

T.C.  
BOĞAZIÇI ÜNİVERSİTESİ  
MÜHENDİSLİK FAKÜLTESİ  
DEKANLIK

Sayı : B.30.2.BÜN.0.17.00.00/ 604.01.03 -1226

Konu :


23.11.2011

ÜLGEN HUKUK BÜROSU  
HAKAN BÜYÜK VEKİLLERİ  
AVK. CELAL ÜLGEN VE AVK. HÜSEYİN ERSÖZ

İlgi: 11.11.2011 tarihli yazı.

İlgi yazınız ile talep edilen "Hakan Büyük Dosyası Teknik Mütalaa" işi Fakültemiz Bilgisayar Mühendisliği Bölümü öğretim üyelerimizden Prof.Dr. M. Ufuk Çağlayan tarafından hazırlanarak ekte sunulmuştur.

Bilgilerinizi saygılarımla rica ederim.

  
Doç.Dr. Kunt Atalık  
Dekan Yardımcısı

## Teknik Rapor

Hakan Büyük vekilleri Avukat Celal Ülgen ve Avukat Hüseyin Ersöz tarafından, ekli belgeler ile beraber incelenmesini talep ettiği hususlar konusunda Bilgisayar Mühendisliği Bölümü'nden bir akademisyen seçilmesi ve talep ekinde yer alan sorular doğrultusunda bir teknik rapor hazırlanması Mühendislik Fakültesi Dekanlığı'ndan 11.11.2011 tarihinde talep edilmiştir. Mühendislik Fakültesi Dekanlığı ve Bilgisayar Mühendisliği Bölüm Başkanlığı tarafından bu amaçla görevlendirilen Prof. Dr. Mehmet Ufuk Çağlayan tarafından hazırlanan cevaplar, sorulan sorularla beraber bu Teknik Rapor'dadır.

Talep yazısı ekinde bir Flash Disk'de sunulan belgeler arasından sorulan soruları cevaplamak için kullanılan belgeler cevaplarda belirtilmiştir.

İncelenmesi talep edilen hususlarla ilgili olarak tarafımdan hazırlanan cevaplar, sorularla beraber aşağıdadır.

### Soru 1:

Kullanıcıların göremediği, özel yazılımlarla bulunan, dijital dosya üzerindeki oluşturma, değiştirme, yazar bilgisi vb üst veriler anlamına gelen metadeta bilgileri, bir dijital doküman için değiştirilemez bilgiler mi içermektedir? Üzerinde bilinçli olarak veri çıkarma, değiştirme vb işlemleri yapılmadığı sürece bu bilgilerin kendiliklerinden değişmeleri mümkün müdür? Türkiye ile saat farklılığı olan bir ülkeye gitmeniz, çölde veya kutuplarda bulunmanız, değerlere bugün veya 10 yıl sonra bakmanız metadeta bilgilerini herhangi bir değişikliğe uğratar mı?

### Cevap 1:

Kullanıcıların göremediği, özel yazılımlarla bulunan, dijital dosya üzerindeki oluşturma, değiştirme, yazar bilgisi vb üst veriler anlamına gelen metadeta bilgileri, dijital doküman CD-ROM, DVD-ROM gibi sadece okunabilen bir ortamda depolanmadığı sürece, dijital doküman için değiştirilemez bilgiler içermez. Dijital doküman hard disk, flash bellek vb yazılabilen bir ortamda depolanmışsa, meta data bilgilerinin dijital dokümanın neresinde yer aldığını ve formatını bilen uzman bir kişi, editör olarak da adlandırılabilir özel bir yazılım kullanarak, meta data bilgilerinden istediğini istediği bir şekilde değiştirebilir.

Üzerinde bilinçli olarak veri çıkarma, değiştirme vb işlemleri yapılmadığı sürece bu bilgilerin kendiliklerinden anlamlı bir şekilde değişmeleri mümkün değildir. Ancak çevre şartları, medya materyalinde bozulmalar olması gibi sebeplerle bu bilgiler bozulabilir ve okunamaz hale gelebilir.

Türkiye ile saat farklılığı olan bir ülkeye gidilmesi, çölde veya kutuplarda bulunulması, değerlere bugün veya 10 yıl sonra bakılması metadeta bilgilerini normal olarak herhangi bir değişikliğe uğratmaz. Mesela, resim içeren .jpg, .gif vb uzantılı dosyalarda böyle durumlarda metadeta bilgilerinde her hangi bir değişiklik olmaz. Metin, çizim, tablo vb bilgileri içeren .doc, .docx, .xls, .xlsx, .ppt, .pptx vb uzantılı dijital dosyaların metadeta bilgileri arasında dijital dosyaya en son erişim tarih ve zamanı, yani dosyanın en son okunma tarih ve zamanı, da olabilir, bu durumda meta datanın sadece erişim zaman ve tarihi bilgilerinde bir değişiklik olacak, diğer meta data bilgilerinde ise her hangi bir değişiklik olmayacaktır.



**Soru 2:**

Farklı klasörlerdeki Hash Değerleri aynı olan “jpg” uzantılı iki dijital dokümanın metadata bilgileri değişik ise, bu durum ne anlama gelmektedir? Aksi düşünüldüğünde yani metadata bilgileri aynı ancak Hash Değerleri farklı iki dijital doküman söz konusu ise bu durum ne ifade etmektedir? Bu hususların delil bütünlüğü ve sağlığı noktasındaki etkileri nedir?

**Cevap 2:**

Farklı klasörlerdeki hash değerleri aynı olan “jpg” uzantılı iki dijital dokümanın metadata bilgileri değişik olamaz çünkü hash değeri “jpg” uzantılı dijital dokümanın, metadata bilgileri dahil tümü dikkate alınarak hesaplanır.

Hash değerleri aynı olan “jpg” uzantılı iki dijital dokümanın metadata bilgileri değişik, yani birbirinden farklı ise, bu durum iki dokümandan birinin metadata bilgilerinde dosya hash değeri hesaplandıktan değişiklik olduğu anlamına gelmektedir. Doküman metadata bilgilerinde değişiklik medya hatalarından kaynaklandıysa metadata bilgisi genelde pek anlamlı olarak değişmiş olmayacaktır. Doküman metadata bilgilerinde değişiklik, Cevap 1’de anlatıldığı gibi, metadata bilgileri arasında dijital dosyaya en son erişim tarih ve zamanı varsa, dosya kazara ya da bilinçli olarak okunduğunda oluşabileceği gibi, konusunda uzman bir kişi tarafından da yapılmış olabilir.

Metadata bilgileri aynı ancak hash değerleri farklı iki dijital doküman söz konusu ise, bu durum dijital dokümanların birinde, metadata bilgileri hariç, dokümanın gövdesinde değişiklik olduğu anlamına gelmektedir. Örneğin, dijital dokümanda bir metin varsa, dokümanın gövdesini oluşturan metinde, dijital dokümanda bir resim varsa, dokümanın gövdesini oluşturan resimde değişiklik olmuştur.

Yukarıda anlatılan her iki durumda da, söz konusu dijital dokümanların **delil bütünlüğü ve sağlığının artık kaybolmuş olduğu varsayılmalıdır.**

**Soru 3:**

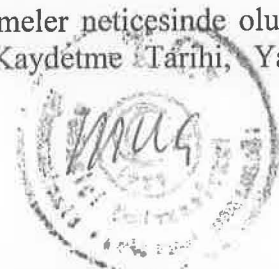
Aynı dijital medya için farklı tarihlerde yapılan incelemeler neticesinde oluşturulan raporlardaki Hash Değeri, Oluşturma Tarihi, Son Kaydetme Tarihi, Yazar vb bilgilerdeki farklılıkları delil bütünlüğü ve sağlığı noktasında değerlendiriniz?

**Cevap 3:**

Aynı dijital medya için farklı tarihlerde yapılan incelemeler neticesinde oluşturulan raporlardaki Hash Değeri, Oluşturma Tarihi, Son Kaydetme Tarihi, Yazar vb bilgiler, **inceleme dijital medyada her hangi bir değişiklik olmayacak bir şekilde yapıldığı takdirde aynı olmalıdır.**

İncelemenin her zaman, dijital medyada her hangi bir değişiklik olmayacak bir şekilde yapılması gerekir. Mesela, dijital medyanın orijinalini bozmadan bir kopyası alınarak kopya üzerinde inceleme yapılabilir. Dijital medyanın doğrudan orijinali üzerinde, medyanın orijinalini bozmadan, inceleme yapılabilmesi de teknik olarak mümkündür.

Aynı dijital medya için farklı tarihlerde yapılan incelemeler neticesinde oluşturulan raporlardaki Hash Değeri, Oluşturma Tarihi, Son Kaydetme Tarihi, Yazar vb



bilgilerin her hangi birinde **farklılıklar varsa, bu durum dijital medya içeriğinde değişiklik olduğu anlamına gelmektedir.** Burada, incelenen dijital medyanın Hash Değeri, Oluşturma Tarihi, Son Kaydetme Tarihi, Yazar vb bilgilerinin çarpıtılmadan, değiştirilmeden dürüst bir şekilde raporlara aktarıldığı ve raporlara yazılmış olduğu varsayılmaktadır.

Aynı dijital medya için farklı tarihlerde yapılan incelemeler neticesinde oluşturulan raporlardaki Hash Değeri, Oluşturma Tarihi, Son Kaydetme Tarihi, Yazar vb bilgilerinin her hangi birinde **farklılıklar varsa, bu durum dijital medya içeriğinde değişiklik olduğu anlamına geleceğinden, dijital medyanın delil bütünlüğü ve sağlığı artık kaybolmuştur.**

**Soru 4:**

İçeriğinde 12.05.2009 tarihine ait bir gazetenin scan edilmiş görüntüsü olan dijital bir verinin oluşturulma tarihi 19.04.2007 olabilir mi?

Dilekçe ekinde yer alan flash disk içinde müvekkilimize isnat edilen suçlamalara dayanak olarak kabul edilen dijital dokümanlar bulunmaktadır. Bu dijital dokümanların dosya yolları aşağıdaki gibidir:

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

Yukarıdaki soruya cevabınız olumsuz ise, dosya yolları verilen dijital dokümanların üst veri bilgileri ve içeriklerinden yola çıkarak bu durumun bir manipülasyonun göstergesi olduğu söylenebilir mi?

**Cevap 4:**

Dilekçe ekinde yer alan flash disk içindeki

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

dosyaları ve bu dosyaların metadata bilgileri tarafımdan incelenmiştir. Her iki dosya da JPEG formatında resim içeren dosyalardır. Bu dosyaların metadata bilgileri şöyledir.

- **BİLVANİS ÇİFTLİĞİ\ESKİŞEHİR\3-ISLAK İMZALILAR.zip\tara0059.jpg Dosyası**  
Dosya Tipi: JPG dosyası, Resolüsyon: 1700x2338 pixel, Dosya Büyüklüğü: 525 Kbyte, Dosyaya Son Yazılış Tarih ve Zamanı: 19.04.2007 18:58:00, Kamera Özellikleri: Yok

Dosya içinde bulunan resmin iki ayrı yerinde 12.05.2009 tarihi ve bir yerinde de 12 Mayıs 2009 tarihi açıkça görülmektedir.

- **BİLVANİS ÇİFTLİĞİ\ESKİŞEHİR\3-ISLAK İMZALILAR.zip\tara0053.jpg Dosyası**  
Dosya Tipi: JPG dosyası, Resolüsyon: 2550x3507 pixel, Dosya Büyüklüğü: 911 KByte, Dosyaya Son Yazılış Tarih ve Zamanı: 19.04.2007 18:49:14, Kamera Özellikleri: Yok



**Dosya içinde bulunan yazının tarihinin 12 Şubat 2008 olduğu açıkça görülmektedir.**

İçeriğinde 12.05.2009 tarihine ait bir gazetenin taranmış (scan edilmiş) görüntüsü olan dijital bir verinin oluşturulma tarihi hiç bir şekilde 12.05.2009 tarihinden önce, yani 19.04.2007 olamaz. Benzer şekilde, içeriğinde 12 Şubat 2008 tarihli bir yazı olan dijital bir verinin oluşturulma tarihi hiç bir şekilde 12 Şubat 2008 tarihinden önce, yani 19.04.2007 olamaz.

**Bu durum, dijital verileri içeren bilgisayar dosyalarının metadata bilgileri arasında bulunan son yazılma tarihinde Cevap 1’de izah edildiği şekilde değişiklik olduğu ve dosyaların delil bütünlüğü ve sağlığının artık kaybolmuş olduğu anlamına gelmektedir.**

**Soru 5:**

İçeriğinde 15.06.2005 tarih ve 5365 Sayılı Yasanın 7. Maddesi bulunan bir Kanun Tasarı Taslağı bulunan, “BİLVANİS ÇİFTLİĞİ\ESKİŞEHİR\EK-A 926 Teklifler.doc” dosya yolunda yer alan dijitalin oluşturulma ve son kayıt tarihlerinin 2003 yılı olması mümkün müdür? Cevabınız olumsuz ise bu hususun adli bilişim esasları çerçevesindeki açıklaması nedir?

**Cevap 5:**

“BİLVANİS ÇİFTLİĞİ\ESKİŞEHİR\EK-A 926 Teklifler.doc” dosyası metadata bilgileri tarafından incelenmiştir. Bu dosya Microsoft .doc formatında metin içeren bir dosyadır. Bu dosyanın metadata bilgileri şöyledir.

**Dosya Tipi:** Microsoft Office Word 97-2003 dosyası, **Dosya Büyüklüğü:** 91.648 Byte, **Dosyaya Son Yazılış Tarih ve Zamanı:** 05.04.2003 12:49:10,

İçeriğinde 15.06.2005 tarih ve 5365 Sayılı Yasanın 7. Maddesi bulunan bir Kanun Tasarı Taslağı’nın bulunduğu belirtilen, “BİLVANİS ÇİFTLİĞİ\ESKİŞEHİR\EK-A 926 Teklifler.doc” dosya yolunda yer alan dijitalin oluşturulma ve son kayıt tarihlerinin hiç bir şekilde 15.06.2005 tarihinden önce, yani 05.04.2003 olamaz.

**Bu durum, dijital veriyi içeren bilgisayar dosyasının metadata bilgileri arasında bulunan son yazılış tarihinde Cevap 1’de izah edildiği şekilde bir değişiklik olduğu ve dosyaların delil bütünlüğü ve sağlığının artık kaybolmuş olduğu anlamına gelmektedir.**

**Soru 6:**

“GUID” Değeri ne anlama gelmektedir? MSword dokümanlarının “GUID” Değerlerine bakılarak hangi bilgisayarda oluşturulduğunun tespiti mümkün müdür?

**Cevap 6:**

GUID (Globally Unique Identifier, yani Dünya Çapında Tek Kimlik Numarası) 128 bit (ikili), yani 16 byte boyunda oldukça büyük bir sayıdır ve genellikle 16’lık sayı sisteminde 0-9, A, B, C, D, E, F rakamları kullanılarak ve rakamlar 8, 4, 4, 4, 12’lik gruplar halinde 32 rakam yazılarak ifade edilmektedir.

Örnek: 2A2506E5-4F8B-12D0-9A0E-03F5E72C330F



GUID sayıları genellikle rastgele olarak üretilir ve GUID çok büyük bir sayı olduğundan iki GUID sayısının aynı olma ihtimali çok düşüktür. Farklı firmalar GUID sayılarını farklı amaçlar için kullanmaktadır. Veri tabanı sistemlerinde GUID kullanımını yaygındır.

Microsoft firması GUID sayılarını Windows işletim sisteminde ve Komponent Nesne Model (Component Object Model, COM) ile Dağıtık Komponent Nesne Model'e (Distributed Component Object Model, DCOM) uygun uygulama yazılımlarında yaygın olarak yazılım arayüzlerini, yazılım sınıflarını ve objelerini numaralayıarak birbirinden ayırmakta kullanmaktadır. Ayrıca GUID sayıları, bir bilgisayara kurulu Microsoft Office yazılımı tarafından Word, Excel, vb dokümanların metadata bilgileri içine de yerleştirilmektedir. GUID sayıların Microsoft yazılımları tarafından kullanım detayları oldukça karmaşık olduğundan burada daha fazla bir teknik bilgi verilmesine gerek olmadığı düşünülmüştür.

Eldeki bir Microsoft Word dokümanındaki, varsa GUID değerlerine bakılarak dokümanın hangi bilgisayarda oluşturulduğunun tespitiyle ilgili bir yöntem tarafımdan bilinmemektedir. Böyle bir yöntemin olup olmadığı literatürde ve İnternet kaynaklarında araştırılmış ve GUID değerlerine bakılarak bir dokümanın hangi bilgisayarda oluşturulduğunun tespitiyle ilgili bir yöntem rastlanmamıştır.

Microsoft Office yazılımı tarafından Word, Excel, vb dokümanların metadata bilgileri içine yerleştirilen GUID değerlerinin Microsoft firması tarafından belli bir bilgisayardaki Microsoft Office yazılımı ile eşleştirilerek Microsoft firmasının Microsoft Office yazılımı kurulum bilgilerine ve dolayısıyla Microsoft Office yazılımı kullanıcı kimliğine ulaşabileceği iddiaları İnternet kaynaklarında yer almış, Microsoft firması ise hiç bir durumda bu şekilde bir kullanıcı bilgisine erişmeye teşebbüs etmediğini beyan ederek bir Office ya da Word dokümanından gerektiğinde metadata bilgilerinin bir bölümünü yok etmeye yarayacak yazılım araçlarını dağıtmaya başlamıştır.

**Soru 7:**


“**World Document**” isminde bir “**File Type**” tipi var mıdır? Bir dijital verinin dosya yollarında boşluk bulunması teknik olarak mümkün müdür?

**Cevap 7:**

“**World Document**” isminde bir “**File Type**” tipi tarafımdan bilinmemektedir. “**World Document**” isminde bir “**File Type**” tipinin olup olmadığı literatürde ve İnternet kaynaklarında araştırılmış ve böyle bir **File Type**” tipine rastlanmamıştır.

Bir dijital verinin dosya yollarında, yani dosya adlarında, boşluk bulunması teknik olarak mümkündür ve yaygın olarak kullanılmaktadır.

Saygılarımla arz ederim. 22.11.2011

  
Prof. Dr. Mehmet Ufuk Çağlayan  
Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü  
Boğaziçi Üniversitesi, Bebek, İstanbul