|  |  |
| --- | --- |
| **ACTA- N°** | **0312** |

**SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

**OFICINA DE TECNOLOGÍA E INFORMÁTICA**

**GRUPO DE TRABAJO DE INFORMÁTICA FORENSE Y SEGURIDAD DIGITAL**

**RADICADO 101540**

En la ciudad de Bogotá, el dieciocho (18) del mes de Diciembre de dos mil veintidos (2022), el Grupo de Trabajo de Informática Forense y Seguridad Digital (en adelante “GTIFSD”) de la Superintendencia de Industria y Comercio (en adelante “SIC”), recibe por parte del Analistas Rápidos y Sinuosos (en adelante “ARS”), el expediente con radicado N° diez quince cuarenta con el fin de realizar el informe técnico de doscientos cincuenta (250) dispositivo(s) contenedor(es) de evidencia digital (CD/DVD/BLURAY/USB/DD). El objetivo de este informe técnico es obtener una comprensión clara de cómo ocurrió el ataque y quién fue el responsable directo o indirecto del mismo. Además, se busca evaluar las medidas de seguridad implementadas por la empresa y determinar si hubo alguna negligencia o incumplimiento de las políticas y procedimientos establecidos.

1. **DESCRIPCIÓN DEL REQUERIMIENTO**

Fedrico Rojas Hernandez, Jefe de Tecnología de Información , (AnálisisMarket+): Agencia de investigación de mercado.solicita al GTIFSD el día dieciocho (18) del mes de Diciembre de dos mil veintidos (2022) el informe técnico de doscientos cincuenta (250) dispositivos contenedores de evidencia digital **(Discos Duros ,Ordenadores y Servidores),** con número de radicado N°**101540**  **–OPERACIÓN RESCATE DE DATOS: INVESTIGACIÓN RANSOMWARE EN ANÁLISISMARKET+**. Al finalizar el informe técnico se solicita al GTIFSD todos los mensajes de datos almacenados en los dispositivos de origen revisados en **(Discos Duros , Ordenadores y Servidores)**, esto con el fin de análizar exhaustivamente los dispositivos afectados, identificar el punto de entrada del ransomware, las acciones realizadas por el malware y las posibles vulnerabilidades en los sistemas de seguridad de la empresa.

1. **CONTENEDOR DE EVIDENCIA DIGITAL EXAMINADO**

Daniel Alejandro Olarte, Experto Forense Digital, Analistas Rápidos y Sinuosos hace allegar los dispositivos contenedores de evidencia digital **(Discos Duros, Ordenadores y Servidores)**

| **CARACTERÍSTICA** | **DESCRIPCIÓN DE DISPOSITIVO DESTINO** |
| --- | --- |
| Tipo de Dispositivo | Discos Duros |
| Marca | TOSHIBA |
| Serial Físico | MK261GSYB |
| Estado Físico | Buen estado, sin daños físicos aparentes |
| Capacidad total | 2 TB (aproximadamente 2,000 GB) |
| Espacio utilizado o Peso | 500 GB |
| Número Archivos | 10,000 archivos |
| Número Carpetas | 500 carpetas |
| Serial Lógico | Sí, sin indicios de problemas lógicos detectados durante el análisis |
| Estado Lógico | Buen estado, sin corrupción de datos aparente |

Tabla 1. Inspección preliminar del contenedor de evidencia Digital

| **CARACTERÍSTICA** | **DESCRIPCIÓN DE DISPOSITIVO DESTINO** |
| --- | --- |
| Tipo de Dispositivo | Discos Duros |
| Marca | Samsung |
| Serial Físico | BT123XYZ42 |
| Estado Físico | Buen estado, sin daños físicos aparentes |
| Capacidad total | 2 TB (aproximadamente 2,000 GB) |
| Espacio utilizado o Peso | 750 GB |
| Número Archivos | 12,000 archivos |
| Número Carpetas | 600 carpetas |
| Serial Lógico | Sí, sin indicios de problemas lógicos detectados durante el análisis |
| Estado Lógico | Buen estado, sin corrupción de datos aparente |

Tabla 2. Inspección preliminar del contenedor de evidencia Digital

| **CARACTERÍSTICA** | **DESCRIPCIÓN DE DISPOSITIVO DESTINO** |
| --- | --- |
| Tipo de Dispositivo | Discos Duros |
| Marca | Samsung |
| Serial Físico | SBC123XYZ434 |
| Estado Físico | Buen estado, sin daños físicos aparentes |
| Capacidad total | 2 TB (aproximadamente 2,000 GB) |
| Espacio utilizado o Peso | 500 GB |
| Número Archivos | 10,000 archivos |
| Número Carpetas | 400 carpetas |
| Serial Lógico | Sí, sin indicios de problemas lógicos detectados durante el análisis |
| Estado Lógico | Buen estado, sin corrupción de datos aparente |

Tabla 3. Inspección preliminar del contenedor de evidencia Digital

| **CARACTERÍSTICA** | **DESCRIPCIÓN DE DISPOSITIVO DESTINO** |
| --- | --- |
| Tipo de Dispositivo | Discos Duros |
| Marca | Samsung |
| Serial Físico | EBC123XYZ457 |
| Estado Físico | Buen estado, sin daños físicos aparentes |
| Capacidad total | 2 TB (aproximadamente 2,000 GB) |
| Espacio utilizado o Peso | 1 TB |
| Número Archivos | 20,000 archivos |
| Número Carpetas | 800 carpetas |
| Serial Lógico | Sí, sin indicios de problemas lógicos detectados durante el análisis |
| Estado Lógico | Buen estado, sin corrupción de datos aparente |

Tabla 4. Inspección preliminar del contenedor de evidencia Digital

| **CARACTERÍSTICA** | **DESCRIPCIÓN DE DISPOSITIVO DESTINO** |
| --- | --- |
| Tipo de Dispositivo | Computador |
| Marca | Asus |
| Serial Físico | ABC123XYZ456 |
| Estado Físico | Buen estado, sin daños físicos aparentes |
| Capacidad total | 2TB SSD |
| Espacio utilizado o Peso | 500 GB |
| Número Archivos | 20,000 archivos |
| Número Carpetas | 800 carpetas |
| Serial Lógico | Sí, sin indicios de problemas lógicos detectados durante el análisis |
| Estado Lógico | Buen estado, sin corrupción de datos aparente |

Tabla 5. Inspección preliminar del contenedor de evidencia Digital

| **CARACTERÍSTICA** | **DESCRIPCIÓN DE DISPOSITIVO DESTINO** |
| --- | --- |
| Tipo de Dispositivo | Computador |
| Marca | Dell |
| Serial Físico | EBC123XYZ4543 |
| Estado Físico | Buen estado, sin daños físicos aparentes |
| Capacidad total | 2TB SSD |
| Espacio utilizado o Peso | 1TB |
| Número Archivos | 36,000 archivos |
| Número Carpetas | 900 carpetas |
| Serial Lógico | Sí, sin indicios de problemas lógicos detectados durante el análisis |
| Estado Lógico | Buen estado, sin corrupción de datos aparente |

Tabla 6. Inspección preliminar del contenedor de evidencia Digital

| **CARACTERÍSTICA** | **DESCRIPCIÓN DE DISPOSITIVO DESTINO** |
| --- | --- |
| Tipo de Dispositivo | Computador |
| Marca | Dell |
| Serial Físico | TABC123XYZ46 |
| Estado Físico | Buen estado, sin daños físicos aparentes |
| Capacidad total | 2TB SSD |
| Espacio utilizado o Peso | 500 GB |
| Número Archivos | 19000 archivos |
| Número Carpetas | 750 carpetas |
| Serial Lógico | Sí, sin indicios de problemas lógicos detectados durante el análisis |
| Estado Lógico | Buen estado, sin corrupción de datos aparente |

Tabla 7. Inspección preliminar del contenedor de evidencia Digital

| **CARACTERÍSTICA** | **DESCRIPCIÓN DE DISPOSITIVO DESTINO** |
| --- | --- |
| Tipo de Dispositivo | Computador |
| Marca | Dell |
| Serial Físico | DBC123XYZ4566 |
| Estado Físico | Buen estado, sin daños físicos aparentes |
| Capacidad total | 2TB SSD |
| Espacio utilizado o Peso | 1TB |
| Número Archivos | 25,000 archivos |
| Número Carpetas | 1000 carpetas |
| Serial Lógico | Sí, sin indicios de problemas lógicos detectados durante el análisis |
| Estado Lógico | Buen estado, sin corrupción de datos aparente |

Tabla 8. Inspección preliminar del contenedor de evidencia Digital

| **CARACTERÍSTICA** | **DESCRIPCIÓN DE DISPOSITIVO DESTINO** |
| --- | --- |
| Tipo de Dispositivo | Servidor |
| Marca | Dell PowerEdge |
| Serial Físico | 789XYZ123ABC |
| Estado Físico | Buen estado, sin daños físicos aparentes |
| Capacidad total | 8 TB (terabytes) |
| Espacio utilizado o Peso | 3.5 TB |
| Número Archivos | 50,000 archivos |
| Número Carpetas | 1,200 carpetas |
| Serial Lógico | Sí, sin indicios de problemas lógicos detectados durante el análisis |
| Estado Lógico | Buen estado, sin corrupción de datos aparente |

Tabla 9. Inspección preliminar del contenedor de evidencia Digital

| **CARACTERÍSTICA** | **DESCRIPCIÓN DE DISPOSITIVO DESTINO** |
| --- | --- |
| Tipo de Dispositivo | Servidor |
| Marca | Dell PowerEdge |
| Serial Físico | 789XYZ123ABT |
| Estado Físico | Buen estado, sin daños físicos aparentes |
| Capacidad total | 8 TB (terabytes) |
| Espacio utilizado o Peso | 3.5 TB |
| Número Archivos | 50,000 archivos |
| Número Carpetas | 1,200 carpetas |
| Serial Lógico | Sí, sin indicios de problemas lógicos detectados durante el análisis |
| Estado Lógico | Buen estado, sin corrupción de datos aparente |

Tabla 10. Inspección preliminar del contenedor de evidencia Digital

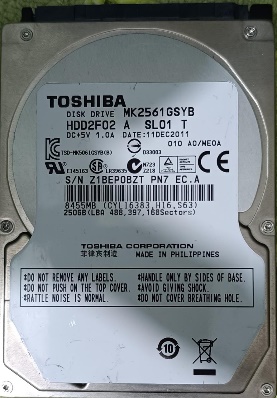
1. **DESCRIPCIÓN GENERAL DEL PROCEDIMIENTO**
   1. **ANÁLISIS TÉCNICO DE LOS DISPOSITIVOS DE ORIGEN**
   2. **Identificación física:** Este procedimiento consiste en establecer el estado físico de los dispositivos, para lo cual se identifica el tipo de embalaje en el que se entrega cada contenedor de evidencia digital (Discos Duros, Ordenadores y Servidores), el serial físico y se toman fotografías para establecer las características visuales tales como marcaciones y adhesivos.

**Discos Duros :**

TOSHIBA

Serial : MK261GSYB

Observaciones : el disco duro se encuentra en buen estado sin ninguna raya.



Ordenador:

Asus Vivobook 14/15

Serial: **ABC123XYZ456**

Observaciones : El ordernador se encuentra sin daños físicos y con funcionamiento correcto, solamente se encontró una anomalia de archivos encriptados.

Imagen que contiene mostrador, cocina, tabla, hombre

Descripción generada automáticamente Laptop encendida junto a un teclado de computadora

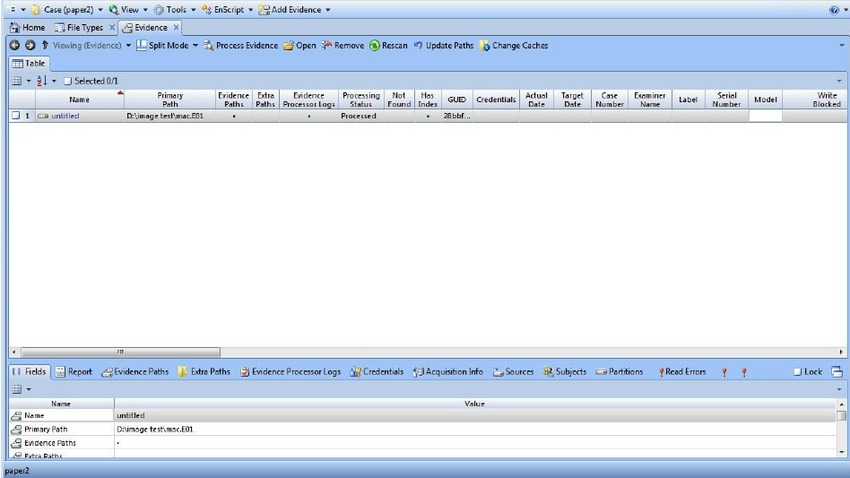
Descripción generada automáticamente



**b. Revisión de datos lógicos:** Este procedimiento consiste en utilizar diferentes herramientas de software para visualizar el estado lógico de los dispositivos contenedores de evidencia digital, tales como, la vista preliminar de Dispositivos y Unidades de Windows, el serial lógico, la cantidad de archivos y de carpetas, entre otros. Para esta verificación se utilizaron las herramientas de y las herramientas de software :

Software:

* EnCase Forensic: Herramienta líder en el campo de la investigación forense digital, para adquirir y analizar datos de manera forense, así como realizar búsquedas avanzadas y recuperar información oculta.



* AccessData FTK (Forensic Toolkit): Adquisición de datos, análisis de imágenes, recuperación de contraseñas y búsqueda rápida de información relevante.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Hardware:

* Hardware write blockers: Obtener acceso de sólo lectura a un ordenador y evitar dañar los datos que contiene evitando cualquier escritura accidental o maliciosa en el dispositivo durante la adquisición.



* 1. **GRADO DE ACEPTACIÓN POR LA COMUNIDAD TÉCNICO - CIENTÍFICA DE LOS PROCEDIMIENTOS REALIZADOS**

Los procedimientos técnicos empleados para realizar la preservación, recolección y análisis de la información almacenada en dispositivos de almacenamiento digital, gozan de total aceptación por la comunidad técnico - científica, al tratarse de actividades debidamente reconocidas y avaladas en la realización de los diferentes análisis forenses de computadoras y dispositivos electrónicos de datos que se efectúan a nivel mundial por parte de expertos en esta área, en donde, apoyados en herramientas de software y hardware especializado se lleva a la práctica un conjunto de conocimientos científicos y de técnicas que hace posible el tratamiento de la información almacenada en un medio digital preservando la integridad de la evidencia.

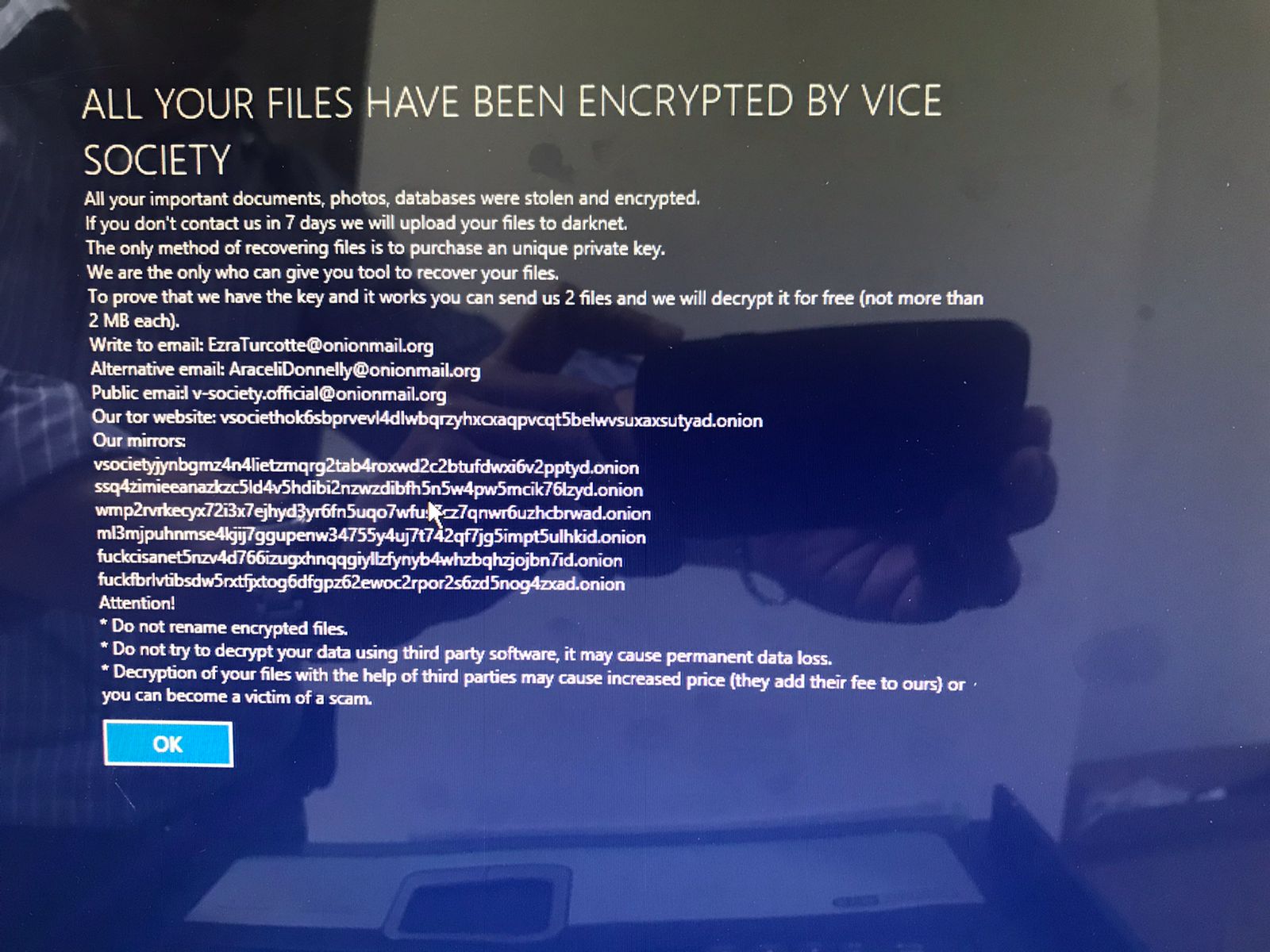
* 1. **PRINCIPIOS TÉCNICOS– CIENTÍFICOS APLICADOS Y SU GRADO DE ACEPTACIÓN**

**a**. **Principio de disponibilidad:** Cuando la información es accesible a los usuarios autorizados por el Analistas Rápidos y Sinuosos(ARS) en el momento de requerirla.

**b.** **Principio de no repudiación:** Cuando la información involucrada en un evento corresponde a quien participa en el mismo, quien no podrá desconocer su intervención en dicho evento.

**c.** **Principio de integridad:** cuando se garantiza que la información es exacta y completa, no se modifica desde el momento de su creación y se almacena en un formato que asegura la exactitud de la información original mediante la huella HASH.

**d. Observancia:** Cuando se lleva el registro de los eventos importantes en la respectiva cadena de custodia.



1. **HERRAMIENTAS DE SOFTWARE Y HARDWARE UTILIZADAS**

A continuación, se relacionan las herramientas de software y hardware utilizadas para realizar la actividad de identificación e informe técnico de doscientos cincuenta (250) dispositivos contenedores de evidencia digital **(Discos Duros , Ordernadores y Servidores):**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SOFTWARE/HARDWARE** | **PROPÓSITO** | **NOMBRE** | **VERSIÓN** | **FABRICANTE** |
| SOFTWARE | como realizar búsquedas avanzadas y recuperar información oculta. | EnCase Forensic | v10. | Guidance Software |
| SOFTWARE | Adquisición de datos, análisis de imágenes, recuperación de contraseñas y búsqueda rápida de información relevante. | AccessData FTK | 8.0 | AccessData Group. |
| HARDWARE | Obtener acceso de sólo lectura a un ordenador y evitar dañar los datos que contiene evitando cualquier escritura accidental o maliciosa en el dispositivo durante la adquisición | Hardware write blockers | CRU WiebeTech Forensic ComboDock. | CRU |

Tabla 2 Relación de herramientas de software y hardware utilizadas en la actividad.

1. **RESULTADOS DEL INFORME TECNCO**
   1. **IDENTIFICACIÓN FÍSICA:**

| **CARACTERÍSTICA** | **DESCRIPCIÓN DE DISPOSITIVO DESTINO** |
| --- | --- |
| Tipo de Dispositivo | Computador |
| Marca | Asus |
| Serial Físico | ABC123XYZ456 |
| Estado Físico | Buen estado, sin daños físicos aparentes |
| Capacidad total | 2TB SSD |
| Espacio utilizado o Peso | 500 GB |
| Número Archivos | 20,000 archivos |
| Número Carpetas | 800 carpetas |
| Serial Lógico | Sí, sin indicios de problemas lógicos detectados durante el análisis |
| Estado Lógico | Buen estado, sin corrupción de datos aparente |
| Registro fotográfico Frontal | Imagen que contiene mostrador, cocina, tabla, hombre  Descripción generada automáticamente  Laptop encendida junto a un teclado de computadora  Descripción generada automáticamente |
| Registro fotográfico Posterior |  |

Tabla 5. Inspección preliminar del contenedor de evidencia Digital

| **CARACTERÍSTICA** | **DESCRIPCIÓN DE DISPOSITIVO DESTINO** |
| --- | --- |
| Tipo de Dispositivo | Discos Duros |
| Marca | TOSHIBA |
| Serial Físico | MK261GSYB |
| Estado Físico | Buen estado, sin daños físicos aparentes |
| Capacidad total | 2 TB (aproximadamente 2,000 GB) |
| Espacio utilizado o Peso | 500 GB |
| Número Archivos | 10,000 archivos |
| Número Carpetas | 500 carpetas |
| Serial Lógico | Sí, sin indicios de problemas lógicos detectados durante el análisis |
| Estado Lógico | Buen estado, sin corrupción de datos aparente |
| Registro fotográfico Frontal | Imagen que contiene disco duro, medidor, estacionamiento, lado  Descripción generada automáticamente |
| Registro fotográfico Posterior |  |

Tabla 1. Inspección preliminar del contenedor de evidencia Digital

* 1. **REVISIÓN DE DATOS LÓGICOS**

1. **Vista preliminar de Dispositivos y Unidades de Windows**

Se utiliza la Vista preliminar de Dispositivos y Unidades de Windows para determinar que la unidad conectada puede identificarse mediante la letra (C:) y sus propiedades.

|  |
| --- |
|  |

Ordenador Asus,. Visualización de navegación mediante Vista preliminar de Dispositivos y Unidades de Windows, Obtenida con impresión por pantalla la Aplicación de Microsoft Windows Recortes.

1. **FTK Imagen**

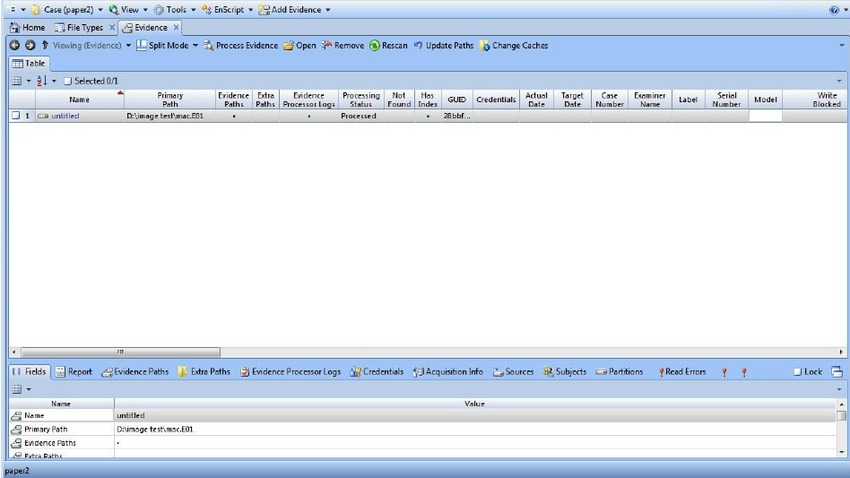
Se utiliza la herramienta FTK Imager para realizar la navegación en el Dispositivo Contenedor de Evidencia Digital la cual se encuentra en la unidad con la letra (C:)

|  |
| --- |
|  |

Unidad C:,. *Visualización de navegación mediante FTK Imagen, Obtenida con impresión por pantalla la Aplicación de Microsoft Windows Recortes.*

1. **EnCase Forensic**

como realizar búsquedas avanzadas y recuperar información oculta.



1. **Hardware write blockers**

Obtener acceso de sólo lectura a un ordenador y evitar dañar los datos que contiene evitando cualquier escritura accidental o maliciosa en el dispositivo durante la adquisición

|  |
| --- |
|  |

Hardware write blockers,. Inspección realizada mediante Hardware write blockers, Obtenida con impresión por pantalla la Aplicación de Microsoft Windows Recortes

1. **CONCLUSIONES**

Este descubrimiento resalta la importancia de la concienciación y la educación sobre seguridad informática tanto para los empleados como para sus familiares, especialmente cuando se trata de dispositivos y redes empresariales. Es esencial enseñar a los niños sobre los riesgos asociados con dispositivos y medios desconocidos para evitar incidentes similares en el futuro.

Con estos hallazgos, ARS puede concluir que el incidente de ransomware fue resultado de una acción no intencion

La actividad termina el primero (1) de mes febrero del dos mil veintitrés (2023) a las 16: 00, firman los encargados de las actividades técnicas mencionadas y la revisión de la presente acta por parte del GTIFSD,

|  |  |
| --- | --- |
| **Realizado por:**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **NOMBRE Daniel Olarte**  C.C 19024930 de Bogotá  Servidor Público y/o Contratista – ARS  Analistas Rápidos y Sinuosos | **Revisado por:**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **NOMBRE Bryan Hernandez**  C.C 2043455 de Bogotá  Servidor Público y/o Contratista – ARS Analistas Rápidos y Sinuosos |