ESCENARIO DE INVESTIGACIÓN FORENSE “NARCOS 2019”

NICOLAS PERDOMO REYES

GERMÁN DAVID LOZANO PUENTES

EDICSON PINEDA CADENA
ASESOR MONOGRAFIA

UNIVERSIDAD PILOTO DE COLOMBIA SECCIONAL DEL ALTO MAGDALENA

INGENIERIA DE SISTEMAS X SEMESTRE

INFORMATICA FORENSE

GIRARDOT

2022

Contenido

Tablas

Tabla de contenido ilustraciones

Resumen

Esta investigación tiene como objetivo y finalidad la realización de un examen forense a tres computadoras pertenecientes a John Fredricksen, Jane Esteban y Steve Kowhai todo esto con el fin de desentramar y comprender mejor sus motivos, metas y objetivos que los llevo a cometer el ilícito descrito a continuación.

Tanto John Fredricksen como Jane Esteban fueron detenidos en el aeropuerto de Wellington transportando 1 kg de droga y les fueron incautados dos computadores tipo laptop. Por su parte Steve Kowhai fue vinculado a la investigación gracias a el testimonio entregado a las autoridades por Jane Esteban lo que conllevo al allanamiento del lugar de su residencia, donde se encontró un Pc de escritorio además de algunas sustancias al parecer psicoactivas.

Teniendo en cuenta lo anterior se puso a disposición de los analistas German David Lozano y Nicolas Perdomo Reyes dos (2) archivos de formato EnCase01 que la informática identifica como imágenes forenses de los computadores pertenecientes a John Fredricksen y Steve Kowhai, los cuales fueron sometidos a las 4 fases de análisis forense para tratar de recopilar información suficiente que permita hallar la relación de los dos sujetos y su participación en el ilícito.

Se utilizó como herramienta de análisis el software Autopsy el cual soporto y proceso la información de las 2 imágenes forenses brindando las garantías suficientes para la elaboración de los respectivos informes que permitieron encontrar la relación y desarrollo de actividades ilegales de los 2 implicados.

Palabras clave: Incautar, Análisis Forense, Receptor, Imagen, Volcado de Memoria, Evidencia, Droga.

Abstract

The objective and purpose of this investigation is to carry out a forensic examination of three computers belonging to John Fredricksen, Jane Esteban, and Steve Kowhai, all this in order to unravel and better understand their motives, goals and objectives that led them to commit the crime described. next.

Both John Fredricksen and Jane Esteban were arrested at Wellington airport transporting 1 kg of drugs and two laptop-type computers were seized from them. For his part, Steve Kowhai was linked to the investigation thanks to the testimony given to the authorities by Jane Esteban, which led to the search of his place of residence, where a desktop PC was found in addition to some apparently psychoactive substances.

Taking into account the foregoing, two (2) EnCase01 format files were made available to the analysts, German David Lozano and Nicolas Perdomo Reyes, which the computer identifies as forensic images of the computers belonging to John Fredricksen and Steve Kowhai, which were subjected to the 4 phases of forensic analysis to try to collect enough information to find the relationship of the two subjects and their participation in the crime

The Autopsy software was used as an analysis tool, which supported and processed the information of the 2 images, providing sufficient guarantees for the preparation of the respective reports that allowed finding the relationship and development of illegal activities of the 2 involved.

Keywords: Seize, Forensic Analysis, Receiver, Image, Memory Dump, Evidence, Drug.

Introducción

El tráfico de drogas o estupefacientes es un problema global que afecta a todos los países del mundo sin distinguir ideología política, religión y economía, una de las formas más comunes para cometer este ilícito es por medio de fuentes de trasporte aéreo ya sea en vuelos comerciales como privados. Un modus operandi común es transportar la droga ya sea en el equipaje de un pasajero como también varios, también existe el denominado transporte de droga a través de "mulas" y que consiste en que el individuo ingiere varias cantidades de droga en capsulas selladas con látex para que sea más fácil su ingesta.

Con base a esto se dispuso a realizar el respectivo análisis de dos sospechosos de participar en tráfico de drogas con el fin de establecer la relación entre los 2 sujetos, sus planes futuros y objetivos que los llevaron a cometer el ilícito. Cabe resaltar que el siguiente caso es un escenario ficticio y su uso es únicamente académico.

Antecedentes del caso

El cuerpo de investigación e inteligencia del gobierno australiano logró la interceptación de dos pasajeros identificados como Jane Esteban y John Fredricksen al cual se le incauto un kilogramo de metanfetamina en su bolso por la Aduana al llegar a Wellington, Nueva Zelanda desde Brisbane. Dentro de las primeras pesquisas se logró evidenciar que los 2 sospechosos estaban e inmersos en actividades ilegales y también a los cuales se les fue interceptados 2 computadores.

Posteriormente fueron interrogados por separado, John Fredricksen se negó a dar declaraciones ante las autoridades. Y Jane Esteban manifestó la implicación de un tercero que sería el receptor de la mercancía.

La declaración suministrada por Jane Esteban indicó que el punto de encuentro con el sospecho hasta el momento no identificado, seria en la "*biblioteca de Eastbourne"* en Wellington, Nueva Zelanda, y entrego otra dirección muy cercana a Wellington que la cual seria *"666 Rewera Avenue, Petone",* por si lo demás fallaba.

La policía allanó la residencia con la dirección entregada anteriormente. Durante el operativo no se realizó ninguna captura ya que el bien inmueble se encontraba vacío en ese momento. Sin embargo, se logró la incautación de drogas, armas y una computadora de escritorio del sospecho ahora identificado como Steve Kowhai.

Objetivos del caso

Analizar las respectivas imágenes forenses y encontrar evidencia suficiente que muestre la relación entre John Fredricksen y Steve Kowhai y establecer la participación de ambos en la ejecución, planificación y puesta en marcha del ilícito.

Objetivos específicos del caso

- Analizar los contenidos de las 2 imágenes forenses tipo EnCase01 entregadas por las autoridades y que pertenecen a los capturado John Fredricksen y el sospechoso Steve Kowhai.

- Identificar y recolectar la mayor cantidad de evidencia posible que pruebe la relación del ilícito entre los dos implicados

- Presentar y documentar las evidencias como también los resultados de los reportes que arrojo el análisis forense de las imágenes forenses EnCase01 de los equipos incautados y que los resultados de los análisis permitan llegar a la conclusión del caso.

Marco teórico

Delitos informáticos

Hablamos de un delito informático cuando una persona tiene intenciones de realizar u obtener información confidencial de manera ilegal, que puede estar alojada en cualquier equipo electrónico, puede ser computadores, USB, discos duros, hasta correos electrónicos. Estos tipos de delitos se clasifican de la siguiente manera: (Contadores, 2019)

Tipos de delitos Informáticos más comunes

La estafa

Se define como la alteración, borrado o supresión indebida de datos informáticos, siendo los más comunes datos de identidad, por otra parte, abarca también la alteración ilegitimas de softwares o medios digitales, cuyo fin sea la transferencia indebida de un activo patrimonial a un tercero. Sin embargo, debido a que las víctimas de tales violaciones a veces no informan estos delitos debido a diferentes motivos, como el miedo y la intimidación, la propagación es muy grande. (Observatorio de Delitos Informaticos de Bolivia, 2018)

El skimming

El skimming es el copiado de la banda magnética de una tarjeta ya sea de crédito o débito, lo que permite, el robo y fuga de información de las tarjetas dicho acto ilícito se ejecuta al momento de ingresar la tarjeta a un datafono o cajero electrónico que ha sido adulterado para cometer tal fin. (Unidad de Investigación Criminal de la Defensa, 2019)

la Carta Nigeriana

La carta nigeriana es una estafa que hace soñar a la víctima con tener una riqueza grandísima y lo persuade de pagar una suma de dinero por adelantado como condición para obtener la supuesta riqueza que le prometen. Esta actividad ilegal también se conoce como una "estafa nigeriana". Tradicionalmente, este robo se realiza a través de correos electrónicos no solicitados de la víctima, son similares al "spam". (Unidad de Investigación Criminal de la Defensa, 2019)

el Smishing: se fundamenta con la utilización de técnicas de Ingeniería Social por canales de mensajería instantánea a las víctimas si este primer filtro falla su siguiente táctica es gestionar llamadas telefónicas a la posible victima para que esta entregue información o se vea obligada a entrar a un sitio web malicioso. (Unidad de Investigación Criminal de la Defensa, 2019)

Sabotaje informático

El sabotaje informático es cuando se realiza toda acción de alterar, modificar, borrar o eliminar información sobre programas o archivos que se encuentren en diferentes dispositivos a fin de impedir su funcionamiento normal. (Porolli, 2013)

Espionaje informático

Es un acceso de forma ilícita y fraudulenta a un sistema informático y una vez allí filtrar, hacer visible o públicos los datos o información de personas, empresas o entidades gubernamentales con el objetivo ideal de chantajear u obtener algún beneficio. (Bonet, 2021)

Informática forense

La informática forense se centra en la utilización de prácticas y métodos científicos probados que permiten la identificación, recolección, preservación, análisis y validación, presentación y documentación de evidencias digitales o físicas con el objetivo principal de hacer una reconstrucción de un escenario en el que se cree hubo la ejecución de actividades delictivas. (Dominguez, 2014)

Análisis Forense

El análisis forense digital corresponde a un conjunto de tecnologías diseñadas para extraer información valiosa de un disco sin cambiar su estado. Esto le permite buscar datos previamente conocidos, intentar encontrar un patrón o comportamiento determinado o descubrir información oculta. (Porolli, 2013)

Copia o imagen forense

La imagen forense es una copia bit a bit del medio de almacenamiento de uno o más archivos. La imagen forense es muy útil allí porque se copia en ella Cada espacio del disco. Los metadatos no se modifican, la fecha y hora originales del archivo se conservan y la información eliminada de los medios se puede recuperar; por lo tanto, si elimina el archivo o se "pierde", es posible que la imagen pueda recuperarlo. (Legis, Ambito Juridico , 2018).

Encriptación

es un método de seguridad a nivel informático que permite transformar y disfrazar un mensaje o archivo de tal forma que el contenido que en el existe sea ilegible con métodos convencionales de lectura, salvo para su destinatario. (Sede Electronica, Real casa de la moneda y Timbre Española , 2021)

Objetivos de la informática forense

La informática forense consta de unos objetivos claros que se caracterizan y se deben tener en cuenta en cualquier caso forense. El primero es la compensación sobre los daños causados por personal criminales, el segundo objetivo es la persecución y el procesamiento judicial de los criminales, por otro lado, uno de los objetivos primordiales es la de detectar posibles vulnerabilidades en seguridad en diferentes dispositivos que hagan parte de una empresa, tratando de corregir dichos errores en caso de ser encontrados.

Usos de la informática forense

La informática forense tiene varias aplicaciones y usos que se emplean en la mayoría de las veces en las empresas, una de ellas y la más importante es para la recopilación de pruebas admitidas a un caso judicial forense informático. Por otro lado, también tiene casos de uso para nivel interno en las empresas, es decir la supervisión del uso indebido de equipos de trabajo durante las horas de trabajo. En este caso se usa con el fin de demostrar o tener evidencias para la empresa en caso de que el empleado use los recursos de la empresa para beneficio propio que pueda perjudicar a la empresa más adelante.

Por último, también tiene el uso de a través de las auditorias y el trabajo de peritos detectar diferentes vulnerabilidades y debilidades que puedan tener internamente en equipos o dispositivos mitigando así posible infiltraciones o ataques maliciosos de terceros

Retos de la informática Forense

Los retos que principalmente debe cumplir un investigador o perito forense, es principalmente contrarrestar con diferentes herramientas o técnicas antiforense la recolección de información de casos informáticos judiciales a través de nuevas tecnologías con el fin de buscar evidencia relevante en un determinado juicio.

Marco conceptual

Aduana

La aduana tiene como objetivo administrar todo el tránsito de mercancía o recursos materiales que se importen o se exporten, por medio de impuestos como los aranceles los cuales son pagados por organizaciones privadas o públicas. (Significados, 2021)

Narcotráfico

Se conoce como narcotráfico a todo acto ilegal relacionado con el cultivo, manufactura, distribución y venta de drogas ilegales. A este acto delincuencial se une a una gran cadena de carteles o grupos armados ilegales que se dedican a la comercialización de drogas. (ConceptoDefinicion, 2021)

Metanfetamina

la metanfetamina es una droga estimulante que se considera sumamente adictivo que principalmente afecta el sistema nervioso central. Es un polvo blanco cristalino, inodoro y de sabor amargo que se disuelve fácilmente en agua o alcohol. (NIDA, 2021)

Allanamiento

el allanamiento se refiere a una acción legal que le permite a la autoridad ingresar, en ciertos casos con una orden judicial para capturar a cualquier individuo o persona sospechosa sobre algún delito, con el fin de recolectar información o evidencia referente a un echo ilegal (UNIVERSO, 2020)

Marco metodológico

La metodología llevada a cabo para la ejecución y realización del análisis y recolección de evidencia es la investigación exploratoria. Este tipo de investigación se adapta fácilmente a este caso puesto que, su objetivo es el estudio de un problema que no está esclarecido previamente, y lo que se pretende con este análisis forense es encontrar o socavar información, con el fin de proporcionar resultados o evidencias relacionadas que demuestren si hay o no una relación entre John Fredricksen y Steve Kowhai. (Arias, 2020)

Para la investigación o el análisis forense que se realizará se usaran diferentes técnicas y fases de estudio el cual ayudará a la recopilación de información, el uso de peritos de datos con el fin de realizar un análisis a los dispositivos electrónicos notificando sobre alguna modificación o alteración de la información que podría ser usada para responder ante un caso de incidente legal.

En la fase de **adquisición** se realizan las copias de la información incautada y que posiblemente sea sospechosa sobre algún delito. De este modo se evita la modificación o manipulación de esta información recolectada con la copia de bite a bite con las herramientas y dispositivos adecuados.

En la fase de **preservación** lo que se busca es que la evidencia no sea manipulada y que se mantenga intacta para esto es necesario efectuar lo que se denomina cadenas de custodia para que la información siempre permanezca protegida

En la fase de **análisis** se obtiene toda la información ya recopilada, en esta fase técnica se usan herramientas como programas específicamente para el análisis forense. Debemos de tener en cuenta que tipo de información y que es lo que estamos buscando para así poder tener un mayor grado de exactitud y precisión para el análisis de la información. (welivesecurity, 5 fases fundamentales del análisis forense digital, 2015)

El medio utilizado para el análisis completo de la unidad será el software Autopsy el cual cuenta con el respaldo y las garantías necesarias para efectuar el correcto análisis de la imagen puesta a disposición para el peritaje forense.

Por último, la fase de **presentación** del informe se destaca por mostrar y exponer los hallazgos más importantes y relevantes de forma resumida evitando tocar la investigación en detalles muy técnicos, se recomienda siempre entregar los datos de forma certera y explicita dejando a un lado cualquier cuestión que genere algún tipo de duda en el análisis de la información (welivesecurity, 5 fases fundamentales del análisis forense digital, 2015)

Marco Legal

En esta parte del mundo, Oceanía es uno de los continentes con mayor diversidad, en ella viven alrededor de 34 millones de personas con diferentes culturas y dialectos distintos. Países como nueva Zelanda y diferentes islas pacificas en donde la cercanía de esta zona a países de grandes productores de drogas en el este de Asia y la alta demanda de drogas en países como nueva Zelanda, hacen que se conviertan en territorio propicio para el establecimiento de rutas de narcotráfico.

En nueva Zelanda se produce cannabis, la gran parte de esta producción se consume localmente y hasta el día de hoy no hay evidencias que haya comercialización por fuera de esta región. Geográficamente Oceanía no cuenta aún con una ruta de drogas específicas. Su actual mercado de cocaína aun es muy pequeño, pero las incautaciones en los años 2009-2010 han aumentado cuatro veces con relación a los años 2005-2006. A nivel local el consumo anual de drogas en Oceanía sigue siendo mucho más alto que la media mundial. La región se caracteriza por altas tasas de consumo de drogas como el éxtasis (2.9%), anfetaminas (entre 2% y 2.8%). (idpc, 2012)

Al ser el estado de Nueva Zelanda una democracia parlamentaria regido por una monarquía, las leyes o estatutos son establecidos por un consenso entre la figura principal que es la Reina y el parlamento. Sin embargo, para luchar contra el narcotráfico y/o otros delitos está nación se acoge a las políticas dictaminadas por la ONU. Esto no implica que el país no rija unas normar o leyes de control de uso sobre las drogas. Estas normas son las siguientes, las cuales son articuladas por el país para el buen uso y manejo de las drogas y evitar conflictos de violencia como hurtos o asesinatos

Políticas Regionales De Drogas

Reducción de la oferta

Esta política lo que busca es la reducción de la oferta orientada hacer cumplir la prohibición del uso no medicado de sustancias fiscalizadas y a regular el acceso a drogas legales, incluyendo el tabaco, alcohol, farmacéuticos y otras sustancias licitas. (idpc, 2012)

Violencia relacionada con las drogas

Esta política se refleja en las tasas de homicidio y diferentes formas de violencia que pueda generar el uso y comercio de drogas. Sabiendo así que existen organizaciones delictivas que están involucradas en el tráfico de drogas no son una amenaza mayor para la seguridad de los habitantes. (idpc, 2012)

Desarrollo del caso

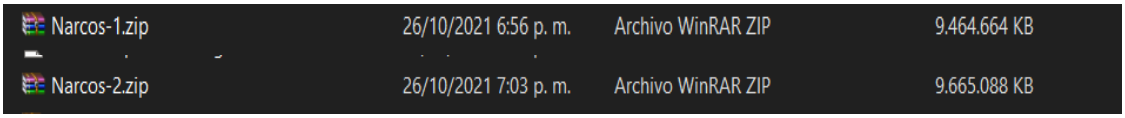
A continuación, se presentará las 5 fases efectuadas para el desarrollo del análisis forense de sus resultados.

Adquisición

Se obtuvo el material para el análisis en el sitio web denominado **CFReDS** que se encarga de la publicación de escenarios gratuitos y de licencia libre para el desarrollo e investigación de análisis forense de carácter académico y profesional.

El material descargado se relaciona a continuación

Ilustración 1. Material descargado para el estudio del caso (Fuente propia)



Se descargaron dos archivos .zip los cuales tenían un peso aproximado de 10 GB.

Al descomprimirlos presentaban un peso aproximado de 32 GB cada uno divididos en 21 imágenes tipo EnCase01 de aproximadamente 1,6 GB.

Las imágenes se clasificaron de la siguiente forma:

Tabla 1. Clasificación de las imágenes EnCase01. (fuente propia).

Nombre	**Hardware**	**Sistema Operativo**	**Propietario**	**Extensión**	**Fecha de Descarga**	**Tamaño**
Narcos-1	Pc-Desktop	Windows 10 Pro	Steve Kowhai	EnCase01	26/10/2021	31.5 GB

Nombre	Hardware	Sistema Operativo	Propietario	Extensión	Fecha de Descarga	Tamaño
Narcos-2	Laptop	Windows 10 Pro	John Fredricksen	EnCase01	26/10/2021	31.5GB

Datos técnicos de los equipos incautados

Tabla 2. Datos software de la imagen Narcos-2. (Fuente propia)

Objetivo	Información detallada	
Imagen sistema operativo	**Arquitectura Procesador**	AMD64
	Nombre sistema operativo	Windows 10 pro
	Fecha de instalación	2019-01-28 14:15:39 COT
	Id producto	00330-80000-00000-AA502
	Directorio de archivos temporales	%SystemRoot%\TEMP
	Versión	Windows_NT
	Archivos exploratorios	/img_Narcos-1.001/vol_vol7/Windows/System32/config/SYSTEM

Tabla 3. Datos software de las imágenes EnCase 01. (fuente propia).

Objetivo	**Información detallada**	
Imagen sistema operativo	**Arquitectura Procesador**	AMD64
	Nombre sistema operativo	Windows 10 pro
	Fecha de instalación	2019-01-28 14:12:46 COT
	Id producto	00330-80000-00000-AA310
	Directorio de archivos temporales	%SystemRoot%\TEMP
	Versión	Windows_NT
	Archivos exploratorios	/img_Narcos-2.001/vol_vol7/Windows/System32/config/SYSTEM

Preservación

Se procedió luego a la implementación de esta fase en la que se efectuaron los debidos procesos para salvaguardar la evidencia para esto se realizó la respectiva copia de las imágenes EnCase01 y establecer el personal que efectuó la cadena de custodia.

Copias de Seguridad

Se posee una copia de cada una de las imágenes sujetas para análisis y están etiquetadas y rotuladas así:

Narcos-1- copia(1)

Narcos-2- copia(1)

Cadena de Custodia

El personal encargado y destinado para realizar el análisis de la imagen de la unidad es:

1. Germán David Lozano Puentes
2. Nicolas Perdomo Reyes

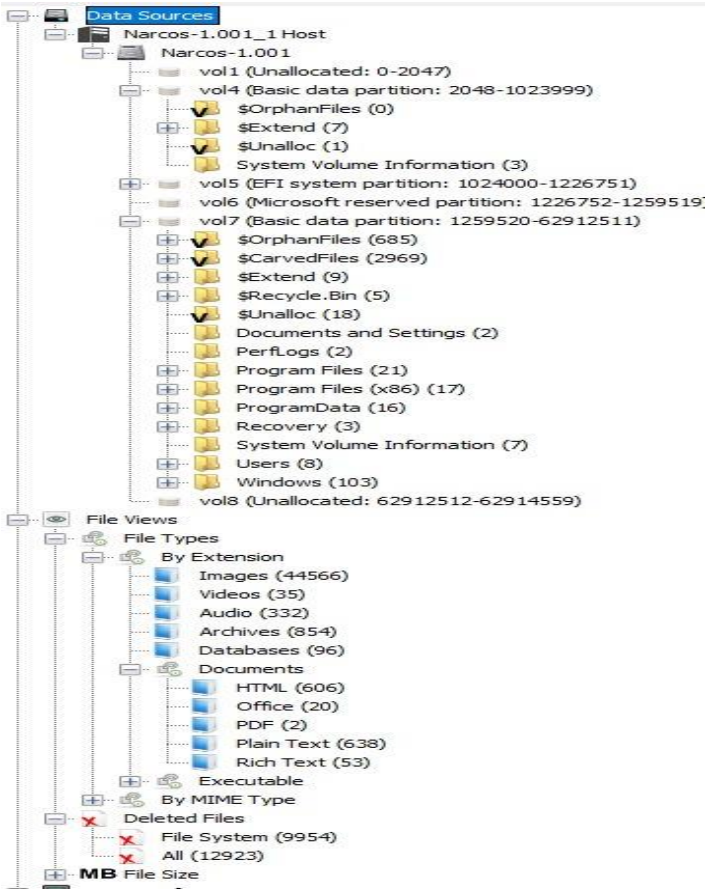
Análisis

Análisis de la imagen Narcos-1

la imagen analizada tiene como evidencia la siguiente cantidad de archivos con diferentes extensiones.

- imágenes analizadas: 44566
- Videos: 35
- Audios: 332
- Archivos: 854
- Bases de datos: 96
- HTML: 606
- Office: 20
- PDF: 2
- Archivos de texto plano: 638
- Archivo del sistema eliminados: 9954
- Total, de archivos eliminados: 12923

Ilustración 2. Datos Analizados de la imagen Narcos-1. (Fuente Autopsy)



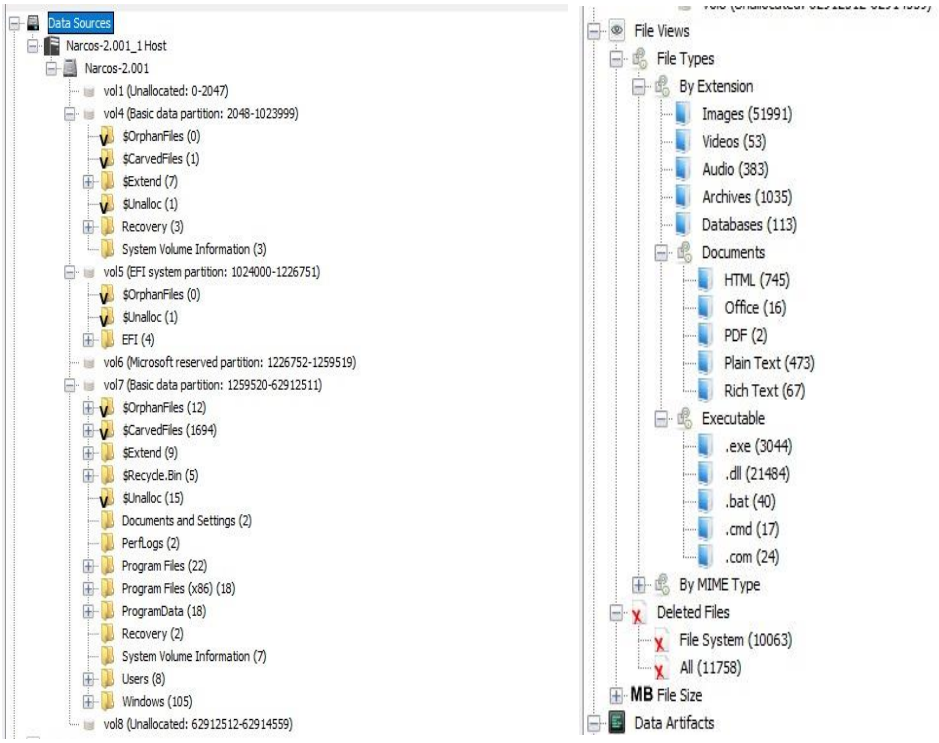
Análisis de la imagen Narcos-2

la segunda imagen analizada tiene como evidencia la siguiente cantidad de archivos con diferentes extensiones.

- imágenes analizadas: 51991
- Videos: 53
- Audio: 383
- Archivos: 1035
- Bases de datos: 113
- HTML: 745

- Office: 16
- PDF: 2
- Archivos de texto plano: 473
- Archivos del sistema eliminados: 10063
- Total, de archivos eliminados: 11758

Ilustración 3. Datos Analizados de la imagen Narcos-2. (Fuente Autopsy)



Línea de Tiempo

Se organizaron las evidencias de los dos computadores en orden cronológico con el fin de dar trazabilidad y seguimiento y establecer la relación de los sujetos en la participación del ilícito anteriormente mencionado.

Fecha de creación del archivo (evidencia #1)
2019-01-28 15:26:09 Imagen Narcos-2

Ilustración 4. Base de datos de clientes obtenida del pc de John Fredricksen (Fuente: Autopsy, clients.ods)

A18

	A	B	C	D	E
1	**Name**	**Location**	**Product**	**Amount**	**Delivery**
2	Ricky Ross	Los Angeles	Mama Coca	20kg	Monthly
3	Frank Lucas	New York, USA	Ferry Dust	15kg	Quarterly
4	Chris Coke	Kingston Jamaica	Coke	20kg	Monthly
5	Steve Kowhai	Wellington, New Zealand	Crank	15kg	Monthly
6	Don Cholito	Puerto Rico	Snow	25kg	Quarterly
7	Manuel Noriega	Panama	Smack	15kg	Monthly
8	Joaquin Guzman	Guadalajara, Mexico	China White	15kg	Monthly
9	Leroy Barnes	New York, USA	Load pack	15kg	Quarterly
10	AL Capone	Siciliy, Italy	Silly putty	25kg	Monthly
11	Jane Esteban	Brisbane, Austraila	Uppers	1 gram	On demand
12	Pablo Esocbar	Colombia	White horse	15kg	Quarterly
13	Franz Sanchez	Isthmus City	Mary Jane	20kg	Quarterly

Fecha de creación del archivo (evidencia #2)
2019-01-29 19:00:48 Imagen Narcos-2

Ilustración 5. Evidencia documento "Crystal Method" (Fuente Documento Word f0240272.odt)

Crystal Method

Destination – Wellington
Product – 1 kg crystal
Source – Brisbane (JF)

Wellington is part of the lower north island of New Zealand. It is accessable by road and sea. As tempting as the sea is, be aware that the coast of NZ may seem ideal, but everyone knows it's vulnerable as there have been several news reports about it.

The product is coming from Brisbane, Australia and as a result, will need to be delivered by sea or plane. Shipping the product would be ideal, the risk of detection is lower but would result in higher costs for a small amount of product. The product being delievered is only a test to check it's quality and will be the deciding factor in any decision to continue doing business with you. If the product is up to scratch, I will buy a larger supply next time. If we continue to do business it might be more practical to use shipping for future transactions.

This consignment will be delievered by plane, which will decrease travel time and lower the cost for all parties involved. Delievery by plane will bring along with it its own complications such as concealment, security screening/checks and drug dogs. I trust that you are aware of the risks and will take all necessary precautions.

Below is a map of drup flows from countires, could give us some info for later trades and where we can get more product from in the future.

Main trafficking flows of heroin

Fecha de creación del archivo (evidencia #3)
2019-01-29 18:59:16 Imagen Narcos-2

Ilustración 6.Evidencia de software de encriptación TrueCrypt (Fuente Autopsy)

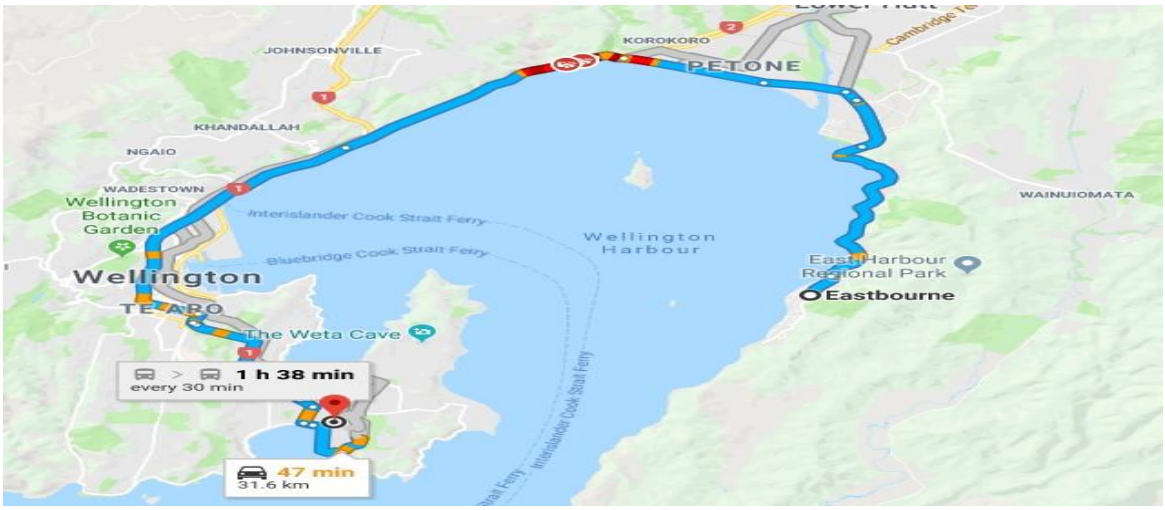
TrueCrypt.exe	/img_Narcos-2.001/vol_vol7/Program Files/TrueCrypt/True...		2019-01-29 18:59:16 COT	2019-01-29 18:59:17 COT	2019-02-01 22:03:08 COT
TrueCrypt Setup.exe	/img_Narcos-2.001/vol_vol7/Program Files/TrueCrypt/True...		2019-01-29 18:58:55 COT	2019-01-29 18:59:17 COT	2019-01-29 20:57:31 COT
TrueCrypt	/img_Narcos-2.001/vol_vol7/Program Files/TrueCrypt		2019-01-29 18:59:16 COT	2019-01-29 18:59:16 COT	2019-02-01 21:48:00 COT
TrueCrypt Setup 7.1a.exe	/img_Narcos-2.001/vol_vol7/Users/JohnF/Downloads/True...		2019-01-29 18:58:55 COT	2019-01-29 18:58:59 COT	2019-02-01 21:48:15 COT

Fecha de creación del archivo (evidencia #4)
2019-01-30 16:21:24 COT Imagen Narcos-1

Ilustración 7. Imagen satelital de desplazamiento a 2 puntos (Fuente Autopsy; Google Maps)

Fecha de creación del archivo (evidencia #5)
2019-01-30 16:25:18 Imagen Narcos-1

Ilustración 8. Imagen satelital de desplazamiento. (Fuente Autopsy, Google Maps)



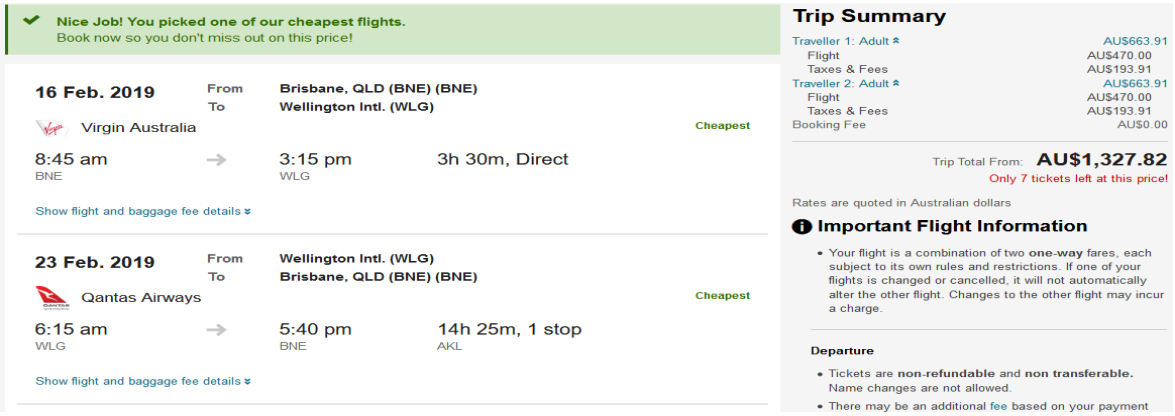
Fecha de creación del archivo (evidencia #6)
2019-01-31 19:21:32 Imagen Narcos-1

Ilustración 9. Evidencia de software de encriptación (Fuente Autopsy)

Image Steganography 1.5.2 Setup.exe		4	2019-01-31 19:16:34 COT	2019-01-31 19:16:46 COT	2019-02-01 09:23:31 COT	2019-01-31 19:16:32 COT
TrueCrypt Setup 7.1a.exe		4	2019-01-29 18:27:51 COT	2019-01-29 18:28:14 COT	2019-02-01 09:23:32 COT	2019-01-29 18:27:43 COT

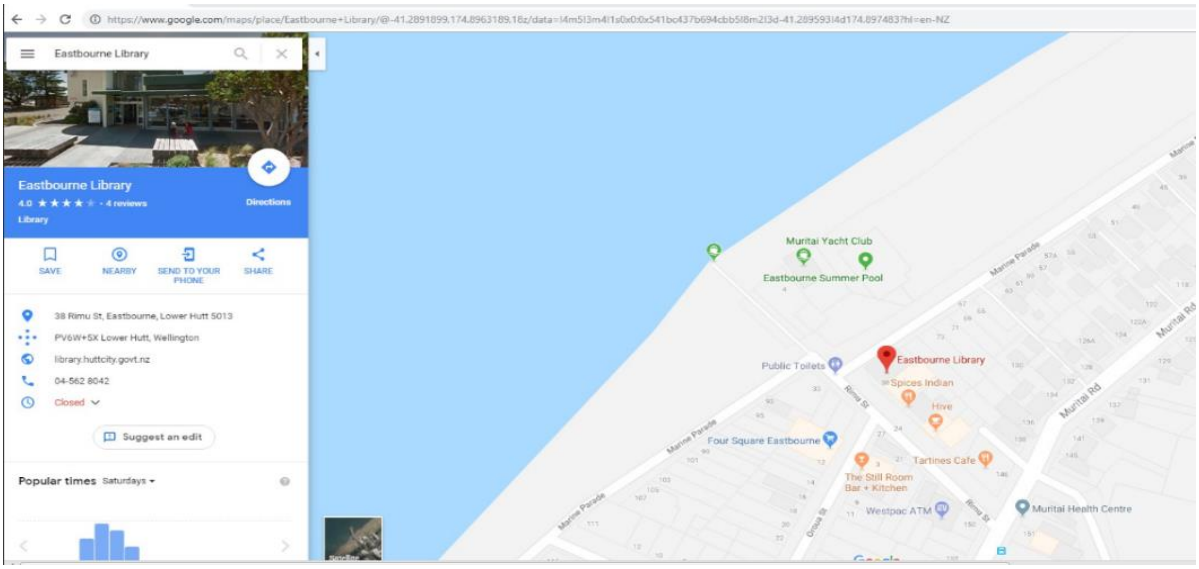
Fecha de creación del archivo (evidencia #7)
2019-02-01 21:28:44 Imagen Narcos-2

Ilustración 10. Reservación de vuelo (Fuente Autopsy)



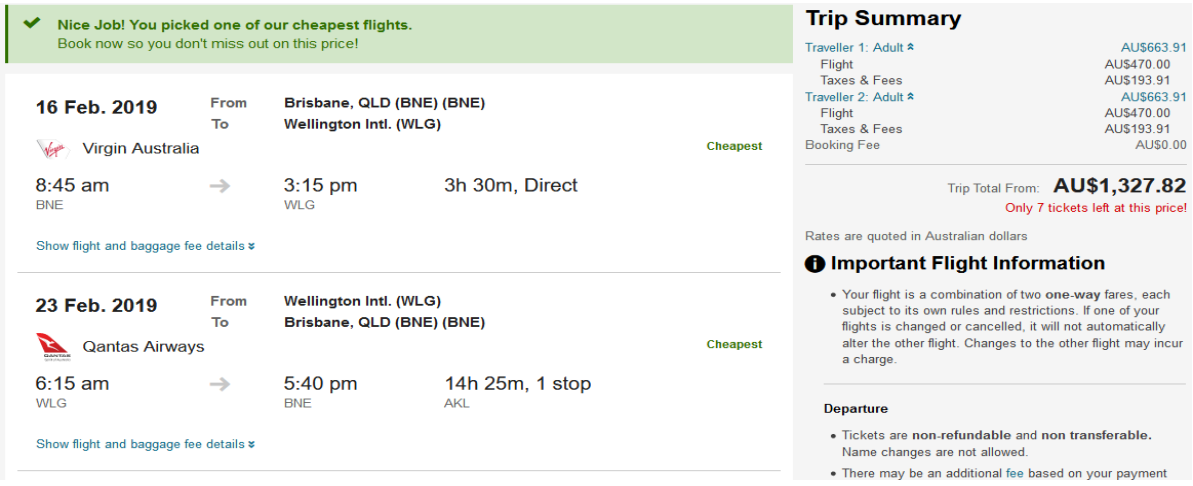
Fecha de creación del archivo (evidencia #8)
2019-02-01 20:06:05 Imagen Narcos-1

Ilustración 11. Imagen de librería de Eastbourne (Fuente: Autopsy, Google Maps)



Fecha de creación del archivo (evidencia #9)
2019-02-01 17:43:20 Imagen Narcos-1

Ilustración 12. Reservación de vuelo (Fuente Autopsy)



Documentación y Presentación

Para las imágenes marcadas con la etiqueta “Narcos-1” y “Narcos-2” correspondiente a los equipos de escritorio y portátil incautados por las autoridades del sospechoso identificado como Steve Kowhai y John Fredricksen se evidenciaron los siguientes hallazgos.

Archivos Etiquetados (Tagged Files)

Ilustración 13. Listado de evidencia encontrado en la imagen Narcos-1(Fuente: Reporte Autopsy)

Tagged Files

Tag	File	Comment
Archivo sospechoso (PC Steve Kowhai)	/img_Narcos-1.001/vol_vol7/Users/Steve/Documents/secret	
Confirmación ticket DE Vuelo (Notable)	/img_Narcos-1.001/vol_vol7/Users/Steve/Documents/Misc/flightbookings.PNG	
imagen de ubicación de biblioteca de Eastbourne (Notable)	/img_Narcos-1.001/vol_vol7/Users/Steve/Documents/Misc/dropoff.jpg	
imagen de Mapa con Distancia de una Ciudad a Otra (Notable)	/img_Narcos-1.001/vol_vol7/Users/Steve/Documents/Misc/airport crystals.jpg	
Imagen sateliatal de desplazamiento terrestrete	/img_Narcos-1.001/vol_vol7/Users/Steve/Documents/Misc/Method run.jpg	
Software de Encryptación (Notable)	/img_Narcos-1.001/vol_vol7/Users/Steve/Downloads/Image Steganography 1.5.2 Setup.exe	
Imagen sospecha	/img_Narcos-1.001/vol_vol7/Users/Steve/Downloads/Misc/BNE.png	
Imagen con Supuestos cristales (droga) (Notable)	/img_Narcos-1.001/vol_vol7/Users/Steve/Pictures/620x349.jpg	
Imagen evidencia (Notable)	/img_Narcos-1.001/vol_vol7/Users/Steve/Pictures/price-meth-bust-4.jpg	

Ilustración 14. Listado de evidencia encontrado en la imagen Narcos-2 (Fuente: Reporte Autopsy)

Tagged Files

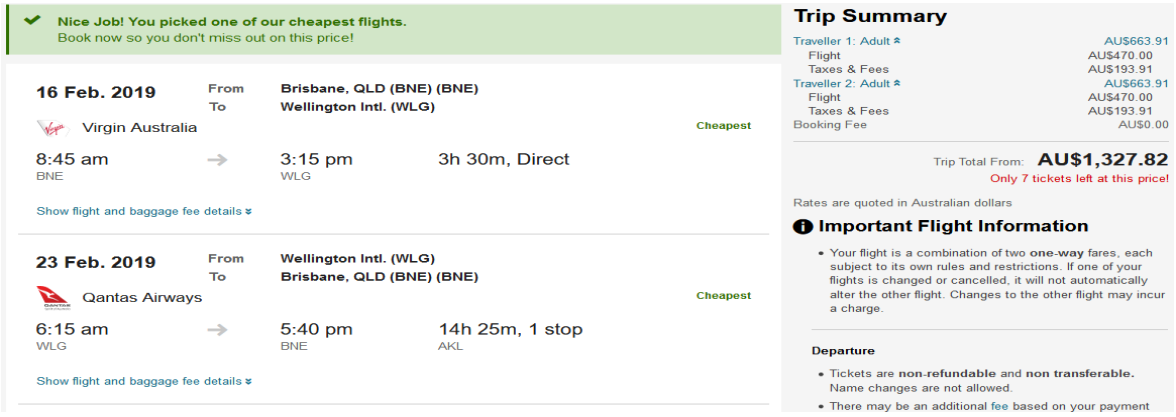
Tag	File
Software de Encryptación (Notable)	/img_Narcos-2.001/vol_vol7/Program Files/TrueCrypt/TrueCrypt.exe
Software de Encryptación (Notable)	/img_Narcos-2.001/vol_vol7/Program Files/TrueCrypt/TrueCrypt Setup.exe
Software de Encryptación (Notable)	/img_Narcos-2.001/vol_vol7/Program Files/TrueCrypt
Confirmación ticket DE Vuelo (Notable)	/img_Narcos-2.001/vol_vol7/Users/JohnF/Documents/Business/Steve K.PNG
Ticket de Envio DHL	/img_Narcos-2.001/vol_vol7/Users/JohnF/Documents/Business/shipping.PNG
Bse de datos con Información comprometedora	/img_Narcos-2.001/vol_vol7/Users/JohnF/Documents/Business/clients.ods
Notable Item (Notable)	/img_Narcos-2.001/vol_vol7/Users/JohnF/Documents/Business/clients.ods
Software de Encryptación (Notable)	/img_Narcos-2.001/vol_vol7/Users/JohnF/Downloads/TrueCrypt Setup 7.1a.exe
archivo con información sospechosa (Notable)	/img_Narcos-2.001/vol_vol7/Users/JohnF/Downloads/Attachments-Important, crucial to our method
Información relevante (Notable)	/img_Narcos-2.001/vol_vol7//$CarvedFiles/f0240272.odt

Evidencia Relevante para el caso imagen Narcos-1 (Steve Kowhai)

Número 1: (Confirmación Ticket de Vuelo (Notable))
Directorio de ubicación

/img_Narcos-1.001/vol_vol7/Users/Steve/Documents/Misc/flightbookings.PNG

Ilustración 15. Reservación de vuelo (Fuente Autopsy)



La *ilustración 15* muestra la captura de pantalla de reservación de un vuelo para dos personas adultas de Brisbane Australia como ciudad de origen y Wellington Nueva Zelanda como ciudad destino con fecha de salida del 16 de febrero 2019 y Fecha de Regreso el 23 de febrero 2019.

Tabla 4. Creación y modificación de la ilustración 15. (Fuente propia)

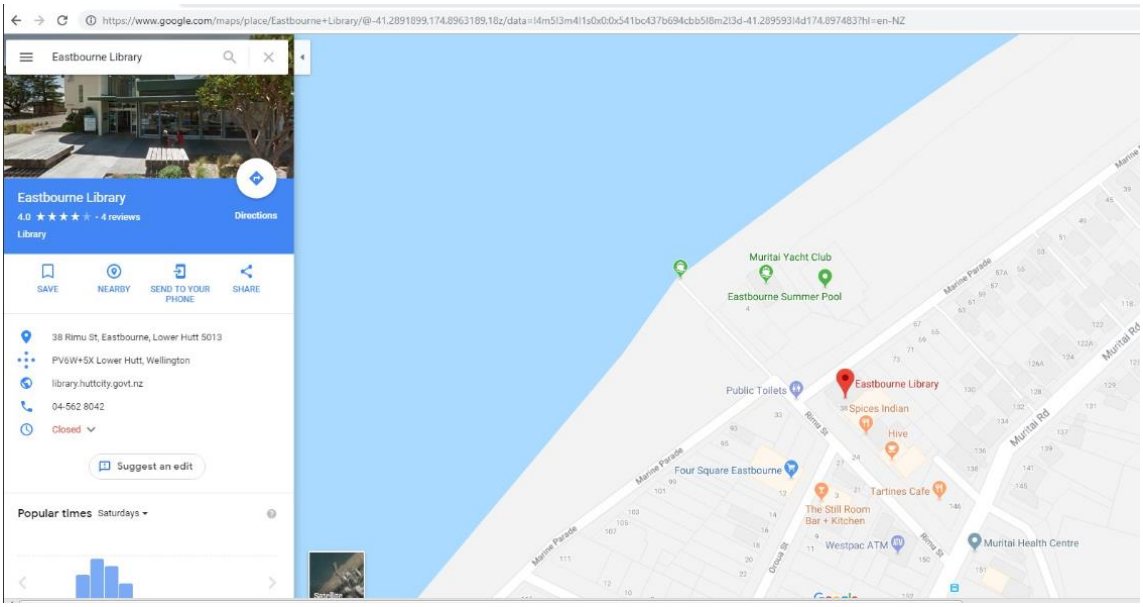
Hora de modificación	Fecha de Modificación	Fecha y hora Ultimo Acceso	Fecha y hora de creación
21:28:45	2019-02-01	2019-02-01 21:31:06	2019-02-01 21:28:44

Número 2: imagen de ubicación de biblioteca de Eastbourne (Notable)

Directorio de ubicación

/img_Narcos-1.001/vol_vol7/Users/Steve/Documents/Misc/dropoff.jpg

Ilustración 16. Imagen de librería de Eastbourne (Fuente: Autopsy, Google Maps)



La *ilustración 16* muestra la utilización de Google Maps para encontrar un lugar el cual se puede detallar en la imagen que corresponde a la biblioteca de Eastbourne que se encuentra a 24, 3 Km de la ciudad de Wellington en Nueva Zelanda.

Tabla 5. Creación y modificación de la ilustración 16. (Fuente propia)

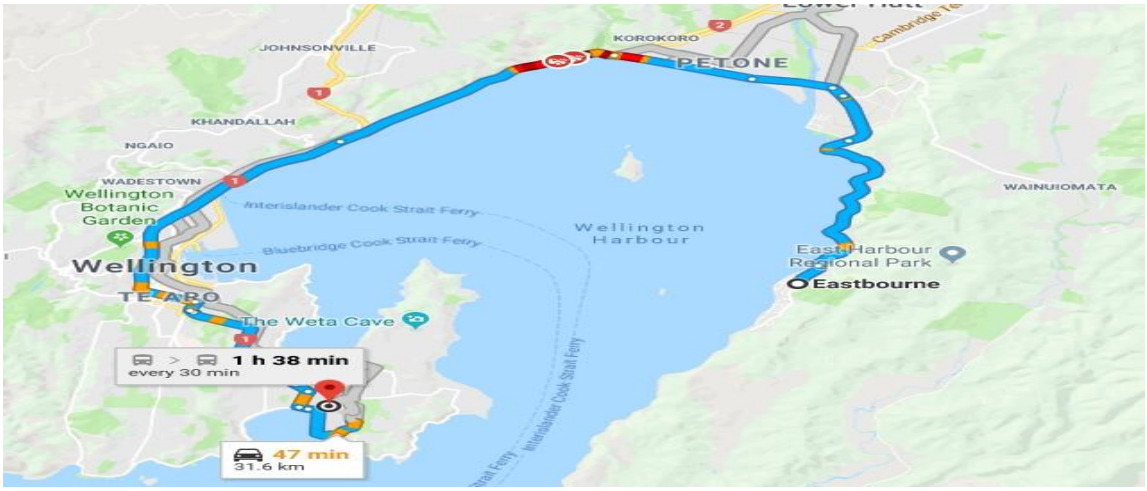
Hora de modificación	Fecha de Modificación	Fecha y hora Ultimo Acceso	Fecha y hora de creación
20:06:06	2019-02-01	2019-02-01 21:31:06	2019-02-01 20:06:05

Número 3: Desplazamiento de Aeropuerto de Wellington a Eastbourne (Notable)

Directorio de ubicación

/img_Narcos-1.001/vol_vol7/Users/Steve/Documents/Misc/airport crystals.jpg

Ilustración 17. Imagen satelital de desplazamiento. (Fuente Autopsy, Google Maps)



La *ilustración 17* muestra el desplazamiento terrestre por toda la costa marítima de la ciudad de Wellington explícitamente al aeropuerto de dicha ciudad presuntamente para calcular la distancia de desplazamiento que les tomaría a los sospechosos Jane Esteban y John Fredricksen hasta el punto de encuentro en la librería de Eastbourne.

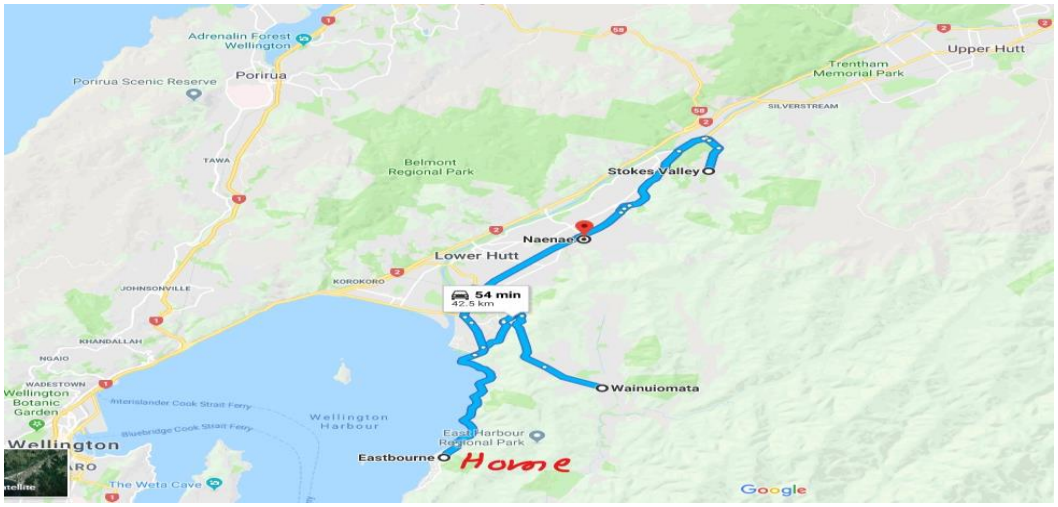
Tabla 6. Creación y modificación de la ilustración 17. (Fuente propia)

Hora de modificación	**Fecha de Modificación**	**Fecha y hora Ultimo Acceso**	**Fecha y hora de creación**
16:25:18	2019-01-30	2019-01-30 22:04:13	2019-01-30 16:25:18

Número 4: Imagen satelital de desplazamiento terrestre
Directorio de ubicación

/img_Narcos-1.001/vol_vol7/Users/Steve/Documents/Misc/Method run.jpg

Ilustración 18. Imagen satelital de desplazamiento a 2 puntos (Fuente Autopsy; Google Maps)



La *Ilustración 18* muestra un mapa con vista satelital el cual marca dos (2) posibles destinos partiendo desde la ciudad de Eastbourne el cual se identificó presuntamente por el sospechoso como *"Home"* a dos (2) localidades identificadas la más cercana como Wainuiomata suburbio de Wellington y Stokes Valley también suburbio de este.

Tabla 7. Creación y modificación de la ilustración 18. (Fuente propia)

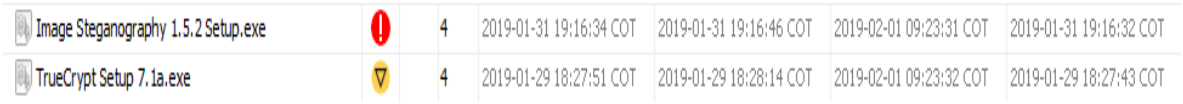
Hora de modificación	**Fecha de Modificación**	**Fecha y hora Ultimo Acceso**	**Fecha y hora de creación**
16:22:24	2019-01-30	2019-01-30 22:04:13	2019-01-30 16:21:24

Número 5. Utilización de softwares de encriptación y esteganografía.

Directorio de ubicación

/img_Narcos-1.001/vol_vol7/Users/Steve/Downloads/

Ilustración 19. Evidencia de software de encriptación (Fuente Autopsy)



La *ilustración 19* revela que existe alojado en el equipo del sospechoso la instalación de 2 programas de encriptación y esteganografía que permiten el ocultamiento de información.

Tabla 8. Creación y modificación de la ilustración 19. (Fuente propia)

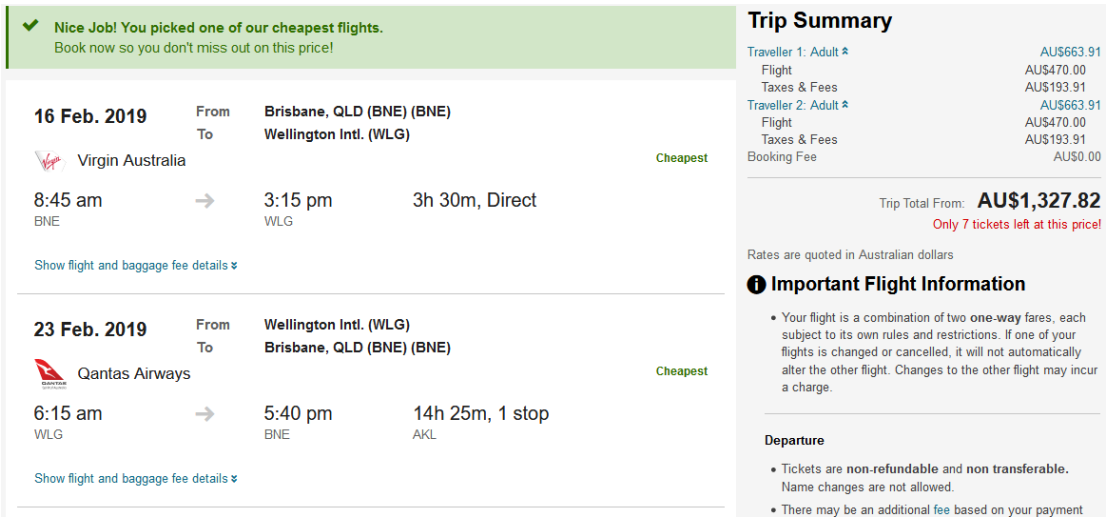
Hora de modificación	**Fecha de Modificación**	**Fecha y hora Ultimo Acceso**	**Fecha y hora de creación**
19:16:34	2019-01-31	2019-02-01 09:23:31	2019-01-31 19:16:32

Evidencia Relevante para el caso imagen Narcos-2 (John Fredricksen)

Número 6: (Confirmación Ticket de Vuelo (Notable))
Directorio de ubicación

/img_Narcos-2.001/vol_vol7/Users/JohnF/Documents/Business/Steve K.PNG

Ilustración 20. Reservación de vuelo (Fuente Autopsy)



La *ilustración 20* revela la confirmación de un ticket de vuelo, misma que fue encontrada en el anterior análisis al equipo de Steve Kowhai lo que al parecer demuestra una posible relación y comunicación entre el sospechoso y el capturado.

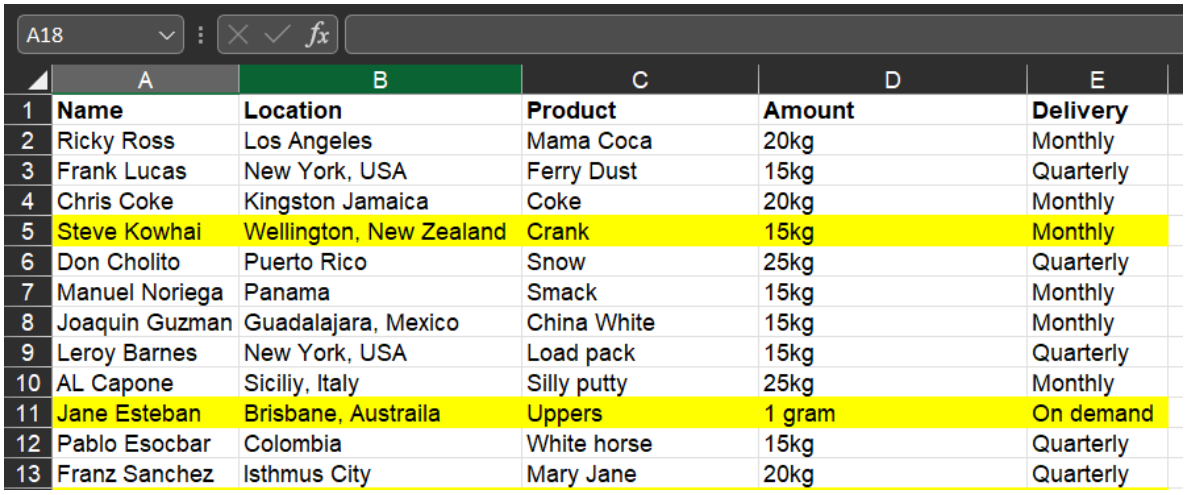
Tabla 9. Creación y modificación de la ilustración 20. (Fuente propia)

Hora de modificación	Fecha de Modificación	Fecha y hora Ultimo Acceso	Fecha y hora de creación
17:43:21	2019-02-01	2019-02-01 20:57:27	2019-02-01 17:43:20

Número 7: Base de datos con Información comprometedora (Notable))
Directorio de ubicación

/img_Narcos-2.001/vol_vol7/Users/JohnF/Documents/Business/clients.ods

Ilustración 21. Base de datos de clientes obtenida del pc de John Fredricksen (Fuente: Autopsy, clients.ods)



	A	B	C	D	E
1	**Name**	**Location**	**Product**	**Amount**	**Delivery**
2	Ricky Ross	Los Angeles	Mama Coca	20kg	Monthly
3	Frank Lucas	New York, USA	Ferry Dust	15kg	Quarterly
4	Chris Coke	Kingston Jamaica	Coke	20kg	Monthly
5	Steve Kowhai	Wellington, New Zealand	Crank	15kg	Monthly
6	Don Cholito	Puerto Rico	Snow	25kg	Quarterly
7	Manuel Noriega	Panama	Smack	15kg	Monthly
8	Joaquin Guzman	Guadalajara, Mexico	China White	15kg	Monthly
9	Leroy Barnes	New York, USA	Load pack	15kg	Quarterly
10	AL Capone	Siciliy, Italy	Silly putty	25kg	Monthly
11	Jane Esteban	Brisbane, Austraila	Uppers	1 gram	On demand
12	Pablo Esocbar	Colombia	White horse	15kg	Quarterly
13	Franz Sanchez	Isthmus City	Mary Jane	20kg	Quarterly

La *ilustración 21* destaca una captura de pantalla de un documento de Excel recuperado con una tabla cuya información detalla nombres de personas, locaciones, tipo de producto, cantidad, y tiempo de entrega en la cual resaltan los nombres de Steve Kowhai y Jane Esteban uno sospechoso de participar en el tráfico de drogas y la otra persona retenida por las autoridades en el aeropuerto de Wellington, Nueva Zelanda por transporte de drogas.

Tabla 10. Creación y modificación de la ilustración 21. (Fuente propia)

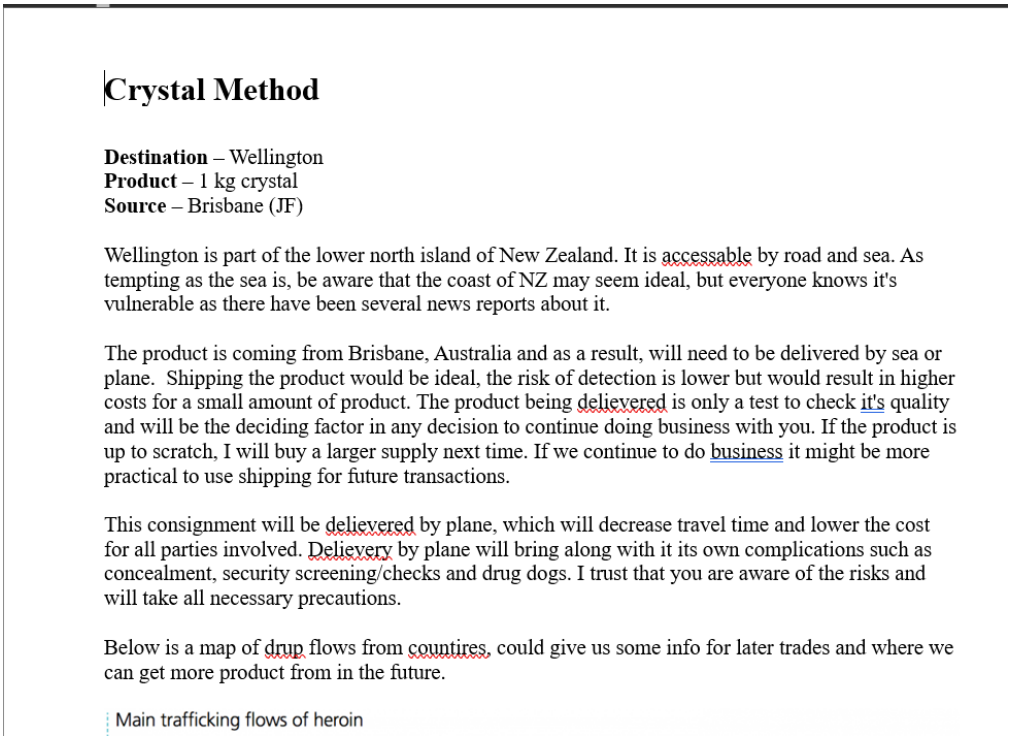
Hora de modificación	Fecha de Modificación	Fecha y hora Ultimo Acceso	Fecha y hora de creación
23:02:47	2019-01-28	2019-01-29 19:04:14	2019-01-28 15:26:09

Numero 8: Información relevante (Notable))

Directorio de ubicación:

/img_Narcos-2.001/vol_vol7//$CarvedFiles/f0240272.odt

Ilustración 22. Evidencia documento "Crystal Method" (Fuente Documento Word f0240272.odt)



Crystal Method

Destination – Wellington
Product – 1 kg crystal
Source – Brisbane (JF)

Wellington is part of the lower north island of New Zealand. It is accessable by road and sea. As tempting as the sea is, be aware that the coast of NZ may seem ideal, but everyone knows it's vulnerable as there have been several news reports about it.

The product is coming from Brisbane, Australia and as a result, will need to be delivered by sea or plane. Shipping the product would be ideal, the risk of detection is lower but would result in higher costs for a small amount of product. The product being delievered is only a test to check it's quality and will be the deciding factor in any decision to continue doing business with you. If the product is up to scratch, I will buy a larger supply next time. If we continue to do business it might be more practical to use shipping for future transactions.

This consignment will be delievered by plane, which will decrease travel time and lower the cost for all parties involved. Delievery by plane will bring along with it its own complications such as concealment, security screening/checks and drug dogs. I trust that you are aware of the risks and will take all necessary precautions.

Below is a map of drup flows from countires, could give us some info for later trades and where we can get more product from in the future.

Main trafficking flows of heroin

Ilustración 23. Principales flujos de tráfico de heroína (Fuente: Autopsy, Documento Word f0240272.odt)

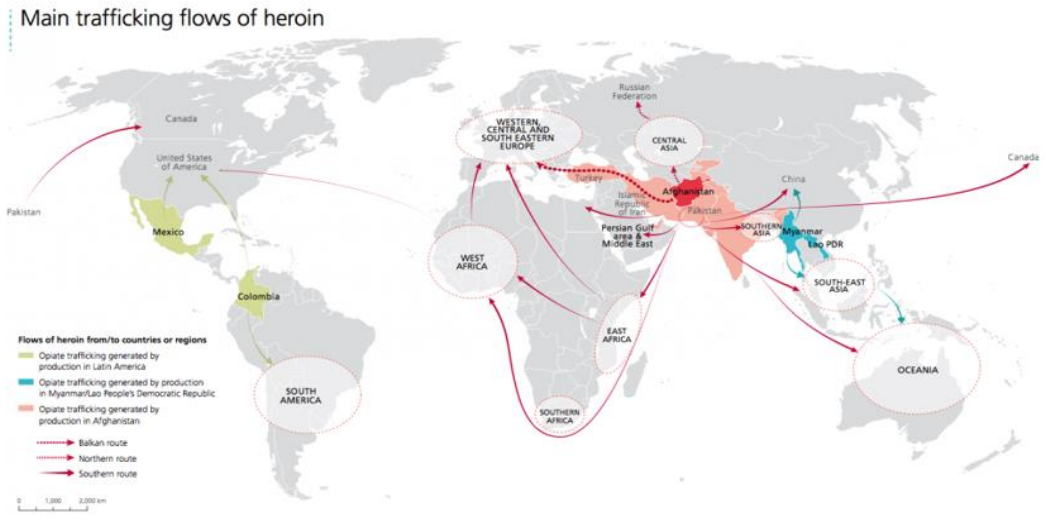
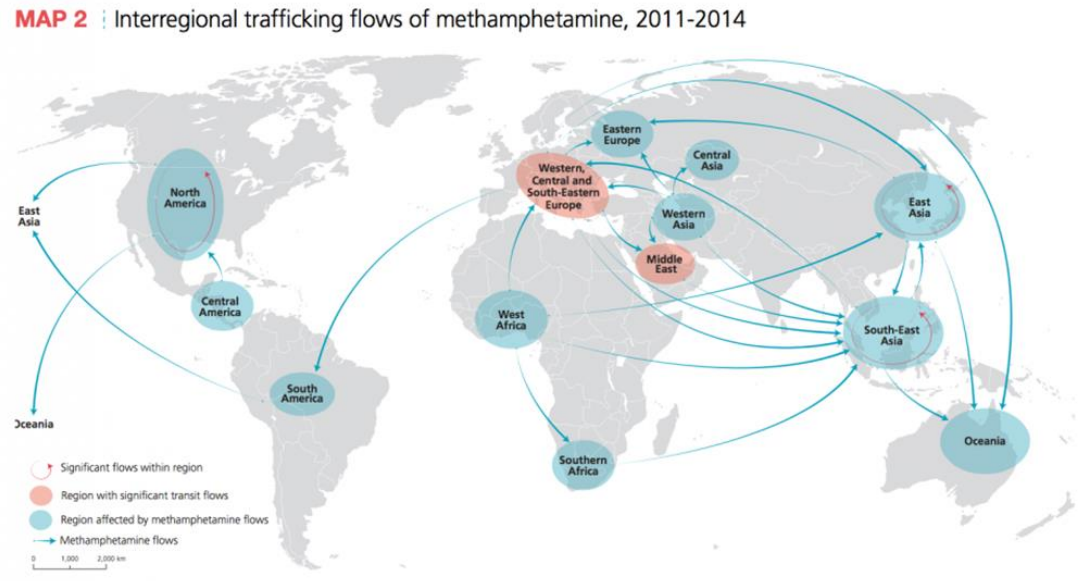
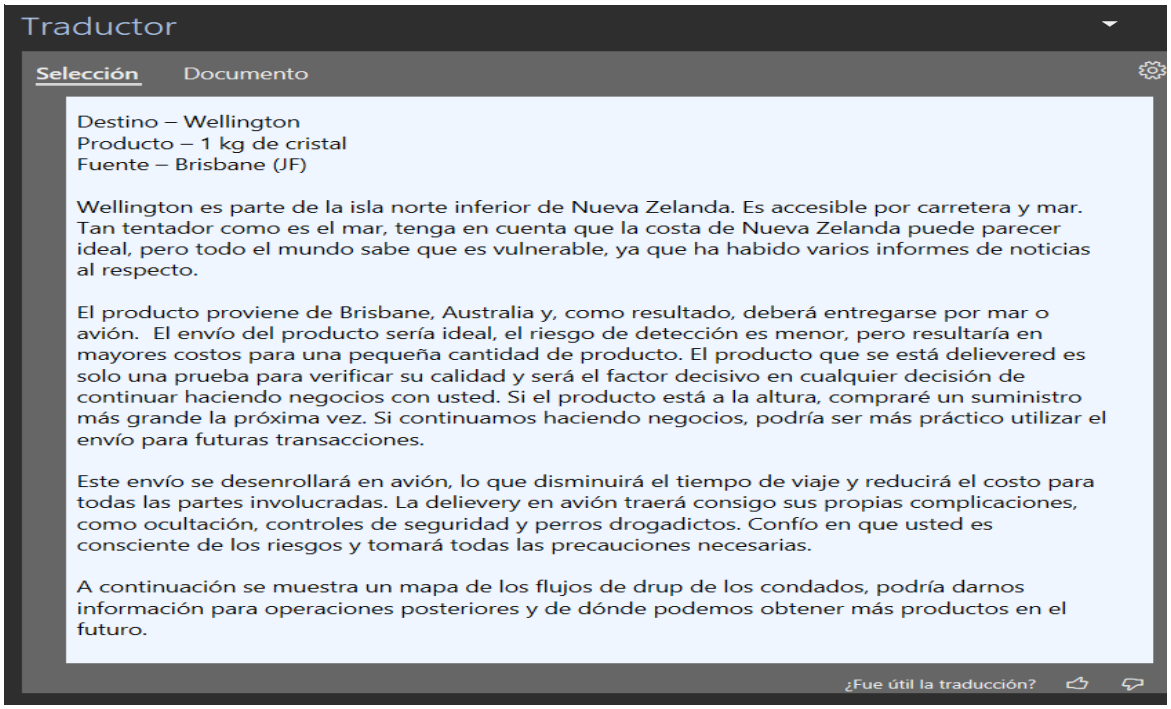


Ilustración 24. Flujos de tráfico interregional de metanfetamina (Fuente: Autopsy Documento Word f0240272.odt)



La *ilustración 22, 23 y 24* hacen parte de un documento en Word extraído del análisis forense el cual el cuerpo del texto y las imágenes son descritas en Ingles como vocabulario elegido para su desarrollo; sometido a una herramienta de traducción el cuerpo del texto declara lo siguiente:

Ilustración 25.Traducción Evidencia documento "Crystal Method" (Fuente Documento Word f0240272.odt)



Lo descrito en la *ilustración 25* evidencia la traducción de un documento enviado al parecer por Steve Kowhai a John Fredricksen en el cual detalla el modo en el que se va a realizar el envio de la mercancía, sus posibles negocios y posteriores rutas para realizar tráfico de drogas cabe resaltar que este archivo fue recuperado por el proceso de carved files del software AUTOPSY lo que se presume es que dicho documento fue cifrado dentro de otro archivo o eliminado de la unidad.

Tabla 11. Creación y modificación de la ilustración 22 que contine evidencia del documento f0240272.odt. (Fuente propia)

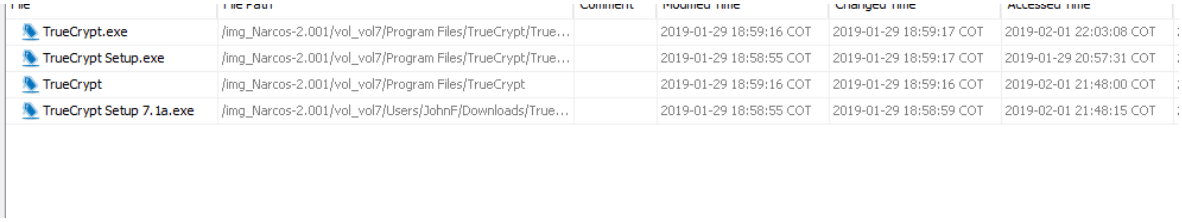
Hora de modificación	Fecha de Modificación	Fecha y hora Ultimo Acceso	Fecha y hora de creación
19:00:49	2019-01-29	2019-02-01 21:50:38	2019-01-29 19:00:48

Número 9. Utilización de softwares de encriptación y esteganografía.

Directorio de ubicación

/img_Narcos-2.001/vol_vol7/Program Files/TrueCrypt

Ilustración 26. Evidencia de software de encriptación TrueCrypt (Fuente Autopsy)



File	File Path	Comment	Modified Time	Changed Time	Accessed Time	
TrueCrypt.exe	/img_Narcos-2.001/vol_vol7/Program Files/TrueCrypt/True...		2019-01-29 18:59:16 COT	2019-01-29 18:59:17 COT	2019-02-01 22:03:08 COT	
TrueCrypt Setup.exe	/img_Narcos-2.001/vol_vol7/Program Files/TrueCrypt/True...		2019-01-29 18:58:55 COT	2019-01-29 18:59:17 COT	2019-01-29 20:57:31 COT	
TrueCrypt	/img_Narcos-2.001/vol_vol7/Program Files/TrueCrypt		2019-01-29 18:59:16 COT	2019-01-29 18:59:16 COT	2019-02-01 21:48:00 COT	
TrueCrypt Setup 7.1a.exe	/img_Narcos-2.001/vol_vol7/Users/JohnF/Downloads/True...		2019-01-29 18:58:55 COT	2019-01-29 18:58:59 COT	2019-02-01 21:48:15 COT	

La *ilustración 27* evidencia la descarga de softwares para encriptar archivos y unidades de un sistema dentro de la computadora del sospechoso John Fredricksen.

Tabla 12. Creación y modificación de la ilustración 26. (Fuente propia)

Hora de modificación	Fecha de Modificación	Fecha y hora Ultimo Acceso	Fecha y hora de creación
18:59:16	2019-01-29	2019-02-01 21:48:00	2019-01-29 18:59:16

Conclusiones

De acuerdo con las evidencias encontradas en el caso de narcotráfico sucedido en Wellington, Nueva Zelanda y tomando de apoyo los resultados obtenidos del análisis forense se darán las conclusiones para su respectiva interpretación y toma de decisiones por parte del ente que lleve a cabo el juzgamiento sobre este caso.

- Se evidencia el cargo y las intenciones que tenía el sospechoso Steve Kowhai con los otros dos cómplices por medio de una carta o correo donde específicamente detallo las operaciones que iban hacer para el transporte de la mercancía y las funciones que debían de cumplir Jane Esteban y John Fredricksen.

- Se registraron los modus operandi y respectiva relación "comercial" entre los sospechosos Steve Kowhai Y John Fredricksen, en la cual también se encontró rutas fluviales y aéreas para el trasporte de estupefacientes fuera del continente oceánico.

- Se obtuvo también evidencia en la computadora de Steve Kowhai sobre la búsqueda y ubicación de la biblioteca de "Eastbourne" mismo lugar que detalla Jane Esteban en su interrogatorio como punto de encuentro para entregar la mercancía proveniente de Brisbane Australia.
- Se evidenció también una lista de que contenía alias y nombres de presuntas personas a las cuales John Fredricksen les hacía entrega de "productos" al parecer droga y su periodo en términos de tiempo para distribuirla.

- Se logro encontrar durante los análisis la foto-captura y reservación de vuelo con destino a Wellington Nueva Zelanda por lo cual se estipula que si existía comunicación y entrega de información constante entre John Fredricksen y Steve Kowhai

Referencias

Arias, E. R. (10 de Diciembre de 2020). *Economipedia.com*. Obtenido de https://economipedia.com/definiciones/investigacion-exploratoria.html

Bonet, F. B. (14 de Abril de 2021). *Bonatti* . Obtenido de https://www.bonattipenal.com/ciberdelitos-empresariales-el-espionaje-informatico/

ConceptoDefinicion. (13 de 12 de 2021). *Narcotráfico*. Obtenido de Narcotráfico: https://conceptodefinicion.de/narcotrafico/

Contadores, T. A. (2019). *Acciones que son consideradas un delito informático en Colombia.* bogota: Tus Abogados y Contadores.

Dominguez, F. L. (2014). *Introducción a la Informatica Forense.* Madrid: RA-MA S.A.

Elizarrarás, J. C. (2007). *El Estudio de Caso en las Relaciones Jurídicas Internacionales, Modalidades de Aplicación del Derecho Internacional.* Ciudad de Mexico: Universidad Nacional Autonoma de Mexico.

idpc. (2012). *International Drug Policy Consortium*. Obtenido de International Drug Policy Consortium: https://idpc.net/es/oceania

Legis, Ambito Juridico . (07 de Noviembre de 2018). *Legis, Ambito Juridico* . Obtenido de https://www.ambitojuridico.com/noticias/tecnologia/tic/las-imagenes-forenses-y-su-uso-en-procesos-judiciales

NIDA. (9 de 11 de 2021). *QUE ES LA METANFETAMINA?* Obtenido de QUE ES LA METANFETAMINA?: https://www.drugabuse.gov/es/publicaciones/serie-de-reportes/abuso-y-adiccion-la-metanfetamina/que-es-la-metanfetamina

Observatorio de Delitos Informaticos de Bolivia. (01 de Septiembre de 2018). *Observatorio de Delitos Informaticos de Bolivia*. Obtenido de https://www.odibolivia.org/2018/09/01/fraude-estafa-informatica/

Porolli, M. (12 de agosto de 2013). *welivesecurity*. Obtenido de https://www.welivesecurity.com/la-es/2013/08/12/en-que-consiste-analisis-forense-de-informacion/

POSTGRADO, C. E. (8 de 11 de 2021). *CEUPE*. Obtenido de CEUPE: https://ceupe.mx/blog/que-es-una-aduana.html

Sede Electronica, Real casa de la moneda y Timbre Española . (2021). *Sede Electronica, Real casa de la moneda y Timbre Española*. Obtenido de https://www.sede.fnmt.gob.es/preguntas-frecuentes/otras-preguntas/-/asset_publisher/1RphW9IeUoAH/content/1024-que-es-la-encriptacion-o-cifrado-?inheritRedirect=false

Significados. (02 de 11 de 2021). *Significados*. Obtenido de Significados: https://www.significados.com/delitos-informaticos/

Unidad de Investigación Criminal de la Defensa. (08 de Mayo de 2019). *Unidad de Investigación Criminal de la Defensa*. Obtenido de https://uid.org.co/los-tipos-de-delitos-informaticos-mas-comunes-en-colombia/

UNIVERSO, E. (12 de 08 de 2020). *¿Cuál es el procedimiento para hacer un allanamiento?* Obtenido de ¿Cuál es el procedimiento para hacer un allanamiento?: https://www.eluniverso.com/noticias/2020/08/12/nota/7939456/cual-es-procedimiento-hacer-allanamiento-ecuador/

welivesecurity. (15 de 04 de 2015). *5 fases fundamentales del análisis forense digital*. Obtenido de 5 fases fundamentales del análisis forense digital: https://www.welivesecurity.com/la-es/2015/04/15/5-fases-analisis-forense-digital/

welivesecurity. (15 de 04 de 2015). *5 fases fundamentales del análisis forense digital*. Obtenido de 5 fases fundamentales del análisis forense digital: https://www.welivesecurity.com/la-es/2015/04/15/5-fases-analisis-forense-digital/