Çetin Doğan
T.C. İSTANBUL10. AĞIR CEZA MAHKEMESİ
2010/283

Preliminary Report

March 21, 2012

I. Introduction

I am the President of Arsenal Consulting ("Arsenal") where I lead engagements involving computer forensics for law firms, corporations, and government agencies. I have more than a decade of computer forensics experience in law enforcement and the private sector. In addition, I am an adjunct professor at Bunker Hill Community College and was an instructor at the Computer Security Institute for eight years. A true and accurate copy of my CV is attached as Exhibit A to this report.

Arsenal Consulting, Inc. ("Arsenal") was retained on February 15, 2012 by Attorney Hüseyin Ersöz to provide computer forensics consulting services in connection with his representation of Çetin Doğan in a criminal matter. More specifically, Attorney Ersöz requested Arsenal's assistance in identifying anything suspicious regarding Microsoft Office documents contained on three CDs known as "CD 11", "CD 16", and "CD 17."

Computer forensics practitioners obtain forensic images from electronic media to preserve all the data on that media, including "deleted space." Forensic images can be authenticated at any time in the future by calculating hash values (also known as digital fingerprints) which are associated with each forensic image. Arsenal's analysis is based on forensic images of CDs 11, 16, and 17[1] which were obtained on November 11, 2011 by "Bilirkişiler" using Guidance Software's EnCase v6.15.

II. Executive Summary

Arsenal has concluded that dates and times related to at least 76 documents found on CDs 11 and 17 have been forged. Arsenal has also concluded that dates and times related to the creation of CDs 11 and 17 have been forged. The earliest that CDs 11 and 17 could have been created is mid 2006. Arsenal has serious concerns about the authenticity of all the documents on CDs 11 and 17 due to the evidence tampering that has been uncovered thus far. Our analysis of CDs 11, 16, and 17 is ongoing.

[1] Arsenal authenticated these forensic images using EnCase v6.19.3.11

III. Calibri Typeface Analysis

Microsoft Office ("Office") 2007, released to the public mid 2006[2] in beta form and January 2007 in final form, was the first version of Office to contain the Calibri typeface ("Calibri"). Microsoft released the "Microsoft Office Compatibility Pack" in November 2006[3] so that earlier versions of Office would be able to work with new typefaces (such as Calibri) included with Office 2007.

Arsenal found 67 Office documents on CDs 11 and 17, purportedly last saved in 2002 and 2003, which contained references[4] to Calibri. It is not possible that these 67 Office documents were last saved in 2002 and 2003 as Calibri was not available then. It is also not possible that CDs 11 and 17 were burned in 2003 (which according to CD metadata they were, see section V below) because they contain these 67 documents which reference Calibri. It should be noted that Calibri is the default font of Office 2007[5] and references to it can be found in Office 2007 documents, even if no visible characters appear as such.

Exhibit B, attached to this report, contains a detailed listing of these 67 Office documents.

IV. PowerPoint XML Analysis

Arsenal searched the 337 Office documents found on CDs 11, 16, and 17 for references to XML (Extensible Markup Language) and found them in 9 PowerPoint documents on CDs 11 and 17. The presence of XML in Microsoft Office documents created before 2007 is unusual.

[2] While beta versions were released earlier than mid 2006, they were only released to testers and lacked significant functionality. See http://en.wikipedia.org/wiki/Microsoft_Office_2007 (Accessed March 21, 2012)

[3] http://office.microsoft.com/en-us/downloads/CD010060208.aspx (Accessed March 21, 2012)

[4] These references (87 total) are embedded inside the documents - e.g. in the Word documents, they are in Word's 1Table stream. These references can be found by searching each document for "Calibri" (in Unicode) using a hex editor or computer forensics software.

[5] http://en.wikipedia.org/wiki/Calibri (Accessed March 21, 2012)

Arsenal found 1,692 Zip containers[6] inside these 9 PowerPoint documents which were related to XML. Once the Zip containers were decompressed, Arsenal found 6,274 references to Office Open XML schemas which were finalized in late 2006[7]. The references themselves contain the string "2006" - for example, "http://schemas.openxmlformats.org/drawingml/2006/main". The first version of Microsoft Office which referred to these schemas was Office 2007.

Arsenal researched the domain "openxmlformats.org" and found that both current and cached[8] WHOIS records indicated it was not registered until October 25, 2005. Arsenal also found that openxmlformats.org was not assigned a name server or IP address until October 27, 2005[9].

Office and file system metadata indicates that all 9 of these PowerPoint documents were last saved in February 2003. It is not possible for these documents to have been last saved in 2003 because they contain references to XML schemas introduced in Office 2007. Arsenal considers all Office and file system metadata on CDs 11 and 17 to be unreliable due to the existence of these 9 sets of forged last saved dates.

Details on these 9 PowerPoint documents:

Filename	EK-B TERTİPLENME PLANI.ppt
Full Path	CD_11\(1) 030305_2350\2002-2003\Jandarma \İSTANBUL BÖLGE\EYLEM PLANLARI\CARSAF EYLEM PLANI\EK-B TERTİPLENME PLANI.ppt
Attached	Exhibit E
CD Created	03/05/03 11:50:42PM
File Created	02/19/03 09:45:32PM
File Last Saved	02/19/03 09:45:32PM

[6] Using Digital Detective's Blade v1.9 & customized ZIP Archive profile ("File Length/Data Boundary/Minimum Length" of 1 byte, deselected "Start / End of File/File Header/Sector Boundaries Only")

[7] http://www.ecma-international.org/publications/standards/Ecma-376.htm (Accessed March 21, 2012)

[8] Cached June 22, 2006, attached as Exhibit C

[9] See Exhibit D

PowerPoint Created	02/17/03 08:54:19PM
PowerPoint Last Saved	02/19/03 09:45:32PM
Zip Containers	24
References to 2006	84
Sample Reference Attached As	Exhibit F

Filename	EK-D HEDEF BÖLGE KROKİSİ.ppt
Full Path	CD_11\(1) 030305_2350\2002-2003\Jandarma \İSTANBUL BÖLGE\EYLEM PLANLARI\CARSAF EYLEM PLANI\EK-D HEDEF BÖLGE KROKİSİ.ppt
Attached	Exhibit G
CD Created	03/05/03 11:50:42PM
File Created	02/19/03 10:57:14PM
File Last Saved	02/19/03 10:57:14PM
PowerPoint Created	02/18/03 07:48:43PM
PowerPoint Last Saved	02/19/03 10:56:46PM
Zip Containers	12
References to 2006	42
Sample Reference Attached As	Exhibit H

Filename	EK- D HEDEF BÖLGE KROKİSİ.ppt
Full Path	CD_11\(1) 030305_2350\2002-2003\Jandarma \İSTANBUL BÖLGE\EYLEM PLANLARI\SAKAL EYLEM PLANI\EK- D HEDEF BÖLGE KROKİSİ.ppt
Attached	Exhibit I
CD Created	03/05/03 11:50:42PM

File Created	02/18/03 10:44:21PM
File Last Saved	02/18/03 10:44:21PM
PowerPoint Created	02/15/03 08:13:06PM
PowerPoint Last Saved	02/18/03 10:30:31PM
Zip Containers	8
References to 2006	27
Sample Reference Attached As	Exhibit J

Filename	EK-B TERTİPLENME PLANI.ppt
Full Path	CD_11\(1) 030305_2350\2002-2003\Jandarma \İSTANBUL BÖLGE\EYLEM PLANLARI\SAKAL EYLEM PLANI\EK-B TERTİPLENME PLANI.ppt
Attached	Exhibit K
CD Created	03/05/03 11:50:42PM
File Created	02/19/03 09:42:50PM
File Last Saved	02/19/03 09:42:50PM
PowerPoint Created	02/15/03 07:32:19PM
PowerPoint Last Saved	02/19/03 09:42:58PM
Zip Containers	28
References to 2006	97
Sample Reference Attached As	Exhibit L

Filename	KARADENİZ TEHDİT DEĞERLENDİRMESİ.ppt
Full Path	CD_11\(1) 030305_2350\2002-2003\KARADENİZ TEHDİT DEĞERLENDİRMESİ.ppt

Attached	Exhibit M
CD Created	03/05/03 11:50:42PM
File Created	02/25/03 06:46:10PM
File Last Saved	02/25/03 06:46:10PM
PowerPoint Created	12/03/97 06:22:14PM
PowerPoint Last Saved	02/25/03 06:46:09PM
Zip Containers	1548
References to 2006	5774
Sample Reference Attached As	Exhibit N

Filename	EK-B TERTİPLENME PLANI.ppt
Full Path	CD_17\(1) 030304_2351\CARSAF EYLEM PLANI\EK-B TERTİPLENME PLANI.ppt
Attached As	Exhibit O
CD Created	03/04/03 11:52:02PM
File Created	02/19/03 09:45:32PM
File Last Saved	02/19/03 09:45:32PM
PowerPoint Created	02/17/03 08:54:19PM
PowerPoint Last Saved	02/19/03 09:45:32PM
Zip Containers	24
References to 2006	84
Sample Reference Attached As	Exhibit P

Filename	EK-D HEDEF BÖLGE KROKİSİ.ppt

Full Path	CD_17\(1) 030304_2351\CARSAF EYLEM PLANI\EK- D HEDEF BÖLGE KROKİSİ.ppt
Attached As	Exhibit Q
CD Created	03/04/03 11:52:02PM
File Created	02/19/03 10:57:14PM
File Last Saved	02/19/03 10:57:14PM
PowerPoint Created	02/18/03 07:48:43PM
PowerPoint Last Saved	02/19/03 10:56:46PM
Zip Containers	12
References to 2006	42
Sample Reference Attached As	Exhibit R

Filename	EK- D HEDEF BÖLGE KROKİSİ.ppt
Full Path	CD_17\(1) 030304_2351\SAKAL EYLEM PLANI\EK- D HEDEF BÖLGE KROKİSİ.ppt
Attached As	Exhibit S
CD Created	03/04/03 11:52:02PM
File Created	02/18/03 10:44:21PM
File Last Saved	02/18/03 10:44:21PM
PowerPoint Created	02/15/03 08:13:06PM
PowerPoint Last Saved	02/18/03 10:30:31PM
Zip Containers	8
References to 2006	27
Sample Reference Attached As	Exhibit T

Filename	EK-B TERTİPLENME PLANI.ppt
Full Path	CD_17\(1) 030304_2351\SAKAL EYLEM PLANI\EK-B TERTİPLENME PLANI.ppt
Attached As	Exhibit U
CD Created	03/04/03 11:52:02PM
File Created	02/19/03 09:42:50PM
File Last Saved	02/19/03 09:42:50PM
PowerPoint Created	02/15/03 07:32:19PM
PowerPoint Last Saved	02/19/03 09:42:58PM
Zip Containers	28
References to 2006	97
Sample Reference Attached As	Exhibit V

V. CD Metadata Analysis

CD metadata indicates that CD 11 was created on March 5, 2003, CD 16 on October 14, 2003, and CD 17 on March 4, 2003. CDs 11 and 17 have a single track, which means they were written to in one "session." It is not possible for CDs 11 and 17 to have been created in March 2003 as they contain documents that reference XML schemas and Calibri which were not introduced until Office 2007.

VI. Conclusion

Arsenal has concluded that dates and times related to at least 76 documents found on CDs 11 and 17 have been forged. Arsenal has also concluded that dates and times related to the creation of CDs 11 and 17 have been forged. It is simply not possible that documents purportedly last saved and subsequently burned to CD in 2003 would contain references to XML schemas and the Calibri typeface, which were not introduced until Office 2007. The earliest that CDs 11 and 17 could have been created is mid 2006. Arsenal has serious concerns about the authenticity of all the documents on CDs 11 and 17 due to the evidence tampering that has been uncovered thus far. Our analysis of CDs 11, 16, and 17 is ongoing.