TECHNICAL REPORT

SUBJECT:

We have been asked to analyse CD image files contained in a DVD that was delivered to us in order to clarify the following matters:

1. Whether there are any files in CD image nos. 11, 16 and 17 contained in the DVD that are created through Microsoft applications after the date of creation of the CDs.

2. Depending on the answer to the first question above, whether the presence of findings in CD nos. 11, 16 and 17 of a date later than the date of creation is normal; if it is not normal, how it can be explained.

3. Depending on the answer to the second question above, what are the consequences regarding the coherence and reliability of the evidence provided by CD nos. 11, 16 and 17 in terms of judicial computer science.

4. Whether it is possible for these three CDs or any other similar CDs to have been created in such a manner that they seem to be prepared earlier; whether even an ordinary user can produce such CDs or DVDs or Flash Memories and the methods that can be used for such a purpose

5. Whether the Hash Value of a CD or DVD guaranties that no alteration has been carried out on such CD or DVD until the date when the Hash Values were taken.

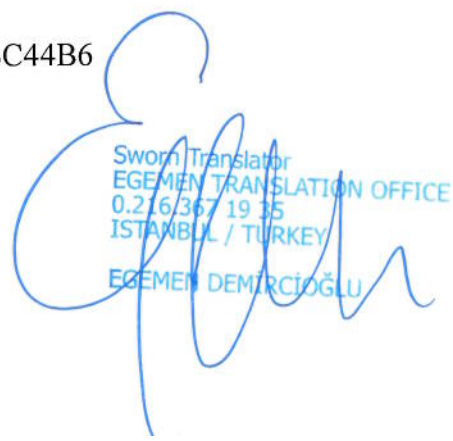
EXAMINATION

The DVD that we received in the enclosure of the request contains 3 separate directories containing image files of CD nos. 11, 16 and 17 taken separately with versions 4.20 and 6.15 of the software named Encase. Each directory contains two directories named 4.20 and 6.15 relating to images of different versions and each directory contains an image file with E01 extension and a hash file of rich text format (extension .rtf) to be used to verify the images created during the taking of the images.

It was verified for each CD that the images 4.20 and 6.15 had the same content and for each CD it was found fit to use the 4.20 image for each CD and therefore these images were used for the examination. 128-bit hash value of each 4.20 image file was obtained as explained below and these values were compared to the registered hash files and so it was verified that the images in the form they have been extracted had not been altered.

Name: CD_11
Start Sector: 0
Stop Sector: 185.552
Hash Value: E814AF82D3E832A5AE4EC59BEEBC44B6

Name: F
Start Sector: 0
Stop Sector: 12.616



Hash Value: 80FBD6BC151A3E9A1E38B0AB46C453CC

Name: CD_17
Start Sector: 0
Stop Sector: 2.144
Hash Value: 6322E5683C06D4B963D51FCE144075B0

About the images mentioned above we observed the following:

1. All three CD images were created on 11 November 2011 and the CDs they contain were created at the dates provided below with the program Roxio Easy CD Creator 5.2. The version of the program used is compatible with the dates of creation of the CDs.

a. CD11 05 March 2003 23:50
b. CD16 14 October 2003 11:42
c. CD17 04 March 2003 23:52

2. The CDs contain files with extensions doc, xls, ppt and htm. An examination with respect to these files showed that all of these files had been created with Microsoft Office suite containing the programs Word, Excel and Powerpoint. We identified signatures relating to the various versions of these programs in the files. Those versions that we identified are Office 97 (Office 8), Office 2000 (Office 9), Office XP (also known as Office 2002 – Office 10) and Office 2003 (Office 11). The dates of issue of these versions have become part of their names. The dates of creation of the CDs and the files they contain are compatible with the versions mentioned here.

3. During the creation of document files, to enable the user and the system to identify and monitor the files, in addition to the information added by the user, information named metadata are recorded by the application program used and also by the operating system. For instance, such details as the user who has created the file, the user who last modified the file, version number of the document are monitored by the application program and such details as the dates of creation, access and modification by the operating system. These data that are recorded by the operating system are saved on a one-to-one basis during the extraction of images. As for the data monitored by the application, as they are contained in the document, they are carried together with the document. According to the records kept by the operating system relating to the files contained in the images examined, the dates of creation and the dates of modification are between the interval 14 December 2001 and 13 October 2003.

4. The somewhat superficial examination described above shows no discrepancy regarding the information contained in the images and in the files. A more detailed examination of the file conducted to answer question no. 1 revealed the following.

a. An examination of the contents of the files showed that the font Calibri had been used in the file ÇALIŞMALAR_A/YENİ YAPILANMADA GÖREVLENDİRİLECEKLER/Müzahir.xls contained in CD no. 11. The font Calibri was developed in 2004 by Microsoft together with the font Cambria and used in 2005 as Beta (trial) and commercially launched in the products Windows Vista and Office

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

2007. This font cannot have been used on 12 February 2003 when this file was last modified.

b. A search conducted relating to the font Calibri revealed that there were records relating to the font Calibri in font details in 66 documents contained in CD nos. 11 and 17 in addition to the above-mentioned document. The presence of information relating to the font Calibri shows that the 67 documents (some of them copies of each other in different locations) a list of which is attached must have been created or modified after 2005.

c. Similarly, a search conducted relating to the font Cambria revealed that there were records relating to the font Cambria in the font information of 5 documents contained in CD nos. 11 and 17. One of these documents (_GEN ETÜD.XLS) contains both fonts and figures in the table above as well. The presence of information relating to this font shows that the 5 documents a list of which is attached must have been created or modified after 2005.

d. The file system of the Office series launched by Microsoft underwent some radical changes from 2007. One of these changes was about saving the files in a format named Office Open XML. Files saved in this way are prepared as XML and compressed before being stored. Microsoft had previously used the XML file system but failed to standardize and launch it before 2006. The standard was created in 2006 and used only in Office 2007 that was launched in 2007. An examination conducted with respect to this aspect of the matter revealed the presence of a non-compressed XML content and the address http://schemas.openxmlformats.org/drawingl/2006/main in the file 2002-2003/KARADENİZ TEHDİT DEĞERLENDİRMESİ.ppt contained in CD no. 11, which shows that this file was prepared with Office 2007 or a newer version. This standard was created in 2006 and can be used in Office 2007 and later versions.

e. Similarly, in addition to the above-mentioned file, the fact that two files contained in 4 different directories were in compressed XML format and that they contained the address http://schemas.openxmlformats.org/drawingml/2006/main shows that these 9 files a list of which is attached as Annex C must have been prepared with Office 2007 or a newer version.

f. In the light of the explanations provided above, we conclude that a total of 80 files were prepared with programs launched after the date of creation of the CDs or have features that did not exist at the dates when the CDs were created.

5. According to the observations explained in the previous item, CD nos. 11 and 17 contain technology that belong to a later period than the year 2003 when they were created. This can be possible only if the CDs were prepared after the appearance of these technologies and that the date and time information has been altered in one way or another.

6. According to the conclusion mentioned in the previous item, there is a discrepancy between the dates of creation of the CDs as identified in the images and their actual dates of creation. Then, the dates of creation/access/modification of the files become at least unreliable. The dates of preparation of the files and CDs in question are not

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

reliable. The examination conducted for the present report does not allow any further comments regarding the coherence and reliability of evidence.

7. All date and time information regarding the creation of the CDs are obtained from the system clock of the computer. If a user manages to change this clock, then it can be possible to create or update a file with a date and time that is not the true date and time. Changing the clock of a system is an operation that can be carried out by any user, whatever his level. It is also possible to download from the Internet special software that will enable a user to easily change such information in existing files. In addition, during the creation of a CD, the application program may give the user the option of changing or leaving intact some specific items of information regarding the files.

8. Obtaining a hash is an operation of creating a value of a fixed unique length for any given information of any length. "Unique" means here that the probability of there being more than one text with the same hash value is so low that it can be assumed nil. The smallest change (for instance one that can is comparable to changing a letter in an encyclopaedia) will cause the hash to be different from the previous one. Similarly, when the hash of a disc is obtained, it will be possible to notice any change carried out on this disk by re-obtaining the hash. The hash value will provide inherent information pertaining only to the data where it was produced. It will not provide any information relating to changes that occurred before its production. But, it can be used to monitor the coherence of the data after the date the hash was obtained.

CONCLUSION

For the reasons explained above and according to the CD images contained in the DVD examined:

1. We conclude that at total of 80 files were prepared with programs that were launched after the date of preparation of the CDs or that they have features that did not exist at the dates they were prepared.

2. CD nos. 11 and 17 must have been prepared in 2007 or later with untrue earlier dates. It is not possible for them to have been prepared before 2007.

3. As for the images of CD nos. 11 and 17, the information about the dates of the files in these CDs cannot be considered to be conclusive evidence since they do not constitute unchangeable true information.

4. It is possible to fix wrong dates of creation, access or modification for any document by simply altering the clock of the system.

5. A Hash Value only shows whether or not the data to which it is applied has changed or not. It does not provide any information retrospectively about when it was changed. It can be used for the period after its production.

Prof. Dr. A. Coşkun Sönmez

Dr. Ö. Özgür Bozkurt

Sworn Translator
EGEMEN TRANSLATION OFFICE
0 216 367 19 35
İSTANBUL / TURKEY
EGEMEN DEMİRCİOĞLU

Enclosure:

1. Annex A. List of files containing the font Calibri
2. Annex B. List of files containing the font Cambria
3. Annex C. List of files saved as Office Open XML

The persons whose names appear above are lecturers at our Faculty.

…/03/2012
Prof. Dr. Celal Kocatepe
Dean
Yıldız Technical University,
Faculty of Electronic and Electrical Engineering

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