

REPUBLIC OF TURKEY
BOĞAZIÇI UNIVERSITY
FACULTY OF ENGINEERING
OFFICE OF THE DEAN

Number: B.30.2.BÜN.0.17.00.00/ 604.01.03-1226
Subject:

23 November 2011

ÜLGEN LAW OFFICE
CELAL ÜLGEN AND HÜSEYİN ERSÖZ, ATTORNEYS-AT-LAW
REPRESENTING HAKAN BÜYÜK

Reference: Letter of 11 November 2011

Please find enclosed the “Hakan Büyük File Technical Opinion” issued by Prof. Dr. M. Ufuk Çağlayan of the Faculty of Engineering, Department of Computer Engineering upon a request received through your above-mentioned letter.

Best Regards

(signed)
Associate Prof. Kunt Atalık
Vice Dean

Sworn Translator
EGEMEN TRANSLATION OFFICE
0.216.367 39 35
ISTANBUL / TURKEY
EGEMEN DEMİRCİOĞLU

Technical Report

The Office of the Dean of the Faculty of Engineering was asked on 11 November 2011 to appoint an academician from the Department of Computer Engineering to issue a technical report on the basis of the questions enclosed with the request on matters that Celal Ülgen and Hüseyin Ersöz, attorneys-at-law, representing Hakan Büyük, wanted to be clarified in conjunction with the attached documents. The following report consists of the answers to the above-mentioned questions provided by Prof. Dr. Mehmet Ufuk Çağlayan who was appointed to the mentioned job by the Office of the Dean of the Faculty of Engineering and by the Office of the Head of the Department of Computer Engineering.

Those documents, from among the documents that were provided in a Flash Disk attached to the request letter, that were used in answering the questions are mentioned in each related answer.

Find below the answers that we prepared on the matters that were asked to be clarified.

Question 1

Does Metadata information, which mean upper data that are not visible to users and are included in special software such as data regarding creation, modification, author etc. on a digital file, contain information that are not modifiable for a digital document? Can they change by themselves without any deliberate action carried out on them such as data extraction, data modification etc.? Can such factors as going to a country that has a time difference with respect to Turkey, being in a desert or in polar areas, having access to the values today or in 10 years cause a modification in metadata information?

Answer 1

Metadata information, which mean upper data that are not visible to users and are included in special software such as data regarding creation, modification, author etc. on a digital file do not contain information that are not modifiable for the digital document unless the digital document in question is stored in a medium that is only readable such as a CD-ROM or a DVD-ROM etc. If the digital document is stored in a medium that it is possible to write on such as a hard disk or a flash memory, a specialist knowing the location of the metadata information in the digital document and their format can change any part of such metadata the way he wishes using a special software that can be described as an editor.

These data cannot change significantly without deliberate action carried out on them such as data extraction, modification etc.. However, such data can be damaged and become unreadable due to various reasons such as environmental conditions, damaged media material etc.

Such factors as going to a country that has a time difference with respect to Turkey, being in a desert or in polar areas, having access to the values today or in 10 years cannot normally cause any change in metadata information. For instance, such factors

Sworn Translator
EGEMEN TRANSLATION OFFICE
0.216.367 19 35
ISTANBUL / TURKEY
EGEMEN DEMİRCİOĞLU

will not cause any change in files containing pictures such as files with .jpg or .gif extensions. Metadata information of digital files containing texts, drawings, tables etc. such as those with .doc, docx, .xls, .xlsx, .ppt, .pptx etc. extensions may contain such information as the date and time of last access to the digital file, i.e. the date and time when the file was last read. In such a case, there will be a change only in metadata information relating to access date and time and there will be no change at all in other metadata information.

Question 2

If metadata information of two .jpg digital documents in different directories with the same Hash Values are different, what would that mean? Conversely, if there are two digital documents that have the same metadata information but different Hash Values, what would that mean? What would be the effect of such factors on the coherence and reliability of the evidence?

Answer 2

The metadata information of two .jpg digital documents in different directories with the same hash values cannot be different because hash values are calculated on the basis of .jpg digital document as a whole including the metadata information.

If the metadata information of two .jpg digital documents with the same hash values is different, then this means that a change has occurred in the metadata information of one of these two digital files after the calculation of the file's hash value. If the change in the document's metadata information was caused by media errors, then usually the metadata should not have changed in a very meaningful manner. As explained in Answer 1, a modification in a document's metadata information may have been the result of an accidental or deliberate reading or of the action of a specialist if the metadata information includes the date and time of last access to the digital file.

If there are two digital documents with the same metadata information but different hash values, this would mean that in one of the digital documents a change has occurred in the body of the document except metadata information. For instance, if there is a text in the digital document or if there is a picture in the text that constitutes the body of the document or in the digital document, a change must have occurred in the picture that constitutes the body of the document.

In both cases explained above, it should be assumed that the digital documents in question have lost their quality of being coherent and reliable evidence.

Question 3

What is your opinion about differences in information such as Hash Value, Date of Creation, Date of Last Saving, Author etc. in reports resulting from examinations carried out at different dates on the same digital media from the point of view of the coherence and reliability of evidence?

Answer 3

Sworn Translator
EGEMEN TRANSLATION OFFICE
0.216.367 19 35
ISTANBUL / TURKEY
EGEMEN DEMİRCİOĞLU

Information such as Hash Values, Date of Creation, Date of Last Saving, Author etc. in reports resulting from examinations carried out at different dates for the same digital media should be the same if the examinations have been carried out without causing any change in the digital media.

The examination must be carried out always making sure that no change will occur in the digital media. For instance, a copy can be obtained of the digital media without modifying the original and the examination carried out on it. It is also technically possible to carry out an examination directly on the original of digital media without damaging them.

If there are differences in any items of information such as Hash Value, Date of Creation, Date of Last Saving, Author etc. in reports resulting from examinations carried out at different dates on the same digital media, this would mean that a change has occurred in the content of the digital media. We assume here that the digital media examined was transferred to and written in the reports honestly without altering or modifying information such as Hash Value, Date of Creation, Date of Last Saving, Author etc.

If there are differences in any items of information such as Hash Value, Date of Creation, Date of Last Saving, Author etc. in reports resulting from examinations carried out at different dates on the same digital media, as this will mean that a change has occurred in the content of the digital media, the digital media will no longer have the quality of being coherent and reliable evidence.

Question 4

Can the date of creation of a digital data containing the scanned image of a newspaper issue dated 12 May 2009 be 19 April 2007?

The flash disk enclosed with the request contains digital documents that are supposed to support the accusations directed against our client. The locations of these digital documents are as follows:

BİLVANİS ÇİFTLİĞİ/ESKİŞEHİR/3-ISLAK İMZALILAR.zip/tara0059.jpg
BİLVANİS ÇİFTLİĞİ/ESKİŞEHİR/3-ISLAK İMZALILAR.zip/tara0053.jpg

If your answer to the question above is negative, then can we say that this proves the existence of a manipulation on the basis of the upper data information and content of the digital documents whose locations are provided above?

Answer 4

I have examined the digital documents

BİLVANİS ÇİFTLİĞİ/ESKİŞEHİR/3-ISLAK İMZALILAR.zip/tara0059.jpg
BİLVANİS ÇİFTLİĞİ/ESKİŞEHİR/3-ISLAK İMZALILAR.zip/tara0053.jpg

Sworn Translator
EGEMEN TRANSLATION OFFICE
0.216.367 1935
İSTANBUL / TURKEY
EGEMEN DEMİRCİOĞLU

contained in the flash memory enclosed with the request and the metadata information of these files. Both are files of JPEG format containing pictures. The metadata information of these files is as follows:

- BİLVANİS ÇİFTLİĞİ/ESKİŞEHİR/3-ISLAK İMZALILAR.zip/tara0059.jpg
Type of file: JPG file, Resolution: 1700x2338 pixel, File size: 525 Kbyte, Date and time of last writing on the file: 19 April 2007 18:58:00 Camera features: none

At two points in the picture in the file the date “12 May 2009” is clearly visible. At one point in the picture, the date “12 May 2009” is clearly visible.

- BİLVANİS ÇİFTLİĞİ/ESKİŞEHİR/3-ISLAK İMZALILAR.zip/tara0053.jpg
Type of file: JPG file, Resolution: 2550x3507 pixel, File size: 911 Kbyte, Date and time of last writing on the file: 19 April 2007 18:49:14 Camera features: none

It is clearly visible that the date of the letter in the file is “12 February 2008”.

The date of creation of a digital data containing the scanned image of a newspaper issue dated 12 May 2009 can by no means be prior to 12 May 2009 and therefore it cannot be 19 April 2007. Similarly, the date of creation of a digital data containing a letter dated 12 February 2008 can by no means be prior to 12 February 2008 and therefore it cannot be 19 April 2007.

This means that a change occurred as explained in Answer 1 in the date of last writing which is an item of the metadata information of the computer files that contains the digital data in question and that the files have lost the quality of being coherent and reliable evidence.

Question 5

Can the dates of creation and last saving of the digital that figures in the file location “BİLVANİS ÇİFTLİĞİ/ESKİŞEHİR/EK-A 926 Teklifler.doc” containing a draft bill containing Article 7 of Law no. 5365 of 15.06.2005 be dates in 2003? If your answer is negative, how can such a situation be explained in terms of judicial computer sciences?

Answer 5

I have examined the metadata information of “BİLVANİS ÇİFTLİĞİ/ESKİŞEHİR/EK-6 926 Teklifler.doc”. This file contains a text in the form of a Microsoft .doc document. The metadata information of the mentioned file is as follows:

Type of file: Microsoft Office Word 97-2003 file, File Size: 91.648 Byte, Date and time of last writing on the file: 05 April 2003 12:49:10

The dates of creation and last saving of the digital that figures in the file location “BİLVANİS ÇİFTLİĞİ/ESKİŞEHİR/EK-A 926 Teklifler.doc” that is said to contain a Bill containing Article 7 of Law no. 5365 of 15 June 2005 can by no means be prior to 15 June 2005, therefore they cannot be 05 April 2003.

Sworn Translator
EGEMEN TRANSLATION OFFICE
0.216.367 19 35
İSTANBUL / TURKEY
EGEMEN DEMİRCİOĞLU

This shows that a change occurred as explained in Answer 1 in the date of last writing figuring among the metadata information of the file containing the digital data in question and that the files in question have lost their quality of being coherent and reliable evidence.

Question 6

What does "GUID" value mean? Is it possible to identify using "GUID" values the computer in which an MS Word document has been created?

Answer 6

GUID (Globally Unique Identifier) is a very large number of 128 bits (binary), in other words, of 16 bytes and consists usually of numbers 0-9 and the letters A, B, C, D, E, F in a 16-digit system and the numbers are in the form of groups of 8, 4, 4, 4, 12, a total of 32 digits.

Example: 2A2506E5-4F8B-12D0-9A0E-03F5E72C3305

Usually GUID numbers are created randomly and, as GUID is a very large number, the probability of two GUID numbers being the same is extremely low. Companies use GUID numbers for various purposes. GUID is widely used in database systems.

The company MICROSOFT widely uses GUID numbers in its Windows operating system and in applications compatible with the Component Object Model (COM) and the Distributed Component Object Model (DCOM) to identify software interfaces, software classes and objects. In addition, GUID numbers are placed by Microsoft Office software installed in a computer in the metadata information of Word, Excel etc. documents. The details of the use of GUID numbers by Microsoft software being technically too complicated, no further explanation would be helpful for the purposes of the present report.

I am not aware of any method of identifying which document was created in which computer using the GUID values in a Microsoft Word document. I have checked the literature and Internet resources to find out whether there is such a method but did not find any method of identifying the computer in which a given document was created using GUID values.

The claim that the company Microsoft can match GUID values placed by Microsoft Office software in the metadata information of Word, Excel etc. documents with Microsoft Office software in a given computer and so become able to have access to installation details of Microsoft Office software and therefore to user identity details circulated in the Internet but the company Microsoft declared that they had never attempted to have access to user details using this method and started to distribute software tools to destroy, if need be, a part of the metadata information of an Office or Word document.

Question 7

Sworn Translator
EGEMEN TRANSLATION OFFICE
0 216 367 19 35
ISTANBUL / TURKEY
EGEMEN DEMIRCIÖĞLU

Is there a "File type" called "World Document"? Is it technically possible that there is a gap in the file location of a digital data?

Answer 7

I am not aware of any "File Type" called "World Document". I scanned the literature and the Internet to find out whether there is a "File Type" called "World Document" but did not find any such "File Type".

It is technically possible that a gap exists in the file location, in other words, in the file name of a digital data and this method is widely used.

Best Regards

22 November 2011

(seal and signature)

Prof. Dr. Mehmet Ufuk Çağlayan

Faculty of Engineering, Department of Computer Engineering

Boğaziçi University, Bebek, Istanbul

www.translato
EGEMEN TRANSLATION OFFICE
0.236 367 19 35
ISTANBUL / TURKEY
EGEMENDEMIRCIOGLU

