

Name: Ashish Das

Reg. No.: 19BCE1160

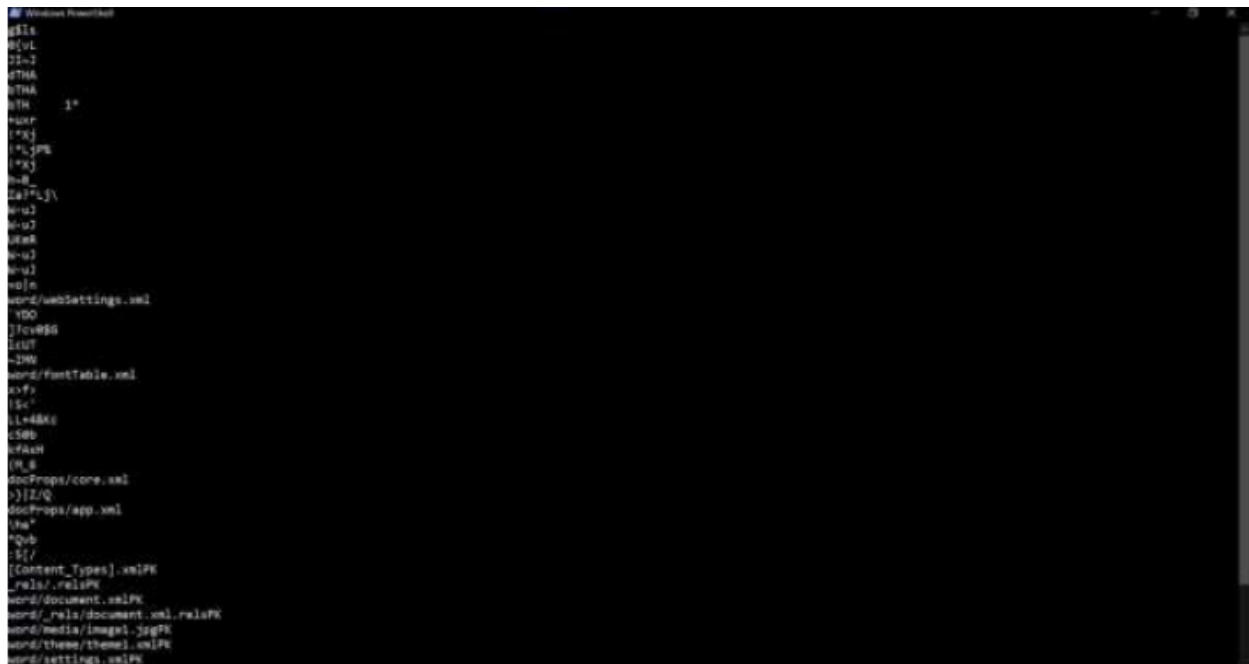
Faculty: Nagraj S. V.

1. Note: DOCX is the file format for Microsoft Office 2007 and later. DOCX should not be confused with DOC, the format used by earlier versions of Microsoft Office.

It is possible to say something about the revision history of MS Word documents using forensic tools.

- a) The Strings utility is available from the following Web site
<https://docs.microsoft.com/en-us/sysinternals/downloads/strings>

Strings just scans the file you pass it for UNICODE (or ASCII) strings of a default length of 3 or more UNICODE (or ASCII) characters



```
gila
0x01
21-2
0THA
0THA
0TH 1*
ruxr
"0j
"0jPK
"0j
0j
0j7Lj\
0u1
0u2
0es
0-u1
0-u1
0u)n
word/webSettings.xml
YDO
}f0v000
iOUT
-200
word/fontTable.xml
0x01
1x0
11-4800
0500
0fAch
0L8
docProps/core.xml
0}IZ/Q
docProps/app.xml
0wa
"Qvb
0{
[Content_Types].xmlPK
_r/01/.rel0PK
word/document.xmlPK
word/_rels/document.xml.relaPK
word/media/image1.jpgPK
word/theme/theme1.xmlPK
word/settings.xmlPK
```

- b) DCode is a forensic tool (currently available free) at the following Web site:
<https://www.digital-detective.net/dcode/>

This utility was designed to calculate date/time values from the various timestamps that may be found inside data files. During a forensic examination,

you may need to decode a date or verify the date provided to you by forensic software. This is where the utility helps. The tool can take an integer or hex value and convert it into a date and time in a variety of formats. It is a helpful tool for verifying the accuracy of forensic tools.

Use the above tools to see if you can say something about the revision history of MS Word documents.

The screenshot shows the DCode v5.5 application window. It has a menu bar with 'File', 'Tools', 'Theme', and 'Help'. Below the menu bar are two tabs: 'Time Decoding' (selected) and 'Time Encoding'. The main area is divided into three sections: a table of time formats, a 'Value Input' section, and a 'Time Zone' section. The table lists various time formats and their corresponding timestamps. The 'Value Input' section has a 'Format' dropdown set to 'Numeric' and a 'Value' input field containing '58'. The 'Time Zone' section has a 'Name' input field containing '(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi' and two buttons: 'No Adjustment' and 'Select'. The 'Date Output' section has a 'Pattern' dropdown set to 'yyyy'-MM'-dd HH':'mm':'ss'.ffffff K' and a 'Sample' input field containing '2021-08-29 18:00:37.2610313 +05:30'. A 'Default' button is also present.

Name	Timestamp
Apple Absolute Time (UTC)	2001-01-01 00:00:58.0000000 Z
Apple Absolute Time	2001-01-01 05:30:58.0000000 +05:30
Apple Absolute Time (ns) (UTC)	2001-01-01 00:00:00.0000001 Z
Apple Absolute Time (ns)	2001-01-01 05:30:00.0000001 +05:30
Apple HFS (Local)	1904-01-01 00:00:58.0000000
Apple HFS+ (UTC)	1904-01-01 00:00:58.0000000 Z
Apple HFS+	1904-01-01 05:30:58.0000000 +05:30
Chromium Time Microseconds (UTC)	1601-01-01 00:00:00.0000580 Z
Chromium Time Microseconds	1601-01-01 05:30:00.0000580 +05:30
Chromium Time Milliseconds (UTC)	1601-01-01 00:00:00.0580000 Z
Chromium Time Milliseconds	1601-01-01 05:30:00.0580000 +05:30
Chromium Time Seconds (UTC)	1601-01-01 00:00:58.0000000 Z
Chromium Time Seconds	1601-01-01 05:30:58.0000000 +05:30
GPS System Time	1980-01-06 00:00:58.0000000
GPS Time (UTC)	1980-01-06 00:00:58.0000000 Z
GPS Time	1980-01-06 05:30:58.0000000 +05:30
Microsoft Ticks (Local)	0001-01-01 00:00:00.0000058

Value Input

Format: Numeric

Value: 58

Decode

Time Zone

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

No Adjustment Select

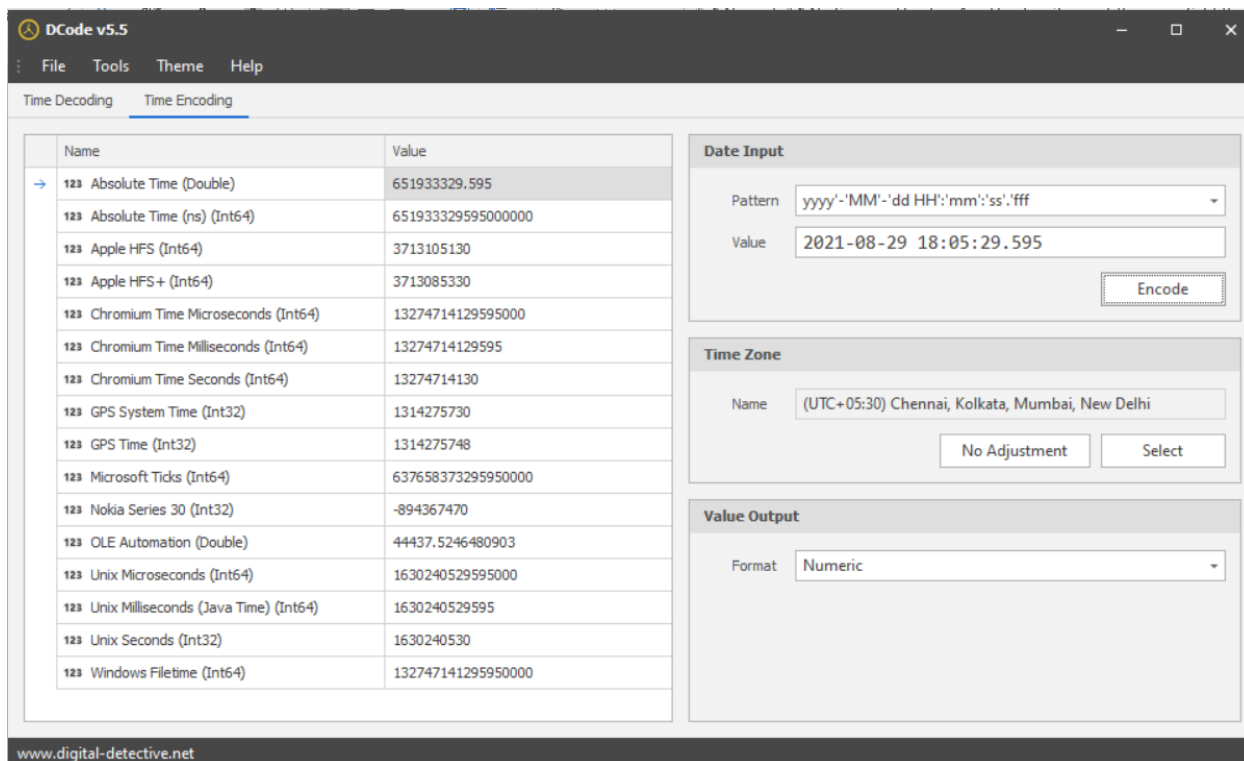
Date Output

Pattern: yyyy'-MM'-dd HH':'mm':'ss'.ffffff K

Sample: 2021-08-29 18:00:37.2610313 +05:30

Default

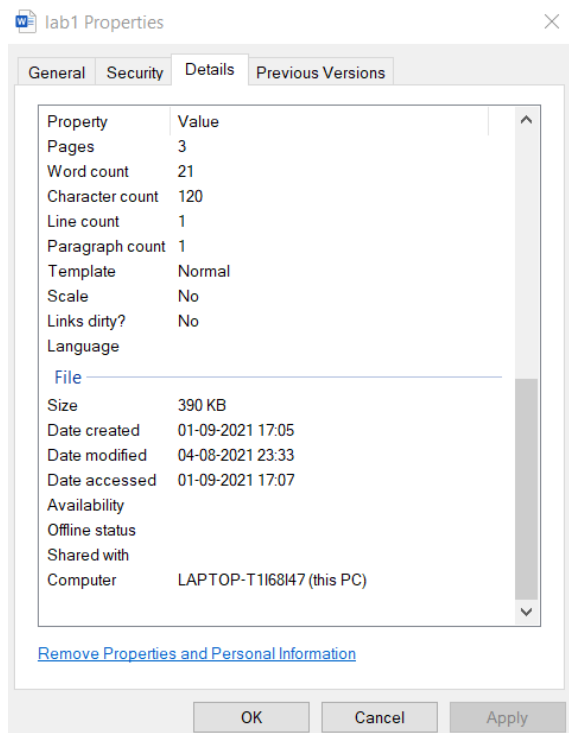
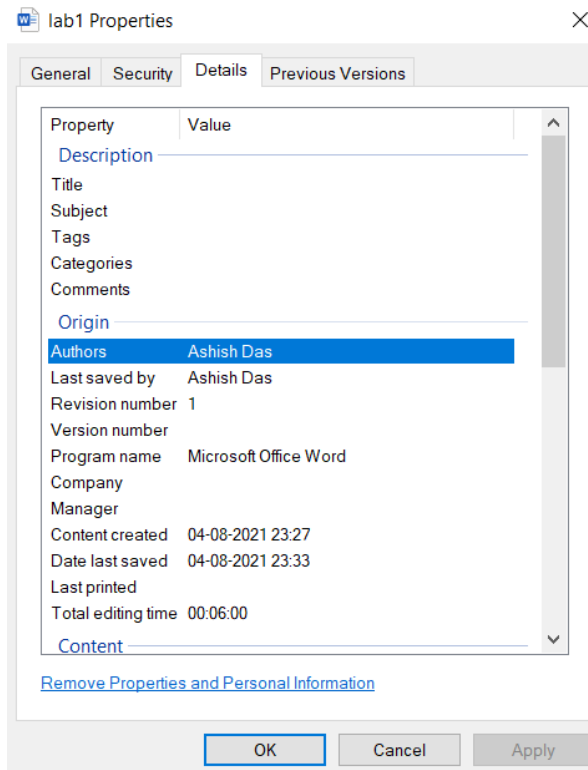
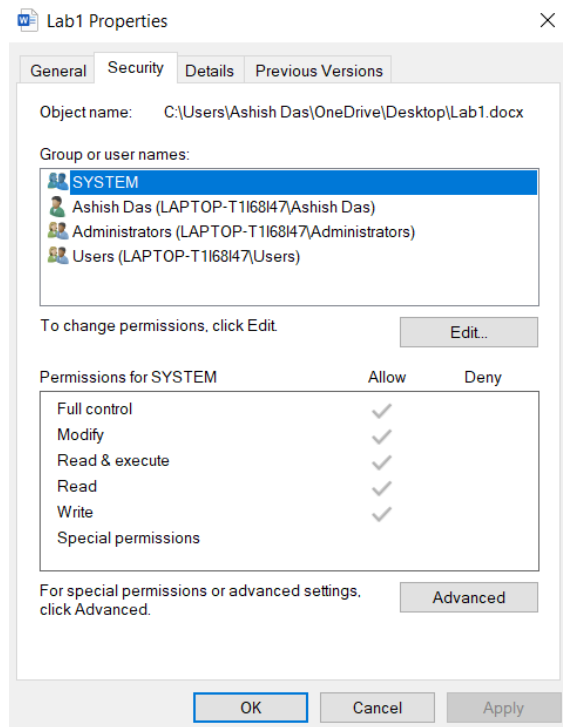
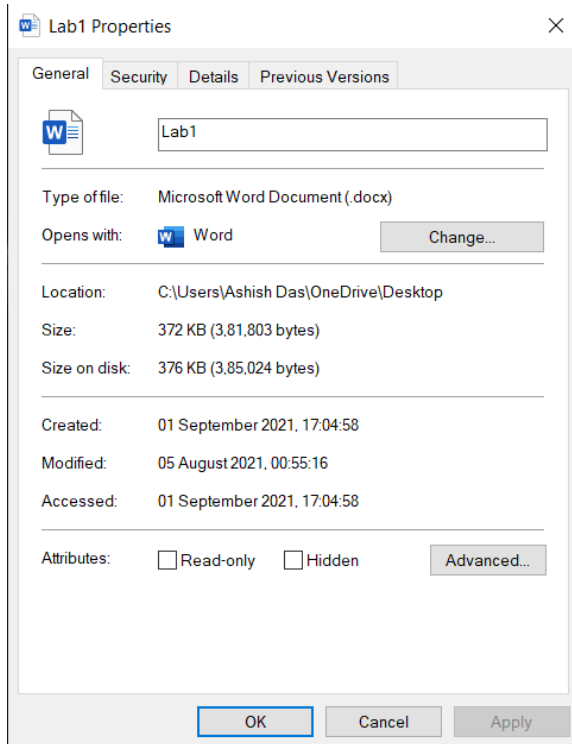
www.digital-detective.net



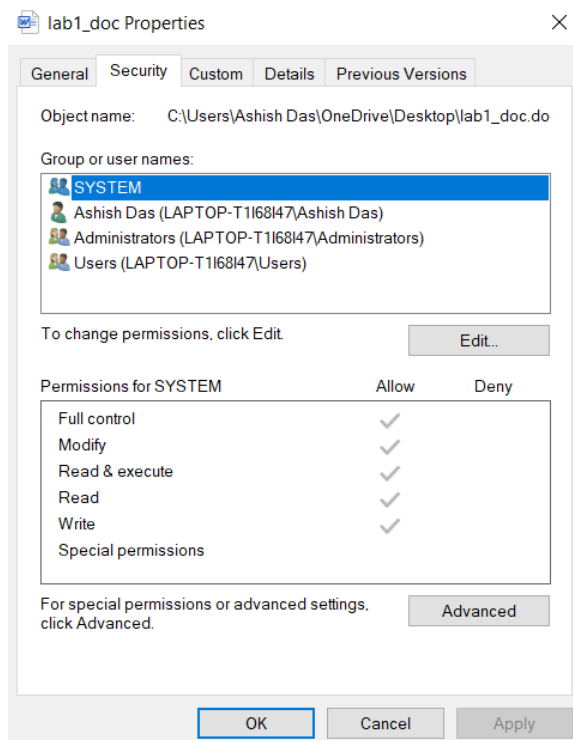
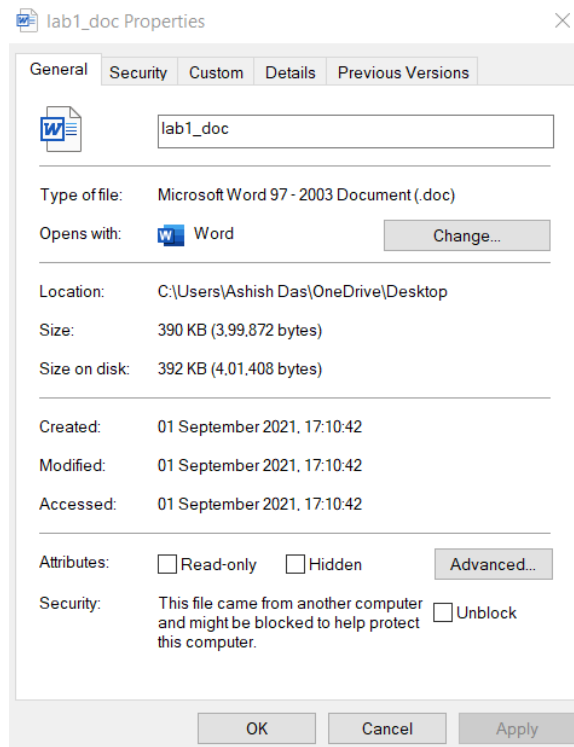
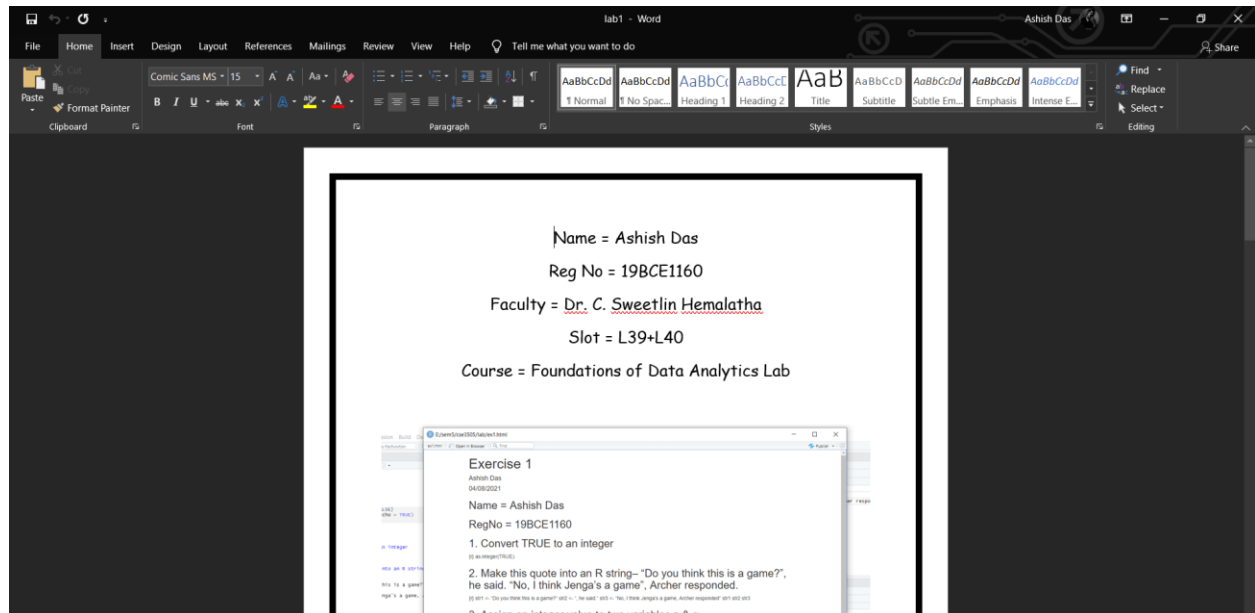
- Have you ever tried to open a Word Docx file in notepad? If so, then you know that you get a screen full of unintelligible characters. All you need to do is run the Docx file through an unzip program and you can see several files and folders full of XML data. The files can now be opened in Notepad, but if you just double click on them, they will open in your Web browser and be a bit more readable. Browse through the newly created folders and you will find plenty of formatting information and the complete text of the document. You will also find information that could be very useful for forensics including files revision, creation and modify dates, document creator and who was the last one to modify the document.

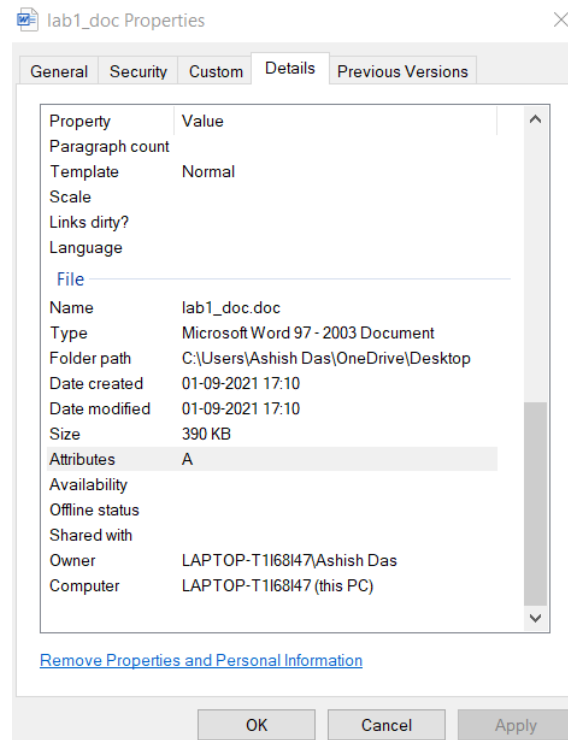
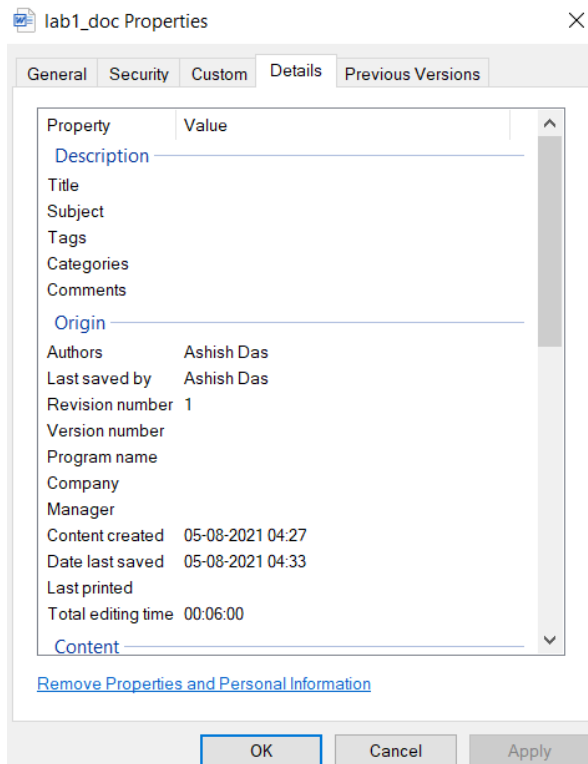
Investigate doc and docx files and include screenshots in your submission.

Docx:

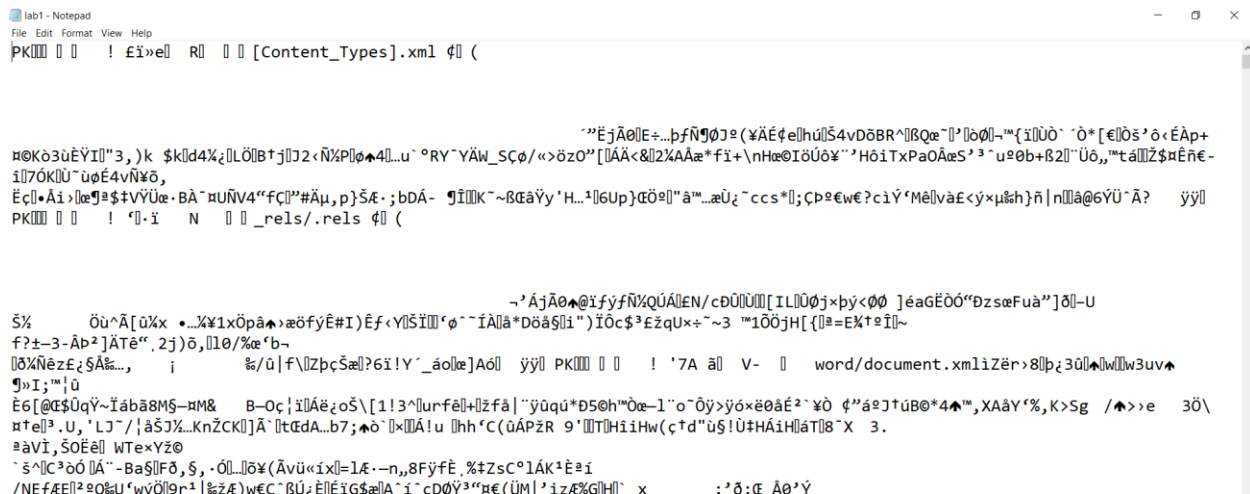


Doc:

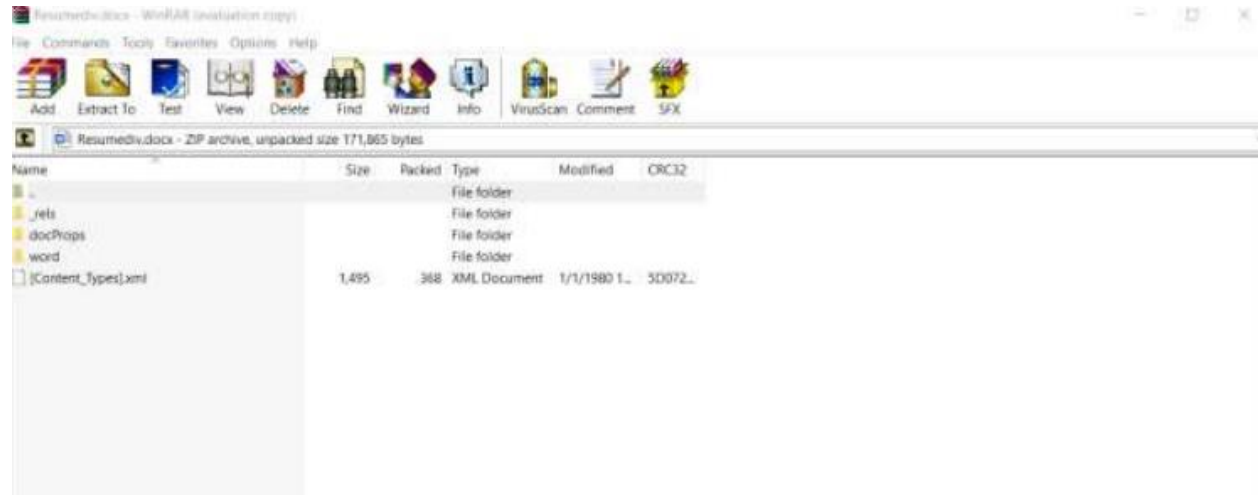




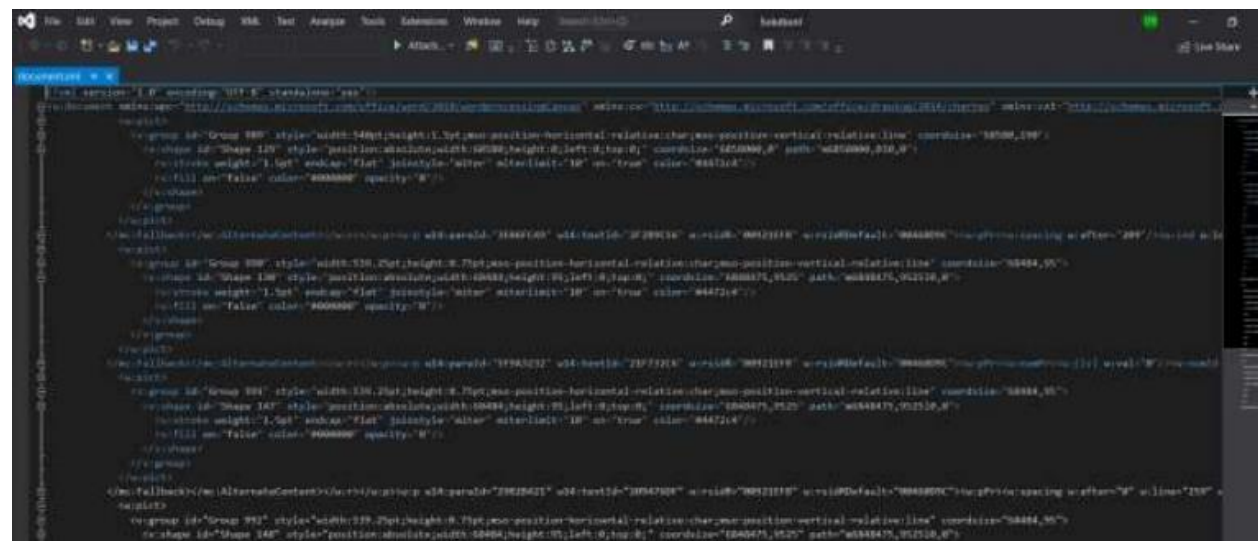
Word doc opened with notepad:



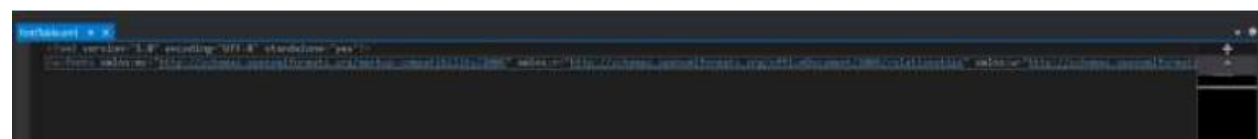
After extracting:



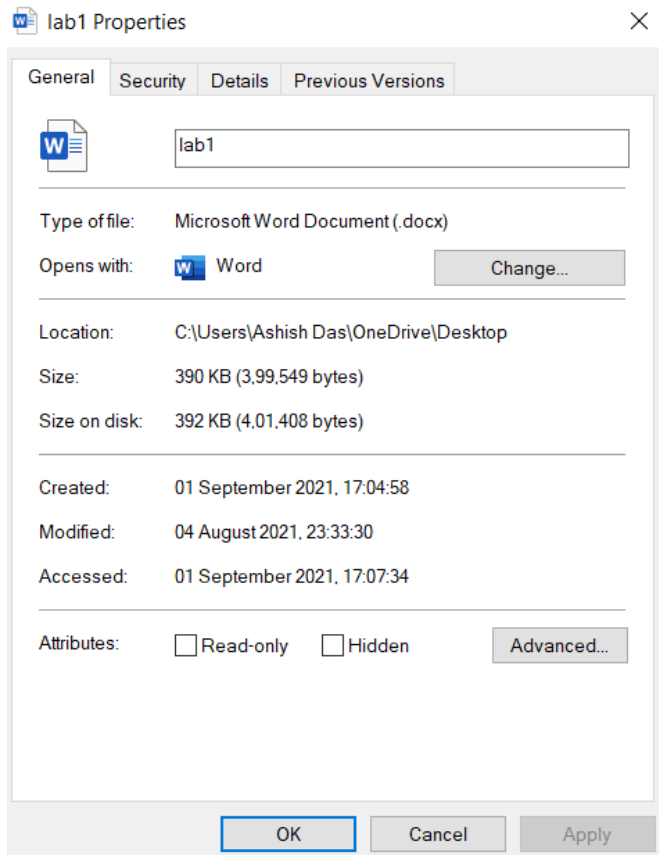
Document.xml:



Font_tables.xml:



Creation time and size of the file:



app.xml:

```
<?xml version='1.0' encoding='UTF-8' standalone='yes'?>
<Properties xmlns='http://schemas.microsoft.com/office/documentformat/2006/extended-properties' xmlns:c='http://schemas.microsoft.com/office/docprop/2009/docprops/types'>
  <TemplateNormal.dotm/Template>
    <TotalLines/TotalLines>
      <Pages/1/Pages>
        <Words/155/Words>
          <Characters/805/Characters>
            <Application/Microsoft Office Word/Application>
              <DocSecurity/0/DocSecurity>
                <Lines/1/Lines><Paragraphs/2/Paragraphs>
                  <ScaleCrop/false/ScaleCrop>
                    <Image/Company/IsDirty/false/LinkIsDirty/CharacterWithSpace/800/CharacterWithSpace/ShareDoc/false/ShareDoc>
                      <HyperlinkChanged/false/HyperlinkChanged/AppVersion/16.0000/AppVersion/Properties>
```