Cyber Law and Forensics (CS402)

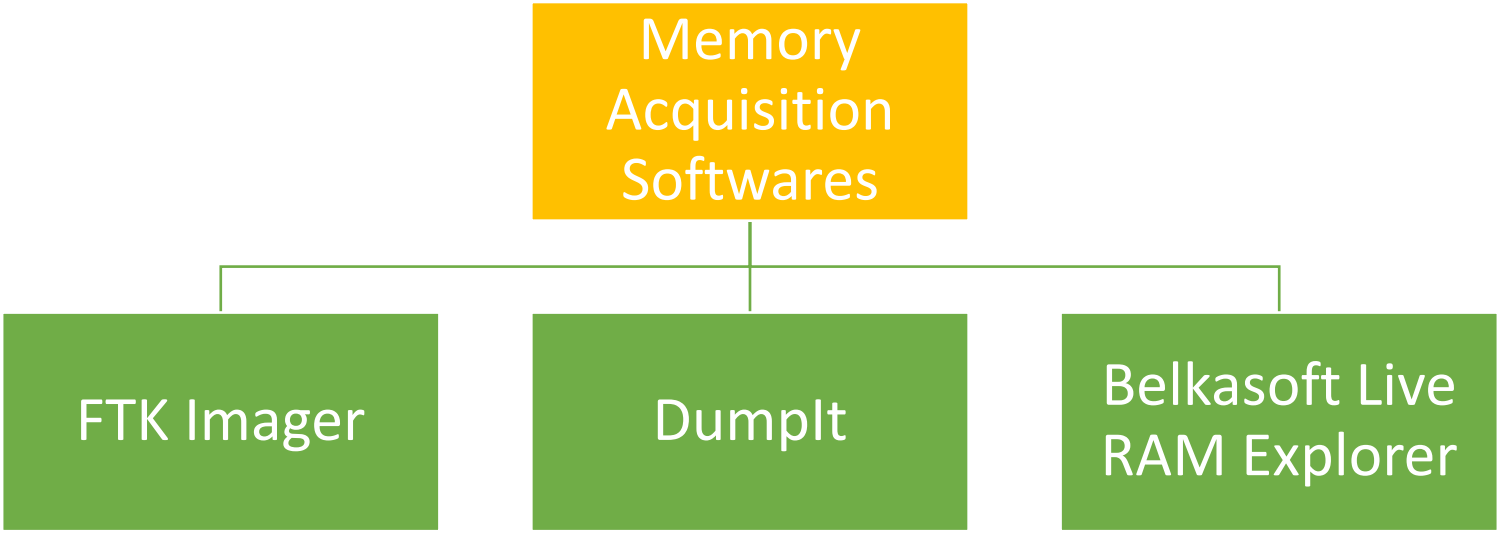
Lab Assignment 1

U19CS012

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

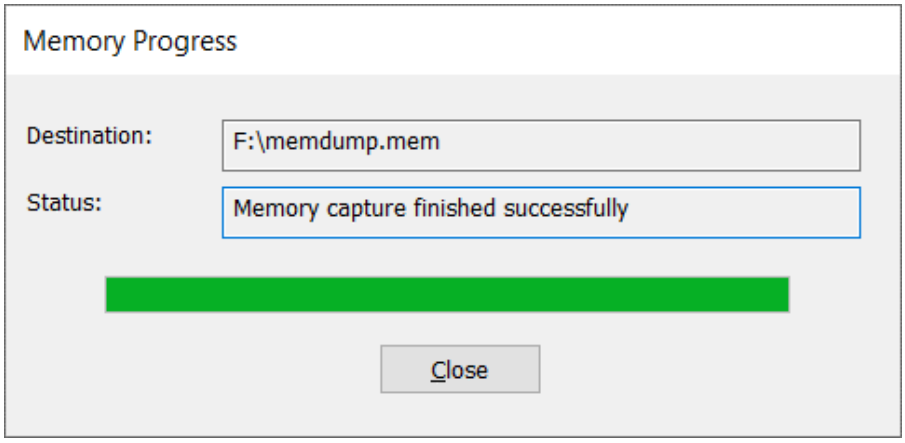
```
C:\Users\Admin\Downloads\exiftool-12.55>"exiftool(-k).exe" "SEM_8_TIME_TABLE.pdf"
ExifTool Version Number         : 12.55
File Name                       : SEM_8_TIME_TABLE.pdf
Directory                       : .
File Size                       : 22 kB
Zone Identifier                 : Exists
File Modification Date/Time     : 2023:01:09 14:15:34+05:30
File Access Date/Time           : 2023:01:18 16:25:03+05:30
File Creation Date/Time         : 2023:01:18 16:23:29+05:30
File Permissions                : -rw-rw-rw-
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
Linearized                      : No
PDF Version                     : 1.5
Page Count                      : 1
Language                        : en
Has XFA                         : No
Keywords                        : DAFXJy12TAI, BAEat6hVS0Q
Author                          : BHAGYA VINOD RANA SVNIT
Creator                         : Canva
Producer                        : 3.0.0.M5 (5.0.0.M4)
Title                           : SEM_8_TIME_TABLE
Create Date                     : 2023:01:09 07:46:18+00:00
Modify Date                     : 2023:01:09 09:45:29+01:00
-- press ENTER --
```

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

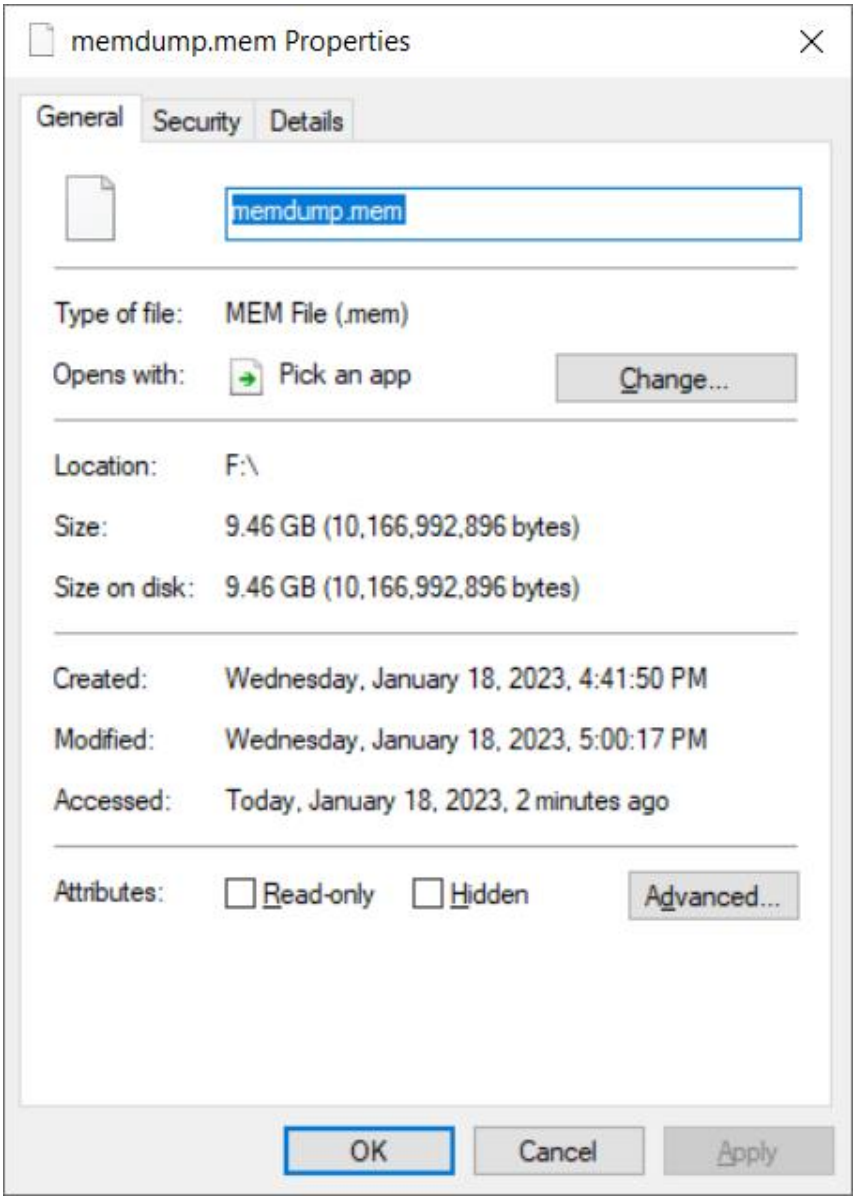


2.) Capture RAM using **FTK Imager by AccessData**

- Page File is Extended Version of RAM. – Pagefile.sys
- Hiberfil.sys
- Hibernation vs Sleep Mode



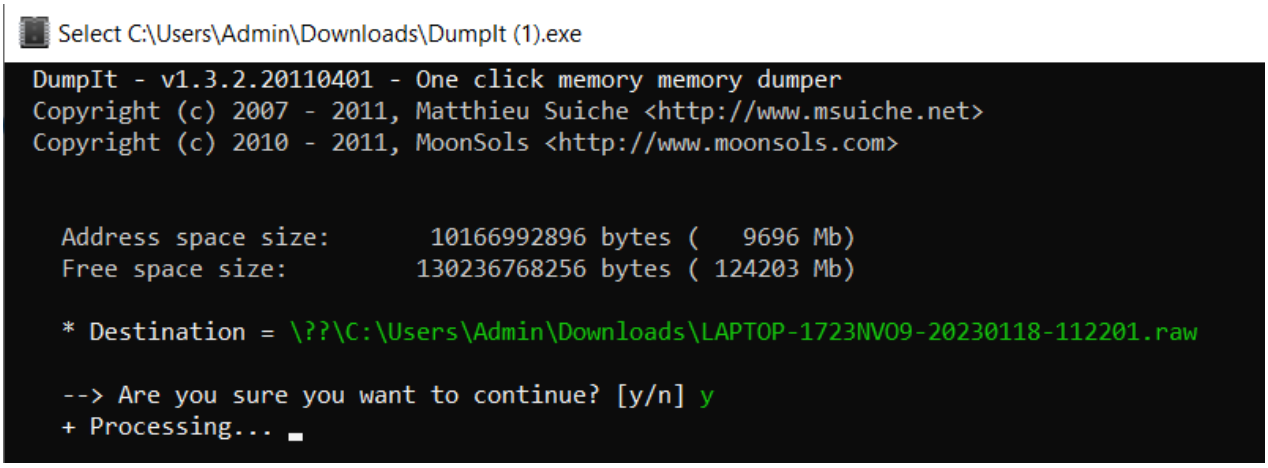
Good Practice to store the RAM (memdump.mem) File in External Drive. (Eg. Pendrive).

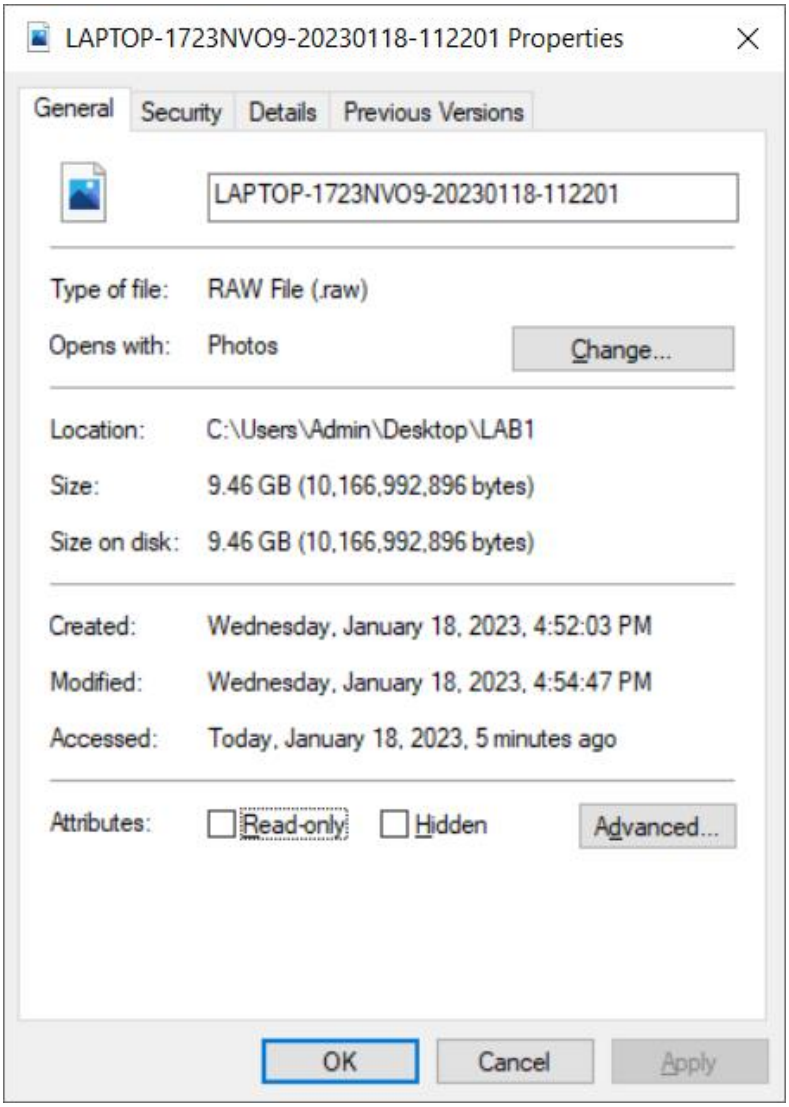



```
C:\Users\Admin\Downloads\exiftool-12.55>"exiftool(-k).exe" "F:\memdump.mem"
ExifTool Version Number         : 12.55
File Name                       : memdump.mem
Directory                       : F:/
File Size                       : 10 GB
File Modification Date/Time     : 2023:01:18 17:00:17+05:30
File Access Date/Time           : 2023:01:18 17:02:20+05:30
File Creation Date/Time         : 2023:01:18 16:41:50+05:30
File Permissions                : -rw-rw-rw-
Error                           : First 4.1 kB of file is binary zeros
-- press ENTER --
```

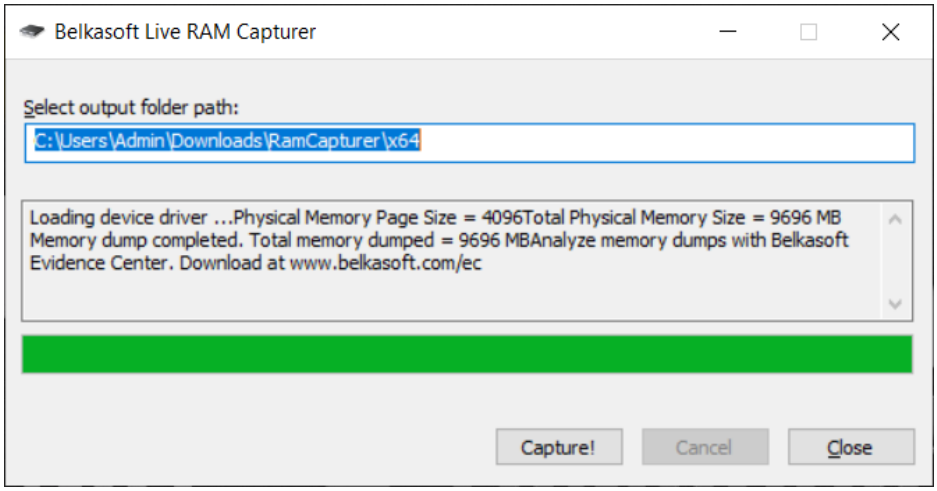
Also, Checked it with exiftool for Information.

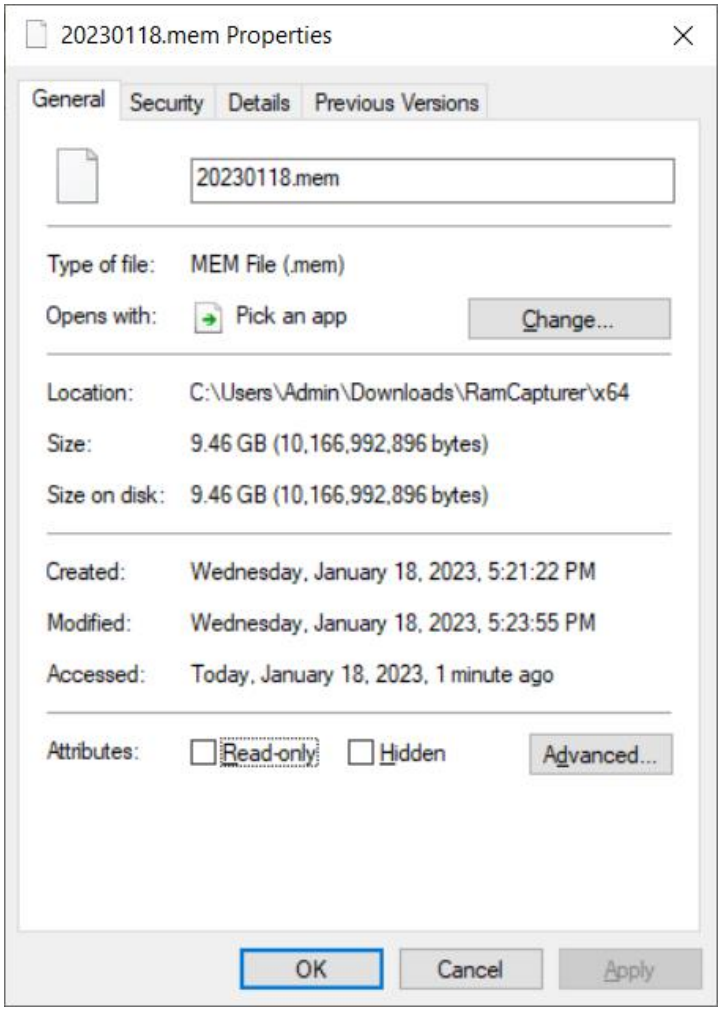
3.) Capture RAM using **DumpIt (Camoe Memory Toolkit by Comae Technologies)**





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





SUBMITTED BY: U19CS012

BHAGYA VINOD RANA