Digital Forensics - Lab 4

Class No :	**CH2021221000516**	Slot :	**L49 + L50**
Course Code :	**CSE4004**	Faculty Name :	**Nagaraj SV**

Aadhitya Swarnesh

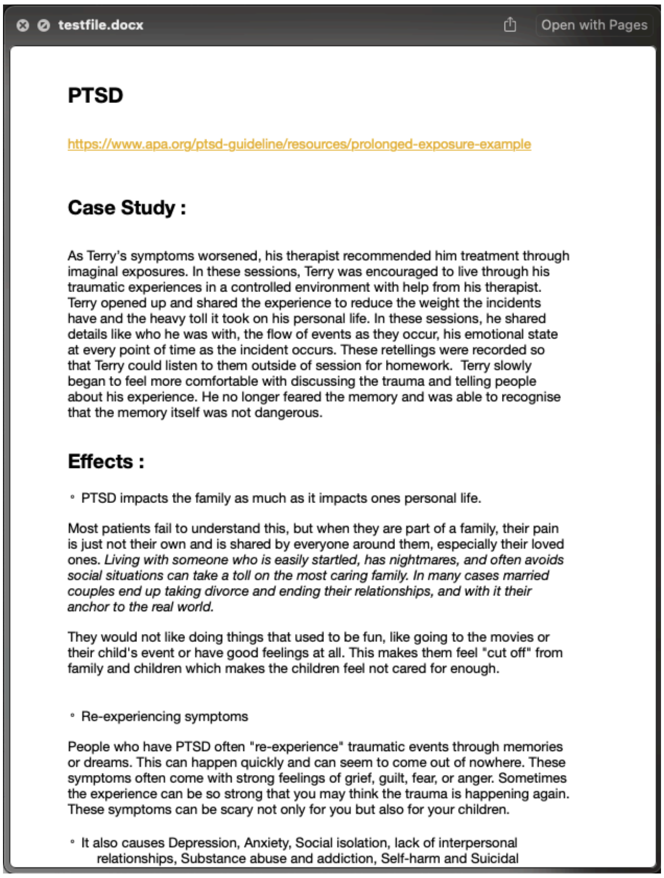
- 26 August 2021

Question 1 :

Using a Microsoft Office 2007 and later DOCX file, and view its properties in windows.

In order to proceed with this experiment, we first create a word document with some sample content as follows :

With this done, we then right click and open its properties in the windows operating system, on opening, the properties of the file can be viewed, which includes details like the location, type, size of the file, the last modified and created dates and times, the file permissions for different groups of users, etc.



PTSD

https://www.apa.org/ptsd-guideline/resources/prolonged-exposure-example

Case Study :

As Terry's symptoms worsened, his therapist recommended him treatment through imaginal exposures. In these sessions, Terry was encouraged to live through his traumatic experiences in a controlled environment with help from his therapist. Terry opened up and shared the experience to reduce the weight the incidents have and the heavy toll it took on his personal life. In these sessions, he shared details like who he was with, the flow of events as they occur, his emotional state at every point of time as the incident occurs. These retellings were recorded so that Terry could listen to them outside of session for homework. Terry slowly began to feel more comfortable with discussing the trauma and telling people about his experience. He no longer feared the memory and was able to recognise that the memory itself was not dangerous.

Effects :

- PTSD impacts the family as much as it impacts ones personal life.

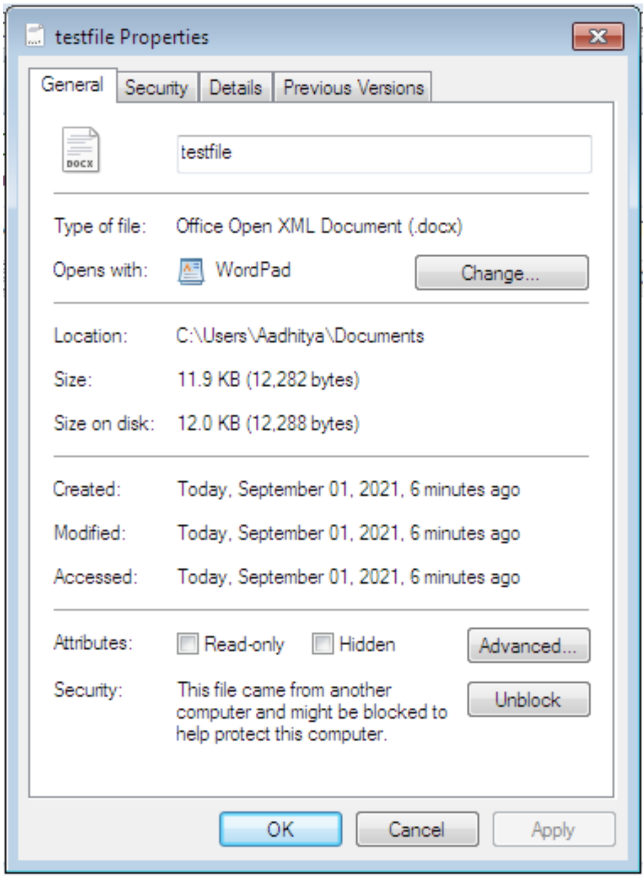
Most patients fail to understand this, but when they are part of a family, their pain is just not their own and is shared by everyone around them, especially their loved ones. *Living with someone who is easily startled, has nightmares, and often avoids social situations can take a toll on the most caring family. In many cases married couples end up taking divorce and ending their relationships, and with it their anchor to the real world.*

They would not like doing things that used to be fun, like going to the movies or their child's event or have good feelings at all. This makes them feel "cut off" from family and children which makes the children feel not cared for enough.

- Re-experiencing symptoms

People who have PTSD often "re-experience" traumatic events through memories or dreams. This can happen quickly and can seem to come out of nowhere. These symptoms often come with strong feelings of grief, guilt, fear, or anger. Sometimes the experience can be so strong that you may think the trauma is happening again. These symptoms can be scary not only for you but also for your children.

- It also causes Depression, Anxiety, Social isolation, lack of interpersonal relationships, Substance abuse and addiction, Self-harm and Suicidal



testfile

Type of file: Office Open XML Document (.docx)

Opens with: WordPad

Location: C:\Users\Aadhitya\Documents

Size: 11.9 KB (12,282 bytes)

Size on disk: 12.0 KB (12,288 bytes)

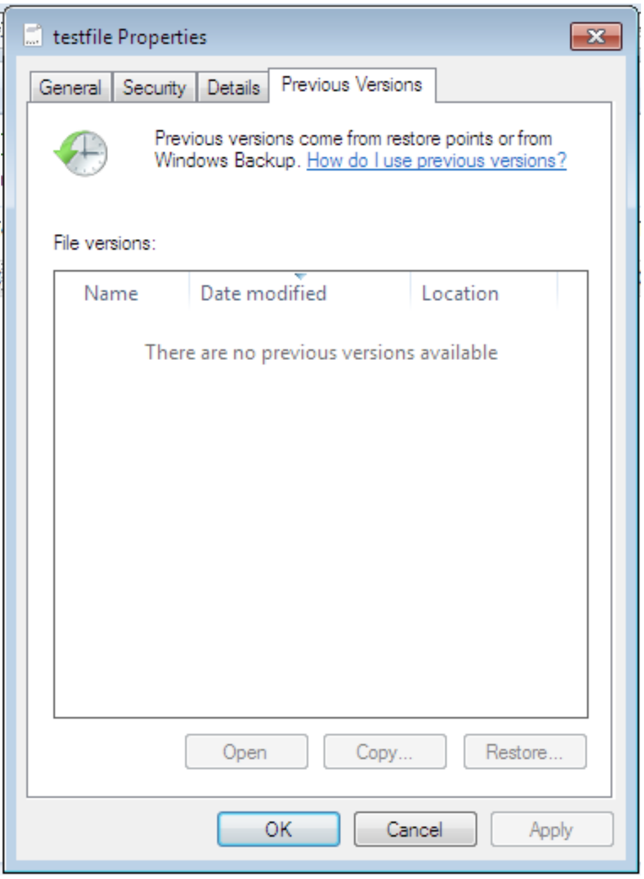
Created: Today, September 01, 2021, 6 minutes ago

Modified: Today, September 01, 2021, 6 minutes ago

Accessed: Today, September 01, 2021, 6 minutes ago

Attributes: □ Read-only □ Hidden

Security: This file came from another computer and might be blocked to help protect this computer.

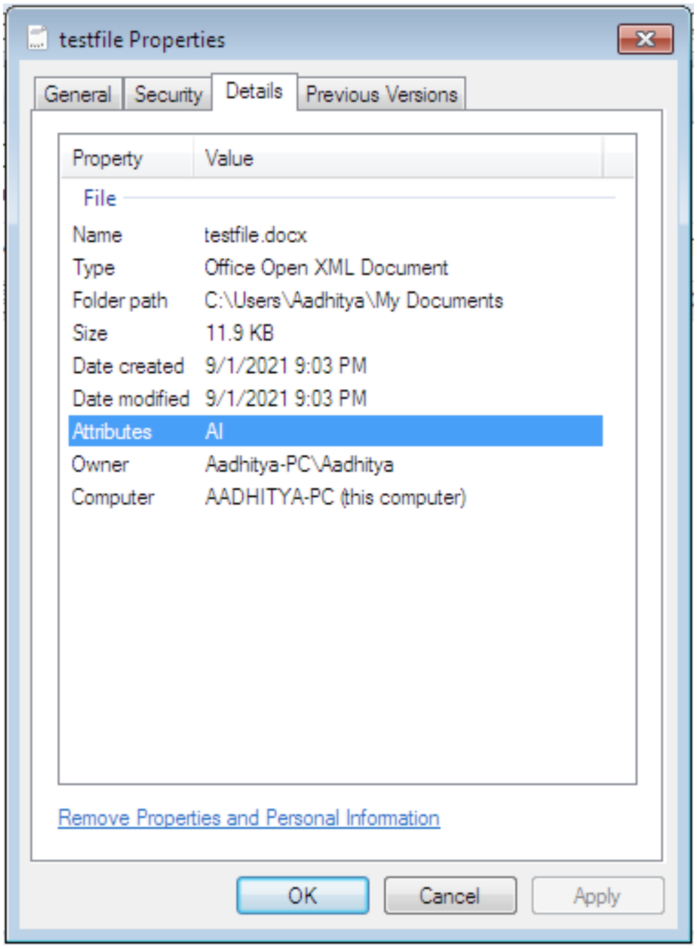


Previous versions come from restore points or from Windows Backup. How do I use previous versions?

File versions:

Name	Date modified	Location

There are no previous versions available



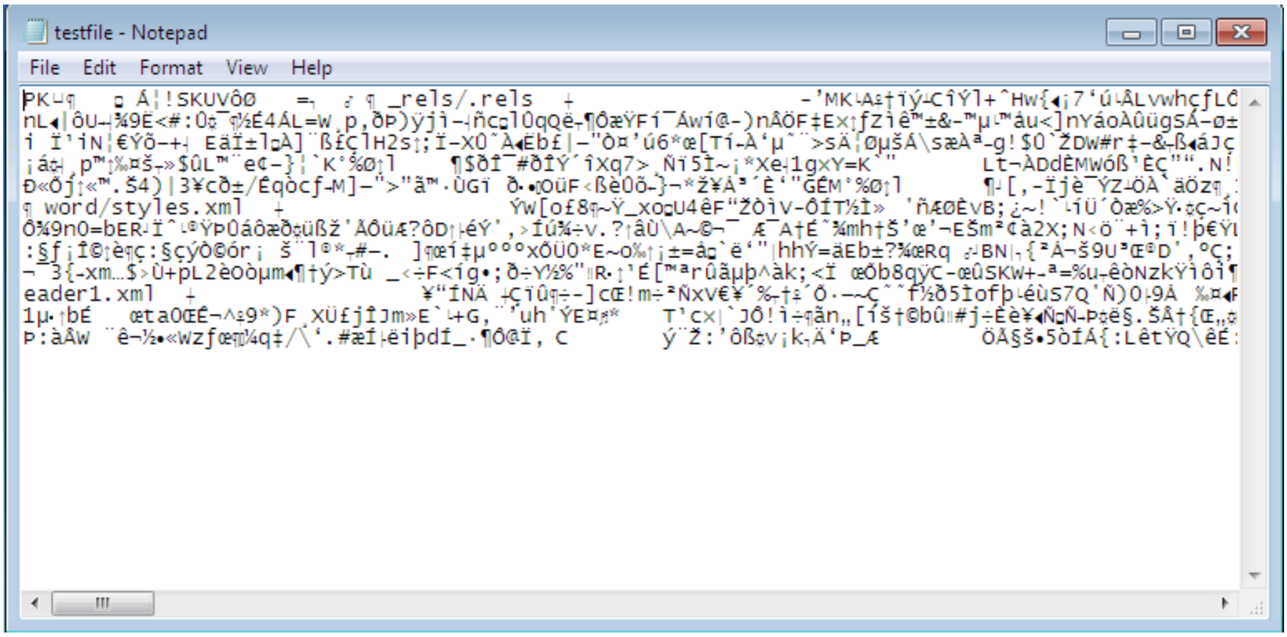
Property	Value
File	
Name	testfile.docx
Type	Office Open XML Document
Folder path	C:\Users\Aadhitya\My Documents
Size	11.9 KB
Date created	9/1/2021 9:03 PM
Date modified	9/1/2021 9:03 PM
Attributes	AI
Owner	Aadhitya-PC\Aadhitya
Computer	AADHITYA-PC (this computer)

Remove Properties and Personal Information

Question 2 :

Open a Microsoft Office 2007 and later DOCX file using a nominal text editor, like notepad in the Windows OS, and view its how such a file occurs in such an editor.

We utilise the same file as created above for this experiment, we open this docx file using the notepad application, and the file is viewed as follows :



```
PK└¶    ◘ Á¦!SKUVôØ    ═╕  ♂ ¶ _rels/.rels  ┼                    -'MK└A±†ïý┴CîÝ]+ˆHw{◄¡7'ú└ÅLvwhçƒLĈ
nL◄|ôU─┤¾9Ë<#:Û☼¯¶½É4ÁL=W,p,ðÞ)ÿjì─┤ñc◘lÛqQë┬¶ÔæŸFí¯Áwí@-)nÂÖF‡Ex↕ƒZìê™±&-™µ└™âu<]nYáoÀûügSÁ-ø±
ì Ï'ìN¦€Ýõ─+┤ EäÏ±l◘À]¨ß£ÇlH2s↕;Ï-XÛˆÀ◄Ëb£|-"Ò¤'ú6*œ[Tí┴À'µˆ¨>sÄ¦ØµšÁ\sæÀª-g!$Û`ŽDW#r‡-&┬ß◄áJç
¡á☼┤ ¸p™↕‰¤š┬»$ûL™¨e¢-}¦`K°%Ø↕l     ¶$ðÎ¯#ðÎÝ´îXq7> ¸Ñï5Ì~¡*Xe┤1g×Y=K`"        Lt¬ÀDdÈMWóß'ÈÇ"".N!
Ð«Õj↕«™.Š4)|3¥cð±/Êqòcƒ┤M]-">"ã™·ÙGï ð·•◘OüF<ßèÛõ┘}¬*ž¥Å³´È'"GÊM°%Ø↕l       ¶┘[,-ÏjèˉÝZ┘ÖÀ`äÖz¶ :
¶ word/styles.xml  ┼                         ÝW[o£8¶~Ÿ_xo◘U4êF"ŽÒìV-ÔÍT½Ì» 'ñÆØÈvB;¿~!`└íÜ´Òæ%>Ÿ·☼ç~í
Ô¾9nO=bER┘Ï^└®ŸÞÛáôæð☼üßž'ÄÔüÆ?ôD↕├éÝ',›Íú¾÷v.?↑âÙ\A~©¬¯ Æ¯A†É˜¾mh†Š'œ'¬EŠm²¢à2X;N<ö¨+ì;ï!þ€ŸL
:§ƒ¡Î©↕è¶ç:§çýÒ©ór¡ š¨l®*┬#-. ]¶œí‡µ°°°xÕÜO*E~o‰↑¡±=â◘`ë'"|hhÝ=äEb±?¾œRq ♂┘BN|┐{²Å¬š9U³Œ®D',°Ç;
¬¯3{┤xm…$›Ù+pL2èOòµm◄¶†ý>Tù _<÷F<íg•;ð÷Ý½%"‖R·↕'É[™ªrûãµþ^àk;<Ï œÕb8qÿC-œûSKW+┤ª=%u┬êòNzkŸìôì¶
eader1.xml  ┼                  ¥"ÍNÄ ┼Çïîû¶÷-]cŒ!m÷²ÑxV€¥´%┬†♀´Õ·-~Ç˜˜f½ð5Ìofþ└éùS7Q'Ñ)O├9Á %¤◄F
1µ·↑bÉ   œtaOŒÊ¬^♀9*)F¸XÜ£jÎJm»E`└+G,¨'uh'ÝE¤♫*    T'cx|`JÔ!ì÷¶ăn„[íš†©bû‖#j÷Èè¥◄Ñ◘Ñ┘Þ☼ë§.ŠÅ†{Œ„☼
Þ:àÂW ¨ê¬½•«WzƒœЩ¼q‡/\'.#æÍ├ëiþdÍ_·¶Ô@Ï, C          ý¨Ž:'ôß☼v¡k┐Ä'Þ_Æ           ÖÅ§š•5òÍÁ{:LêtŸQ\êÉ:
```

We can notice that the file when opened in a text editor is in a raw version and is just a bunch of random symbols which do not make any sense. The spaces in the middle are just non printable characters, and overall this is the encoded format of the file.

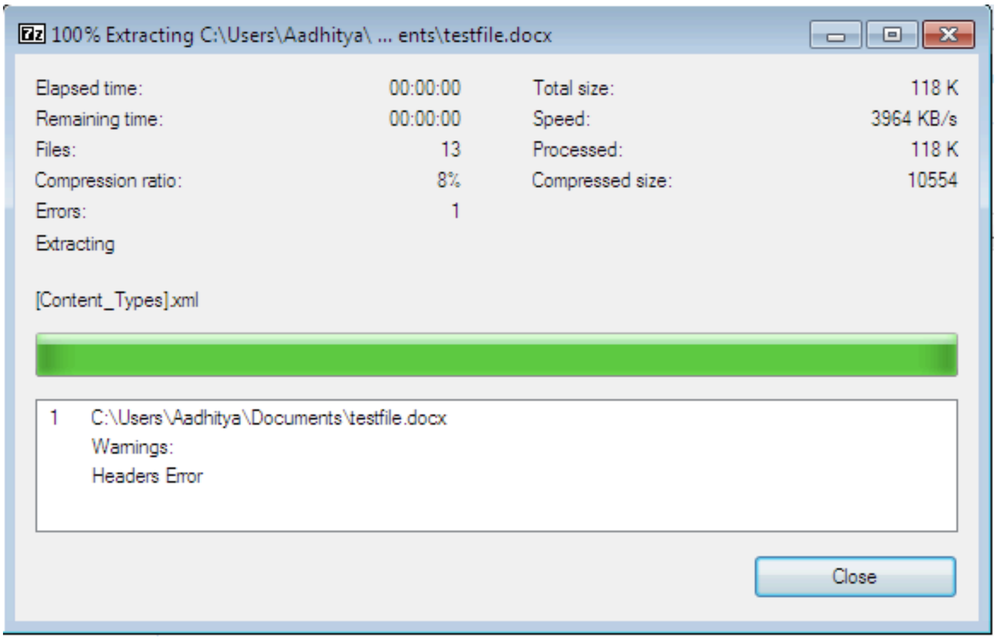
The text entered into a docx file is in a formatted and encoded version, and when this is opened using a text editor, it displays only a raw version of the file which is filled with just symbols.

With this, we can conclude that we cannot open all files using a text editor, because it would open them in an encoded format with no meaning.

Question 3 :

Open a Microsoft Office 2007 using any unzipping software, and now try to view the raw files, and notice if there is any difference in this case.

We utilise the same file as created above for this experiment, we use the 7zip unzipper software application to extract the file. The extraction process is shown below :



100% Extracting C:\Users\Aadhitya\ ... ents\testfile.docx

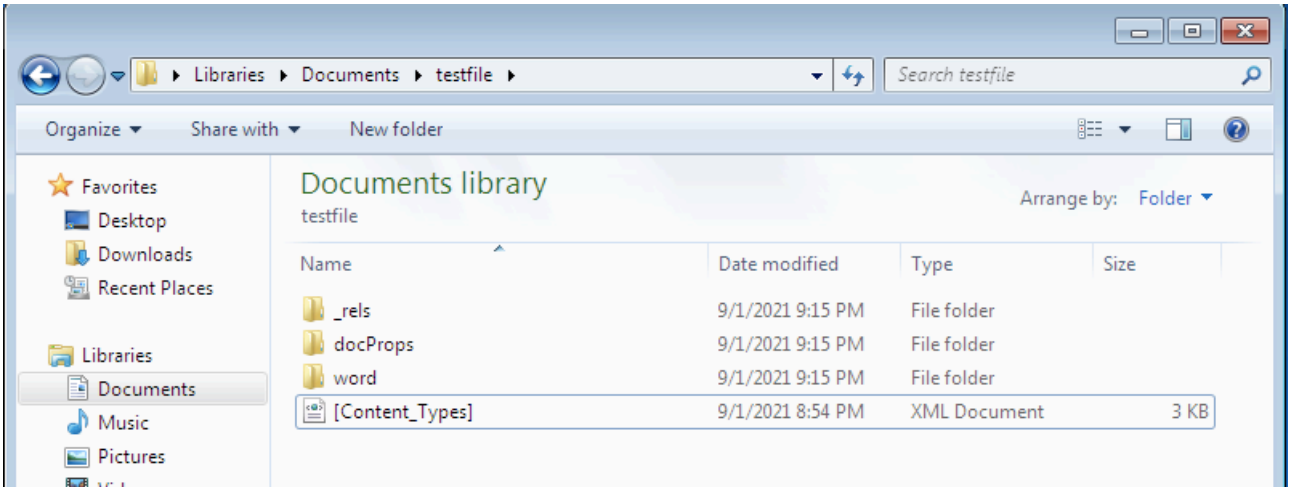
Elapsed time:	00:00:00	Total size:	118 K
Remaining time:	00:00:00	Speed:	3964 KB/s
Files:	13	Processed:	118 K
Compression ratio:	8%	Compressed size:	10554
Errors:	1		

Extracting

[Content_Types].xml

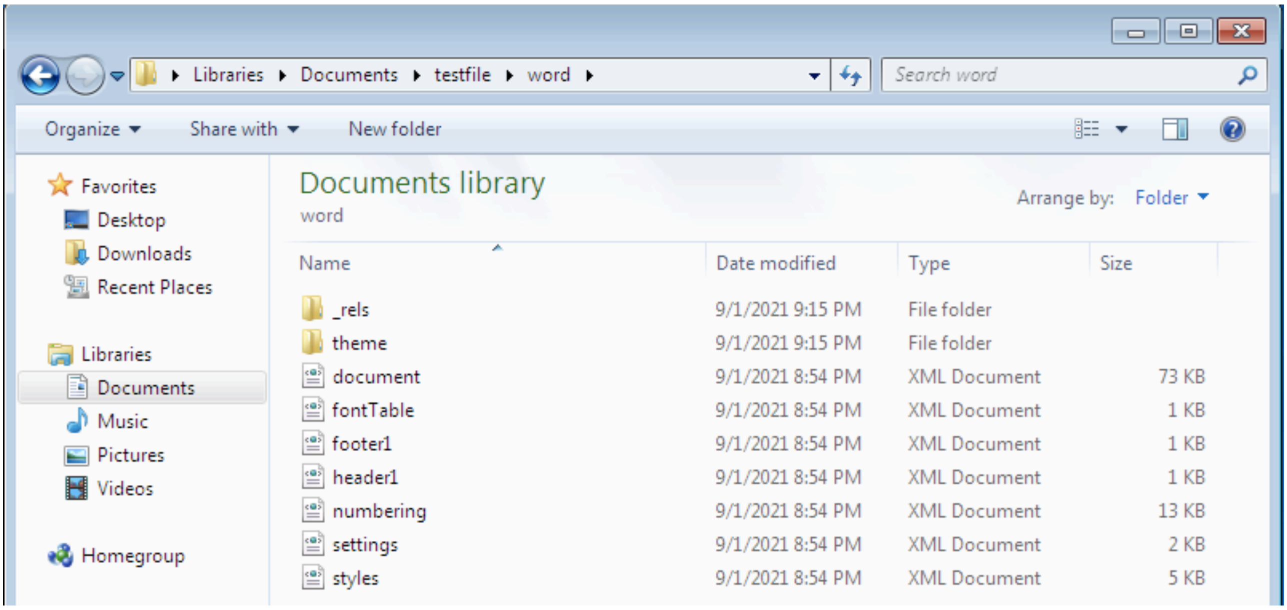
```
1   C:\Users\Aadhitya\Documents\testfile.docx
    Warnings:
    Headers Error
```

Once the file has been unzipped, we have a host of files and folders as follows :



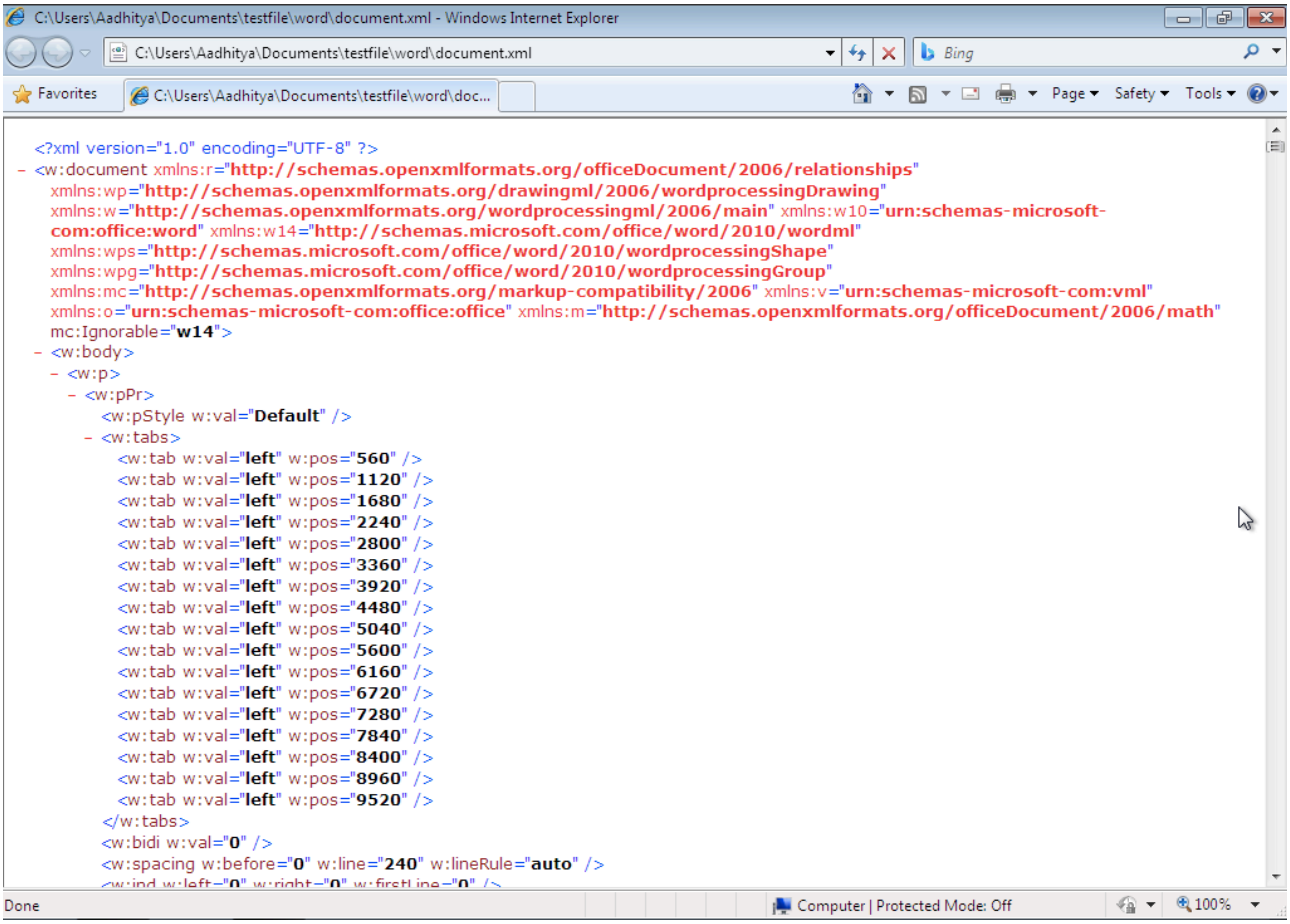
Name	Date modified	Type	Size
_rels	9/1/2021 9:15 PM	File folder	
docProps	9/1/2021 9:15 PM	File folder	
word	9/1/2021 9:15 PM	File folder	
[Content_Types]	9/1/2021 8:54 PM	XML Document	3 KB

This is how an docx file occurs with all the support files needed to display the file in a proper formatted version inside a word processing application. Let us now move into the "word" folder to open this file in a better manner than done in the previous question.



Name	Date modified	Type	Size
_rels	9/1/2021 9:15 PM	File folder	
theme	9/1/2021 9:15 PM	File folder	
document	9/1/2021 8:54 PM	XML Document	73 KB
fontTable	9/1/2021 8:54 PM	XML Document	1 KB
footer1	9/1/2021 8:54 PM	XML Document	1 KB
header1	9/1/2021 8:54 PM	XML Document	1 KB
numbering	9/1/2021 8:54 PM	XML Document	13 KB
settings	9/1/2021 8:54 PM	XML Document	2 KB
styles	9/1/2021 8:54 PM	XML Document	5 KB

In order to open a more detailed version of the document, we open the “document.xml” file found here, and this file is opened using an browser and it looks in a standard manner as follows :


C:\Users\Aadhitya\Documents\testfile\word\document.xml - Windows Internet Explorer
C:\Users\Aadhitya\Documents\testfile\word\document.xml
Bing
Favorites
C:\Users\Aadhitya\Documents\testfile\word\doc...
Page ▾
Safety ▾
Tools ▾
Done
Computer | Protected Mode: Off
100%

```
  <?xml version="1.0" encoding="UTF-8" ?>
- <w:document xmlns:r="http://schemas.openxmlformats.org/officeDocument/2006/relationships"
    xmlns:wp="http://schemas.openxmlformats.org/drawingml/2006/wordprocessingDrawing"
    xmlns:w="http://schemas.openxmlformats.org/wordprocessingml/2006/main" xmlns:w10="urn:schemas-microsoft-
    com:office:word" xmlns:w14="http://schemas.microsoft.com/office/word/2010/wordml"
    xmlns:wps="http://schemas.microsoft.com/office/word/2010/wordprocessingShape"
    xmlns:wpg="http://schemas.microsoft.com/office/word/2010/wordprocessingGroup"
    xmlns:mc="http://schemas.openxmlformats.org/markup-compatibility/2006" xmlns:v="urn:schemas-microsoft-com:vml"
    xmlns:o="urn:schemas-microsoft-com:office:office" xmlns:m="http://schemas.openxmlformats.org/officeDocument/2006/math"
    mc:Ignorable="w14">
  - <w:body>
    - <w:p>
      - <w:pPr>
          <w:pStyle w:val="Default" />
        - <w:tabs>
            <w:tab w:val="left" w:pos="560" />
            <w:tab w:val="left" w:pos="1120" />
            <w:tab w:val="left" w:pos="1680" />
            <w:tab w:val="left" w:pos="2240" />
            <w:tab w:val="left" w:pos="2800" />
            <w:tab w:val="left" w:pos="3360" />
            <w:tab w:val="left" w:pos="3920" />
            <w:tab w:val="left" w:pos="4480" />
            <w:tab w:val="left" w:pos="5040" />
            <w:tab w:val="left" w:pos="5600" />
            <w:tab w:val="left" w:pos="6160" />
            <w:tab w:val="left" w:pos="6720" />
            <w:tab w:val="left" w:pos="7280" />
            <w:tab w:val="left" w:pos="7840" />
            <w:tab w:val="left" w:pos="8400" />
            <w:tab w:val="left" w:pos="8960" />
            <w:tab w:val="left" w:pos="9520" />
          </w:tabs>
          <w:bidi w:val="0" />
          <w:spacing w:before="0" w:line="240" w:lineRule="auto" />
          <w:ind w:left="0" w:right="0" w:firstLine="0" />
```

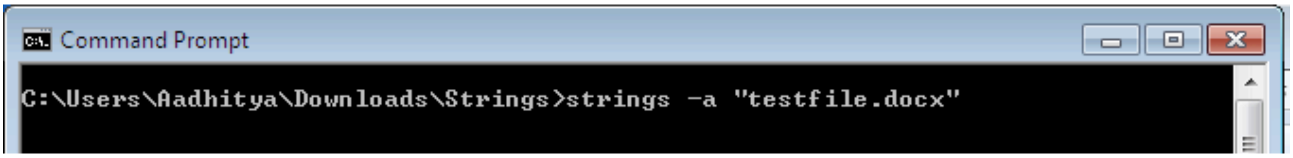
Question 4 :

Use the "strings" utility available in the Microsoft web site to scan the file you pass it for UNICODE (or ASCII) strings of a default length of 3 or more UNICODE (or ASCII) characters.

We utilise the same file as created above for this experiment, we download the strings library from the link :

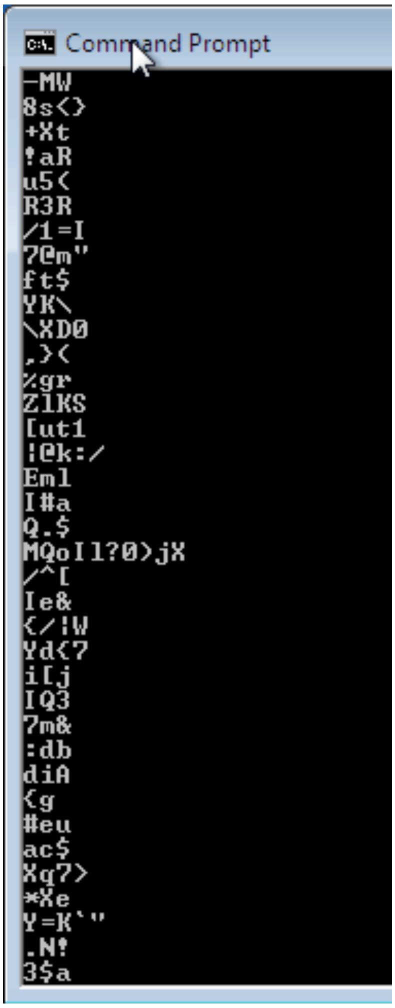
https://docs.microsoft.com/en-us/sysinternals/downloads/strings

and run the command with the terminal opened in that folder and note that the docx file is also placed in the same folder for convenience.

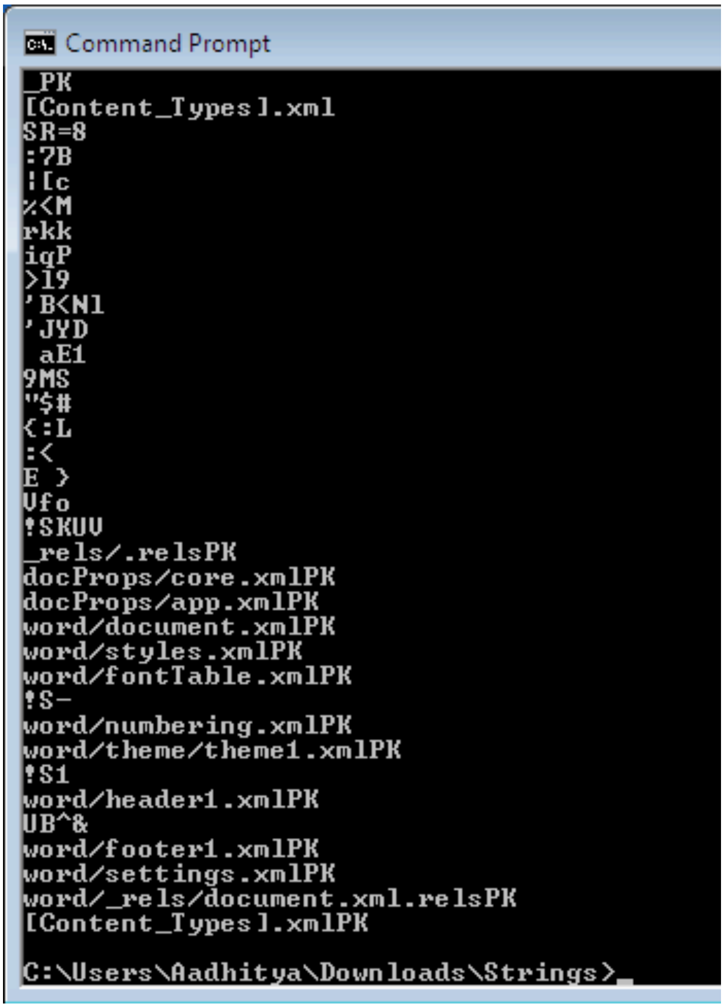


```
C:\Users\Aadhitya\Downloads\Strings>strings -a "testfile.docx"
```

When the command is entered, it searches through the complete file and returns the matched instances. A few instances are listed below :



```
-MW
8s<>
+Xt
!aR
u5<
R3R
/1=I
7@m"
ft$
YK\
\XD0
,><
%gr
Z1KS
[ut1
!@k:/
Eml
I#a
Q.$
MQoIl?0>jX
/^[
Ie&
</!W
Yd<7
i[j
IQ3
7m&
:db
diA
<g
#eu
ac$
Xq7>
*Xe
Y=K`"
.N!
3$a
```



```
_PK
[Content_Types].xml
SR=8
:7B
![c
%<M
rkk
iqP
>l9
'B<Nl
'JYD
 aE1
9MS
"$#
<:L
:<
E >
Ufo
!SKUV
_rels/.relsPK
docProps/core.xmlPK
docProps/app.xmlPK
word/document.xmlPK
word/styles.xmlPK
word/fontTable.xmlPK
!S-
word/numbering.xmlPK
word/theme/theme1.xmlPK
!S1
word/header1.xmlPK
UB^&
word/footer1.xmlPK
word/settings.xmlPK
word/_rels/document.xml.relsPK
[Content_Types].xmlPK

C:\Users\Aadhitya\Downloads\Strings>_
```

Question 5 :

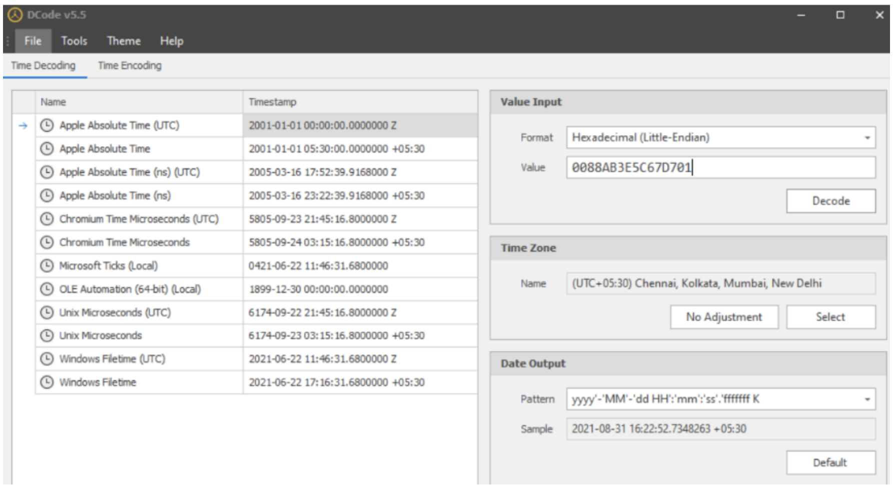
Use the "DCode" forensic tool to encode and decode the dates in which the chosen files were modified. Use the above tool to see if you can say something about the revision history of MS Word documents.

We utilise the same file as created above for this experiment, we download the strings library from the link :

https://www.digital-detective.net/dcode/

and run this application after installing it in a windows os computer.

We then use the date in which file used above was created, and then perform encoding to get an encoded hash string of the date, we then feed in the same string to the decoder and verify if the final date obtained matches with the initially taken date.

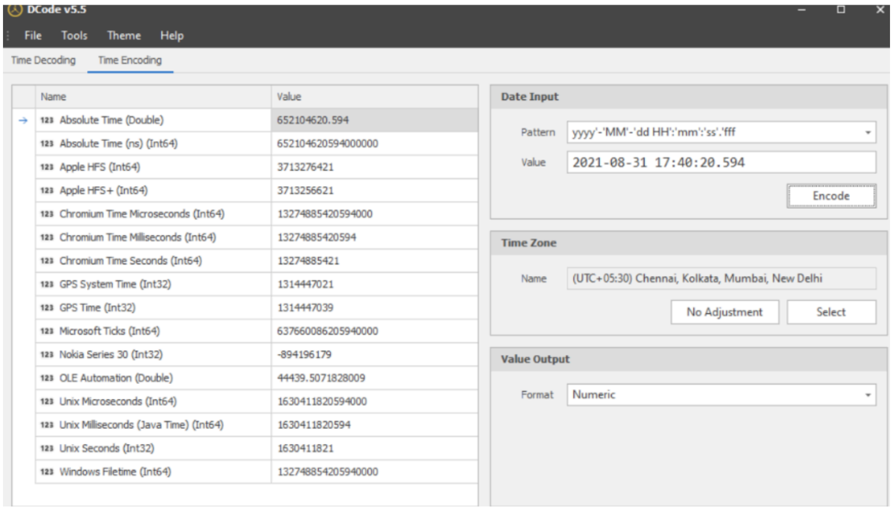


Name	Timestamp
Apple Absolute Time (UTC)	2001-01-01 00:00:00.0000000 Z
Apple Absolute Time	2001-01-01 05:30:00.0000000 +05:30
Apple Absolute Time (ns) (UTC)	2005-03-16 17:52:39.9168000 Z
Apple Absolute Time (ns)	2005-03-16 23:22:39.9168000 +05:30
Chromium Time Microseconds (UTC)	5805-09-23 21:45:16.8000000 Z
Chromium Time Microseconds	5805-09-24 03:15:16.8000000 +05:30
Microsoft Ticks (Local)	0421-06-22 11:46:31.6800000
OLE Automation (64-bit) (Local)	1899-12-30 00:00:00.0000000
Unix Microseconds (UTC)	6174-09-22 21:45:16.8000000 Z
Unix Microseconds	6174-09-23 03:15:16.8000000 +05:30
Windows Filetime (UTC)	2021-06-22 11:46:31.6800000 Z
Windows Filetime	2021-06-22 17:16:31.6800000 +05:30

Value Input
Format: Hexadecimal (Little-Endian)
Value: 0088AB3E5C67D701

Time Zone
Name: (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi

Date Output
Pattern: yyyy'-'MM'-'dd HH':'mm':'ss'.'fffffff K
Sample: 2021-08-31 16:22:52.7348263 +05:30



Name	Value
Absolute Time (Double)	652104620.594
Absolute Time (ns) (Int64)	652104620594000000
Apple HFS (Int64)	3713276421
Apple HFS+ (Int64)	3713256621
Chromium Time Microseconds (Int64)	13274885420594000
Chromium Time Milliseconds (Int64)	13274885420594
Chromium Time Seconds (Int64)	13274885421
GPS System Time (Int32)	1314447021
GPS Time (Int32)	1314447039
Microsoft Ticks (Int64)	637660086205940000
Nokia Series 30 (Int32)	-894196179
OLE Automation (Double)	44439.5071828009
Unix Microseconds (Int64)	1630411820594000
Unix Milliseconds (Java Time) (Int64)	1630411820594
Unix Seconds (Int32)	1630411821
Windows Filetime (Int64)	132748854205940000

Date Input
Pattern: yyyy'-'MM'-'dd HH':'mm':'ss'.'fff
Value: 2021-08-31 17:40:20.594

Time Zone
Name: (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi

Value Output
Format: Numeric

We can notice that the dates are processed correctly in both cases, and thus the encoding and decoding process of dates has been verified.

CONCLUSION

In this lab experiments, we have dealt with and seen the properties of word documents (DOCX) files, like viewing it under different circumstances, using different tools and also performing date encoding and decoding which provide useful functionalities for efficient and ease of forensic analysis.