PRÁCTICA 5: Análisis Post-mortem de artefactos Windows

Richard Eduardo Warner es un empleado en una empresa de desarrollo software muy importante. En los últimos meses, la empresa ha estado haciendo jugadas muy arriesgadas en el desarrollo de proyectos. Por ejemplo, han estado desarrollando una app llamada "Ligueitor", que seguramente se convierta en el nuevo Tinder, un buscador web llamado "Social Query" que, de tener éxito, podría desbancar a Google y a Bing, o un servidor de streaming de vídeo llamado "Palomitas". Sin embargo, no todo son alegrías. Fruto del riesgo que entrañan estos proyectos, algunos esparcen rumores de que a la empresa no le está yendo tan bien como esperaba, ya que en realidad no puede competir con los grandes. También se dice que pronto habrá un ERE y muchos se irán a la calle. Richard es más listo que el resto y sabe que no es una excepción. A pesar de los rumores, se le ha visto bastante calmado en los últimos días. Sin embargo, hoy se ha puesto chulo contra su jefe y acto seguido se ha marchado de la empresa. Como así no va a cobrar el dinero del ERE, pensábamos que aquí huele a gato encerrado. Por ello, la empresa ha decidido encargarte un examen forense de su disco, a ver si averiguas alguna cosa rara. No obstante, la imagen del disco la ha hecho Alan, el de sistemas, que te pasa los hashes en un post-it.

- MD5: dfdfba2231e3fa409676b1b737474208
- SHA-1: f476a81089a10f9d5393aa8c2f8bbccdb87f7d3c
- SHA-256: 66d6ee7a61ea7a986e8f6bb54b9986f79d95b5a0278bef86678ed42ace320d96

Software a utilizar:

A. Imagen de disco en https://informatica.ieszaidinvergeles.org:5001/sharing/j8arRuDs8 o \\10.5.100.1\forense\curso MISLATA\traidoer.img
B. Windows 10 (32 o 64 bits)
C. FTK Imager FTK Imager
D. Arsenal Image Mounter
E. Registry Explorer
F. Reg Ripper
G. WRR
H. USB Detective
I. MZ History Viewer
J. MBOX Viewer

Objetivos: Establecer una línea temporal del incidente. En particular, responder a las siguientes cuestiones:

1. A fin de que no haya dudas en la investigación, queremos comprobar con CMD o PowerShell que la evidencia no ha sufrido alteraciones. ¿Coinciden los tres hashes? Si coinciden, todo bien. Si no, ¿a qué se puede deber esto?

2. Comprueba que Richard tiene un usuario en el equipo, y cuándo hizo login por última vez.

3. Comprueba el nombre de equipo y la versión del Sistema Operativo.

4. Aunque la máquina tiene puertos USB, la empresa no autoriza a Richard a usarlos. ¿Introdujo algún pendrive? En caso afirmativo, ¿cuál es dicho pendrive y qué día y a qué hora lo introdujo?

5. Sabemos que Richard es fan del Barça y le gusta la música rock y heavy, por lo que a veces escucha música o ve noticias en su navegador. Incluso mira alguna cosilla en Amazon. Pero para poder justificar el despido procedente, nos gustaría saber si ha perdido el tiempo en algo más grave. Por suerte para nosotros, tenemos indicios de que ha estado viendo una película online. Consigue la información de dicha película (título, año, etc.).

6. Tras salir de la empresa, Richard tiene pensado ir a otro lugar. ¿Cuál es dicho lugar y cómo tiene pensado ir?

7. ¿Hay algún navegador web que no sea de Microsoft preparado para ejecutarse cuando Richard inicie sesión?

8. ¿Hay alguna prueba de que Richard haya ayudado a la competencia exfiltrando datos por email?