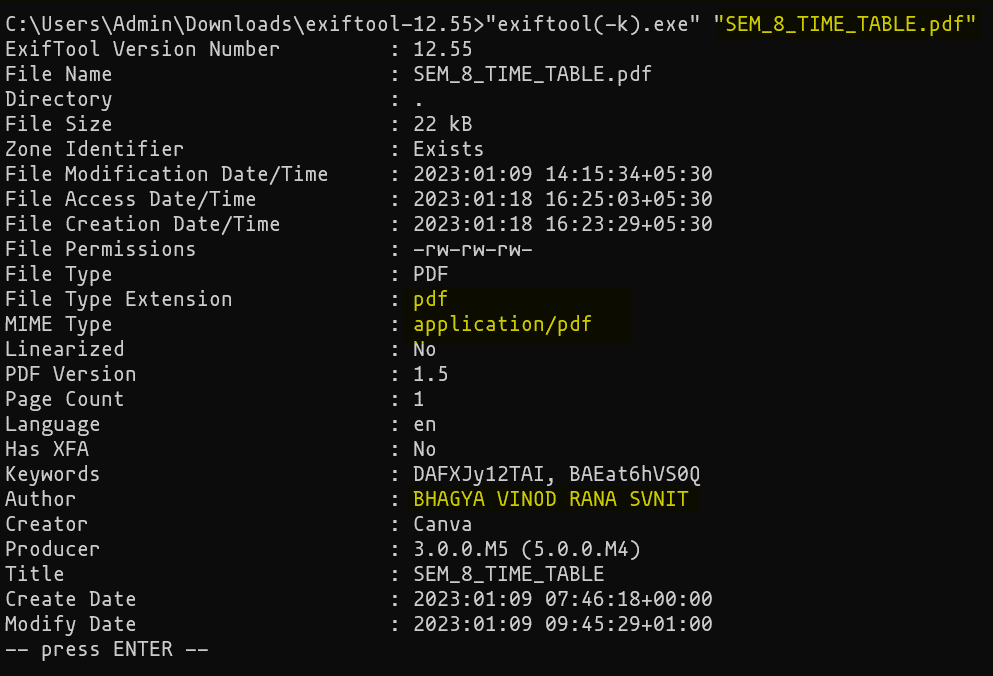
Cyber Law and Forensics (CS402)

Lab Assignment 1

**U19CS012**

1.) Find **Original Extension** of File. [Exif Tool]



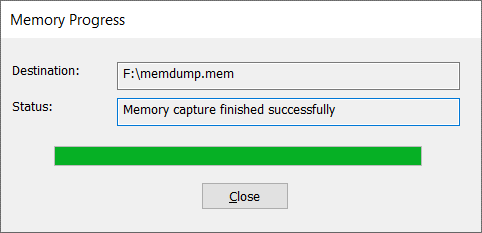
**Memory Acquisition –** Dumping of memory of Target Machine to Disk. {Process of acquiring Volatile Memory to Non-Volatile Storage [from file to disk]}

2.) Capture RAM using **FTK Imager by AccessData**

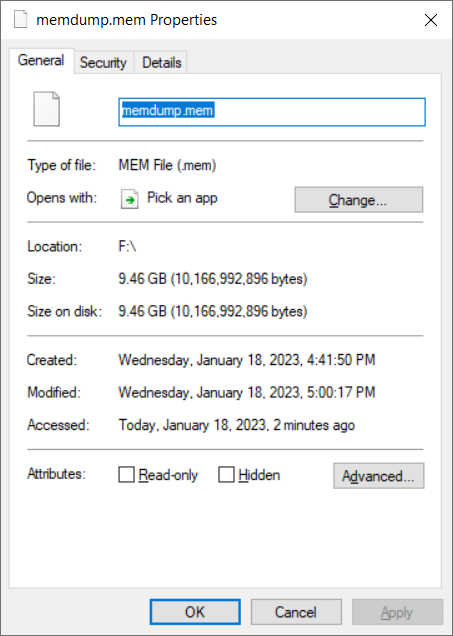
- Page File is Extended Version of RAM. – Pagefile.sys

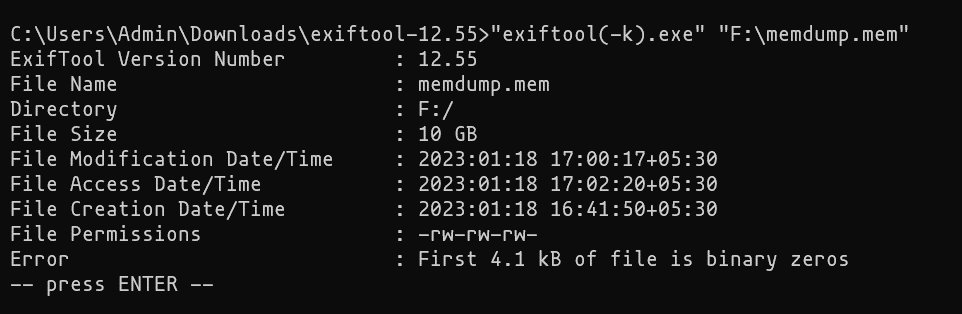
- Hiberfil.sys

- Hibernation vs Sleep Mode



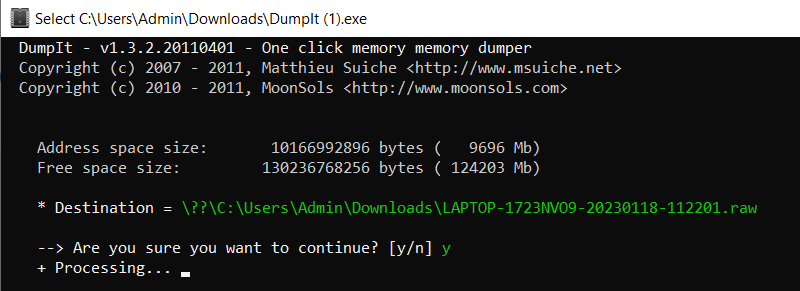
Good Practice to store the RAM (memdump.mem) File in External Drive. (Eg. Pendrive).

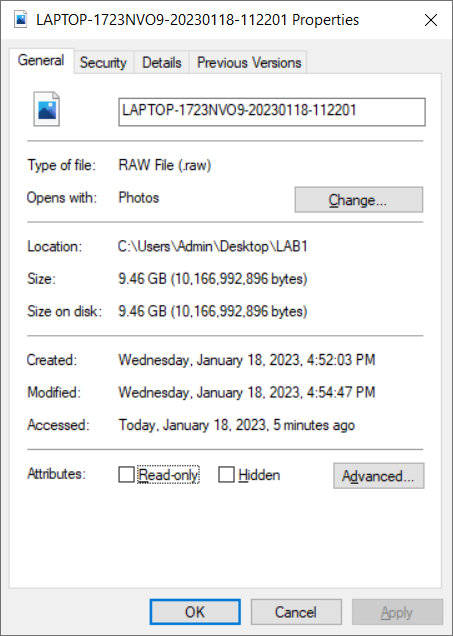




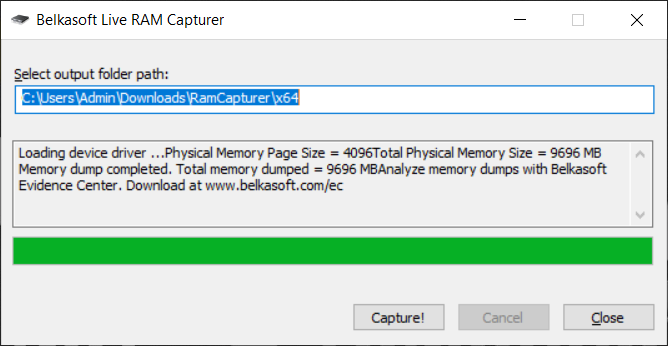
Also, Checked it with exiftool for Information.

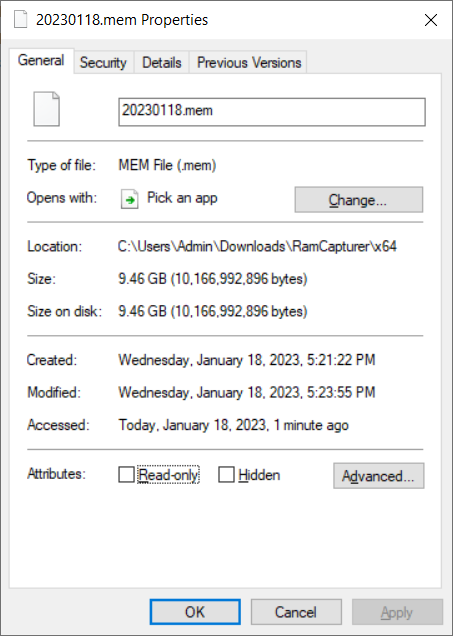
3.) Capture RAM using **DumpIt (Camoe Memory Toolkit by Comae Technologies)**





4.) Capture RAM using **Belkasoft Live RAM Explorer**





**SUBMITTED BY**: U19CS012

BHAGYA VINOD RANA