INFORMÁTICA FORENSE – PRIMER PARCIAL

NOMBRE: **FECHA:**

El archivo **pendrive.E01** es una imagen forense de un dispositivo de almacenamiento usb (pendrive).

Sobre éste archivo responda las siguientes preguntas:

1. ¿Cuál es el código hash sha1 de la imagen forense?
   fede4cc1cef10fa05efc59a9748e3774a2333403

2. ¿Cuántos archivos tiene el pendrive, cuántos son archivos eliminados y cuáles?
   7 archivos, 2 eliminados: !opo.jpg y we will rockyou.txt

3. ¿Cuáles archivos son ocultos?
   Aventuraspinocho.jpg
   Becerro.jpg
4. ¿Cuál es el tamaño real del dispositivo pendrive?

   7620MB

El archivo **tiger.rar** es un archivo que tiene contraseña, sobre éste archivo responda las siguientes preguntas:

5. ¿Cuál es el código hash de su contraseña?
   $rar5$16$80f53498ed6cebcb1fbababae4c4862d$15$29a7cf76198bf2b34bffa7a4a2ed35ca$8$9beada2f1ab3870b

6. ¿Cuál es la contraseña?

   pedro2

El archivo **examen.raw** es un volcado de memoria, sobre este archivo responda las siguientes preguntas:

7. ¿A cuáles procesos llamó el proceso **explorer.exe**?
   notepad.exe, Dumpit.exe, vmtoolsd.exe, mspaint.exe, iexplorer.exe, calc.exe

8. ¿Qué proceso se ejecutó el 27 de abril de 2023 a horas 22:45:59?
   notepad.exe

9. ¿Cuál es el código hash sha1 de este volcado?
   64301a955384af8257a0ed37db8dcd8ac8a3306b

10. ¿Cuál es la IP v4 del equipo al que corresponde ésta memoria?
    192.168.100.90