**FORENSIA DIGITAL**

**HACKATHON 2.0**

**TEAM NETWORKING B**

**FRIDA GONZÁLEZ**

**JUAN FORBES**

**JULIO GARCÍA**

**JAIR CAMPOS**

Forensia Digital

* Objetivos:
* Determinar si la evidencia recabada fue alterada o no, antes de realizar el peritaje forense.
* Recabar información que permita a las autoridades pertinentes dar un veredicto final sobre el caso.
* Suministrar a las autoridades pertinentes de información íntegra que pueda ser tomada para la resolución del caso.
* Alcance:

Con esta investigación se busca comprobar la integridad de los datos en el caso presentado, recopilar información detallada de los datos capturados.

* Metodología:

Nuestra metodología se basó en la técnica de la observación, examinamos atentamente la información sobre el caso. Seguidamente utilizamos herramientas para la prueba de peritaje, tales herramientas: AccessData FTK imager para comprobar la integridad de los datos junto con MultiHasher, también utilizamos Autopsy para el análisis de los archivos y su contenido oculto.

* Procedimiento:

Primero descargamos las herramientas, descomprimimos los archivos que nos suministraron, seleccionamos el archivo USB.dd y le realizamos una copia forense, validamos que la copia y el archivo original contengan los hash iguales para comprobar que el archivo original no ha sido corrompido o alterado esto se realizó con los software AccessData FTK imager y MultiHaser, seguidamente analizamos la imagen USB.dd con el software Autopsy la cual al terminar el análisis obtuvimos imágenes ocultas dentro del USB.dd.

Los archivos de captura los abrimos con WireShark y analizamos línea por línea buscando alguna anormalidad y tratando de ver su contenido para obtener una vinculación con las imágenes encontradas del USB.dd.

* Hallazgos:

Imágenes ocultas dentro del archivo USB.dd.

Comunicación entre un usuario y el servidor de correo.

Información transferida mediante el correo.

Imágenes que se compartían hacia el servidor con vinculación a las imágenes de rinocerontes.

Creación de usuario a servidor FTP.

Obtención de contraseña.

Trafico de la comunicación del usuario al servidor mediante el protocolo TELNET.

Obtención de archivo comprimido.

* Conclusiones:

En este reto pudimos obtener información de una persona posiblemente vinculada a un delito, con esta experiencia pudimos poner en práctica nuestros conocimientos en forensia, Seguridad informática, criptografía, queda claro que para estos casos se necesita mucha paciencia y ser observador y no creer en todo lo que se ve.