

Çetin Doğan
T.C. İSTANBUL 10. AĞIR CEZA MAHKEMESİ
2010/283

Başlangıç Raporu
21 Mart 2012



I. Giriş

Ben, hukuk firmaları, şirketler ve hükümet kuruluşları için adli bilişim çalışmalarını yürüttüğüm Arsenal Danışmanlık'ın ("Arsenal") Genel Müdürüyüm. Emniyet ve özel sektörde on yıldan fazla adli bilişim tecrübesine sahip bulunmaktayım. Ayrıca, Bunker Hill Community College'da part-time öğretim üyesiyim ve Computer Security Institute'da sekiz sene öğretim görevlisi olarak çalıştım. Gerçek ve doğru özgeçmişim bu rapora Ek A olarak eklenmiştir.

Arsenal Danışmanlık A.Ş. ("Arsenal") 15 Şubat 2012'de Çetin Doğan'ı temsil eden Avukat Hüseyin Ersöz ile bir ceza konusuyla ilgili olarak adli bilişim danışmanlık hizmetleri temini için sözleşme yapmıştır. Spesifik olarak, Avukat Ersöz, "CD 11", "CD 16" ve "CD 17" olarak bilinen üç CD'deki Microsoft dokümanları ile ilgili şüpheli olabilecek konuların saptanması konusunda Arsenal'ın yardımını istemiştir.

Adli bilişim uzmanları elektronik medyanın içindeki, silinmiş alanlar dahil, tüm verileri muhafaza eden adli imajları temin ederler. Adli imajlar, her adli imajla ait olan (aynı zamanda dijital parmak izi olarak da bilinen) karma (hash) değerlerinin istenen herhangi bir zamanda hesaplanması suretiyle doğrulanabilmektedir. Arsenal'in analizleri, 11 Kasım 2011'de "Bilirkişiler" in 11, 16 ve 17 numaralı CDlerin Guidance Software'in Encase v6.15'ı kullanarak oluşturduğu adli imajları¹ üzerinden yapılmıştır.

II. İdari Özet

Arsenal 11 ve 17 numaralı CD'lerde bulunan en az 76 dokümanın tarih ve zamanlarında sahtecilik yapıldığı sonucuna varmıştır. Arsenal, aynı zamanda, 11 ve 17 numaralı CD'lerin oluşturma tarih ve zamanlarında sahtecilik olduğu sonucuna da varmıştır. 11 ve 17 numaralı CD'ler en erken 2006 ortasında oluşturulmuş olabilir. Arsenal, şu ana kadar saptadığı delillerde yapılan oynamalar nedeniyle, 11 ve 17 numaralı CD'lerdeki tüm dokümanların orijinalliği hakkında ciddi bir endişe taşımaktadır. 11, 16 ve 17 numaralı CD'ler üzerindeki analizlerimiz devam etmektedir.

¹ Arsenal, bu adli imajları EnCase v6.19.3.11 kullanarak doğrulamıştır.



III. Calibri Yazı Karakteri Analizi

Kamunun erişimine beta versiyonu 2006² ortasında, son haliyle ise Ocak 2007'de sunulan Microsoft Office ("Office") 2007, Calibri yazı karakterini ("Calibri") taşıyan ilk Office versiyonudur. Microsoft, Office 2007'ye dahil edilen (Calibri gibi) yeni yazı karakterlerinin Office'in daha eski versiyonlarında kullanımını mümkün kılmak için Kasım 2006'da "Microsoft Office Compatibility Pack"i piyasaya sürmüştür.³

Arsenal, 11 ve 17 numaralı CD'lerin içinde, son kayıtları 2002 ve 2003'de yapılmış gibi görünen ve Calibri referansları⁴ taşıyan 67 Office dokümanı bulmuştur. Bu 67 Office dokümanının son kayıt tarihlerinin 2002 ve 2003 olması mümkün değildir; zira o tarihlerde Calibri mevcut değildir. Aynı şekilde, Calibri referanslarını taşıyan 67 dokümanın bulunduğu 11 ve 17 numaralı CD'lerin 2003'de oluşturulmuş olması mümkün değildir. Calibri'nin Office 2007'nin varsayılan (default) yazı karakteri olduğu ve de Office 2007⁵ dokümanlarında görünen yazı karakterlerinin hiçbirisi Calibri olmasa dahi dokümanların Calibri referansları içerebileceği bilinmelidir.

Söz konusu 67 dokümanın detaylı listesini içeren Ek B, bu rapora eklenmiştir.

IV. PowerPoint XML Analizleri

Arsenal 11, 16 ve 17 numaralı CD'lerde bulunan 337 Office dokümanını XML (Extensible Markup Language) referansları için taramış ve 11 ile 17 numaralı CD'lerde bulunan 9 doküman içinde bu referanslara rastlamıştır. 2007'den önce oluşturulan Microsoft Office dokümanlarının içinde XML'lerin mevcudiyeti olağandışıdır.

² Beta sürümleri 2006 ortasından önce piyasaya sürülmüş ancak bu sürüm test amaçlı olup işlevsellikten yoksundur. Bkz. http://en.wikipedia.org/wiki/Microsoft_Office_2007 (Erişim tarihi: 21 Mart 2012)

³ <http://office.microsoft.com/en-us/downloads/CD010060208.aspx>

⁴ Bu referanslar (toplam 87 adet) dokümanların içine gömülmüş bir şekildedir—örneğin, Word dokümanlarında Word'ün Tablo sıralı karakter dizisinde bulunmaktadır. Bu referanslar, hex editor ya da bilgisayar adli bilişim yazılımı ile her dokümanın içinde (Unicode'da) "Calibri"nin aranması ile bulunabilir.

⁵ <http://en.wikipedia.org/wiki/Calibri> (Erişim tarihi 21 Mart 2012)



Arsenal, söz konusu 9 PowerPoint dokümanının içinde 1692 adet zip konteyneri bulmuştur. Zip konteynerlerinin çözülmesi (decompress) sonucunda Arsenal, 2006 sonlarında finalize edilen Office Open XML şemalarına⁷ ait 6274 adet referans bulmuştur. Bu referansların kendileri “2006” karakter dizisini içermektedir –Örneğin, <http://schemas.openxmlformats.org/drawingml/2006/main>. Bu şemalara referansta bulunan ilk Microsoft Office versiyonu, Ocak 2007’de piyasaya sürülen Office 2007’dir.

Arsenal, “openxmlformats.org” domain’ini de araştırmış ve hem mevcut, hem de ön bellekteki⁸ WHOIS kayıtlarına göre bu domain’in 25 Ekim 2005 tarihinden önce kayıtlı olmadığını saptamıştır. Arsenal aynı zamanda openxmlformats.org’a 27 Ekim 2005 tarihine kadar bir hizmet birimi ismi (name server) ya da IP adresi tahsis edilmediğini de tespit etmiştir⁸.

Office ve dosya sistem üst verileri bütün bu 9 PowerPoint dokümanlarının en son Şubat 2003’de kaydedildiğini göstermektedir. Bu dokümanların en son 2003’de kaydedilmiş olması mümkün değildir, çünkü bu dokümanlar Office 2007 ile birlikte sunulan XML şemalarına referanslar içermektedir. Son kayıt tarihlerindeki 9 grup sahteciliğin mevcudiyeti nedeniyle, Arsenal 11 ve 17 numaralı CDdeki tüm Office ve dosya sistem üst verilerini güvenilirmez addetmektedir.

Söz konusu 9 dokümana ait detaylar:

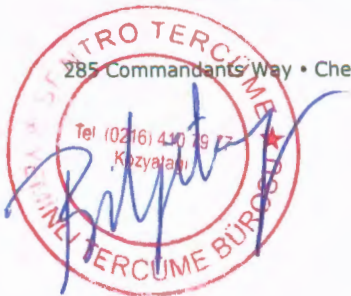
Dosya Adı	EK-B TERTİPLENME PLANI.ppt
Dosya Yolu (Full Path)	CD_11\1\030305_2350\2002-2003\Jandarma \İSTANBUL BÖLGE\EYLEM PLANLARI\CARSAF EYLEM PLANI\EK-B TERTİPLENME PLANI.ppt
EK	Ek E
CD Oluşturma	03/05/03 11:50:42PM
Dosya Oluşturma	02/19/03 09:45:32PM
Dosya Son Kayıt	02/19/03 09:45:32PM
PowerPoint Oluşturma	02/17/03 08:54:19PM
PowerPoint Son Kayıt	02/19/03 09:45:32PM

⁶ Digital Detective’s Blade v1.9 & customized ZIP Archive profile kullanılarak (“File Length/Data Boundary/Minimum Length” of 1 byte ve “Start / End of File/File Header/Sector Boundaries Only” seçimini kaldırarak)

⁷ <http://www.ecma-international.org/publications/standards/Ecma-376.htm>

⁸ 22 Haziran 2006’da kaydedilmiştir, Ek C olarak eklidir.

⁸ Ek D’ye bakınız



Zip Konteynerleri	24
2006'ya Referanslar	84
Örnek Referans İçin EK	Ek F

Dosya Adı	EK-D HEDEF BÖLGE KROKİSİ.ppt
Dosya Yolu (Full Path)	CD_11\\(1) 030305_2350\\2002-2003\\Jandarma \\İSTANBUL BÖLGE\\EYLEM PLANLARI\\CARSAF EYLEM PLANI\\EK-D HEDEF BÖLGE KROKİSİ.ppt
EK	Ek G
CD Oluşturma	03/05/03 11:50:42PM
Dosya Oluşturma	02/19/03 10:57:14PM
Dosya Son Kayıt	02/19/03 10:57:14PM
PowerPoint Oluşturma	02/18/03 07:48:43PM
PowerPoint Son Kayıt	02/18/03 07:48:43PM
Zip Konteynerleri	12
2006'ya Referanslar	42
Örnek Referans İçin EK	Ek H

Dosya Adı	EK- D HEDEF BÖLGE KROKİSİ.ppt
Dosya Yolu (Full Path)	CD_11\\(1) 030305_2350\\2002-2003\\Jandarma \\İSTANBUL BÖLGE\\EYLEM PLANLARI\\SAKAL EYLEM PLANI\\EK- D HEDEF BÖLGE KROKİSİ.ppt
EK	Ek I
CD Oluşturma	03/05/03 11:50:42PM



Dosya Oluşturma	02/18/03 10:44:21PM
Dosya Son Kayıt	02/18/03 10:44:21PM
PowerPoint Oluşturma	02/15/03 08:13:06PM
PowerPoint Son Kayıt	02/18/03 10:30:31PM
Zip Konteynerleri	8
2006'ya Referanslar	27
Örnek Referans İçin EK	Ek J

Dosya Adı	EK-B TERTİPLENME PLANI.ppt
Dosya Yolu (Full Path)	CD_11\1 030305_2350\2002-2003\Jandarma \İSTANBUL BÖLGESİ\EYLEM PLANLARI\SAKAL EYLEM PLANI\EK-B TERTİPLENME PLANI.ppt
EK	Ek K
CD Oluşturma	03/05/03 11:50:42PM
Dosya Oluşturma	02/19/03 09:42:50PM
Dosya Son Kayıt	02/19/03 09:42:50PM
PowerPoint Oluşturma	02/15/03 07:32:19PM
PowerPoint Son Kayıt	02/19/03 09:42:58PM
Zip Konteynerleri	28
2006'ya Referanslar	97
Örnek Referans İçin EK	Ek L

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



EK	Ek M
CD Oluşturma	03/05/03 11:50:42PM
Dosya Oluşturma	02/25/03 06:46:10PM
Dosya Son Kayıt	02/25/03 06:46:10PM
PowerPoint Oluşturma	12/03/97 06:22:14PM
PowerPoint Son Kayıt	02/25/03 06:46:09PM
Zip Konteynerleri	1548
2006'ya Referanslar	5774
Örnek Referans İçin EK	Ek N

Dosya Adı	EK-B TERTİPLENME PLANI.ppt
Dosya Yolu (Full Path)	CD_17\1) 030304_2351\CARSAF EYLEM PLANI\EK-B TERTİPLENME PLANI.ppt
EK	Ek O
CD Oluşturma	03/04/03 11:52:02PM
Dosya Oluşturma	02/19/03 09:45:32PM
Dosya Son Kayıt	02/19/03 09:45:32PM
PowerPoint Oluşturma	02/17/03 08:54:19PM
PowerPoint Son Kayıt	02/19/03 09:45:32PM
Zip Konteynerleri	24
2006'ya Referanslar	84
Örnek Referans İçin EK	Ek P



Dosya Adı	EK-D HEDEF BÖLGE KROKİSİ.ppt
Dosya Yolu (Full Path)	CD_17\1) 030304_2351\CARSAF EYLEM PLANI\EK-D HEDEF BÖLGE KROKİSİ.ppt
EK	Ek Q
CD Oluşturma	03/04/03 11:52:02PM
Dosya Oluşturma	02/19/03 10:57:14PM
Dosya Son Kayıt	02/19/03 10:57:14PM
PowerPoint Oluşturma	02/18/03 07:48:43PM
PowerPoint Son Kayıt	02/18/03 07:48:43PM
Zip Konteynerleri	12
2006'ya Referanslar	42
Örnek Referans İçin EK	Ek R

Dosya Adı	EK-D HEDEF BÖLGE KROKİSİ.ppt
Dosya Yolu (Full Path)	CD_17\1) 030304_2351\CARSAF EYLEM PLANI\EK-D HEDEF BÖLGE KROKİSİ.ppt
EK	Ek S
CD Oluşturma	03/04/03 11:52:02PM
Dosya Oluşturma	02/18/03 10:44:21PM
Dosya Son Kayıt	02/18/03 10:44:21PM
PowerPoint Oluşturma	02/15/03 08:13:06PM
PowerPoint Son Kayıt	02/18/03 10:30:31PM
Zip Konteynerleri	8
2006'ya Referanslar	27



Örnek Referans İçin EK	Ek T
Dosya Adı	EK-B TERTİPLENME PLANI.ppt
Dosya Yolu (Full Path)	CD_17\1) 030304_2351\SAKAL EYLEM PLANI\EK-B TERTİPLENME PLANI.ppt
EK	Ek U
CD Oluşturma	03/04/03 11:52:02PM
Dosya Oluşturma	02/19/03 09:42:50PM
Dosya Son Kayıt	02/19/03 09:42:50PM
PowerPoint Oluşturma	02/15/03 07:32:19PM
PowerPoint Son Kayıt	02/19/03 09:42:58PM
Zip Konteynerleri	28
2006'ya Referanslar	97
Örnek Referans İçin EK	Ek V

V. CD Üstveri Analizi

CD üstverilerine göre CD 11, 5 Mart 2003'de; CD16, 14 Ekim 2003'de; ve CD17, 4 Mart 2003'de oluşturulmuştur. 11 ve 17 numaralı CD'lerde tek trak mevcuttur, yani bu CD'ler tek bir oturumda yazılmıştır. 11 ve 17 numaralı CD'lerin Mart 2003'de oluşturulmuş olmaları mümkün değildir; zira bu CD'ler içinde Office 2007'ye kadar mevcut olmayan XML şemalarına ve Calibri'ye referans veren dokümanlar kayıtlıdır.

VI. Sonuç

Arsenal 11 ve 17 numaralı CD'lerde bulunan en az 76 dokümanın tarih ve zamanlarında sahtecilik yapıldığı sonucuna varmıştır. Arsenal, aynı zamanda, 11 ve 17 numaralı CD'lerin oluşturma tarih ve zamanlarında sahtecilik olduğu sonucuna da varmıştır. Son kayıtlarının yapılmasının akabinde 2003'de CD'ye kaydedilmiş gibi görünen dokümanların, Office 2007'den önce mevcut olmayan XML şemalarına ve Calibri yazı karakterlerine referanslar taşıması mümkün değildir. 11 ve 17 numaralı CDlerin oluşturulma tarihi, en erken 2006 ortası olabilir. Arsenal, şu ana kadar saptadığı delillerde yapılan oynamalar nedeniyle, 11 ve 17 numaralı



CD'lerki tüm dokümanların orijinallığı hakkında ciddi bir endişe taşımaktadır. 11, 16 ve 17 numaralı CD'ler üzerindeki analizlerimiz devam etmektedir.

Tam Adı

Mark Spence

İmza

(İmza)

Ünvan

Başkan

