26/11/2018

“Garson” Adlı Gizli Tanık Tarafından Teslim Edilen SD Kartın İncelendiği Teknik Rapor Hakkında Bilgi Notu

T. Koray PEKSAYAR

İÇİNDEKİLER

1. Sayısal Deliller: Elektronik Ortamda Depolanan Dosyaların Belge Niteliği.....3
2. Sayısal Verilerin Kaynağı.....3
3. Özüt Değeri (Kriptografik Özet) Kavramı.....4
4. Özüt Değerinin Dosya veya Mesaj Bütünlüğü Doğrulamada Kullanımı.....5
5. Sayısal Verilerin Doğruluğu, Delil Özelliği ve Özüt Değerinin Yasalarımızdaki Yeri.....5
6. Üst Veri Kavramı.....6
7. Sayısal Verilerin Doğrulanması: Kaynak ve Sahtecilik Tespiti.....7
8. 05/06/2018 Tarihli İnceleme Raporunun İncelenmesi.....8

1. Sayısal Deliller: Elektronik Ortamda Depolanan Dosyaların Belge Niteliği

Bilgisayar bilimleriyle ilgili tartışmalarda, bilgi, bilinç ve anlamsallık konuları açıldığında en önemli konulardan biri verinin her zaman anlamlı bilgi olmadığı olgusudur.

Sayısal verinin bilgi niteliği taşıyabilmesi için bulunduğu ortamdaki diğer benzer veriyle tutarlı bir bütün oluşturması gerekir.

Bir sayısal kütüğün[1] aynı zamanda bir veritabanı olduğu düşünülürse, bu veritabanına belirli şartlarla ve kurallarla erişildiği varsayıldığında anlamlı bilgi içerdiğinden emin olunabilir.

Veritabanı üzerinde kayıt tutan bir muhasebe yazılımını örnek verilirse veritabanındaki alacak verileri tek başlarına borç verileriyle kıyaslandıklarında sadece incelenen dönemdeki alacak borç dengesi hesaplanabilir.

Bu veriler ancak müşteri verileriyle ilişkilendirildiğinde anlamlı borç alacak bilgisine ulaşılabilir.

Veritabanındaki müşteri kayıtlarında sadece müşteri numaraları da hiçbir anlamlı bilgi içermemektedir. Bu veri bir dış veriyle yorumlandığında anlamlı bilgiye erişilmektedir.

Bir işlemin kimin tarafından yapıldığının belli olmaması durumu da yine anlamsal bütünlüğün bozulmasına sebep olur.

Bir kaydın hangi kullanıcı tarafından girildiği bilgisi olmadığında bu kayıt ve tüm ilgili kayıtlar da geçersiz olacaktır ve sistemin bütününde kararsızlık oluşacağı için anlamlı bilgi de bu durumdan etkilenmiş olacaktır.

Sistem üzerindeki bir açıktan faydalanılmak suretiyle sistem güvenliği aşılarak, parolası elde edilerek ya da zaten kullanıcı girişi yapılmış olan bir sisteme veri kaydedilerek yapılan işlemlerde de ortaya çıkan sonuç verinin tutarsızlığıdır.

Dolayısıyla, verinin anlamlı bilgi olarak kabul edilebilmesi için aynı ortamda bulunan diğer benzer veriyle tutarlılık oluşturması, kararlı çalışan, güvenliği sağlanmış olan bir sistemde depolanması, bu sisteme belirli kurallar ve şartlarla erişimin sağlanıyor olması gereklidir.

Sayısal ortamdaki veriler herhangi bir sistem kullanılarak, herhangi bir kişi tarafından, herhangi bir zamanı gösterecek şekilde oluşturulabilir. Bu verinin doğruluğu ve geçerliliği günümüz şartlarında sayısal imzalar kullanılarak sağlanır.

Dolayısıyla, verinin anlam kazanması için elde edilen verinin, 5N1K sorularını “Ne? Ne zaman? Nerede? Nasıl? Neden? Kim?” cevaplayabiliyor olması gereklidir.

Diğer bir deyişle, “hangi veri, ne zaman, hangi sistemde ve veri depolama ortamında, ne şekilde ve tipte, hangi veriyle ilişki kuracak şekilde, kim tarafından oluşturulmuştur” olarak açıklanabiliyor olması gereklidir.

Yukarıda sıralanan şartlar sağlandığında kayıtlı veri anlamlı bilgi içermektedir ve belge niteliği taşımaktadır yorumu yapılabilir.

2. Sayısal Verilerin Kaynağı

Sayısal ortamda depolanan veriler, istenilen şekilde; istenilen zamanı gösterecek, istenilen bilgiyi içerecek, istenilen içeriğe sahip olacak, istenilen kişi tarafından oluşturulduğu izlenimini verecek şekilde, herhangi kişi ya da kişiler tarafından oluşturulabilir.

5271 sayılı Ceza Muhakemesi Kanunu'nun “Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve El koyma” konusunu düzenleyen 134. maddesinin 1. bendinde;

> “*Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.*”

denilmektedir.

Yukarıda yapılan teknik tespit ve alıntılanan yasa maddesi sayısal delilin illiyet bağının önemini ortaya koymaktadır.

Yasaya göre esas olan, aramanın “şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde” yapılmasıdır.

1 Sayısal kütük: Sayısal veri depolanabilen her tür cihaz ve kayıt ortamı. Günümüzde “sayısal varlık” olarak da anılmaktadır.

Günümüzde bilgisayar ve diğer bilgi işlem sistemleri çeşitlilik arz etmekte, bu sistemler artık tek başlarına çalışmaktan ziyade dışarıya kapalı[2] ve dışarıya açık[3] ağlarla etkileşimde bulunmaktadırlar.

Bu sebeple oluşturulmuş her sayısal verinin aidiyeti, kullanıcı tarafından kullanıldığı bilinen bir bilgisayar kütüğünde kayıtlı bulunsa bile, denetlenebiliyor ve kaynağı incelenerek açıklanabiliyor olmalıdır.

Örneğin; İnternet'e bağlı bir bilgisayarda bulunabilecek bir resim dosyasının kullanıcının normal kullanıcı davranışları dahilinde gezdiği bir web sitesindeki bir reklamdan kaynaklanması olasıdır.

Dışarıya açık ağlarla bağlantılı sistemlerde kullanıcı istemi dışında durumlar da oluşabilir.

Buna örnek olarak kullanıcının bir uygulama yazılımında var olduğunu bilmediği ve bilmesine imkan olmayan program hatasının 3. şahıslarca tespit edilerek bu program hatasının sebep olduğu zafiyetin kullanılmasıdır.

Kullanıcı istemi dışında oluşan durumların bir diğer örneği de, görünür işlevinden başkaca amaçlar taşıyan kötü amaçlı yazılımların sistemde çalışmasıyla ortaya çıkar.

Örneğin, bir oyun ya da ekran koruyucu olarak çalışan bir yazılım, çalıştığı sistemde bir arka kapı açarak, bu sistemin kullanıcının bilgisi dışında dışarıdan kontrol edilmesine, sistemden dosya indirilmesine ve sisteme dosya yüklenmesine olanak sağlayabilir.[4][5]

Yapılan bir incelemeye konu olan kütük bir bilgisayar sistemine takıldığı bilinen ya da tespit edilebilen okunabilir ve yazılabilir bir kütükse, bu kütükte bu çeşit bir yazılıma rastlanması durumunda incelenen sayısal delilde bu yazılımın izlerine ve kalıntılarına rastlamak mümkündür.

Salt okunur ve arşiv niteliği olan[6] kütüklerin oluşturulduğu sistemlerin bilgi işlem cihazları olmaları sebebiyle içlerindeki dosyalarda bu çeşit yazılımların ve diğer başka izlerin bulunması da mümkündür.

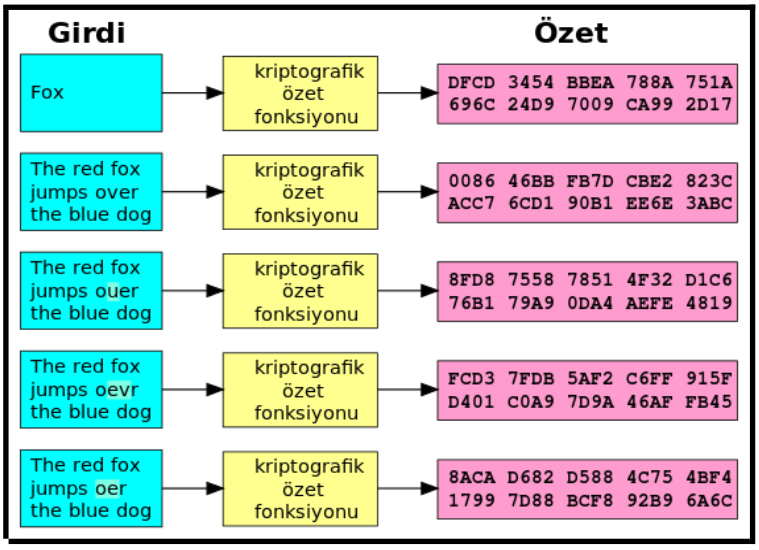
3. Özüt Değeri (Kriptografik Özet) Kavramı

Kriptografik özet[7] fonksiyonu, çeşitli güvenlik özelliklerini sağlayan bir özet fonksiyonudur.

Kriptografik özet fonksiyonu veriyi belirli uzunlukta bir bit dizisine, (kriptografik) özet değerine, dönüştürür. Kısaca, uzun bir verinin sayısal temsilini daha kısa bir veriye dönüştürerek yapar.

Bu dönüşüm verideki herhangi bir değişiklik durumunda özüt değerini[8] değiştirir.

Örneğin bir kriptografik özet fonksiyonu olan SHA1'in çeşitli girdiler için ürettiği özet değerleri aşağıdaki grafikte temsil edilmektedir. Girdi üzerindeki en küçük değişiklik bile özetin değerini önemli ölçüde değiştirmektedir. Bu durum çığ etkisi olarak adlandırılır.



2 Yerel ağ sistemleri. Intranet sistemleri ve benzerleri
3 İnternet bağlantılı sistemler gibi
4 Bkz: "Bu Kitabı Çalın II" İnternet güvenliği üzerine yazılmış ücretsiz e-kitabın 66. sayfası
5 Bkz: İtalyan HackingTeam firması hakkında haber: http://www.hurriyet.com.tr/polise-faturali-hackerlik-hizmeti-29497905
6 CD, DVD gibi
7 Türkçe VikiPedi'nin "Kriptografik özet fonksiyonu" maddesinden alıntılanmıştır. https://tr.wikipedia.org/wiki/Kriptografik_%C3%B6zet_fonksiyonu
8 İngilizce: Hash value

Özetlenecek veri “mesaj”, özet değeri ise “mesaj özeti” veya kısaca özet olarak da adlandırılır.

İdeal bir kriptografik özet fonksiyonu şu dört özelliği sağlamalıdır:

1. Herhangi bir mesaj için özet hesaplamak kolay olmalıdır.
2. Bir özete karşılık gelecek mesajı oluşturmak zor olmalıdır.
3. Özeti değişmeyecek şekilde mesajı değiştirmek zor olmalıdır.
4. Aynı özete sahip iki farklı mesaj bulmak zor olmalıdır.

Kriptografik özet fonksiyonları, bilgi güvenliği konuları olan sayısal imza, mesaj doğrulama kodu ve diğer doğrulama yöntemlerinde yaygın olarak kullanılmaktadır.

Sıradan özet fonksiyonları gibi veriyi komut çizelgesine eşlemede, eşdeğer veri bulmada, dosyaları tekil olarak tanımlamada ve veri bütünlüğü sağlamasında da kullanılır.

Bilgi güvenliği konularında kriptografik özet fonksiyonları, terim anlamları farklı olsa da “sayısal parmak izi”, “sağlama”, “özüt değeri” veya “özet değeri” ile benzer anlamlarda kullanılır.

4. Özüt Değerinin Dosya veya Mesaj Bütünlüğü Doğrulamada Kullanımı

Güvenli özetlerin önemli kullanım alanlarından birisi mesaj bütünlüğü doğrulamasıdır.

Bir mesajda veya dosyada değişiklik olup olmadığı, gönderim veya bir başka olaydan önce ve sonra hesaplanan özetlerin karşılaştırılması ile mümkündür.

Çoğu sayısal imza algoritması tüm mesaj yerine yalnızca özetin doğrulamasını yapmaktadır.

Özetin özgünlüğünün doğru olması mesajın kendisinin özgün olduğunu gösteren yeterli bir kanıt olarak kabul edilmektedir.

Adli bilişimde birinci derecede önem arz eden konu delilin değişmezliğidir. Adli bilişim incelemelerinde, değişmezliğin sağlamasının yapılması için sayısal ortamda bulunan dosyaların ve veri depolanan cihazların imaj kopyalarının özüt değerleri çıkarılarak tutanak altına alınır.

Kriptografik özet fonksiyonlarının yukarıda anlatılan özellik gereksinimi, birbirinden farklı veri kümelerinin aynı kriptografik özet fonksiyonundan geçirildiğinde farklı özet değerlerinin elde edileceği sonucunu doğurur.

Ancak bazı kriptografik özet fonksiyonlarının çalışma şekillerinden dolayı, rastlantısal olarak düşük olasılıkta olsa bile, farklı veri kümelerinin aynı özet değerini verdiği durumlarla karşılaşıldığı bilinmektedir.

Bu duruma çakışma denilmektedir ve pratik adli bilişim uygulamasında bu durumun bertarafı en kolay bulunan ve en hızlı çalışan 2 ya da daha fazla kriptografik özet fonksiyonu kullanılarak özüt sonucu not edilir.

Kolay kullanımı ve hızlı çalışması kriterlerine uyduğu için en çok kullanılan kriptografik özet fonksiyonları MD5 ve SHA1'dir.

5. Sayısal Verilerin Doğruluğu, Delil Özelliği ve Özüt Değerinin Yasalarımızdaki Yeri

Yasalarımızda sayısal verilerin delil özelliğinin korunması ve sağlamasının yapılması konusundaki en önemli madde 5271 sayılı Ceza Muhakemesi Kanunu'nun “*Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve El koyma*” konusunu düzenleyen 134. maddesidir

Bu maddede;

> “*(1) Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.*
>
> (2) Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere el konulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, el konulan cihazlar gecikme olmaksızın iade edilir.
>
> (3) Bilgisayar veya bilgisayar kütüklerine el koyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır.

(4) İstemesi halinde, bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.

(5) Bilgisayar veya bilgisayar kütüklerine el koymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır."

hükümleri kayıtlıdır.

5070 sayılı Elektronik İmza Kanunu'nda da bir sayısal verinin, temin edildiği zamanın ve değişmezliğinin sağlanması için ne gibi önlemler alınması gerektiği, özellikle zaman damgasından bahsedilen bölümlerde yer almaktadır. Elektronik imza, Elektronik İmza[9] Kanunu'nun[10] 3. maddesinde "*Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri*" olarak tanımlanmıştır.

Zaman Damgası[11], Elektronik İmza Kanunu'nun 3. maddesinde "*Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve/veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kayıt*" olarak tanımlanmıştır.

Zaman damgası elektronik ortamda her türlü belge ve sözleşme gibi önemli elektronik verilerin, belirli bir zamandan önce var olduğunu kanıtlamak için kullanılır.

6. Üst Veri Kavramı

Üst veri bir veri bütünü ya da bir dosya hakkındaki veridir.

Üst veriler teknik olarak 3 şekilde bulunurlar:

1. Bağımsız üst veri:
   Veriyi oluşturan uygulama yazılımı tarafından oluşturulan, veri bütününü oluşturan dosya içeriğindeki değişiklikler, yorumlar, dipnotlar gibi, insan tarafından anlaşılabilen, çeşitli öğeleri saklayan üst veridir. Bu tip üst veri kümesi genellikle ayrı bir depolama sisteminde, çoğunlukla da veritabanı sistemleri kullanılarak saklanır. Bu tip üst veri kümelerinin kullanım alanına en uygun örnek kütüphane ve hastane otomasyon sistemleridir.

2. Sistem üst verisi:
   İşletim sistemleri ya da dosyalama sistemleri tarafından oluşturulan, dosya sistemi, veritabanı gibi yapılarda tutulan, veri bütününü oluşturan dosyanın diskteki konumu, oluşturulma, değişiklik, erişim ve kullanıcı sahipliği gibi verilerini saklayan üst veridir.

3. Gömülü üst veri:
   Veriyi oluşturan uygulama yazılımı tarafından oluşturulan, veri bütününü oluşturan dosya hakkındaki oluşturan kullanıcı, değişik yapan kullanıcı, uygulama adı, içeriğindeki veri miktarı, oluşturulma tarihi, resim çözünürlüğü, oluşturan cihaz gibi verileri saklayan üst veridir. Bu tip üst veri kümesi oluşturulan dosyanın içinde kayıtlıdır. Bu sebeple bu tip üst veriyi "verinin kendisi hakkında bilgi veren veri" şeklinde tanımlamak da mümkündür.

Bu 3 üst veri tipi de farklı kategorilerde, veri bütününün özet bilgisini sağlar.

Resim ve ofis dosyaları gibi sık kullanılan dosya tipleri gömülü üst veri tutarlar.

Bu dosyalara ait sistem üst verileri dosyaların bulundukları dosya sisteminde kayıtlıdır.

Bir dosyanın gömülü üst verileriyle sistem üst verileri arasındaki tutarlılık, dosyanın geçerli veri içerip içermediği ve dosya üzerinde yapılan işlemler hakkında ipucu sağlar.

Elektronik ortamda saklanan her veri gibi, üst veri içeren dosyalar da istenilen şekilde; istenilen zamanı gösterecek, istenilen bilgiyi içerecek, istenilen içeriğe sahip olacak, istenilen kişi tarafından oluşturulduğu izlenimini verecek şekilde, oluşturuldukları uygulama yazılımları veya başka uygulamalar kullanılarak oluşturulabilir ve değiştirilebilir.

Üst veri içeren dosyalardaki üst verilerin kolayca oluşturulması ve değiştirilmesi mümkün olduğundan, bu üst verilerden elde edilen bilgilerin sadece güvenilir bir sistem ya da kaynaktan sağlandığına emin olunması şarttır.

9 E-imza Portalı http://www.e-imza.gen.tr/
10 5070 Sayılı Elektonik İmza Kanunu http://www.tbmm.gov.tr/kanunlar/k5070.html
11 Hoşgeldin Zaman Damgası (Makale) http://www.e-imza.gen.tr/index.php?Page=KoseYazisi&YaziNo=30&YazarNo=31

Dolayısıyla maddi gerçeğe ulaşılabilmesi için, bu bilgilerin geçerli ve gerçek bilgiler olduğunun sağlamasının yapılabilmesi için kullanılabilecek, dosyaların oluşturuldukları düşünülen bilgi işlem sisteminden ya da ağından[12] elde edilmesi olası, ikincil veriye ihtiyaç vardır.

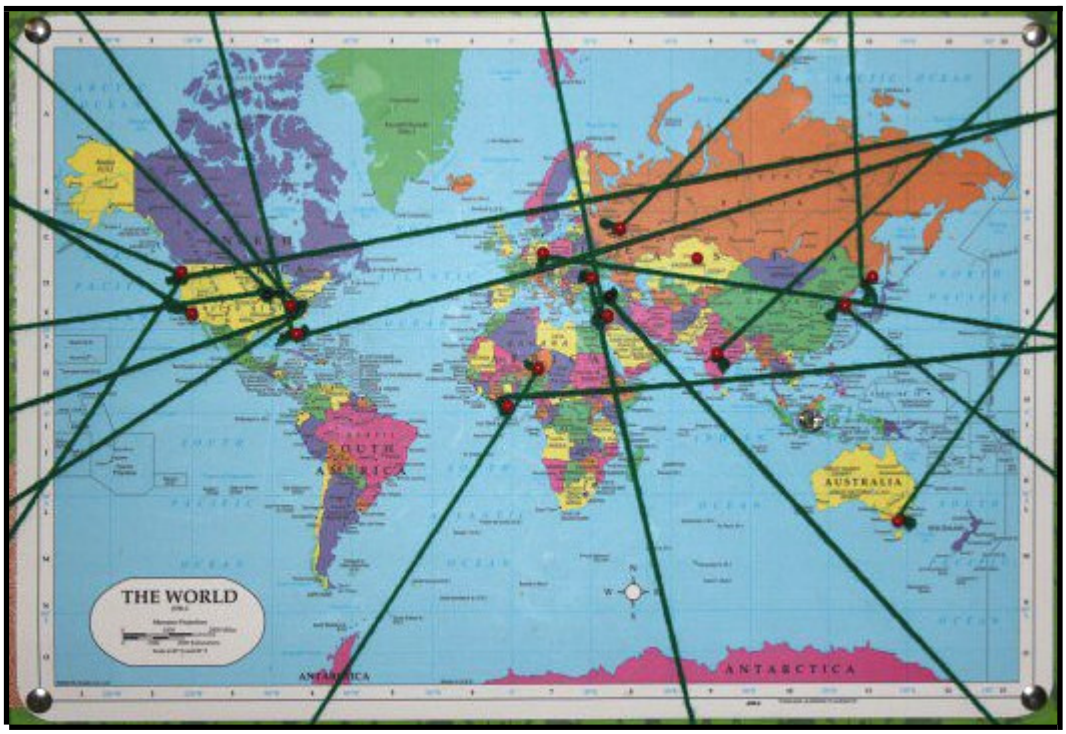
Dosyaların kendisini oluşturan bilgisayarın noksan olduğu durumlarda üst verilerden elde edilen bilgilerin yorumlanması teknik olarak imkansızdır ve dolayısıyla tek başlarına sağlıklı, tutarlı ve güvenilir delil olarak kullanılmaları mümkün olmayabilir.

7. Sayısal Verilerin Doğrulanması: Kaynak ve Sahtecilik Tespiti

Adli bilişim prensiplerinde sayısal verilerin doğrulaması fiziksel olaylarla kıyaslanması, genellikle fiziksel olayların sayısal ortamda bıraktıkları izlerin bulunması ve incelenmesi yoluyla yapılır.

Gerçek olayların somut sayısal izleri “pivot noktaları” ya da kısaca “pivot” tabir edilir.

Maddi gerçeği gösteren pivotlar birbirleriyle hiçbir zaman çelişmez. Çelişen yerler not edilerek pivotlar arasına adeta sanal ipler gerilir.



Bu iplerin içinde kalanlar maddi gerçeği, dışında kalanlar değişiklikler dolayısıyla oluşan tutarsızlıkları, şüpheleri ve sahtecilikleri temsil eder.

Pivotların çeşitli tipleri olmakla birlikte, genellikle incelenen sayısal verinin öznitelikleri ve yakınında olan fakat dışında kalan diğer veri kümelerinin özellikleridir.

En çok kullanılan pivot tipleri

1. Kayıtlı olduğu sistemden elde edilen tarih özellikleri,
2. Üst veriden elde edilen tarih özellikleri,
3. Üst veriden elde edilen diğer özellikler,
4. Oluşturulduğu ya da değişikliğe uğradığı uygulamanın bıraktığı kalıntılar,
5. Kaynağı

şeklinde sıralanabilir.

12 Dışarıya kapalı kurumsal ağlar kapsamı dışında kalan halka açık web sunucuları, kişiden kişiye (P2P) dosya paylaşım ağları gibi sistemlerden de sistem üst verisi elde edilebilir.

8. 05/06/2018 Tarihli İnceleme Raporunun İncelenmesi

Söz konusu raporun girişinde şu ifade yer almaktadır:

Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı

62018024-87055.(63044)/2017-68532 Sayılı Yazı.

DOSYA HAKKINDA

Ankara Cumhuriyet Başsavcılığınca yürütülmekte olan 2017/68532 sayılı soruşturma kapsamında Ankara 5.Sulh Ceza Hâkimliğinin 2017/2920 D.İş kararı gereğince kopyasının alınması, inceleme yapılarak verilerin metin haline getirilmesi ile hazırlanacak rapor ile gönderilmesi istenmiştir.

Raporda incelenen materyalin;

1. Lexar marka, 1000X model, seri numarası noksan, 64 GB sığalı, üzerinde Porteus Kiosk adlı Linux işletim sistemi kurulu SD bellek kartı,
2. Samsung marka, modeli noksan, seri numarası noksan, 32 GB sığalı, üzerinde Porteus Kiosk adlı Linux işletim sistemi kurulu SD bellek kartı

olduğu görülmektedir.

Raporda 64 GB sığalı, üzerinde Porteus Kiosk Linux işletim sistemi kurulu SD bellek kartında VirtualBox sanallaştırma yazılımı üzerinde 2 farklı Windows işletim sisteminin kurulu olduğu tespiti bulunmaktadır.

Pivot analizi ile iç tutarlılık için raporda görülen her sayısal varlığın tarih özellikleri önem taşımaktadır. Bu özellikler aşağıda sırlanmıştır:

1. Lexar marka, 1000X model SD bellek kartının piyasaya sürülüş tarihi,
2. Lexar marka, 1000X model SD bellek kartının üzerinde kayıtlı tüm dosyaların tarihsellik özellikleri:
3. Porteus kerneli 3.17.4 sürümünün çıkış tarihi,
4. Lexar marka, 1000X model SD bellek kartında VirtualBox sanallaştırma ortamına kurulu bulunan Windows işletim sistemlerinin sürüm bilgileri,
5. Lexar marka, 1000X model SD bellek kartında VirtualBox sanallaştırma ortamına kurulu bulunan Windows işletim sistemlerinin dosya sistemi üzerinde kayıtlı tüm dosyaların tarihsellik özellikleri,

Söz konusu tarih özellikleri dosyaların dosya olarak kaydedildiği tarih (modified date), dosyaların dosya sistemine kaydedildiği tarih (created date/changed date) ve dosyaların dosya sisteminde erişildiği son tarih (accessed date) olarak sıralanır.

Dosya sistemlerinde dosyalara ait parçalar olan öbekler veya düğümler disk üzerine rastgele yazılmalarına rağmen dosya yerleşim tablosundaki numaralanması her zaman birbirini takip eder.

Dosya sistemi kayıt girdileri dosya oluşturulma tarihleriyle uyumluluk içinde sayıları ardışık olarak artarak birbirini takip ederler.

Bu girdi numaraları takip edilerek hangi dosyanın hangisinden sonra oluşturulduğu kolaylıkla belirlenebilir. Dolayısıyla, dosyaların işlem tarihlerinden bağımsız olarak bu girdi numaralarından kayıt sıraları kolayca tespit edilebilir.

LSN yapısında sıra numaraları kullanılarak, dosya sistemi üzerinde yapılan dosya işlemlerinin kaydı tutulur.

Yukarıda da anlatıldığı üzere, disk üzerine yeni dosyalar kaydedildikçe girdi numaraları artmaktadır. Bu girdiler üzerinde yapılan değişiklikler ise LSN sıra numaralarında artış olarak görünmektedir.

Yani, dosya sistemi girdi numaraları tarihten bağımsız olarak ardışıldır, yani sistem tarihi ne olursa olsun birbirini izleyen işlemlerin girdi numaraları artarak kaydedilir.

Böylece, dosya sistemi girdi numaraları ve LSN sıra numaraları takip edilerek dosya kayıt işlemlerinin ayrıntısına ulaşmak kolaylaşır.

Dosya işlemlerini (log/journal) saklayan dosya sistemlerinde bu işlemlerin ayrıntıları elde edilerek zaman çizelgesine dökülerek inceleme yapılması elzemdir.

Örneğin söz konusu Windows işletim sistemlerinin kayıtlı bulunduğu NTFS dosya sistemlerinde bulunan MFT, LogFile ve USNJrnl yapıları (örneğin) serbestçe edinilebilen Sleuthkit Autopsy[13] programı kullanılarak dosya olarak kaydedilebilir.

Bu yapıların içerdiği veriler (örneğin) serbestçe edinilebilen NTFS Log Tracker[14] programı kullanılarak analiz edilerek dosya sisteminde kaydedilmiş olan dosya işlemlerinin tarihsellik ve niteliği hakkında veri elde edilebilir.

Aynı inceleme işlemleri Linux işletim sisteminin desteklediği ext2, ext3, ext4, ReiserFS, XFS ve diğer dosya sistemlerinde yapılması da mümkün ve elzemdir.

İncelenen raporda her ne kadar yapılan işlem incelemelerin "*uluslararası adli bilişim standartalarına uyumlu*" olduğu yazılmış olsa da, başlıca iç tutarlılık testleri olan;

1. İncelenen materyalde kayıtlı dosya sistemlerinin tipleri,
2. Bu dosya sistemlerinin oluşturulma tarihleri,
3. Bu dosya sistemlerinde kayıtlı dosyaların tarihsellik özellikleri

unsurlarının incelemesinin noksan olduğu görülmektedir.

Ek olarak başlıca dış denetim unsurları olan

1. Lexar marka, 1000X model SD bellek kartının piyasaya sürülüş tarihi,
2. Porteus kerneli 3.17.4 sürümünün çıkış tarihi

unsurlarının incelemesinin noksan olduğu görülmektedir.

Bu iç ve dış denetim unsurlarının noksan olması nedeniyle kıyaslanmaları ve elde edilip incelenen materyalin tahrifata uğramış olup olmadığı, tarihleri ileri-geri alınarak kayedeilmiş dosyalar içerip içermedikleri ve sahtecilikle oluşturulmuş veri içermeleri olasığı üzerinde durulmadığı anlaşılmaktadır.

Sayılı nedenlerle bu materyalin içerdiği verinin;

1. Eksik görülen bu tutarlılık denetimleri olmaksızın,
2. Dış veriyle desteklenmeksizin,
3. Fiziksel delillerle uyumluluğu, yani olmuş olayların bıraktığı izlerin doğrulaması yapılmaksızın

delil olarak kabul edilmeleri sakıncalıdır.

Saygılarımla kamuoyunun bilgilerine sunarım,
T. Koray PEKSAYAR

Bilişim ve Adli Bilişim Uzmanı
Bilgi Teknolojileri Yüksek Lisans
İTÜ Y. Lis. Dip. No: 76-387

13 Sleuthkit Autopsy https://www.sleuthkit.org/autopsy/v2/index.php
14 NTFS Log Tracker https://sites.google.com/site/forensicnote/ntfs-log-tracker