

Mediante este esquema, logró apropiarse de \$110,672.66. Cruz Correa no informó los ingresos tributables provenientes de dicho fraude al Departamento de Hacienda por los años contributivos 2014, 2015 y 2016 y no reportó planillas de contribución sobre ingresos de individuo. La jueza Alfrida Tomey Imbert, del Tribunal de Primera Instancia de San Juan, encontró causa probable para arresto contra Cruz Correa por 54 cargos bajo el Artículo 182 de

apropiación ilegal agravada del Código Penal; un cargo por Artículo 181 por apropiación ilegal menos grave; dos cargos por violación al Artículo 202 por fraude; tres cargos bajo el Artículo 209 por apropiación ilegal de identidad; y tres cargos bajo el Artículo 6030.16 por planillas falsas y fraudulentas del Código de Rentas Internas.

La fianza fue de \$315,000. La vista preliminar fue señalada para el 3 de julio. La investigación estuvo a cargo de los fiscales Brenda Rosado Aponte y Leilani Dominicci Vazquez, de la División de Delitos Económicos, en conjunto con el agente Juan José Pereira de la División de Robos a Bancos y Fraude del Negociado de la Policía de Puerto Rico y el agente especial Cintrón de la Unidad de Inteligencia y Fraude Contributivo del Departamento de Hacienda.

**United States of America v. Gerald Ursin, Jr., Case # 2: 16-cr-00112-EEF-MBN**

Según publicación de Morelaw.com (2017, 20 de febrero), Gerald Ursin, JR., de 63 años de edad, de New Orleans y retirado Jefe del Diputado de la Oficina del Alguacil de la Parroquia de Orleans, fue sentenciado por haberse declarado culpable de conspiración por cometer fraude electrónico. El Juez de Distrito de los Estados Unidos, Eldon E. Fallon, condenó a Ursin a tres años de libertad condicional, una multa de \$10,000, \$25,178 en restitución y una evaluación especial de \$100. Según los documentos judiciales, comenzaron en 2009 y continuaron hasta enero de 2014.

Ursin y otros participaron en una conspiración para cometer fraude electrónico. Ursin admitió que, en su papel de Jefe de Diputado en la Oficina del Alguacil de la Parroquia de Orleans, participó en un plan para defraudar entidades y eventos locales, como *Mardi Gras Krewes*, festivales de música y comida y eventos deportivos, completando los documentos de

facturación con nombres de personas que no proporcionaron ningún servicio de seguridad (*Ghost Employees*).

Además, Ursin admitió que después de que las facturas infladas de manera fraudulenta se enviaran por medio de *interstate wires*, se le entregó una parte de la cantidad sobre facturada en por medio de cheques pagaderos a miembros de la familia de manera fraudulenta por pagos de trabajos que nunca se realizaron. El abogado *Polite* de los Estados Unidos elogió el trabajo de la Oficina Federal de Investigaciones, con la asistencia de la Oficina del Auditor Legislativo de Louisiana para investigar este asunto y reconoció la asistencia proporcionada por los Auditores Legislativos de Louisiana. El acusado fue sentenciado a tres años de libertad condicional, una multa de \$10,000 y \$25,178 en restitución.

**United States of America v. Tamara Housley, Case # 5:14-cr-00046\_HE (Western District of Oklahoma)**

Según publicación de Morelaw.com (2014, 27 de agosto), Tamara Housley (a/k/a “Tami Housley”), de Loudon, Tennessee, fue sentenciada por el Juez de Distrito de los Estados Unidos Joe Heaton a cumplir 30 meses de prisión por malversación por parte de su empleador por cometer fraude electrónico y por presentar una declaración de impuestos falsa, anunció Sanford. C. Coats, Fiscal de los Estados Unidos para el Distrito Oeste de Oklahoma. Además, a Housley se le ordenó pagar \$336,950 en restitución.

Housley trabajó como contable para una empresa de contratación eléctrica en Chickasha, Oklahoma. Como tenedor de libros, los deberes de Housley incluían preparar cheques, documentar cuentas por pagar, y por cobrar, ingresar a nuevos empleados en el sistema de nómina de giros automáticos, pagar impuestos de la empresa y recoger correo. Aunque no estaba

autorizada para firmar cheques de la compañía, preparó cheques para todos los pagos, incluidos los extractos de las tarjetas de crédito comerciales. Housley también tenía acceso exclusivo a la cuenta de nómina de la empresa.

Según los registros judiciales, Housley comenzó a usar tarjetas de crédito comerciales en 2006 para realizar compras personales no autorizadas y realizar pagos a su cuenta personal de PayPal pagar sus facturas personales de servicios públicos, televisión por cable y facturas de teléfonos celulares, y comprar entradas para conciertos. Housley tuvo acceso exclusivo al correo de la compañía y retuvo los estados de cuenta mensuales de la tarjeta de crédito de su jefe y, cuando renunció incluso cambió la dirección de facturación de una tarjeta a la dirección de la casa. A partir de 2007, según los registros de la corte, Housley usó su acceso a la cuenta de nómina de la empresa para agregar fraudulentamente a su novio a la nómina semanal como un *ghost employee*. Housley también fue acusada de presentar declaraciones de impuestos falsas.

Housley fue acusada el 6 de febrero de 2014. El 22 de abril de 2014, se declaró culpable de cometer fraude electrónico y de presentar una declaración de impuestos falsa para 2010. Fue sentenciada hoy a 30 meses de prisión, seguida de tres años de libertad supervisada y se le ordenó pagar \$336,950 en restitución a su empleador y al IRS.

### **Herramientas de Investigación**

Un elemento fundamental en todas las empresas es la nómina. A menudo es objeto de errores, fraude y robos. Los constantes cambios y las regulaciones en el tiempo trabajado, las asistencias, pagos basados en incentivos y cambios de salario, además del volumen alto y las frecuencias de las operaciones hacen que el proceso de la nómina sea bastante complejo a la hora de evaluar.

Según la ACFE (2018b), los estafadores hacen que sus empleados les emitan un pago de compensación al que no tiene derecho por medio de:

- Esquemas de empleados fantasmas
- Salarios y falsos esquemas salariales
- Esquemas de comisiones

Las alertas o banderas rojas para detectar este tipo de fraude son:

- Anomalías en la información del empleado
- Anomalías en el registro de nómina
- Anomalías en el control de la nómina
- Anomalías en el pago

Las pruebas para identificar las anomalías se deben realizar en:

- Información del empleado
- Registro de nómina
- Cheques de nómina
- Aumento de bonos o de pago
- Tendencias de tiempo de inactividad del empleado

Los estafadores manipulan los factores con la compensación para aumentar su paga y las alertas o banderas rojas para detectar los sueldos falsos y esquemas de salarios son los siguientes:

- Anomalías salariales brutas
- Anomalías en las tasas de pago
- Anomalías en la paga neta

- Anomalías en el número de horas trabajadas
- Anomalías en el número de piezas o productos producidos

Las pruebas para identificar estas anomalías se deben realizar en:

- Salario bruto
- Tasa de pago
- Pago neto
- Números de horas trabajadas
- Número de piezas o productos producidos

A continuación, se mencionan las herramientas que pueden ser utilizadas para el análisis de fraude:

***CaseWare Analytics: IDEA:*** permite que una organización detecte actividades erróneas, sospechosas y fraudulentas antes de que se efectúen los pagos. La solución ofrece la posibilidad de definir todo el entorno de control, desde la creación del registro del empleado hasta los pagos de salario final. Una vez completado, el marco de control y alerta automáticamente a las personas pertinentes para que tomen medidas sobre los elementos descubiertos, en el momento oportuno. Los responsables de los procesos financieros y de negocios pueden centrarse en optimizar el rendimiento de la empresa y maximizar los beneficios a la vez que se mitigan los riesgos de fraude (CaseWare Analytics, 2018).

***ActiveData:*** herramienta para un auditor, examinador de fraudes, o analista de negocios, que ofrece un análisis de datos al entorno familiar de Microsoft Excel.

*ActiveData* se integra fácilmente al flujo de trabajo existente. (Capterra, s.f.a).

***AP Forensics Enterprise Suite:*** conjunto de herramientas para cualquier profesional de finanzas para reducir los sobrepagos, detectar fraudes y proteger el gasto general de una organización. Su uso puede ser constante, diaria o semanalmente, y funciona junto con cualquier sistema de contabilidad. (Capterra, s.f.b).

***Argoscope:*** es una solución de monitoreo de pagos, diseñada para detectar y prevenir el fraude en las organizaciones. El sistema controla todo el proceso de pago, realizando evaluaciones de riesgo en tiempo real antes de aprobar transferencias de fondos. Argospe está compuesto por cientos de algoritmos únicos que permiten el nivel de gestión, la supervisión continua y la exclusión de cualquier pago inusual, en tiempo real y en una forma de segundos. Además, proporciona cumplimiento normativo sin interferir en el flujo de trabajo (Capterra, s.f.c).



### Sección 3: Simulación

#### Introducción

En esta simulación de hechos que estamos analizando y discutiendo en este trabajo investigativo, se muestra una reconstrucción de la secuencia de cómo se efectuó el fraude. De esta manera, tendremos como investigadores, un mejor entendimiento del esquema; esto según las condiciones y declaraciones que se afirma o se presume ocurrió.

Como se ha expuesto a través de este trabajo, el esquema de fraude al estado de Michigan fue perpetrado por Bertram Johnson, Jr., senador estatal. Johnson tomó prestados miles de dólares en efectivo de un co-conspirador anónimo, y más tarde colocó a ese co-conspirador en la nómina pública bajo el nombre de *Community Liaison* y lo incluyó en su plantilla de empleados, certificando sus hojas de asistencia quincenalmente; esto sabiendo que el mismo era un *ghost employee* y que en ningún momento realizaría trabajos para él. La acusación formal alega que Johnson colocó a este *ghost employee* en la nómina pública con el único propósito de pagarle la deuda del préstamo personal que había adquirido con él. Luego del acusado Johnson haber ingresado al *ghost employee*, en la nómina del senado de Michigan, específicamente el 31 de marzo de 2014, visitó la empresa de consultoría perteneciente a Glynis Thornton (*ghost employee*) y aceptó la cantidad de \$4,000 en efectivo la cuál le fue entregado por una empleada de ella. Durante el periodo de marzo de 2014 hasta el 2 de enero de 2015, se le pagaron aproximadamente \$23,133.89 al *ghost employee* en dinero que pertenecía a los contribuyentes.

Basado en la información recopilada de los documentos legales y otras fuentes, se presenta en la figura 9 el esquema de cómo se cometió el fraude:

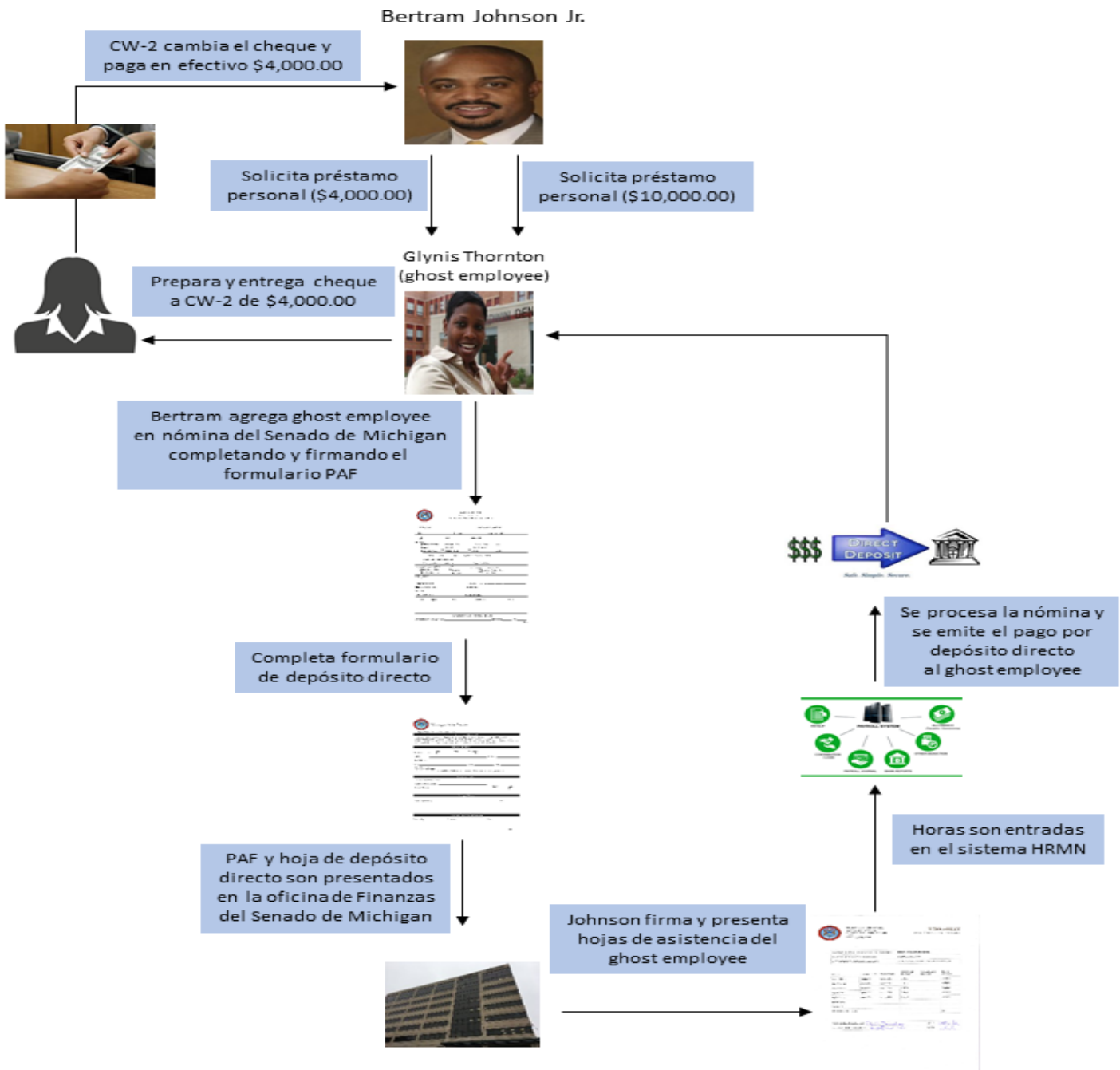


Figura 9: Esquema de Fraude

Sin duda alguna, el principal factor que permitió que el esquema de fraude se llevara a cabo, era el poder y la autoridad que el senador estatal y acusado Johnson, tenía para seleccionar y contratar empleados para su oficina en el estado de Michigan.

Esto nos muestra la falta de fiscalización que existe en las áreas del gobierno de cualquier país, facilitando de esta manera, los esquemas de fraude de cualquier índole y en cualquier jerarquía. Con el abuso de poder o el exceso de confianza, y mientras más autorizaciones o accesos tengan los perpetradores, más presión, oportunidad y justificación tendrán para cometer el acto.

## Sección 4: Informe del Caso

### Resumen Ejecutivo

De acuerdo a las circunstancias descritas en el caso de Bertram Johnson Jr., (2015), el Agente Especial Timothy R. Slater de la División del FBI de Detroit y en común y mutuo acuerdo con los fiscales federales J. Michael Buckley y Frances Carlson, contrataron los servicios de VDD Forensics Digital para analizar la imagen de un disco contenido en un USB Drive de 2 GB, esto, como parte de los esfuerzos y trabajos que se están llevando a cabo en la investigación del fraude cometido al estado de Michigan, en donde Johnson emplea a un *ghost employee* en la nómina pública únicamente para pagar una deuda de un préstamo personal que tenía con el co-conspirador.

Como parte de los servicios contratados, se realizará el análisis forense de la información de la imagen del disco incautado y contenida en un USB Drive de 2 GB. Estos resultados serán utilizados como evidencia en el proceso judicial contra el acusado. Como resultado del análisis la imagen del disco, se identificaron 3 documentos, en formato *Adobe Acrobat Document*, los formularios que se utilizaron para el ingreso en la nómina del Senado de Michigan del *ghost employee*. Será necesario investigar la evidencia aquí descrita con otros documentos oficiales para que el análisis sea completado en su totalidad.

Al completar el análisis forense, el dispositivo electrónico fue devuelto al Agente Especial del FBI, Timothy R. Slater.

### Objetivo

La Oficina de Investigación Federal (FBI), contrató los servicios de VDD Forensics Digital, para descubrir, analizar y recuperar información electrónica contenida en el USB Drive BJ20233, este dispositivo contiene una copia fiel y exacta del disco duro de la computadora de

Bertram Johnson JR., esto, con el objetivo de obtener posible evidencia y material que muestren que el senador empleó en su plantilla de empleados a un *ghost employee* cometiendo fraude en el cual fueron pagados más de \$23,000 en dinero perteneciente a los contribuyentes.

### **Alcance del Trabajo**

El 26 de noviembre de 2018, Timothy R. Slater, Agente Especial, División del FBI de Detroit, le hace entrega a la Sra. Vanessa De Jesús Díaz, Investigadora Forense de VDD Forensics Digital, del USB Drive identificado como BJ20233, el cual fue incautado como parte de la investigación del acusado Bertram Johnson Jr., en el Estado de Michigan. El propósito de este procedimiento es hacer un análisis del material y documentación para recopilar la evidencia de mayor relevancia y necesaria para este caso.

Conforme a los estándares de la industria forense, se realizó el proceso de análisis utilizando la herramienta *Forensic Toolkit*. Esta herramienta te permite hacer un escaneo en la máquina o dispositivo de interés, para buscar cualquier evidencia la cual es necesaria para ayudar a esclarecer cualquier tipo de investigación y se pueda preparar y entregar los hallazgos que serán utilizados en los procesos judiciales.

### **Datos del Caso**

1. Número de caso: 2:17-cr-20233-MFL-APP-1
2. Investigador: Vanessa De Jesús Díaz
3. Cliente: Ciudad de Michigan, Detroit
4. Representante del Cliente: Timothy R. Slater, Agente Especial del FBI

## Descripción de los Dispositivos Utilizados

A continuación, se detallan los dispositivos electrónicos utilizados durante el proceso investigativo:

1. Laptop HP Pavilion, Modelo 15cs0085cl, en donde se encuentran instaladas las herramientas que se utilizaron en el proceso forense.
2. USB Drive, de 2 GB, identificado como BJ20233

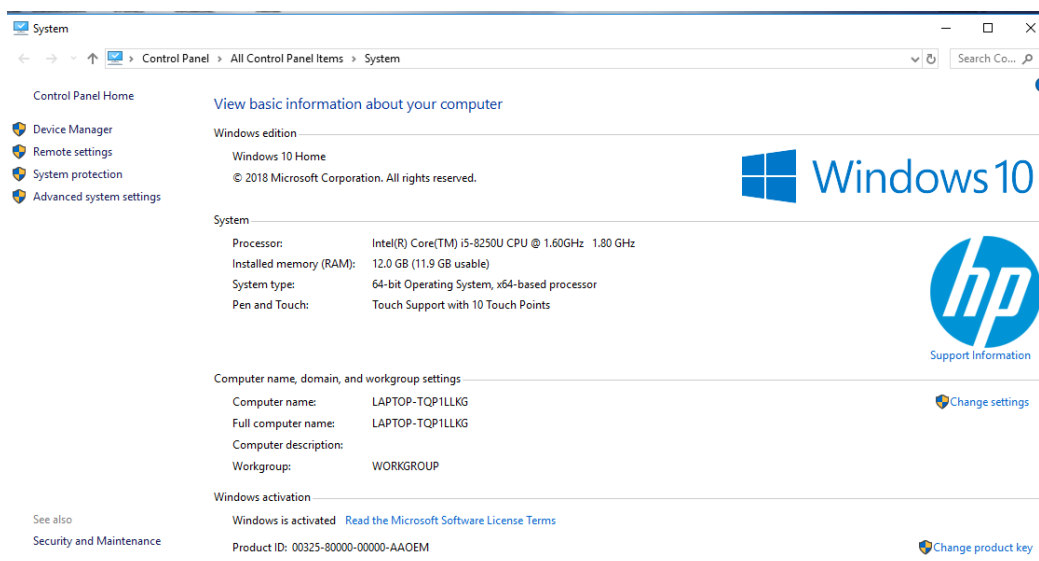


Figura 10: Imagen de la información de la computadora utilizada para este examen

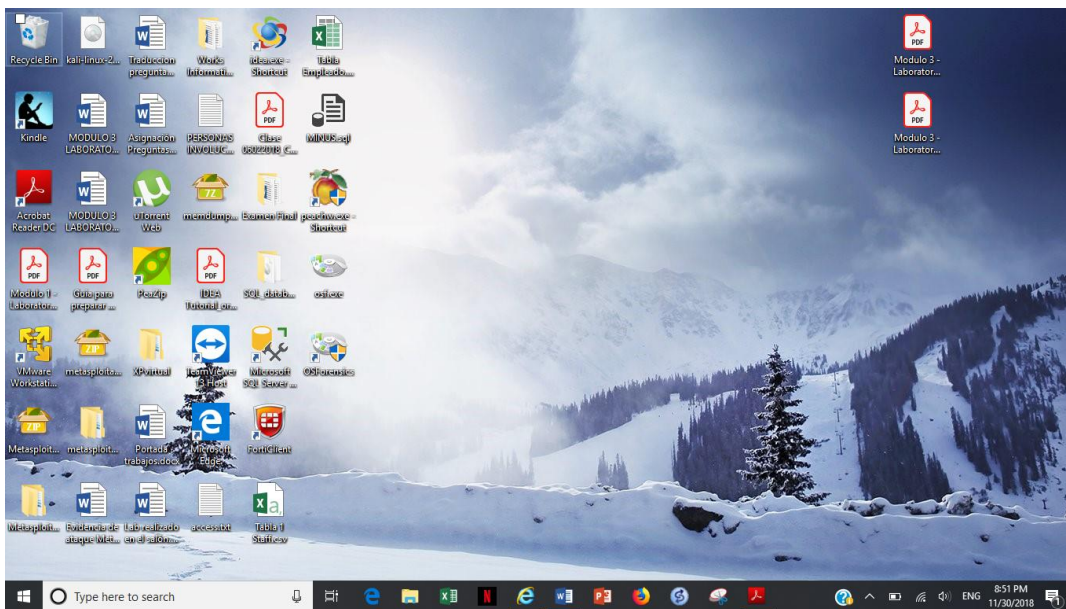


Figura 11: Imagen de la pantalla de la computadora forense



Figura 12: Imagen del USB Drive que se analizará

## Resumen de Hallazgos

El Perito Forense comienza a proveer un análisis de toda la evidencia. Es fundamental que realice el debido proceso de recopilar, almacenar y analizar la prueba correctamente, sin contratiempos para que pueda ser trabajada según es requerido por ley y la misma pueda ser admisible en los foros que se presente. A continuación, se presentan los hallazgos que han sido identificados en este análisis y que se encuentran contenidos en el USB Drive, identificado como BJ20233 con la herramienta *Forensic Toolkit*:

1. Documento en formato .pdf, *Adobe Acrobat*, el cual muestra la hoja de nombramiento utilizada por el Senado de Michigan (PAF), del *ghost employee*, efectivo el 28 de marzo de 2014, firmado por el Senador Johnson.

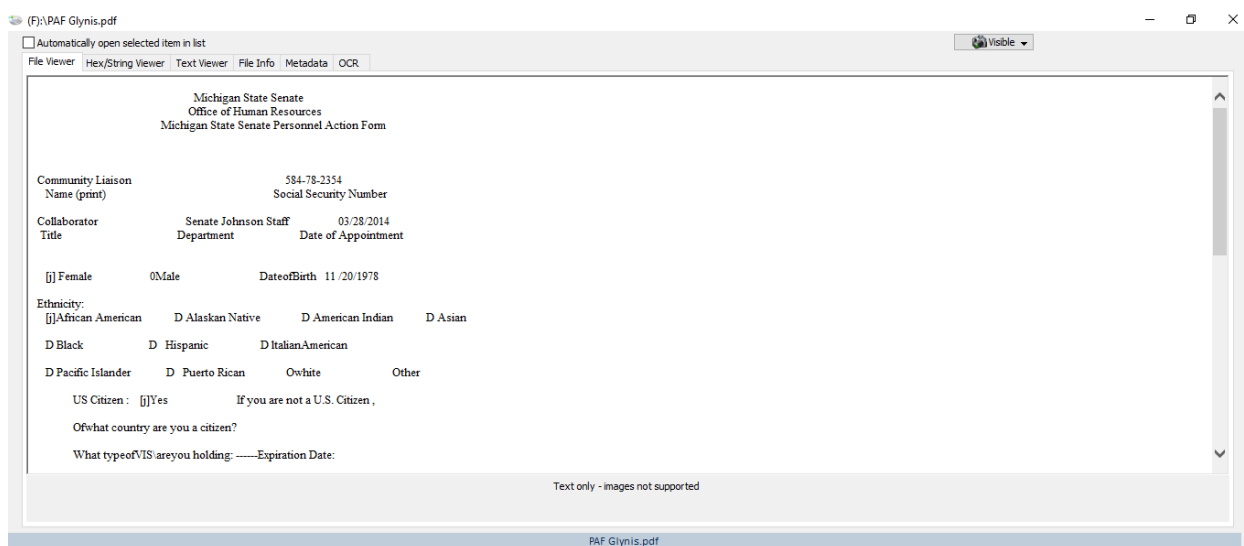


Figura 13: Imagen recuperada en Forensic Toolkit de Formulario del "PAF"



Michigan State Senate  
Office of Human Resources  
Michigan State Senate Personnel Action Form

Community Liaison 584-78-2354  
Name (print) Social Security Number

Collaborator Senate Johnson Staff 03/28/2014  
Title Department Date of Appointment

Female  Male Date of Birth 11/20/1978

Ethnicity:  
 African American  Alaskan Native  American Indian  Asian  
 Black  Hispanic  Italian/American  
 Pacific Islander  Puerto Rican  White Other

US Citizen:  Yes  No If you are not a U.S. Citizen,  
Of what country are you a citizen?

What type of VISI are you holding? Expiration Date:

Are you a Veteran?  Yes  No If you are a veteran, please specify:  
 Active Reserve  Disabled  Disabled Vietnam Era  
 Inactive Reserve  Retired  Vietnam Era

Home Address (and): 1997 Klingensmith Rd Unit 52 Bloomfield Hills Detroit, MI 48302-0278  
Telephone Number: 1(517)240-5060 E-Mail Address: communityliaison@gmail.com

Emergency Contact: James Smith Relationship: Brother in law  
Address: 12050 WOODWARD AVE. HIGHLAND PARK MI 48203  
Telephone Number: 1(517)850-9010 Business Number:

Education: Degree Master Date Earned Institution  
Master degree in Business Administration in University of Detroit Mercy  
Note: The employee will work 30 hours a week at a rate of \$22 per hour.

To be completed by the Immediate Supervisor  
Work Authorization Signature: Betty Lambert TB Sup. Initial: BT Date: 3/28/2014

Figura 14: Imagen "PAF"

2. Documento en formato .pdf, *Adobe Acrobat*, el cual muestra la hoja de autorización de depósito directo del *ghost employee*, el cuál fue entregado a la Oficina de Finanzas del Senado de Michigan.

(F:\)Direct Deposit Glynis.pdf

Michigan State Senate  
Employee Direct Deposit Agreement Form  
Authorization Agreement

I hereby request and authorize Michigan State Senate to deposit payments to the account provided below. In situations where a payment has been made in error, Michigan State Senate is authorized to correct that error. This agreement will remain in effect until Michigan State Senate receives a written notice of change or cancellation from me or my financial institution, or until I submit a new direct deposit form to the Accounts Payable Office.

Employee Information

New Cancellation  
Type of Authorization [Z] D  
Name Glynis Thornton ss ID # 584-78-2354

Street Address 1997 Klingensmith Rd Unit 52 Bloomfield Hills Phone 1(517)240-5060  
City Michigan state Detroit Zip 48302-0278  
Email address for notification of payment\* communityliaison@gmail.com

Text only - images not supported

Direct Deposit Glynis.pdf

Figura 15: Figura Imagen recuperada en Forensic Toolkit de Formulario de Depósito directo

The image shows a form titled "Michigan State Senate Employee Direct Deposit Agreement Form". It is divided into several sections: "Authorization Agreement", "Employee Information", "Account Information", "Employee Signature", and "For Accounts Payable Office Use Only".

**Authorization Agreement:** A statement of authorization to deposit payments to a specified account.

**Employee Information:** Includes fields for Name (Glynis Thornton), SS ID # (584-78-2354), Street Address (1997 Klingsmith Rd Unit 52 Bloomfield Hills), City (Michigan), State (Detroit), Zip (48302-0278), and Email address for notification of payment (communityliaison@gmail.com).

**Account Information:** Includes Name of Financial Institution (Western Fed Savings), Routing Number (221572702), and Account Number (123567988). It also has checkboxes for "Checking" (checked) and "Savings".

**Employee Signature:** A handwritten signature and the date 3/08/14.

**For Accounts Payable Office Use Only:** Includes fields for "Received By" (PA), "Signature" (Patricia Anderson), and "Date" (3/08/14).

Figura 16: Imagen formulario de depósito directo

3. Documento en formato .pdf, *Adobe Acrobat*, del timesheet del *ghost employee* de la primera semana de abril 2014, firmada y certificada por el Senador Johnson.

The image is a screenshot of a PDF document titled "Timesheet Glynis.pdf" viewed in a software application. The document content includes:

MICHIGAN STATE SENATE  
Binsfeld Office Building, 201  
Townsend Street, Lansing, Michigan, 48933  
Phone: 1 517-373-2400


TIME SHEET  
WEEK OF: 04/07/2014 - 04/11/2014

EMPLOYEE NAME: COMMUNITY LIAISON TITLE: COLLABORATOR  
EMPLOYEE NUMBER: 0000001111 STA TUS: ACTIVE  
DEPARTMENT: SENATE OFFICE SUPERVISOR: BERTRAM JOHNSON JR.

DATE	START TIME	REGULAR END TIME	OVERTIME HOURS	TOTAL HOURS	HOURS
04/07/2014	09:00AM	03:00PM	6HRS	6HRS	
04/08/2014	09:00AM	03:00PM	6HRS	6HRS	

Text only - images not supported

Figura 17: Imagen recuperada en Forensic Toolkit del timesheet


**MICHIGAN STATE SENATE**  
 Blodgett Office Building, 201  
 Townsend Drive, Lansing, Michigan  
 48933  
 Phone: 517/373-4400

**TIME SHEET**  
 WEEK OF: 04/07/2014 - 04/11/2014

EMPLOYEE NAME: COMMENT LIABON		TITLE: COLLABORATOR	
EMPLOYEE NUMBER: 000001111		STATUS: ACTIVE	
DEPARTMENT: SENATE OFFICE		SUPERVISOR: HERTRAM JOHNSON JR.	

DATE	START TIME	END TIME	REGULAR HOURS	OVERTIME HOURS	TOTAL HOURS
04/07/2014	09:00AM	03:00 PM	6 HRS		6 HRS
04/08/2014	09:00AM	03:00 PM	6 HRS		6 HRS
04/09/2014	09:00AM	03:00 PM	6 HRS		6 HRS
04/10/2014	09:00AM	03:00 PM	6 HRS		6 HRS
04/11/2014	09:00AM	03:00 PM	6 HRS		6 HRS
04/12/2014					
04/13/2014					
<b>WEEKLY TOTALS</b>					<b>30</b>

EMPLOYEE SIGNATURE: <i>Comment Liabon</i>	DATE: 04/11/14
SUPERVISOR SIGNATURE: <i>Hertram Johnson Jr.</i>	DATE: 11/04/14

Figura 18: Imagen Timesheet

## Cadena de Custodia

Con la cadena de custodia, se realiza el proceso de recopilar, almacenar, y analizar evidencia, de manera correcta para garantizar un proceso justo. Se debe llevar a cabo en el orden que se requiere ya que, si la misma se altera, se puede convertir en evidencia inadmisibles en el caso. A continuación, el detalle de la misma:

### 1. Primer evento:

- Descripción del evento: Evidencia entregada por Timothy R. Slater, Agente Especial del FBI y recibida por la Sra. Vanessa De Jesús Díaz, investigadora de VDD Forensics Digital. La evidencia consiste en: USB Drive BJ20233
- Evento verificado por: Sra. Vanessa De Jesús Díaz, Investigadora Forense y Timothy R. Slater, Agente Especial del FBI

- Fecha de comienzo: 30 de noviembre de 2018 1:00 p.m.
- Fecha de terminación: 30 de noviembre de 2018 1:10 p.m.
- Lugar de origen: Oficina del FBI de Detroit, del Agente Especial Timothy R. Slater
- Destino: Laboratorio Forense de VDD Forensics Digital

2. Segundo evento:

- Descripción del evento: Creación de número de caso y asignación de evidencia
- Evento realizado por Sra. Vanessa De Jesús Díaz, Investigadora Forense
- Asignar número de evidencia: E:1-2:17-cr-20233
- Fecha de comienzo: 30 de noviembre de 2018 1:20 p. m.
- Fecha de terminación: 30 de noviembre de 2018 1:24 p.m.
- Lugar de origen: Laboratorio Forense VDD Forensics Digital
- Destino: Laboratorio Forense VDD Forensics Digital

3. Tercer evento:

- Descripción del evento: Realizar el análisis de la evidencia para la redacción del informe que se le brindará a fiscalía
- Evento realizado por: Sra. Vanessa De Jesús Díaz, Investigadora Forense
- Número de evidencia: E:1-2:17-cr-20233
- Fecha de comienzo: 30 de noviembre de 2018 1:30 p.m.
- Fecha de terminación: 30 de noviembre de 2018 1:35 p.m.
- Lugar de origen: Laboratorio Forense VDD Forensics Digital

- Lugar de destino: Laboratorio Forense VDD Forensics Digital

4. Cuarto evento:

- Descripción del evento: Entrega de informe a Timothy R. Slater, Agente Especial del FBI
- Evento realizado por: Sra. Vanessa De Jesús Díaz, Investigadora Forense
- Número de evidencia: E:1-2:17-cr-20233
- Fecha de comienzo: 1 de diciembre de 2018 11:00 a. m.
- Fecha de terminación: 1 de diciembre de 2018 12:20 p.m.
- Lugar de Origen: Laboratorio Forense VDD Forensics Digital
- Lugar de Destino: Oficina del FBI de Detroit, del Agente Especial Timothy R. Slater

5. Quinto evento:

- Descripción del evento: Devolución de la evidencia a Timothy R. Slater, Agente Especial del FBI, identificada por E:1-2:17-cr-20233
- Evento verificado por Vanessa De Jesús Díaz, Investigadora Forense
- Número de evidencia: E:1-2:17-cr-20233
- Fecha de comienzo: 1 de diciembre de 2018 12:20 p.m.
- Fecha de Terminación: 1 de diciembre de 2018 12:26 p.m.
- Lugar de origen: Laboratorio Forense VDD Forensics Digital
- Lugar de Destino: Oficina del FBI de Detroit, del Agente Especial Timothy R. Slater

## Procedimiento

A continuación, se detallan los procedimientos realizados durante el transcurso de este análisis el cual contiene descubrimiento, adquisición, recuperación y preservación de la evidencia que fue encontrada

1. Procedimiento: Creación del Caso de imagen del archivo de evidencia E:1-2:17-cr-20233
  - a. Herramienta: *Forensic Toolkit*
  - b. Fecha de comienzo: 30 de noviembre de 2018 2:30 p.m.
  - c. Fecha de terminación: 30 de noviembre de 2018 2:35 p.m.
  - d. Descripción: Se crea una imagen del USB Drive entregado como evidencia # E:1-2:17-cr-20233

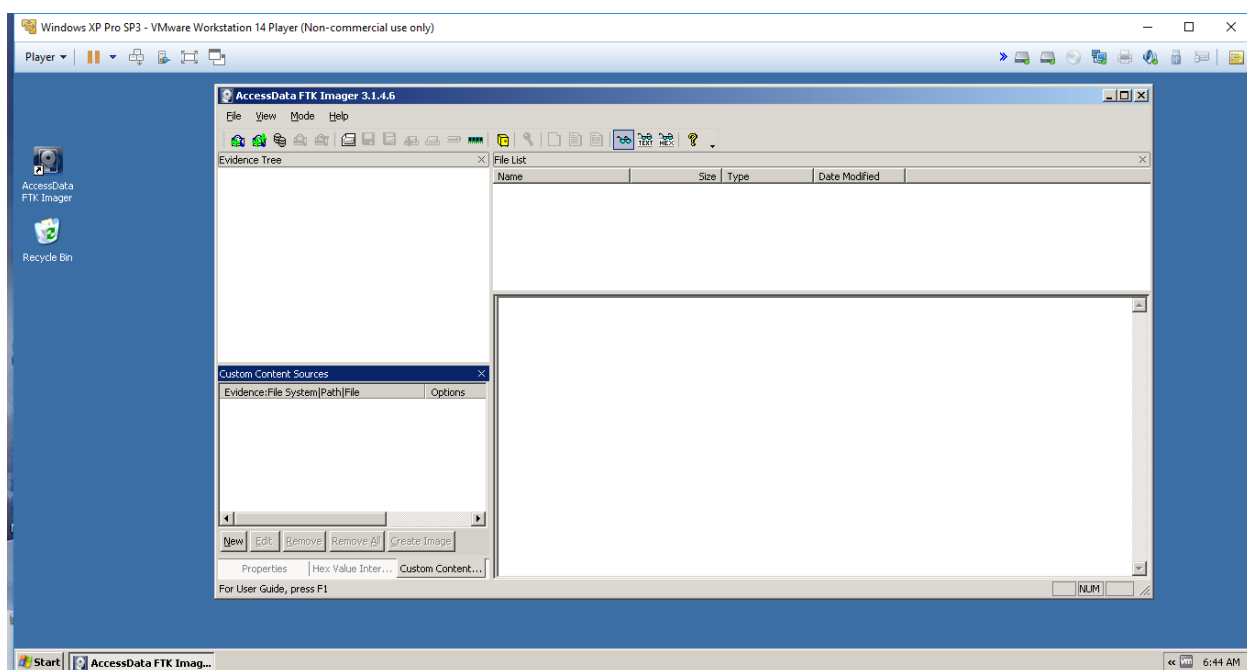


Figura 19: Imagen pantalla máquina virtual e inicio de FTK Imager

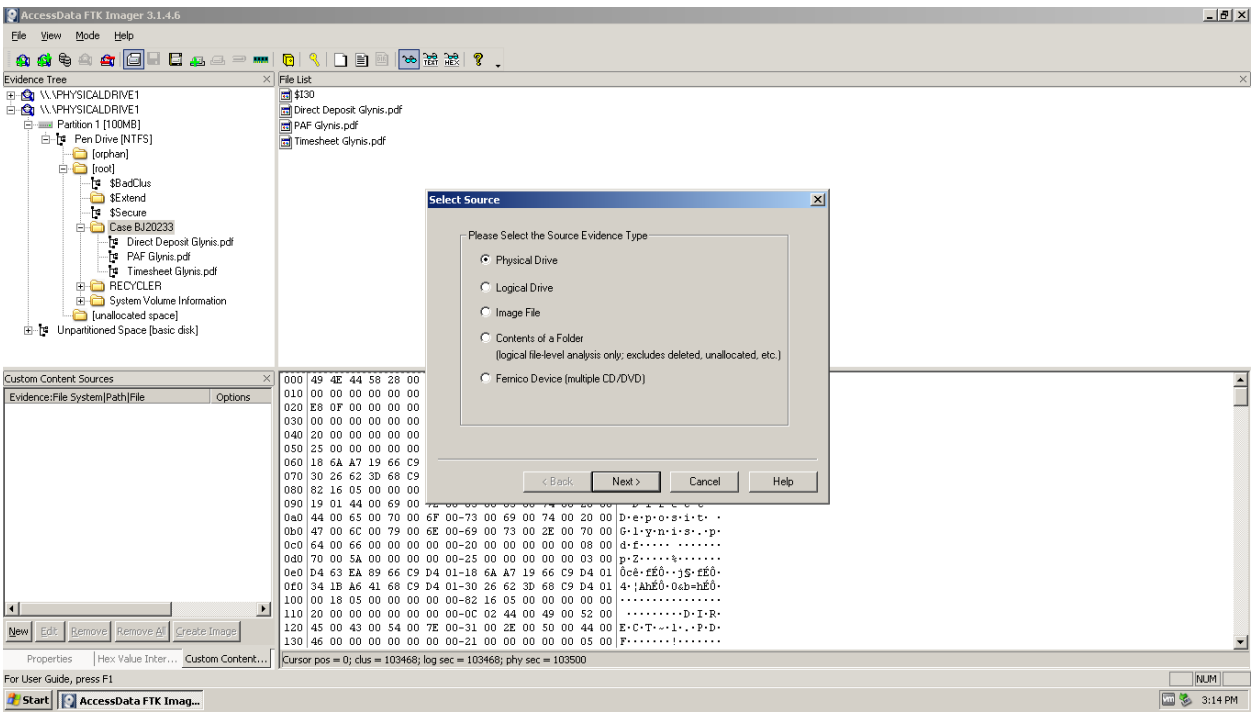


Figura 20: Selección del tipo de fuente de evidencia

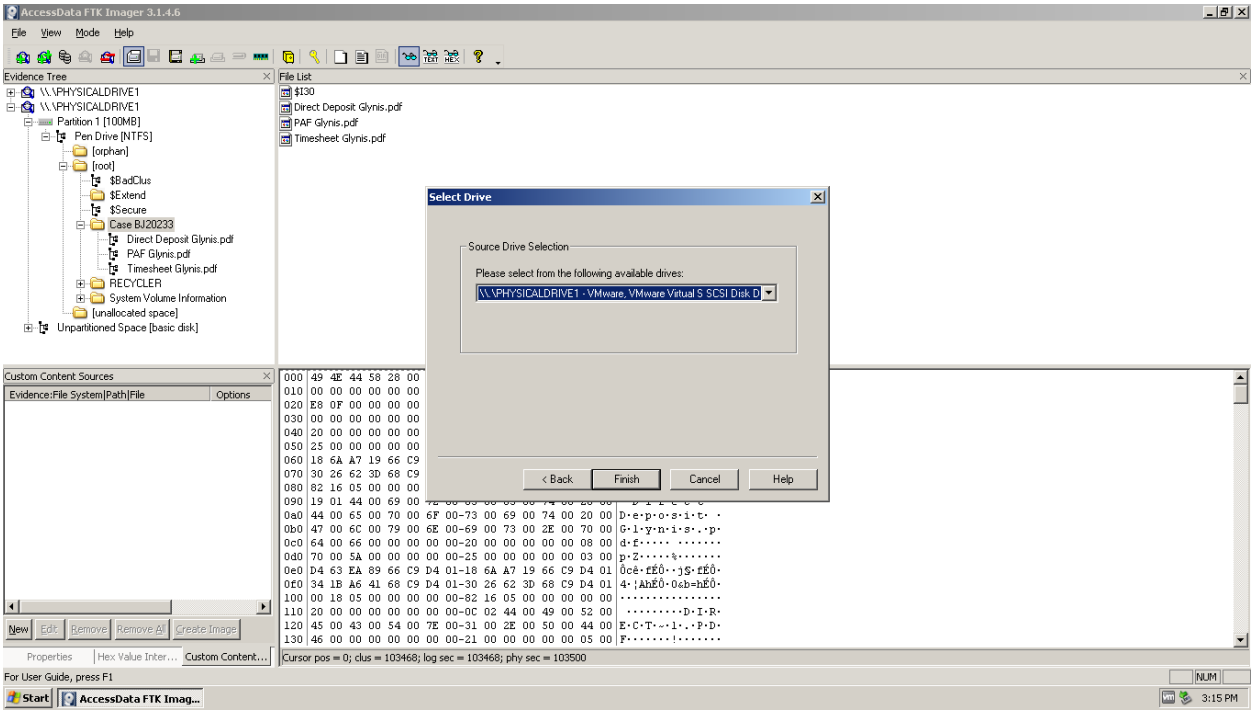


Figura 21: Selección de la unidad de origen

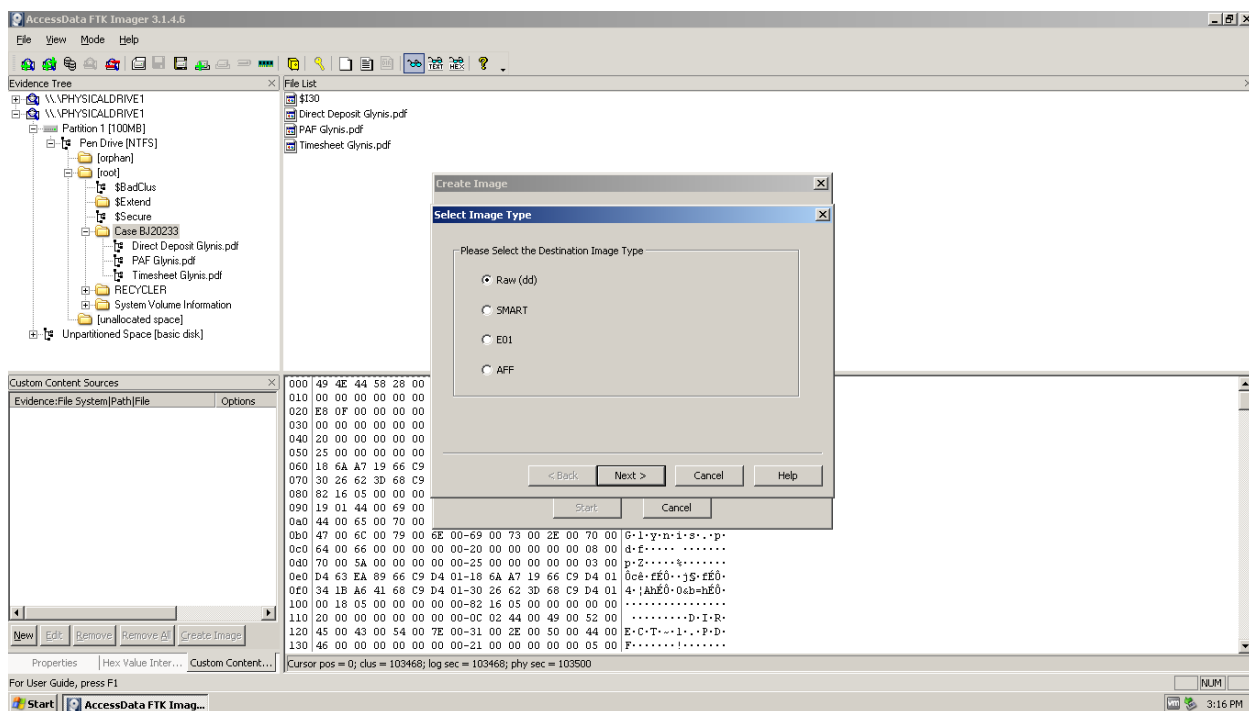


Figura 22: Selección del tipo de imagen

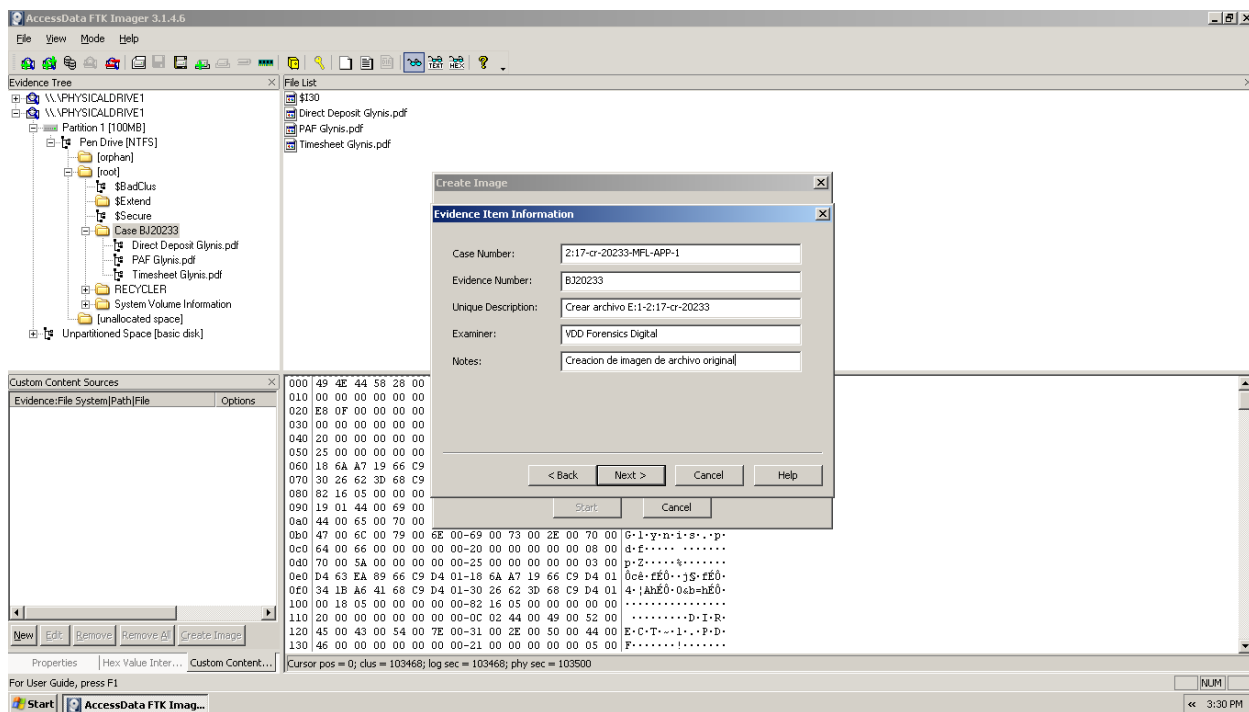


Figura 23: Información del elemento de evidencia



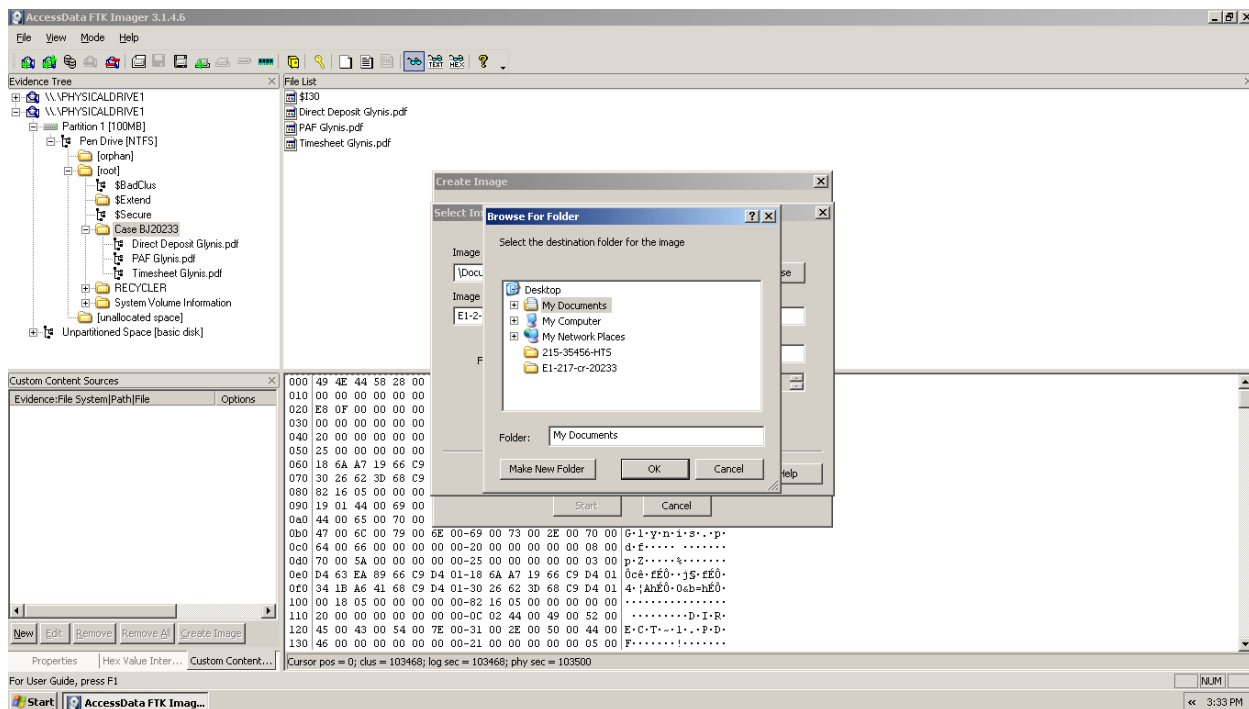


Figura 24: Selección de carpeta para guardar imagen

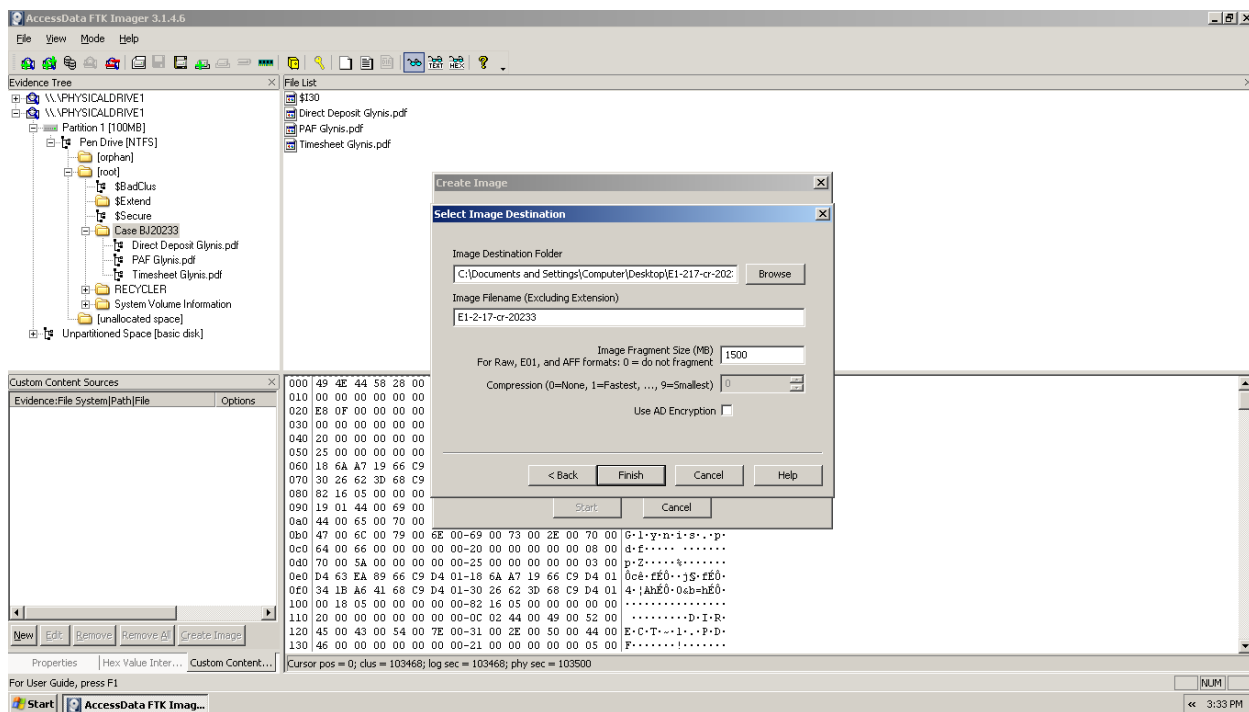


Figura 25: Selección de ubicación donde se guardará imagen

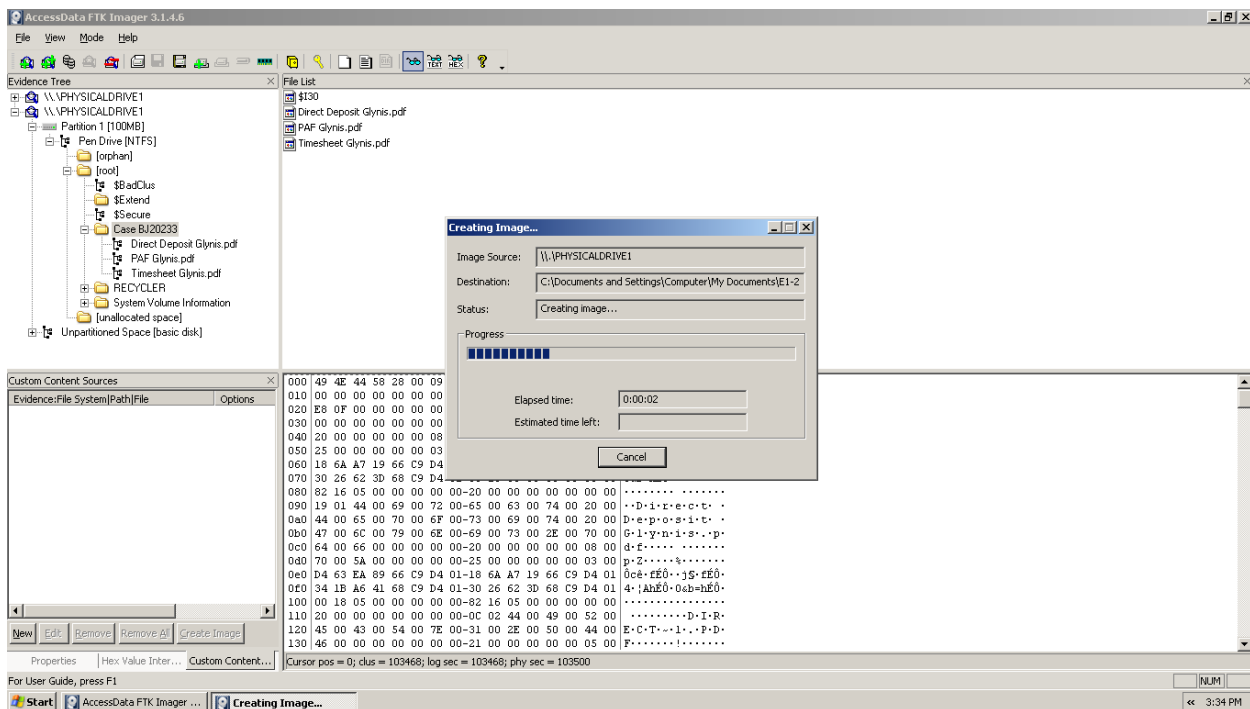


Figura 26: Creación de imagen

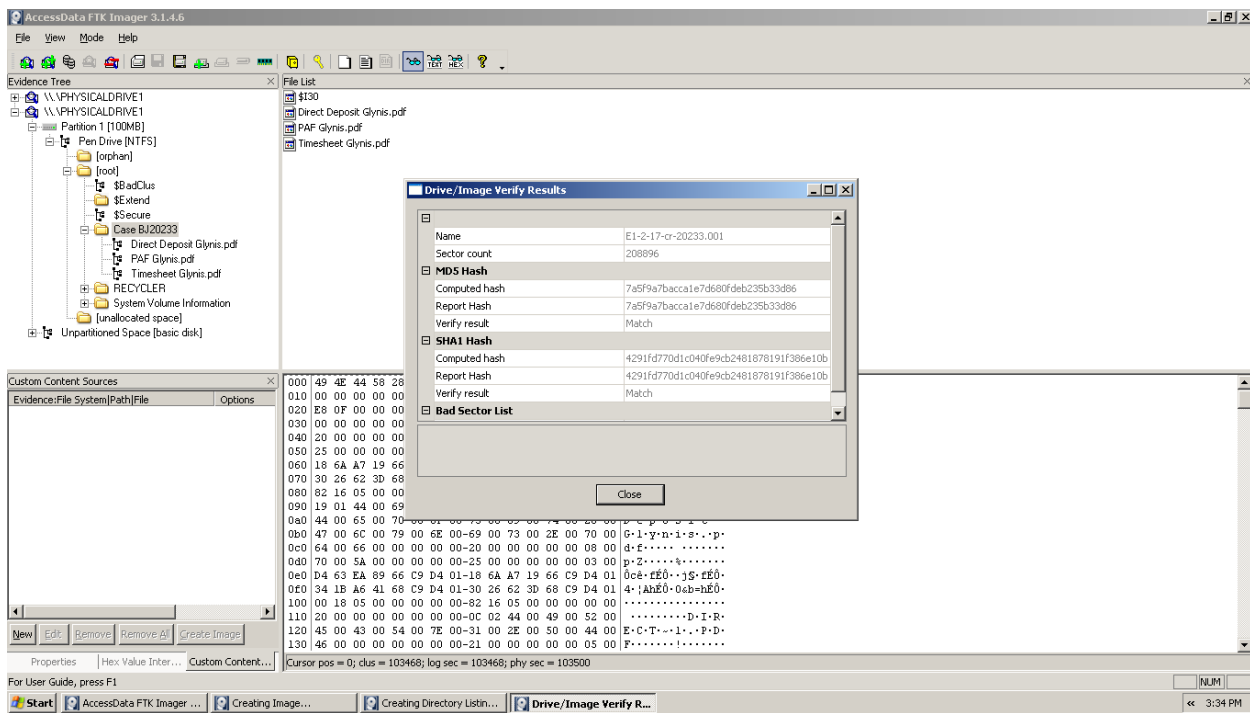


Figura 27: Resultado de los Hash Values del archivo creado

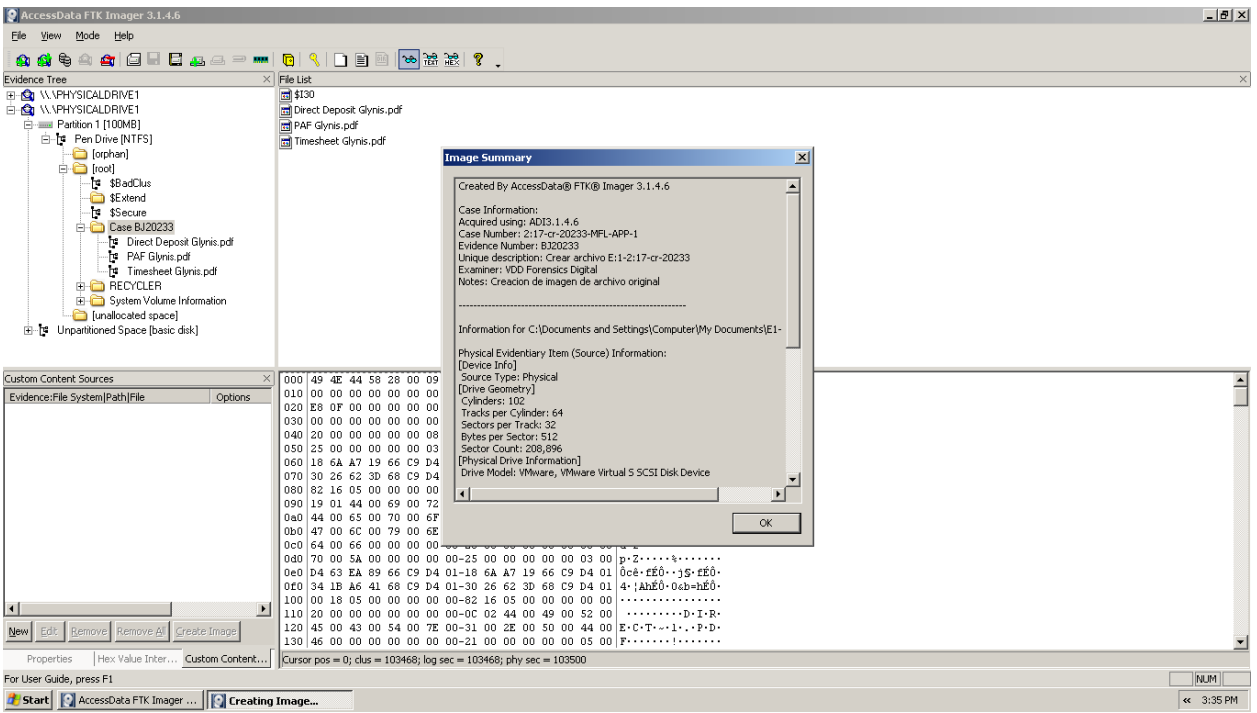


Figura 28: Resumen de la imagen creada

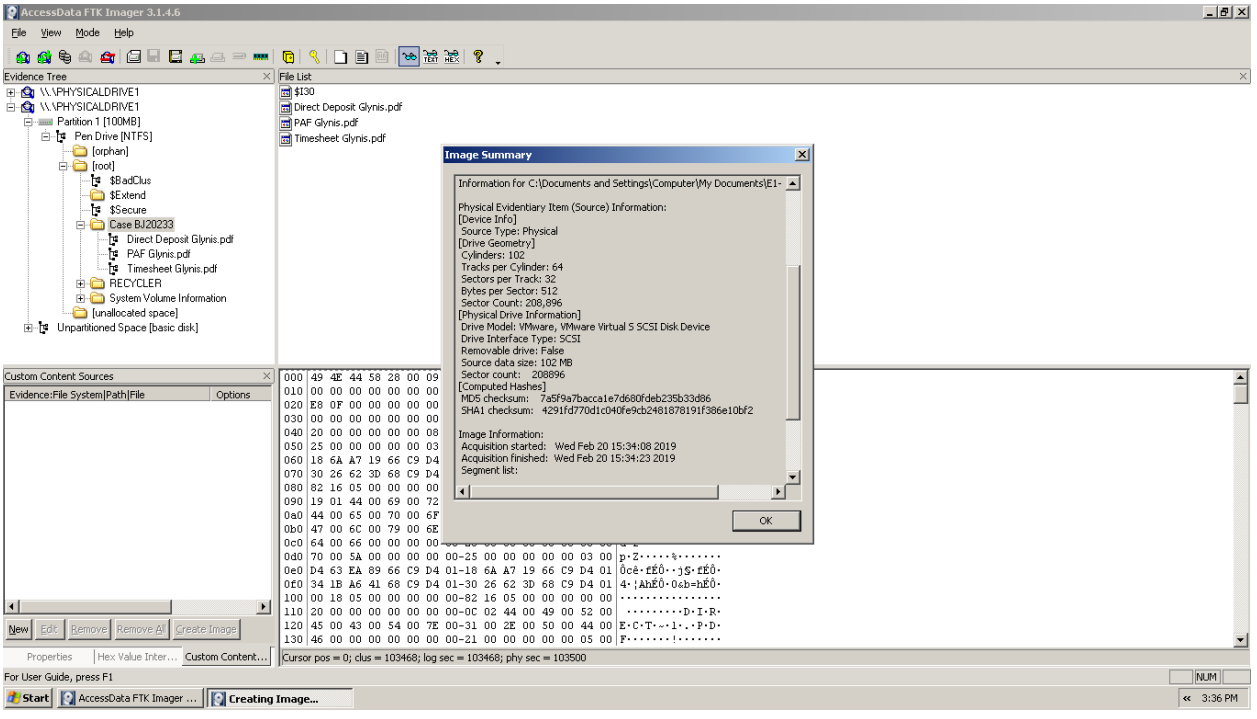


Figura 29: Verificación de Hashes y datos del archivo creado

2. Procedimiento: Análisis de la imagen del archivo creado
  - a. Herramienta: *Forensic Toolkit*
  - b. Fecha de comienzo: 30 de noviembre de 2018 2:36 p.m.
  - c. Fecha de terminación: 30 de noviembre de 2018 2:42 p.m.
  - d. Descripción: Se analiza la imagen del archivo de evidencia y la recuperación de 3 archivos

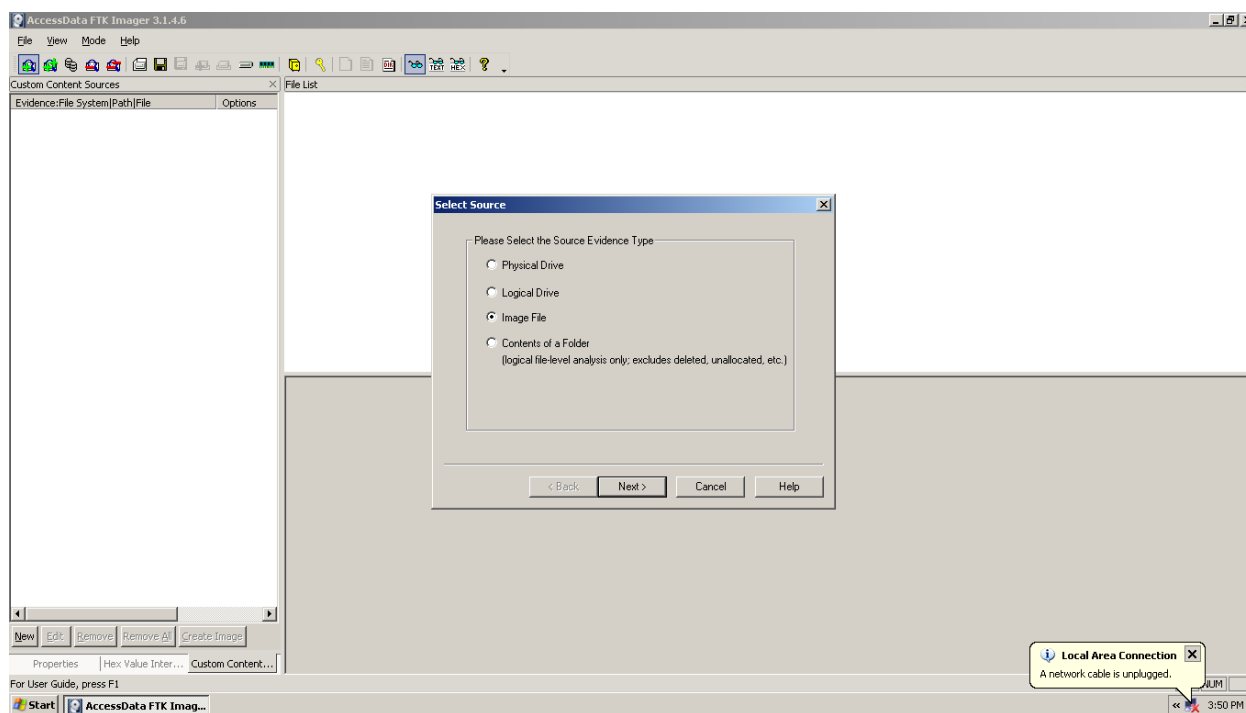


Figura 30: Seleccionar tipo de fuente de evidencia

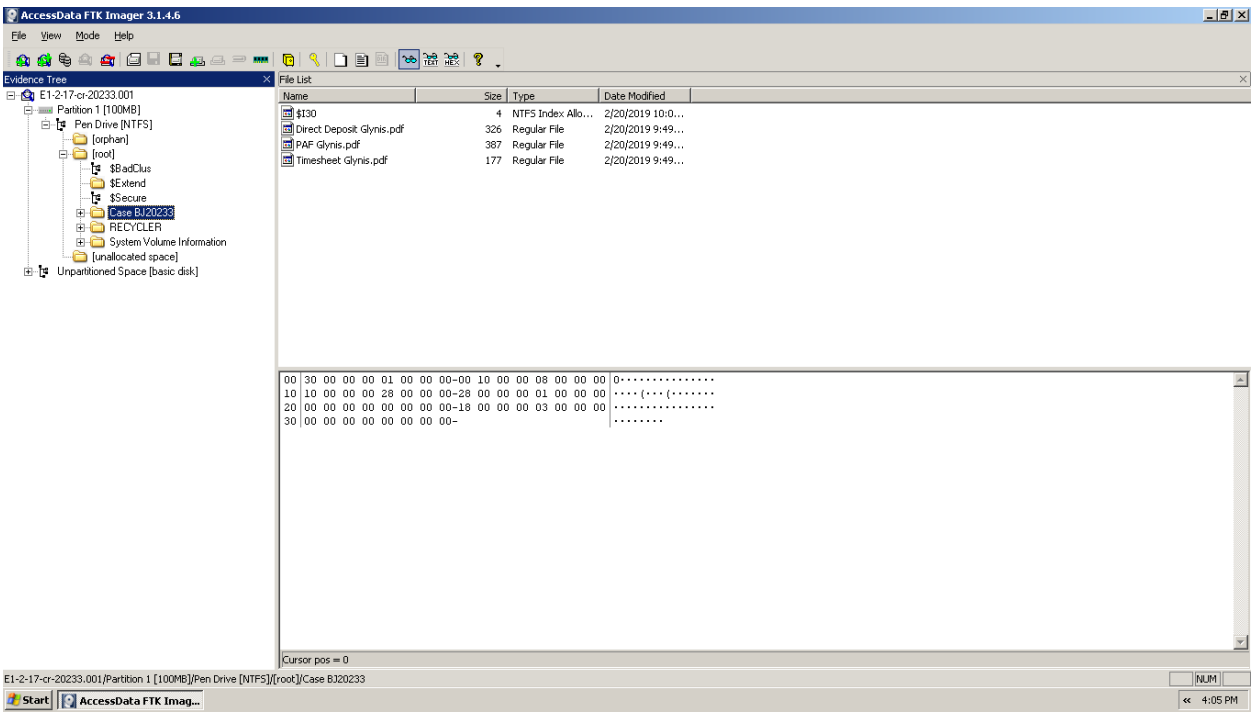


Figura 31: Evidencia para análisis

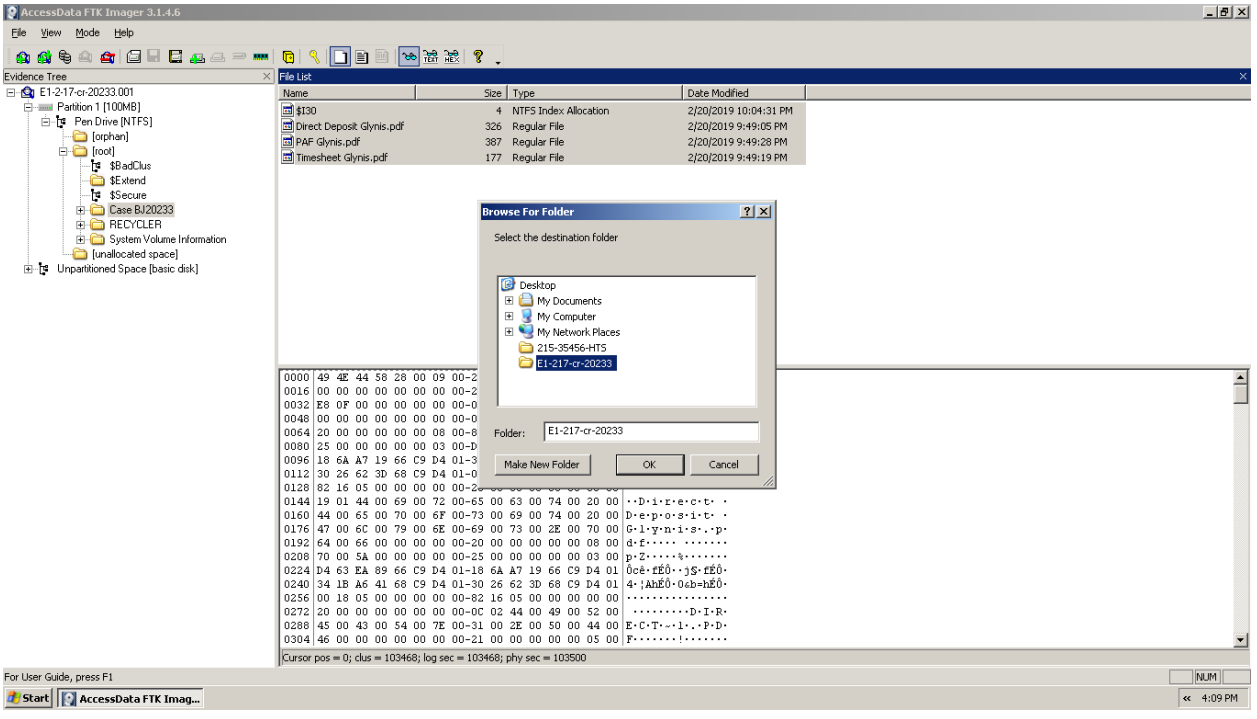


Figura 32: Transferencia de los 3 documentos encontrados

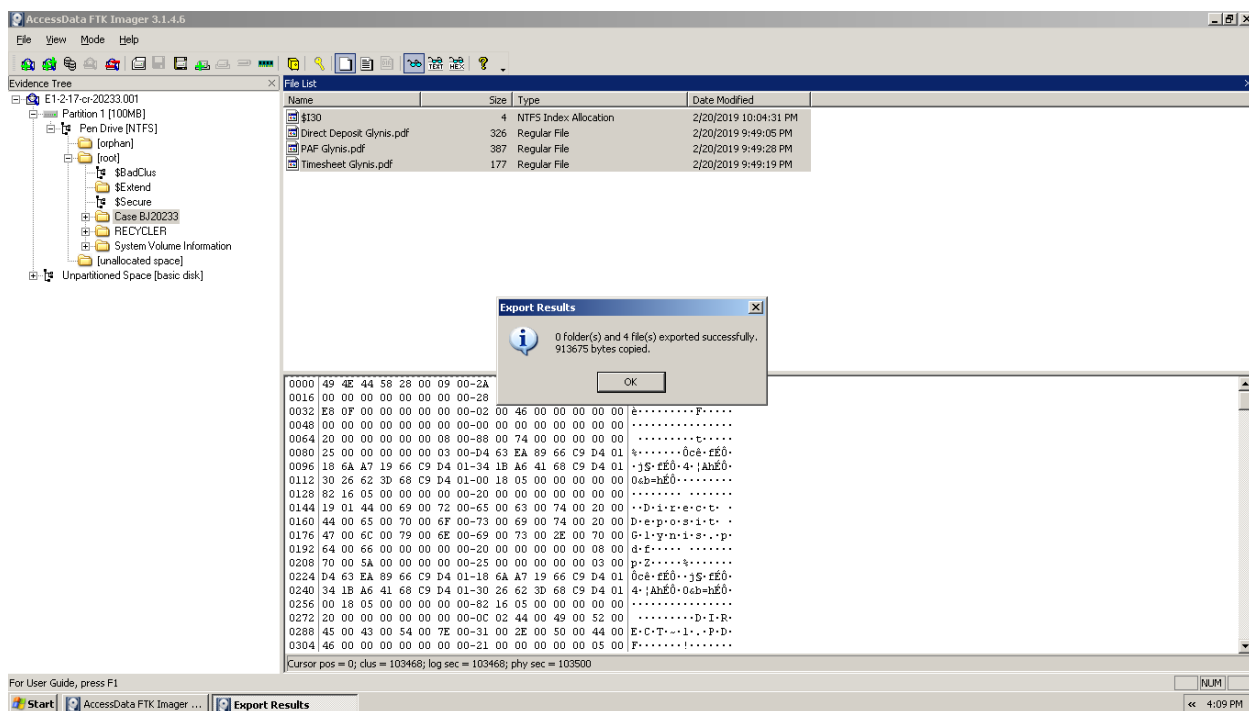


Figura 33: Transferencia de Hashes de los documentos encontrados

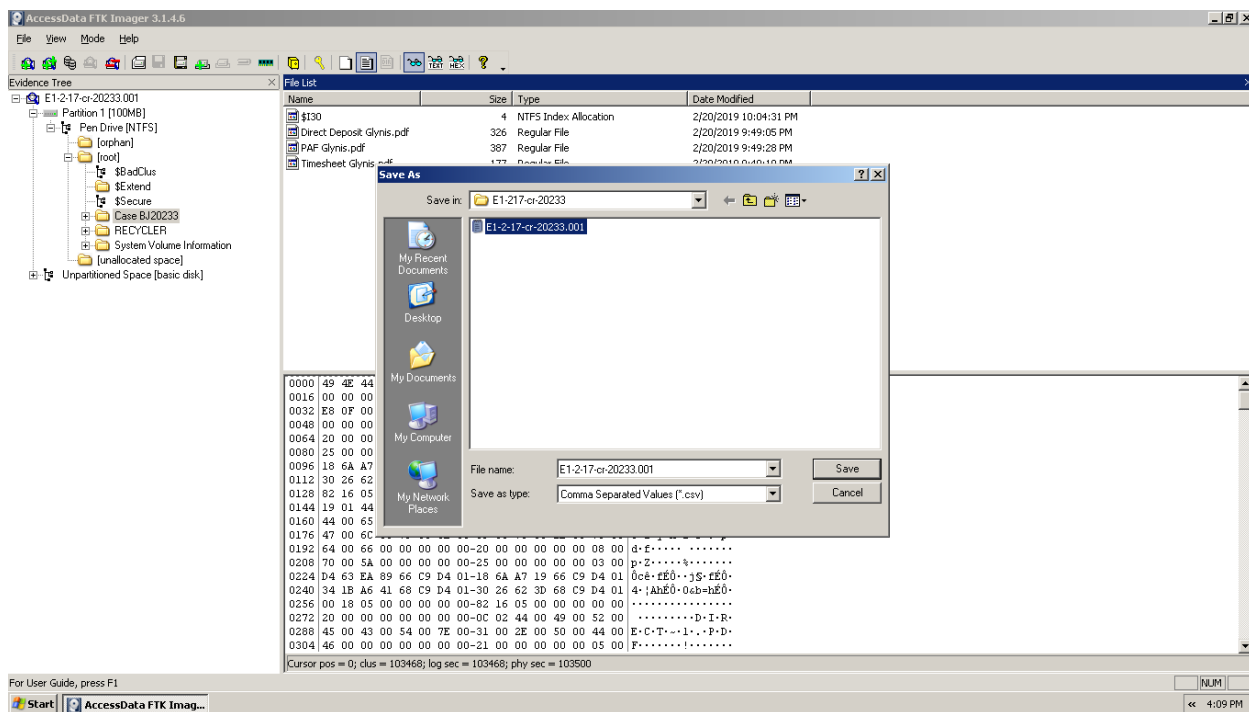


Figura 34: Evaluación del archivo del caso

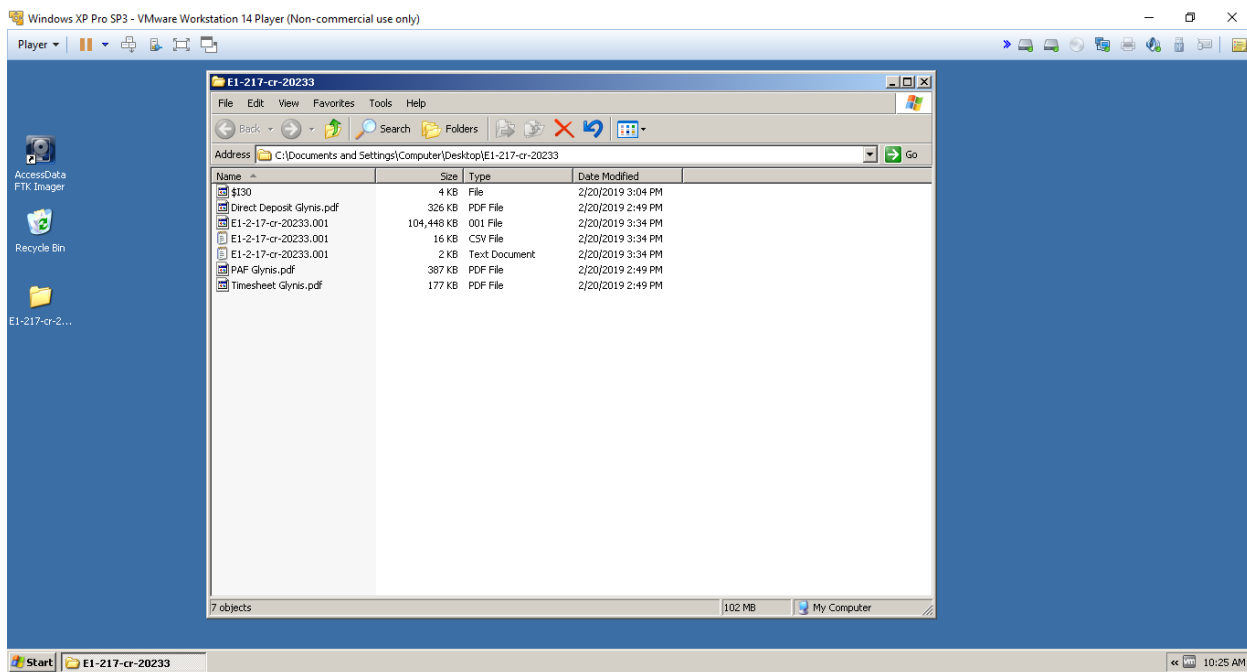


Figura 35: Datos contenidos en el expediente

## Conclusión

Luego de analizar los documentos que se encuentran contenidos en el USB Drive, identificado como BJ20233 con la herramienta *Forensic Toolkit*, estos reflejaron claramente, las evidencias relacionadas con el fraude y de las cuales se puede indicar que Bertram Johnson Jr., contrató a un ghost employee en su personal, cuando este ocupaba el cargo de senador. El *ghost employee* fue matriculado en el sistema de nómina que existe en la Oficina de Finanzas del Senado de Michigan. Todos los documentos fueron aprobados y firmados por el acusado.

Esta información puede ser corroborada o comparada con otros archivos que sean considerados durante esta investigación, sin embargo, la evidencia aquí descrita, nos corrobora el esquema de fraude al cual está siendo relacionado el acusado Bertram Johnson Jr.

## Sección 5: Discusión del Caso

Según se desprende en el acuerdo de culpabilidad del caso United States of America v. Bertram Johnson Jr. (2017), y de la evidencia analizada por parte de fiscalía en el caso: 2:17-cr-20233-MFL-APP-1, el acusado se declara culpable y se le imputa de cometer robo de un programa financiado por el gobierno federal en contra del Distrito de Michigan. Del 28 de marzo de 2014 al 2 de enero de 2015 el acusado era Senador del Gobierno del Estado de Michigan y durante ese periodo, obteniendo por el fraude cometido, aproximadamente \$23,133.89, contratando oficialmente a un *ghost employee* como parte de sus empleados senatoriales para poder pagar de este modo, una deuda personal.

Luego de haber realizado un análisis de la evidencia encontrada en e la investigación forense y siguiendo como guía, estrictas medidas de seguridad y confidencialidad, se puede obtener un panorama más claro de lo sucedido y concluimos lo siguiente:

- Se puede confirmar que el acusado contrató a un *ghost employee* nombrándolo como “*Community Liaison*” certificando y firmando hojas de asistencias de trabajos no realizados por el periodo descrito en el caso.
- Se puede confirmar que el *ghost employee*, fue nombrado bajo los empleados del Senador Johnson, completando el documento *Michigan State Senate Personnel Action Form* conocido por sus siglas como “PAF” de las Oficinas del Senado de Michigan.
- Se puede confirmar que el *ghost employee*, completó el formulario de depósito directo y fue ingresado en el sistema de nómina de las Oficinas del Senado de Michigan para que se efectuaran los pagos por trabajos no realizados, a su cuenta



bancaria, los cuales fueron parte del fraude perpetrado durante el periodo descrito en el caso.

- Se puede confirmar que el acusado abusó de su poder y puesto de confianza para defraudar las Oficinas de Gobierno del Senado de Michigan.

## Sección 6: Auditoría y Prevención

### Introducción

Una herramienta fundamental para las organizaciones es la auditoría. Durante este proceso, el cual debe ser uno objetivo e imparcial, se examinan las operaciones de la empresa y de esta manera poder evaluar su eficiencia, tomando en consideración el cumplimiento de las leyes aplicables. Existen dos (2) tipos de auditoría, las cuales son: (a) auditoría externa, la cual se realiza por personal que no pertenece a la empresa; por lo general, es una firma de Contadores Públicos Autorizados, que emiten una opinión objetiva del funcionamiento de la misma; y (b) auditoría interna, la cual es realizada por el personal de la empresa; y su objetivo es revisar el funcionamiento de la misma, si los procesos se llevan a cabo de acuerdo a los reglamentos y políticas establecidas para luego, hacer recomendaciones en aquellas áreas que así lo ameriten.

El sistema de control interno se compone de cinco (5) componentes relacionados entre sí, los cuales se describen a continuación:

1. **Ambiente de control** – los estándares y procedimientos que sirven como guía para que se cumplan los controles internos dentro de la organización. Esto incluye la integridad y cultura ética de la organización
2. **Evaluación de riesgo** – la identificación de posibles eventos que pueden ser tanto internos como externos y que pueden afectar de manera adversa a los logros y objetivos de la organización.
3. **Actividades de control** – los procedimientos y políticas que aseguran los logros y objetivos de la organización.

4. **Información y comunicación** – proceso de compartir, proveer y obtener información ya sea de fuentes externas o internas y que son necesarias para cumplir con los objetivos de la organización y con los requerimientos de las agencias reguladoras.
5. **Monitoreo** – consiste de una evaluación continua del funcionamiento del sistema de la organización.

### **Resumen de Hallazgos**

En el transcurso de la investigación del caso, resaltaron varios elementos que reflejaron el fraude perpetrado por Bertram Johnson Jr. Fue el puesto de confianza, el abuso de poder y la autoridad del ex senador Johnson, que le permitieron perpetrar este fraude. Como tal, el ex senador Johnson, tenía el privilegio de contratar y supervisar sus empleados lo que le facilitó la manipulación de los documentos, entiéndase como; completar el formulario de nuevo ingreso de personal del Senado de Michigan conocido por sus siglas como “PAF”, completar la hoja de depósito directo del *ghost employee* el cual fue sometido a la Oficina de Finanzas y la creación de hojas de asistencia las cuales fueron certificadas y aprobadas por el.

Durante este proceso y luego de identificar las deficiencias que ayudaron a cometer este fraude, se detallan los pasos que se deben seguir como guía para detectar anomalías en una nómina:

1. Pagos de empleados por fecha de cheque
  - Enfoca los periodos de auditoria en periodos de fecha de mayor actividad
  - Reporte de registro de nómina
2. Dividir en sueldos por hora, horas trabajadas, cantidad neta de paga y horas extras
  - La auditoría se centra en tasas altas de pago

- Reporte de registro de nómina
3. Comparar el año actual con el archivo de nómina del año anterior para detectar empleados adicionales y/o despedidos
    - Se hace énfasis en los empleados nuevos y despedidos de acuerdo a los registros de personal. Los nuevos empleados deben revisarse para determinar si existen *ghost employees* que reciben pagos fraudulentos
    - Reporte de registro de nómina
    - Archivo de personal de empleados
  4. Comparar empleados reportados por sistema de ponches con el sistema de nómina
    - Separar las diferencias de empleados entre el registro de ponches y el registro de nómina. El enfoque debe estar en los empleados que se encuentran en el registro de nómina y que no aparecen sus ponches lo cual indica que pudo haber sido agregado fraudulentamente.
    - Reporte de registro de nómina
    - Registro de ponches
  5. Comparar los archivos de data de nómina con los archivos de datos de recursos humanos para buscar las diferencias entre ambos
    - Verificar los acuerdos de nombramiento entre los dos archivos para identificar aquellos pagos que no estén autorizados
    - Reporte de registro de nómina
    - Archivo de personal de empleados
  6. Extraer todos los pagos de empleados sin deducción/impuestos retenidos

- Identificar pagos sin descuentos de deducciones/impuestos que por lo regular son los más propensos al fraude
  - Reporte de registro de nómina
7. Extraer todos los empleados que no contengan seguro social
- Reporta los posibles *ghost employees* que no están autorizados a los pagos. Regularmente, el perpetrador deja este campo en blanco o lo identifica con series de números como: 999999999
  - Reporte de registro de nómina
  - Archivo de personal de empleados
8. Extraer los empleados que han recibido pagos después de su fecha de terminación
- Reporta los pagos no autorizados a empleados despedidos que puede estar realizando el posible perpetrador
  - Reporte de registro de nómina
  - Archivo de personal de empleados
9. Extraer empleados sin nombre
- Informa sobre la posibilidad de que los pagos no autorizados o los pagos realizados se impriman en blanco para luego ser completado por el perpetrador
  - Reporte de registro de nómina
  - Archivo de personal de empleados
10. Secuencia duplicada de los números de seguro social que son pagados en el mismo periodo de pago

- Lista de los posibles pagos duplicados a empleados que los cuáles son más propensos al fraude
- Reporte de registro de nómina
- Archivo de personal de empleados

11. Secuencia duplicada en los números de depósitos directo pagados en el mismo periodo de pago

- Lista de posibles pagos duplicados los cuáles tienden a ser los más propensos al fraude
- Reporte de registro de nómina
- Archivo de personal de empleados

12. Secuencia posible de pagos duplicados basados en un valor absoluto en el pago neto y la fecha de cheque

- Lista de posibles pagos duplicados a empleados los cuáles tienden a ser los más propensos
- Reporte de registro de nómina

13. Secuencia duplicada en direcciones postales pagados en el mismo periodo de pago

- Lista de posibles pagos duplicados a empleados los cuáles tienden a ser los más propensos
- Reporte de registro de nómina

14. Extraer usuarios que pueden emitir cheques de pago y también agregar nuevos empleados en el sistema nómina y de ponches

- Los usuarios que pueden entrar nuevos empleados, entrar sus horas y generar los cheques, se convierte en un problema por no existir una segregación de tareas y se presta para cometer el fraude
- Reporte de registro de nómina
- Archivo de los accesos de usuarios
- Archivo de los accesos de usuarios al sistema de ponches
- Archivo de los accesos de usuarios al sistema de ponches

15. Calcular la nómina promedio por empleado y clasificar del más alto al más bajo

- Informe de pagos de empleados que son altos y posiblemente no autorizados
- Reporte de registro de nómina

16. Comparar los archivos del año actual con el año anterior para detectar cambios en sueldos de empleados

- Reporte de registro de empleados
- Archivo de personal de empleados

17. Recalcular pagos netos y brutos

- Recalcular el pago neto y bruto de acuerdo a los nombramientos de los empleados. Cualquier diferencia puede indicar un débil control en el sistema o que un pago ha sido ajustado de manera fraudulenta
- Reporte de registro de nómina

## Recomendaciones

1. En el caso de los accesos, los mismos deben ser segregados de acuerdo a las funciones de cada empleado. Cada uno de los usuarios deberá ingresar los datos en el sistema y su contraseña validará su autorización de entrada. De esta manera, al momento de hacer una auditoría, se verán reflejados todos los cambios hechos en el sistema por usuario.
2. Los registros de personal deben mantenerse independientemente de la nómina y el departamento de personal debe verificar cualquier cambio a la nómina.
3. La organización deberá periódicamente verificar la nómina con los registros de personal de empleados despedidos y los no autorizados.
4. Deben tener un empleado independiente de la función de nómina para que ejecute periódicamente un informe para las personas que carecen de información personal, tal como el seguro social, dirección, aquellos que no contengan deducciones o impuestos definidos, entre otros.
5. Realizar periódicamente una comparación de los gastos de nómina y revisar las distribuciones de horas que se estén registrando a las actividades correspondientes para que cada supervisor valide la información para validar que concuerde con las cantidades presupuestadas.
6. Deberán existir segregaciones de funciones tales como; persona encargada de entrar al empleado nuevo, persona encargada de entrar cambios y mantener los datos de la nómina y otra persona encargada de validar y aprobar, y distribución de cheques.
7. En el caso de depósitos directos, se debe ejecutar un informe en cada período de pago para revisar e identificar anomalías.



**Opinión de Auditoría**

Después del análisis de la evidencia encontrada, se confirma que las Oficinas del Senado de Michigan tiene una estructura de control interno deficiente ya que no cuentan con los mecanismos necesarios para la detección de empleados de nuevo ingreso y que son nombrados por el personal de confianza e ingresados al sistema de nómina, sin la debida verificación y validación por la oficina de Recursos Humanos. Esto permitió que por aproximadamente 10 meses, se hicieran pagos fraudulentos a un empleado que nunca llevo a cabo sus funciones.

## Sección 7: Conclusión

En este trabajo investigativo se han reflejados las vulnerabilidades que existen en el sector público, específicamente en las áreas de mayor jerarquía, ya que es en este nivel en donde mayor ausencia de controles y supervisión se encuentran. Como hemos descrito anteriormente, el ex senador Bertram Johnson del senado de Michigan, tenía la flexibilidad de contratar al personal que trabajaría bajo su mando, esto sin existir ninguna validación o un proceso establecido por un reglamento de personal en donde las políticas son más estrictas y conlleva varios pasos al momento del reclutamiento y nombramiento de un nuevo empleado. El reglamento de personal, se rige por las leyes establecidas de acuerdo al estado o lugar en donde se encuentra la organización y sus normas básicas deben ser como, por ejemplo; publicar las plazas vacantes por medio de convocatorias en anuncios públicos, internet y otros medios lo cual en lo que respecta a este caso, nunca existió por medio de Johnson ni de su oficina, porque nunca fue divulgada la necesidad de contratar algún empleado para una plaza en particular. Esto es reflejo de irregularidades que nos pueden indicar la intención de cometer un acto ilegal.

El próximo paso para el reclutamiento de personal en el sector público y que debe ser llevado a cabo única y exclusivamente por la Oficina de Recursos Humanos de la organización, es evaluar cada una de las solicitudes que han sido recibidas para la plaza anunciada para revisar que las mismas cumplan con los requisitos mínimos del puesto y aquellas que no, para luego, asignar las puntuaciones que serán medidas de acuerdo a su experiencia laboral, académica y técnica y otros factores de acuerdo a los requerimientos que se estén solicitando. Luego de esto, los candidatos que se consideren elegibles, pasaran a un registro y de ahí, se debe proceder con el proceso de entrevistas de los candidatos para que el personal de la organización pueda hacer el

escogido del nuevo empleado. De esta manera, el proceso es uno organizado y disminuye la posibilidad de que se contraten empleados fantasmas para cometer fraude.

Se puede concluir, que para evitar estos tipos actos, no importa el rango ni el puesto que tenga el posible perpetrador, se deben mantener controles establecidos en las organizaciones, independientemente del sector; público o privado, para que no exista el abuso de poder y de confianza que es en la mayoría de los casos, el punto clave para la comisión de actos irregulares.

Es en muchas ocasiones y recae en las organizaciones la responsabilidad, por no realizar los cotejos necesarios y como en este caso, no validar la información sometida por el ex senador para el nombramiento del empleado fantasma. Todas las organizaciones deben ser más proactivos para minimizar riesgos futuros que se convierten en pérdidas que pueden ser millonarias en muchos casos y que afectan como es en este escenario, al contribuyente por ser en el sector público.

Cabe mencionar que la conducta humana, es un factor determinante ya que, si analizamos este caso, pudo existir como hemos mencionado, abuso de autoridad y un poco de falta de segregación de tareas ya que el ex senador, reclutaba, sometía documentación falsa como; solicitud de nuevo ingreso, hojas de asistencia las cuales certificaba y firmaba el mismo para luego someter a la Oficina de Finanzas para la tramitación del pago correspondiente. Al contar con esta flexibilidad, tuvo el escenario perfecto para perpetrar el acto de fraude y poder de esta manera, solucionar su problema personal y pagar su deuda de dinero con fondos públicos y pertenecientes a un programa federal del estado de Michigan.

## Sección 8: Referencias

Antilavado de Dinero. (2017, 13 marzo). ¿Qué se entiende por corrupción y qué por fraude financiero? Recuperado de <http://www.antilavadodedinero.com/antilavadodedinero-entrevistas-articulo.php?id=435&title=que-se-entiende-por-corrupcion-y-que-por-fraude-financiero>

Association of Certified Fraud Examiners, Inc. (2018a). Report to the Nations 2018 Global Study on Occupational Fraud and Abuse. Recuperado de [https://www.acfe.com/uploadedFiles/ACFE\\_Website/Content/rtnn/2018/RTTN-Government-Edition.pdf](https://www.acfe.com/uploadedFiles/ACFE_Website/Content/rtnn/2018/RTTN-Government-Edition.pdf)

Association of Certified Fraud Examiners, Inc. (2018b). Using Data Analytics to Detect Fraud. Recuperado de [https://www.acfe.com/uploadedFiles/ACFE\\_Website/Content/review/da/07-Tests-for-Payroll-and-Expense-Reimbursement.pdf](https://www.acfe.com/uploadedFiles/ACFE_Website/Content/review/da/07-Tests-for-Payroll-and-Expense-Reimbursement.pdf)

Auditool.org. (2014, 24 septiembre). 14 Tipos de Fraude. Recuperado de <https://www.auditool.org/blog/fraude/2981-14-tipos-de-fraudes>

Ballotpedia.org. (s.f.). Bert Johnson (Michigan). Recuperado 5 diciembre, 2018, de [https://ballotpedia.org/Bert\\_Johnson\\_\(Michigan\)](https://ballotpedia.org/Bert_Johnson_(Michigan))

Capterra.com. (s.f.a). Financial Fraud Detection Software-Active Data. Recuperado de <https://www.capterra.com/p/81255/ActiveData/>

Capterra.com. (s.f.b). Accounts Payable Software-AP Forensics Enterprise Suite. Recuperado de <https://www.capterra.com/p/73970/AP-Forensics-Enterprise-Suite/>

Capterra.com. (s.f.c). Financial Fraud Detection Software-Argoscope. Recuperado de <https://www.capterra.com/p/145472/Argoscope/>

- CaseWare Analytics. (s.f.). Control de nómina. Recuperado de <https://www.casewareanalytics.com/es/solutions/soluciones-empresariales/control-de-n%C3%B3mina>
- Department of Justice U.S. Attorney's Office Eastern District of Michigan. (2018, 2 marzo). State Senator Pleads Guilty to Conspiracy and Theft Charges. Recuperado de <https://www.justice.gov/usao-edmi/pr/state-senator-pleads-guilty-conspiracy-and-theft-charges>
- Departamento de Justicia Gobierno de Puerto Rico. (2018, 20 junio). Departamento de Justicia radica cargos contra exempleada de compañía al apropiarse de más de \$110 mil creando empleados fantasmas. Recuperado de <http://www.justicia.pr.gov/departamento-de-justicia-radica-cargos-contra-exempleada-de-compania-al-apropiarse-de-mas-de-110-mil-creando-empleados-fantasmas/>
- Diario Financiero. (2013). Fraude corporativo:nómina de sueldos. Recuperado de <https://www.df.cl/noticias/opinion/columnistas/fraude-corporativo-nomina-de-sueldos/2013-03-18/190354.html>
- FindLaw. (s.f.). 18 U.S.C. § 372 - U.S. Code - Unannotated Title 18. Crimes and Criminal Procedure § 372. Conspiracy to impede or injure officer. Recuperado de <https://codes.findlaw.com/us/title-18-crimes-and-criminal-procedure/18-usc-sect-372.html>
- Iberdrola. (2018, 23 octubre). Política contra la corrupción y el fraude. Recuperado de [https://www.iberdrola.com/wcorp/gc/prod/es\\_ES/corporativos/docs/politica\\_contra\\_corrupcion\\_fraude.pdf](https://www.iberdrola.com/wcorp/gc/prod/es_ES/corporativos/docs/politica_contra_corrupcion_fraude.pdf)
- Legal Information Institute. (s.f.). 18 U.S. Code § 666 - Theft or bribery concerning programs receiving Federal funds. Recuperado de <https://www.law.cornell.edu/uscode/text/18/666>
- Morelaw.com. (2018, 9 julio). United States of America v. Bertram Johnson, Jr. Recuperado de <https://www.morelaw.com/verdicts/case.asp?n=2:17-cr-20233-MFL-APP-1&s=MI&d=119227>

Morelaw.com. (2014, 27 agosto). United States of America v. Tamara Housley. Recuperado de <https://www.morelaw.com/verdicts/case.asp?n=5:14-cr-00046-HE&s=OK&d=71593>

Morelaw.com. (2017, 20 febrero). United States of America v. Gerald Ursin, Jr. Recuperado de <https://www.morelaw.com/verdicts/case.asp?n=2:16-cr-00112-EEF-MBN&s=LA&d=100047>

USA vs. Bertram Johnson Jr. (United States District Court for the Eastern District of Michigan, 2017, 18 abril). Appearance Bond. Recuperado de <https://www.mied.uscourts.gov/PDFFiles/Johnson%20Bond%20Order.pdf>

USA vs. Bertram Johnson Jr. (United States District Court Eastern District of Michigan, 2017, 11 abril). Indictment. Recuperado de <https://www.mied.uscourts.gov/PDFFiles/Johnson%20Indictment.pdf>

Wells, J. (2013). Principles of Fraud Examination, Fourth Edition. New Jersey: Wiley