**DIGITAL FORENSICS LAB**

|  |  |
| --- | --- |
| Exercise 4 | |
| Name | S Shyam Sundaram |
| Registration Number | 19BCE1560 |
| Slot | L39+L40 |
| Faculty | Dr. Seshu Babu Pulgara |
| Date | 31st August, 2021 |

**AIM**

To investigate MS Word documents.

**PART 1**

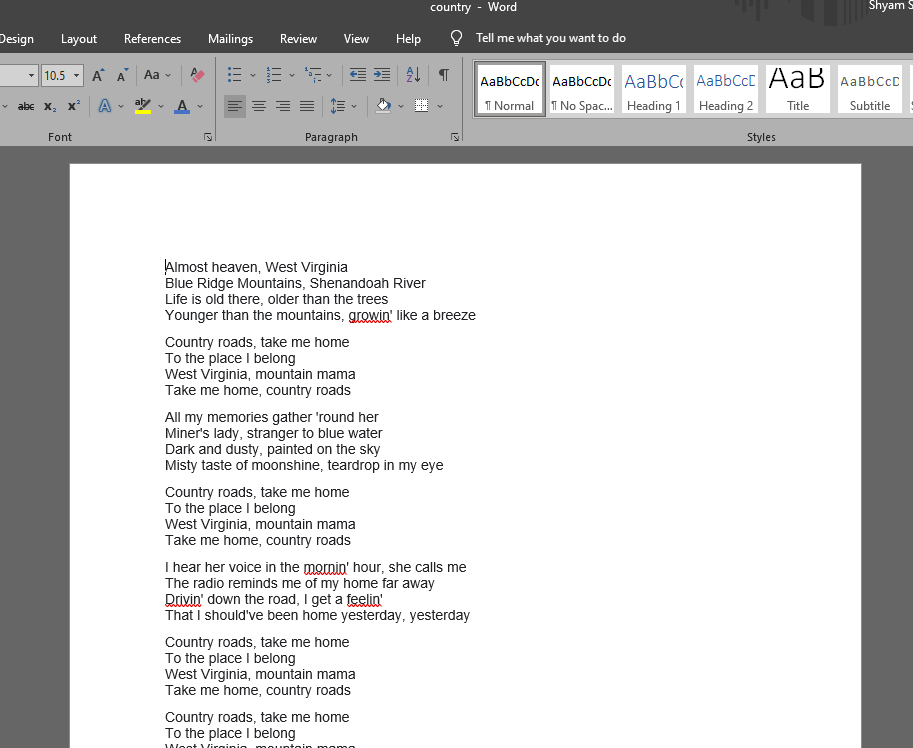
**STRINGS**

Strings just scans the file passed to it for UNICODE or ASCII strings of a default length of 3 or more characters.

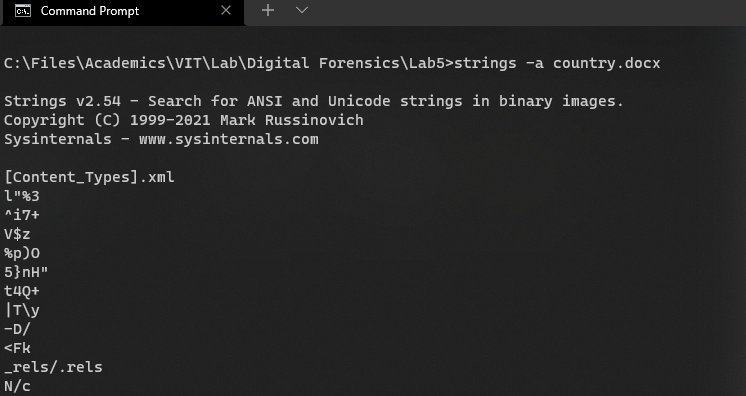
**STEPS**

1. Install strings and extract to a path.
2. Add the path to environment variable ‘PATH’.
3. Open the command prompt and start working.

**DOCUMENT USED**

****

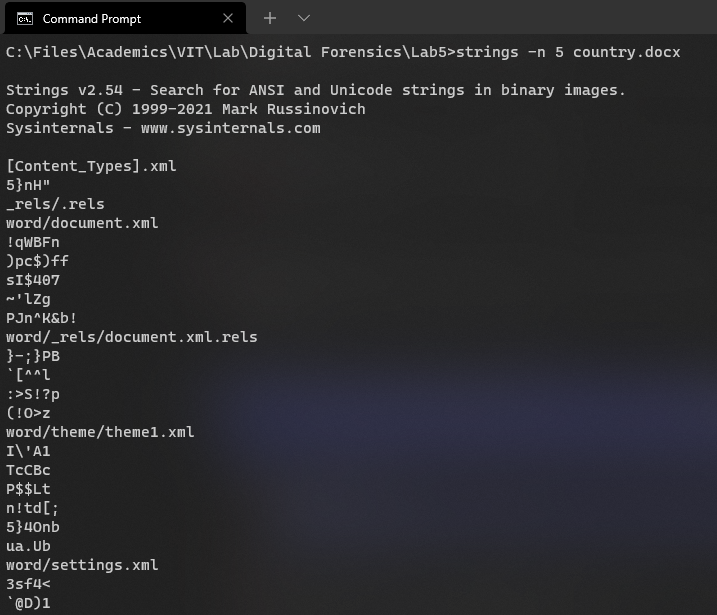
**ASCII only search**



**OBSERVATION**

This gives a list of three-character long ASCII strings, which is the default length.

**Search for strings that are at least 5 characters long**



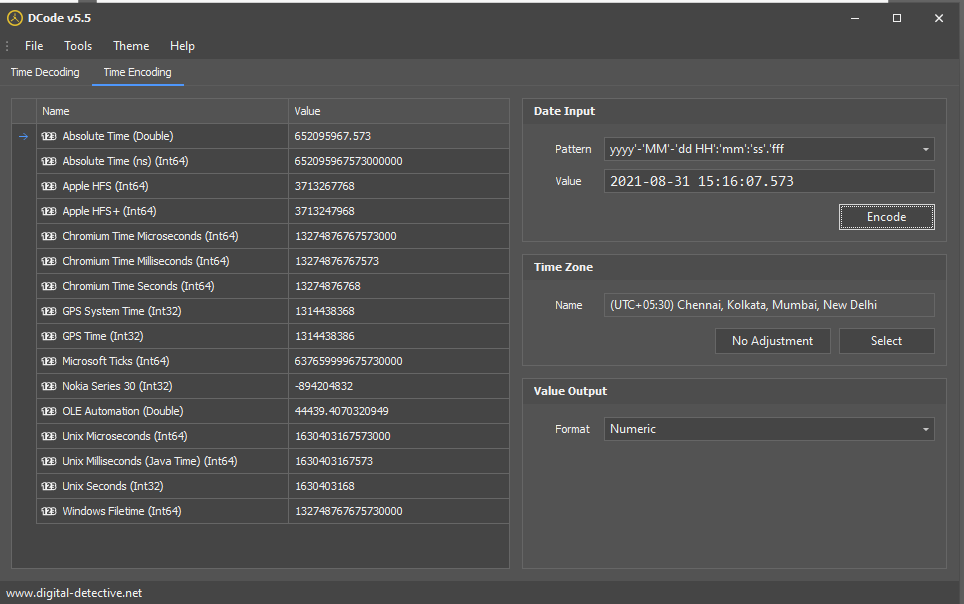
**OBSERVATION**

The -n 5 tells the tool to search for strings that are at least 5 characters long.

**DCODE**

Dcode is a utility designed to calculate date/time values from various timestamps that are found in a data file. It takes an input and gives out the decoded/encoded values.

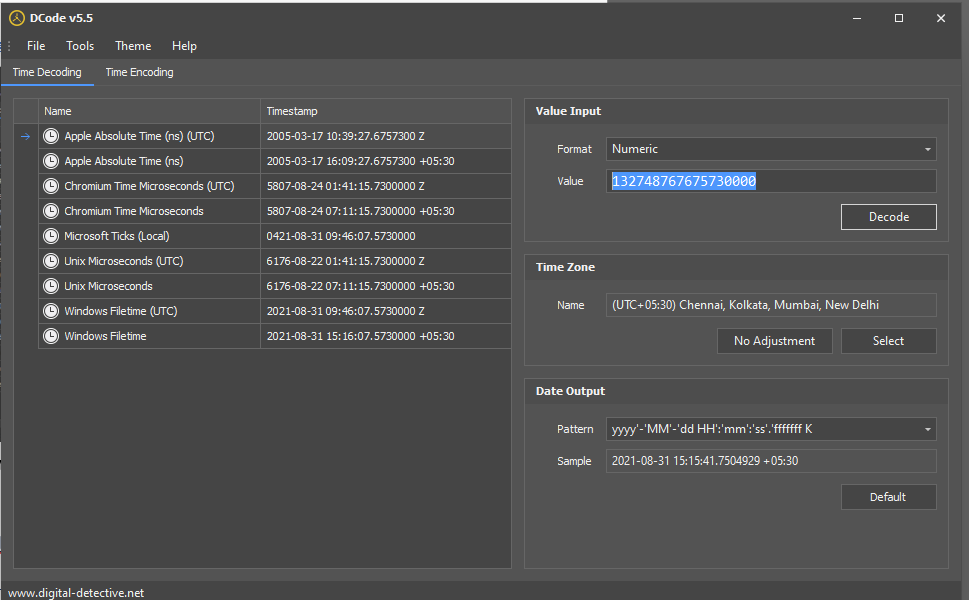
**Encode a date given in readable form**



**OBSERVATION**

We enter the date and time to encode in the Date Input dialog box, along with the pattern. Then, we click ‘Encode’ and get the list of encoded values on the left.

**Decodes a value given into readable timestamp**

****

**OBSERVATION**

We enter the value obtained in the ‘Windows File Time’ row of the encode section and enter here. Upon doing so, we get back nearly the same date and time in the Windows Filetime row.

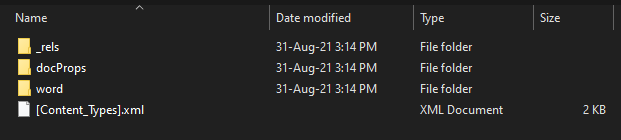
**PART 2**

DOCX contains a bunch of XML files that describes the document, has some settings, themes and even the content itself. In this section, we explore them.

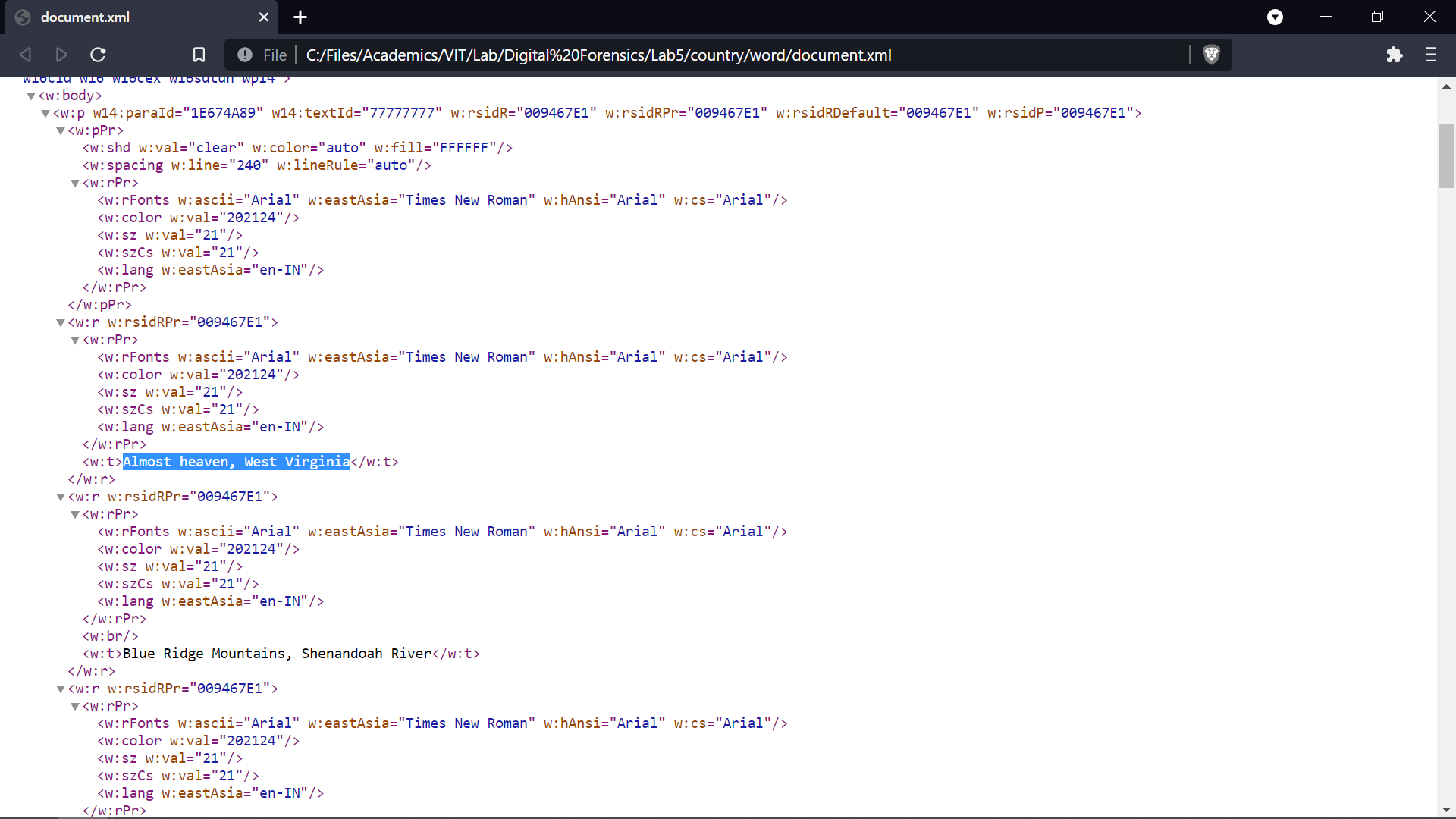
**STEPS**

1. Open WinRAR or WinZip.
2. Open the docx file and click ‘Extract’ to obtain the XML files.
3. All XML files can be seen in the folder.

List of files extracted from country.docx.



**WORD/DOCUMENT.XML**



**OBSERVATION**

We see each line of the document within a <w:t> tag. They are also nested in tags that contain formatting information like font, size and color.

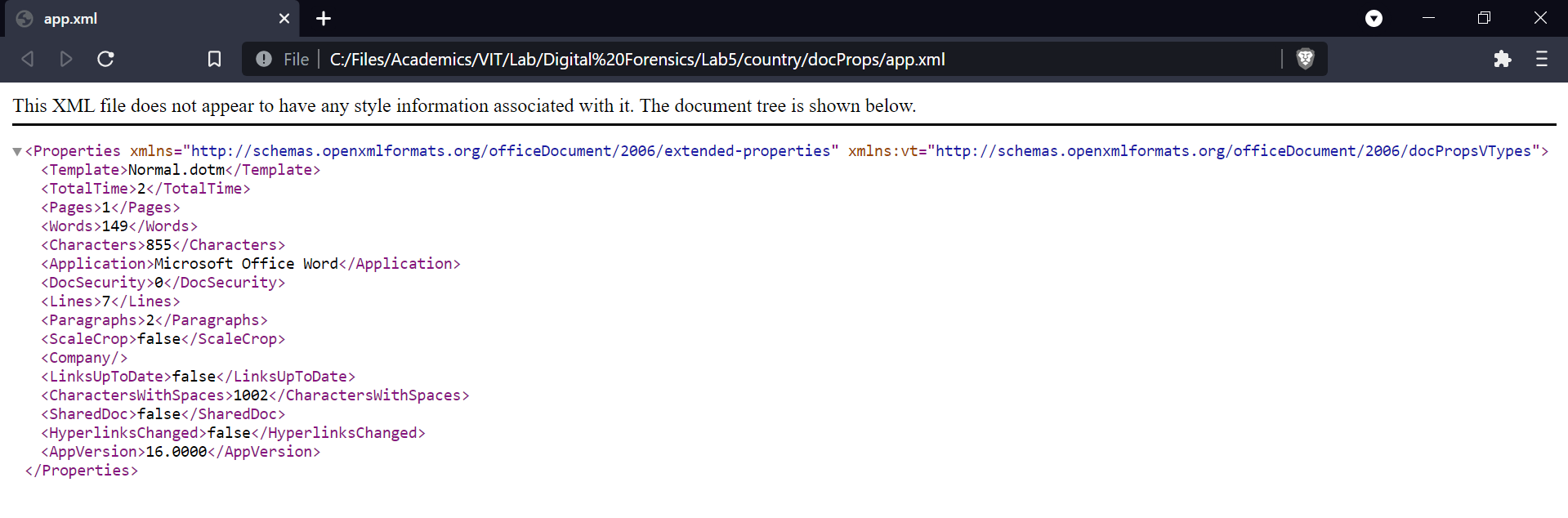
**DOCPROPS/CORE.XML**



**OBSERVATION**

We see details such as who created the document (Shyam Sundaram), who modified it last (Shyam Sundaram), when it was created and modified (in the <dcterms:created> and <dcterms:modified> tags) and also how many times the file was edited or revised (3 times, as shown by the <cp:revision> tag).

**DOCPROPS/APP.XML**



**OBSERVATION**

This XML file contains details such as the template the document follows, how many pages, characters and words it contains.

**CONCLUSION**

We have thus applied file forensics on a DOCX file and fetched details from its XML files such as revision count, author, date and time of modifications etc.