GOBIERNO DEL
ESTADO DE MÉXICO

TECNOLÓGICO DE ESTUDIOS SUPERIORES
IXTAPALUCA

TECNOLOGICO DE ESTUDIOS SUPERIORES DE IXTAPALUCA

MATERIA:

AUDITORÍA DE LA SEGURIDAD INFORMÁTICA

PROFESOR:

KEVIN RAMIREZ VITE

ESTUDIANTE:

LAURA RAMOS GONZÁLEZ

GRUPO:

1951

TRABAJO:

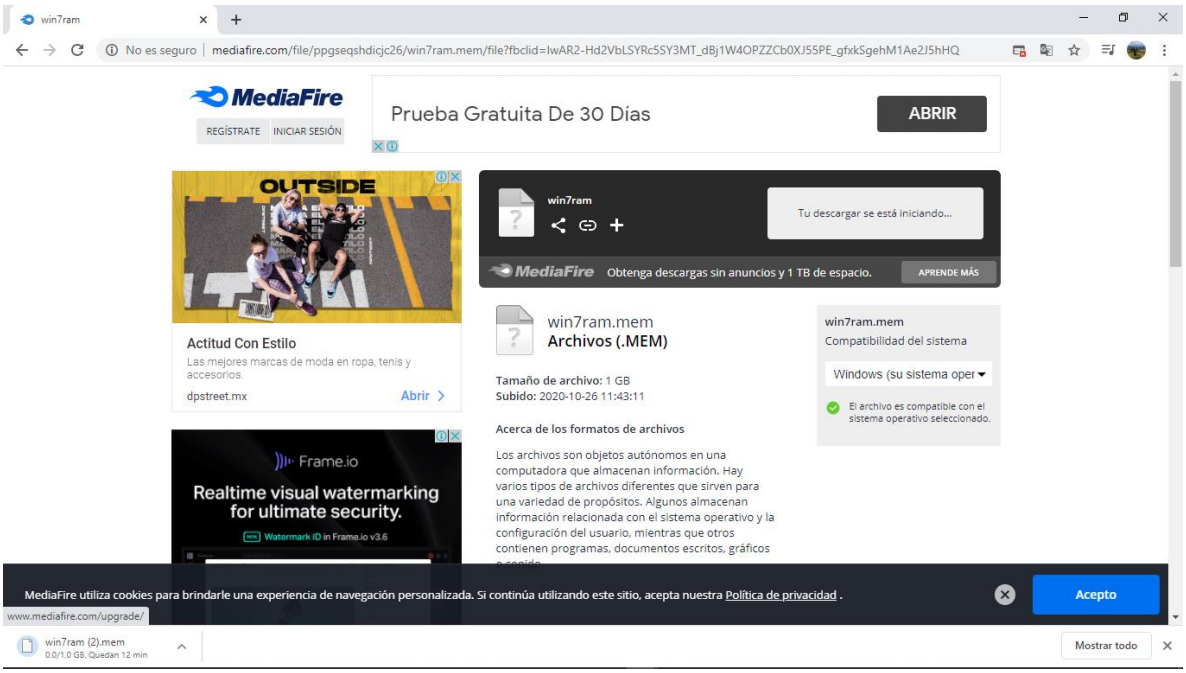
REPORTE DE PRACTICA

FECHA DE ENTREGA:

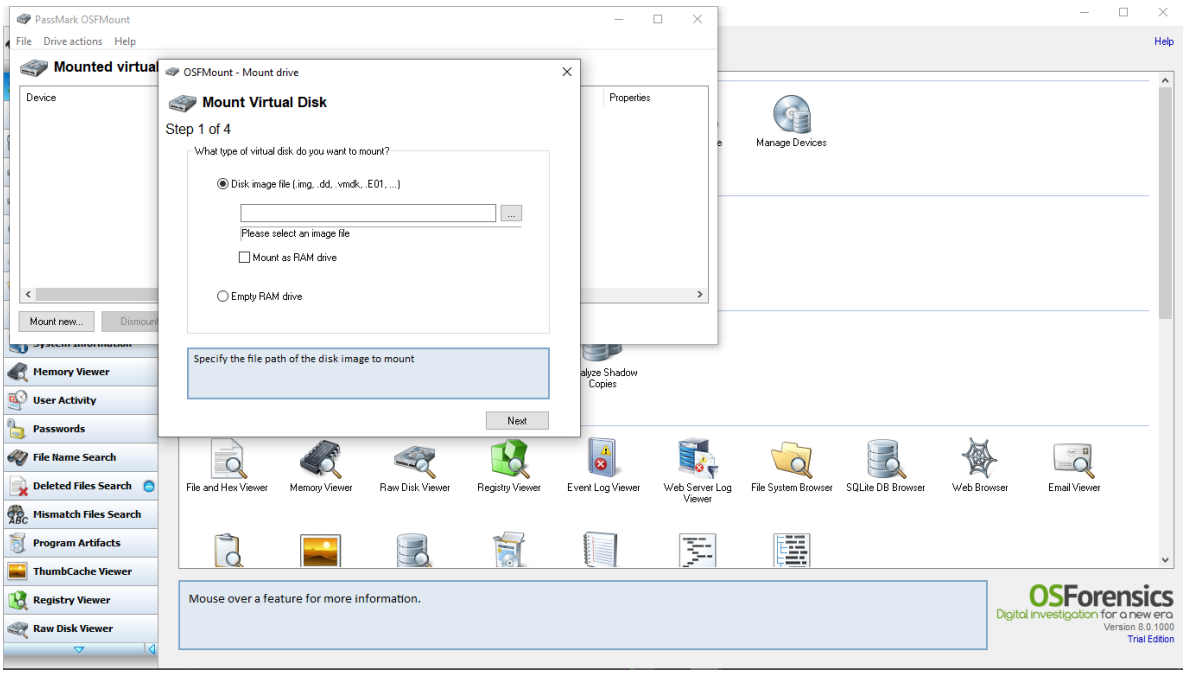
31 DE OCTUBRE DEL 2020

Como herramienta utilizare osforencis, ya que sirve para realizar exámenes forenses, es un software que permite realizar diversas tareas, este programa permite utilizar un framework que tiene como objetico introducir a las personas en las complejas técnicas de extracción digitales de memora ram.

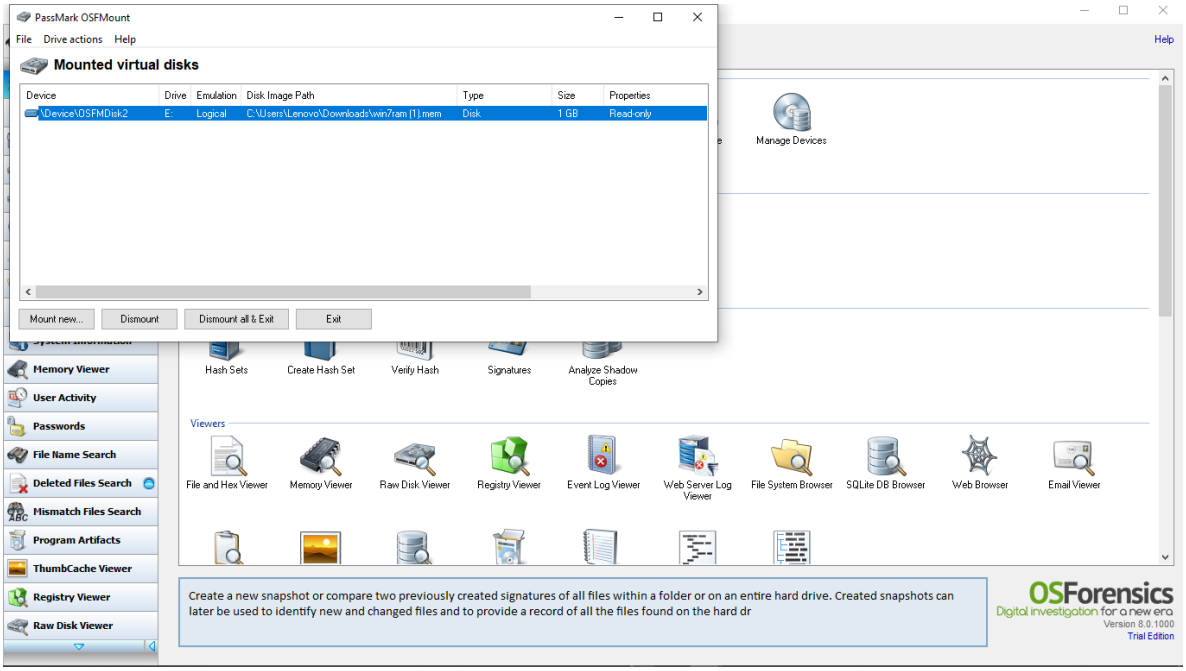
1. Descargo el archivo que me compartió mi compañero



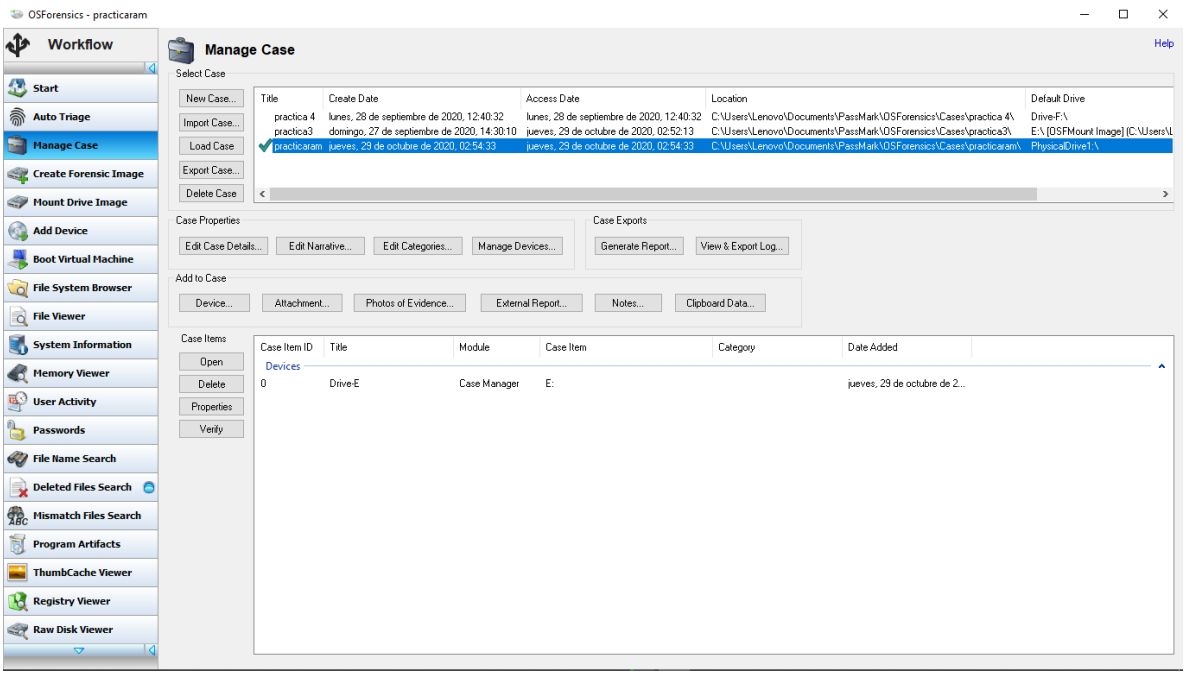
2. Monto la memoria RAM en el programa osforensics



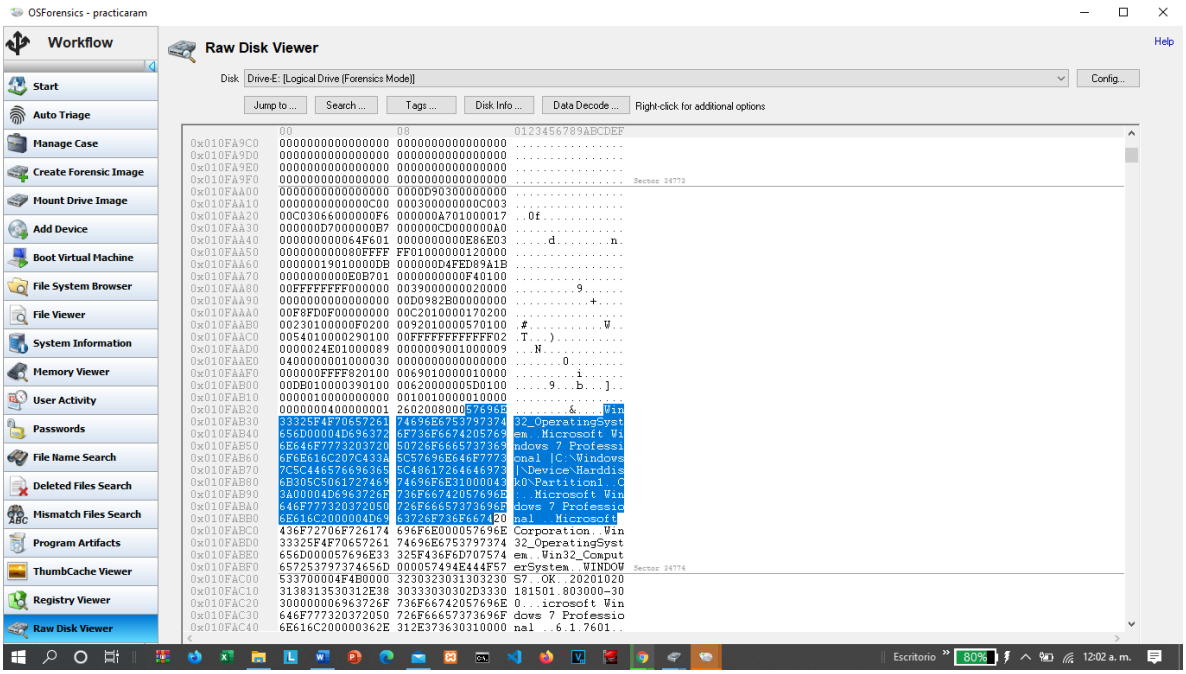
3. En la siguiente imagen se visualiza que ya esta montada y que esta utilizando la unidad E



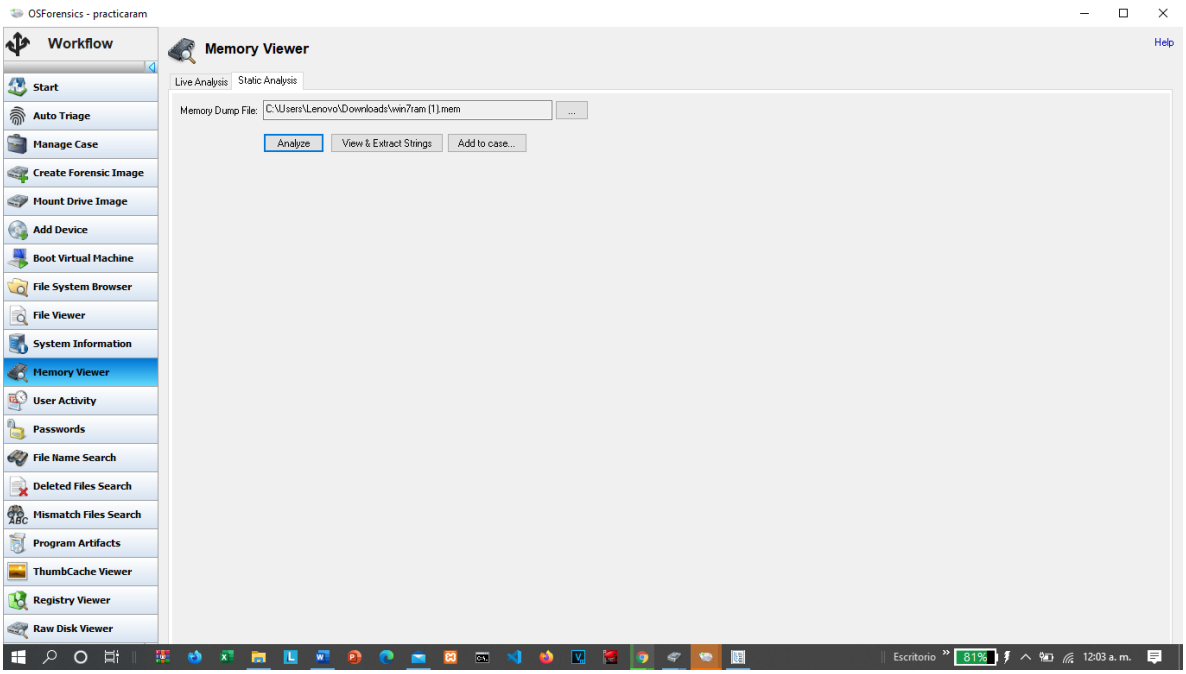
4. Creare un caso y agregare la evidencia



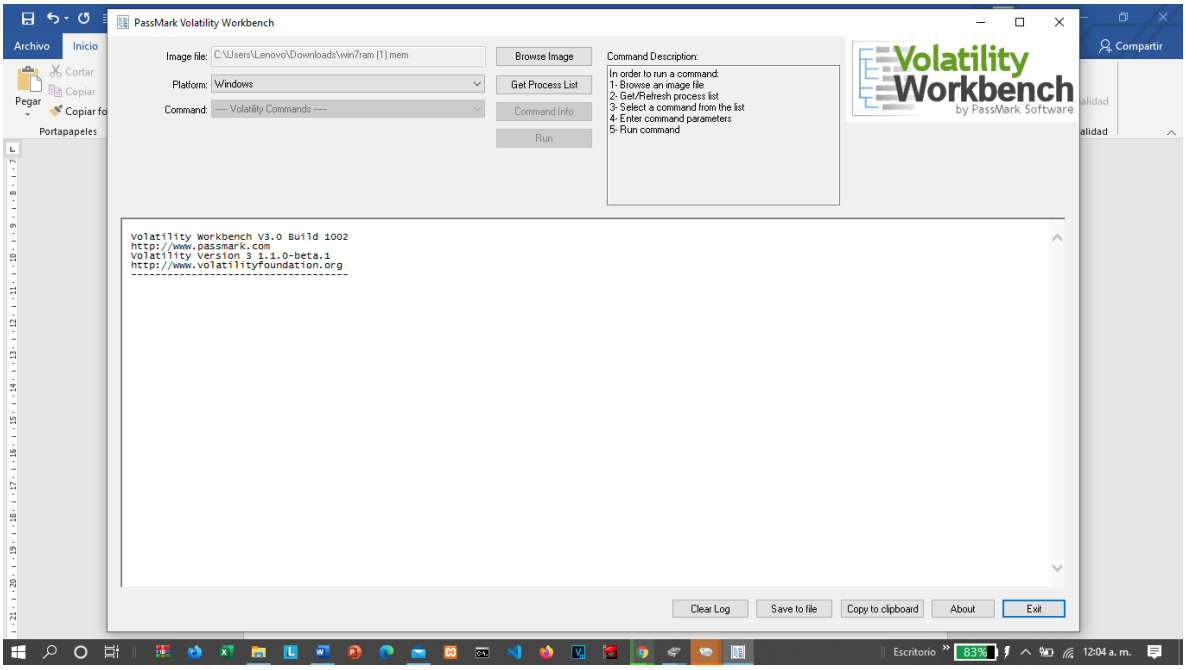
5. Busque en los metadatos que versión del sistema de Windows 7 se utilizo



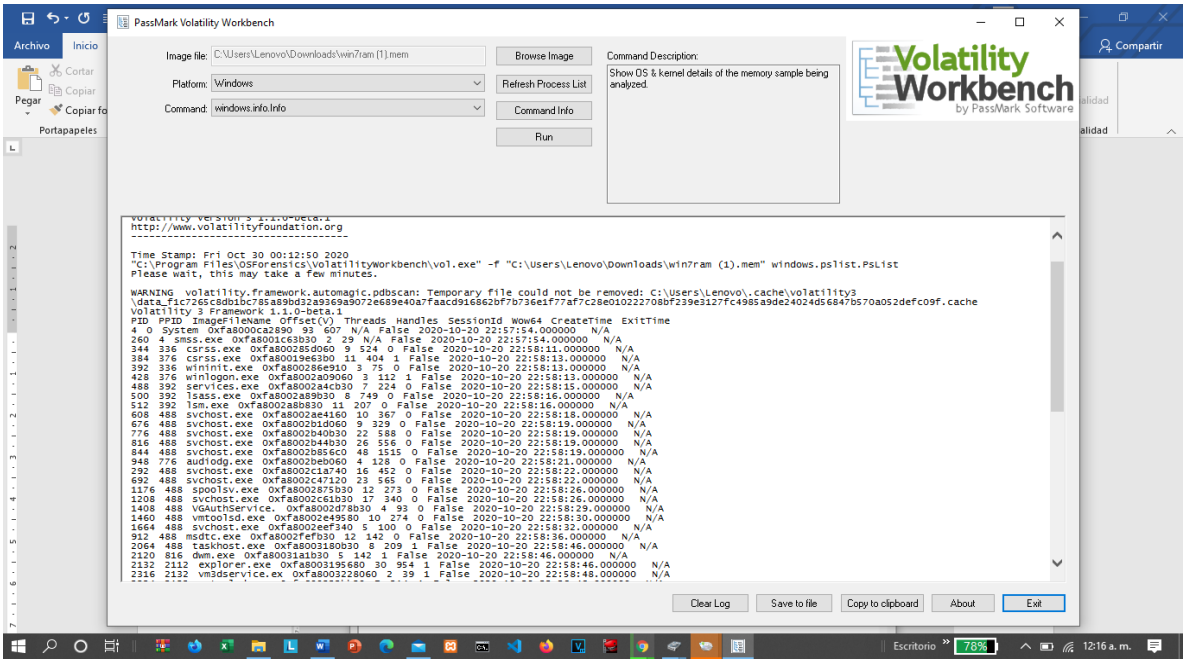
6. Ahora analizare la memoria con el apartado de memory viewer, selecciono el archivo que deseo analizar y le doy en el botón de analyze.



7. Nos abrirá la siguiente ventana y le damos en get process list



8. Tenemos que esperar unos minutos para que cargue la información, una vez cargada nos aparece el PID que es el identificador del proceso dentro del sistema operativo, PPID es el proceso padre que disparo al proceso



9. Siempre es importante tener el hash en cualquier tipo de investigación, para poder comprobar si un archivo se ha sido modificado o no, el hash de cada archivo es único