# DIGITAL FORENSICS LAB

| Exercise 3 | |
|---|---|
| Name | S Shyam Sundaram |
| Registration Number | 19BCE1560 |
| Slot | L39+L40 |
| Faculty | Dr. Seshu Babu Pulgara |
| Date | 24th August, 2021 |

## AIM

Working with Windows Event Viewer and the Event Log Explorer tool to find security related events.

## EVENT VIEWER

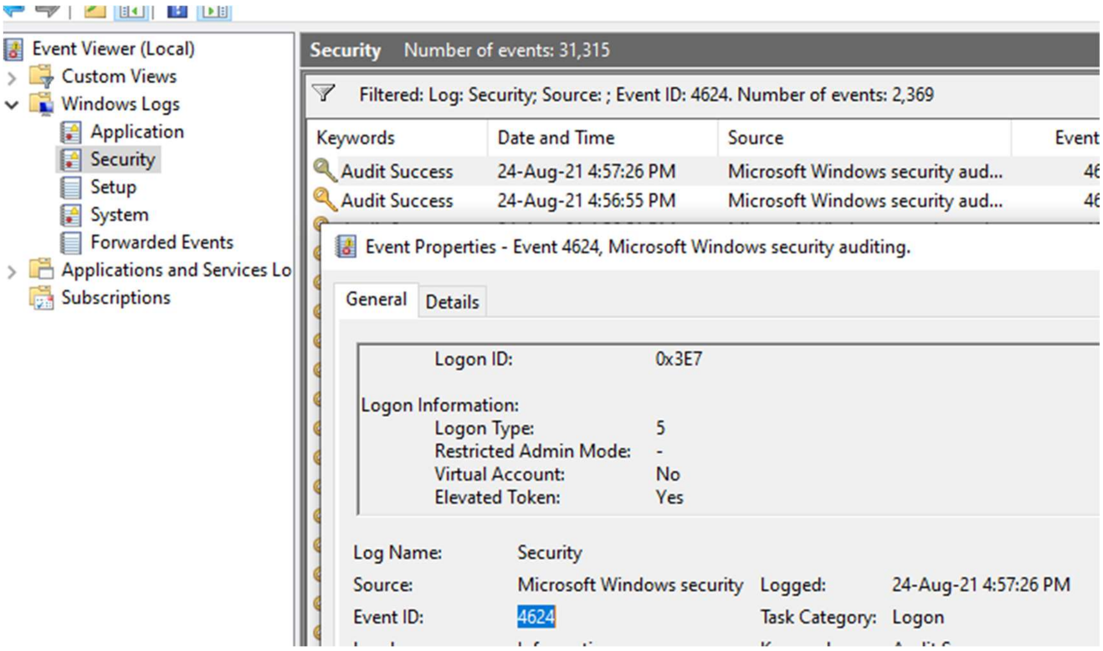
This is a tool built into Windows Operating Systems to let administrators and users view event logs on a machine. We use this to find security events such as logon, logoff using Event IDs.

To find an Event by its ID, click on the 'Find' option under the 'Actions' pane on the right. Then enter the Event id that needs to be found.

### STEPS

1. Open Event Viewer
2. Go to Windows Logs>Security
3. Select 'Filter Current Log' in the pane on the right side.
4. Enter the Event ID needed and click 'Ok'.

## LOGON (Event ID – 4624)



Security Number of events: 31,315

Filtered: Log: Security; Source: ; Event ID: 4624. Number of events: 2,369

| Keywords | Date and Time | Source | Event |
|---|---|---|---|
| Audit Success | 24-Aug-21 4:57:26 PM | Microsoft Windows security aud... | 46 |
| Audit Success | 24-Aug-21 4:56:55 PM | Microsoft Windows security aud... | 46 |

Event Properties - Event 4624, Microsoft Windows security auditing.

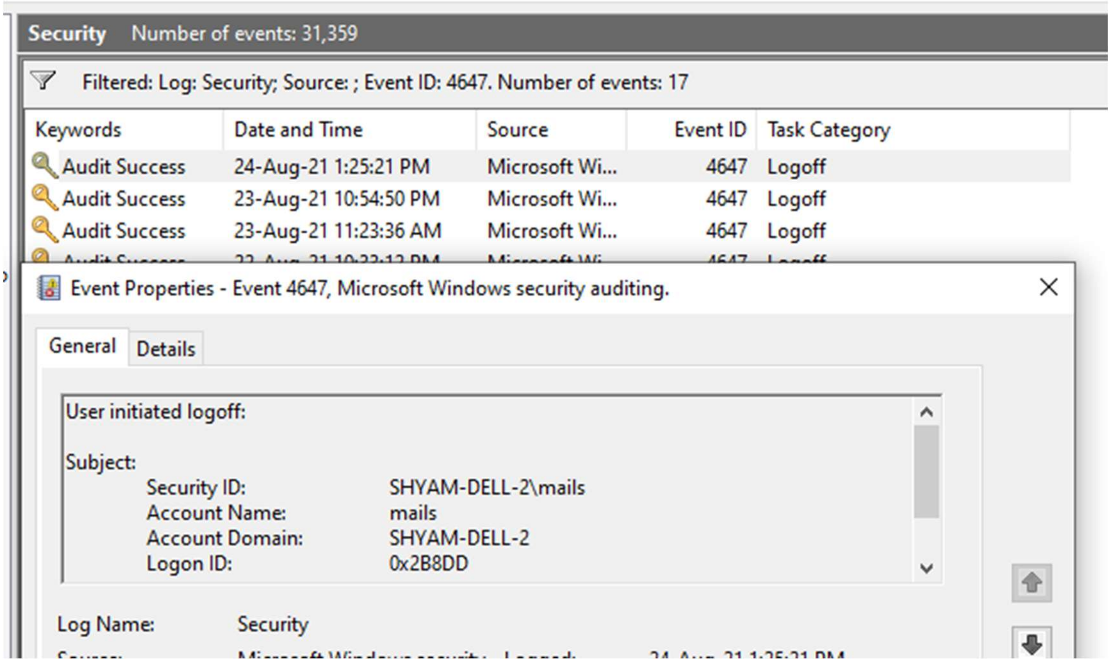
```
        Logon ID:               0x3E7

Logon Information:
        Logon Type:             5
        Restricted Admin Mode:  -
        Virtual Account:        No
        Elevated Token:         Yes
```

Log Name: Security
Source: Microsoft Windows security    Logged: 24-Aug-21 4:57:26 PM
Event ID: 4624    Task Category: Logon

### OBSERVATION

This event documents each and every successful attempt to logon to the local computer for all types of logons. Logon type 7 shown in the screenshot above is used to indicate 'Unlock', i.e., password protected screen saver was shown as it was unattended. We see that this event has happened 2376 times.

## LOGOFF (Event ID – 4647)



Security Number of events: 31,359

Filtered: Log: Security; Source: ; Event ID: 4647. Number of events: 17

| Keywords | Date and Time | Source | Event ID | Task Category |
|---|---|---|---|---|
| Audit Success | 24-Aug-21 1:25:21 PM | Microsoft Wi... | 4647 | Logoff |
| Audit Success | 23-Aug-21 10:54:50 PM | Microsoft Wi... | 4647 | Logoff |
| Audit Success | 23-Aug-21 11:23:36 AM | Microsoft Wi... | 4647 | Logoff |

Event Properties - Event 4647, Microsoft Windows security auditing.

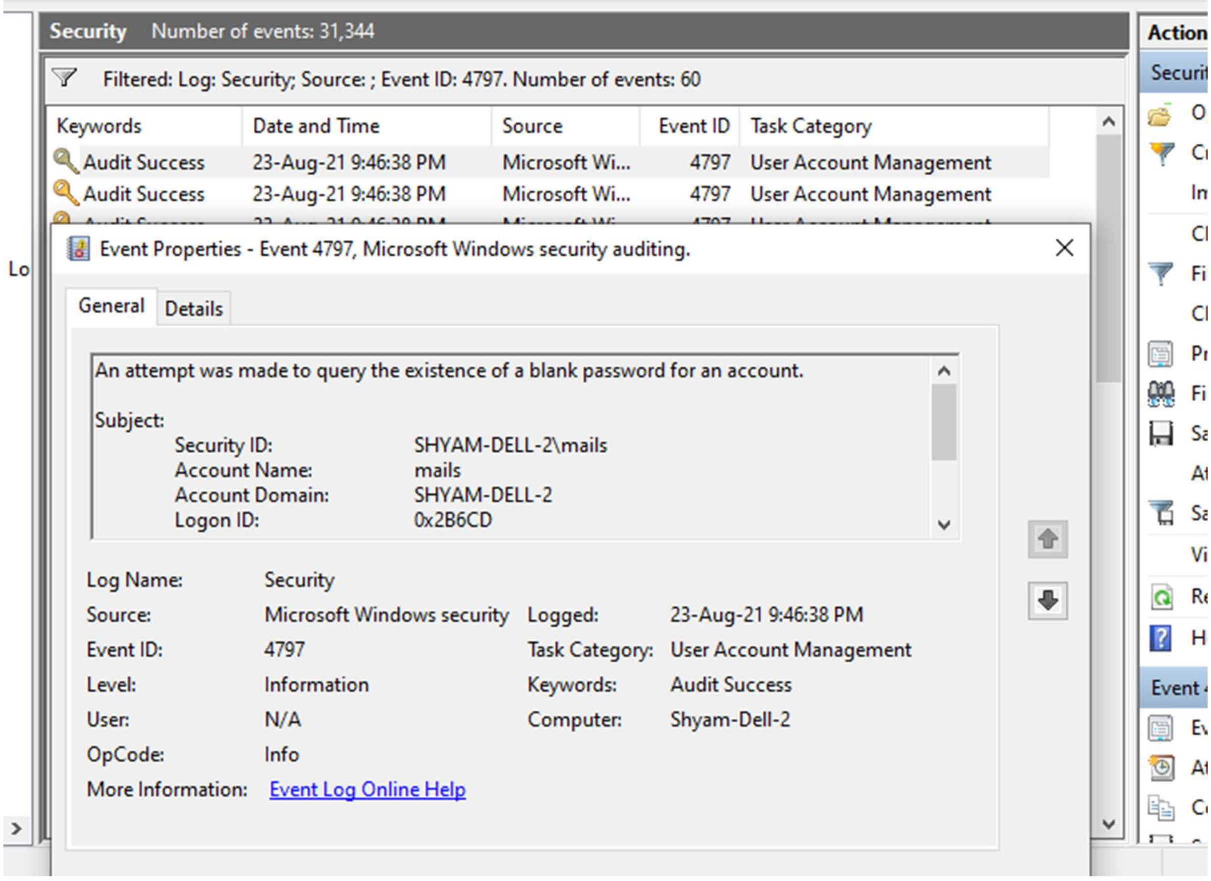
```
User initiated logoff:

Subject:
        Security ID:            SHYAM-DELL-2\mails
        Account Name:           mails
        Account Domain:         SHYAM-DELL-2
        Logon ID:               0x2B8DD
```

Log Name: Security

### OBSERVATION

This event signals the end of a logon session. We see that this event has occurred 17 times.

## ATTEMPT MADE TO QUERY THE EXISTENCE OF A BLANK PASSWORD FOR AN ACCOUNT (EVENT ID – 4797)



Security Number of events: 31,344

Filtered: Log: Security; Source: ; Event ID: 4797. Number of events: 60

| Keywords | Date and Time | Source | Event ID | Task Category |
|---|---|---|---|---|
| Audit Success | 23-Aug-21 9:46:38 PM | Microsoft Wi... | 4797 | User Account Management |
| Audit Success | 23-Aug-21 9:46:38 PM | Microsoft Wi... | 4797 | User Account Management |

Event Properties - Event 4797, Microsoft Windows security auditing.

An attempt was made to query the existence of a blank password for an account.

Subject:

| | |
|---|---|
| Security ID: | SHYAM-DELL-2\mails |
| Account Name: | mails |
| Account Domain: | SHYAM-DELL-2 |
| Logon ID: | 0x2B6CD |

| | | | |
|---|---|---|---|
| Log Name: | Security | | |
| Source: | Microsoft Windows security | Logged: | 23-Aug-21 9:46:38 PM |
| Event ID: | 4797 | Task Category: | User Account Management |
| Level: | Information | Keywords: | Audit Success |
| User: | N/A | Computer: | Shyam-Dell-2 |
| OpCode: | Info | | |
| More Information: | Event Log Online Help | | |

**OBSERVATION**

This event can usually be ignored. We also see that this event has occurred 60 times as shown on the bar up top. If this event is logged with multiple other user accounts, only then it is of concern.

# EVENT LOG EXPLORER

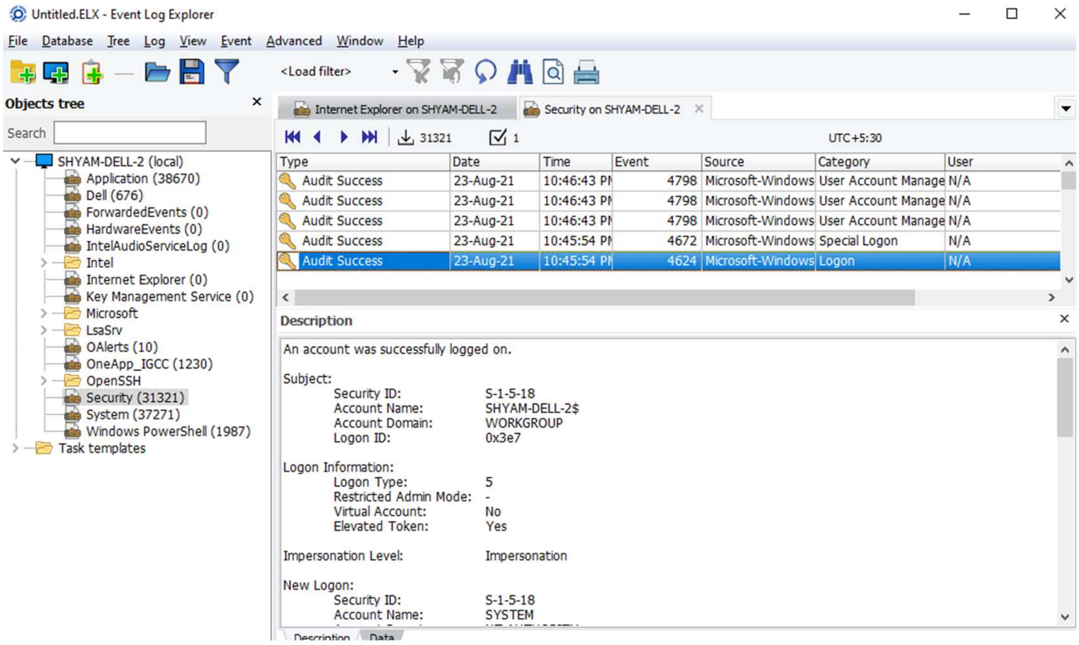
This is a tool built into Windows Operating Systems to let administrators and users view event logs on a machine. We use this to find security events such as logon, logoff using Event IDs.

To find an Event by its ID, click on the 'Find' option under the 'Actions' pane on the right. Then enter the Event id that needs to be found.

## STEPS

1. Download and Install Event Log Explorer
2. In the 'Objects Tree' pane, select the local machine and choose 'Security' from the expanded list.
3. Choose the Filter option or just press CTRL+F.
4. Enter the Event ID needed and click 'Ok'.

## LOGON (Event ID – 4624)



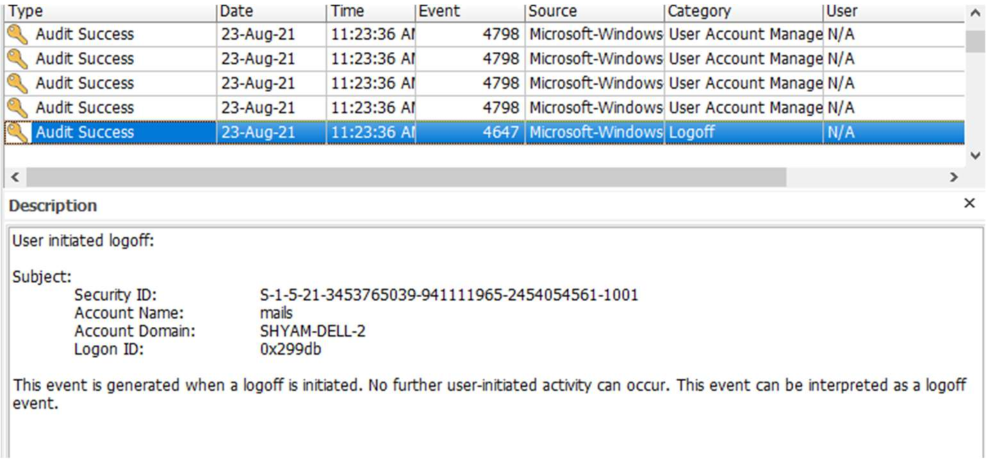
| Type | Date | Time | Event | Source | Category | User |
|---|---|---|---|---|---|---|
| Audit Success | 23-Aug-21 | 10:46:43 PI | 4798 | Microsoft-Windows | User Account Manage | N/A |
| Audit Success | 23-Aug-21 | 10:46:43 PI | 4798 | Microsoft-Windows | User Account Manage | N/A |
| Audit Success | 23-Aug-21 | 10:46:43 PI | 4798 | Microsoft-Windows | User Account Manage | N/A |
| Audit Success | 23-Aug-21 | 10:45:54 PI | 4672 | Microsoft-Windows | Special Logon | N/A |
| Audit Success | 23-Aug-21 | 10:45:54 PI | 4624 | Microsoft-Windows | Logon | N/A |

```
An account was successfully logged on.

Subject:
        Security ID:            S-1-5-18
        Account Name:           SHYAM-DELL-2$
        Account Domain:         WORKGROUP
        Logon ID:               0x3e7

Logon Information:
        Logon Type:             5
        Restricted Admin Mode:  -
        Virtual Account:        No
        Elevated Token:         Yes

Impersonation Level:            Impersonation

New Logon:
        Security ID:            S-1-5-18
        Account Name:           SYSTEM
```

### OBSERVATION

This shows the logon event similar to Event Viewer. A description of the event is also shown.

## LOGOFF (Event ID – 4647)



| Type | Date | Time | Event | Source | Category | User |
|---|---|---|---|---|---|---|
| Audit Success | 23-Aug-21 | 11:23:36 AI | 4798 | Microsoft-Windows | User Account Manage | N/A |
| Audit Success | 23-Aug-21 | 11:23:36 AI | 4798 | Microsoft-Windows | User Account Manage | N/A |
| Audit Success | 23-Aug-21 | 11:23:36 AI | 4798 | Microsoft-Windows | User Account Manage | N/A |
| Audit Success | 23-Aug-21 | 11:23:36 AI | 4798 | Microsoft-Windows | User Account Manage | N/A |
| Audit Success | 23-Aug-21 | 11:23:36 AI | 4647 | Microsoft-Windows | Logoff | N/A |

```
User initiated logoff:

Subject:
        Security ID:        S-1-5-21-3453765039-941111965-2454054561-1001
        Account Name:       mails
        Account Domain:     SHYAM-DELL-2
        Logon ID:           0x299db

This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff
event.
```

**OBSERVATION**

This shows the logoff event similar to Event Viewer. A description is shown too.

# CONCLUSION

We have used the Event Viewer and Event Log Explorer tools to search for specific security events. These tools are powerful and aid those in Digital Forensics to get insights as to what happened on the device and how it was used or if it was compromised.

# 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

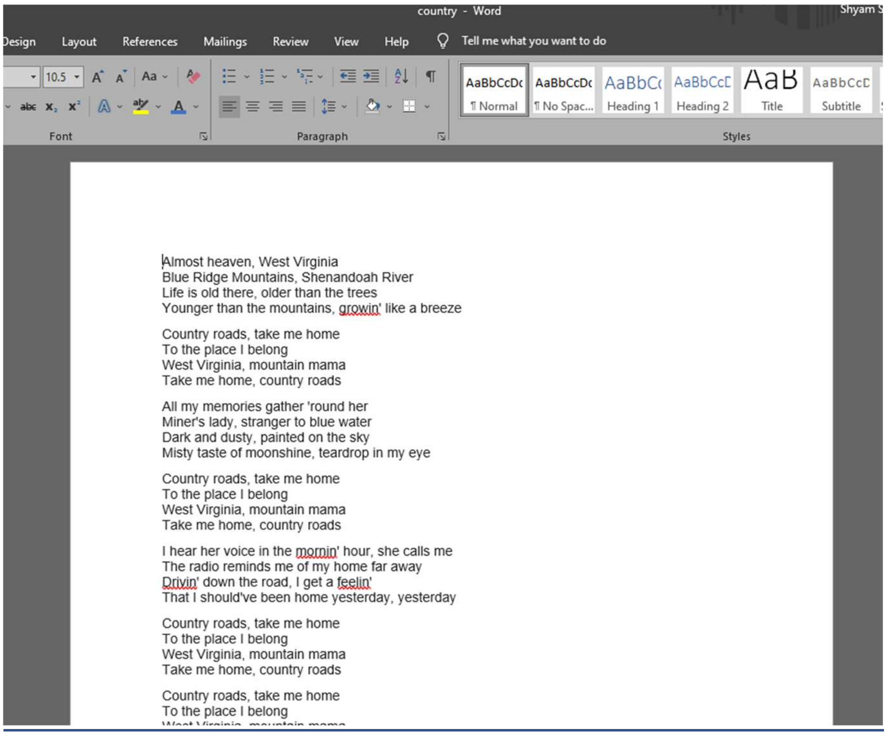
### STRINGS

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



Almost heaven, West Virginia
Blue Ridge Mountains, Shenandoah River
Life is old there, older than the trees
Younger than the mountains, growin' like a breeze

Country roads, take me home
To the place I belong
West Virginia, mountain mama
Take me home, country roads

All my memories gather 'round her
Miner's lady, stranger to blue water
Dark and dusty, painted on the sky
Misty taste of moonshine, teardrop in my eye

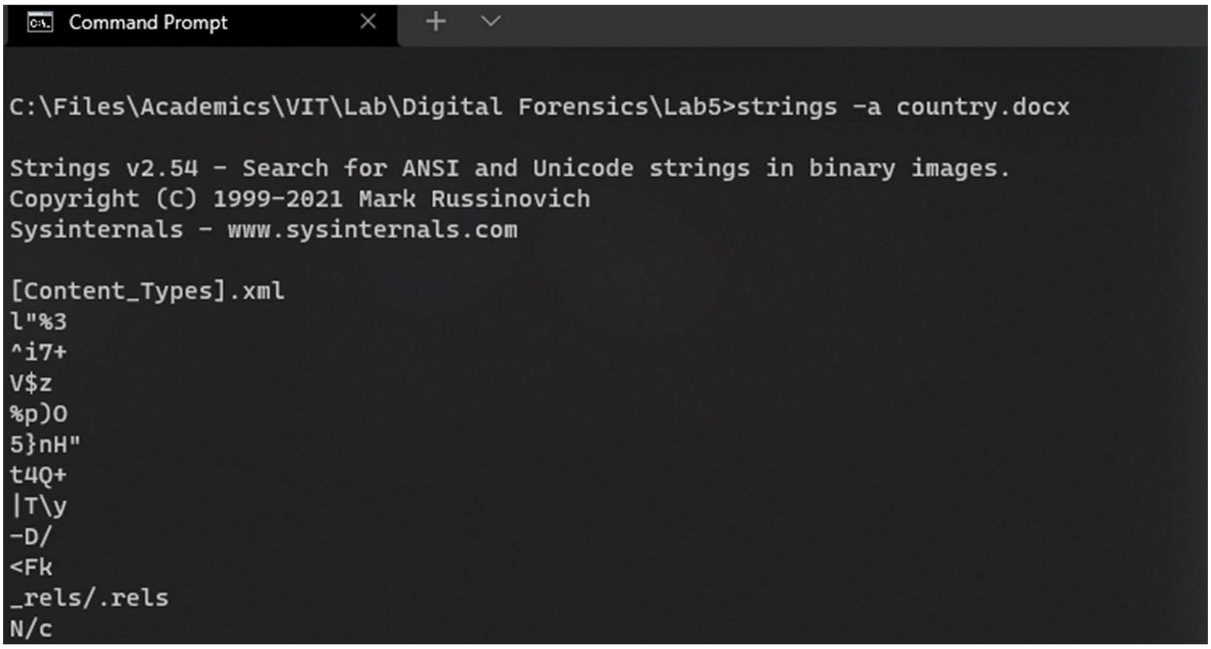
Country roads, take me home
To the place I belong
West Virginia, mountain mama
Take me home, country roads

I hear her voice in the mornin' hour, she calls me
The radio reminds me of my home far away
Drivin' down the road, I get a feelin'
That I should've been home yesterday, yesterday

Country roads, take me home
To the place I belong
West Virginia, mountain mama
Take me home, country roads

Country roads, take me home
To the place I belong

## ASCII only search

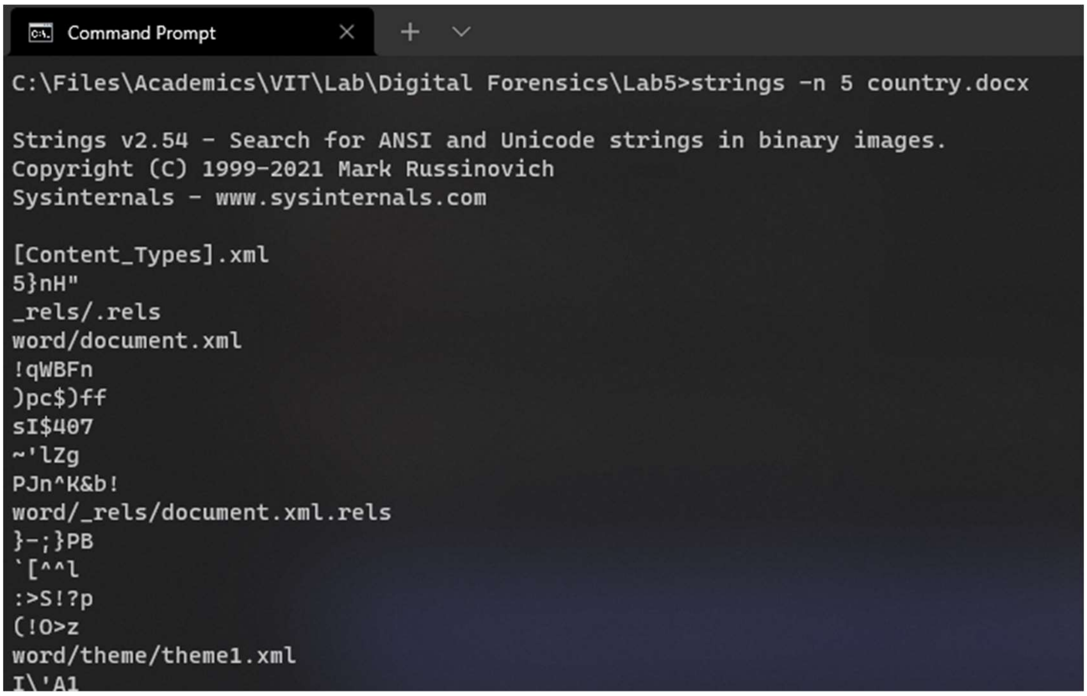


```
C:\Files\Academics\VIT\Lab\Digital Forensics\Lab5>strings -a country.docx

Strings v2.54 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2021 Mark Russinovich
Sysinternals - www.sysinternals.com

[Content_Types].xml
l"%3
^i7+
V$z
%p)O
5}nH"
t4Q+
|T\y
-D/
<Fk
_rels/.rels
N/c
```

**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



```
C:\Files\Academics\VIT\Lab\Digital Forensics\Lab5>strings -n 5 country.docx

Strings v2.54 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2021 Mark Russinovich
Sysinternals - www.sysinternals.com

[Content_Types].xml
5}nH"
_rels/.rels
word/document.xml
!qWBFn
)pc$)ff
sI$407
~'lZg
PJn^K&b!
word/_rels/document.xml.rels
}-;}PB
`[^^l
:>S!?p
(!O>z
word/theme/theme1.xml
I\'A1
```

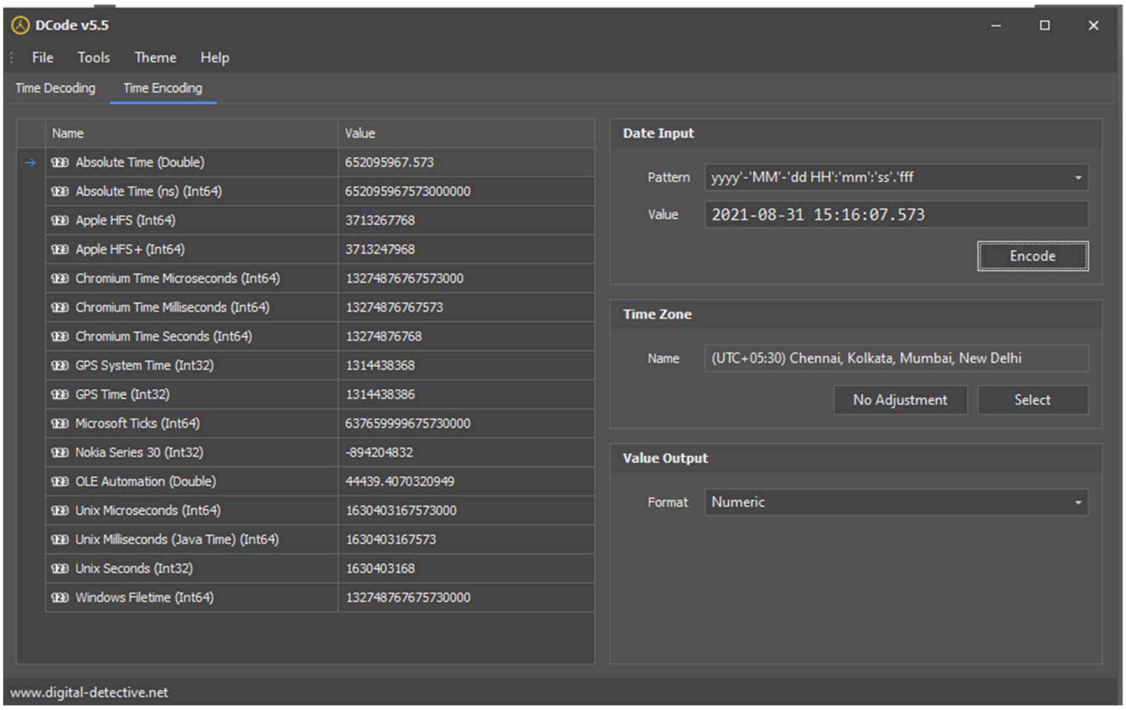
**OBSERVATION**

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



| Name | Value |
|---|---|
| Absolute Time (Double) | 652095967.573 |
| Absolute Time (ns) (Int64) | 652095967573000000 |
| Apple HFS (Int64) | 3713267768 |
| Apple HFS+ (Int64) | 3713247968 |
| Chromium Time Microseconds (Int64) | 13274876767573000 |
| Chromium Time Milliseconds (Int64) | 13274876767573 |
| Chromium Time Seconds (Int64) | 13274876768 |
| GPS System Time (Int32) | 1314438368 |
| GPS Time (Int32) | 1314438386 |
| Microsoft Ticks (Int64) | 637659999675730000 |
| Nokia Series 30 (Int32) | -894204832 |
| OLE Automation (Double) | 44439.4070320949 |
| Unix Microseconds (Int64) | 1630403167573000 |
| Unix Milliseconds (Java Time) (Int64) | 1630403167573 |
| Unix Seconds (Int32) | 1630403168 |
| Windows Filetime (Int64) | 132748767675730000 |

Date Input

Pattern: yyyy'-'MM'-'dd HH':'mm':'ss'.'fff

Value: 2021-08-31 15:16:07.573

Time Zone

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

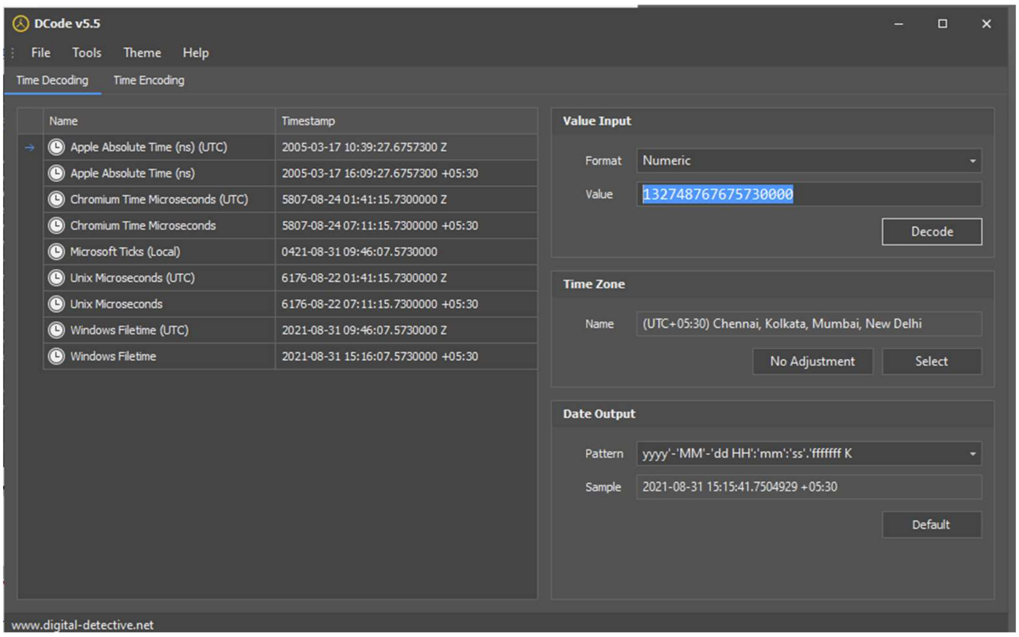
Value Output

Format: Numeric

**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



| Name | Timestamp |
|---|---|
| Apple Absolute Time (ns) (UTC) | 2005-03-17 10:39:27.6757300 Z |
| Apple Absolute Time (ns) | 2005-03-17 16:09:27.6757300 +05:30 |
| Chromium Time Microseconds (UTC) | 5807-08-24 01:41:15.7300000 Z |
| Chromium Time Microseconds | 5807-08-24 07:11:15.7300000 +05:30 |
| Microsoft Ticks (Local) | 0421-08-31 09:46:07.5730000 |
| Unix Microseconds (UTC) | 6176-08-22 01:41:15.7300000 Z |
| Unix Microseconds | 6176-08-22 07:11:15.7300000 +05:30 |
| Windows Filetime (UTC) | 2021-08-31 09:46:07.5730000 Z |
| Windows Filetime | 2021-08-31 15:16:07.5730000 +05:30 |

Value Input

Format: Numeric

Value: 132748767675730000

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 15:15:41.7504929 +05:30

**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.

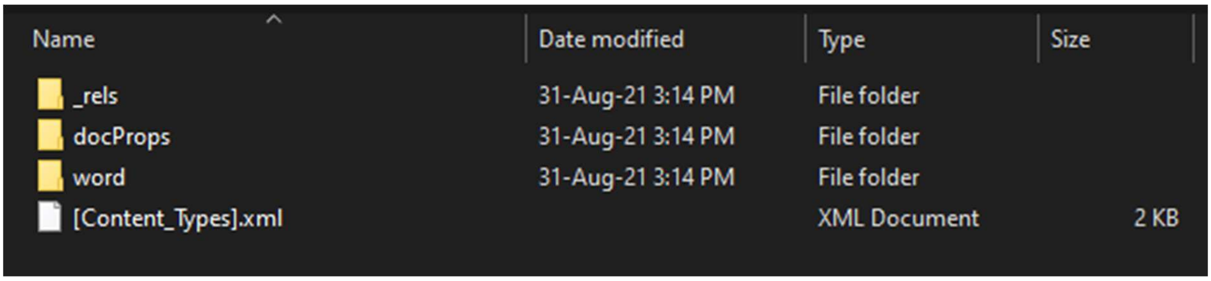
## PART 2

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

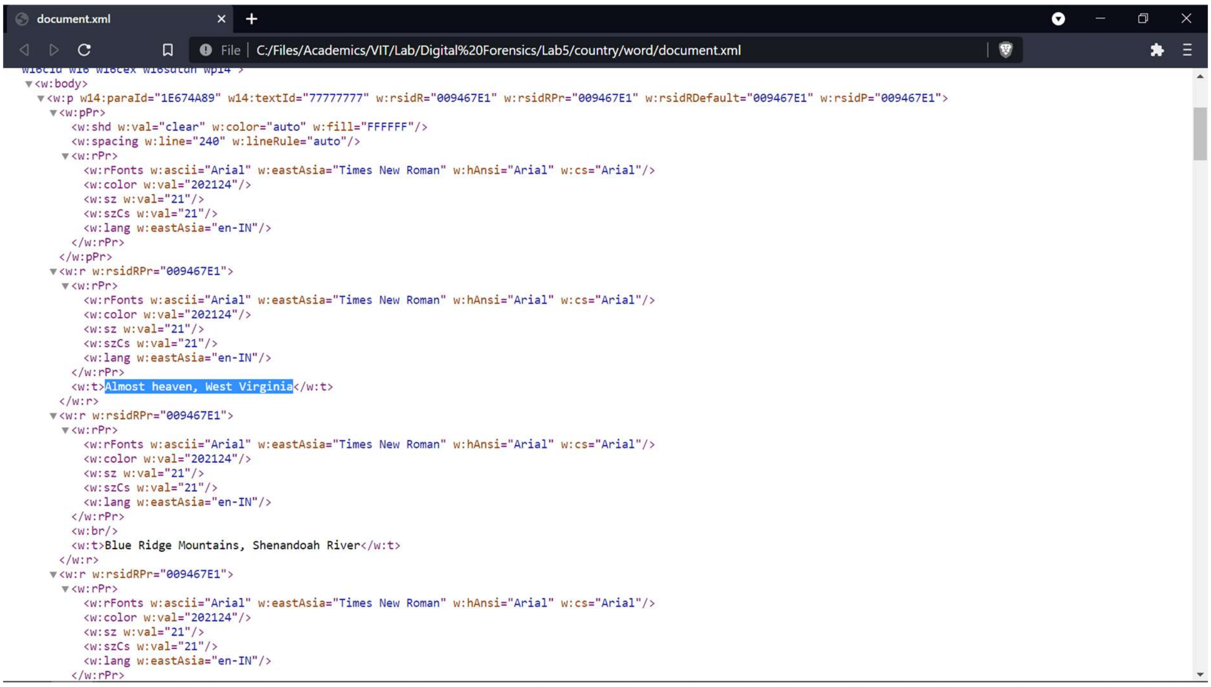
1. Open WinRAR or WinZip.
2. Open the docx file and click 'Extract' to obtain the XML files.
3. All XML files can be seen in the folder.

List of files extracted from country.docx.



| Name | Date modified | Type | Size |
|---|---|---|---|
| _rels | 31-Aug-21 3:14 PM | File folder | |
| docProps | 31-Aug-21 3:14 PM | File folder | |
| word | 31-Aug-21 3:14 PM | File folder | |
| [Content_Types].xml | | XML Document | 2 KB |

## WORD/DOCUMENT.XML



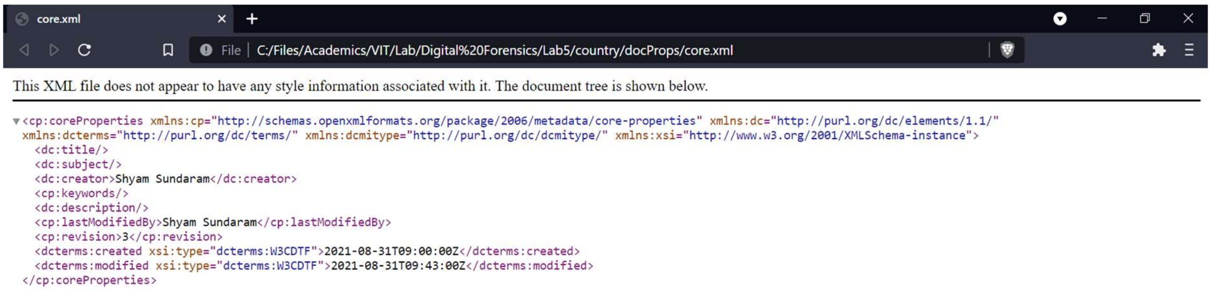
document.xml
File
C:/Files/Academics/VIT/Lab/Digital%20Forensics/Lab5/country/word/document.xml

```
w16cid w16 w16cex w16sdtdh wp14">
▼<w:body>
  ▼<w:p w14:paraId="1E674A89" w14:textId="77777777" w:rsidR="009467E1" w:rsidRPr="009467E1" w:rsidRDefault="009467E1" w:rsidP="009467E1">
    ▼<w:pPr>
        <w:shd w:val="clear" w:color="auto" w:fill="FFFFFF"/>
        <w:spacing w:line="240" w:lineRule="auto"/>
      ▼<w:rPr>
          <w:rFonts w:ascii="Arial" w:eastAsia="Times New Roman" w:hAnsi="Arial" w:cs="Arial"/>
          <w:color w:val="202124"/>
          <w:sz w:val="21"/>
          <w:szCs w:val="21"/>
          <w:lang w:eastAsia="en-IN"/>
        </w:rPr>
      </w:pPr>
    ▼<w:r w:rsidRPr="009467E1">
      ▼<w:rPr>
          <w:rFonts w:ascii="Arial" w:eastAsia="Times New Roman" w:hAnsi="Arial" w:cs="Arial"/>
          <w:color w:val="202124"/>
          <w:sz w:val="21"/>
          <w:szCs w:val="21"/>
          <w:lang w:eastAsia="en-IN"/>
        </w:rPr>
        <w:t>Almost heaven, West Virginia</w:t>
      </w:r>
    ▼<w:r w:rsidRPr="009467E1">
      ▼<w:rPr>
          <w:rFonts w:ascii="Arial" w:eastAsia="Times New Roman" w:hAnsi="Arial" w:cs="Arial"/>
          <w:color w:val="202124"/>
          <w:sz w:val="21"/>
          <w:szCs w:val="21"/>
          <w:lang w:eastAsia="en-IN"/>
        </w:rPr>
        <w:br/>
        <w:t>Blue Ridge Mountains, Shenandoah River</w:t>
      </w:r>
    ▼<w:r w:rsidRPr="009467E1">
      ▼<w:rPr>
          <w:rFonts w:ascii="Arial" w:eastAsia="Times New Roman" w:hAnsi="Arial" w:cs="Arial"/>
          <w:color w:val="202124"/>
          <w:sz w:val="21"/>
          <w:szCs w:val="21"/>
          <w:lang w:eastAsia="en-IN"/>
        </w:rPr>
```

**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


core.xml
File
C:/Files/Academics/VIT/Lab/Digital%20Forensics/Lab5/country/docProps/core.xml

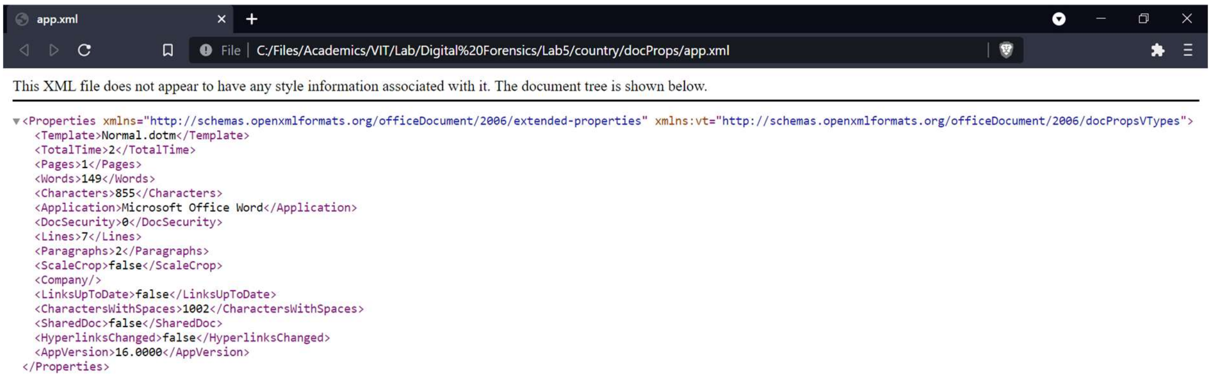
This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<cp:coreProperties xmlns:cp="http://schemas.openxmlformats.org/package/2006/metadata/core-properties" xmlns:dc="http://purl.org/dc/elements/1.1/"
 xmlns:dcterms="http://purl.org/dc/terms/" xmlns:dcmitype="http://purl.org/dc/dcmitype/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <dc:title/>
   <dc:subject/>
   <dc:creator>Shyam Sundaram</dc:creator>
   <cp:keywords/>
   <dc:description/>
   <cp:lastModifiedBy>Shyam Sundaram</cp:lastModifiedBy>
   <cp:revision>3</cp:revision>
   <dcterms:created xsi:type="dcterms:W3CDTF">2021-08-31T09:00:00Z</dcterms:created>
   <dcterms:modified xsi:type="dcterms:W3CDTF">2021-08-31T09:43:00Z</dcterms:modified>
 </cp:coreProperties>
```

**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


app.xml
File
C:/Files/Academics/VIT/Lab/Digital%20Forensics/Lab5/country/docProps/app.xml

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<Properties xmlns="http://schemas.openxmlformats.org/officeDocument/2006/extended-properties" xmlns:vt="http://schemas.openxmlformats.org/officeDocument/2006/docPropsVTypes">
   <Template>Normal.dotm</Template>
   <TotalTime>2</TotalTime>
   <Pages>1</Pages>
   <Words>149</Words>
   <Characters>855</Characters>
   <Application>Microsoft Office Word</Application>
   <DocSecurity>0</DocSecurity>
   <Lines>7</Lines>
   <Paragraphs>2</Paragraphs>
   <ScaleCrop>false</ScaleCrop>
   <Company/>
   <LinksUpToDate>false</LinksUpToDate>
   <CharactersWithSpaces>1002</CharactersWithSpaces>
   <SharedDoc>false</SharedDoc>
   <HyperlinksChanged>false</HyperlinksChanged>
   <AppVersion>16.0000</AppVersion>
 </Properties>
```

**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.