

07 Mayıs 2010

T.C.  
BESİKTAS  
4. NO  
Müşahade No: 202 Besiktas-IST.

AKADEMİ

09 2714

Çeviri Hizmetleri • Translation Services

CIA Computer  
Investigative  
Associates

Bilgisayar Soruşturma Kurulu

**Danışmanlık hizmeti amacıyla hazırlanmıştır**

4 Mayıs 2010

Peter A. Biagetti, Esq.

Mintz., Levin, Cohn, Ferris, Glovsky and Popeo, P.C.

One Official Center

Boston, MA 02111

Yanıt : Çetin Doğan Konusu

Sayın Peter,

Bilgisayar Soruşturma Kurulunda müşterilerimizin erişiminin engellendiği belli başlı CD'ler, DVD'ler ve elektronik dosyalarda depolandığı iddia edilen verilerin doğruluğunun gözden geçirilmesi istenmiştir. Bu verilere müşterilerimizin erişimi sağlandığı anda daha kesin bir analizi üstlenmeyi istemekteyiz, ancak bu süre zarfında teyit ederiz ki:

- (1) Bir bilgisayar kullanıcısının, o bilgisayarda depolanan birçok bilgiyi; hatta görünen tarihe veya bilgisayardaki bir belgenin yazarına veya bilgisayarın IP adresine kadar değiştirmesi çok kolaydır.
- (2) Windows™ sistemleri dokümanlara ya da dosyalara genellikle kaynaklarının kolaylıkla tespit edilmesini sağlayan bilgiler koymazlar.
- (3) Sonuç olarak, her doküman veya dosya hakkında, herhangi bir kimsenin doğruluğundan veya bütünlüğünden emin olmadan önce, meydana geldiği tüm sistemin konteksti içerisinde incelenmelidir. Zira burada bu tür bir inceleme yapılmamaktadır, bu nedenle söz konusu dokümanlar ve belgeler; oluşturulma tarihleri, yazarı, şirketi, sistem orijini ve/veya kurucu bilgiler açısından tamamen yanlış olabilmektedir.

Daha belirgin olarak, tarafımızdan CD'ler, DVD'ler ve bilgisayar sistemlerinde depolanan verilerin ve ayrıca ve ayrıca belli Microsoft Office™ dosyalarında bulunan verilerin (üst veri olarak da adlandırılır) niteliği ve doğruluğu hakkında araştırma yapmamız ve ilgili soruları yanıtlamamız talep edilmiştir.



BESİKTAS (4) NOTER  
VEKİLİ  
SEMİH ÖZTÜRK



bilgi@akademitercume.com  
ankara@akademitercume.com

www.akademitercume.com



09274

Ancak bununla birlikte, tarafımıza orijinal dokümanların veya veri saklama ortamının erişimi sağlanmamıştır, bu nedenle bu zamana kadar depolanan verilerin niteliğine, belirli verilerin doğruluğuna ve Microsoft Office™ dokümanlarının niteliğine ve zaman damgasındaki tarihi incelemeye dair yapılan analizlerimiz sınırlı olmuştur. Bu yüzden bilgisayar dosyalarındaki ve bilgisayar sistemlerindeki tanımlayıcı bilgilerin, 'kullanıcı tarafından seçilebilir durumda', yani sistemin bir kullanıcısının herhangi bir bilgiyi herhangi bir anda değiştirebileceğinin vurgulanması önemlidir. Bilgisayar sisteminin kendisi tanımlayıcı verilerin kesin ve doğru olduğunu garanti etmemektedir.

**Tarih ve Zaman :** Bir bilgisayardaki tarihin ve zamanın veya belli bir dosyadaki tarihin ve zamanın doğru olmaması her zaman mümkündür. Yapıları itibarıyla bilgisayarlardaki tarih ve zaman kullanıcının ayarladığı şekildedir. Sistem çalışmaya başladığında kullanıcının BIOS (Temel Giriş-Çıkış Sistemi) ayarlarına girerek tarih ve zamanı istediği gibi değiştirmesi kolaydır. Bu işlem den itibaren de oluşturulan ya da erişilen her dosya değiştirilmiş tarih ve zamanı gösterecektir. Bu ayrıca daha eski bir bilgisayarın iç pili boşaltıldığında da meydana gelmektedir, şöyle ki ; dahili saat doğruluğunu kaybeder ve pil öldükten sonra, sistem çalışmaya başladığında kullanıcıdan yeni bir tarih ve zaman sorar , ya da sadece üretici tarafından gelişigüzel belirlenmiş tarihi kullanır. Bu tür tahrifatların üstesinden gelmenin teknik yolları vardır, örneğin ; - BIOS' u kilitlemek ve sistemi tarih ve zamanı, bir tarih sunucusundan (server) almaya zorlamaktır- ancak bu olayda bu tür bir korumanın sağlandığına dair herhangi bir kanıtın sunulduğunu görememekteyiz.

Elbette, bilgisayarda oluşturulan herhangi bir dosya, tarihi ve zamanı değiştirildikten sonra, değiştirilmiş olan tarih ve zamanı gösterecektir. Bu durum, o bilgisayarda oluşturulan Microsoft Office™ dokümanları, bilgisayara taranarak aktarılan dosyalar ya da bilgisayardan gönderilen e-postalar için de geçerli olmaktadır. (e-postalar konusunda; e-postaları işleyen bir sunucu (server) bulunmaktadır, sunucunun bilgisi dahilinde tarih ve zaman göstermesi için tarih ve zaman ayarlanabilmektedir) Benzer şekilde, sistemde oluşturulan CD'ler ve DVD'ler de değiştirilmiş zamanı gösterecektir. Sonuç olarak, tarih ve zaman bilgisinin tam doğruluğuna dair kesin bir soruşturma yürütmek için, enine boyuna inceleme yapılmalıdır, örneğin, sistem kayıt dosyaları, birbirine uymayan zaman dilimlerinde girişler olup olmadığına dair ve aynı zamanda ilgili dokümanların ve dosyaların tarih bilgisini destekleyecek diğer bağlamsal bilgilere dair incelenmelidir. *Orijinal bilgisayar sistemi ve sistemin uygun hukuki soruşturması bulunmadığında, herhangi bir dosyanın oluşturulduğu tarih ve zamanı sorumlu bir şekilde belirlemenin bir yolu yoktur.*

**Yazar :** Microsoft Office™ kullanılarak oluşturulan dokümanlarda saklanan üst veri , dokümanın 'Yazar' kaydını içermemektedir, ancak *bu dokümanı oluşturmak için bilgisayarı kullanan kişinin değil, sadece kullanılan bilgisayarın bilgisini göstermektedir.* Tarihlerde ve zamanda olduğu gibi bu 'Yazar' verisi kullanıcı tarafından , dokümanın üzerine sağ tıklanmak, 'Özellikler' seçilmek, 'Özet' sekmesine gidilmek ve yazarın adını değiştirmek suretiyle, ister doküman oluşturulurken isterse herhangi bir zaman sonra kolaylıkla değiştirilebilir. Aynı basit işlem, üst veride saklanan herhangi bir 'Şirket' verisini değiştirmek için de kullanılabilir.



Merkez İstanbul: Tel: (0212) 236 11 81 Fax: (0212) 236 80 04  
Ankara : Tel: (0312) 427 31 74 Fax: (0312) 427 61 04

www.akademitercume.com



bilgi@akademitercume.com  
ankara@akademitercume.com



09 2714

**Orijin :** Yukarıda açıklandığı gibi, birçok doküman ve belirli dosyalar 'yazar' veya 'şirket' olarak görülen kolayca değiştirilebilen veriler içermekteyken, çoğu, hangi bilgisayar sisteminden geldikleri bilgisini kaydetmezler. Dijital haklar yönetimi (DRM) yazılımının ya da donanımın bulunduğu, genellikle müzik ya da filmleri kapsayan birtakım ortam dosyaları gibi bazı istisnalar olmakla birlikte, herhangi bir ortamda çalınmak ya da oynatılmak üzere tasarlanmamış dosya ya da dokümanları içeren diskleri oluştururken kullanılan CD ya da DVD yazılımlarının hiçbiri bu DRM kontrollerini kullanmaz. Sonuç olarak, bir CD veya DVD'yi belli bir bilgisayar sistemiyle ilişkilendirmek genellikle o CD veya DVD'deki tüm dokümanların özelliklerinin incelenmesiyle gerçekleştirilmektedir ve yukarıda belirtildiği gibi, bu özelliklerin birçoğunun kullanıcı tarafından değiştirildiği akılda tutulmalıdır.

**IP Adresi :** Son olarak, dosyalarda belirtilen IP adresleri bile değiştirilebilmektedir. Genellikle dosyaların ve dokümanların oluşturulduğu sistemin IP adres bilgisi tutulmamaktadır. Belirli iş paylaşım yazılımları (örneğin Lotus Notes™ veya Microsoft Exchange™) iş akışı prosesinin bir parçası olarak bu bilgiyi içerebilir ancak yine de bu bilginin kullanıcı tarafından ayarlanmasına da izin vermektedirler. Sonuç olarak, hiçbir sorumlu denetçi, tüm destekleyici bilgisayar ağını (kayıt dosyaları, ağ trafiği aktarımlar-capture'ları,vs) gözden geçirmeden belirli bir dosyadan IP adresini kesinlikle kabul etmeyecektir. Bir kullanıcı için, bir sistemde gerçekteki IP adresinden başka olarak kendi istediği IP adresini gösteren dosya oluşturmak çok kolaydır.

**Sonuç :** Bilgisayar Soruşturma Kurulunun görüşüne göre; orijinal (ya da orijinal gibi görülen) sistemin yetkili bir hukuki analiz uzmanı tarafından incelenmemesi durumunda, herhangi bir bilgisayar dosyasında, dokümanlardaki üst verilerin veya zaman damgasındaki tarihlerin doğruluğu şüphelidir ve gerçek olarak kabul edilemez.

Saygılarımla,

John D. Tessel, CISSP

Teknolojiden Sorumlu Başkan  
Bilgisayar Tahkikat Kurumu (CIA)



Bu tercüme aslına uygun  
olarak .....'dan .....'ya  
tarafından çevrilmiştir.  
Yeminli Tercüman

Ayla Tıgılı

Bu tercüme yeminli tercümanımız  
Ayla Tıgılı tarafından  
yapılmıştır.

