MICROSOFT OFFICE WORD 2010 YAZILIMI İLE OLUŞTURULAN BELGELERDE ÜST VERİ (METADATA) ANALİZİ

Mehmet BAKAN, Murtaza TEMİZTÜRK, Ahmet SALUK ve Adem AŞKAR
Jandarma Genel Komutanlığı/Kriminal Daire Başkanlığı, Ankara, Türkiye
mehmetbakan82@gmail.com, murtitemiz@yahoo.com, ahmetsaluk@gmail.com, askaroglu@hotmail.com

ÖZET

Dijital dosyalarda üst veri (metadata) çoğu zaman kullanıcı farkında olmadan kaydedilmekte ve bu bilgiler adli bilişim analizleri açısından faydalı bir kaynak oluşturmaktadır. Farklı durumlarda farklı değişikliklere uğramasından dolayı üst verilerin analizi ayrıntılı bir inceleme gerektirmektedir. Rapor yazımında karar vermeye yardımcı olan bu verilerin doğru değerlendirilmesi güvenilir rapor verebilme açısından önemlidir. Dijital belgeler önemli üst veri bilgileri ihtiva etmektedir. Microsoft şirketinin geliştirdiği belge ve kelime işleme yazılımı olan "Microsoft Office Word" bu alanda kullanılan en yaygın yazılımlardandır. Yapılan çalışmada, MS Word 2010 yazılımı ile hazırlanmış bir dokümanın üst veri bilgilerinin yapısı incelenmiş, dosya üzerinde kullanıcının yaptığı işleme bağlı olarak değişebilen veya sabit kalan üst veri bilgilerinin tespit edilmesi için 18 farklı işlem sonucunda önemli olduğu değerlendirilen 6 adet üst veri bilgisinde meydana gelen değişiklikler izlenmiş ve tablo halinde sunulmuştur. Elde edilen sonuçlar kapsamında bu alanda inceleme yapan uzmanlar açısından dikkat edilmesi gereken hususlar ortaya konulmaya çalışılmıştır. Bu makale, ISDFS 2015 konferansına sunulan bildiriler içinden seçilmiş ve yayımlanmıştır.

Anahtar Kelimeler: Dijital belge, Metadata, Üst Veri, MS Word 2010.

METADATA ANALYSIS IN DOCUMENTS CREATED WITH MICROSOFT OFFICE WORD 2010

ABSTRACT

Generally metadata information of digital files is saved automatically without notice of the user and this data contains useful source for the computer forensic analyses. Metada information changes at different conditions, for that case it should be examined with details. It is important to analyse this useful information truely which helps giving reliable results at the prepared reports. Digital documents exit important metadata information in them. MS Office Word 2010 document metadata structure is examined by applying 18 different processes to the digital document. Six different metadata changes are monitored to determine changing and unchanging metadata according to the users' activities. The results have shown and evaluated. The important points are outlined for the experts who make examinations at this field.

Keywords: Digital document, Metadata, MS Word 2010

I. GİRİŞ (INTRODUCTION)

Metadata kavramı "Meta" ve "data" kelimelerinin birleşiminden oluşmaktadır. "Meta" kelimesi Yunanca kökenli olup, "birlikte, ile, sonrasında, yanında" anlamına gelmektedir [1]. Daha sonra Latince ve İngilizce kullanımında "bir şeyin ötesine geçme" anlamında kullanılmıştır. "Data" kelimesi ise Latince "verilen şey" anlamına gelen "datum" kelimesinin çoğul hali olup "ölçüm, deney, gözlemler sonucu elde edilen bilgi, veri" anlamına gelmektedir. Metadata ise "bir veri hakkında başka bir veri" yi içeren yapıdır [2].

Metadata bilgileri, kullanıldığı alana göre farklı verilerden oluşabilmektedir. Örneğin kütüphanecilik, metadata sisteminin en eski ve en yaygın olarak kullanıldığı alandır. Hatta metadata kavramının oluşumu, ilk kütüphanecinin bir raftaki el yazısıyla yazılmış kağıt tomarlarının fihristini yapmasına dayandırılmaktadır.

Kütüphanedeki kitap için metadata bilgileri kitabın adı, yazarı, basım yılı, konusu ve kitabın raftaki yerini belirten bilgiler gibi açıklayıcı bilgilerden oluşur [3]. Kütüphaneciler tarafından uzun süredir bilinen ve kullanılan metadata bilgilerinin oluşturulması ve yönetiminden, geçen yüzyıllarda bilgi/belge yönetimiyle uğraşan profesyonel kişiler sorumluydu. Günümüzde ise, bilgi kaynakları artan bir eğilimle dijital hale gelmiş, internet kullanımı yaygınlaşmış, organizasyonlar kendi iç bilgisayar ağları üzerinden veri paylaşımı yapmaya başlamıştır. Bu durum, istenilen veriye ulaşmak için verilerin dizinlenebilme ve filtrelenebilme ihtiyacını ortaya çıkarmıştır. Dolayısıyla dijital verilere metadata sınıflama bilgilerinin eklenmesi gerekliliği tekrar gündeme gelmiş, bu konu bilgi/belge yönetimiyle uğraşan profesyonel kişilerle sınırlandırılabilecek bir konu olmaktan çıkarak tüm bilgisayar kullanıcılarını ilgilendirir hale gelmiştir [4].

Bir bilişim sistemi ile ilgili adli soruşturma yürüten soruşturmacı, o sistemde meydana gelen ve güvenilir sonuçlara ulaşmaya yardımcı olabilecek mümkün olduğu kadar olayı yeniden canlandırma ihtiyacı duyar. Adli bilişim soruşturmacısı için cevaplanması gereken temel sorular 5N1K olarak da kısaltılan; kim, ne, nerede, ne zaman, nasıl, neden sorularıdır [5]. Metadata bilgileri bu soruları cevaplamada yardımcı olabilecek veriler içermektedir.

Metadata kullanıldığı alana göre farklılık gösterebilmektedir. Bu alan kütüphane veya müzede bulunan nesnelerin kayıtları olabileceği gibi dijital ortamda oluşturulan bir dosyanın kayıtları da olabilmektedir. Kullanıldığı alana göre metadata standartları oluşturulmuştur. Standartlar oluşturulurken yapı, kullanılacak değerler, içerik ve formata göre sınıflandırılarak her biri için farklı standartlar üretilmiştir. Bu standartlar örnekleri ile Tablo 1'de sunulmuştur.

Microsoft Word, merkezi Amerika Birleşik Devletleri'nde bulunan ve Bill Gates'in sahibi olduğu yazılım firması Microsoft tarafından Microsoft Windows ve Apple Macintosh işletim sistemleri tabanında çalışmak üzere yazılan ve dağıtımı yapılan bir belge ve kelime işleme yazılımıdır. İçinde bulunan detaylı metin biçimlendirme seçenekleri, ayrıntılı tablo, şekil ve grafik oluşturma başarıları nedeniyle, kendi türünde şu anda dünyadaki en popüler yazılımlardan biridir [7].

Microsoft, elektronik belge oluşturmada Office 2007'den itibaren kendi geliştirdiği Office Open XML dosya formatını kullanmaktadır. Open XML, XML tabanlı bir dosya sistemi olup, elektronik belgelerin (grafikler, sunumlar, çalışma kitaplar ve metinler gibi) saklanmasını amaçlar. Bu format 2008 yılında ISO/IEC 29500:2008 standardı olarak kabul görmüştür [8].

TABLO I. VERİ STANDARTLARININ TİPOLOJİSİ [6]

Tip standartları	Örnekler
Veri yapısı standartları (metadata öğeleri, dizileri, şemaları): Bunlar bir kaydı veya bilgi nesnesini oluşturan "kategoriler" veya "taşıyıcılar"ın verisidir.	MARC (Machine Readable Cataloging format), Encoded Archival Description (EAD), Dublin Core Metadata Element Set (DCMES).
Veri değeri standartları (kontrollü kullanılan kelimeler, kontrollü listeler): Bunlar metadata öğeleri veya veri yapısı standartlarında kullanılan terim, isim ve diğer değerlerdir.	Library of Congress Subject Headings (LCSH), Library of Congress Name Authority File (LCNAF), LC The saurus for Graphic Materials (TGM), Medical Subject Headings (MeSH).
Veri içeriği standartları (fihristleme kuralları ve kodlar): Bunlar metadata elementlerinde kullanılan verinin söz dizimi kuralları ve formatı için kullanılan ana hatlardır.	Anglo-American Cataloguing Rules (AACR), Resource Descriptionand Access (RDA), International Standard Bibliographic Description (ISBD).
Veri formatı/teknik değişim standartları (makine dilinde anlaşılabilir metadata standartları): Bu standart türü veri yapısı standardının makine dilince kodlanarak ortaya konmuş halidir.	MARC21, MARCXML, EAD XML DTD, METS, MODS, CDWA Lite XML schema, Simple Dublin Core XML schema, Qualified Dublin Core XML schema, VRA Core4.0 XML schema

Office Open XML doküman özelliklerini depolamak için "Dublin Core Metadata" elemanları setini ve "Dublin Core Metadata Initiative" (DCMI) metadata terimlerini kullanmaktadır. "Dublin Core", dokümanlara ait üst verilerin belirli bir standart içerisinde tanımlanması, kaydedilmesi, farklı uygulamalar ile kolay iletişim kurabilmesi ve yapısal değişikliklerin bir bütün olarak kendi içerisinde tutulabilmesini sağlayan bir alt yapı modelidir ve "ISO 15836:2003" standardı olarak kabul edilmiştir. "Dublin Core Metadata" elemanları seti 15 öğeden oluşmaktadır. Bunlar Title (başlık), Creator (oluşturan), Subject (konu), Description (açıklama), Publisher (yayımcı), Contributor (katkı sağlayan), Date (tarih), Type (tür), Format (format), Identifier (tanımlayıcı), Source (kaynak), Language (dil), Relation (ilişki), Coverage (kapsam), Rights (haklar) gibi öğelerdir [9].

II. GEREÇ VE YÖNTEM

Öncelikle Windows 7 işletim sistemine sahip bilgisayarda "MS Word 2010" yazılımı ile oluşturulan ".docx" uzantılı dosyanın başlık (header) bilgisi incelenerek dosyanın yapısı ortaya çıkarılmıştır. Dosya yapısında metadata bilgilerinin nerede yer aldığı tespit edilerek içeriğindeki veriler yorumlanmıştır.

Metadata bilgilerinden adli bilişim incelemesi açısından daha çok önem taşıyan 6 (altı)'sı üzerinde araştırma yapılmıştır. Bunlar: Yazan, son değiştiren, düzeltme numarası, oluşturma tarihi, son değiştirme tarihi, son yazdırma tarihidir.

Yapılan araştırmada 18 (on sekiz) adet işlem uygulanarak her işlem sonucunda 6 (altı) adet metadata bilgisinin herbirisinde meydana gelen değişiklikler tespit edilmiş ve sonuçlar tablo halinde sunulmuştur. Farklı kullanıcı ile yapılan işlem sonuçlarını görebilmek için bilgisayarda farklı kullanıcı hesapları oluşturulmuştur. Yapılan işlemler sırasıyla şunlardır.

i. Doğrudan yazılım çalıştırılarak yeni boş belge oluşturulmuştur.
ii. Bilgisayarda farenin sağ tuşuna basılarak yeni boş belge oluşturulmuştur.
iii. Yeni belge oluşturulup içerisine veri yazılarak kaydedilmiştir.
iv. Belge farklı kaydedilmiştir.
v. Belge farklı kullanıcı tarafından farklı kaydedilmiştir.
vi. Önceden oluşturulmuş belgenin içeriğinde değişiklik yapılarak kaydedilmiştir.
vii. Önceden oluşturulmuş belge farklı kullanıcı tarafından değiştirilmiş ve kaydedilmiştir.
viii. Belge Fat32 ve NTFS formatlı bölümler arasında kopyalanmıştır.
ix. Belge Fat32 formatlı bölüm içerisinde kopyalanmıştır.
x. Belge NTFS formatlı bölüm içerisinde kopyalanmıştır.
xi. Belge Fat32 ve NTFS formatlı bölümler arasında kopyalanmış, kopyalandığı bölümde içeriği değiştirilerek kaydedilmiştir.
xii. Belge yazdırılmış kaydedilmeden kapatılmıştır.
xiii. Belge yazdırılmış ve kaydedilmiştir.
xiv. Belge farklı kullanıcı tarafından yazdırılmış ve kaydedilmiştir.
xv. Belge içeriğinde değişiklik yapılarak yazdırılmış ve kaydedilmiştir.
xvi. Belge içeriğinde farklı kullanıcı tarafından değişiklik yapılarak yazdırılmış ve kaydedilmiştir.
xvii. Belge yazdırılmış ve farklı kaydedilmiştir.
xviii. Belge farklı kullanıcı tarafından yazdırılmış ve farklı kaydedilmiştir.

III. BULGULAR

A. MS Word 2010 Metadata Bilgileri

Oluşturulan ".docx" uzantılı dosya dosyanın yapısı Encase yazılımı ile incelenmiştir. Başlık (header) bilgisinin ASCII değeri olarak "PK", heksadesimal değeri olarak "50 4B 03 04" olduğu görülmüştür. Bu bilgiler bu dosyanın sıkıştırılmış yapıda olduğunu göstermektedir. Dosyanın uzantısı, sıkıştırılmış dosya uzantısı olan "zip" olarak değiştirilerek içeriğinin görüntülenebildiği tespit edilmiştir. Sıkıştırılmış yapıdaki ".docx" dosyası içerisindeki verilerin XML formatta olduğu ve belgeye ait metadata bilgilerinin "docProps" klasörü altındaki "core.xml" dosyasına kaydedildiği tespit edilmiştir. "core.xml" dosyası içerisinde yer alan metadata bilgilerini incelediğimizde şu bilgilerin bulunduğu görülmüştür. Başlık (Title), Konu (Subject), Yazan (Creator), Etiketler (Keywords), Açıklamalar (Descriptions), Son Değiştiren (Last Modified by), Düzeltme Numarası (Revision), Oluşturma Tarihi (Created), Son Değiştirme Tarihi (Modified), Son Yazdırma Tarihi (Last Printed).

Oluşturulan "docx" uzantılı dosyayı incelemek maksadıyla sıkıştırılmış yapıda olan dosyalar için Encase yazılımında kullanılan "File Mounter" scripti çalıştırılarak mount işlemi yapılmıştır. Bu işlem sonrasında "core.xml" dosyası, doküman görünümü seçilerek incelendiğinde mevcut olan metadata bilgileri XML yapıdaki sıra ile alt alta görülebilmiştir.

MS Word yazılımının kendi özellikleri kullanılarak da metadata bilgilerini görmek mümkündür. "Dosya" sekmesi altında yer alan "Bilgi" bölümünde görüntülenebilmektedir.

Ayrıca NTFS veya FAT formatlı bölümde MS Word dosyası üzerinde sağ tık yapılarak açılan pencerede "Özellikler" daha sonra "Ayrıntılar" sekmesi seçildiğinde "Kaynak" bölümünde metadata bilgileri görüntülenebilmektedir. MS Word dosyası doğrudan yazılım çalıştırılarak veya farenin sağ tuşuna basılarak oluşturulabilmektedir. Seçilen yönteme göre metadata verilerinin oluşum zamanı da değişmektedir. Farenin sağ tuşuna basılıp "Yeni" sekmesinden "Microsoft Word Belgesi" seçeneği seçilerek boş bir belge oluşturulduğunda, oluşan dosyanın boyutunun "0" (sıfır) olduğu ve metadata verilerinin kaydedildiği XML yapısının oluşmadığı görülmüştür. Boş belge açılıp içeriğinde değişiklik yapılarak kaydedilmesinden sonra metadata verilerinin oluştuğu tespit edilmiştir. "Başlat" menüsünden Microsoft Office klasörü altındaki "Microsoft Word 2010" sekmesine tıklayarak açılan belge içeriğinde değişiklik yapılmadan boş olarak kaydedilmesi durumunda dahi metadata verileri oluşmaktadır.

B. Yazan (Creator)
Yazan bilgisi belgeyi oluşturan anlamında kullanılmaktadır. Microsoft Office yazılımı kurulduktan sonra ilk çalıştırıldığında, kullanılmak istenilen kullanıcı adı ile baş harflerinin belirleneceği ekran karşımıza çıkmıştır. Farklı kullanıcı hesaplarında oturum açılarak yazılım ilk kez çalıştırıldığında da isim belirleme ekranının geldiği ve varsayılan ayar olarak oturum açılan hesap isminin yer aldığı görülmüştür.

Kullanılacak isim ve baş harfler bilgilerinin Windows kayıt defterinin

"HKEY_USERS\SID\Software\Microsoft \Office\Common\UserInfo"

anahtarında **"UserName"** ve **"UserInitials"** dizesinde yer alan kullanıcı isim bilgisi ve ilk harf bilgilerinden alındığı tespit edilmiştir. MS Office yazılımı ilk kez çalıştırıldığında gelen isim belirleme ekranında "Ad" ve "Baş harfler" bölümü değiştirilebilmektedir. Değiştirilmesi durumunda yeni yazılan "Ad" ve "Baş harfler" kayıt defterindeki "UserInfo" anahtarının "UserName" ve "UserInitials" dizesindeki değerleri değiştirmektedir. Değiştirilen "Ad" daha sonra oluşturulan Word belgelerinde "Yazan-Creator" olarak kaydedilmektedir. Aynı bilgisayarda farklı kullanıcı hesapları ile oturum açılması durumunda, oluşturulan belgelerin "Yazan" ismi oturum açılmış olan kullanıcı hesabının kayıt defterinin "UserInfo" anahtarındaki isim bilgilerini almaktadır. "Yazan" bilgisi incelemeci için belgeyi oluşturan kişi hakkında fikir vermesi açısından çok önemli bir ipucu olmakla birlikte "Yazan" bilgisinin üzerinde sağ tık yapıldığında burada yer alan bilgiyi değiştirme, silme veya farklı isim ekleme seçenekleri çıkmaktadır. Bu seçenekler kullanıldığında ise belgede bir değişiklik yapılmış olduğundan kaydetme işlemi yapılması durumunda son değiştiren kişi ismi ve tarihi kaydolmaktadır. Ancak bu işlem sadece belge üzerinde yapıldığından kayıt defterindeki ayarları değiştirmemektedir.

MS Word dosya üzerinde sağ tık yapılarak metadata bilgileri görüntülendiğinde, bu bölümden de "Yazan" bilgisi değiştirilebilmektedir. Bu bölümden "Yazan" bilgisi değiştirildiğinde "Son Değiştiren" ve "Son Değiştirme Tarihi" metadataları ile Windows kayıt defteri ayarları değişmemektedir. Dosya sisteminde dosyanın değişiklik tarihi güncellenmektedir.

C. Son Değiştiren (Last Modified by)
Belge içerisinde en son değişiklik yaparak kaydetme işlemi yapan kullanıcıya ait bilgidir. Belgeyi son kaydeden bilgisi, aktif olan kullanıcı hesabının kayıt defterindeki "UserInfo" anahtarının "UserName" dizesindeki değerden alınmaktadır. MS Office yazılımı özellikleri kullanılarak ya da dosya üzerinde sağ tık yapılarak metadata bilgilerinin görüntülendiği bölümden "Son Değiştiren" bilgisi değiştirilememektedir.

Ç. Oluşturma Tarihi
Oluşturma tarihi, oluşturulan boş MS Word belgesinin içeriğinde yapılan ilk değişiklik tarihini ve saatini ifade eden, oluşturma işleminin yapıldığı sistemden alınan zaman bilgisidir. İlk değişiklik yapıldıktan sonra kaydetme işlemi ile oluşmaktadır.

Metadata bilgilerinin yer aldığı "core.xml" dosyasının içeriği incelendiğinde; oluşturma tarih

"<dcterms:createdxsi:type="dcterms:W3CDTF" >2013-06-T11:07:00Z</dcterms:created>"

bilgisi olarak kaydedildiği görülmüştür. Burada yer alan "dcterms: created" ibaresi "Dublin Core" metadata standartlarına göre kullanılmış olan "created" yani "oluşturma tarihi" bilgisini "dcterms:W3CDTF" ibaresi ise yine söz konusu standarda göre kullanılan tarih zaman formatı olup "World Wide Web Consortium Datetime Format"ının kullanıldığını ifade etmektedir. "T" harfi "time" kelimesinin kısaltması olup zamanı ifade etmekte, "Z" ise "Zulu" yani GMT saat diliminin kullanıldığını göstermektedir.

MS Word yazılımı "core.xml" dosyasına tarih saat bilgilerini belgenin oluşturulduğu sistemin saat ayarlarını GMT olarak kaydetmektedir. Dosya, MS Word belgesinin yer aldığı sistemde açıldığında ise sistem ayarlarında kayıtlı saat dilimine göre görüntülenmektedir. MS Office yazılımı özellikleri kullanılarak ya da dosya üzerinde sağ tık yapılarak metadata bilgilerinin görüntülendiği bölümden "Oluşturma Tarihi" bilgisi değiştirilememektedir.

D. Son Değiştirme Tarihi (Modified)
Son değiştirme tarihi, MS Word dosyasında herhangi bir değişiklik yapılıp kaydetme işlemi gerçekleştirildiğinde sistemden alınan tarih saat bilgisini ifade etmektedir. "core.xml" dosyası içeriğinde görülen ve "modified" bölümünde yer alan tarih saat bilgileri "Son Değiştirme Tarihi"ne ait zaman bilgisidir. "Oluşturma Tarihi" bölümünde açıklanan aynı format burada da kullanılmaktadır. Dolayısıyla belge içeriğinde değişiklik yapılarak kaydedilen bilgisayarın saat ayarları, belgenin son değiştirme tarihi bilgisi için önem arz etmektedir.

MS Office yazılımı özellikleri kullanılarak ya da dosya üzerinde sağ tık yapılarak metadata bilgilerinin görüntülendiği bölümden "Son Değiştirme Tarihi" bilgisi değiştirilememektedir.

E. Düzeltme Numarası (Revision)
Düzeltme numarası, belgenin içeriğinde değişiklik yapılarak kaydedilmesi ile oluşan sayıdır. MS Word

yazılımının Dosya/ Bilgi/ Özellikler/ Gelişmiş Özellikler/ İstatistikler sekmesi altında görülebilmektedir. Belgede değişiklik yapıldığını göstermesi açısından önemlidir. Önceden oluşturulmuş MS Word belgelerinin önceki düzeltme numarası kaç olursa olsun dosya farklı kaydedildiğinde düzeltme numarasının "2" olarak değiştiği tespit edilmiştir. MS Office yazılımı özellikleri kullanılarak "Düzeltme Numarası" bilgisi değiştirilememektedir. MS Word dosyası üzerinde sağ tık yapılarak metadata bilgileri görüntülendiğinde, bu bölümden "Düzeltme Numarası" bilgisi değiştirilebilmektedir. Bu bölümden "Düzeltme Numarası" bilgisi değiştirildiğinde "Son Değiştiren" ve "Son Değiştirme Tarihi" metadataları değişmemektedir. Dosya sisteminde dosyanın değişiklik tarihi güncellenmektedir.

F. Son Yazdırma Tarihi (Last Printed)

Son yazdırma tarihi belgenin yazdırıldığı anda sistemden alınan tarih ve saati ifade etmektedir. "core.xml" dosyası içeriğinde görülen ve "Last Printed" bölümünde yer alan tarih saat bilgileri "Son Yazdırma Tarihi"ne ait zaman bilgisidir. "Oluşturma Tarihi" bölümünde açıklanan aynı format burada da kullanılmaktadır.

Yapılan çalışmada belge içeriğinde değişiklik yapıldıktan sonra belge yazdırılarak kaydetme işlemi yapıldığında bu bilginin güncellendiği, diğer durumlarda, yani belge içeriğinde değişiklik yapılmadan yazdırılması veya değişiklik yapılmadan yazdırılıp kaydedilmesi durumlarında ise son yazdırma tarihinin güncellenmediği tespit edilmiştir. MS Office yazılımı özellikleri kullanılarak ya da dosya üzerinde sağ tık yapılarak metadata bilgilerinin görüntülendiği bölümden "Son Yazdırma Tarihi" bilgisi değiştirilememektedir.

G. MS Word Dosyasında Yapılan Testler ve Sonuçları

MS Word dosyasının 6 (altı) metadata bilgisinde meydana gelen değişiklikleri görmek için 18'er adet test yapılmıştır. Test sonuçları Tablo 2'de sunulmuştur.

Tablodaki ikinci işlem olan, farenin sağ tuşuna basılıp "Yeni" seçeneği ve ardından "Microsoft Word Belgesi" seçeneği seçilerek boş bir belge oluşturulması durumunda, belgenin boyutunun "0" (sıfır) olduğu ve metadata verilerinin kaydedildiği XML yapısının oluşmadığından dolayı bu işlemde metadata bilgileri oluşmamış olarak belirtilmiştir.

IV. SONUÇ VE TARTIŞMA

Bu çalışmada dijital bir belge ile ilgili olarak meydana gelebilecek 18 senaryo üzerinden işlem yapılarak 6 adet metadata bilgisinde meydana gelen değişim sonuçları sunulmuştur. Yapılacak incelemelerde bu sonuçlara bakılarak kanaat oluşturulabilecektir. "Yazan" yani belgeyi ilk oluşturan bilgisi, belge ilk oluşturulduktan sonra yapılan işlemlerde sabit kalmış ve değişmemiştir. Ancak MS Word yazılımı ile bu bilginin değiştirilebildiği görülmüştür. İnceleme esnasında "yazan" bilgisinden yola çıkarak kesin kanaate varılmamalıdır. Ayrıca belgenin tespit edildiği sistem mevcut ise Windows kayıt defterindeki "UserInfo" anahtarında yer alan bilgiler kontrol edilmelidir.

Metadata bilgilerinin kaydedildiği "core.xml" dosyası içerisindeki oluşturma, son değiştirme ve yazdırma tarihleri belge üzerinde bu işlemlerin yapıldığı andaki sistemin tarih saat bilgisi GMT saat dilimine dönüştürülmesi ile oluşmaktadır. Dolayısıyla, "core.xml" dosyasındaki tarih saat bilgisinden yola çıkarak inceleme yapılması durumunda, belge üzerinde bu işlemlerin yapıldığı andaki sistemin kayıtlı saat dilim ayarı ve saat bilgisi dikkate alınmalı, buna göre saat bilgisine ekleme veya çıkarma yapılarak gerçek zaman bulunmalıdır.

Önceki düzeltme numarası kaç olursa olsun, MS Word dosyası farklı kaydedildiğinde farklı kaydedilen belgenin düzeltme numarası 2'den başlamaktadır. İnceleme esnasında bu numara 2 görüldüğünde dosya ismi değiştirilerek veya değiştirilmeden farklı kaydedilme işlemi yapılmış olabileceği göz önünde bulundurulmalıdır. Son yazdırma tarihi her ne kadar belgenin yazdırılmış olduğu bilgisini verse de güncellenmiş olmayabilir. Dolayısıyla bu tarih ve saat bilgisinden yola çıkarak kesin kanaatte bulunulmamalıdır. MS Word dosyalarında yer alan metadata bilgileri incelemelerde bazı bilgi ve ipuçları sunuyor olmasına karşı bu bilgilerin bazı yöntemler ve özel yazılımlar ile değiştirilebildiğinden dolayı bilgilerin gerçekliği konusunda emin olunmamalıdır. Sistemde yüklü ve kaldırılmış yazılım bilgileri de incelenerek bu türde bir yazılım kullanılmış mı tespit edilmelidir.

Kayıt defterindeki bilgiler, kullanıcı isimleri, tarih saat ayarları, işletim sisteminin ve MS Office yazılımının kurulma tarihi gibi uzmanlık raporuna yazılacak kanaati destekleyici veriler mutlaka dikkate alınarak değerlendirilmelidir.

V. KAYNAKLAR

[1] Purohit A.T., Hemrajani N., Dave R., "Role of metadata in cyber forensic and status of Indian cyber law, International Journal of Computer Technology and Applications", Sept-Oct 2011, Vol 2 (5), pp.1582-1588.

[2] Küçük M.E., Al U., "Metada kavramı", Bilgi Dünyası, 2001, 2(2), s:169-187.

Tablo II. MS Word 2010 Dosyasında Yapılan Test Sonuçları

Yapılan İşlem	Metadata					
	Yazan	**Son Değiştiren**	**Oluşturma Tarihi**	**Son Değiştirme Tarihi**	**Son Yazdırma Tarihi**	**Düzeltme Numarası**
Doğrudan Yazılım Çalıştırılarak Yeni Boş Belge Oluşturuldu	Windows kayıt defterinde "UserName" dizesindeki kayıtlı değeri aldı.	Windows kayıt defterinde "UserName" dizesindeki kayıtlı değeri aldı.	Belge oluşturulduğu andaki sistemin tarih ve saatini aldı.	Belgenin kaydedildiği andaki sistemin tarih ve saatini aldı.	-	1 oldu.
Bilgisayarda Farenin Sağ Tuşuna Basılarak Yeni Boş Belge Oluşturuldu	-	-	-	-	-	-
Yeni Belge Oluşturulup İçerisine Veri Yazılarak Kaydedildi	Windows kayıt defterinde "UserName" dizesindeki kayıtlı değeri aldı.	Windows kayıt defterinde "UserName" dizesindeki kayıtlı değeri aldı.	Doğrudan yazılım ile oluşturulan belge oluşturulduğu andaki sistemin tarih ve saatini aldı. Sağ tıklayarak oluşturulan belge içerisine ilk verinin yazıldığı andaki sistemin tarih ve saatini aldı.	Belgenin kaydedildiği andaki sistemin tarih ve saatini aldı.	-	Doğrudan yazılım ile oluşturulan "1", sağ tıklayarak oluşturulan "2" oldu.
Belge Farklı Kaydedildi	Değişmedi.	Değişmedi.	Belgenin farklı kaydedildiği andaki sistemin tarih ve saatini aldı.	Belgenin farklı kaydedildiği andaki sistemin tarih ve saatini aldı.	-	2 oldu.
Belge Farklı Kullanıcı Tarafından Farklı Kaydedildi	Değişmedi.	Windows kayıt defterinde "UserName" dizesindeki kayıtlı değeri aldı.	Belgenin farklı kaydedildiği andaki sistemin tarih ve saatini aldı.	Belgenin farklı kaydedildiği andaki sistemin tarih ve saatini aldı.	-	2 oldu.
Önceden Oluşturulmuş Belgenin İçeriğinde Değişiklik Yapılarak Kaydedildi	Değişmedi.	Değişmedi.	Değişmedi.	Belgede değişiklik yapıldıktan sonra kaydedildiği andaki sistemin tarih ve saatini aldı.	-	Kaydetme işleminden sonra 1 arttı.
Önceden Oluşturulmuş Belge Farklı Kullanıcı Tarafından Değiştirildi ve Kaydedildi	Değişmedi.	Windows kayıt defterinde "UserName" dizesindeki kayıtlı değeri aldı.	Değişmedi.	Belgede değişiklik yapıldıktan sonra kaydedildiği andaki sistemin tarih ve saatini aldı.	-	Kaydetme işleminden sonra 1 arttı.
Belge Fat32 ve NTFS Formatlı Bölümler Arasında Kopyalandı	Değişmedi.	Değişmedi.	Değişmedi.	Değişmedi.	-	Değişmedi.
Belge Fat32 Formatlı Bölüm İçerisinde Kopyalandı	Değişmedi.	Değişmedi.	Değişmedi.	Değişmedi.	-	Değişmedi.
Belge NTFS Formatlı Bölüm İçerisinde Kopyalandı	Değişmedi.	Değişmedi.	Değişmedi.	Değişmedi.	-	Değişmedi.

Belge Fat32 ve NTFS formatlı Bölümler Arasında Kopyalandı, Kopyalandığı Bölümde İçeriği Değiştirilerek Kaydedildi	Değişmedi.	Değişmedi.	Değişmedi.	Belgede değişiklik yapıldıktan sonra kaydedildiği andaki sistemin tarih ve saatini aldı.	-	Kaydetme işleminden sonra 1 arttı.
Belge Yazdırıldı Kaydedilmeden Kapatıldı	Değişmedi.	Değişmedi.	Değişmedi.	Değişmedi.	Oluşmadı.	Değişmedi.
Belge Yazdırıldı ve Kaydedildi	Değişmedi.	Değişmedi.	Değişmedi.	Değişmedi.	Oluşmadı.	Değişmedi.
Belge Farklı Kullanıcı Tarafından Yazdırıldı ve Kaydedildi	Değişmedi.	Değişmedi.	Değişmedi.	Değişmedi.	Oluşmadı.	Değişmedi.
Belge İçeriğinde Değişiklik Yapılarak Yazdırıldı ve Kaydedildi	Değişmedi.	Değişmedi.	Değişmedi.	Belgede değişiklik yapıldıktan sonra kaydedildiği andaki sistemin tarih ve saatini aldı.	Belgenin yazdırıldığı andaki sistemin tarih ve saatini aldı.	Kaydetme işleminden sonra 1 arttı.
Belge İçeriğinde Farklı Kullanıcı Tarafından Değişiklik Yapılarak Yazdırıldı ve Kaydedildi	Değişmedi.	Windows kayıt defterinde "UserName" dizesindeki kayıtlı değeri aldı.	Değişmedi.	Belgede değişiklik yapıldıktan sonra kaydedildiği andaki sistemin tarih ve saatini aldı.	Belgenin yazdırıldığı andaki sistemin tarih ve saatini aldı.	Kaydetme işleminden sonra 1 arttı.
Belge Yazdırıldı ve Farklı Kaydedildi	Değişmedi.	Değişmedi.	Belgenin farklı kaydedildiği andaki sistemin tarih ve saatini aldı.	Belgenin farklı kaydedildiği andaki sistemin tarih ve saatini aldı.	Belgenin yazdırıldığı andaki sistemin tarih ve saatini aldı.	2 oldu.
Belge Farklı Kullanıcı Tarafından Yazdırıldı ve Farklı Kaydedildi	Değişmedi.	Windows kayıt defterinde "UserName" dizesindeki kayıtlı değeri aldı.	Belgenin farklı kaydedildiği andaki sistemin tarih ve saatini aldı.	Belgenin farklı kaydedildiği andaki sistemin tarih ve saatini aldı.	Belgenin yazdırıldığı andaki sistemin tarih ve saatini aldı.	2 oldu.

[3] Dağdaş Y., Elektronik Belge Tanımlaması ve Uluslararası Elektronik Belge Tanımlama Standartları, Marmara Üniversitesi Türkiyat Araştırmaları Enstitüsü, Yüksek Lisans Tezi, 2005.

[4] What is metadata http://dublincore.org/documents usageguide, (Erişim Tarihi:15 Şubat 2015).

[5] Salama U., Varadharajan V. and Hitchens M., "Metadata based forensic analysis of figital information in the web", Annual Symposıum on Informatıon Assurance & Secure Knowledge Management, pp. 9-15, JUNE 5-6, 2012, Albany, NY.

[6] Baca M. (Ed.), Introduction to Metadata, Gilliland A.J., Setting the Stage, The Getty Research Institute, Online Edition Version 3.0. "http://www.getty.edu /research /publications/ electronic_publications /intrometadata /setting.html".

[7] Office Open XML, http://tr.wikipedia. org/ wiki/ Office_Open_XML, (Erişim Tarihi:17 Şubat 2015).

[8] Microsoft Word, http://tr.wikipedia.org/wiki/Microsoft_Word, (Erişim Tarihi:15 Şubat 2015).

[9] Metadata Element Set, http://dublincore.org/ documents/dces/, (Erişim Tarihi:20 Aralık 2014)