Manizales, agosto 29 de 2023

Señores
Empresa Caballitos de Palo
La Ciudad

OBJETIVO DEL ANÁLISIS

Realizar análisis forense de la escena del crimen encontrada en el caso 3, durante el proceso de evaluación de la asignatura Computo Forense.

El caso refiere a la empresa Caballitos de Palo, donde el jefe de la empresa reporta que contrató a 3 personas expertas en sistemas y un día viajó a Bogotá y presuntamente estas personas se le llevaron un dinero.

Sin embargo, el técnico en Sistema de la empresa alcanzó a sacar 3 imágenes de sus equipos antes que se realizarán técnicas anti forenses y no dejarán información alguna que sirva para la investigación

Se realizará el análisis de 3 imágenes encontradas en la memoria USB Kingston con capacidad de 57 GB de espacio disponible y con espacio usado de 749 MB y nombrada "*Practica*":

IMAGEN 1: Chris

Marca **:** Kingston DataTraveler 2.0 USB
Capacidad **:** 64 GIGAS
Serial **:** 0E0F244011D9

IMAGEN 2: Holly

Marca **:** Kingston DataTraveler 2.0 USB
Capacidad **:** 64 GB
Serial **:** 0E0F244011D9

Imagen 3: Mantooth

Marca **:** Kingston DataTraveler 2.0 USB
Capacidad **:** 64 GB
Serial **:** 0E0F244011D9

También se realizará análisis a la escena del crimen, donde se verificarán y se listarán las potenciales evidencias que nos indique el sitio. Para ello dispondremos de personal Forense Experto en crímenes digitales y análisis de evidencias digitales.

IDENTIFICACIÓN DEL ELEMENTOS A ANALIZAR

NUM. EVIDENCIA	DESCRIPCIÓN DE LA EVIDENCIA
01	Kingston DataTraveler 2.0 USB Device
02	USB2.0 Flash Disk USB Device

IDENTIFICACIÓN DEL PROCEDIMIENTO

1. Se realiza una fijación fotográfica de la evidencia.
2. Es utilizado el software Autopsy para el análisis de las imágenes encontradas en la escena del crimen
3. Extracción de la información que contienen dichas imágenes
4. Identificar el posible sospechoso según hipótesis de investigadores

RESULTADO DEL ANÁLSIS

Se ingresa a la escena del crimen siendo las 10:48:00 am hora colombiana, ubicado en la Universidad Católica de Manizales, en el bloque A salón de clases A-204. Inicialmente, ingresa el experto forense, encargado de revisar de primera mano la escena del crimen y quién empieza a dar indicaciones para el personal que lo acompaña. Los acompañantes son: Fotógrafo, Topógrafo, Recolector y escribiente; quienes serán apoyo para realizar el levantamiento de la información y resolución del caso dado.

En la escena, se encuentran algunos dispositivos ubicados en el suelo como discos duros, cámaras, unidad de DVD y otros como audífonos, calculadora y lector de tarjetas seriales, esparcidos de manera aleatoria y sin un patrón fijo, se tratan de identificar los relevantes y que sirvan como posible evidencia.

Al lado izquierdo del ingreso al salón, se encuentra un escritorio con ordenador de escritorio Marca HP con su respectivo monitor y teclado. En este escritorio se encuentran algunos elementos sospechosos como algunos dispositivos USB, SIM CARD y un posible artefacto explosivo. Se recomienda a todo el personal en sitio tratar de no manipular dicho elemento hasta que se encuentre personal antiexplosivos en el lugar de los hechos. Se verifican todos los compartimientos del escritorio y se verifica el estado de encendido del PC, el equipo en el momento del acceso se encontraba apagado y con los periféricos mencionados conectados.

Al momento de ingresar a la escena del crimen se encuentra un sospechoso ubicado en la parte final del salón, el cual se retiene y se le solicita toda la información de identificación; la expresa y se realiza su respectiva inspección para verificar que no tenga algún elemento que pueda inicialmente afectar de manera violenta al Experto Forense y algún elemento que intervenga o modifique la escena del crimen. Es identificado con la cédula de ciudadanía 1053789054 expresa que su nombre es Andrés Vargas. Es puesto a disposición de la autoridad competente para que lo retenga mientras se concluye la investigación de la escena del Crimen.

En la pared derecha y al fondo del salón se encuentra un tablero con algunos bosquejos, donde nos presenta una ubicación entre los bloques A, B, C y D. Se toma esta imagen como evidencia debido a un posible punto de encuentro. En dicho tablero, también se encuentran 2 evidencias más: una tarjeta bancaria y una SIM CARD ubicadas en la parte inferior izquierda y en la parte superior izquierda del tablero respectivamente. Se toma registro fotográfico y se enumeran como evidencias relevantes dentro de la escena.

Adicional a eso, el Experto Forense sigue con la identificación de potenciales evidencias; encontrando en el basurero de dicho salón algunos elementos más, un disco duro encontrado en la bolsa de la basura y tirado como si se tratara de un desecho. Y algunos dispositivos USB encontrados fuera de la bolsa de basura, pero dentro del recipiente de basura. Se toman evidencias fotográficas y se numeran dichos elementos como evidencia para análisis del caso.

Después de identificar las evidencias, se inicia con el proceso de marcación, donde se enumerará de 1 a n, dependiendo el numero de evidencias y se iniciará el barrido de marcación, desde la entrada a la escena del crimen; que inicia en la puerta de entrada al salón hasta finalizar el recorrido por el salón al fondo del mismo. Se inicia registro fotográfico de manera simultanea con la marcación y se registra en video dicha marcación donde se indicará que tipo de evidencia se encontró, consecutivo y alguna descripción breve de porque se reconoce como evidencia. Para el registro fotográfico se utilizan los testigos métricos

suministrados donde nos indicará el tamaño de los elementos y tener como pruebas al momento de llevar al juzgado.

Siendo las 11:25:00 am, hora colombiana, se finaliza la inspección visual y recolección de evidencias de la escena del Crimen. A partir de este momento se inicia el proceso de embalaje de evidencias en los respectivos medios utilizados para conservar la evidencia. Se registran de manera fotográfica las evidencias ya embaladas y rotuladas debidamente para entregar a cadena de custodia.

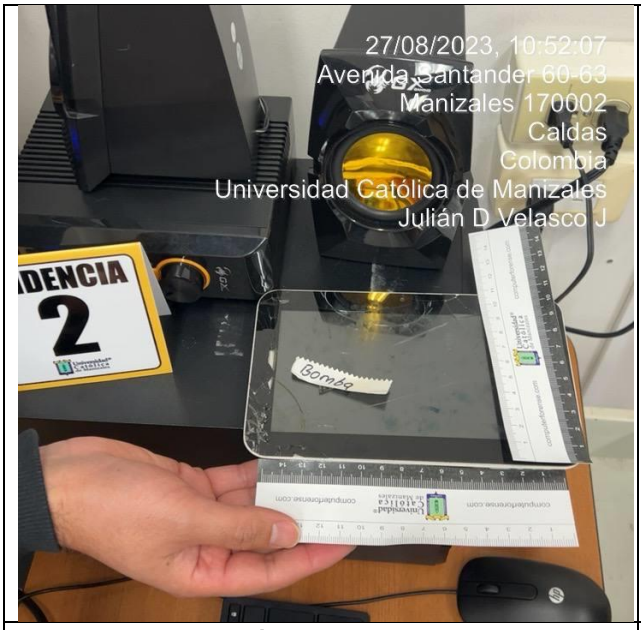
Fijación Fotográfica

EVIDENCIA 1:

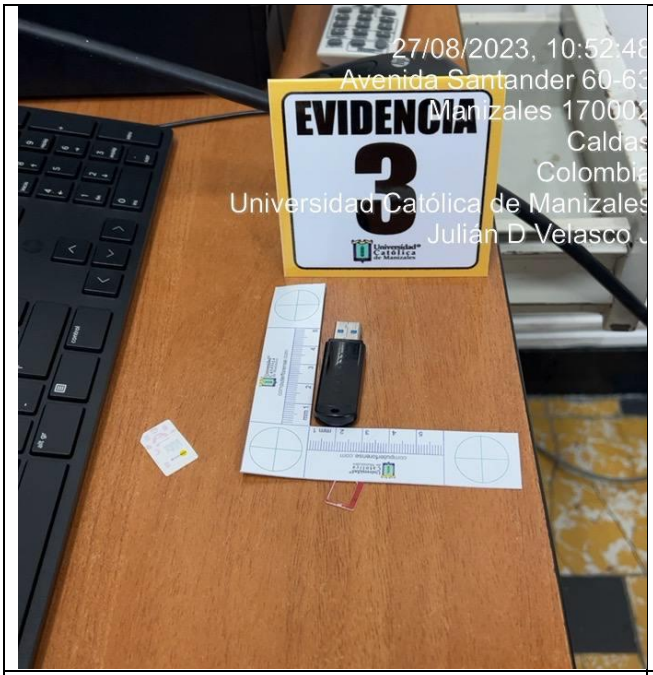
Identificación del PC de escritorio

Identificación de la Evidencia
Marca: Computador de Escritorio HP
Capacidad: Disco duro 500GB RAM 8GB
Serial: FN0LA1DK

EVIDENCIA 2:

	
Identificación Artefacto Explosivo	***Embalaje Evidencia 2***
Identificación de la Evidencia **Marca: Tablet** **Capacidad: Sin identificar** **Serial: N.A**	

EVIDENCIA 3:

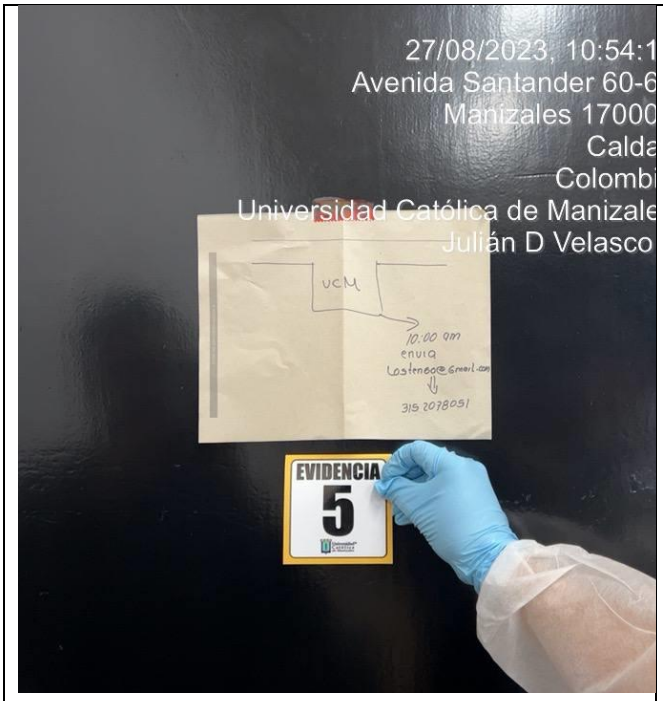
	
Identificación Dispositivo USB	***Embalaje Evidencia 3***
Identificación de la Evidencia **Marca: Kingston USB** **Capacidad: ---** **Serial: C9079383663D33193**	

EVIDENCIA 4:

Identificación Sim Card ubicada debajo del Teclado del PC

Identificación de la Evidencia
Marca: SiMCARD Claro
Capacidad: Sin Identificar
Serial: N.A

EVIDENCIA 5:

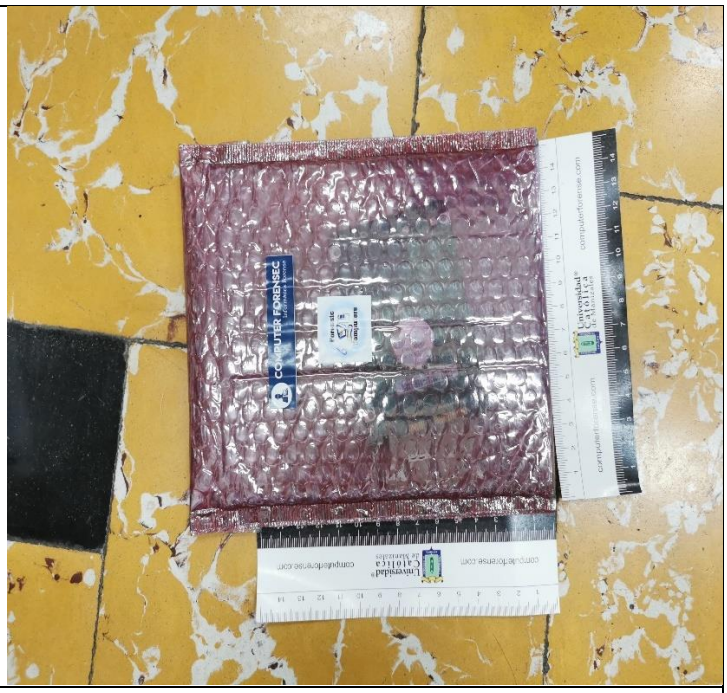


Identificación Hoja con información

Embalaje Evidencia 5

Identificación de la Evidencia
Marca: N.A
Capacidad: N.A
Serial: N.A

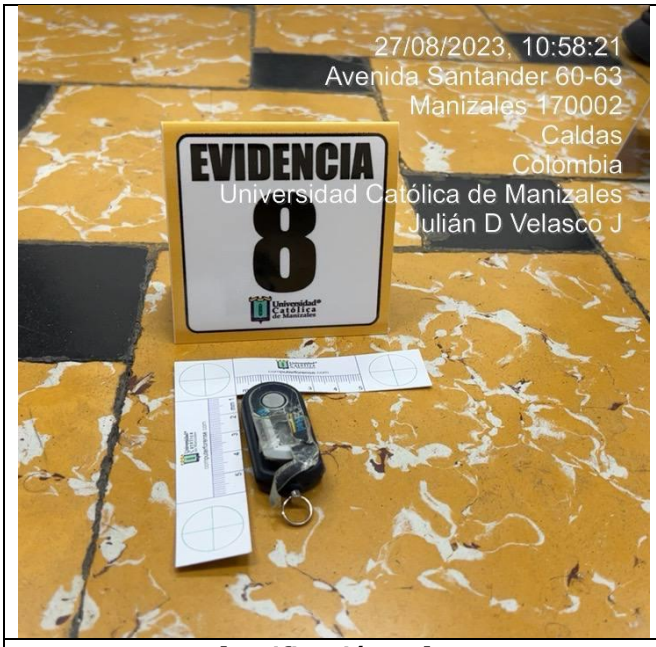
EVIDENCIA 6:

	
Identificación Disco Duro	***Embalaje Evidencia 6***
Identificación de la Evidencia **Marca: Sin identificar** **Capacidad: Sin identificar** **Serial: Sin identificar**	

EVIDENCIA 2:

	
Identificación Dispositivo USB	***Embalaje Evidencia 7***
Identificación de la Evidencia **Marca: Kingston** **Capacidad: Sin identificar** **Serial: Sin identificar**	

EVIDENCIA 8:

	
Identificación Token	***Embalaje Evidencia 8***
Identificación de la Evidencia **Marca: Token** **Capacidad: N.A.** **Serial: N.A**	

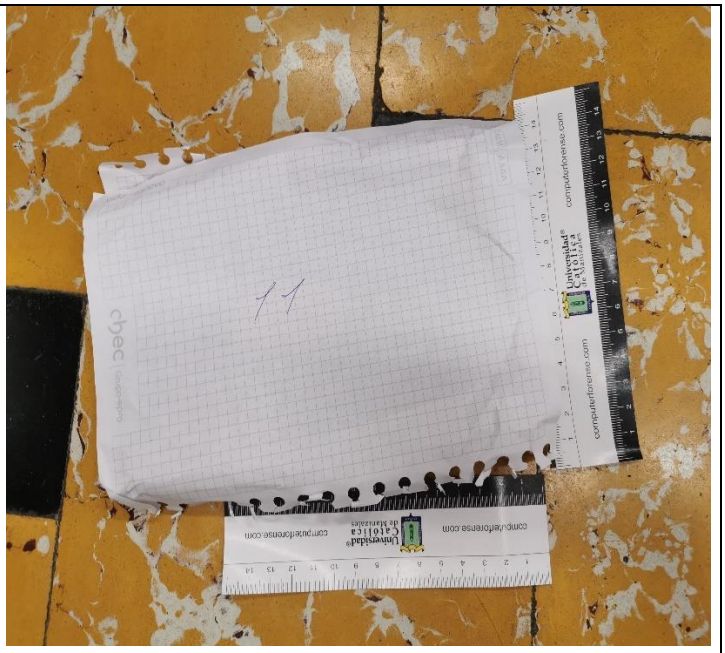
EVIDENCIA 9:

	
Identificación CD Rom - Partido	***Embalaje Evidencia 9***
Identificación de la Evidencia **Marca: CD** **Capacidad: 193 MB** **Serial:**	

EVIDENCIA 10:

	
Identificación Cámara fotográfica 1	***Embalaje Evidencia 10***
Identificación de la Evidencia **Marca: Akon** **Capacidad: Sin identificar** **Serial: Sin identificar**	

EVIDENCIA 11:

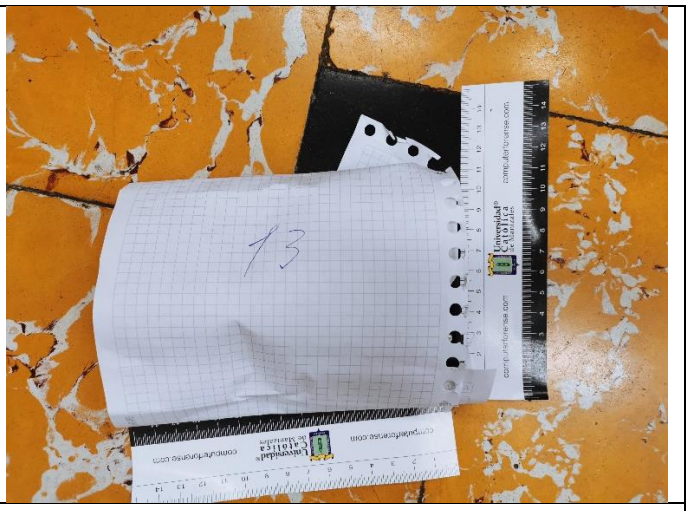
	
Identificación Tablet	***Embalaje Evidencia 11***
Identificación de la Evidencia **Marca: Asus** **Capacidad: Sin identificar** **Serial: Sin identificar**	

EVIDENCIA 12:

Identificación Dispositivos USB	*Embalaje Evidencia 12*

Identificación de la Evidencia
Marca: Kingston
Capacidad: Sin identificar
Serial: Sin identificar

EVIDENCIA 13:

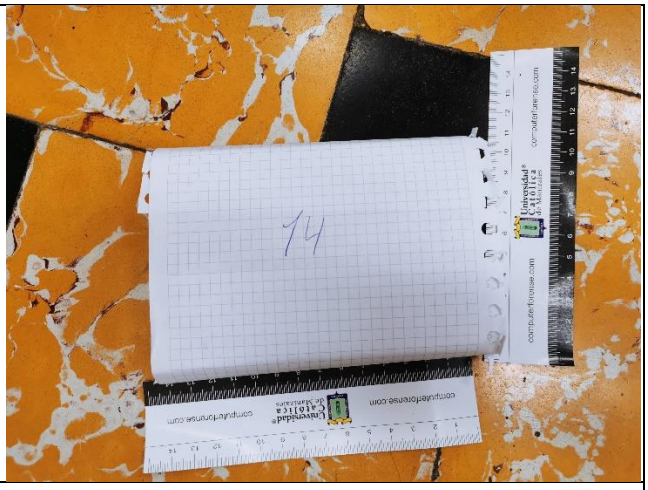


Identificación Disco duro 1	*Embalaje Evidencia 13*

Identificación de la Evidencia
Marca: Sin identificar
Capacidad: Sin identificar
Serial: Sin identificar

EVIDENCIA 14:

Identificación Disco Duro 2

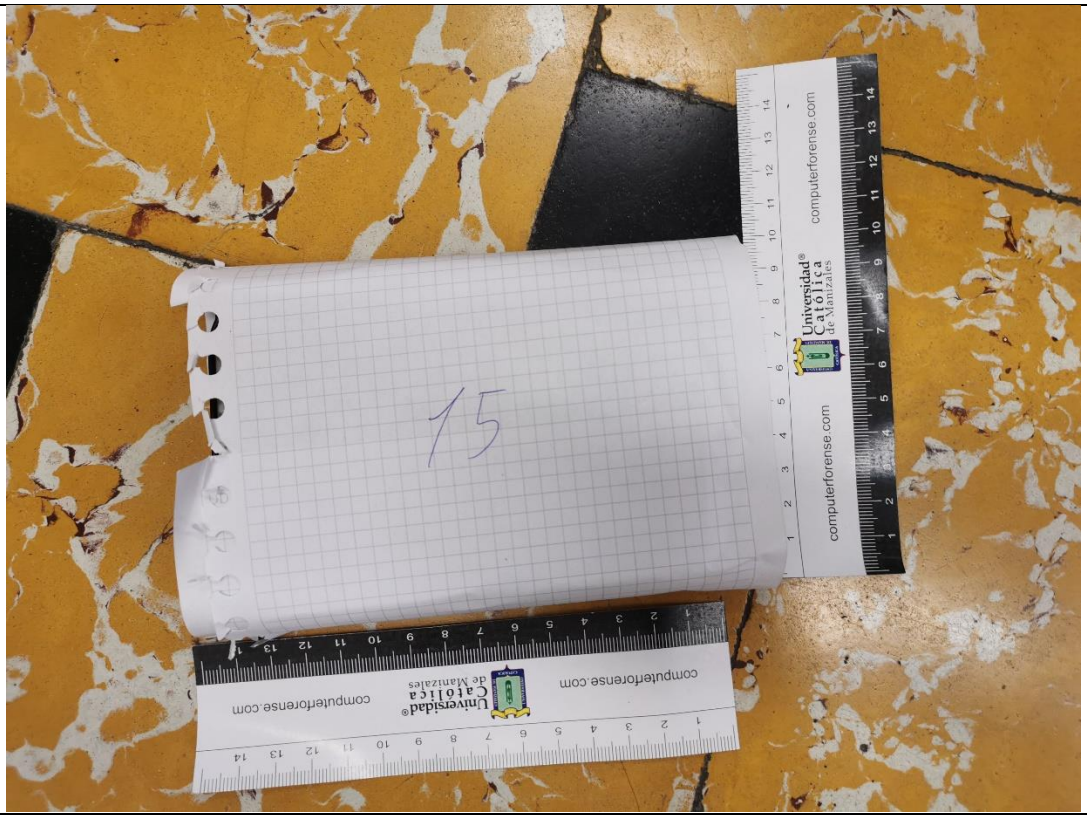


Embalaje Evidencia 14

Identificación de la Evidencia
Marca: Sin identificar
Capacidad: Sin identificar
Serial: Sin identificar

EVIDENCIA 15:

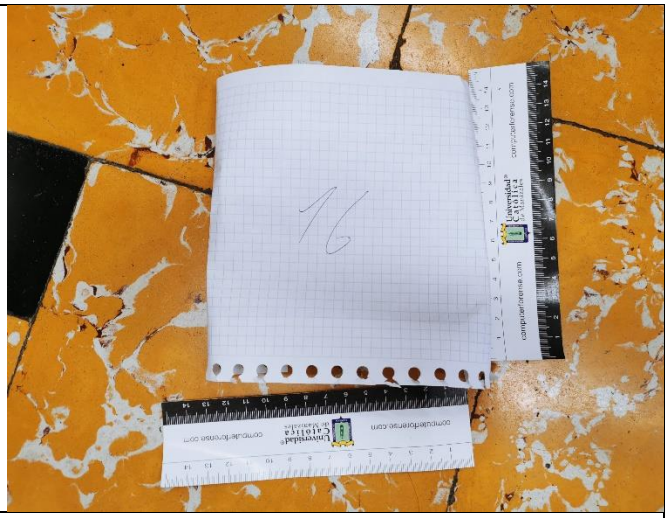
Identificación Disco Duro 3



Embalaje Evidencia 15

Identificación de la Evidencia
Marca: SAMSUNG
Capacidad: 80 GB SATA
Serial: SODEJ1NLC49126

EVIDENCIA 16:



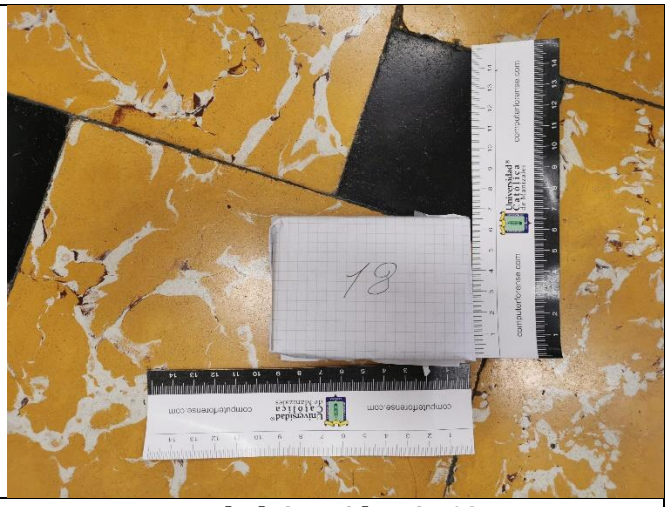
Identificación Unidad de Lectura | ***Embalaje Evidencia 16***

Identificación de la Evidencia
Marca: Sin identificar
Capacidad: Sin identificar
Serial: Sin identificar

EVIDENCIA 17:

	
Identificación Cámara fotográfica 2	***Embalaje Evidencia 17***
Identificación de la Evidencia **Marca: Sin identificar** **Capacidad:** Sin identificar **Serial: Sin identificar**	

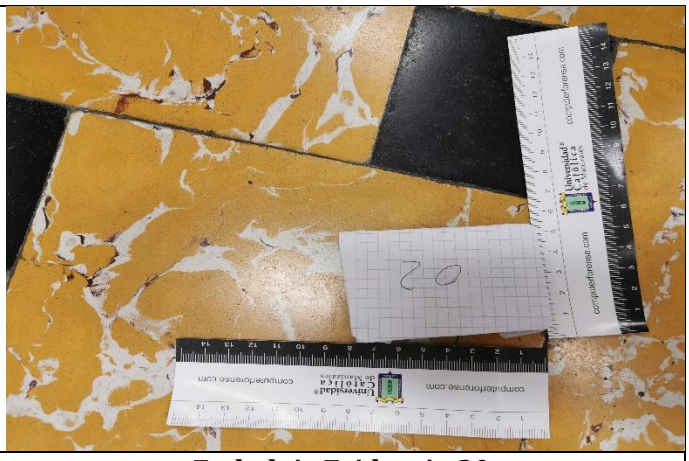
EVIDENCIA 18:

	
Identificación Disco Duro 4	***Embalaje Evidencia 18***
Identificación de la Evidencia **Marca: Sin identificar** **Capacidad:** Sin identificar **Serial: Sin identificar**	

EVIDENCIA 19:

	
Identificación CD rom - Quebrado	***Embalaje Evidencia 19***
Identificación de la Evidencia **Marca: Sin identificar** **Capacidad:** Sin identificar **Serial: Sin identificar**	

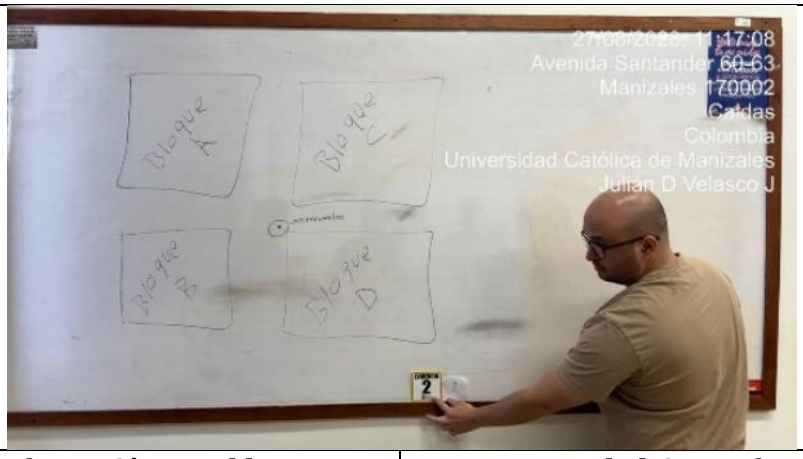
EVIDENCIA 20:

	
Identificación Tarjeta Bancaria	***Embalaje Evidencia 20***
Identificación de la Evidencia **Marca: entidad emisora Davivienda** **Capacidad:** Sin identificar **Serial: Sin identificar**	

EVIDENCIA 21:

	
Identificación Sim Card	***Embalaje Evidencia 21***
Identificación de la Evidencia **Marca: Claro** **Capacidad: 1 KB** **Serial: N.A**	

EVIDENCIA 22:

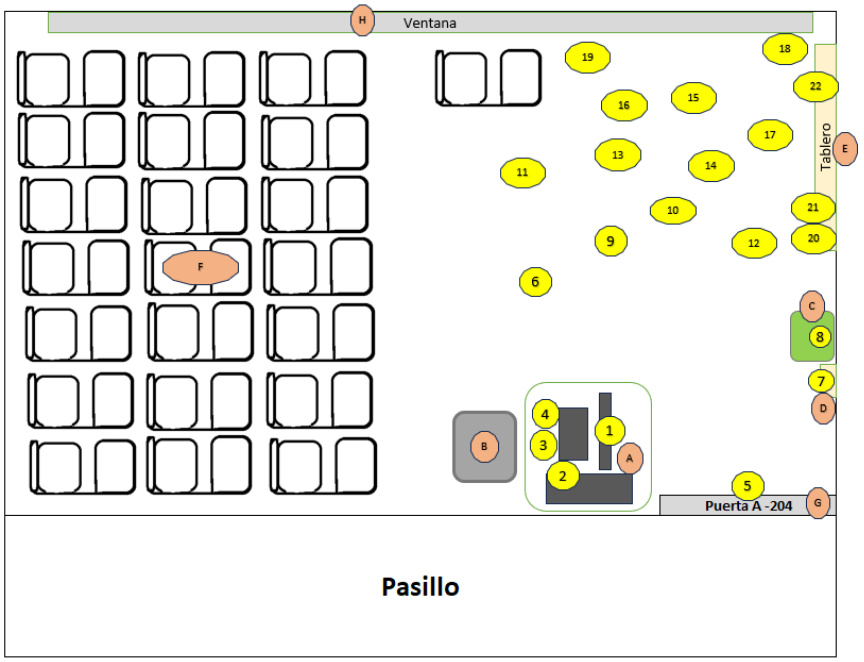
	
Identificación Información en tablero	***Embalaje Artefacto Explosivo***
Identificación de la Evidencia **Marca: N.A** **Capacidad: N.A** **Serial: N.A**	

TOPOGRAFIA

ESCENA DE LOS HECHOS

Referencia:
A. Escritorio
B. Silla escritorio
C. Basurero
D. Interruptor
E. Tablero
F. Sillas estudiantiles
G. Puerta de acceso al salon
H. Ventana

Evidencia:
1 Equipo de computo marca HP - S/N FN0LA1DK
2 Tablet - Sin identificar
3 Kingston USB - C9079383663D33193
4 SiMCARD Claro
5 Hoja - ruta de escape
6 Disco Duro - Sin identificar Serial
7 USB Kingston - Sin identificar Serial
8 Token - Sin identificar Serial
9 CD Rom - Partido - Serial 018343642355
10 Cámara fotográfica 1 - Marca Akon
11 Tablet - Serial sin identificar
12 2 USB - Kingston - Serial sin identificar
13 Disco duro - Serial sin identificar
14 Disco duro - Serial sin identificar
15 Disco duro - S/N SODEJ1NLC49126 - SAMSUNG
16 Unidad de Lectura - Serial sin identificar
17 Cámara fotográfica 2 - Serial sin identificar
18 Disco duro - Serial sin identificar
19 CD Rom - Partido - Serial sin identificar
20 Tarjeta Bancaria - Davivienda
21 Sim Card - Claro
22 Información en tablero - Punto de encuentro



Ubicación: Universidad Catolica de Manizales, bloque A, Piso 2, Salon A 204
Dirección: Av. Santander #No. 60, Manizales, Caldas
Georefrenciación Long. Latitud: 5.060682477204778, -75.48739954931483

EVIDENCIA IMÁGENES USB

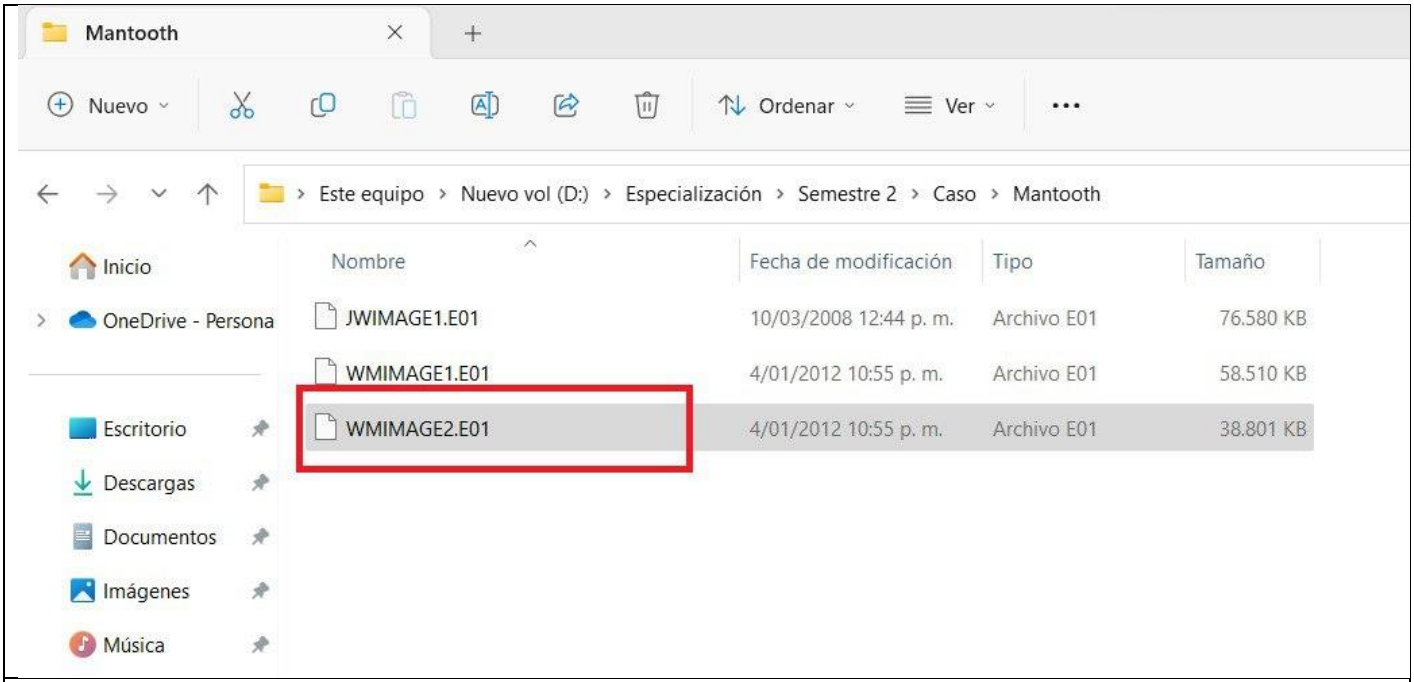
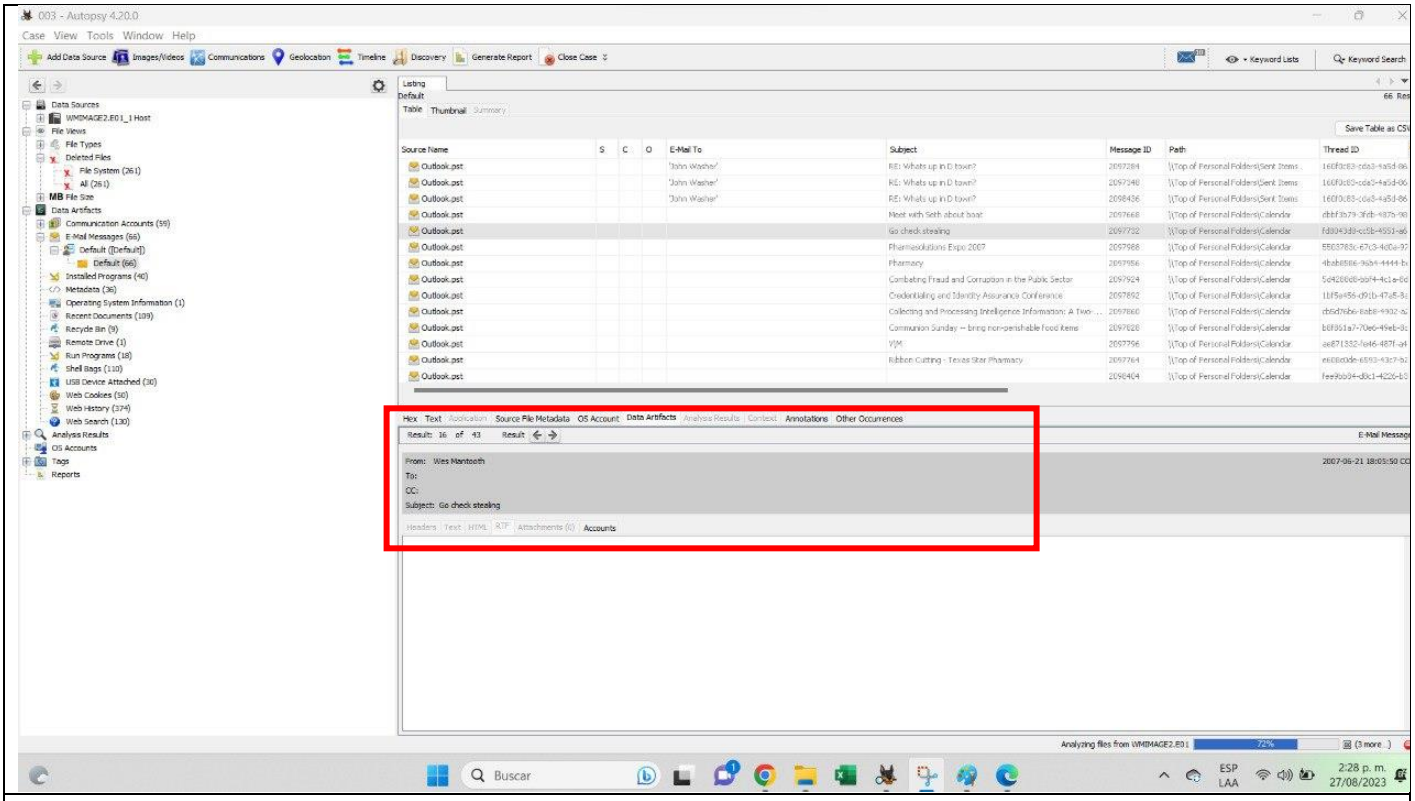
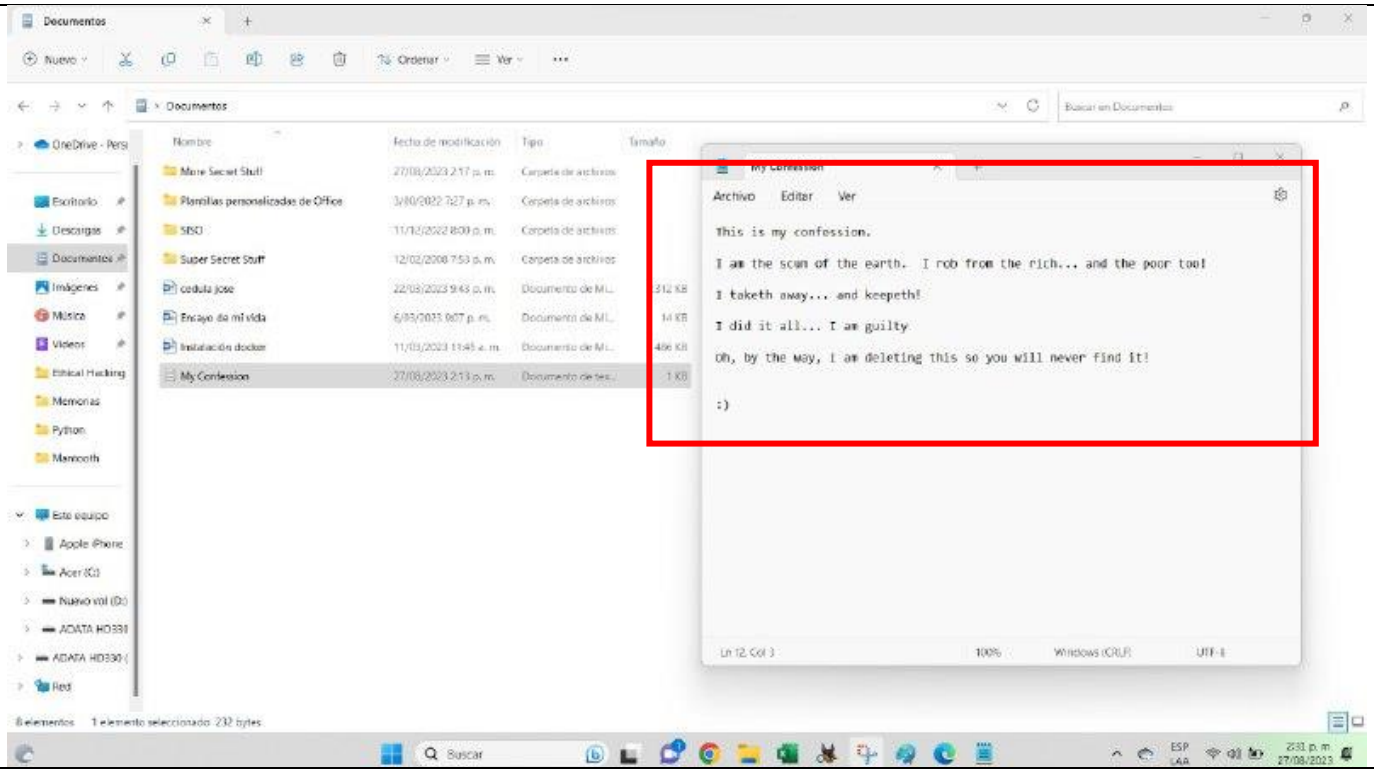


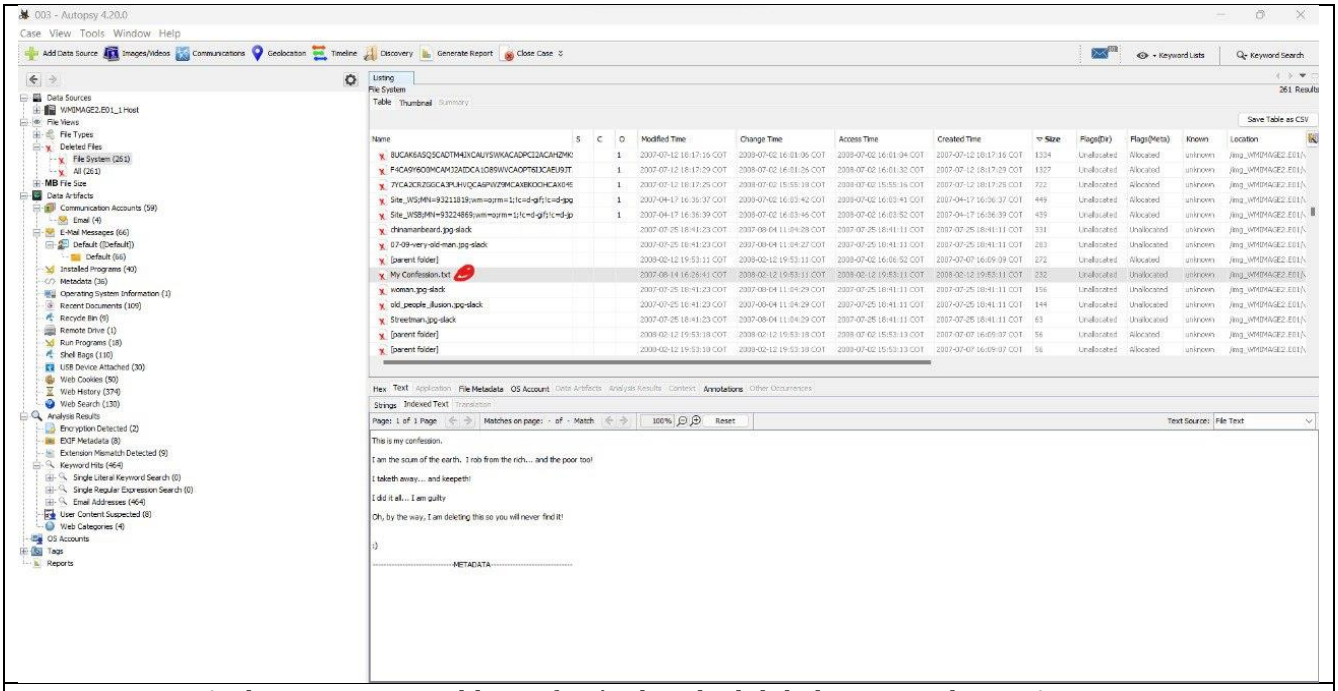
Imagen Analizada de Posible Sospechoso
Tamaño: 38.801 KB



Correo Sospechoso con Información de un robo
Tamaño: 232 KB



Archivo Txt con posible confesión de culpabilidad
Tamaño: 1 KB



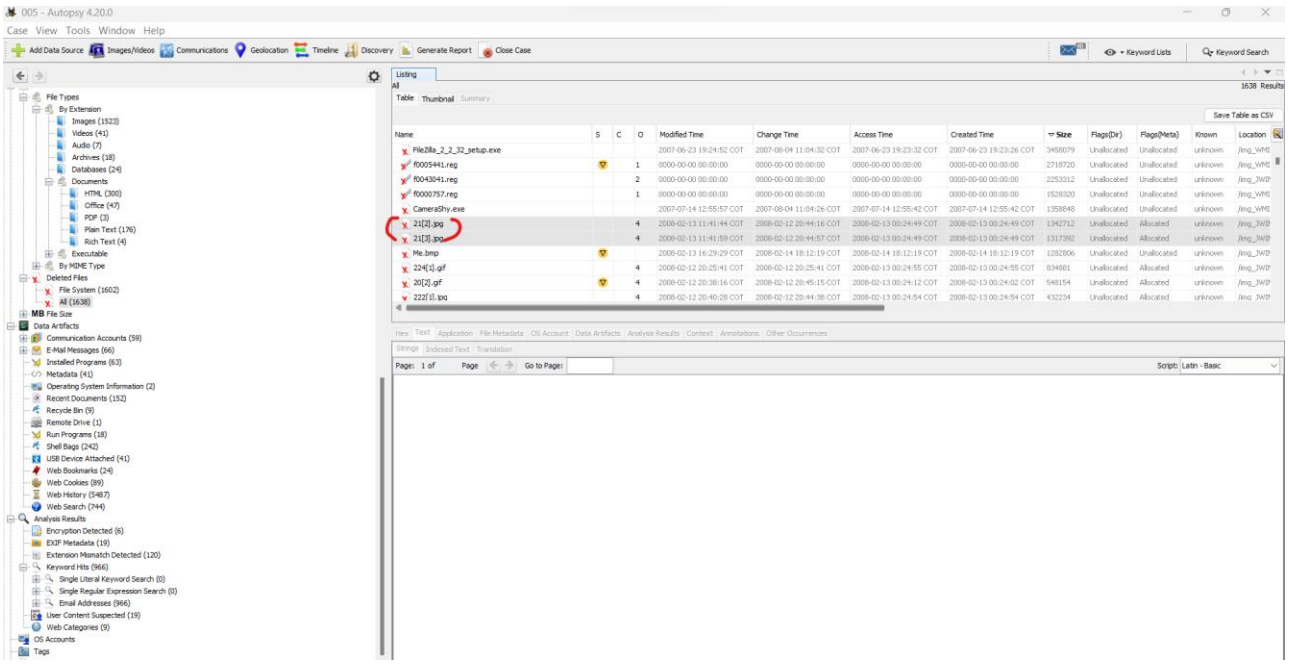
Archivo Txt con posible confesión de culpabilidad encontrado con Autopsy
Tamaño: 1 KB

Imágenes encontradas del posible sospechoso
Tamaño: 18 KB

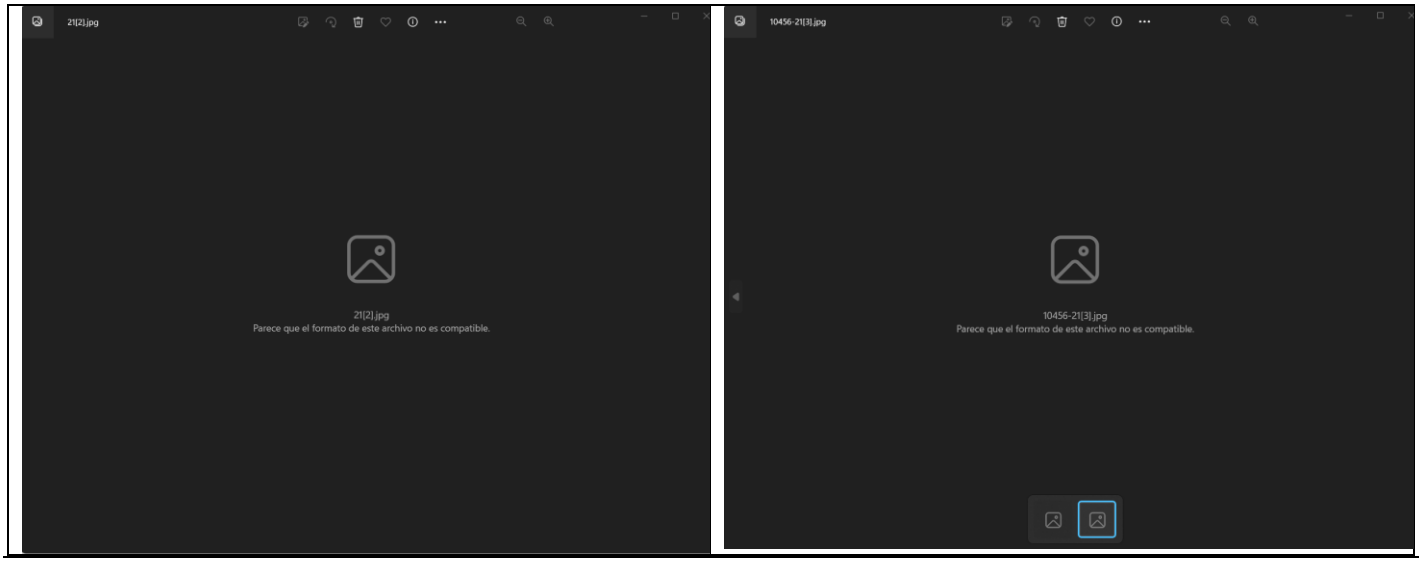
Presentación relacionada con robos a cajeros automáticos Tamaño: 558 KB
Archivo Txt con posible confesión de culpabilidad Tamaño: 1 KB

Imagen encontrada dentro de los archivos recuperados
Tamaño: 1 KB

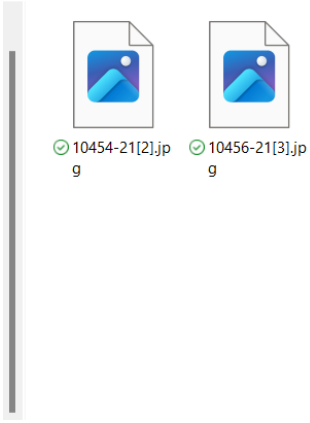
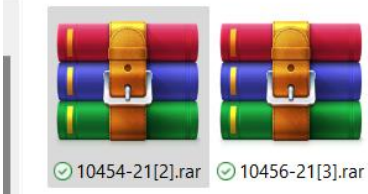
Al realizar el análisis en los archivos eliminados de la imagen JWIMAGE1.E01, se identificaron dos archivos con extensión .jpg, eliminados, pero estos no permiten ser visualizados, generando error en la compatibilidad de lectura.



Al tratar de abrir los archivos 21[2].jpg y 21[3].jpg

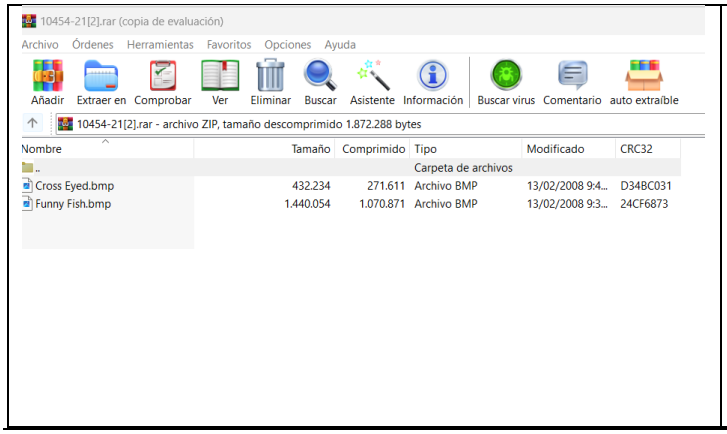


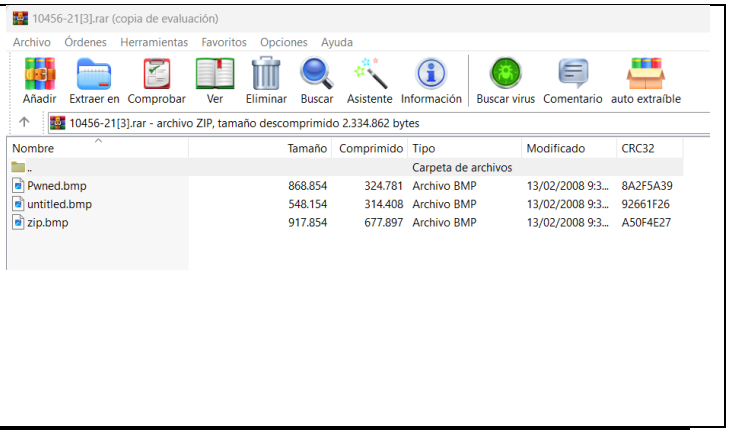
Se pudo evidenciar que los archivos tienen una extensión .jpg falsa y se evidencia que son archivos .rar pues al realizar el cambio de extensión a la .rar se visualizan imágenes dentro de cada uno de los archivos.

Extensión original .jpg	Se modifica Extensión a .rar
	

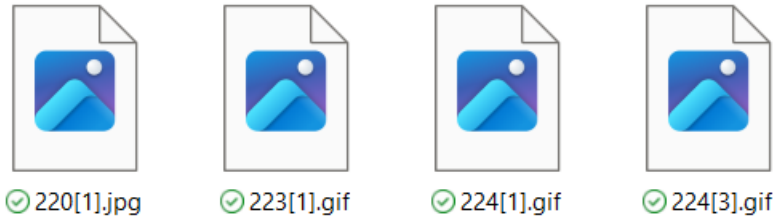
Al verificar dentro de los archivos, se encontraron imágenes ocultas dentro de los archivos .jpg

Imágenes ocultas en el archivo 21[2].jpg	Imágenes ocultas en el archivo 21[3].jpg

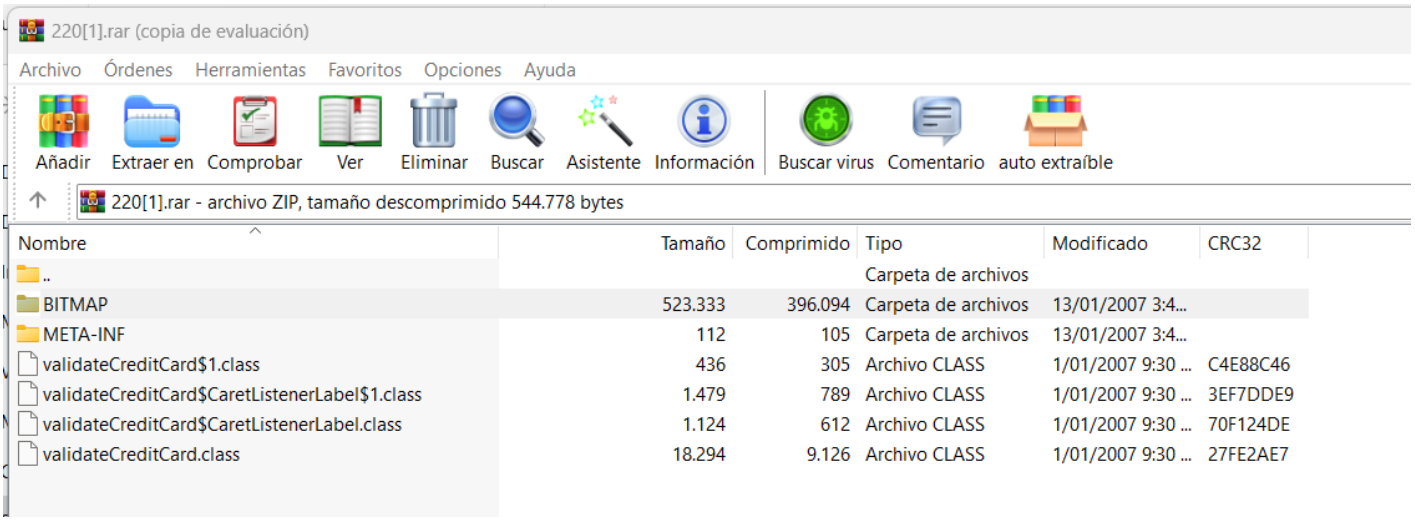


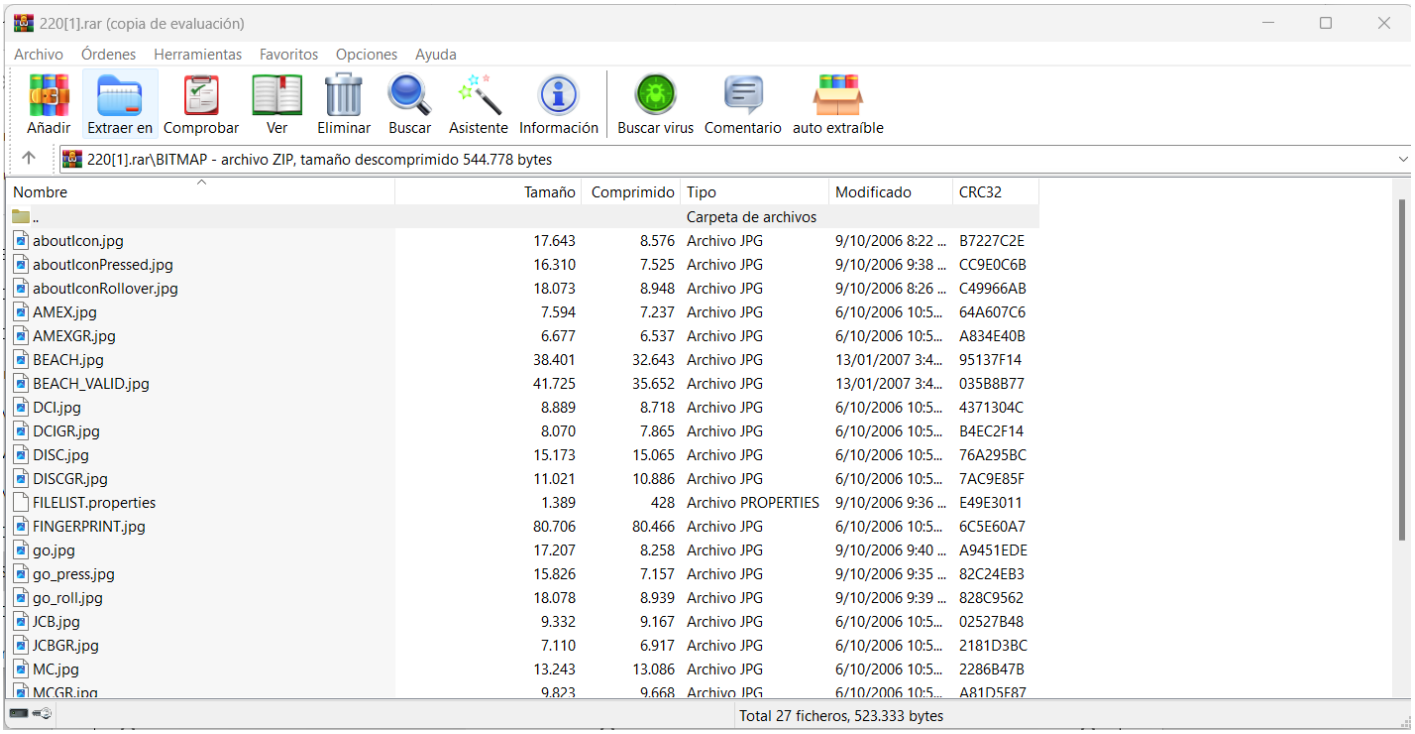


De acuerdo con lo anterior, se procede a revisar más imágenes con la extensión .jpg en los archivos eliminados, ya que se encuentran más archivos con esta extensión que no se pueden visualizar de manera normal, se realiza la validación de los siguientes archivos .jpg en la imagen JWIMAGE1.E01, encontrando que los archivos no son compatibles y no se permiten abrir. Puede ser que estaba realizando pruebas de como ocultar información con extensiones conocidas.



Se realiza el cambio de extensión a * .rar encontrando información relevante a tarjetas de crédito ocultas dentro de estos archivos como se evidencia a continuación:





HIPOTÉSIS:

Después de la documentación, marcación, recolección y embalaje de las evidencias, se realizan los análisis pertinentes a las memorias USB y sus respectivas imágenes para brindar la posible hipótesis del caso:

- **Se evidencia que en los correos electrónicos se comunica con el usuario dollarhigh86@comcast.net, para realizar acciones delictivas, incluida el robo de cajeros automáticos**
- **Según información extraída, se evidencia páginas consultadas para la fabricación de estupefacientes. Específicamente Metanfetaminas y diferentes tipos de drogas farmacéuticas y de fácil expendio en las calles**
- **Se verifica también en archivos encontrados, confesiones como culpabilidad en robos e ideas relacionadas con asesinar a familiares.**
- **Se encuentran presentaciones, imágenes y videos, de como montar y utilizar Skimmer en cajeros automáticos.**

Teniendo en cuenta lo descrito anteriormente, extraído de la imagen del Usuario: Mantooth, y que no se halló evidencia comprometedora relacionada al caso en las imágenes de Chris y Holly; consideramos que Mantooth es el sospechoso principal. Debido a las evidencias halladas, se podría indicar que requiere algún tipo de ingresos extras para realizar todo tipo de actividades delictivas encontradas en su ordenador. Para ello se sugiere realizar un análisis detallado a las declaraciones que pueda presentar el acusado frente a las evidencias encontradas, a partir de allí se podrían debatir nuevas conclusiones frente a su culpabilidad. Sin embargo, según los archivos encontrados todo apunta a que Mantooth viene presentando planeación de una actividad delictiva desde tiempo atrás y según su perfil debería ser investigado a profundidad.

Violaciones Ley 1273 de 2009:

Artículo 269I: Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red

de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

OBSERVACIONES

Una vez analizadas las 3 imágenes encontradas en el dispositivo digital encontrado en la escena del crimen, y se logra llegar a una hipótesis del posible sospechoso inicialmente. Para ello, se recolectan tanto las evidencias físicas que se encontraron en la escena del crimen, como las evidencias digitales, como prueba fehaciente de que Mantooth es un potencial criminal. Sin embargo, todo esto son hipótesis generadas por lo encontrado, se espera realizar un análisis detallado con las declaraciones del sospechoso y en el caso extremo con las actitudes y respuestas ante un juzgado.

Según la información extraída, se evidencia en Mantooth un comportamiento de un criminal potencial quién con su contenido digital logra recalcar posibles actos que atenten contra la vida de las personas, activos digitales bancarios y expendio y fabricación de drogas caseras. Con todo el material recolectado se espera tomar las medidas de aprehensión contra el personaje mencionado y se encuentra bajo la responsabilidad de las autoridades competentes.

De esta manera se rinde el informe, para los fines pertinentes.

Firma,

_____