Imagen que contiene Icono

Descripción generada automáticamente

**12-5-2021**

Mauricio de la Torre León

C.S corp.

Reporte de Investigación

Análisis Forense

Índice

Contenido

[Sobre Nosotros 2](#_Toc72256094)

[Misión 3](#_Toc72256095)

[Visión 3](#_Toc72256096)

[Acuerdo de Confidencialidad 4](#_Toc72256097)

[Objetivo 6](#_Toc72256098)

[Introducción 6](#_Toc72256099)

[Metodología 7](#_Toc72256100)

[Adquisición de la evidencia 8](#_Toc72256101)

[Preservación de la Evidencia 8](#_Toc72256102)

[Cadena de custodia 9](#_Toc72256103)

[Caso 10](#_Toc72256104)

[Evidencia 11](#_Toc72256105)

[FTK IMAGER 11](#_Toc72256106)

[Autopsy 11](#_Toc72256107)

[Reconstrucción del ataque (Posible situación basado en lo evidenciado) 12](#_Toc72256108)

[Resumen Ejecutivo 13](#_Toc72256109)

[Conclusión 14](#_Toc72256110)

[Anexos 15](#_Toc72256111)

[Anexo A-Numero de serie de la usb 15](#_Toc72256112)

[Anexo B-Formateo a bajo nivel 15](#_Toc72256113)

[Anexo C-Realizar copia bit a bit 15](#_Toc72256114)

[Anexo D-MD5 de los archivos sensibles 17](#_Toc72256115)

[Glosario 20](#_Toc72256116)

# Sobre Nosotros

Consultorías de Seguridad, somos una empresa 100% mexicana que surge ante la necesidad en el país sobre especialistas en ciberseguridad que se requieren en México para el aseguramiento las empresas y sus intereses.

Como empresa de seguridad, estamos comprometidos a brindar el más optimo servicio para las empresas en México apegándonos respectivamente a las normas y regulaciones en ambientes nacionales como mundiales.

Contamos con áreas de Pentesting tanto Red como Blue team, además de creación de arquitecturas de red seguras y área de Forense Informático, en todas contamos con las respectivas licencias y nuestros empleados cuentan con certificaciones en sus áreas, todas vigentes.

Imagen que contiene Icono

Descripción generada automáticamente

# Misión

Nuestra empresa está orientada y dedicada a prestar los servicios para la seguridad informática y de seguridad de la información, junto a una visión renovada, usando la experiencia y el conocimiento para resolver los problemas presentados, esto integrado con equipos de trabajo tanto de jóvenes entusiastas de la informática graduados en el área, como aquellos expertos que llevan años en el área de la ciberseguridad.

# Visión

Garantizar un servicio de calidad manteniendo los tres principales pilares de la información que son: Integridad, Disponibilidad y Confidencialidad, para así ser reconocidos como una de las mejores empresas de ciberseguridad a nivel nacional como internacional.

# Acuerdo de Confidencialidad

El presente acuerdo se celebra por una parte CONSULTORIA DE SEGURIDAD S.A DE C.V, persona moral que se encuentra debidamente constituida ante el titular de la notaria 117 Guadalupe, Nuevo León bajo la escritura 27001 de fecha 17 de enero del 2020; y que tiene su domicilio en:

Granada 819, valles de linda vista, código postal 67125, Guadalupe, Nuevo León

Actuando a través de su representante MAURICIO DE LA TORRE LEÓN, persona mayor de edad, que cuenta con las facultades suficientes y necesarias para celebrar el presente acuerdo.

Y por la otra EPZA PROYECTOS Y EDIFICACIONES S.A. DE C.V., persona moral que se encuentra debidamente constituida y que tiene su domicilio en:

José Manuel Othon 2715, Pablo A. de la Garza, 64580 Monterrey, Nuevo León

Actuando a través de su representante GERARDO DE LA TORRE TAPIA, persona mayor de edad que cuenta con las facultades suficientes y necesarias para celebrar el presente acuerdo.

Las cuales en lo sucesivo serán referidas de manera conjunta como “las partes” y de manera individual como “la parte, quienes se reconocen expresa y recíprocamente con capacidad plena para obligarse y establecen lo siguiente:

CLAUSULA PRIEMRA

Objeto de Acuerdo

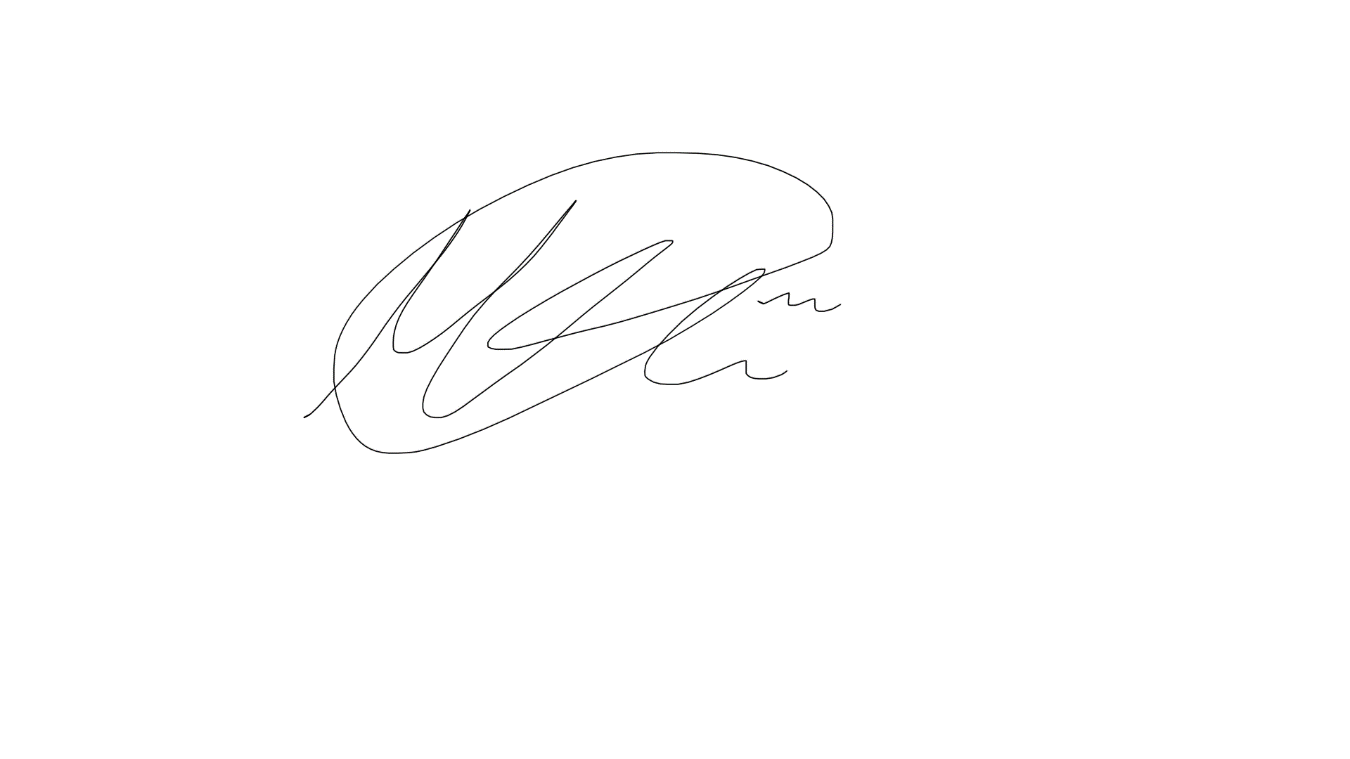
El presente acuerdo se refiere a la información confidencial que compartirán las partes, sin que ninguna de ellas tome ventaja de la otra al recibir los datos o procedimientos que sean clasificados como confidenciales en los términos de este convenio, a fin de colaborar en el desarrollo del siguiente proyecto:

Mantener la confidencialidad de la información obtenida durante el reporte de análisis forense que se realizara a la memoria USB proporcionada.

Los elementos específicos que se consideran como parte de la información confidencial, se detallan en el documento adjunto (Reporte\_Investigacion\_Forense\_EPZA) que se agrega al presente acuerdo como parte integrante del mismo, el cual firman las partes de común acuerdo.

Segunda. Vigencia

Este acuerdo entrara en vigor desde el momento en que las partes los firman extendiéndose su vigencia después de finalizada la relación entre las partes o, en su caso, la prestación del servicio, hasta por un plazo de 5 (cinco) años.



\_\_\_\_Mauricio de la torre león\_\_\_\_

Mauricio de la Torre León en nombre y representación de CONSULTORIA DE SEGURIDAD S.A DE C.V

Diagrama

Descripción generada automáticamente

\_\_\_\_Gerardo de la Torre Tapia\_\_\_\_

Gerardo de la Torre Tapia en nombre y representación de EPZA PROYECTOS Y EDIFICACIONES S.A. DE C.V.

# Objetivo

Asegurar y preservar la integridad de la información de la evidencia, para su posterior análisis y obtención de la mayor cantidad de información para llegar a una resolución por parte de los peritos a quienes se le entregara dicho documento.

# Introducción

El análisis forense tiene como objetivo averiguar la situación ocurrida durante un delito o incidente sucedido en alguna empresa, donde se haya visto afectado la integridad de su información confidencial. Con el objetivo de dar respuesta a las interrogantes de lo sucedido durante dicho incidente, e identificar cuáles fueron las áreas afectadas y/o información.

Se recopilará la mayor cantidad de información, pistas y huellas electrónicas, para detectar donde se ha producido y como se produjo el incidente de seguridad, si este á llegado desde fuera por una situación logro ingresar o este fue un incidente interno intencional, buscando así el origen de dicho incidente, y cuáles fueron los siguientes pasos.

# Metodología



La estrategia utilizada en el presente reporte de investigación ésta basada en la metodología certificación de CHFI.

Primero se realizó la identificación de la evidencia, una vez llegamos a la escena del crimen se solicito el desalojo de todos los empleados de las instalaciones, asegurando el área, identificando el dispositivo y así comenzando la cadena de custodia hasta las instalaciones donde será asignado a investigación.

Una vez dentro se solicitó a la trabajadora el área donde el dispositivo USB fue encontrado se acordono dicha área y se marcó para investigación para los peritos responsables.

La preservación de la evidencia comenzó en el momento del hallazgo del dispositivo donde fue empaquetado con el debido cuidado y bajo las condiciones necesarias con los responsables adecuados para que fuera transportado hasta las oficinas donde se realizaría una copia bit a bit para preservar la evidencia original.

Al momento del análisis de la evidencia se llevaron a cabo técnicas para el análisis forense con la debida herramienta para llevar a cabo la investigación, realizando análisis de datos y reconocimiento de la información recopilada, encontrando así información sensible robada de los equipos e información de uso de herramientas de hacking.

Para su presentación de lo antes mencionado se preparan todos los documentos necesarios para llevar a cabo el informe y presentarlo ante los clientes de manera adecuada.

# Adquisición de la evidencia

La evidencia fue encontrada el martes 11 de mayo del presente año 2021, alrededor de las 9:20 a.m. la memoria USB fue encontrada frente a la puerta de carga/descarga de las instalaciones por una empleada de la empresa mientras procedía a abrir la puerta del área de carga, el dispositivo aparentemente cayo de algún bolsillo de quien haya irrumpido a las instalaciones.

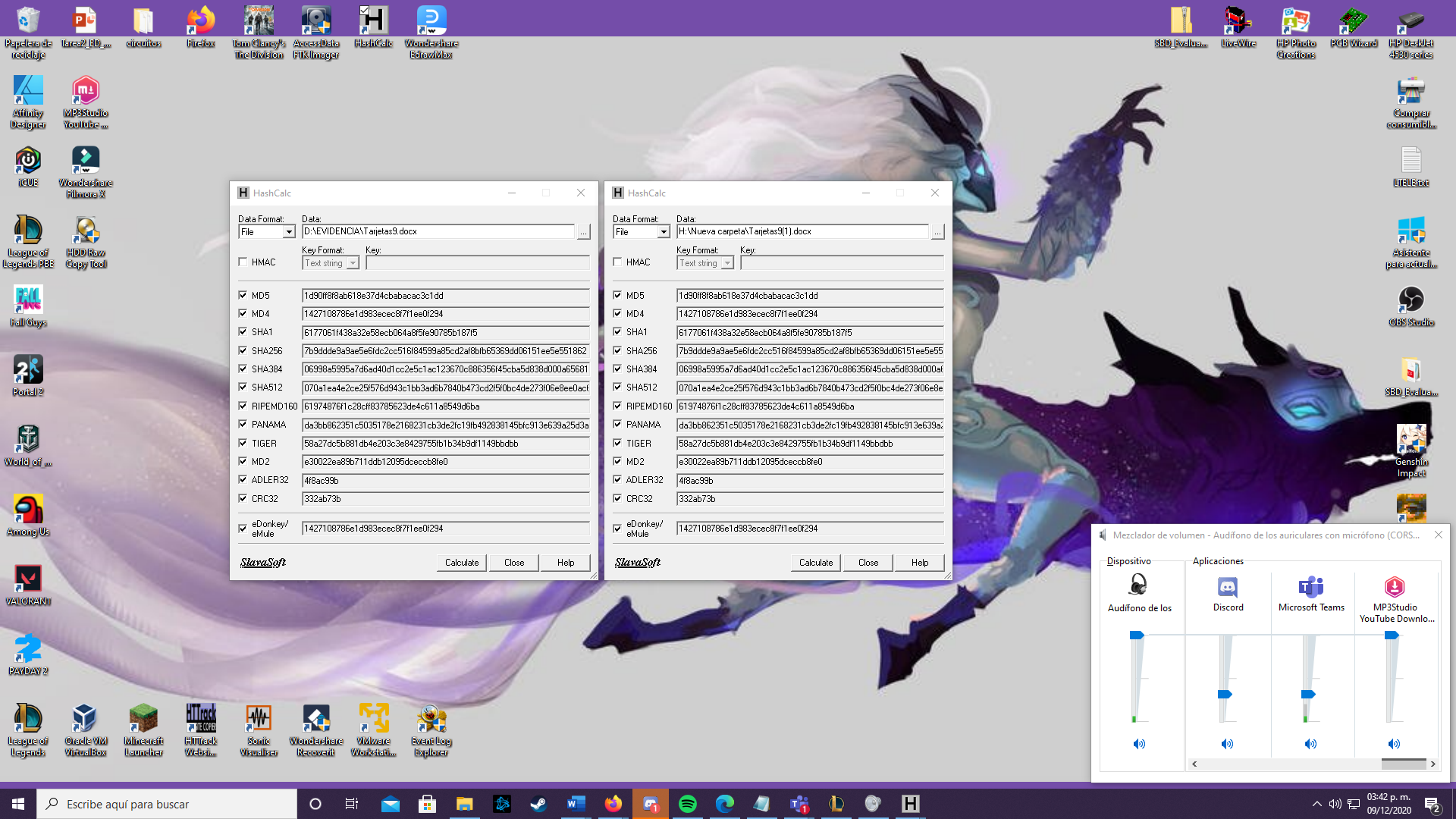
*Imagen del USB donde fue encontrada.*

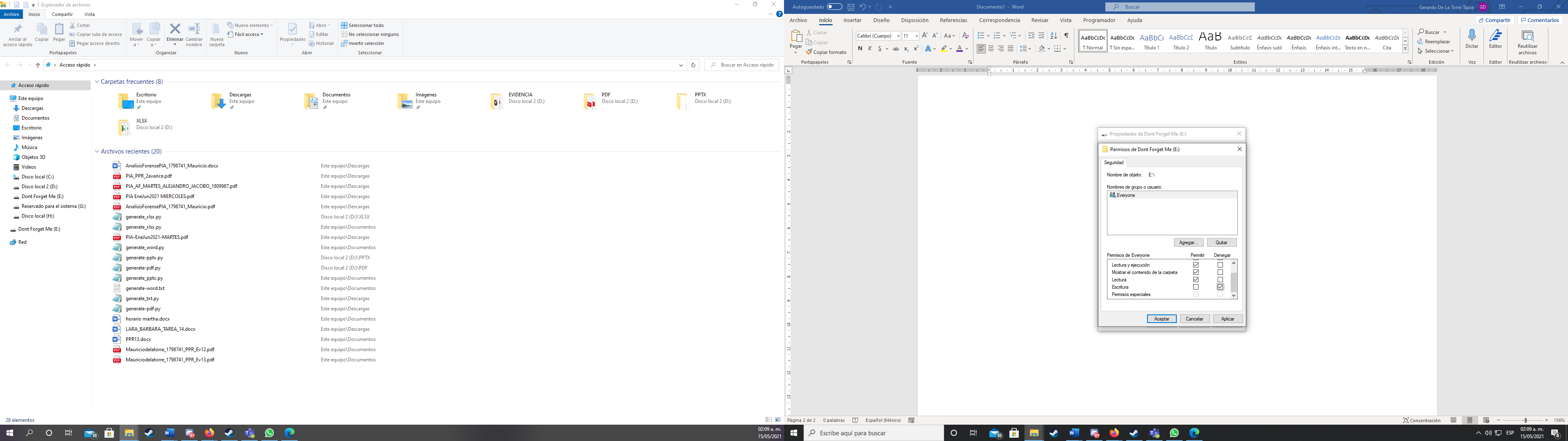
# Preservación de la Evidencia

Para preservar la integridad de la evidencia encontrada y entregada a nuestro socio, se realizó inmediatamente un aislamiento de la evidencia en la cual nadie podría acceder a ella hasta asignarle un equipo de peritos, para iniciar con la copia bit a bit y realizar el análisis de la evidencia en la copia de esta.

Al realizarle una copia bit a bit a la memoria recuperada, fue almacenada en el equipo principal del investigador, en los servidores privados de la empresa designados para el área forense, y una más en el equipo del encargado del área forense.

Se tuvo un total de 3 copias que existen además de la original.





La memoria USB original fue resguardada en una caja fuerte bajo la supervisión del mismo jefe de área forense, esta USB anteriormente fue guardada en un estuche donde fue transportada y tratada, al estuche se le dio la asignación de código de caso N.AA00100248.

# Cadena de custodia

Información de memoria

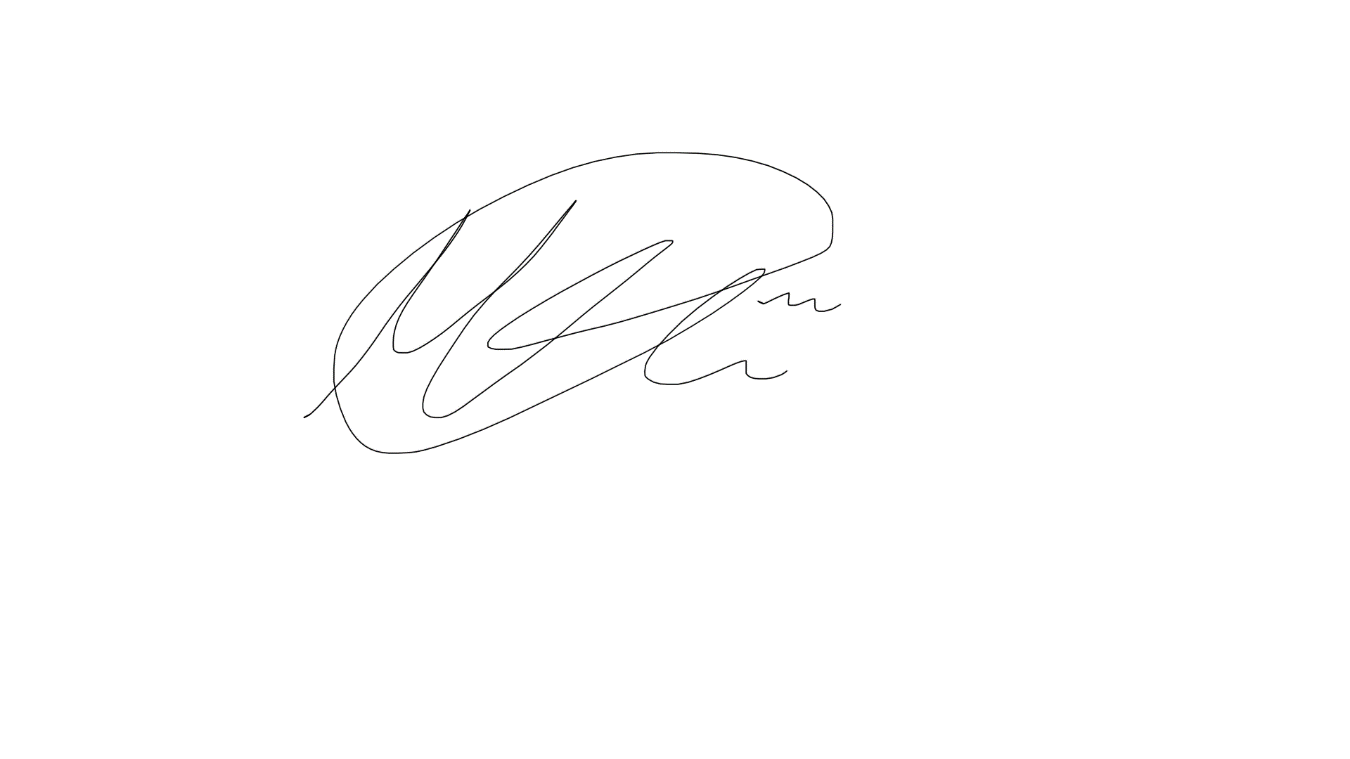
Unidad Marca Greenbeats de 8 gigabytes con número de serie “AA00000000000498”

Se entrega al agente de campo de la empresa CS el día miércoles 12 de Mayo a las 10:00 am, inmediatamente frente al cliente se realiza el asilamiento colocando la memoria dentro de una bolsa antiestática y posterior puesto en un pequeño maletín para que no se pueda acceder a la memoria.

Una vez llegado a las oficinas esta se almacenará en el are de Forense Informático, donde nuestros peritos estarán realizando a asignación del equipo o individuo que llevara a cabo este informe.

Una vez asignado el equipo deberá realizar una copia bit a bit de la evidencia para poder esta montarla y modificarla sin temor de dañar la integridad de la información original.

El individuo asignado es nuestro mismo agente de campo en este caso Mauricio de la Torre León quien fue asignado el martes 8 de diciembre del presente año para realizar la investigación.



\_\_\_\_\_\_Mauricio de la Torre León\_\_\_\_\_\_

Firma de Investigador asignado aceptando el caso.

Evidencia de la entrega de la evidencia al investigador dentro de la empresa para su análisis.

*Agregar foto USB entregada al investigador.*



# Caso

Nosotros como empresa se nos contactó con el propósito de hacer frente a la problemática dentro de la empresa EPZA que tuvo dicho incidente que tuvo lugar el martes 11 alrededor de las 11:27 p.m. del antes mencionado día, una vez que la empresa EPZA se percató de dicho incidente por la falta de archivos en sistema y manipulación de varios equipos dentro de sus instalaciones.

Por ello se pusieron de inmediato en contacto con las autoridades y con nosotros “CONSULTORIA DE SEGURIDAD” para realizar un peritaje de los sistemas a los que tuvieron acceso y a la evidencia que se encontró en el lugar, por ello se realizara una metodología de forense informático para recabar suficiente información para determinar relaciones con aquellos causantes de este ataque informático.

La evidencia será controlado bajo el número de Caso N.AA00100248

Con el uso de las herramientas como:

* FTK Imager
* Autopsy
* HDD Raw Copy Tool
* Kali Linux 2021.1
* HashCalc

# Evidencia

## FTK IMAGER

La evidencia inicialmente se utilizó por medio de la herramienta FTK Imager se realizó una instalación de la imagen de la memoria USB que se recuperó para su análisis lógico por medio del buscador de archivos de Windows.

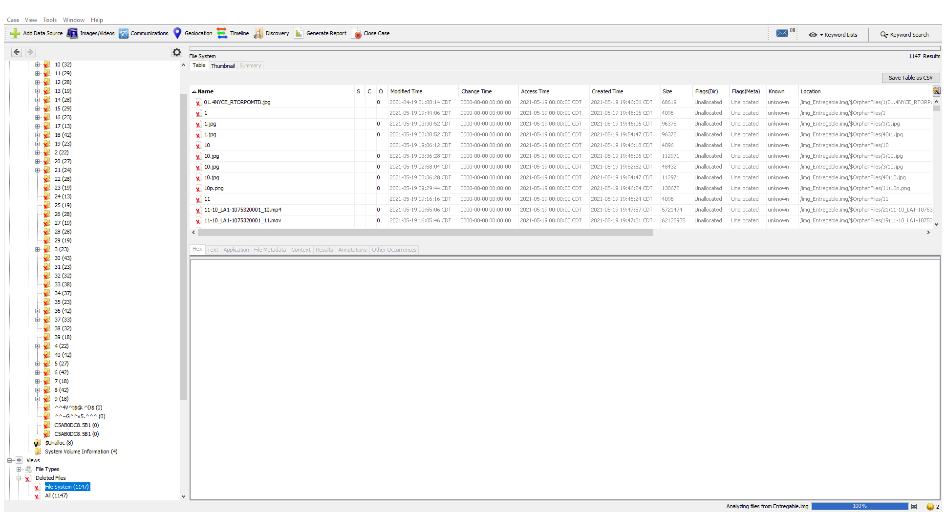
*Interfaz de usuario gráfica, Texto

Descripción generada automáticamente*

La herramienta no arrojo nada de información por ende se cree que realizo un formateo rápido o uno a bajo nivel que de ser así puede dificultar la búsqueda de información

## Autopsy

Por la situación vista en la previa aplicación se procedió a utilizar Autopsy como herramienta de recuperación de los archivos.



Una vez que pudimos visualizar los archivos que intentaron ser borrados, pero como se sospechó solo se realizó un borrado rápido posiblemente la información fue puesta en algún otro dispositivo, pero por ahora se pudo realizar la recuperación de esta y se realizara la debida investigación para encontrar a los perpetradores.

Una vez recuperada la información podemos observar que esta estaba dividida entre carpetas exactamente 30 carpetas y 10 más que estaban ocultas.

*Adjuntar foto de carpetas*

Podemos observar que tenemos un total de 945 archivos repartidos en las 40 carpetas previamente visualizadas.

*Foto*

Dentro de diversos programas podemos observar que en diversos archivos existe nombres de diferentes grupos de cibercriminales, sin embargo, es muy raro ver grupos cibercriminales tan grandes atacando empresas locales, pero queda como sospecha dicho hallazgo.

*Foto*

Archivos más adelante podemos observar indicios de un nombre y también la página de github.

*Foto*

Buscando el nombre dentro de la plataforma podemos encontrar a dicho usuario y podemos observar que este contiene un repositorio bajo el nombre “Was it me” aparentemente había hecho referencia a su repositorio a lo largo de los archivos que se han encontrado en la memoria, pues esta palabra a sido recurrente en los archivos.

*Foto*

Dentro del repositorio podemos observar las principales evidencias que también se encuentran en la memoria, además de un TXT nuevo.

*Foto*

Dentro del TXT podemos observar un pequeño comunicado el cual exige el pago de una cantidad de criptomonedas a cambio de borrar los archivos robados y dejar en paz a la empresa EPZA podemos asumir que es un caso de extorción.

*Foto*

Junto a esto, algunos de los archivos tenían su cabecera ligeramente modificada con esto podemos lograr contabilizar el total de 155 archivos importantes que fueron extraídos de la empresa.

*Foto*

*Tabla de total de archivos y extensiones*

# Reconstrucción del ataque (Posible situación basado en lo evidenciado)

Durante la investigación pudimos encontrar primero el uso del sistema basado en Linux conocido como Kali Linux, herramienta usada principalmente en el área de hacking pues el sistema viene cargado con diversos programas para diferentes situaciones, como phishing, ataques de diccionarios, intrusión a redes, captura de datos, etc.

Podemos observar que en una de las imágenes de búsquedas los usuarios buscaron la mejor forma de hacer phishing, lo que se puede suponer que usaron el phishing por correo electrónico, esto por un correo al cual parece ser de un empleado de la empresa que afirmo haber visto y aparentemente accedió a el y este era de dudosa procedencia.

Podemos ver manuales de uso de las herramientas BetterCap y WireShark con estas herramientas pudieron haber comenzado a observar el comportamiento y la estructura de la red de la empresa.

Culminando su ataque remoto accediendo a diversos equipos de la empresa entre ellos el ingeniero en jefe y/o dueño de la empresa donde se extrajeron planos e información, una vez terminaron con esto todo apunta a que se llevo acabo el allanamiento de las instalaciones en busca de información física.

# Resumen Ejecutivo

Durante la investigación se llevó a cabo la recuperación de un total de 1020 archivos con las herramientas utilizadas, de las cuales 150 archivos eran sensibles, de estos, 50 de ellos estaba corruptos y tuvieron que ser restaurados ya que fueron modificados de su cabecera.

Entre las razones por las cuales el ataque pudo ser llevado a cabo fueron:

* Mala Configuración de los equipos de red al no tener los parches más recientes.
* No había concientización sobre la seguridad que el personal debe tener ya que el usuario es el eslabón más débil.
* La red tenía contraseñas fáciles que fue vulneraba por un diccionario.

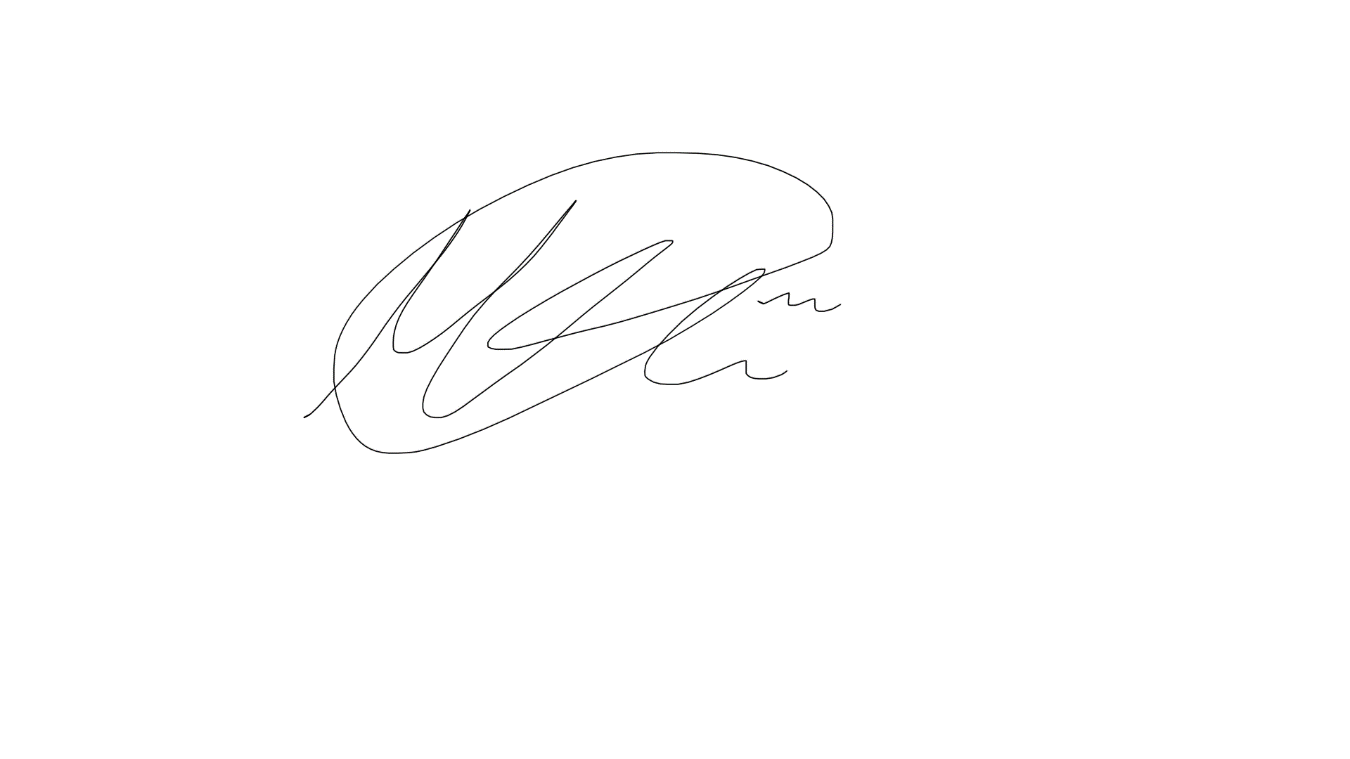
Debido a estas razones la empresa perdió gran parte de la información de sus clientes y empleados, entre esta información estaría

* Tarjetas bancarias.
* Numero de seguros.
* Información personal de los trabajadores.
* Correos electrónicos personales y de empresas.
* Números telefónicos.
* Planos arquitectónicos.

Por medio de este análisis se podrá llevar a cabo una mejora de la seguridad de la empresa constructora, al mostrar las diferentes formas de ataques a las cuales las empresas se enfrentan día a día y que estos puedan ver sus errores y las forma en que estos fueron vulnerados.

# Conclusión

Para concluir este reporte, se ha demostrado quienes han sido los principales perpetradores de los daños informáticos realizados hacia la empresa EPZA. Entre sus perpetradores se encontró la persona que lleva el seudónimo de “supertorreta” el cual aparentemente pertenece a un grupo de cibercriminales terroristas, que tras haber realizado el análisis de la evidencia se ha confirmado al menos la participación de tres personas más dentro del circulo cercano del principal sospechoso. A continuación, se da por finalizado la investigación, a este se le estará dando el seguimiento ante las autoridades gubernamentales para futuras investigaciones del caso.

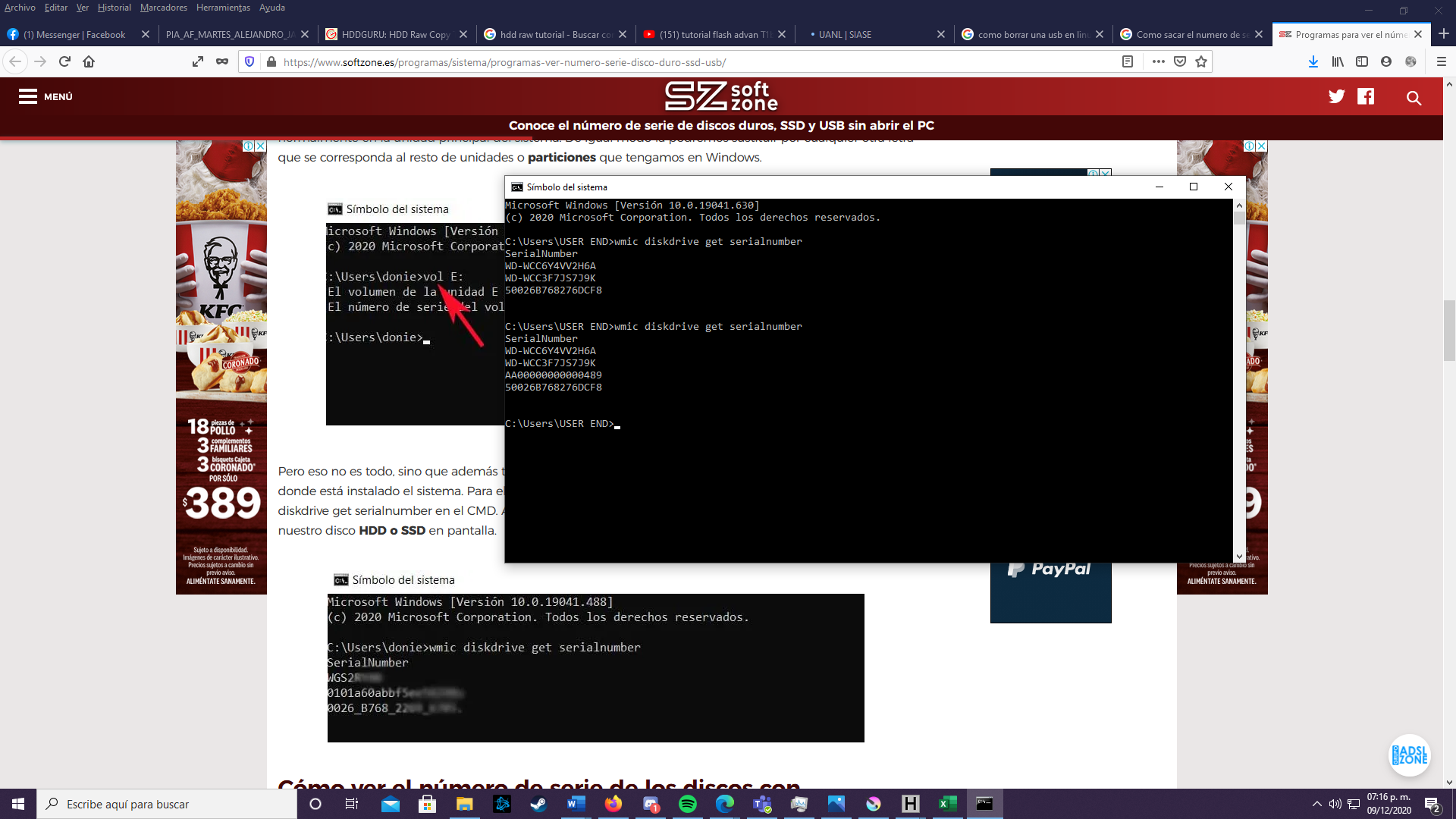


\_\_\_\_\_\_\_Mauricio de la Torre León\_\_\_\_\_\_\_\_

Firma y nombre del investigador

# Anexos

## Anexo A-Número de serie de la usb



Para el número de serie solo se debe de colocar en el CMD el comando mostrado en pantalla en este caso los primeros dos son mis discos Western Digital y el ultimo mi SSD Kingston por lo tanto el único que queda es la USB.

*Agregar CrystalDisk*

## Anexo B-Formateo a bajo nivel

Para realizar el borrado a bajo nivel se realizó en ambos sistemas operativos, tanto en Windows como en Linux desde la distribución de Kali.

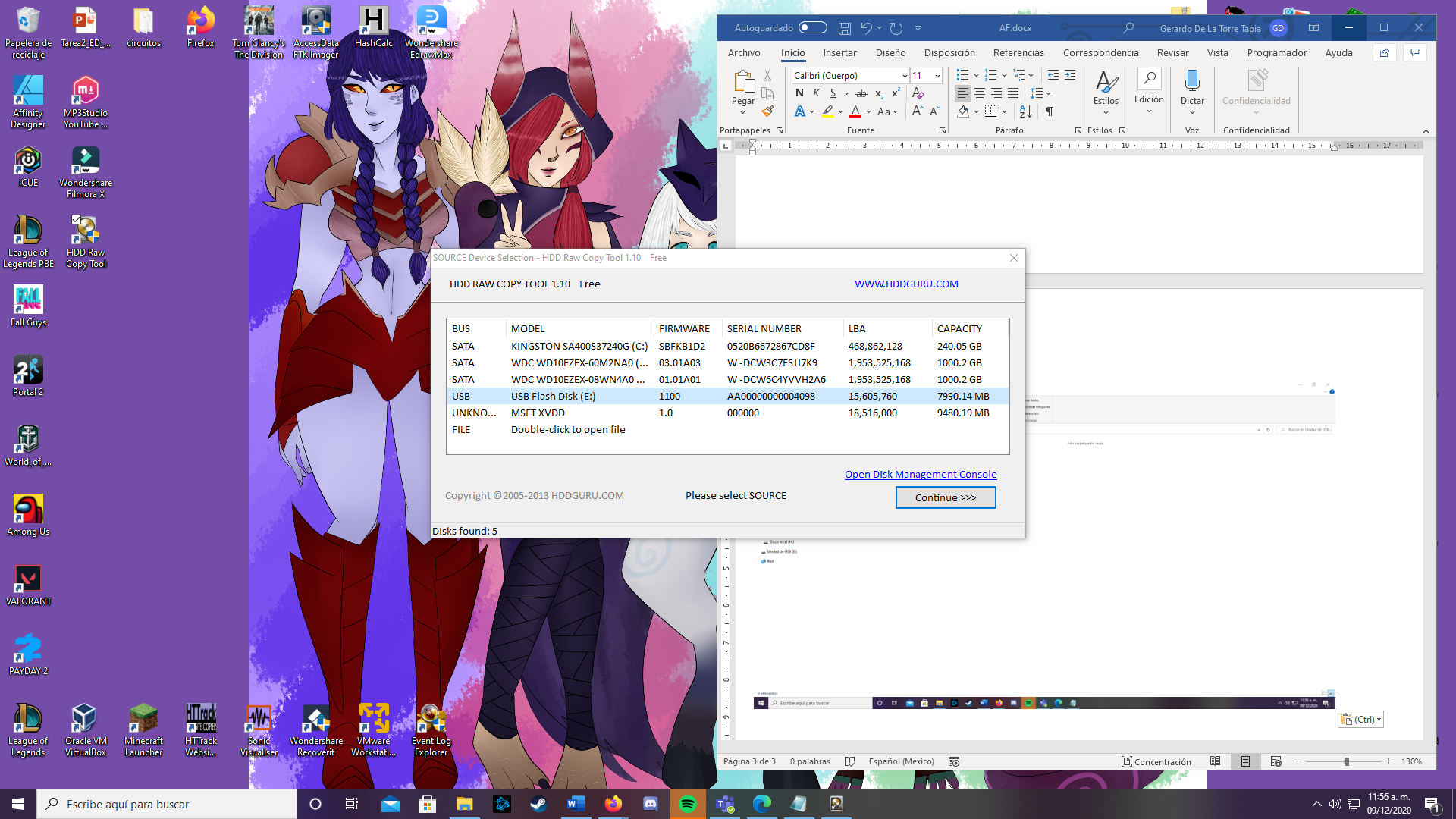
Para ambos casos el borrado tomo aproximadamente 1 hora para borrar perfectamente lo que esta USB contuvo previamente.

Para el caso de Linux tuve que entrar a la consola y entrar al usuario super sudo, después colocar fdisk -l y podemos ver todas las memorias que se encuentran, una vez identificado la memoria colocar “mkdosfs -f 32 -l + la extensión que salga de la memoria” y esta empezará, en este caso no hay una línea o “%” entonces solo será cuestión de esperar

Para el caso de Windows solo tenemos que ingresar al explorador de archivos una vez dentro localizar la memoria y dar clic derecho seleccionar la opción de formatear y quitar la opción de formato rápido.

*Agregar Borrado por HDDLLF*

## Anexo C-Realizar copia bit a bit



Para realizar la copia use HDD raw Copy Tool con la cual solo es seleccionar la memoria o el archivo que se busca copiar una vez hecho esto damos continuar y ahora seleccionamos el disco o carpeta donde queremos que se guarde y damos nuevamente continuar y saldrá.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

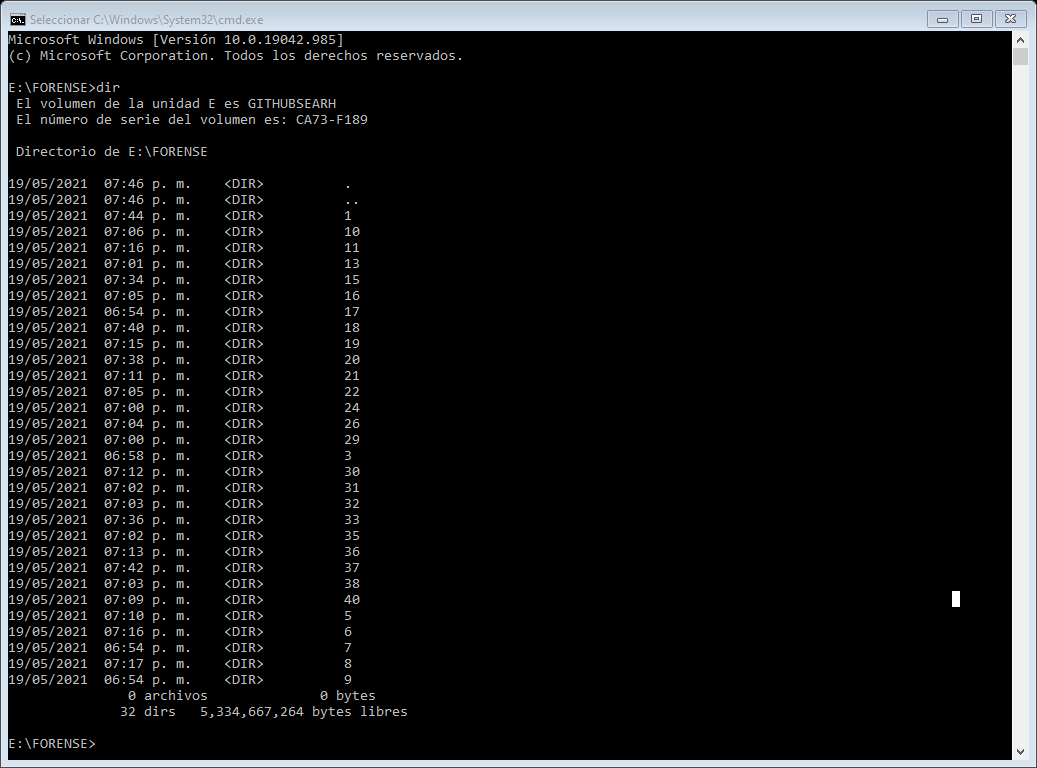
Una vez aquí solo damos en start y la copia iniciara.

*Añadir evidencia de la creación de los archivos por medio de scripts y sus bibliografías*

Anexo D-MD5 de los archivos sensibles

*Actualizar metadatos*

## Anexo E- Riaz del USB



# Glosario