Exercise 4

31/08/2021

File forensics

Investigating MS Word documents

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

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.

2) 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.