UZMAN GÖRÜŞÜ

LİTVANYA'DAKİ BYLOCK SUNUCUSUNDAN ELDE EDİLEN SAYISAL VERİLERİN DOĞRULUĞU VE GÜVENİLİRLİĞİ

1. Giriş ve Kapsam

15 Temmuz 2016 hain darbe girişimi sonrası ByLock mobil iletişim uygulaması kamuoyunun gündemine gelmiş ve sonrasında gerçekleştirilen idari ve adli işlemlerde önemli bir rol oynamıştır. ByLock mobil iletişim uygulamasının FETÖ/PDY yargılamalarının merkezinde yer aldığını söylemek yanlış olmayacaktır.

Bu nedenle, işlemlerin çoğunun merkezinde dijital (sayısal) bir program yer almaktadır; sayısal verilerin analizi / yorumlanması hem teknik hem de hukuki bilgi gerektiren bir uzmanlık konusudur. Yargılamaların meşruiyetini korumak için teknik ve hukuk uzmanlarının işbirliği ve her aşamada hukukun evrensel ilkeleri altında hareket etmek esastır.

Sayısal verilerin doğruluğu ve güvenilirliği her bir vakada hassastır. Sayısal verilerin doğruluğunu ve güvenilirliğini tanımlamak, davalarda her adli ve teknik uzmanın hassasiyatele hareket etmesi gereken kritik aşamalarından biridir. Sayısal verilerin doğruluğu ve güvenilirliği konusunda herhangi bir şüphe varsa, veriler yasal (hukuka uygun) kanıt olarak kabul edilemez.

ByLock mobil uygulama kullanıcılarının tespitine yönelik kullanılan sayısal verilerin doğruluğu ve güvenilirliği ByLock merkezli FETÖ/PDY yargılamalarının en kritik aşamalarından biridir. Bu nedenle uzman görüşü Litvanya'da bulunan ByLock sunucusundan elde edilen sayısal verilerin doğruluğuna ve güvenilirliğine odaklanmıştır.

2. Sayısal Veri ve Sayısal Delil Kavramları

Bilgisayar bilimlerinin en önemli temellerinden biri verinin (data) her zaman anlamlı bilgi (intelligence) olmadığı olgusudur. Verinin bilgi olarak kabul edilebilmesi için iç ve dış tutarlılığının yanı sıra, anlamlı olması da gereklidir.

Sayısal verinin bilgi niteliği taşıyabilmesi için bulunduğu ortamdaki diğer benzer veriyle tutarlı bir bütün oluşturması gereklidir. Buna iç tutarlılık da denebilir.

Benzer şekilde, verinin varsa dış ortamlarda yer alan diğer benzer verilerle de tutarlı olduğunun doğrulanması gereklidir. Buna da dış tutarlılık denebilir.

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

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. Tutarlılığına bakılan dış sistemdeki veriler de aynı özellikleri sağlamalıdır. Özetle hem incelenen hem kıyaslanan sistem kendi içinde tutarlı, diğer sistemle tutarlı ve anlamsallığı olan sistemler olmalıdır ki verilerin delil olarak kabulü mümkün olabilsin.

Sayısal ortamda depolanan veriler, istenilen şekilde; istenilen zamanı gösterecek, istenilen bilgiyi içerecek, istenilen içeriğe sahip olacak, istenilen kişi tarafından oluşturulduğu izlenimini verecek şekilde, herhangi bir kişi veya kişiler tarafından oluşturulabilir. Bu durumun mahkemelere yansımış çok sayıda örneği mevcuttur. Güvenlik seviyeleri üst düzeyde olan banka sistemlerinde dahi açıklar bulunabilmekte ve kredi kartları başta olmak üzere çok farklı konularda usulsüzlükler, yolsuzluklar olabilmektedir.

Bu verinin doğruluğu ve geçerliliği[1] günümüz şartlarında sayısal imzalar kullanılarak sağlanır.

Dolayısıyla, **verinin anlam kazanması için elde edilen verinin, 5N1K sorularını, yani "Ne? Ne zaman? Nerede? Nasıl? Neden? Kim?" sorularını 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.

Yukarıda açıklanan tüm teknik hususlar ve örnekler ve ileride belirtilecek değerlendirmeler esasında sayısal delilin illiyet bağının önemini ortaya koymaktadır. Sayısal verilerin delil olarak kullanılabilmesi illiyet bağının tam olarak kurulabilmesiyle mümkündür.

3. ByLock Mobil Uygulama Kullanıcılarının Belirlenmesi

Herhangi bir mobil uygulamayı kullanırken veri toplayan ve depolayan en az iki taraf vardır. Veri toplayıcılardan ilki GSM operatörleri, özellikle müşteriye atanan IP adresi ve müşterinin bağlanmak istediği uygulama sunucusunun IP adresini internet trafiği için kaydeder. İkinci veri toplayıcı taraf, mobil uygulamanın sunucusudur.

Herhangi bir mobil uygulamayı kullanabilmek içinen azından bu iki taraf arasında bağlantı ve veri aktarımı olmalıdır. İki taraf arasındaki bağlantı ve veri aktarımı, iki banka hesabı arasındaki para transferi (EFT) ile benzetilebilir. İki banka hesabı arasında başarılı bir para transferi varsa banka veritabanlarının anlamlı

[1] Bu kavrama "reddedilmezlik" de denir.

olması ve veritabanlarındaki verilerin de tutarlı olması (iç tutarlılık) koşuluyla iki farklı banka tarafından toplanan ve saklanan veriler birbirleriyle tutarlı (dış tutarlılık) olmalıdır.

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 adli işlemler için geçersiz olacaktır çünkü veri güvenliği ihlal edilmiş olabilir ve veritabanının 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.

Birisi bir güvenlik açığından yararlanarak, bilgisayar korsanlığı yoluyla kullanıcı/yönetici parolalarını elde ederek veya failin sunucuya fiziksel olarak ulaşmasını sağlayan başka bir yöntem/güvenlik açığı elde ederek sunucuyu ihlal edebilir. Bir sunucu ihlal edilirse, fail veritabanının içeriğini sabit sürücülerin fiziksel sektörlerinde değiştirebilir. Fail dikkatli olmazsa, bu müdahaleler sonucunda verilerde tutarsızlıklar olabilir. Verilerde bir tutarsızlık varsa, bu, birinin verileri kurcalaması sonucu olabilir, bu nedenle bu veriler bir kovuşturmada güvenilir bir bilgi kaynağı olarak kullanılmamalıdır.

Litvanya'da bulunan bir şirketten kiralanan ByLock sunucusundan alınan veriler örneğimizdeki muhasebe kayıtlarına benzetilebilir. Sunucu kayıtlarında çok sayıda kayıt bölümü yer almaktadır ve bunlar arasında bizi gerçek kullanıcıya götürebilecek kayıt sadece bir tek tabloda bulunan Genel IP bilgisidir ki bu da örneğimizdeki müşteri hesap numarasına benzetilebilir. Operatörler ise örneğimizdeki bankalara benzetilebilir. Sunucuda yer alan verilerden gerçek kullanıcı bilgisine ulaşmanın tek yolu operatörlerdeki verilerle eşleştirerek olabilir. Bunun için temel şartlar:

i. **Hem ByLock sunucusu hem de operatörlerdeki verilerin kendi içinde ve birbirleriyle tutarlı olmaları,**
ii. **Her iki veritabanındaki kayıtların da kararlı çalışan, güvenliği sağlanmış olan bir sistemde depolanması,**
iii. **Bu sistemlere belirli kurallar ve şartlarla erişimin sağlanıyor olması**
iv. **İki sisteminde zaman senkronizasyonun sağlanabiliyor olması**

şeklinde sıralanabilir.

Bu şartlar sağlandığında veriler bilgi olarak kabul edilebilir ve uygulamanın gerçek kullanıcılarının belirlenmesi mümkün olabilir.

Ne yazık ki istihbarat veya emniyet birimleri, her iki veritabanının anlamlılığını ve iç tutarlılığını kontrol etmeden ve iki ayrı veritabanının dış tutarlılığını kontrol etmeden, bağlantılı iki tarafı ayrı ayrı kullanarak ByLock mobil uygulama kullanıcılarını belirlememektedir. ByLock mobil uygulama kullanımı tespitinin sadece bir tarafa, GSM operatörüne veya ByLock sunucusuna dayandığı on binlerce dava dosyası bulunmaktadır ve bunlarda diğer taraf hakkında herhangi bir veri bulunmamaktadır.

Herhangi bir sayısal veriyi sadece bir taraftan tespit etmek, uçamayan tek kanatlı bir kuşa benzetilebilir. Sadece bir kaynaktan elde edilen sayısal veriler cezai işlemler kapsamında yüzde yüz güvenilir olmayacaktır.

GSM operatörlerinin internet trafik kayıtlarının anlamlılığı ve iç tutarlılığı ile ilgili birçok sorun bulunmaktadır. Ankara Cumhuriyet Başsavcılığı'nın 27 Aralık 2017'deki açıklamasına göre, bazı tuzak uygulamalarıyla ByLock sunucularının kullandığı IP adreslerine bilgisi ve iradesi dışında 11 bin 480 kişi yönlendirildi. Bu tuzak uygulamalar "Morbeyin Uygulamaları" olarak bilinir ve muhtemelen aynı metodolojiyi izleyerek daha fazla masum insanı mağdur eden sayısal tuzaklar, bilinmeyen başka tuzak uygulamalar vardır.

Tuzak uygulamalar sorunu GSM operatörü veritabanlarının temel sorunlarından sadece biridir ve GSM veritabanlarının mobil uygulama kullanıcılarını veya herhangi bir internet trafiğini tespit etmek için doğru ve güvenilir olmadığının güçlü bir kanıtıdır.

GSM operatörlerinin internet trafik kayıtları ve veri tabanları ayrıntılı olarak tartışılmayacaktır. Bunun yerine, uzman görüşü Litvanya'da bulunan ByLock sunucusundan elde edilen sayısal verilerin doğruluğuna ve güvenilirliğine odaklanmıştır.

Tutuklu Avukatlar İnisiyatifi, tespit edilen ByLock kullanıcılarının değişen sayılarına ilişkin "Rapor: Sürekli Değişen Kanıt; ByLock"[2] isimli kapsamlı bir rapor yayınlamıştır. Bu raporda devlet görevlileri tarafından beyan edilen değişken sayılardan bahsedilmektedir. Aslında, tespit edilen ByLock mobil uygulama kullanıcılarının değişen sayıları, tespit prosedürlerindeki karışıklığın bariz bir kanıtıdır. Sayısal verilerle tespitte bu tür bir karışıklık, ceza yargılamasında yasal delil olarak kabul edilemeyecek belirsizliklere neden olacaktır.

4. Litvanya'daki Sunucunun Doğruluğu ve Güvenilirliği ve Sunucudan Elde Edilen Veriler

4.1. Sunucunun Doğruluğu ve Güvenilirliği

Yukarıda belirtildiği gibi, bir sayısal kütüğün aynı zamanda bir veritabanı olduğu düşünülürse, bu veritabanına belirli şartlarla ve kurallarla erişildiği varsayıldığında anlamlı bilgi içerdiğinden emin olunabilir.

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

[2] https://arrestedlawyers.org/2018/01/30/report-ever-changing-evidence-bylock/

ByLock mobil uygulama kullanım iddiası içeren yaklaşık yüz bin soruşturma/dava dosyası vardır ve bunların altmış bini şüpheli/sanık için "Tespit ve Değerlendirme Tutanağı" içermektedir. Tespit ve Değerlendirme Tutanklarının ByLock sunucusundan elde edilen verilerden oluşturduğu iddia edilmektedir. Ancak Litvanya'da bulunan sunucu için 5N1K sorularının cevapları hakkında herhangi bir bilgi yoktur.

Sunucudan elde edilen verilerin doğruluğu ve güvenilirliği ile ilgili ciddi sorunlar vardır ve bazıları aşağıda belirtilmiştir. Elde edilen verilerle ilgili ciddi sorunlar olduğundan, sunucu için yalnızca iki olasılık vardır, sunucudaki veritabanının anlamlı bir verisi yoktur, yani burada veritabanına erişmek ve işlemek için hiçbir kural yoktur veya sunucudan elde edilen veriler bozulmuştur.

4.2. Sunucudan Elde Edilen Verilerin Doğruluğu ve Güvenilirliği

Milli İstihbarat Teşkilatı (Türkiye'nin resmi istihbarat birimi MİT), ceza mahkemelerinin kullanımına yönelik bir rapor (sonrasında "MİT ByLock Raporu" olarak[3] adlandırılacaktır) yayınladı. MİT ByLock Raporu, tanınmış sayısal teknoloji firması FOX-IT tarafından detaylı bir şekilde incelenmiş ve ByLock mobil uygulamasına yönelik kapsamlı analiz ve bulguları içeren[4] bir rapor yayınlanmıştır. Tüm ilgili kişilerin FOX-IT'nin ByLock hakkındaki kapsamlı uzman görüşünü okumaları şiddetle tavsiye edilir.

MİT ByLock Raporu'nun "Açıklamalar" bölümünün ilk sayfasında, tespit edilen ByLock kullanıcı sayısı 102.192 olarak belirtilmiştir. MİT ByLock Raporu'nun 52. Sayfasında ByLock uygulamasına ilişkin istatistiki bilgiler tablolanmış olup, en az bir kez mesaj gönderen veya alan kişi sayısı 60.473 olarak belirtilmiştir. "Rapor: Sürekli Değişen Kanıt; ByLock" raporunda değinildiği gibi ByLock kullanıcı sayısı henüz kesin olarak belirlenmemekle birlikte MİT ByLock Raporu en güvenilir belge olarak kabul edilerek, şüphelileri ByLock kullanmakla suçlayan yüz bin civarında ceza davası olduğu sonucuna varılmıştır. Ayrıca, vakaların yaklaşık altmış bini için ByLock sunucusundan elde edilen iletişim içerikleri olması gerektiği de tahmin edilmektedir.

Ne yazık ki, sayısal veriler bu on binlerce vakanın hiçbirinde yer almamaktadır.

Çoğu durumda, sayısal delilden soruşturma organlarınca doğrudan yararlanılması delilin bulunduğu ortam ve niteliği itibariyle mümkün değildir. Bu delillerin inceleme ve değerlendirmeye elverişli hale getirilmesi için sanal dünyadan gerçek dünyaya aktarılması gerekmektedir. Sayısal delillerin siber dünyadan gerçek dünyaya aktarılması adli bilişim konusudur. Adli bilişim, delil bütünlüğünü korumak, bununla birlikte yasal ve etik sorumlulukları gözetmek doğrultusunda maddi bir gerçeği ortaya çıkarmak için yapılan inceleme, kopyalama ve analizleri içerir Ayrıca kanıt inceleme sürecini, disklerden, sabit disklerden ve taşınabilir disklerden potansiyel kanıtlar için veri kurtarma faaliyetlerini içerir.

Delili oluşturan birincil faktör olgusallığıdır. Delillerin olgusallığı ve bu delilin mahkeme huzurunda güvenilirliği, delilin tahrifat veya hasar içermemesine bağlıdır. Elektronik veriler, diğer delil türlerine kıyasla nispeten kırılgandır ve kolayca tahrif edilebilir veya yok edilebilir. Verilerin değişmezliğini garanti etmek için sayısal verilerin sayısal imzaları, zaman damgaları ve özüt değerleri olmalıdır. Ceza davasının her bir tarafı, orijinal verileri inceleyebilmeli ve aynı anlamlı bilgileri bulabilmeli veya sonuçlara

[3] 09.12.2016 tarihli Sayı: 10.2.001.01.000.390.1960.249-2236/691-92452157 sayılı yazı
[4] https://foxitsecurity.files.wordpress.com/2017/09/bylock-fox-it-expert-witness-report-english.pdf

ulaşabilmelidir. Ceza yargılamasının bu gerekliliğinin sağlanması, dava dosyalarında sayısal veri bulunmadığından imkânsızdır.

Bilindiği üzere ByLock ile ilgili dava dosyalarında yer alan "Tespit ve Değerlendirme Tutanağı" isimli tutanaklarda kullanıcı no, şifre, kimlerle görüştükleri, kaç mesaj atıp-aldıkları, kaç sesli görüşme yaptıkları, kaç mail atıp-aldıkları, grup üyelikleri ve görüşmelerin içerikleri gibi bilgiler bulunmaktadır.

Aslında, tespit ve değerlendirme tutanaklarının hazırlanması ve mahkemelere sunulması oldukça sıradandır. Ancak, sorun tutanakların içeriğidir ve delilin kendisinin olmamasıdır. Tutanaklarda sürecin nasıl başladığına dair bir bilgi olmadığı gibi en başta kanıtların nasıl elde edildiği ve sonra nasıl analiz edildiğine dair bir bilgi de bulunmamaktadır. Tutanaklarda, verilerin analizine kimin ve ne ölçüde katıldığı ve analizin nerede yapıldığı gibi birçok soru cevapsızdır. Mahkeme işlemlerinde de görülebileceği gibi tutanaklar basılı sayfalardır. Polis memurlarının imzaları "çıktısını alan" olarak yer almaktadır, ancak tutanağı kimin hazırladığı ve hazırlama yöntemleri hakkında bilgi bulunmamaktadır. Bu bakımdan bunun delilin müşterekliği ilkesine uygun olduğunu söylemek mümkün değildir.

Delillerin müşterekliği, tüm taraflara sunulması ve tarafların delilleri mahkeme önünde serbestçe tartışma özgürlüğüdür. Bu nedenle, taraflar tüm delillere ulaşabilmelidir. Hakim, kararını ancak mahkemeye çıkarılan ve tüm taraflarca tartışılan delillere dayandırabilir. Karar sadece kürsüde bulunan bilgiye dayandırılamaz. Deliller davadaki tüm taraflara açık olmalıdır. Delillerin müşterekliği ilkesinin amacı, tarafların delilleri özgürce incelemelerini, fikirlerini ifade etmelerini ve gerekli gördükleri takdirde itiraz etmelerini sağlamaktır. Dahası, yargıç bir davada sadece kendi bilgisine güvenerek karar veremez.

Delillerin müşterekliğinin CMK'na yansıması 217. Madde ile olmuştur. CMK m. 217/1: *"Hâkim, kararını ancak duruşmaya getirilmiş ve huzurunda tartışılmış delillere dayandırabilir. Bu deliller hâkimin vicdanî kanaatiyle serbestçe takdir edilir."* Bu maddede ifade edilen "delil" kelimesi gerçek delil anlamındadır. Dosyalardaki tutanak delil değil, ancak nasıl elde edildiği, kim tarafından hazırlandığı ve ne tür yöntemler kullanıldığı hakkında bilgi içermeyen bir belgedir. Bu noktada, savunmanın delillerin doğru bir şekilde incelenip incelenmediğini veya sanıkla gerçek anlamda ilişkilendirilip ilişkilendirilmediğini araştırma şansı yoktur. Tutanaklarla ilgili bir sorun olup olmadığını inceleme şansı yoktur. Bariz bir sorun olsa bile, sorunun temelinin ne olduğunu bilmek mümkün değildir. Bunun nedeni, tutanakların dayanağının mahkemelerde bulunmamasıdır. Tutanaklara bakıldığında, çoğunlukla verilerdeki çelişkiler ve verilerde olası tahrifatlar olmak üzere birçok yanlışlık tespit edilmiş; ancak, gerçek delil dosyada bulunmadığından, verilerin çapraz kontrolü mümkün değildir.

ByLock verilerinin dosyalara kazandırılması bakımından kullanılan bu tutanak usulü savunma hakkının büyük ölçüde kısıtlanmasına neden olmaktadır. Aslında, (tutanak) artık kutsal bir mesele haline gelmiştir. Ayrıca, gerçek delilleri inceleyemeyen tek taraf savunma değildir. Davaya dahil olan tarafların hiçbiri, savcı, savunma ve hakim, gerçek delillere ulaşamamaktadır.

Tespit ve Değerlendirme Tutanaklarının kendi içinde çok fazla tutarsızlığı vardır. Tipik tutarsızlıklardan bazıları ilgili bir makalede belirtilmiştir.[5] "Tespit ve Değerlendirme Tunakları"nda belirlenen yaygın tutarsızlıklar şunlardır:

i. Tespit edilen işlem tarihleri ve logların tarihleri,
ii. Tespit edilen loglar ve işlemler (oturum açma, oturumu kapatma, mesaj gönderme vb.),

[5] [5] Gokce, Y., "The ByLock fallacy: An In-depth Analysis of the ByLock Investigations in Turkey", Digital Investigation, 26 (2018) 81-91, Science Direct

iii. Tespit edilen veriler ve loglar,
iv. Tutanakların farklı bölümleri arasında diğer kullanıcıların tespit edilen iletişim bilgileri tutarlı değildir.

Bahsedilen tutarsızlıklar, veritabanının ve sunucunun bozulmasının güçlü bir kanıtıdır Verilerin doğrulanması veya tutarsızlıkların nedeninin anlaşılması, ancak orijinal delilin, bozulmamış sayısal verilerin müşterekliğinin sağlanması ve sayısal verilerin ceza yargılamasının tüm tarafları tarafından incelenmesi ile mümkün olabilir.

4.3. Sunucudan Elde Edilen Verilerin Adli İncelemesi

Litvanya'da bulunan ByLock sunucusundan elde edilen 109 GB veri yığınını içeren bir sabit sürücü olduğu belirtilmektedir. Hiçbir taraf göremese de birçok kararda ve ayrıca FETÖ/PDY yargılamaları hakkında Yargıtay 16. Ceza Dairesi ilk kararında (2015/3 E. 2017/3 K.) geçmektedir.

Yüksek Mahkeme, elde edilen verilerden sonra Ankara Cumhuriyet Başsavcılığı tarafından yürütülen süreci aşağıdaki şekilde özetlemiştir:

"MİT'in yasal olarak elde ettiği dijital materyaller ve teknik analiz raporunun Ankara Cumhuriyet Başsavcılığına ulaştırılması ile birlikte artık adli sürecin başlatılması ve bu noktadan sonra CMK hükümlerine göre soruşturma işlemlerinin yapılması zorunludur. Nitekim Ankara Cumhuriyet Başsavcılığının, yürütülen soruşturmalar kapsamında Mili İstihbarat Teşkilatı tarafından FETÖ/PDY silahlı terör örgüt üyeleri tarafından kullanılan kapalı devre iletişim programı olan ByLock ile ilgili dijital materyallerin teslim edilmesi üzerine adli süreci başlattığı, 2016/104109 sor. Ve 2016/180056 numara üzerinden CMK 134.maddesine göre gönderilen dijital materyallerle ilgili inceleme, kopyalama, çözümleme işlemini yapmaya karar vererek 09/12/2016 tarih ve 2016/104109 soruşturma sayılı yazısı ile Ankara 4. Sulh Ceza Hakimliğine, Milli İstihbarat Teşkilatınca gönderilen; 1-1 adet Sony marka HD-B1 model, üzerinde bBW3DEK69121056 seri numaralı ve ön yüzünde 1173d7a09195cf0274ce24f0d69ede96 yazılı harddisk, 2-1 adet Kingston marka DataTraveler, uç kısmında DTIG4/8GB 04570-700.A00LF5V 0S7455704 yazılı flash bellek üzerinde, CMK 134.maddesi gereğince inceleme yapılmasına, 2 adet kopya çıkartılmasına, kopya üzerinde kayıtların çözülerek M. haline getirilmesine karar verilmesini istendiği, Ankara 4. Sulh Ceza Hakimliği talebi kabul ederek 09.12.2016 tarih 2016/6774 D.İş nolu kararı ile; dijital materyaller üzerinde inceleme yapılması, kopya çıkarılması ve kopya üzerinde bilirkişi incelemesi yapılarak M. haline getirilmesi için bir kopyasının Ankara Cumhuriyet Başsavcılığına gönderilmesine karar verildiği tespit edilmiştir. Ankara Cumhuriyet Başsavcılığı tarafından Emniyet Genel Müdürlüğü Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığına yazılan 16/12/2016 tarih ve 2016/180056 soruşturma sayılı yazı ile; Ankara 4. Sulh Ceza Hakimliğinden CMK 134.maddesi gereğince alınan inceleme, kopyalama ve çözümleme kararına istinaden içerisinde ByLock verilerinin tamamını içeren harici haddisk ve abonelik listesinin bulunduğu flash belleğinin imajını içerir 1 Seagate marka Z9A4E09G seri numaralı harddisk gönderilerek ByLock ile ilgili yazışmaların Ankara Cumhuriyet Başsavcılığının 2016/180056 soruşturma sayılı dosyası üzerinden sağlanması ve talimat doğrultusunda bir komisyon aracılığıyla gerekli araştırma ve soruşturma işlemlerinin yapılarak, ulaşılan tespitleri içerir raporun gönderilmesinin istendiği tespit edilmiştir."

Bu sayısal verilerle ilgili en önemli belge, 2016/104109 sayılı soruşturma kapsamında Ankara Cumhuriyet BasSavcılığı tarafından görevlendirilen Yardımcı Doçent Doktor Baha Şen ve Adli Bilişim Uzmanı Rafet Öngöçmen tarafından hazırlanan bilirkişi raporudur. Yüksek Mahkeme'nin kararını ve bilirkişi raporunu birlikte incelediğimizde, sabit diskin orijinal verileri değil, istihbarat hizmeti tarafından sağlanan kopyayı

içerdiği sonucuna varıyoruz. Rapor metninden anlıyoruz ki, bilirkişi ataması 27 Eylül 2016 tarihinde yapılmış, ancak rapor tarihi 12 Temmuz 2017 olarak yer almıştır. Raporun ilgili bölümlerinin ekran görüntüleri ve İngilizce çevirisi aşağıda sunulmuştur.

Rapor Tarihi : 12/07/2017

1. Giriş

Ankara C.Başsavcılığının 2016/104109 soruşturma nolu dosyası kapsamında **27/09/2016** günü Ceza Muhakemeleri Kanunun ilgili maddelerine göre yapılan Bilirkişi Görevlendirilmesi ile talep edilen hususlar ile ilgili çalışmalar yapılarak elde edilen sonuçlar aşağıda sunulmuştur.

Date of the Report : **12/07/2017**

1. Introduction

Within the scope of the investigation file of the Ankara Chief Public Prosecutor's Office with the investigation number 2016/104109, the issues requested by the appointment of expert made on **27.09.2016** in accordance with the relevant articles of Turkish Code of Criminal Procedure and the results obtained by doing related works are presented below.

Resim 1: Bilirkişi raporunun ilgili bölümlerinin ekran görüntüsü ve İngilizce çevirisi.

Bilirkişi raporunun 26. sayfasına baktığımızda ve oradan bir ekran görüntüsü verdiğimizde, Litvanya'daki sunucudan elde edilen verilerin doğruluğu ve güvenilirliği hakkında kritik bilgiler bulunmaktadır. Raporun ilgili bölümü, elde edilen verilerin bozulmuş olduğunu tam olarak açıklar. Teknik olarak, bozuk verilerin, adli bilişim yazılımları tarafından nasıl erişilir ve kurtarılırsa kurtarılsın tamamen doğru ve güvenilir olarak kabul edilemeyeceği iyi bilinmektedir. İlgili bölümün ekran görüntüleri ve İngilizce çevirisi aşağıda sunulmuştur.

Disk içerisinde yer alan ve **113.789.140 KB** ***(108 GB (116.520.079.360 bayt))***'lik kapasiteye sahip "**ibdata1"** dosyasının **MySQL** veri tabanı dosyası olduğu görülmüş ve içerisindeki verilerin tablo yapısının ortaya çıkartılması için çalışmalar yapılmıştır. Ancak ilgili dosya yapısı bozuk olduğu için şema bileşenlerine erişilememiştir.

ibdata1 dosyası içerisindeki verilere erişim sağlanabilmesi ve bu verilerin tablolar halinde kurtarılması için **Linux Centos ve Debian** işletim sistemleri üzerinde "**Percona Data Recovery (percona-data-recovery-tool-for-innodb)**" https://www.percona.com/ ve "**TwinDB Data Recovery (undrop-for-innodb)**" araçları kullanılmıştır. https://recovery.twindb.com/

İlgili araçlar ile yapılan işlemler sonucunda **"ibdata1"** içeresinde toplam **(28)** adet tablonun bulunduğu **"appDb"** ve **"wordpress"** isimli iki ayrı veri tabanının yer aldığı, abbDb içerisinde toplam **(15)** adet tablonun bulunduğu, wordpress veri tabanında **(11)** adet tablonun yer aldığı görülmüştür. "**byLock**" veri tabanına ait "**appDb**" detaylı olarak incelenmiştir.

The "ibdata1" file located on the disk and has a capacity of 113.789.140 KB *(108 GB (116.520.079.360 bytes))* has been found to be MySQL database file, and in order to reveal the table structure of the data, required works have been carried out. However, the schema components are not accessible because the corresponding file structure is corrupted.

"Percona Data Recovery tool-for-innodb" on **Linux Centos and Debian** operating systems for accessing and recovering data in **ibdata1** file https://www.percona.com/ and **"TwinDB Data Recovery (undrop-for-innodb)"** tools were used. https://recovery.twindb.com/

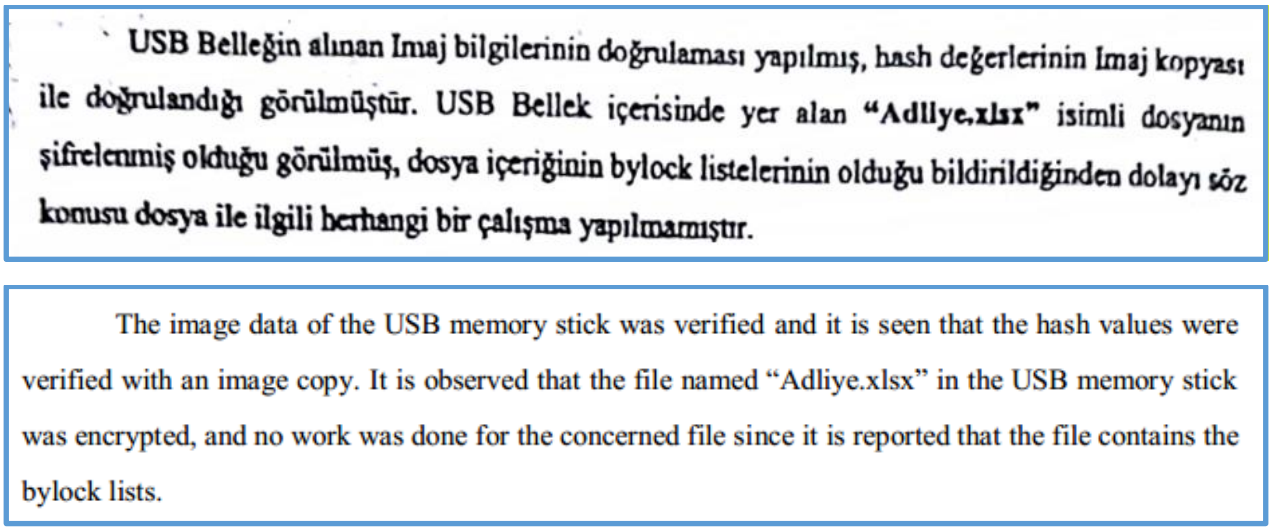
As a result of transactions with related tools, it is observed that "ibdatal" contains a total of (28) tables, contains two separate databases, named "appDb" and "Wordpress" and abbDb contains a total of (15) tables, wordpress database contains (11) tables. The appDb "belonging to the" bylock " database was examined in detail.

Resim 2: Bilirkişi raporunun verilerin bozulduğunu açıklayan ilgili bölümlerinin ekran görüntüsü ve İngilizce çevirisi.

Özetle, uzmanların oldukları bilinen bilirkişiler, dosyanın bozulduğunu ve verilerin bazı teknik yöntemlerle kurtarıldığını anlatmaktadır. Bilirkişi raporu, Litvanya'da bulunan sunucudan elde edilen verilerin bozulmuş olduğunu ve ceza davaları için yasal delil olarak kabul edilemeyeceğini açıklayan güçlü bir kanıttır.

Uzman görüşünün 25. sayfasında, Litvanya'daki sunucudan elde edilen verilerin doğruluğu ve güvenilirliği hakkında başka bir kritik bilgi daha bulunmaktadır. Raporun ilgili bölümünde, sabit sürücüde ByLock

sunucusundan elde edilen veriler dışında fazladan veri olduğu tam olarak açıklanmaktadır. İlgili bölümün ekran görüntüsü ve İngilizce çevirisi aşağıda sunulmuştur.



USB Belleğin alınan Imaj bilgilerinin doğrulaması yapılmış, hash değerlerinin Imaj kopyası ile doğrulandığı görülmüştür. USB Bellek içerisinde yer alan "Adliye.xlsx" isimli dosyanın şifrelenmiş olduğu görülmüş, dosya içeriğinin bylock listelerinin olduğu bildirildiğinden dolayı söz konusu dosya ile ilgili herhangi bir çalışma yapılmamıştır.

The image data of the USB memory stick was verified and it is seen that the hash values were verified with an image copy. It is observed that the file named "Adliye.xlsx" in the USB memory stick was encrypted, and no work was done for the concerned file since it is reported that the file contains the bylock lists.

Resim 3: Uzman görüşünün fazladan veri olduğunu açıklayan ilgili bölümlerinin ekran görüntüsü ve İngilizce çevirisi.

Bilirkişi raporunda verinin kim tarafından oluşturulduğuna dair bir bilgi bulunmamakla birlikte, verilerin yargı sürecinden önce derlendiği ve ByLock mobil uygulaması için kullanıcı listesinin bir şekilde ve büyük ihtimalle istihbarat tarafından tespit edildiğine dair güçlü bir delildir. ByLock kullanımı iddiasıyla soruşturmaların başarısız darbe girişiminden hemen sonra başladığı bilinmektedir. Bilirkişilerin inceleme için görevlendirilmeleri 27 Eylül 2016 tarihinde yapılmıştır. ByLock sunucusundan elde edilen verilerin, Türkiye CMK'sı ile uyumlu olmasa da adli işlem başlamadan istihbarat hizmeti tarafından incelendiği sonucuna varılmıştır. Yasal ve teknik düenlemelere uyulmadan sayısal verilerin dokunulmazlığını garanti etmenin hiçbir yolu yoktur ve istihbarat görevlilerine veya polis birimlerine koşulsuz güvenmek için hiçbir neden yoktur.

4.4. Verilerin Bozulduğuna İlişkin Bariz Bir Kanıt: 1970'te ByLock Kullanma İddiası[6]

1970 yılında internet yoktu, Bylock da kullanılamazdı. Ancak "Tespit ve Değerlendirme Tutanakları"na göre 1970 yılında ByLock kullandığı iddia edilen ihraç edilmiş Yüksek Mahkeme Üyeleri hakkında gözlemlenen sekiz dava dosyası vardır. Bu, Litvanya'da bulunan ByLock sunucusundan elde edilen verilerin bozuk olduğunun güçlü bir kanıtıdır.

Bylock Linux tabanlı bir uygulamadır ve Linux'ta başlangıç (takvim) tarihi (varsayılan tarih) 01 Ocak 1970 olarak ayarlanmıştır. Verilerin silinmesi, değiştirilmesi, bozulması vb. durumda ve verilerin kalan bölümü okunduğunda, 01 Ocak 1970'i veya kalan/tahrif edilmiş verilerle uyumlu ilgili tarihi görebilirsiniz. Bu tür bir sorun/tutarsızlık, verideki silme, değiştirme veya bozulmanın göstergesi olarak değerlendirilir, bu da veri bütünlüğünün bir şekilde bozulduğu anlamına gelir.

[6] https://www.meridyenhaber.com/1970-yilinda-bylock-kullanmak-makale,44630.html
İngilizcesi için: https://arrestedlawyers.org/2019/02/21/using-the-bylock-in-1970/

Bylock uygulamasının Linux tabanlı olması ve başlangıç tarihinin 01 Ocak 1970 olması nedeniyle benzer bir durumun meydana geldiği ve ByLock kullanım tarihlerinin 1970 olarak tespit edilmesinin imkansız olduğu açıktır. Litvanya'dan alınan verilerin ilgili kısmındaki silme/bozulma/değişikliğin (veya her ne ise) göstergesi olarak anlaşılmalıdır.

5. Sonuç

Tespit ve Değerlendirme Tutanakları içeriğindeki tutarsızlıklar, başsavcılık tarafından görevlendirilen teknik bilirkişileri tarafından açıklanan dosyalardaki bozukluklar, yargı süreci öncesinde veri tabanının incelendiğini gösteren bilirkişi raporunda açıklanan fazladan veriler ve 1970 yılında ByLock kullanıldığı iddiaları Litvanya'da bulunan ByLock sunucusundan elde edilen verilerin bozulmuş olduğunu kanıtlayan güçlü delillerdir.

Tutarsızlıkların nedenini anlamak, ancak orijinal delilin, bozulmamış sayısal verilerin müşterekliğinin sağlanması ve sayısal verilerin ceza yargılamasının tüm tarafları tarafından incelenmesiyle mümkün olabilir.

Bozuk sayısal veriler ceza yargılamaları için yasal delil olarak kabul edilemez. 31 Temmuz 2021

LEVENT MAZILIGÜNEY

Digitally signed by LEVENT MAZILIGÜNEY
DN: C=TR, SERIALNUMBER=29857771208, CN=LEVENT MAZILIGÜNEY
Reason: I am the author of this document
Location:
Date: 2021-08-12 15:35:55
Foxit PhantomPDF Version: 9.4.1

T. Koray PEKSAYAR
Mühendis (MS)
Adli Bilişim Uzmanı

Dr. Levent MAZILIGÜNEY
Mühendis (MS), Hukukçu
Adli Bilişim Uzmanı

* Dr. Levent MAZILIGÜNEY tarafından 31 Temmuz 2021 tarihinde yayınlanan İngilizce aslından Türkçe'ye çevrilmiştir. Her iki uzmanın sayısal olarak imzaladığı uzman görüşünün İngilizce aslı "The Accuracy and Reliability of the Digital Data Obtained from the Bylock Server in Lithuania" isimlidir ve https://www.patreon.com/posts/accuracy-and-of-54329745 bağlantısından temin edilebilir.