Digital Forensics

SRN : PES1UG20CS825	NAME : PREM SAGAR J S	SEC : ‘H’

Lab Assignment - 4

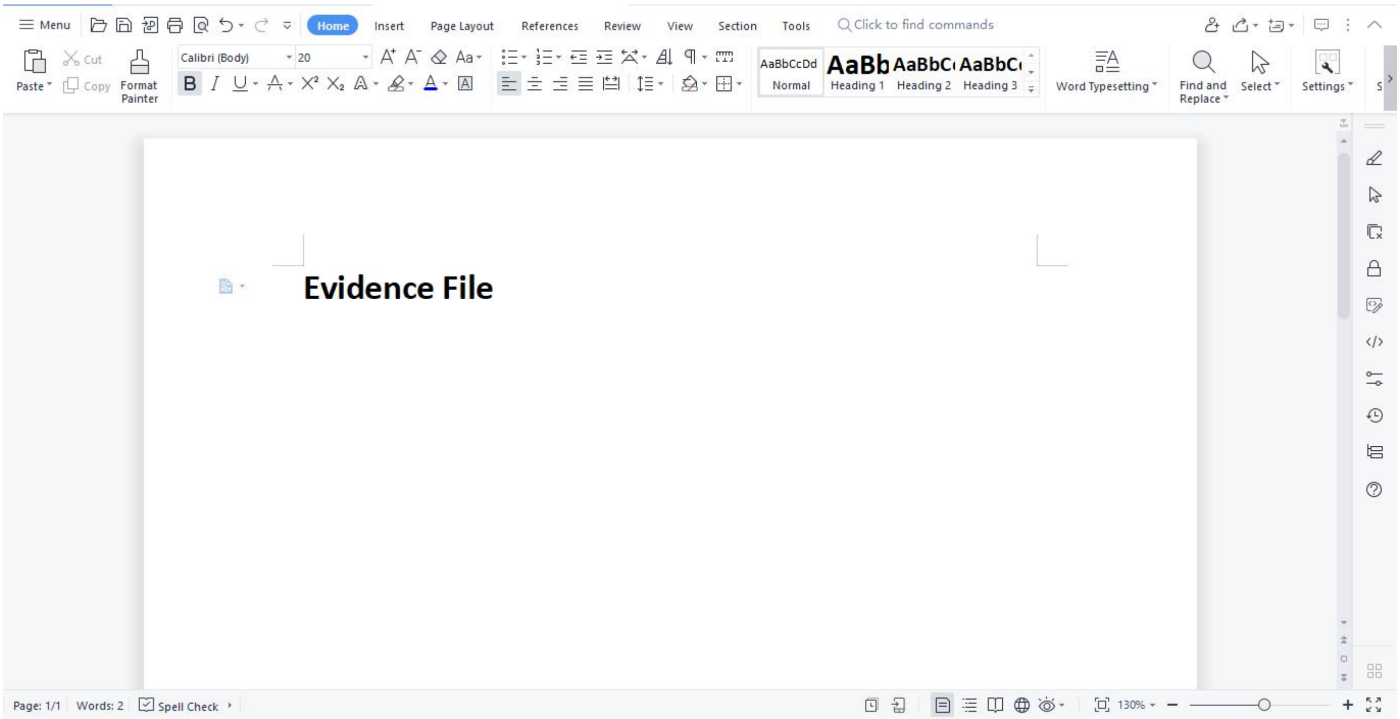
Lab 3 : Identify the file metadata using OSForensics

OSForensics allows you to search for files many times faster than the search functionality in Windows. Results can be analyzed in the form of a file listing, a Thumbnail View, or a Timeline View which allows you to determine where significant file change activity has occurred.

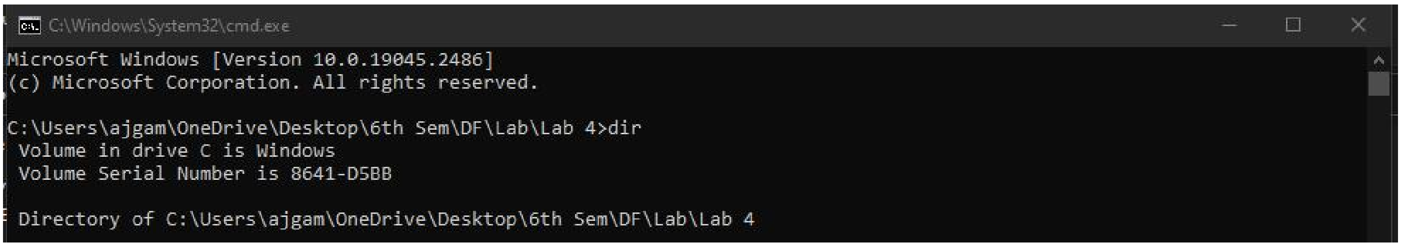
Steps:

- ➢ Downloaded and installed OSFrensics on pc with trail version.

1. Start Microsoft Word, and in a new document, type By creating a file, you can identify the author with file metadata. Save it in your work folder then exit Microsoft Word.



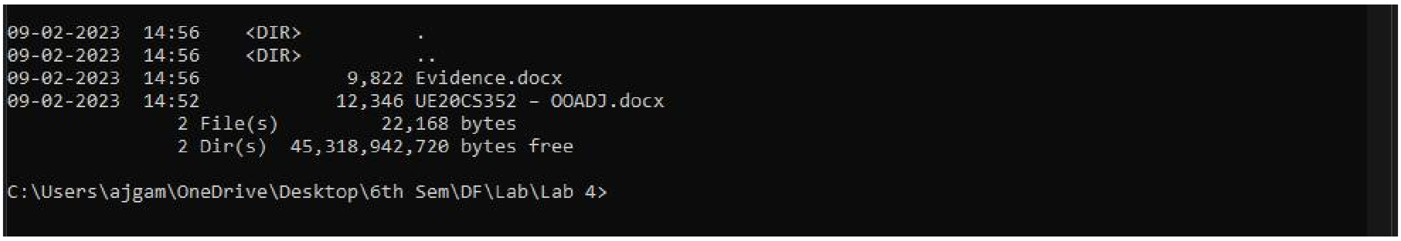
Evidence File



```
Microsoft Windows [Version 10.0.19045.2486]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ajgam\OneDrive\Desktop\6th Sem\DF\Lab\Lab 4>dir
 Volume in drive C is Windows
 Volume Serial Number is 8641-D5BB

 Directory of C:\Users\ajgam\OneDrive\Desktop\6th Sem\DF\Lab\Lab 4
```



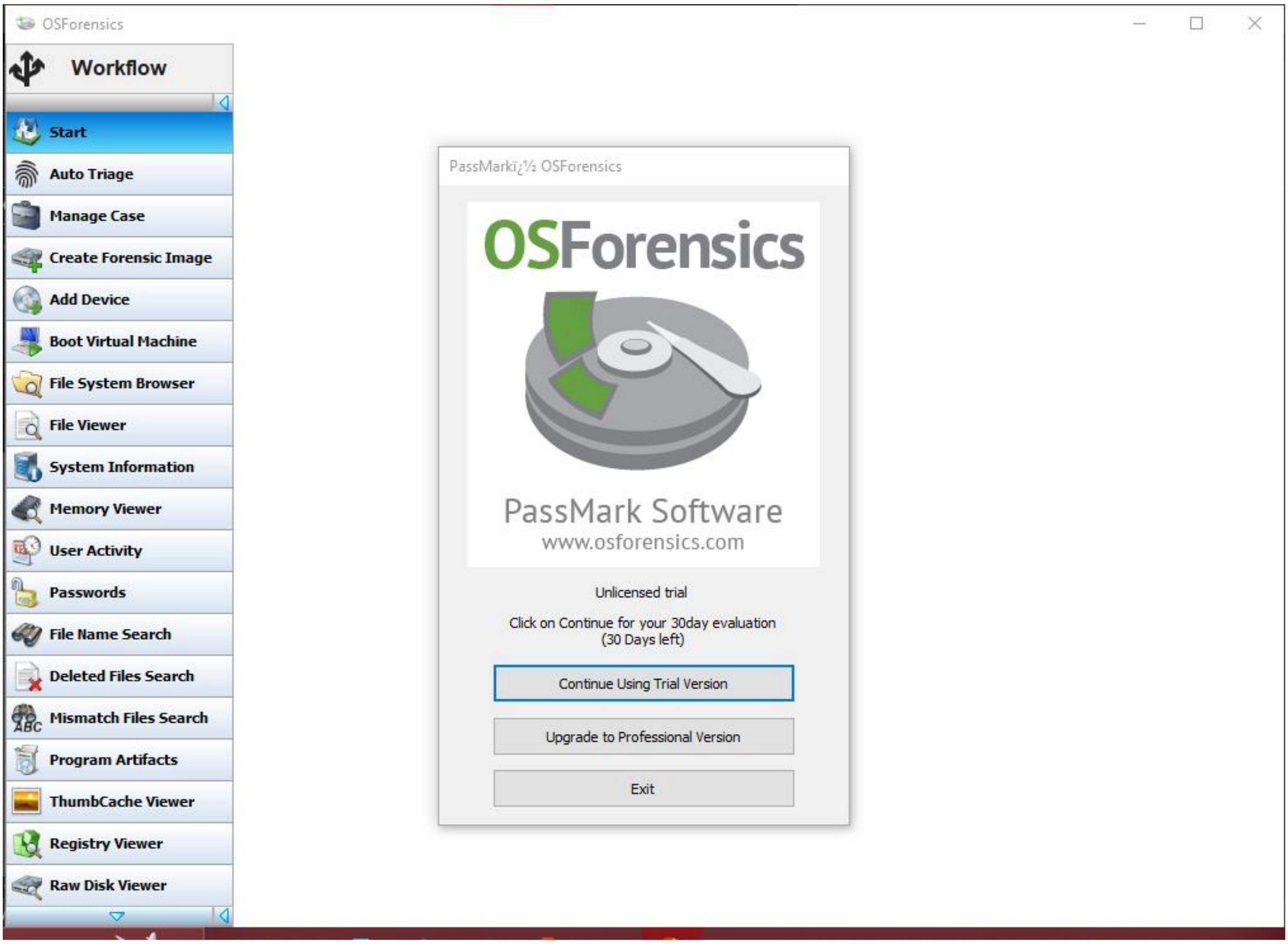
```
09-02-2023  14:56    <DIR>          .
09-02-2023  14:56    <DIR>          ..
09-02-2023  14:56             9,822 Evidence.docx
09-02-2023  14:52            12,346 UE20CS352 - OOADJ.docx
               2 File(s)         22,168 bytes
               2 Dir(s)  45,318,942,720 bytes free

C:\Users\ajgam\OneDrive\Desktop\6th Sem\DF\Lab\Lab 4>
```

2. Start OSForensics by clicking Start, OSForensics. If Windows prompts you to confirm that you trust this program, click OK or Yes. Click Continue Using Trial Version, if prompted.

3. If you see a message asking whether you want to upgrade to the professional version, click the Continue Using Trial Version button.

- Proceeding with the trail version

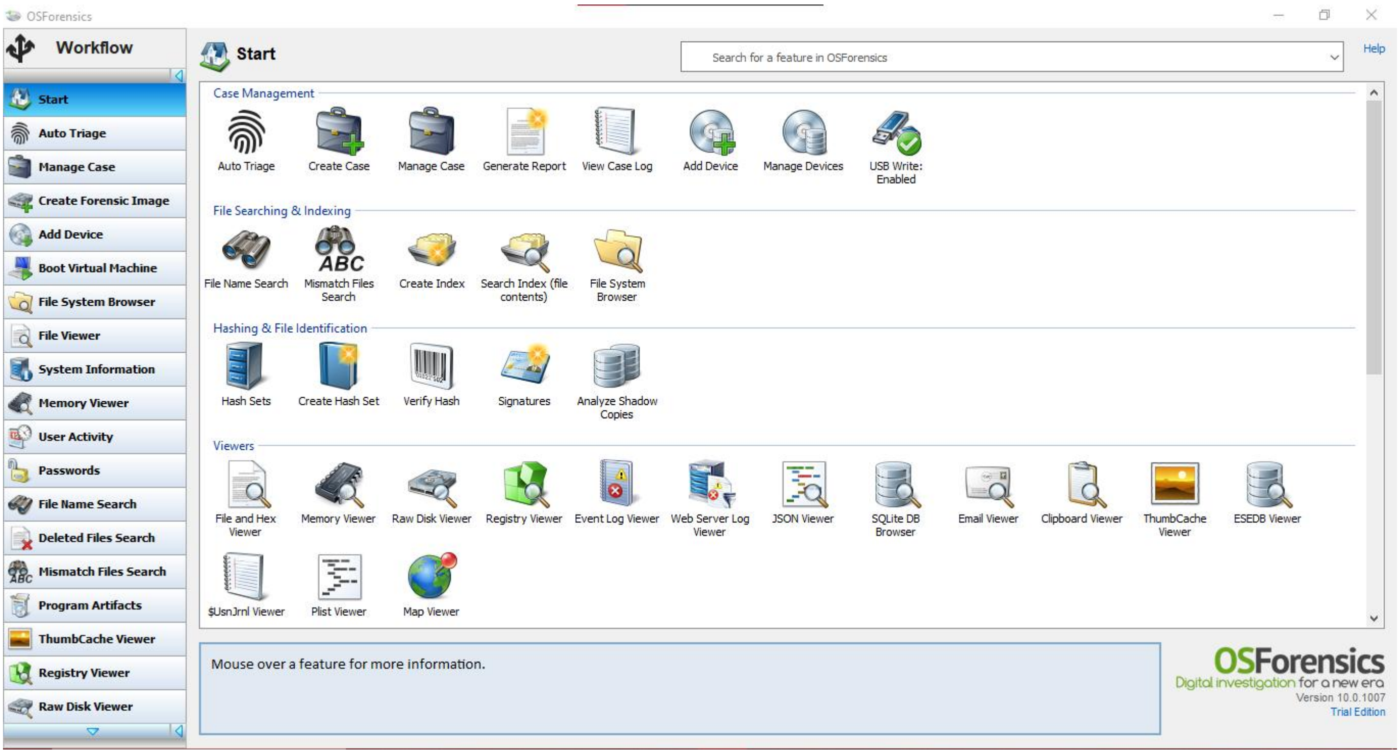


Unlicensed trial

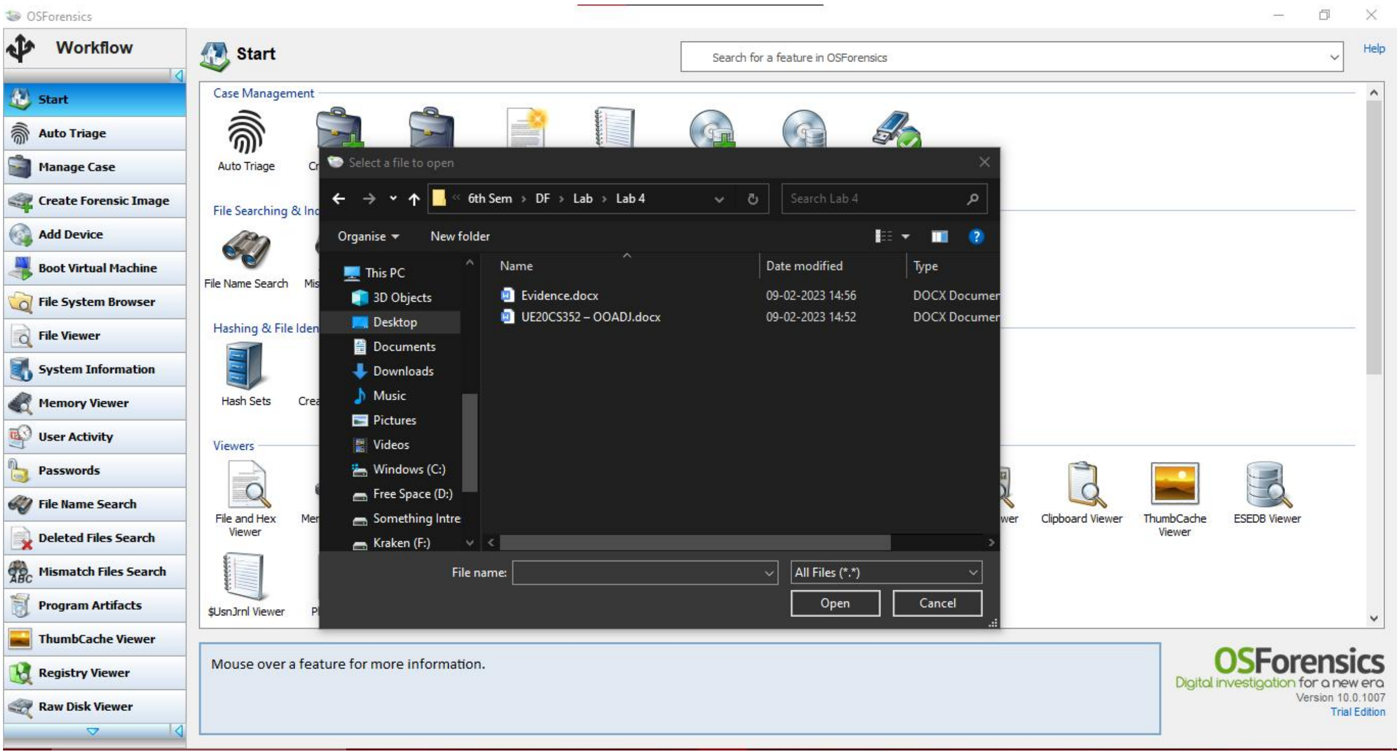
Click on Continue for your 30day evaluation
(30 Days left)

3. In the OSForensics main window, notice the Viewers section in the right pane. Click File and Hex Viewer. In the “Select a file to open” dialog box that opens, navigate to your work folder and double-click the file you created in Step 1.

➢ Selecting the Doc file which was created in the step 1.



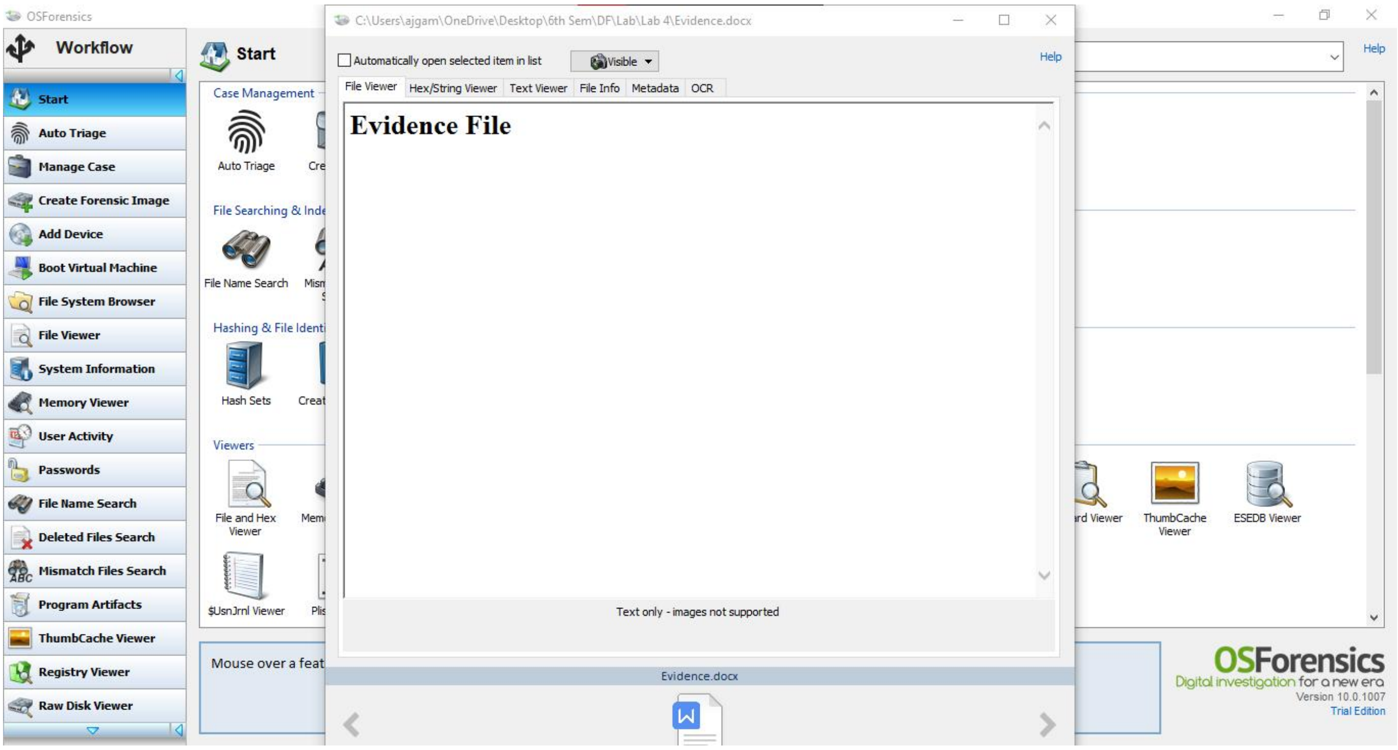
Docx file : Evidence.docx



Name	Date modified	Type
Evidence.docx	09-02-2023 14:56	DOCX Documer
UE20CS352 – OOADJ.docx	09-02-2023 14:52	DOCX Documer

4. The dialog box that opens that has five tabs. Click the File Info tab. You can see where the file is located along with the date and time it was created. Notice that the file size and its size on the disk are different.

- ➢ Viewing the file content using file viewer tab



C:\Users\ajgam\OneDrive\Desktop\6th Sem\DF\Lab\Lab 4\Evidence.docx

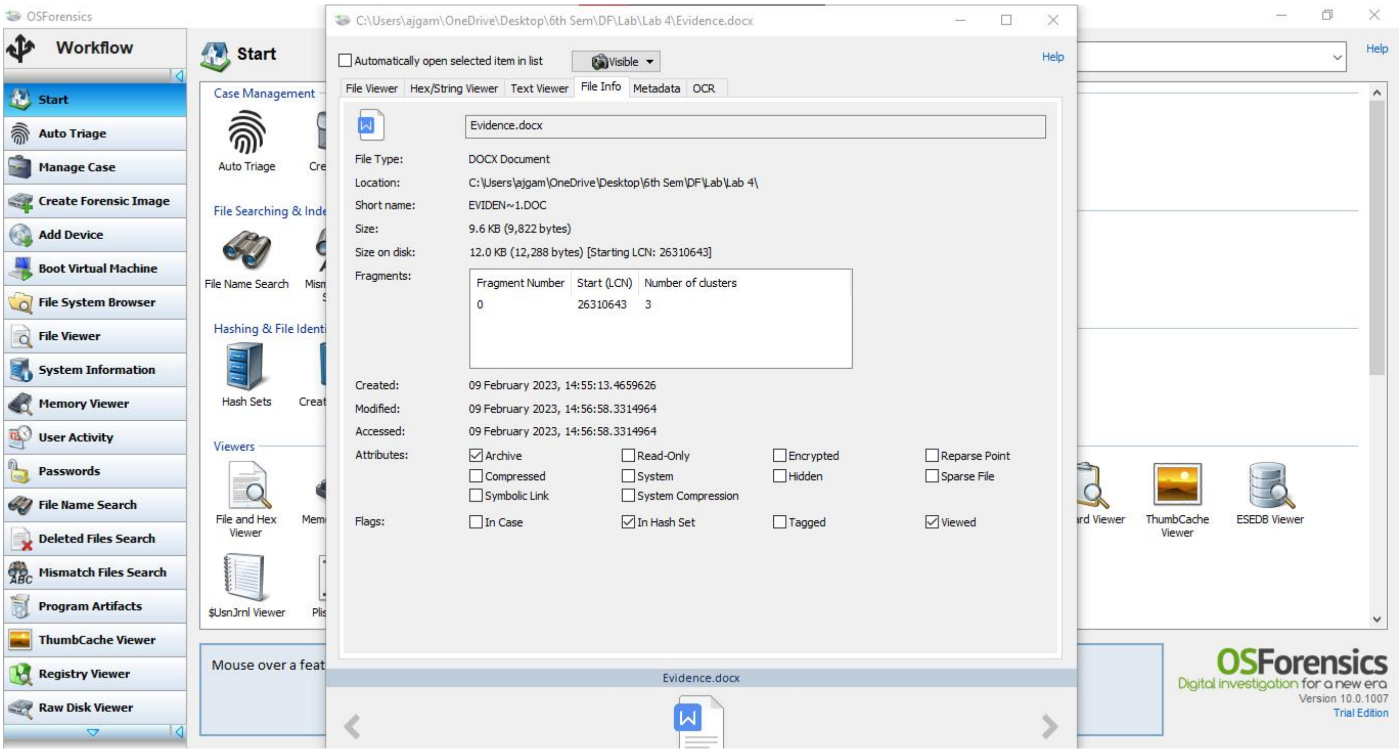
□ Automatically open selected item in list

Evidence File

Text only - images not supported

Evidence.docx

- ➢ File info tab



C:\Users\ajgam\OneDrive\Desktop\6th Sem\DF\Lab\Lab 4\Evidence.docx

□ Automatically open selected item in list

Evidence.docx

File Type: DOCX Document
Location: C:\Users\ajgam\OneDrive\Desktop\6th Sem\DF\Lab\Lab 4\
Short name: EVIDEN~1.DOC
Size: 9.6 KB (9,822 bytes)
Size on disk: 12.0 KB (12,288 bytes) [Starting LCN: 26310643]
Fragments:

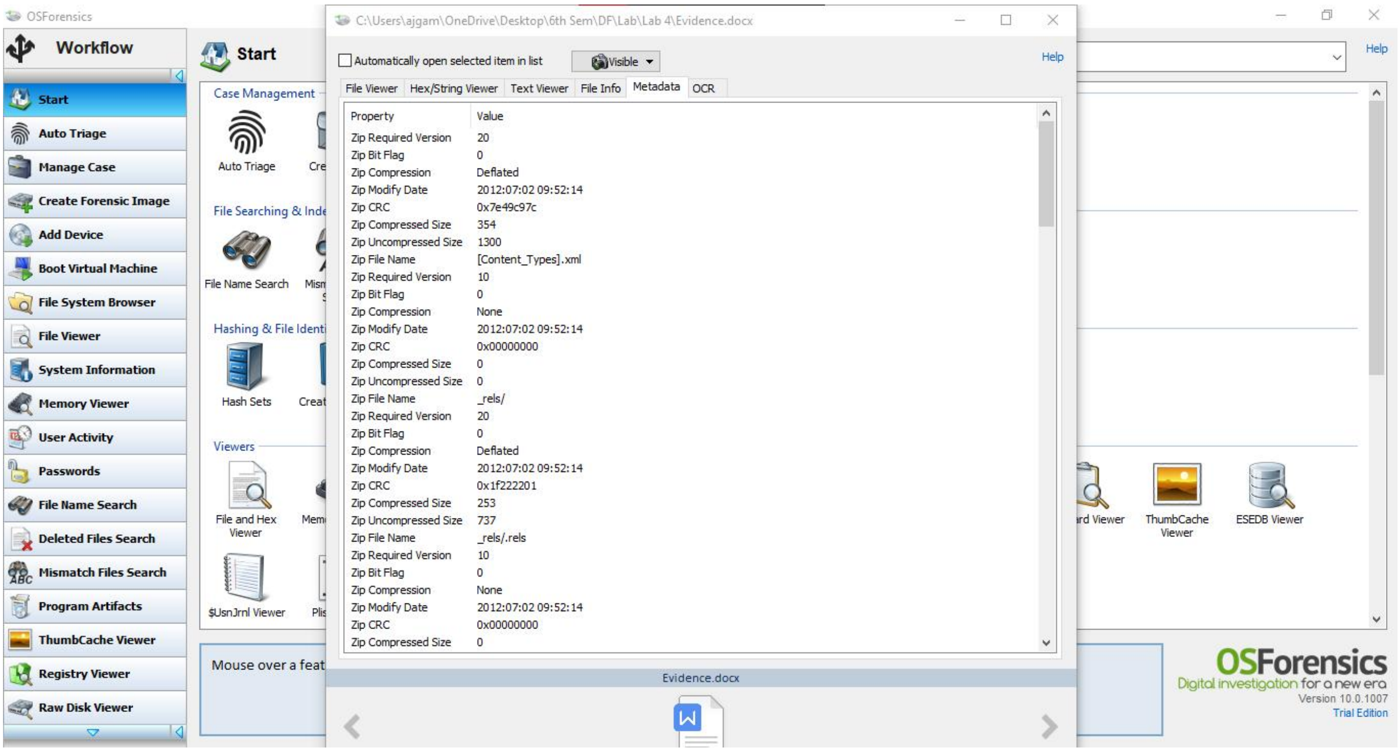
Fragment Number	Start (LCN)	Number of clusters
0	26310643	3

Created: 09 February 2023, 14:55:13.4659626
Modified: 09 February 2023, 14:56:58.3314964
Accessed: 09 February 2023, 14:56:58.3314964
Attributes: ☑ Archive □ Read-Only □ Encrypted □ Reparse Point □ Compressed □ System □ Hidden □ Sparse File □ Symbolic Link □ System Compression
Flags: □ In Case ☑ In Hash Set □ Tagged ☑ Viewed

Evidence.docx

6. Click the Metadata tab. The information in this tab includes file permissions, file type, file size, and other items. Scroll to the bottom of this tab, where you can see who created the file and who last modified the file

- ➢ Metadata tab

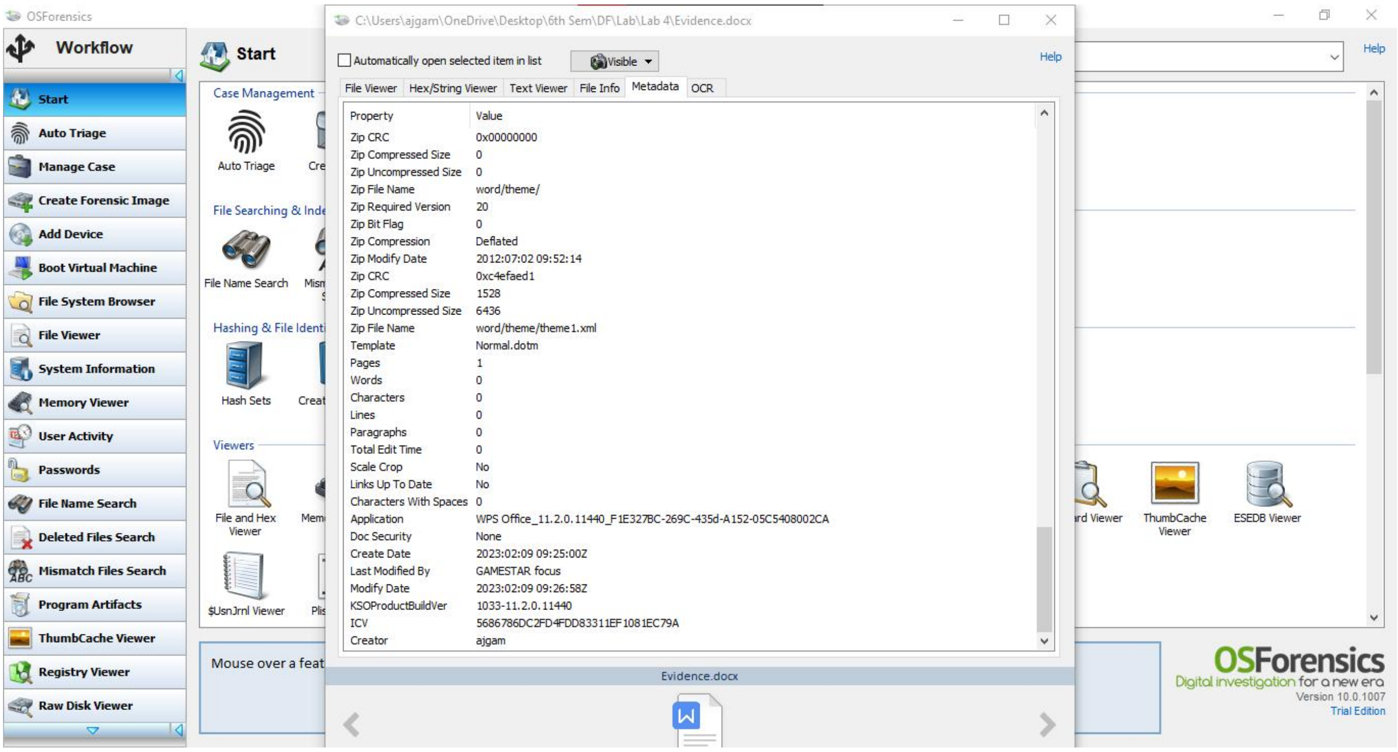


C:\Users\ajgam\OneDrive\Desktop\6th Sem\DF\Lab\Lab 4\Evidence.docx

□ Automatically open selected item in list

Property	Value
Zip Required Version	20
Zip Bit Flag	0
Zip Compression	Deflated
Zip Modify Date	2012:07:02 09:52:14
Zip CRC	0x7e49c97c
Zip Compressed Size	354
Zip Uncompressed Size	1300
Zip File Name	[Content_Types].xml
Zip Required Version	10
Zip Bit Flag	0
Zip Compression	None
Zip Modify Date	2012:07:02 09:52:14
Zip CRC	0x00000000
Zip Compressed Size	0
Zip Uncompressed Size	0
Zip File Name	_rels/
Zip Required Version	20
Zip Bit Flag	0
Zip Compression	Deflated
Zip Modify Date	2012:07:02 09:52:14
Zip CRC	0x1f222201
Zip Compressed Size	253
Zip Uncompressed Size	737
Zip File Name	_rels/.rels
Zip Required Version	10
Zip Bit Flag	0
Zip Compression	None
Zip Modify Date	2012:07:02 09:52:14
Zip CRC	0x00000000
Zip Compressed Size	0

- ➢ All the information of the file is displayed in the metadata tab



C:\Users\ajgam\OneDrive\Desktop\6th Sem\DF\Lab\Lab 4\Evidence.docx

□ Automatically open selected item in list

Property	Value
Zip CRC	0x00000000
Zip Compressed Size	0
Zip Uncompressed Size	0
Zip File Name	word/theme/
Zip Required Version	20
Zip Bit Flag	0
Zip Compression	Deflated
Zip Modify Date	2012:07:02 09:52:14
Zip CRC	0xc4efaed1
Zip Compressed Size	1528
Zip Uncompressed Size	6436
Zip File Name	word/theme/theme1.xml
Template	Normal.dotm
Pages	1
Words	0
Characters	0
Lines	0
Paragraphs	0
Total Edit Time	0
Scale Crop	No
Links Up To Date	No
Characters With Spaces	0
Application	WPS Office_11.2.0.11440_F1E327BC-269C-435d-A152-05C5408002CA
Doc Security	None
Create Date	2023:02:09 09:25:00Z
Last Modified By	GAMESTAR focus
Modify Date	2023:02:09 09:26:58Z
KSOProductBuildVer	1033-11.2.0.11440
ICV	5686786DC2FD4FDD83311EF1081EC79A
Creator	ajgam

Question:

OSForensics allows you to search for files many times faster than the search functionality in Windows - Justify

: -->

- OSForensics use specialised indexing and search algorithms to locate data on a computer's hard disc quickly. These algorithms are capable of instantly scanning the entire hard disc and creating an index of all files and their locations. This index enables OSForensics to search for files rapidly depending on criteria such as keywords, file type, or date changed, without having to scan the entire hard drive each time.

- In comparison, Windows' search functionality use a slower manner of searching. It examines the hard disc in real time as you write your search query and must scan each file separately to decide whether or not it satisfies the search criteria. This process can take a long time, especially on huge hard discs with many files.

- OSForensics can substantially speed up the process of finding files by employing an indexed search, making it several times faster than Windows' search feature. This can save time and effort, particularly when looking for specific files that may be difficult to locate manually.