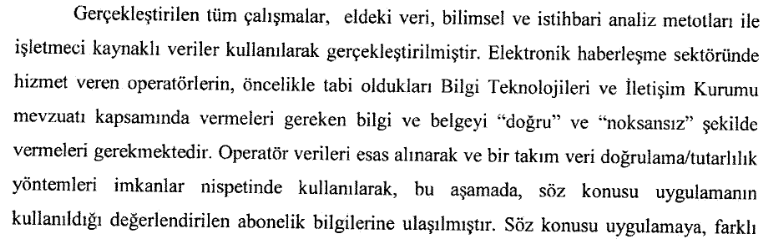
**Gerçeği Aramak**

Suçla mücadelede meşru ve haklı gerekçelerle, kanuna uygun bir şekilde mücadele edilmelidir. Binlerce dava ve komisyonlar ile verilen itiraz dilekçelerini inceleyen kurum veya şahısların, bu ilkelere azami riayet göstermeleri, son derece mühimdir. Aksi halde; darbe teşebbüsünde bulunanların işine gelebilecek mağduriyetler doğacak ve bu da darbeye ve terör örgütlerine karşı yürütülen hukuki ve milli mücadelenin boşa gitmesine sebebiyet verecektir.

Bylock programı ile şimdiye kadar kavram kargaşası yaşandığı ve bu konu ile ilgili sürekli hataların yapıldığı ve bu hatalar neticesinde mağduriyetler meydana geldiği artık herkesin malumudur. Bu nedenle konu hakkında şimdiye kadar ulaşılmış bilgilerin izahına ihtiyaç vardır. Bylockla ilgili neredeyse araştırma yapmak isteyen kişiler, doğrudan terör örgütü mensubu olma iddiasıyla tehdit edilmektedir. Halbuki gerçeğin ortaya çıkmasına mani olmak aslında terör örgütünün ekmeğine yağ sürer. Bu sebeplerle daima gerçeği bulmaya çalışılmalıdır. Gerçeği ve doğruyu arayan insanlar da hemen terör örgütü mensubu olarak yaftalamamalıdır. Tek gaye, gerçeğin ve gerçekten de suçlu olanların ortaya çıkarılması olmalıdır.

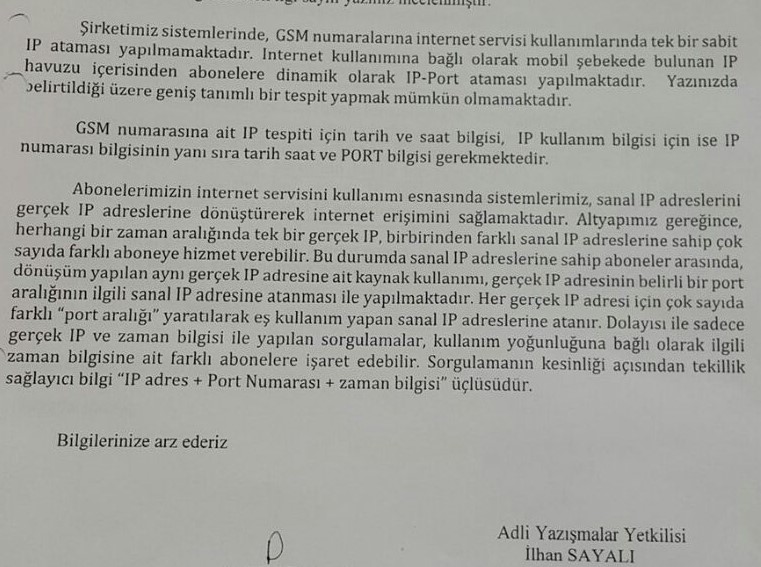
Aşağıda mahkemelere verilmiş savunma ve inceleme yazılarından derlenmiş, konuyu açıkça anlamamıza yardım edecek bilgiler verilmiştir.

MİT Müsteşarlığının ByLock uygulaması raporunun belki de en önemli bölümü Açıklama başlıklı ilk sayfasının 3. paragrafıdır (Şekil 1) ve aşağıda ekran görüntüsüne yer verilmiştir.



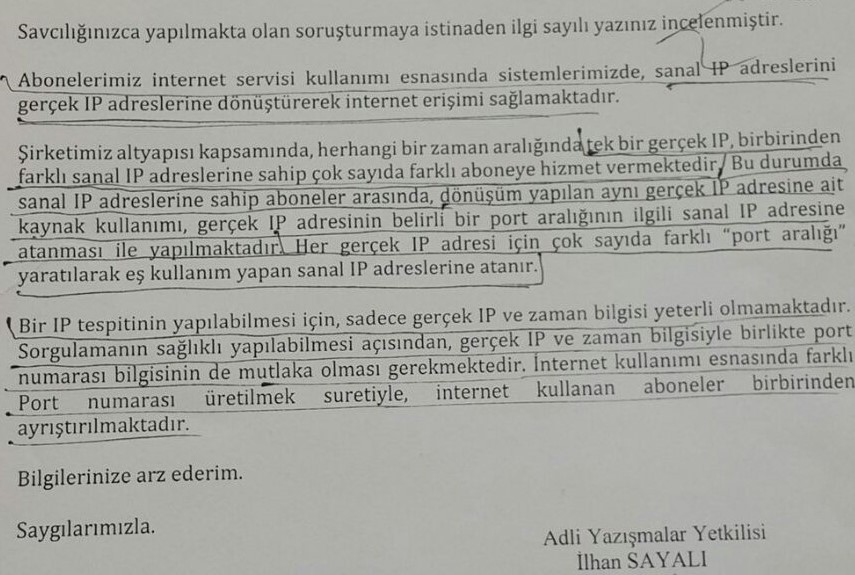
**Şekil 1. MİT Müşteşarlığının ByLock raporunun ilgili bölümü**

MİT, özetle **ByLock kullanıcılarının hatasız tespit edilebilmesi için operatörlerin (Avea (TürkTelekom), Turkcell, Vodafone, Superonline, Digiturk, vb.) yasal sorumlulukları gereği doğru ve noksansız bilgi vermelerine bağlı olduğunu vurgulamaktadır.** Burada, MİT yasal sorumluluğun aslen operatörlerde olduğunu da dolaylı olarak belirtmektedir. Mahkemelerce örneğin Avea(Türk Telekom)’a yazılan yazılarda, (şuan bütün GSM operatörleri bu uygulamayı kullanarak abonelerine hizmet vermekte) ByLock sorgulamalarına yönelik önemli bir cevap (Şekil 2) ise özetle şu şekildedir:

  
**Şekil 2. Avea(Türk Telekom) firmasının 28.06.2017 tarihinde verdiği cevap içeriği**

Avea(Türk Telekom) uygulamayı aslında kullanmayan bir kişinin kullanmış gibi görünebileceği bazı alternatiflerden bahsederek **SANAL IP – PORT** atamadaki sıkıntıları gözler önüne sermektedir.

**Şekil 3. (Türk Telekom) firmasının 26.05.2017 tarihinde verdiği ikinci çok önemli cevap içeriği**

****

**Şekil 3.Türk Telekom( AVEA) yazısı**

MİT Raporu 15. Sayfasında ise, tespit çalışmalarının MİT Kanunun 6. Maddesi (d) bendi kapsamında istihbarat yetkisi kapsamında gerçekleştirildiği belirtilmiştir. Dolayısıyla, Emniyet Genel Müdürlüğü açıkça, MİT ise zımnen (dolaylı olarak) istihbari bilgi hususunu vurgulamakta ve idari ve adli işlemlerde kullanılması sorumluluğunu üstlenmemektedir.

**Ortada tespit aşamasında aktif olan kurumlar tarafından sorumluluğu doğrudan kabul edilmeyen ancak idari ve adli işlemlerde kullanılan bir bulgu söz konusudur.** Peki bu durumda, **"bir masumun cezalandırılmasındansa, bir suçlunun cezasız kalması tercih edilir"** (Cesare Beccaria) evrensel ilkesiyle vicdanen sorumlu olan hakim ve savcılarımız uzman olmadıkları bir alanda 7,5 yıl hapis cezasını neye göre karara bağlamaktadır?

Bu kapsamda, **Adli Veri İnceleme Teknik Raporlarının idari ve adli süreçlerdeki en kıymetli ve muteber veri olduğunu yadsınamaz bir gerçektir.** **ByLock uygulamasının örgüt tarafından yoğun kullanıldığı anlaşılmakla birlikte, iddianamelerde belirtildiği gibi üst düzey üyelerin daha farklı yöntemler kullandığı değerlendirilmektedir. Bu nedenden dolayı ilk olarak ByLock uygulamasının özellikleri teknik olarak tanımlanmak zorundadır.   
  
Buna göre;**

### ByLock güvenli mobil iletişim uygulaması nedir?

(1) ByLock, geliştiricisi tarafından **“kullanıcılar arasında güvenli ve gizli haberleşme olanağı sunan bir iletişim uygulaması”** olarak tanımlanan bir uygulamadır.

(2) **ByLock uygulaması yalnızca mobil cihazlarda (tablet, telefon) çalışacak şekilde tasarlanmış bir uygulamadır**. Masaüstü ve dizüstü bilgisayarlarda çalışmamaktadır. Uygulama incelendiğinde;

(a) Şifreli anlık mesajlaşma,

(b) Şifreli sesli görüşme,

(c) Grup mesajlaşması,

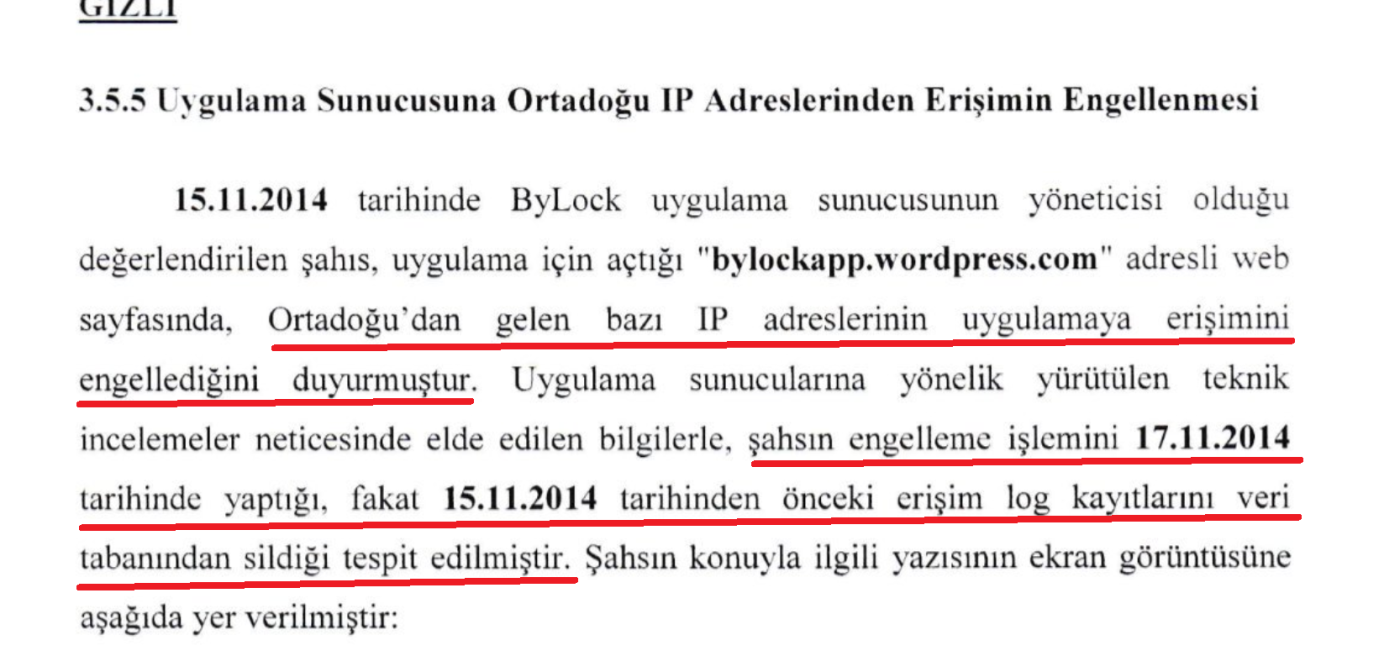
(ç) Dosya paylaşımı,

(d) E-posta gönderme,

(e) Arkadaş ekleme özelliklerinin bulunduğu görülmüştür.

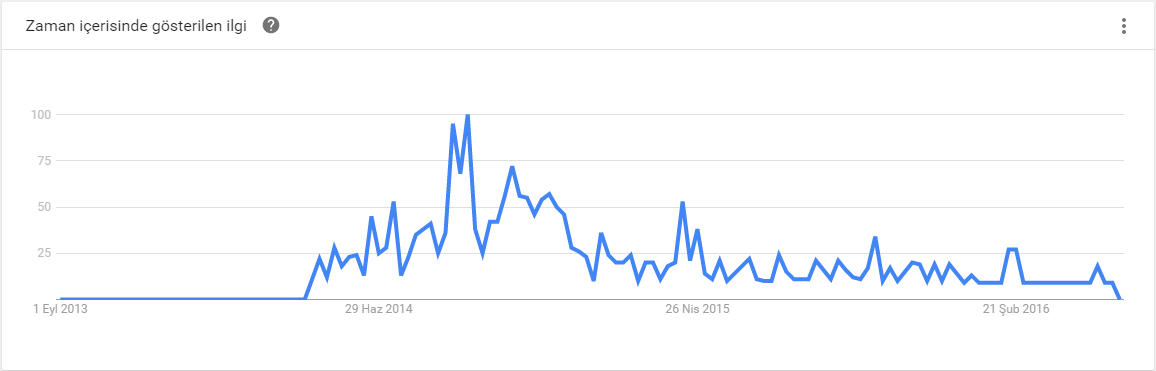
(3)**ByLock uygulaması Google Play ve App Store uygulama mağazasında halihazırda bulunmamaktadır** ancak, internet üzerinde yayın yapan çeşitli uygulama mağazalarında ByLock Android uygulama paketi dosyası bulunabilmektedir.

(4) **15 Kasım 2014 tarihinin program kullanıcıları için VPN kullanım çağrısı olarak algılanabileceği değerlendirilmektedir.** *(MİT Raporunun 25. Sayfasında bu konuya değinilmiş ve 17 Kasım 2014 tarihinde tamamına yakını Türkiye kaynaklı IP adreslerinin erişiminin engellediği ve 15 Kasım 2014 öncesi erişim LOG kayıtlarının veri tabanından silindiği belirtilmiştir).*

  
 (5) MİT Raporunun 26. sayfasında VPN kullanılmasının şart koşularak kullanıcı tespitinin engellenmeye çalışıldığının anlaşıldığı belirtilmiştir. David KEYNES tarafından ***“bir milyon civarındaki beklenmedik sayıdaki kullanıcı”*** bilgisi açık kaynaklardan 15 Kasım 2014 tarihine kadar Google Play Store ve Apple App Store üzerinden 600.000 üzerinde şeklinde doğrulanabilmekte ve MİT raporunda da bu şekilde belirtilmektedir.

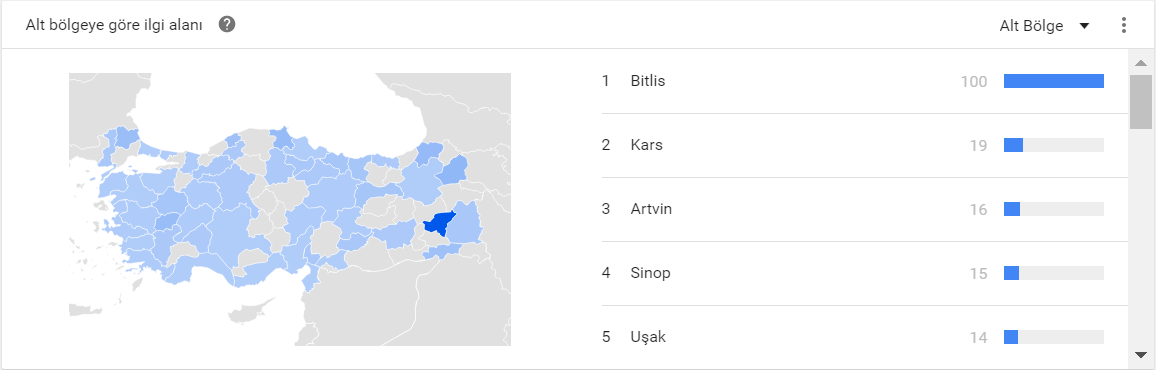
(6) 15 Kasım 2014 tarihine kadar uygulamanın dileyen herkes tarafından indirilmesi ile FETÖ (Fetullahçı Terör Örgütü) üyelerinin perdelenmeye çalışıldığı; 15 Kasım 2014 sonrasında ise VPN kullanım zorunluluğu ile hem tespitin engellenmeye çalışıldığı hem de perdelemenin bir kat daha artırıldığı değerlendirilmektedir.

(7) İnternet üzerinden yayın yapan basın kuruluşlarının 28 Ekim 2016 tarihinde yayınlanmış olduğu haberler incelendiğinde, Adalet Bakanı Bekir BOZDAĞ’ın ABD ziyareti sırasında gazetecilerin ByLock uygulaması ile ilgili yönelttiği bir soruya **“ByLock'a referansla giriliyor. Sizi akredite etmesi gerekiyor. Karşı taraftaki kişinin sizi kabul etmesi gerekiyor. Sonra size bir şifre veriyorlar. Elim değdi indirdim veya AppStore'dan aldım demeleri mümkün değil belli bir süre duruyor orada sonra indiriyorlar.”** şeklinde cevap vermiştir.



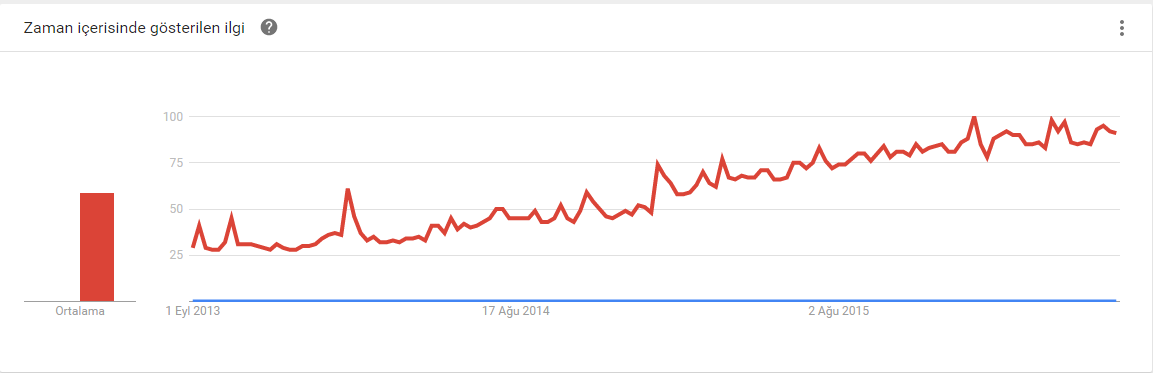
**Şekil 4. 01.09.2013-31.05.2016 tarih aralığı Türkiye ByLock arama grafiği**

Şekil 4'da görülen 01 Eylül 2013 ve 31 Mayıs 2016 tarihleri arası trend incelemesinde, ByLock aramalarının Mayıs 2014’te başladığı, öncesindeki aramaların göreceli olarak sıfır veya sıfıra yakın olduğu görülmektedir. Aramalar Eylül-Ekim 2014 tarihlerinde zirve yapmış ve sonrasında azalarak Mayıs 2016 itibariyle tekrar göreceli olarak sıfırlanmıştır. Türkiye’de aynı tarih aralığında aramaların yoğunlaştığı ilk beş il ve diğer illerin göreceli durumu Şekil 5'de görülmektedir. **Bitlis ilinin diğer illere oranla (en yakın ilin yaklaşık 5 katı) durumu dikkat çekicidir**. Ankara, İzmir, İstanbul gibi büyük ve nüfusu kalabalık illerin, diğer illerden farklı olmayışı da dikkat çekicidir.



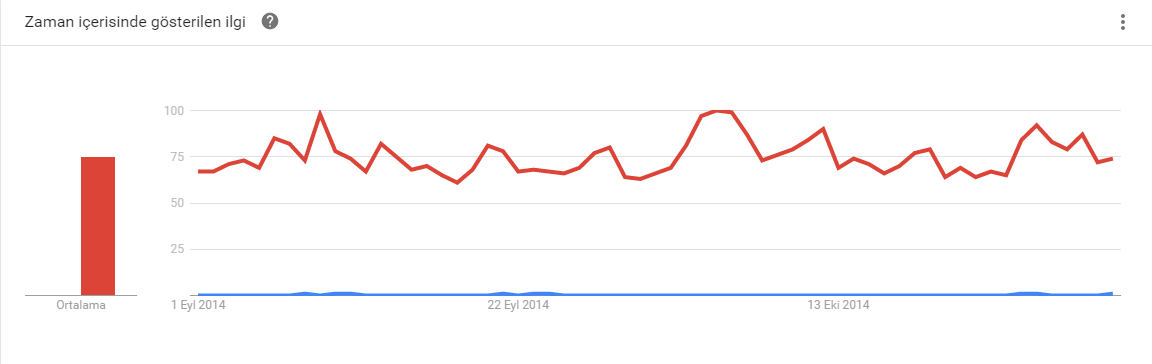
**Şekil 5. 01.09.2013-31.05.2016 tarih aralığı Türkiye bölgesel ByLock arama grafiği**

1. **Bölüm sonu**



**Şekil 6. ByLock ve WhatsApp Türkiye arama karşılaştırması** **(Kırmızı- WhatsApp, Mavi- ByLock)**

Trend uygulaması ile farklı kelimeler de karşılaştırılabilmektedir. Şekil 6’de yaygın kullanılan WhatsApp ve ByLock kelimeleri karşılaştırılmıştır. Sonuç olarak ByLock 01 Eylül 2013-31 Mayıs 2016 arası dönemde her zaman WhatsApp’a oranla sıfır veya sıfıra yakın değerde trende sahiptir. Tarih aralığı daraltılarak ByLock uygulamasının yaygın arandığı 01 Eylül 2014-31 Ekim 2014 aralığı incelendiğinde de Şekil 7’te görülebileceği gibi durum değişmemektedir.



**Şekil 7. ByLock ve WhatsApp Türkiye arama karşılaştırması (01.09-31.10.2014 aralığı) (Kırmızı WhatsApp, Mavi ByLock)**

Bu grafikler açık bir şekilde göstermektedir ki, ByLock en yoğun kullanıldığı Türkiye’de dahi, çok sınırlı sayıda kişi tarafından merak edilmiş ve kullanılmıştır.

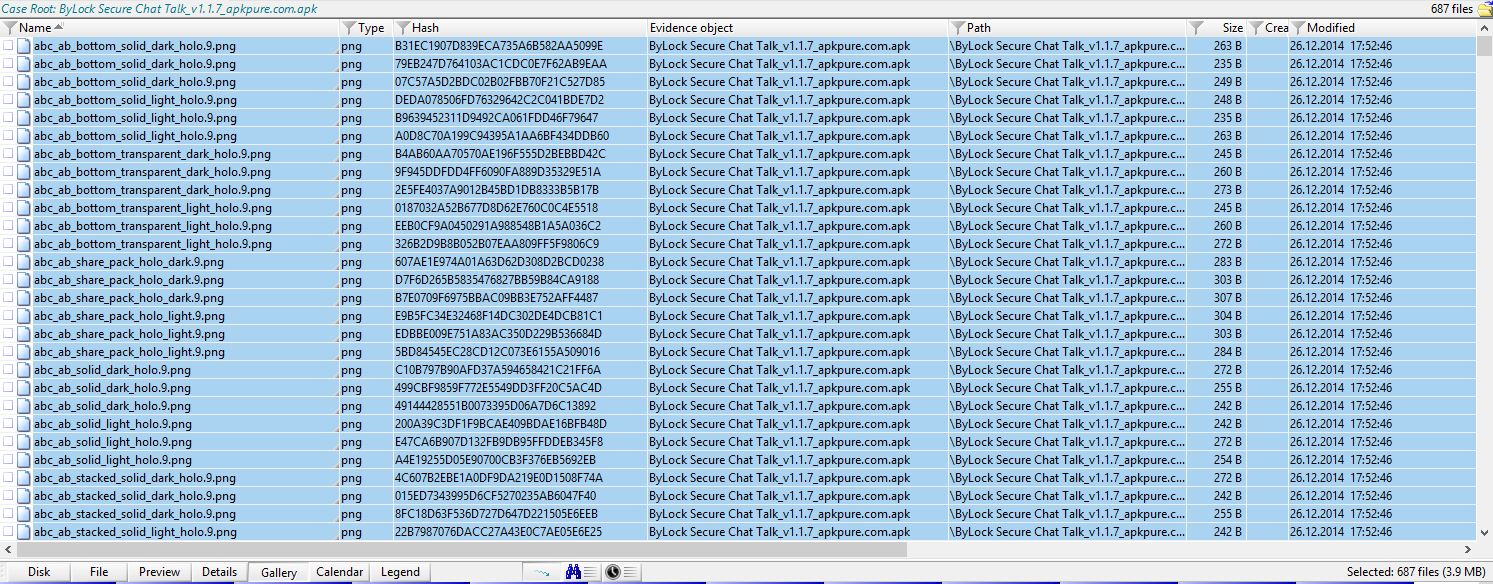
### ByLock uygulamasının teknik incelemesi

(1) ByLock güvenli iletişim uygulamasını incelemek maksadıyla **internet üzerinde yapılan araştırma sonucunda, Google Play uygulama mağazası haricinde tespit edilen “ByLock Secure Chat Talk\_v1.1.7\_apkpure.com.apk”** ByLock Android uygulama paketi indirilmiş öncelikli olarak yazılım kaynak kodları, müteakiben uygulamanın kurulum dosyaları ve ekran görüntüleri incelenmiştir.

(2) **ByLock uygulamasının kaynak kod incelemesinde tespit edilen hususlar aşağıya çıkarılmıştır.**

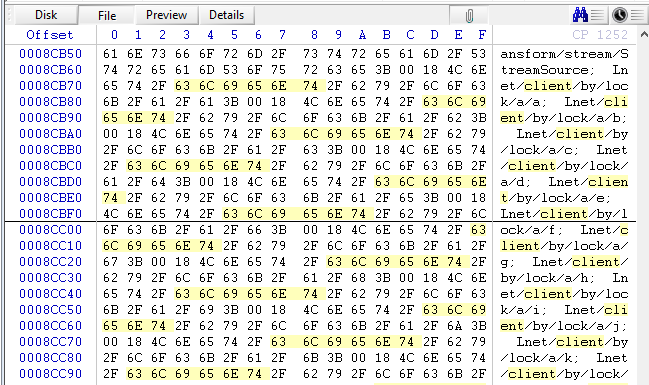
(a) “apk” uzantılı Android uygulama paketi dosyaları sıkıştırılmış dosyalardır. İnternetten indirilen **“ByLock Secure Chat Talk\_v1.1.7\_apkpure.com.apk”** dosyası adli bilişim yazılımı tarafından genişletildiğinde (extracted) toplam (687) adet dosya olduğu görünmektedir. Tespite ilişkin ekran görüntüsü Şekil 8’te sunulmuştur.

(b) “apk" dosyası genişletilip içeriğindeki dosyalar çıkarıldığında ana program kodunu içeren **“classes.dex”** adlı dosya içerisinde ikili dosya düzenleyicisiyle kelime ve anlamlı harf dizileri arandığında uygulama hakkında ayrıntılı bilgi edinilmektedir.



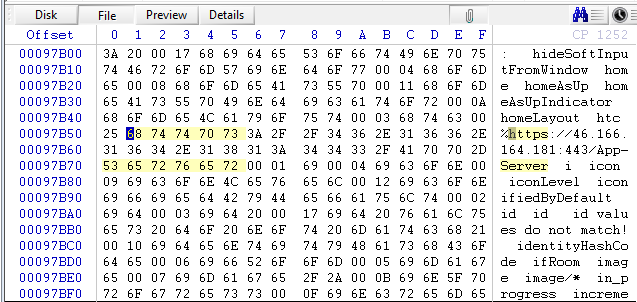
**Şekil 8. “ByLock Secure Chat Talk\_v1.1.7\_apkpure.com.apk” dosyası içeriğinde 687 adet dosya bulunmaktadır.**

(c) İnternet üzerinde yapılan araştırma sonucunda tespit edilen “ByLock” uygulama paketinin incelemesinde, “ByLock” yazılımının Java sınıfı adının **“net.client.by.lock”** olduğu bilgisi edinilmektedir. Tespite ilişkien ekran görüntüsü Şekil 9’de sunulmuştur.



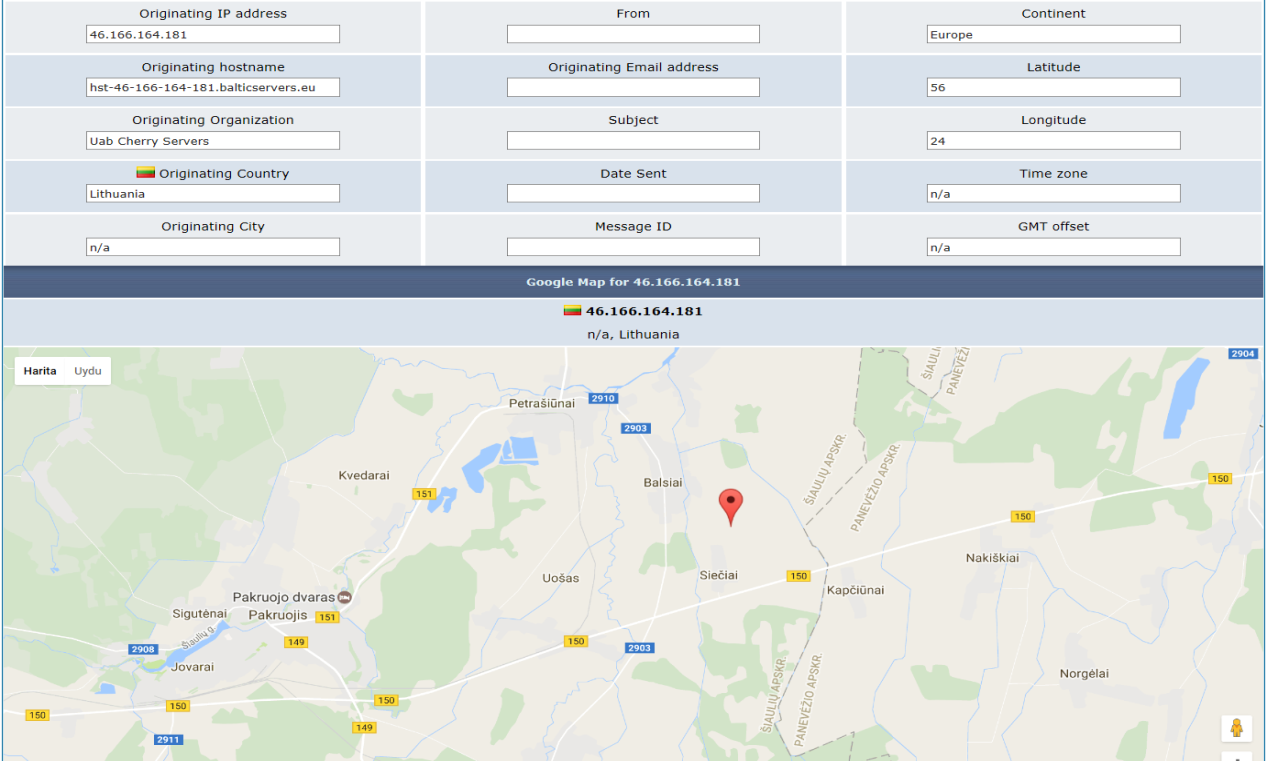
**Şekil 9. “classes.dex” dosya içerik analizi**

(ç) **“classes.dex”** adlı dosya içerisinde ikili dosya düzenleyicisiyle kelime ve anlamlı harf dizileri arandığında yazılımın dış dünyayla olan ilişkisini kurduğu sunucu adresi tespit edilebilmektedir. Tespite ilişkin ekran görüntüsü Şekil 10'da sunulmuştur.



**Şekil 10. “classes.dex” içerik analizi**

(d) Şekil-5’te yazılımın internet üzerinden iletişim kurduğu sunucusunun “**https://46.166.164.181/App-Server**” adresi olduğu görünmektedir. Tepit edilen 46.166.164.181 IP adresinin internetteki açık kaynaklar üzerinde yapılan arama sonucu Şekil 11'de sunulmuştur:



**Şekil 11. 46.166.164.181 IP adresinin tespiti**

• Sunucunun Litvanya’nın Sieciai bölgesinde kurulu olduğu,

• Sunucunun ‘Balticservers’ adlı ağ üzerinde bulunduğu

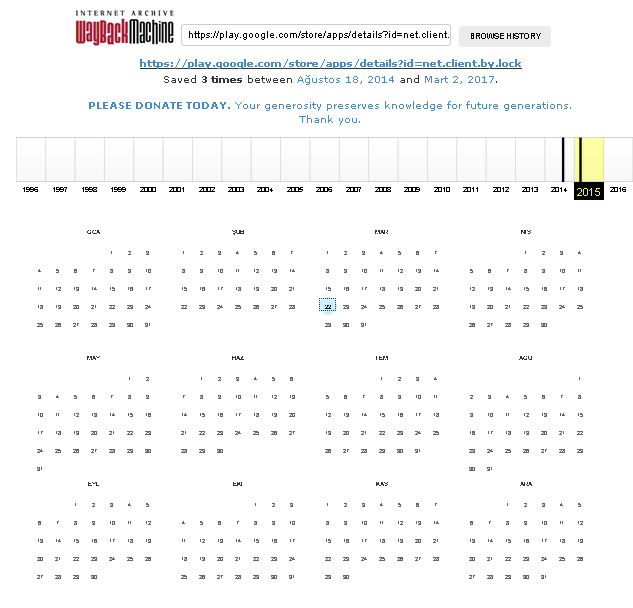
• Sunucu adının ‘hst-46-166-164-181.balticservers.eu’ olduğu,

• Sunucunun barındırıldığı firmanın web adresinin **“balticservers.eu”** olduğu bilgileri elde edilmektedir.

(e) “net/client/by/lock/” dizini altında “c/b.java” ve “f/p.java” dosyalarında görülen “https://46.166.164.181/App-Server” adresinde çalışan uygulama sunucusunun mobil uygulamanın çeşitli işlevlerini gerçekleştirdiği anlaşılmaktadır.

(f) ByLock uygulamasının Google Play uygulama mağazası adresinin [**https://play.google.com/store/apps/details?id=net.client.by.lock**](https://play.google.com/store/apps/details?id=net.client.by.lock) olduğu belirlenmiştir. Söz konusu uygulama adresi kontrol edildiğinde uygulamanın yayında olmadığı görülmüştür.

(g) İnternet sitelerinin arşiv bilgisini tutan [**https://web.archive.org**](https://web.archive.org) internet sitesi üzerinde uygulamaya yönelik yapılan araştırmada, uygulama sayfasınınnın yedeğinin en son 22.03.2015’te alındığı görülmektedir (Şekil 12).



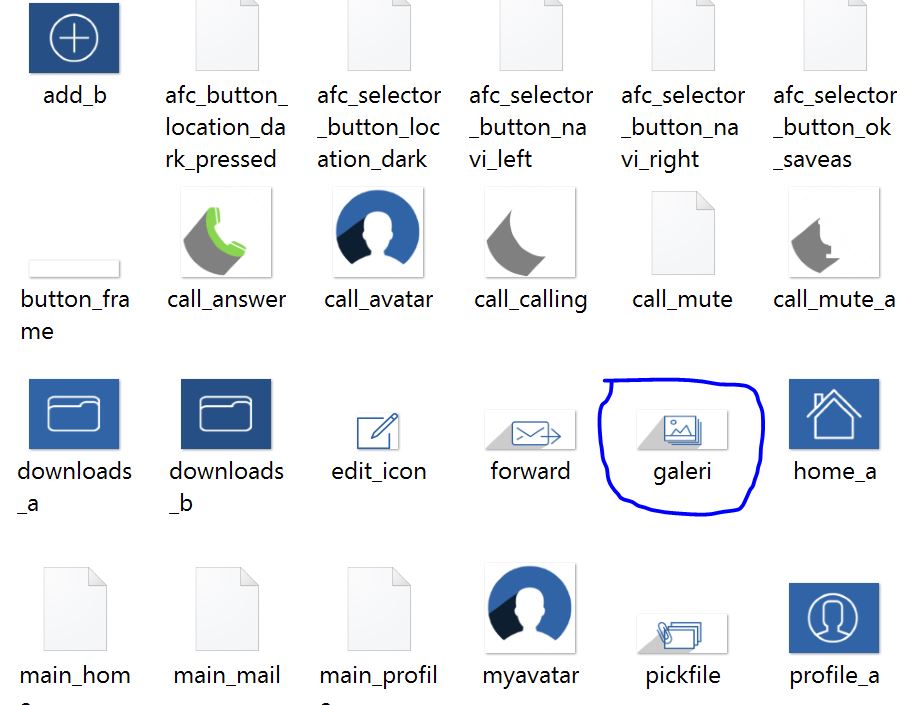
**Şekil 12.** [**https://web.archive.org**](https://web.archive.org) **uygulama kaydı**

(ğ) 22 Mart 2015 yılında otomatik olak alınan yedekteki e-posta bağlantısından program geliştiricisinin **“keynes97209@gmail.com”** adresini kullandığı görülmüştür.

(h) ByLock uygulamasının kurulum dosyaları ve ekran görüntüleri incelendiğinde;

- Dosya isimlerinin tümünün İngilizce olmasına karşın **“galeri”** isminin Türkçe yazılmış olması,

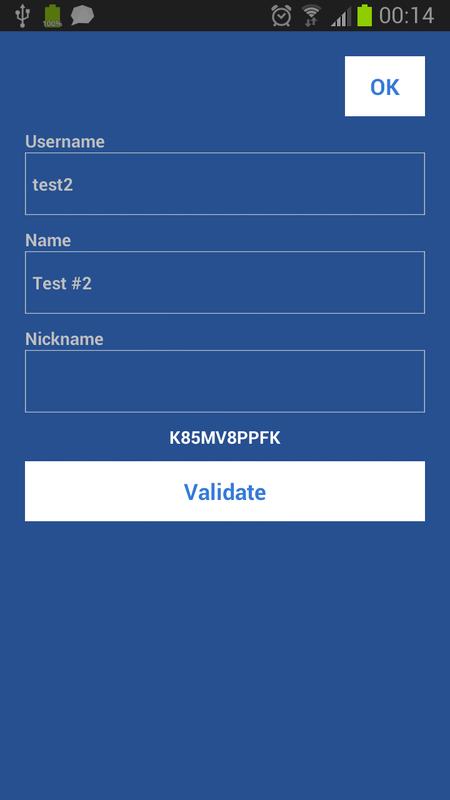
- “net/client/by/lock/a/c.java” dosyasında **“Sesli Arama”** ibaresi dikkat çekmiştir (Şekil 13).

**Şekil** **13. ByLock uygulaması kaynak kodları**

**ByLock uygulamasının kurulumu sonrasında tespit edilen hususlar aşağıya çıkarılmıştır;**

(a) ByLock uygulaması mobil cihaza yüklendikten sonra kullanıcı için bir isim (name) ve bir de programı kullanacağı zaman gireceği kullanıcı adınının (username) belirlenmesi gerekmektedir. Ayrıca her kullanıcı için program tarafından otomatik olarak üretilen (10) karakterli bir “ID” ***(bir çeşit telefon numarası gibi düşünülebilir)****.* giriş penceresi altında gösterilmektedir (Şekil 14).



**Şekil** **14. ByLock uygulaması kullanıcı kayıt ekranı**

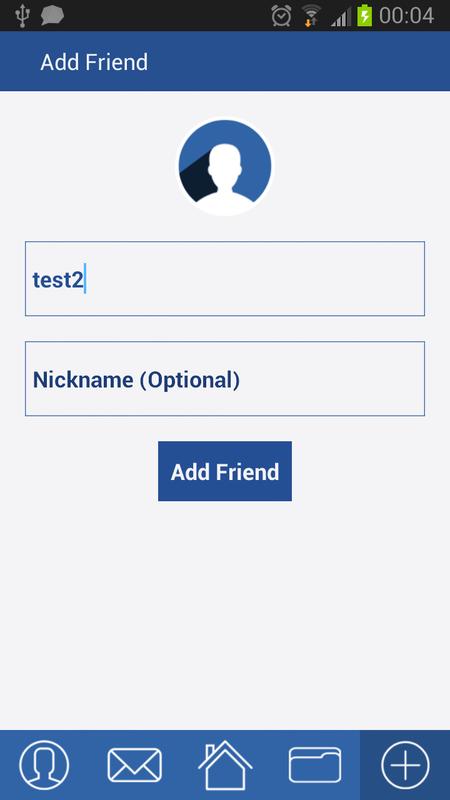
(b) ByLock’un haberleşme aracı olarak Whatsapp ve türevlerinden temel bir farkı bulunmamaktadır. Diğer haberleşme uygulamalarından farklı olarak;

(1) Kullanıcılardan telefon numarası veya e-posta adresi talep edilmemektedir.

(2) E-posta ve SMS doğrulması yapılmamaktadır.

(3) Karşılıklı iletişim kurulması aşamasında Whatsapp ve türevi uygulamalarda olduğu gibi **ByLock kontak listesini (rehber) otomatik olarak eşleştirilmemektedir.**

(c) Kayıt işlemi tamamlandıktan sonra Şekil 15'de gösterilen arkadaş ekleme penceresini kullanarak arkadaşlarının takma adı (Nickname) veya program tarafından verilen 10 karakterli “ID” girilmesi gerekmektedir. Eklenen arkadaş otomatik olarak arkadaş listesine ilave edilmektedir *(Herhangi birinin telefonuna onu zan altına bırakmak için ByLock uygulaması yüklense dahi bir kişi ile iletişime geçebilmesi için yine bu “10 karakterli ID”yi ve Nicname bilgisini girilmek zorundadır.)* **Mevcut yapı incelendiğinde,uygulama üzerinde daha önceden birbirini tanıyan veya karşılıklı ID bilgilerini paylaşarak birbirini uygulamada ekleyen kişilerin iletişim kurabildiği görülmektedir.**



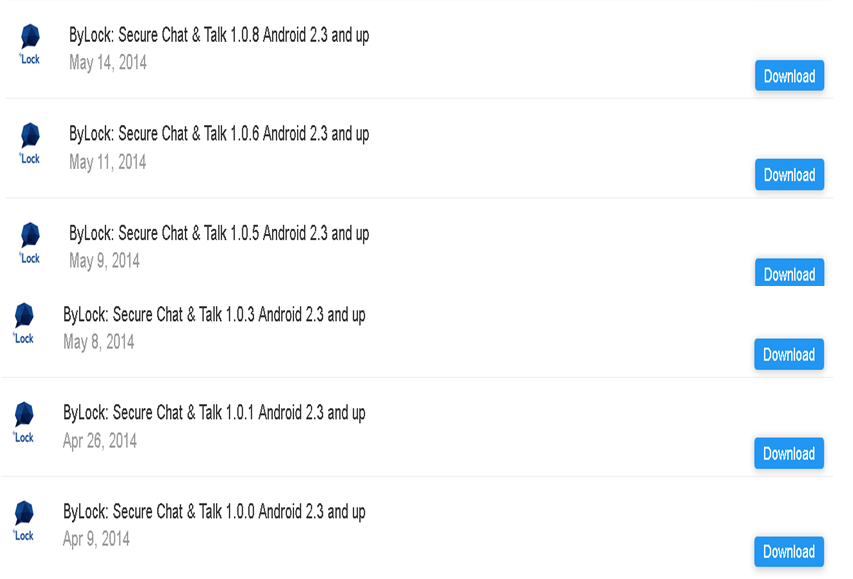
**Şekil 15. ByLock arkadaş ekleme giriş ekranı**

(ç) ByLock’un uygulamasının konuşma ekranı Şekil 16’de gösterilmiştir.

****

**Şekil 16. ByLock konuşma ekranı**

(d) Mobil cihaz uygulamalarının yükleme ve geçmiş versiyonlarını sorgulama amacıyla kullanılan <https://m.downloadatoz.com> internet sitesi üzerinde yapılan incelemeden elde edilen ByLock uygulaması versiyon bilgileri Şekil 17'te sunulmuştur. **Versiyon bilgileri incelendiğinde en son güncellemenin 24 Aralık 2014 tarihinde yapıldığı görülmektedir.**

  
Şekil 17. **https://m.downloadatoz.com/ByLock-secure-chat-talk/net.client.by.lock/ByLock-secure-chat-talk,v1.1.3.html**

### ByLock uygulamasının mobil cihaz üzerinde kullanıldığı tespit edilebilir mi?

(1) Mobil cihaz üzerinde kullanılan ByLock uygulamasının kesin olarak tespiti konusunda inceleme yapılabilmesi için adli bilişim yazılım ve donanımları kullanılarak adli kopyasının alınmasına ihtiyaç duyulmaktadır. Mobil cihazlar üzerinden **fiziksel kopya** *(Fiziksel adli kopyanın temel mantığı, işletim sisteminin orijinal boot loader’ını başka bir loader ile değiştirerek sistem kaynakları üzerinde Ring-0 (kernel düzeyi) düzeyinde veya yazılım bütünlüğü içinde fiziksel bir erişim yetkisine kavuşmaya dayanmaktadır)* ve **mantıksal kopya** *(Mobil cihazın aktif dosya sisteminde yer alan dosyaları başka bir sisteme kopyalayıp, inceleme işlemine verilen addır.)* olmak üzere iki türlü kopya alma işlemi yapılabilmektedir.

**(2) Android işletim sitemini kullanan mobil cihazlarda;**

(a) Fiziksel adli kopya işlemi yapılabilmesi için öncelikle mobil cihaz üzerinde “Geliştirici Seçenekleri” ve “Bilinmeyen Kaynaklar” sekmeleri aktif hale getirilmelidir.

(b) Mobil cihazların incelenmesinde kullanılan adli bilişim yazılımları, mobil cihazlar üzerine yüklemiş oldukları ajan ile cihazın fiziksel kopyasının alınmasını sağlamaktadır. Bu işlem tüm marka ve model mobil cihazlar için geçerli değildir. Adli bilişim yazılımları ile otomatik olarak fiziksel kopyası alınamayan mobil cihazlara manuel olarak “ROOT” işlemi yapılarak “SuperSU” uygulaması yüklenmelidir.

(c) Mobil cihazlar üzerinde manuel olarak yapılan “ROOT” işleminin yapılamaması *(Mobil cihazın marka, model ve işletim sistemine uygun bootloader yazılımının bulunamaması durumunda ROOT işlemi sırasında mobil cihazın fabrika ayarlarına dönme veya işletim sisteminin çökmesi gibi riskler bulunmaktadır.)* gibi durumlarda mantıksal kopya alma işlemi yapılmaktadır.

(ç) Hali hazırda Google Play ve App Store uygulama mağazaları haricinde çeşitli mobil cihaz uygulama mağazalarında bulunan ByLock uygulaması indirilerek sıkıştırılmış dosyalar genişletilmeli, uygulama içerisinde bulunan tüm dosyaların sayısal imza seti (MD5, SHA-1) oluşturularak adli bilişim yazılımı içerisine eklenmelidir.

(d) Mobil cihaz kopyası üzerinde adli bilişim yazılımları ile veri kurtarma işlemi yapılmalı, mevcut ve kurtarılan tüm verilerin saysısal imzası (MD5, SHA-1) hesaplanmalıdır.

(e) Adli bilişim yazılımları ile ByLock uygulaması sayısal imza seti ile mobil cihaz üzerinden tespit edilen sayısal imzaların karşılaştırması yapılmalı, eşleşen dosyalar raporlanmalıdır.

(f) Mobil cihaz etiketinde belirtilen IMEI numarası ile adli bilişim yazılımı ile tespit edilen IMEI numarası karşılaştırılmalıdır.

(g) Mobil cihazın kopyası üzerinde bulunan tüm veriler *(fiziksel kopyada silinmiş alanlar da dahil edilir)* adli bilişim yazılımı ile indekslenmeli, belirlenen anahtar kelimeler ile indeks üzerinde arama yapılmalıdır.

(ğ) Mobil cihaz ile entegre çalışan bulut veri depolama alanları adli bilişim yazılımları kullanılarak incelenmeli, bulut depolama alanları üzerinde kurulan uygulamalara ait veriler incelenmeli, belirlenen anahtar kelimeler ile arama yapılmalıdır.

(h) Mobil cihaz sahibinin cihaz ile entegre çalışan e-posta adresi kullanılarak yüklenen uygulamalara ait bilgiler uygulama mağazalarından tespit edilmelidir.

**(3) iOS işletim sitemini kullanan mobil cihazlarda;**

(a) iOS işletim sistemini kullanan mobil cizalarda *(iPhone 4S üzeri)* fiziksel kopyalama işlemi yapılamamaktadır. iOS cep telefonları üzerinde yapılan incelemeler mantıksal kopya üzerinde yapılmaktadır.

(b) Mobil cihaz etiketinde belirtilen IMEI numarası ile adli bilişim yazılımı ile tespit edilen IMEI numarası karşılaştırılmalıdır.

(c) Mobil cihazın kopyası üzerinde bulunan tüm veriler adli bilişim yazılımı ile indekslenmeli, belirlenen anahtar kelimeler ile indeks üzerinde arama yapılmalıdır.

(ç) Mobil cihaz ile entegre çalışan bulut veri depolama alanları adli bilişim yazılımları kullanılarak incelenmeli, bulut depolama alanları üzerinde belirlenen anahtar kelimeler ile arama yapılmalıdır.

(d) Mobil cihaz sahibinin cihaz ile entegre çalışan e-posta adresi kullanılarak yüklenen uygulamalara ait bilgiler uygulama mağazalarından tespit edilmelidir.

### g. ByLock kullanımı delil olabilir mi?

(1). ByLock uygulamasının mobil cihaz üzerinde tespit edilmesi sonucunda, kullanıcının bilerek isteyerek uygulamayı yüklemesi yanında bilinçsiz veya tuzak kurularak yüklenmiş olması olasılığının bulunduğu göz ardı edilmemelidir. **Konuşma içeriği tespit edilememesi durumunda kişinin kullanıldığı mobil cihazı ile diğer dijital eşyaları eş zamanlı olarak incelenmelidir.**

(2). Mobil cihaz kullanılarak ByLock sunucusuna yapılan bağlantıların tespit edilmesi, yapılan yazışmaların belirlenmesi, yazışmalar kapsamındaki suç unsurlarının ve suçların eyleme geçirildiğinin netleştirilmesi sonucunda şahsın örgüt üyeliğinin tespitini sağlayabileceği değerlendirilmektedir.

(3) Ülkemizde, geçtiğimiz yıllarda kamuoyunda Ergenekon davası olarak bilinen yargılamada kararını açıklayan Yargıtay 16. Ceza Dairesi, dijital delillerle alakalı şu ifadeleri kullanmıştır:

“… *tamamı ‘dijital delil’ olarak adlandırılan,* ***suistimale müsait olan verilerin****…* (sayfa 32, EK-2)” “***Dijital delillere harici müdahalenin teknik olarak mümkün olması****, çoğu zaman kim tarafından hangi tarihte müdahale yapıldığının da belirlenememesi karşısında…* (sayfa 34, EK-2)”.

(4). ByLock kullanıcılarının tespitinin yapılma işleminin ByLock sunucusunun hacklenerek elde edildiği bilgisi basında yer almaktadır. Bu işlem doğru ise kanunsuz elde edilen delilin delil olarak kabul edilmeyeceği hususu göz ardı edildiği değerlendirilmektedir. Konu ilgili yargı mercilerince yapılan hukuki değerlendirme   
Şekil **18**'te sunulmuştur.

|  |
| --- |
| ***Ek Bilgi;*** *Ceza usul hukukunda, re ’sen araştırma ilkesi ve vicdani delil sistemi geçerli olup, amaç maddi gerçeğe ulaşmaktır. Maddi gerçek, hukuka uygun elde edilen her türlü delille ispatlanabilir. Anayasa'ya göre, kanuna aykırı olarak elde edilen bulgular delil olarak kullanılamaz (m.38/6). CMK uyarınca, yüklenen suç, ancak hukuka uygun şekilde elde edilmiş olan delillerle ispat edilebilir (m. 217/2). Delil, kanuna aykırı olarak elde edilmişse, ret olunur (m.206/2-a). Hükmün hukuka aykırı yöntemlerle elde edilen delile dayanması, hukuka kesin aykırılık sebebidir (m. 289). Hukukun uygulanmasında hukuka uygun olmayan bir şeyin üzerine meşru bir şey bina edilemez. Örneğin, yasak yöntemlerle alınan savunmada belirtilen adreste hukuka uygun bir arama yapılsa bile elde edilen deliller hukuka aykırı olacaktır. Buna “hukuka aykırı delillerin dolaylı etkisi, uzak etkisi” ya da “zehirli ağacın meyvesi de zehirlidir” denilmektedir. Bu itibarla ikrar olarak kabul edilen bu itiraflar mahkûmiyet için geçerli ve yeterli değildir. Sanığın ifade, sorgu ve savunmasının alındığı aşamalarda hukuk kurallarına uyulmadan yapılan arama sonucu (suç eşyasının) bulunduğuna dair arama zabıtları önüne konulan ve böylece köşeye sıkıştırıldığını hisseden sanık bu baskı altında itirafta bulunmak zorunda kalabilir. Sanığın hissettiği bu baskı ve köşeye sıkışmışlık, CMUK'nun 135/a (CMK m. 148) maddesinde sayılan yasak yöntemler arasında bulunmamakla birlikte, hukuka aykırı arama ile elde edilen deliller bulunduğuna dair tutanağın kendisine her ifade alınışında gösterilmesinden kaynaklanmaktadır. Böylece sanıktan, hukuka aykırı elde edilmiş delil sayesinde itiraf-ikrar delili elde edilmiş, sanığın kendisini suçlaması sağlanmıştır. CMUK'nun 254/2. (CMK m. 148/3, 217/2) maddesi hükmüne göre bu itiraf hükme esas alınamaz.*  *Yargıtay Ceza Genel Kurulunun 25.11.2014 tarih ve 2014/166-514 sayılı Kararında; "Hukuka uygun olmayan arama işlemi sonucunda ele geçen delillerin hükme esas alınamayacağının belirlendiği olayda; ... arama işleminin hukuka aykırı yapılması nedeniyle ele geçirilen ruhsatsız tabancanın hukuka aykırı yöntemle elde edilmiş olmasından dolayı hükme esas alınmayacağı... başkaca maddi delillerle desteklenmeyen ikrara dayanılarak mahkûmiyet hükmü kurulması usul ve kanuna aykırıdır." Bu şekildeki arama işleminden sonra ele geçen ve ispat aracı olarak yararlı görülen değerlere ilişkin el koyma işleminin sulh ceza hâkimi tarafından onaylanması da arama işlemini geriye dönük olarak hukuka uygun hale getirmeyecektir.*  *Anayasa Mahkemesi de, 19.11.2014 tarih ve 2013/6183 Başvuru Numaralı Kararında, ihtiyar heyetinden veya komşulardan iki kişi bulundurulmadan yapılan arama sonucunda elde edilen hukuka aykırı delillerin hükme esas alınarak adil yargılanma hakkının ihlal edildiğine karar verdiği gibi Yargıtay CGK bir kez daha (28.04.2015 tarih ve 2013/464, 2015/132 sayılı Kararda), arama işleminin, arama tanıkları (komşu veya ihtiyar heyetinden) kimseler hazır edilmeden yapılması sonucu elde edilen delillerin hukuka aykırı olduğunu belirtmiştir.*  *Açıklanan pozitif hukuk normları, Anayasa Mahkemesi ve CGK Kararları karşısında; “hukuka aykırı biçimde” elde edilen deliller hükme esas alınamaz. Bu husus, Avrupa İnsan Hakları Sözleşmesi’nin 6. maddesinde yer alan ve Anayasamıza da eklenen (m. 36) adil yargılanma hakkının gereğidir.* |

**Şekil 18. Delillerin hukukiliği konusunda yargı mercilerince yapılan hukuki değerlendirme**

### ByLock'u Nasıl Kırmışlardır?

(1) "ByLock'u kırmak" yanlış bir tabirdir. ByLock'un kendisi şifreli bir program değildir. Veri elde etmek maksadıyla ya ByLock sunucusu hacklemiş ya da ByLock sunucusu veri tabanı satın alma gibi yöntemlerle elde edilmiş olabilir. Bu konu ile ilgili net bir bilgi bulunmamaktadır.

(2) Basında yer alan bilgilerde ByLock uygulamasında kullanıcıların kullandığı şifrelerin 16-24 karakter olduğu belirtilmesine karşın, MİT raporunda üç karaktere kadar kullanıcı şifrelerini bulunduğu, yaklaşık yarısının 9 karakterden uzun olduğu ifade edilmiştir.

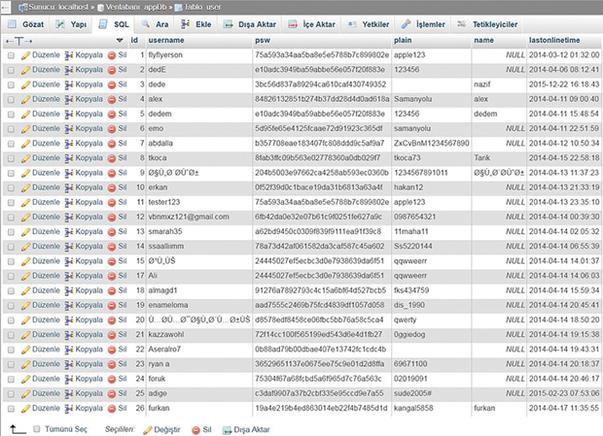
(3) MİT raporunda veritabanı tabloları içerisinde yer alan iletişim verilerinin ByLock uygulaması tarafından 2048 bit anahtar kullanılarak otomatik olarak şifrelendiği belirtilmektedir.

(4) 13/09/2016 tarihinde Hürriyet Gazetesi’nde **“Darbe yolundaki gizli yazışmalar: ByLock”** başlığıyla yayınlanan yazıda ByLock uygulamasına ait olduğu belirtilen ve Şekil-19’te sunulan veri tabanı görüntüsü yer almaktadır. Bu yazıda kullanılan bir görsel MySQL veritabanı yönetim sistemlerini kullanan phpMyAdmin yönetim yazılımına ait aşağıdaki ekran görüntüsüdür *(Haberin doğru olduğu, bu görselin simgesel olmadığı ve kullanıcılar hakkında tutulan veri tiplerinin tamamını gösterdiğini varsaydığımızda devletin ilgili birimlerinin ByLock’un kullanıcı veritabanına sahip oldukları anlaşılmaktadır. Ancak bu görselden edinilemeyen bilgi veritabanında kullanıcılar hakkında başka bilgilerin depolanıp depolanmadığıdır.)*.

(5) Söz konusu veritabanı görüntüsü incelendiğinde;

(a) Veritabanı adı “appDb” ve veritabanı tablosu da “user” olduğu,

(b) Tabloda tutulan veri sütunlarının **id** (kullanıcı kimlik numarası), **username** (kullanıcı adı), **psw** (şifrelenmiş parola), **plain** (şifrelenmemiş parola), **name** (ad) ve **lastonlinetime** (sisteme son bağlanılan tarih) olduğu görülmektedir.



**Şekil-19. İnternet haber sitesinde yayınlanan ByLock veritabanı görüntüsü**

(c) Hazırlanan uygulama bir bütün olarak incelendiğinde yanlızca Şekil-25’de gösterilen sütunlardan oluşmayacağı değerlendirilmektedir. Konu ile ilgili olarak MİT raporu incelendiğinde karartılmış bölümler içerisinde şifreli durumda dosya ekleri, yazışmalar vb. bilgilerin olduğu anlaşılmaktadır.

(ç) MİT raporu ve basına yansıyan bilgiler bir bütün olarak incelendiğinde ByLock uygulamasının birden fazla veri tabanı tablosundan oluştuğu görülmektedir. Tablolar üzerinde bulunan verilerin bir kısmının açık, bir kısmının ise şifreli durumda bulunduğu anlaşılmıştır. Farklı tablolarda yer alan bilgilerin kullanıcı bazlı tutarlılık analizinin titizlikle yapılması tespitlerin kesinliği açısından önem arz etmektedir.

(d) Veri tabanı tablolarında yer alan kriptolu verilerin klasik yöntemlerle çözümlenmesi teknik olarak pek mümkün değildir. Ancak, kriptolu durumda bulunan verilerin çözümü işleminde dünya genelinde yaygın olarak kullanılan ve “Rainbow Table” olarak adlandırılan yöntemin MİT tarafından kullanılmakta olduğu değerlendirilmektedir. Klasik yöntemler kadar uzun sürmese de MİT raporunda yer alan yaklaşık 18 milyon mesajın Rainbow Table kullanarak yapılacak tespitlerinin de uzun bir süre alacağı kaçınılmaz bir sonuçtur. Mesaj çözümlenmesinin de bir önceliklendirme esası doğrultusunda gerçekleştirilmesi gerektiği değerlendirilmektedir.

### ByLock sunucusunda haberleşme içerikleri açık metin olarak sunucuda saklanıyor mudur?

(1) Basında mesajların "karşı taraf okuyunca, ya da 24 saat içinde otomatik olarak silindiği" haberleri bulunmaktadır. İzmir Cumhuriyet Başsavcılığı tarafından hazırlanan iddianamede mesajların 24 saatlik süre içerisinde silinebilecek şekilde ayarlanabildiği bilgisi yer almaktadır.

(2) Görüşme kayıtlarının sunucuda yer alan kopyalarının şifreli olduğu değerlendirilmektedir. Basında yer alan şifrelerin çözümü devam ediyor şeklindeki haberler de bilgilerde bu tezi desteklemektedir.

(3) Mevcut bilgilerden yola çıkılacak olursa, ortada ByLock sunucunda yer alan verilerin elde edilmesiyle ilgili olarak üç ihtimalin bulunduğu görülmektedir. **Bunlardan birincisi ByLock sunucusunu hacklenmesi, ikincisinin sunucu sahibinden verilerin satın alınması, üçüncüsünün ise Türkiye’nin internet çıkışlarından ByLock sunucusuna giden bağlantıların listesinin alınmasıdır.**

(4) İlk iki ihtimalin göz ardı edilmesi durumunda ByLock kullanıcılarının tespiti maksadıyla Türkiye’den ByLock sunucusuna yapılan erişim kayıtlarının tespit edilmesine yönelik çalışmalar yapıldığı kuvvetle muhtemeldir. Bu işlemler geçmişe yönelik olarak güvenlik birimleri tarafından tespit edilebilmektedir. FETÖ yöneticilerinin takip edildiklerini fark edip VPN kullanımına yönelik talimatlar vermesi de bunun bir göstergesi olarak yorumlanabilir. Zira VPN, böyle bir durumda ancak IP adresini gizlemek için kullanılmaktadır *(üçüncü ihtimalin tek başına kullanılması durumundan MİT raporunda yer alan ByLock uygulaması veritabanı tablolarına ulaşmak teknik olarak mümkün değildir).*

(5) **ByLock kullanıcılarının net olarak tespit edilmesi, amacıyla bir ve ikinci yöntemler uygulanarak elde edilen verilerin analizin üçüncü yöntemle elde edilen verilerle karşılaştırılmasının bir zorunluluk olduğu değerlendirilmektedir.**

**----------------------------------------------------------------------------------------------------**

### ByLock'la yapılan haberleşme içerikleri elde edilmiş midir?

(1) Haberleşme içeriğinin iletişim anında yapılacak teknik takiple belirlenmesi ihtimal dahilinde değildir. Aradaki sunucunun, sadece haberleşmek isteyen iki tarafı buluşturmak için bir aracı rolünde kullanıldığı değerlendirilmektedir. İki taraf da hatta ise muhtemelen mesajlar doğrudan birbirlerine gönderiliyor ve sunucuda tutulmuyordur. İki taraftan biri hatta değilse, mesajların 24 saat sunucuda tutulduğu bilgisi bulunmaktadır. Ancak gene de bu mesajlar şifreli (Encrypted) olarak tutulduğu değerlendirilmektedir. Böyle bir şifrelemenin klasik yöntemlerle kırılması teknik olarak pek mümkün değildir.

(2) Kamuoyunda dolaşan diğer bir söylenti daha bulunmaktadır. O da bir ByLock kopyasının (clone) yazıldığı ve bunun Google Play'e konmuş olduğudur. Eğer böyle bir durum varsa, o programı indirip yazışma yapan herkesin tüm yazışma içerikleri güvenlik birimlerinde vardır. Zira program kendi üzerinden geçireceği mesajları açık metin olarak kaydedip, oradan ByLock sunucusuna gönderip aradan çıkıyordur. Fakat böyle bir şey varsa, ne zaman başlamış ve ne kadar sürmüştür; Google Play uygulama mağazasından kaç kişi bu uygulamayı indirmiş bilgisi meçhul olmaktadır. Gerçekleştiyse de, muhtemelen hızla fark etmişlerdir ve önlem almışlardır. Bu durumun pek mümkün olmadığı değerlendirilmektedir *(Bu söylentinin doğru olması uygulamanın Google Play Store uygulama mağazasından rahatlıkla indirilme kullanılma hususunun bir göstergesi olacaktır).*

### İnternet Erişim Sağlayıcılarının IP Atama ve Bağlantı Yönlendirme Yöntemleri

(1) Günümüzde İnternet’in çalışmasında yaygın olarak kullanılan iletişim kuralı IP protokolünün 4. sürümüdür ve kısaca IPv4 olarak anılmaktadır. IPv4 tipindeki IP adresleri “.” ile ayrılan 4 adet 8’li ile tanımlanır. Bu matematiksel gerçek, IPv4 standardında tanımlanabilecek en çok IP adresi sayısının 2 üzeri 32 ile yani 4.294.967.296 (yaklaşık 4,3 milyar) adetle sınırlı bırakmaktadır.  
  
 (2) Bu IP adreslerinin bir bölümü (yaklaşık 589 milyon adet) özel kullanım içindir, “özel İnternet adresleri”, “İntranet adresleri” ve “İnternette yönlendirilemeyen adresler” olarak anılır. Bu tipteki adresler dışarıya kapalı ağlarda istenilen cihaza her bir cihazın adresi farklı olacak şekilde serbestçe atanabilir. Ancak, birbiriyle doğrudan bağlantısı olmayan ağlardaki cihazlarda tanımlanan IP adreslerinin farklı olması gerekliliği yoktur.

(3) IPv4 standardında tanımlanabilecek adreslerden geri kalanı (yaklaşık 3,7 milyar) “açık İnternet adresleri” ve “İnternette yönlendirilebilen adresler” olarak anılır, İnternet kullanımına açıktır. İnternete doğrudan bağlı cihazların IP adreslerinin birbirinden farklı olması şarttır. Günümüzde İnternet erişim sağlayıcılarının abone sayısı zamanla logaritmik oranda artmakta, fakat abonelerine atamaya hakları olan IP adreslerinin sayısı sabit kalmaktadır.

(4) Özellikle mobil operatörler yeterli sayıda İnternet IP’sini abonelerine sağlayamamaktadır (Şekil 20).

|  |
| --- |
| **EK Bilgi:**Günümüzde internet kullanımı hızla artmakta. Bunun sonucu olarak kullandığımız IP adresleri (Internet Protocol) sayıca yetersiz kalmaya başlamıştır. Şu anda yoğun olarak kullanılan IPv4 protokolü 32 bitten oluşur yani 2 üzeri 32= 4,294,967,296 farklı IP adresi tanımlayabilir.  İnternette gideceğimiz yeri bulmak için IP adresleri kullanırız. Ip adres sayısının kısıtlı olması nedeniyle internet servis sağlayıcıları eldeki IP adeslerini genellikle havuz şeklinde kullanıcıların hizmetine sunmaktadır. Yani kimin internet bağlantı ihitiyacı varsa ona otomatik olarak IP adresi tahsisis yapılmaktadır.  Bu IP adresini kullanıcılara ISS'ler (İnternet Servis Sağlayıcıları) veya gene bir tür ISS olan GSM Şirketleri tahsis etmektedir. Bu tahsis de verilen IP adresi kullanıcıların internete bağlı olduğu süre için geçerlidir. Dolayısıyla bu IP Adresi, sabit bir adres değildir ve internete bağlı olunan saatlere göre değişir. Hatta modeminizi kapatıp açarsanız IP Adresinizin değiştiğini görürsünüz. Ne kadar bekledikten sonra adresin bir sonraki gelen kullanıcıya verileceğini ISS'ler tarafından belirlenir. Geçici bağlantı kopmalarına karşı tedbir olsun diye derhal vermeyebilirler, ama sizin internet bağlantınız kesildikten sonra çok kısa bir zaman içerisinde IP Adresiniz boşa çıkar ve bir başkasına tahsis edilir.  Bunun istisnası olarak Statik IP'ler vardır, ama sıradan vatandaşların %99'u Statik IP sahibi değildir. Bu ücretli bir hizmettir ve internet şirketleri veya özel ihtiyacı olanlar haricinde çok kimsenin bir işine yaramaz. Dolayısı ile nadir karşılaşılan bir durumdur.  GSM şirketleri kendilerine tahis edilen IP adresi sayısının azlığı nedeniyle artan kullanıcı sayısının internet bağlantı taleplerini karşılamak için çoğunlukla kullanıcıları **NAT olarak isimlendirilen yöntemi kullanarak tek IP adresi ile bir çok kullanıcıyı aynı anda internete bağlamaktadır**. Örnek olarak bir evde tek bir internet hattı varsa, o evin IP Adresi tektir ve o evden internete bağlanan herkes, internet üzerinde aynı IP Adresi ile gezmektedir. |

**Şekil 20. IP ve NAT sistemi hakkında ek bilgi**

(5) Türkiye'deki IP adreslerinin adedi *(Operatör başına tahsisli IP numarası adedi)* tüm Türkiye için: 15.534.000 dir. Operatör başına dağılımı ise, Türk Telekom 6.930.000, Turkcell 2.228.000, Vodafone 1.655.000, Avea – 811.000, Tellcom 664.000, Superonline 545.000, Türksat (Uydunet) 459.000, Digitürk 410.000 adettir.

(6) Operatörlerin abone sayıları ise yaklaşık Turkcell için 35 milyon, Vodafone için 20 milyon, Avea için ise 15 milyon mertebesindedir. Dolayısıyla, **Avea'da 18.5 kişiye (1) IP, Turkcell'de 15 kişiye (1) IP, Vodafone'da 12 kişiye (1) IP düşmektedir.** Bu hatların yarısı kadar gerçek kullanıcı olsa, internet kullanıcı sayısı bunun yarısı olsa, onların da aynı anda interneti açık olanlar yarısı olduğu varsayılsa da, aynı IP'nin birden fazla kullanıcıya tahsis edilme zorunluluğu açıktır.

### Bir şahsın ByLock kullandığı nasıl tespit edilmiştir?

(1) Kullanımın tespiti ile ilgili olarak ByLock sunucusu üzerinden IP Adresi bilgisinin alındığı değerlendirilmektedir. Her sunucuda olması gerektiği gibi, ByLock sunucusunun kendisine ait özel bir IP Adresi vardır. Bu adrese Türkiye'den yapılan bağlantılar, Türkiye'deki ISS/GSM Şirketleri tarafından tespit edilmiş veya sunucu satın alınarak/hacklenerek, sunucuya bağlanan tüm IP Adreslerinin listesi alınmış olabilir*.*

(2) Her iki durumda da güvenlik birimlerinin elinde muhtemelen şu tarz bir bilgi vardır:

"Bağlantı Tarihi: 12 Ağustos 2014, Saat 14:41”

“Bağlantıyı yapan IP Adresi: 24.133.220.21"

(3) Bu bilgileri aldıktan sonra tespiti yapan güvenlik birimi önce BTK (Bilgi Teknolojileri Kurumu)'ya şu soruyu sorar: "24.133.220.21 adresi, hangi şirkete aittir"? BTK de cevap verir: "24.133.220.21 adresi, AVEA Şirketine ait IP havuzu içindedir" diye. Güvenlik birimi o zaman Avea'ya sorar: "Bu IP adresinden, 14:41'de bağlantı kuran kimdir?" diye. Avea da cevap verir: "12.08.2014 tarihinde saat 14:41'de 24.133.220.21 adresi, Falan Filanoğlu'na tahsis edilmiş durumdadır" diye. İşte savcılıklara gönderilmiş olan "Falan Filanoğlu, ByLock kullanmıştır" bilgisi, %99 ihtimalle bu şekilde elde edilmiş bir bilgidir ve gerçekte şahsi kullanım bilgisi değil, bir internet bağlantısı bilgisidir ***(Kullanıcıların tespit edilmesi işleminde saniyelerin önemli olduğu bir değerlendirmede titiz bir inceleme yapılmamış ise hata yapılmış olma olasılığının oldukça fazla olduğu değerlendirilmektedir)****.* Güvenlik birimleri Falan Filanoğlu'nu elindeki telefonu ByLock'a bağlanırken tespit etmiş ve suçüstü yapmış değildir. Aksi halde iddia edilen 215.000 tane kullanıcıyı *(sonradan 102.000 kişi olarak güncellenen)* böyle tek tek takip etmek ve bağlantılarını fiziksel olarak görüp de tespit etmek teknik olarak imkânsızdır.

(4) IP adreslerinin tespiti konusunda göz ardı edilmemesi gereken diğer bir durum ByLock sunucusunun sistem saatidir. Sistem saatindeki yanlışlık ve saat farklılıkları gibi nedenlerden dolayı yanlış kişilerin kullanıcı olarak tespit edilebilme olasılığı bulunmaktadır.

(5) ByLock uygulamasının kullanımına yönelik olarak yapılan tespit işleminde çoğunlukla IP adresi telefon IMEI adresinin eşleştirilmesi sonucu kullanıcının belirlendiği görülmektedir.

(6) 01 Mart 2017 tarihinde internet üzerinde yayın yapan haber sitelerinde **“MİT, 122 bin kişiyi tespit etti!”** başlığı ile yapılan haberde; “*Milli İstihbarat Teşkilatı ( MİT), FETÖ mensuplarının kullandığı ByLock üzerindeki çalışmalarının büyük kısmını tamamladı. Litvanya’daki ‘server’da bulunan tüm kullanıcılar tespit edildi.* ***Daha önce hazırlanan, illerdeki Terör ve İstihbarat Şube Müdürlükleri’ne gönderilen “ByLock1” ve “ByLock2” listeleri birleştirildi. İki listede güncellemeler yapıldı.*** *MİT, hataya yer vermemek için günlerce titiz çalışmalarda bulundu.* ***Özellikle ortak Wi-Fi kullanımından ortaya çıkan sorunlar ile telefon hattının kimin üzerine alındığı,******ByLock bulunan telefon numarasının kim tarafından kullanıldığı yönündeki çalışmalar detaylı yapıldı.*** *Çalışmalar tamamlandıktan sonra MİT, Türkiye’de ByLock kullandığı tespit edilen 122 bin ismin bulunduğu listeyi Ankara Cumhuriyet Başsavcılığı’na teslim etti.*” ByLock uygulaması ile ilgili yapılan inceleme işlemlerine değinilmiştir. **Haber incelendiğinde yanlış yapılan tespitler üzerinde düzeltmeler yapıldığı, hataya yer vermemek için titiz bir inceleme yapıldığı konuları açıklanmıştır**. Bu haber tespitlerde hatalar bulunduğunun göstergesi olabilir. **Yayınlanan bu haberden ByLock kullandığı bilgisi** **kamu kurumlarına gönderilen ve hakkında işlem yapılarak tutuklanan, açığa alınan ve işten atılan devlet memurları içerisinde hali hazırda masum kişilerin olduğu sonucu çıkarılabilmektedir.** *(Konuyla ilgili olarak 20 Şubat 2017 tarihinde OdaTV internet sitesinde “****Birileri ByLock’u sıfırlıyor”*** *haberi örnek olarak gösterilebilir)*

### Kesinlikle ByLock kullanmamış birisi, kullanmış gibi gözükebilir mi?

(1) Evet bu mümkündür. Eldeki bilgi, "Falan şahıs internet/cep telefonu hattı üzerinden ByLock sunucusuna bağlandı" bilgisidir. İşte bu bağlantıyı resmi hat sahibinin yapıp yapmadığı meselesinin ayrıca tespit edilmesi gerekmektedir.

(2) ByLock kullanımı ile ilgili olarak yapılan tespitlere ilişkin olasılıklar aşağıda açıklanmıştır.

**(a) Eğer kullanım yerel internet hattı üzerinden tespit edilmiş ise:**

- Eğer Kablosuz İnterneti şifresiz kullanıyorsanız, civarda bulunan üçüncü bir şahıs, sizin internetinize bağlanarak, sizin hattınız üzerinden ByLock sunucusuna bağlanırsa, karşı tarafta modemin IP adresi gözükeceği için hattın resmi sahibi zan altında kalmaktadır.

- Kablosuz internetin şifreli olması durumunda, eski şifreleme teknolojileri olan ve artık çok zayıf kaldıkları için terk edilen WEP veya WPA tipi şifreleme kullanan kablosuz ağların şifrelerini basit hazır programlar yardımıyla kolayca kırarak, bu hatların üzerinden ByLock kullanan birileri, hat sahibini zan altında bırakabilir *(Arama motorlarında "Wireless Password Cracker" yazarsanız, karşınıza bu konu ile alakalı çok sayıda sayfa bulabilirsiniz).*

- Evin herhangi bir ferdinin yaptığı bir haberleşme, hattın resmi sahibini zan altında bırakabilir.

- Apartmanda ortaklaşa kullanılan kablosuz internet ağlarında, herhangi bir kullanıcının yaptığı haberleşme nedeniyle resmi hat sahibi zan altında kalabilir.

- Eve gelen misafirlerin şifresini isteyip ev internetini kullanarak haberleşme yapması ve ByLock kullanması sonucunda resmi hat sahibi zan altında kalabilir.

- Kötü niyetli üçüncü şahısların, "spoofing” denilen bir yöntemle kendi IP Adresini başkasının internet adresi gibi göstererek ByLock sunucusuna bağlanmaları sonucunda, IP Adresinin o an resmi olarak tahsis edildiği kişi zan altında kalabilir.

- Üçüncü şahısların "saplama” denilen yöntemle, başkasının internet hattının geçtiği kabloya fiziki müdahale ile ayrı bir hat çekip, hat sahibinin interneti üzerinden ByLock’a bağlanmaları durumunda, resmi hat sahibi zan altında kalabilir.

**(b) Eğer kullanım GSM numarası üzerinden tespit edilmiş ise;** *(Burada kastedilen, cep telefonunda kullanılan internet üzerinden yapılan bir bağlantı bilgisidir.)*

- Dershane, hastane, sigorta şirketleri vb. kimlik fotokopisi bırakılan yerlerde, örgüt üyelerinin bırakılan kimlik fotokopisi ile GSM hattı alarak, o hat üzerinden haberleşip hat sahibini zanlı durumuna düşürmeleri mümkündür.

- Kendi cep telefonunun interneti olmayan veya kotası biten bazı örgüt üyelerinin, arkadaşlarına veya ortamdaki diğer şahıslara rica ederek, onların cep telefonlarını wireless-hot-spot yapılmasını sağlayarak internet üzerinden ByLock kullanmaları mümkündür.

- Benzer şekilde, açık kalmış wireless-hot-spotların şifrelerini hazır programlar yardımıyla kırarak, hiç tanımadıkları insanların cep telefonlarının interneti üzerinden ByLock kullanarak hat sahiplerini zan altında bırakmaları mümkündür.

- “Trojan (Truva Atı)” / “Backdoor (Arka kapı)” gibi yöntemlerle birisinin cep telefonunu uzaktan hack’leyerek gizlice ByLock yükleyip, o telefon üzerinden telefon üzerinde gözükmeyecek şekilde arka planda (background process olarak) haberleşme yapmaları ve telefon sahibini zan altında bırakmaları mümkündür.

- Benzer şekilde “IMSI-catcher” denilen bir cihazla, (sahte) gezici baz istasyonu kullanarak, şahsın cep telefonu ile GSM şirketinin baz istasyonunun arasına girip (Man in the Middle), sonra da ByLock’a bağlanıp, asıl hat sahibini zan altında bırakmak teknik olarak mümkündür.

- **Mobil cihazların yoğun saatlerde GSM şirketinin elindeki IP adresleri tükenmişse, aynı IP Adresini birden fazla kişiye tahsis ederek, kendi içi ağı üzerinde NAT yoluyla trafik yönlendirmesi yaptığı bilinmektedir. Bu şekilde sağlanan internet kullanıcı bilgilerinin kayıt altına alınması kanuni bir zorunluluk olsa da, aynı IP adresi tahsis edilen şahıslara ait kayıtlar operatörlerce birbirine karıştırılmış olabilir.**

**(c) Tüm ISS'ler/GSM Operatörleri için geçerli olmak üzere:**

- Güvenlik birimleri tespit ettikleri bağlantı bilgilerini gönderilirken rakam hatası yapılmış olabilir *(24.233.220.21 yazarken bir klavye hatasıyla 24.233.220.12 olarak yazılmış olabilir. Ya da tarih ve saat yazarken 12.08 yerine 12.07 yazılır).* Bu durumda, BTK’dan hiç alakası olmayan birisinin bilgisi istenmiş olur.

- BTK veya GSM Operatörü, kendisinden istenen sorgunun cevabı hazırlanırken kullanıcı personel hata yapmış olabilir *(Aynı dakika içerisinde bir kullanıcı internetini kapatıp diğer kullanıcının internetini açması gibi oluşabilecek kullanıcı değişikliği nedeniyle farklı bir kişilerin ismine ulaşılabilir).*

- Bu bağlantı bilgisinin istendiği saatlerin saat dilimleri ile ilgili karışıklık olabilir. *(Örneğin ByLock sunucusu GMT+8 üzerinden çalışıyor olsun. Türkiye GMT+3 saat dilimindedir. Böyle bir durumda ByLock sunucusunda saat 15:00 olarak gözüken vakit, Türkiye için 10:00 olabilir. Güvenlik birimleri Türkiye’de hizmet sağlayan operatörlerden bağlantının yapıldığı IP adresinin saat 15:00’de kime tahsis edildiği bilgisini ister. Oysa 5 saat içinde önceki kullanıcı mobil veriyi kapatmıştır ve o IP artık başkasına tahsis edilmiştir).*

- Yaz saati uygulaması ile ilgili olarak bir karışıklık olabilir. Bağlantı tespit edildiği dönemde Türkiye yaz saatindedir. Bilgisayarda 20:00 gibi gözüken bağlantı bilgisi, gerçekte 19:00’dır. O bir saat içinde IP adresi serbest kalmış ve başkasına tahsis edilmişse, yanlış kişi tespit edilebilir.

- Ay/Gün tarih bilgisinin yazımı ile ilgili karışıklıklar olabilir. Örneğin; Avrupa’da “12.08” yazdığınız zaman, “8 Aralık” demektir. Türkiye’de ise “12 Ağustos”. Türkiye içinde de bölge ayarları (regional settings) yapılmamış veya Avrupa/Amerika olarak kaydedilmiş bilgisayarlarda da aynı karışıklık yaşanabilir. **Excel gibi bir veri tabanı üzerinden formül yolu ile otomatik karşılaştırma yapılıyorsa, bu tarz tutarsızlıklar ve hatalar da çok rahat gözden kaçabilir.**

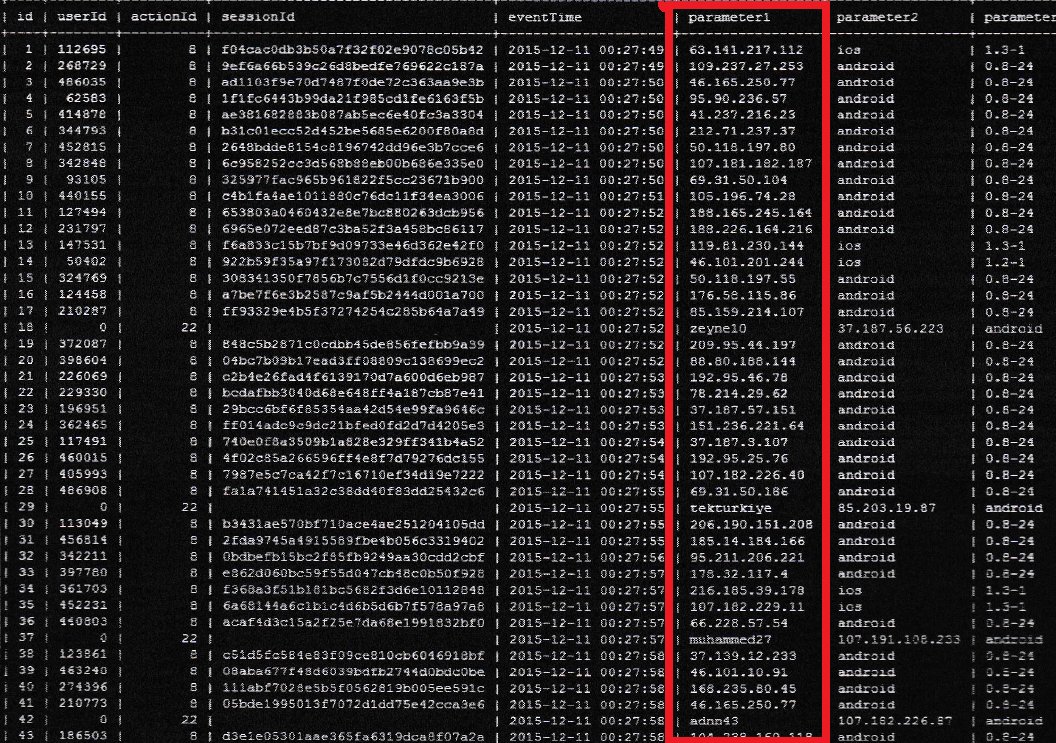
- Kötü niyetli güvenlik görevlisi, BTK veya GSM Operatörü görevlisi, kasten rakamları karıştırıp farklı isimler gönderebilir.

**(ç) Bağlantı Proxy (VPN) üzerinden yapılmışsa:**

- MİT tarafından hazırlanan "ByLock Teknik Analiz Raporu"nun 25 ve 26. sayfasında, ByLock Server yöneticisinin 17 Kasım 2014 tarihinde (15 Kasım 2016'da yaptığı) ortadoğu'dan ByLock'un Litvanya'daki serverine erişim sağlayan IP Bloklarının banlandığı, bu IP Bloklarının büyük çoğunluğunun Türkiye'den Bylock Serveri'ne erişim sağlayan IP Blokları olduğu belirtilmektedir. Bu yöntem sayesinde de örgütün ByLock sunucusuna bağlantıda VPN kullanmaya başladığı iddiası MİT tarafından öne sürülmektedir. Bu durum şöyle açıklanabilir; Doğrudan ByLock sunucusuna bağlanmak yerine, önce arada bir başka bilgisayara (Proxy-VPN) bağlanılmakta, ByLock sunucusuna o adres üzerinden bağlanılmaktadır.

- Böyle bir durumda ByLock sunucusunda IP adresi olarak hizmet alınan VPN’in adresi gözükecektir. Bu durumda Güvenlik birimleri bağlantı yapıldığı belirlenen VPN’lerden erişebildiğinin ilk IP adres bilgilerini almıştır*.* VPN firmasının vereceği yanlış bilgi ile yanlış kişiler kullanıcı olarak belirlenebilir. Bununla birlikte şuana kadar gerek adli süreçte görülen davalar olsun gerekse de MİT tarafından kamuoyuna yansıyan hiç bir açıklama veya haber bulunmamaktadır. Dolayısıyla şuana kadar MİT ya da adli kolluk görevlileri, ByLock kullanıcısı olduğu iddiasıyla her hangi bir şüpheliye ait olan bir VPN IP adresini ilgili hizmeti sağlayan her hangi bir VPN şirketinden talep etmemiştir.

- İnternet üzerinde yapılan araştırma sonucunda, MİT tarafından hazırlanan raporda yer aldığı belirlenen VPN IP adreslerini içeren tablo Şekil -21’de sunulmuştur. Söz konusu IP adreslerinin ByLock uygulamasına bağlantı yapan VPN servislerine ait olduğu açık kaynaktan öğrenilebilmektedir.



**Şekil -21 MİT raporu VPN IP'lerini içeren ilgili resim**

- 15 Kasım 2014 sonrası Türkiye’den bağlanan kişilerin VPN kullanma zorunluluğuna yukarıda değinilmişti. VPN üzerinden yapılan bağlantılarda tespit edilen IP adresleri VPN şirketlerine ait olduğundan gerçek kullanıcıların tespitinin ancak VPN şirketlerinin kendi log kayıtlarını vermesiyle mümkün olduğu değerlendirilmektedir.

- Bu konunun farklı bir boyutu da şudur ki: MİT raporunda belirtildiği kadarıyla alınan tüm veri bankası kapasitesi (109) GB büyüklüğündedir. Bu boyutun kullanıcı sayısı, mesaj sayısı vb. bilgilerle karşılaştırıldığında oldukça düşük olduğu değerlendirilmektedir. Ayrıca MİT raporunda yer alan bilgiler genellikle 2015 yılının son aylarına aittir. Sunuculardan kiralama işlemlerinde bir kapasite üzerinden anlaşma yapılır ve genellikle bu kapasitenin % 10 oranında artmasına izin verilir. **Dolayısıyla, ByLock uygulaması için Baltic Servers firmasından kiralanan depolama kapasitesinin 100 GB mertebesinde olduğu anlaşılabilir. Bu kapasite aşıldığı taktirde sunucunun otomatik olarak eski verilerin üzerine yazacağı değerlendirilmektedir.**

- Açık kaynak bilgilerden anlaşıldığı kadarıyla ByLock gerekçesiyle haklarında idari veya adli işlem yapılan kişilerin tamamına yakını için 2014 yılı bağlantı tarihleri gerekçe gösterilmiştir. 15 Kasım 2014 tarihi sonrası VPN zorunluluğu, 15 Kasım 2014 öncesi sunucudan bağlantı LOG larının silinmiş olması hususları birlikte değerlendirildiğinde, 2014 yılı tespitlerinin sadece yerli operatör verileri üzerinden belirlenme ihtimali ortaya çıkmaktadır. 15 Kasım 2014 sonrasına ait tespitlerin ise **“user id”** üzerinden olma ihtimali yüksektir.

- Yukarıda belirtilen ihtimalin doğru olması halinde, örgütün perdeleme amacıyla uygulamanın yaygınlaştırılması aşamasında yapılan IP bağlantı tespitleri hem çok sayıda mağduriyetin oluşmasına neden olabilecek hem de yürütülen tüm davaların çökmesine neden olabilecek seviyeye ulaşabilecektir.

**(d) Eğer kullanım bilgisi, kullanıcı adı veya mail adresi üzerinden tespit edilmişse:**

- İnternet üzerinde yayınlanan bir haberde, ByLock sunucusuna bağlanan şahısların isim ve şifrelerinin açık olarak göründüğü bir veritabanı fotoğrafı mevcut bulunmaktadır. Eğer ByLock yazılımını örgüt üyeleri yapmış ise, isim ve şifreleri açık metin (clear text) tutuyor olması mantıklı değildir.

- Örgüt üyelerinin maske isim kullanmaları veya kasten başkalarının isim ve soyadları ile mail adresleri, kullanıcı adları almaları, facebook/twitter adresleri almaları, hatta kullanıcının fotoğrafları ile de süslemeleri çok kolaydır ve yaygındır. ByLock kullanım bilgisi, ByLock sunucularına bağlanmakta kullanılan kullanıcı adı veya mail adresleri üzerinden tespit edilmişse, bağlantının yapıldığı hat bilgileri ile kıyaslayarak durumu ayrıca teyid etmek gerekmektedir.

- Bunların da ötesinde bir ihtimal daha var ki, "ifrime" metoduyla yapılan tuzaklama sonucu her hangi bir web sayfasına yerleştirilen ve reklam içeriği taşıyan bir gizli linke tıklanması sonucu kullanıcıyı farkında olmadan **ByLock Sunucusuna ait "46.166.160.137" IP numarasına yönlendirmiş olması.** Bu durum, farkında olmadan kullanıcıyı ByLock Serveri'ne yönlendirirken, sadece sinyal bilgisi vermiş olur ve kullanıcı ByLock Sunucusuna erişim sağlamış şekilde gözükür.

- Ayrıca başkasıymış gibi gözükerek işlem yapmanın, maskeleme ve perdelemenin yukarıda sayılanlar haricinde daha gelişmiş yöntemleri de vardır. Fakat bunlar maliyetli olduğu ve ancak üst düzey vakalarda söz konusu olabilecek durumlardır *(Yukarıda açıklanan maddeler herkes için karşılaşılabilecek, yaygın durumlardır. Bunlardan bazıları daha nadir rastlanabilecek ve/veya kumpas durumlarında olabilecek şeylerdir. Fakat gene de ihtimal dahilindedir.).*

- Tespit edilen bilgiler dikkatsiz bir şekilde incelemeye tabi tutulması durumunda, ByLock kullanımı ile ilgisi bulunmayan kişiler mağdur edilebilir.

(e) Açık kaynak bilgilerden anlaşıldığı kadarıyla **ByLock gerekçesiyle haklarında idari veya adli işlem yapılan kişilerin tamamına yakını için 2014 yılı bağlantı tarihleri gerekçe gösterilmiştir.** 15 Kasım 2014 tarihi sonrası VPN zorunluluğu, 15 Kasım 2014 öncesi sunucudan bağlantı LOG larının silinmiş olması hususları birlikte değerlendirildiğinde, 2014 yılı tespitlerinin sadece yerli operatör verileri üzerinden belirlenme ihtimali ortaya çıkmaktadır. 15 Kasım 2014 sonrasına ait tespitlerin ise **“user id”** üzerinden olma ihtimali yüksektir.

(f) Yukarıda belirtilen ihtimalin doğru olması halinde, örgütün perdeleme amacıyla uygulamanın yaygınlaştırılması aşamasında yapılan IP bağlantı tespitleri hem çok sayıda mağduriyetin oluşmasına neden olabilecek hem de yürütülen tüm davaların çökmesine neden olabilecek seviyeye ulaşabilecektir.

Program kullanımına yönelik ilk IP çakışmasının tespit edildiği tarih baz alınarak ByLock kullanımının tarihlere göre üç ayrı aşamada incelenmesi gerektiği değerlendirilmektedir. Bu aşamalar;

(1) iOS işletim sistemli (iPhone) telefonlar için 07 Eylül 2014, Android işletim sistemli telefonlar için ise 24 Aralık 2014 sonrasında ilk yüklemeyi yapan ve kullanan kişiler bu uygulamayı mağazalardan indirme, indirse de VPN olmadan kullanma imkanı olmadığından özel bir uğraşla indirmiş ve kullanmıştır; kanaatimizce birinci öncelikle incelenmelidir. Android telefonlarda Aralık 2014 sonu öncesinde Türkçe versiyon yüklenme ihtimali zaten bulunmamaktadır.

(2) 15 Kasım 2014 tarihinde lisans sahibi uygulamayı kaldıracağını bildirmiş fakat kaldırılacak uygulama için VPN kullanımı önermiştir. 15 Kasım 2014 tarihi itibariyle de Türkiye kaynaklı IP adreslerini engellemiş ve önceki erişim kayıtlarını silmiştir. 15 Kasım 2014 ile Aralık 2014 sonuna kadar ilk yüklemeyi yapanlar, uygulama mağazalarını kullanabilmelerine karşın, söz konusu açıklama ve VPN kullanımı nedeniyle ikinci öncelikle incelenmelidir.

(3) iOS işletim sistemli telefonlar için 07 Eylül 2014, Android işletim sistemli telefonlar için 15 Kasım 2014 öncesi herhangi bir kişi uygulama mağazalarından indirmiş ve kullanmış olabileceğinden, bu tarih öncesi ise gerekmesi halinde son aşamada incelenmelidir.

**İnternet servis sağlayıcı ve GSM operatörlerince yapılan tespitlerin netleştirilmesi için adli bilişim uzmanlığına başvurulması gerektiği görüşüne katılıyoruz ve bu uzmanlığa sahip kişilerin sorumluluk bilinciyle katkı sağlamalarının gerekli olduğunu düşünüyoruz.**

# DEĞERLENDİRMELER

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. Ancak önemli ölçüde kavram kargaşası bulunduğu ve detayları amaç bölümünde verilen yazışmalardan anlaşıldığı kadarıyla tespit aşamasında rol alan kurumların sorumluluk üslenmekten çekindiği değerlendirilmektedir.

Ortada tespit aşamasında aktif olan kurumlar tarafından sorumluluğu doğrudan kabul edilmeyen ancak idari ve adli işlemlerde kullanılan bir bulgu söz konusudur. Her koşulda nihai hukuki ve vicdani sorumluluk şüphelilerle ilgili adli işlemleri gerçekleştiren hâkim ve savcılarımızda olacaktır. Hâkim ve savcılarımızın iddiaları hukuk çerçevesinde değerlendirerek ve somut deliller doğrultusunda karar oluşturmaları azami önem arz etmektedir.

Delillendirme ve delillerin değerlendirilmesi aşamalarının sağlıklı olması için internet servis sağlayıcı ve GSM operatörlerince yapılan tespitlerin netleştirilmesi için adli bilişim uzmanlığına başvurulması gerektiği görüşü sabitken, ByLock sinyali üzerinden insanların tüm hayatını etkileyecek hatta ileride çocuklarının yaşamını etkileyecek olan bir karar verilmesi ne kadar doğrudur?. Üstelik verilen bu karar Silahlı Terör Örgütüne Üye Olmakla birlikte Vatan Hainliği kapsamındadır ve psikolojik ve vicdan dairesinde yıkımı diğer adli suçlardan çok daha fazladır.

Yürütülen mücadelenin ve açılan davaların ulusal ve uluslararası meşruiyetinin zarar görmemesi için yürütülen işlemlerin her aşamasında hukuk kurallarına bağlılık azami önem arz etmektedir. Yukarıda açıklandığı şekilde, incelenmesi gereken veri miktarı çok büyüktür. İncelenmesi gereken cihaz sayısı da değerlendirildiğinde bir önceliklendirme yapılması zorunluluğu ortaya çıkmaktadır. Dolayısıyla, söz konusu hukuki değerlendirmelerle birlikte, önceliklendirmeye yönelik öneriler şu şekilde sıralanabilir.

### Tespitlerin Delil Niteliği Üzerine Değerlendirmeler

Öncelikle belirtilmesi ve vurgulanması gereken bir hususlar olarak, rapor kapsamında değinildiği gibi ByLock mobil iletişim uygulamasının FETÖ üyelerince kullanıldığının tespit edilmesi ve uygulamaya ait veritabanının elde edilmesi ödüllendirilmesi gereken önemli bir istihbari başarıdır. Bu istihbari başarının hukuki süreç içerisinde ve her koşulda hukuka uygun devam ettirilmesi yürütülen mücadelenin meşruiyetinin sağlanması ve mağduriyetlerin önüne geçilmesi için zaruridir.

Bilişim alanında en önemli hususlardan biri elde edilen verilerin anlamlı ve diğer benzer verilerle tutarlı olması hususudur. Anlamlı ve tutarlı veriler bilgi olarak adlandırılabilir ve delil niteliği tartışılabilir hale gelir; anlamlı ve tutarlı olmayan verilerin delil niteliğinden bahsedilmesi mümkün değildir. Her sayısal kütük aynı zamanda bir veritabanıdır ve bu veritabanına belirli şartlarla ve kurallarla erişildiği varsayıldığında anlamlı bilgi içerdiğinden bahsedilebilir.

Örneğin, bilgisayar ortamında (sayısal ortamda) muhasebe yazılımı kullanarak kayıt tutan bir muhasebecinin veritabanının temin edildiğini düşünelim. Muhasebe yazılımı veritabanına göre de çok sayıda kişinin borçlu olduğunu varsayalım. Yalnızca bu veritabanındaki içerik kullanılarak borçlu görünenlerden borçlarını ödemeleri istemek ne kadar doğru olabilir? Muhasebecinin elindeki veriler, senet vb. belgelere dayandırılabilirse veya borçlu ve alacaklı verileriyle/kayıtlarıyla da tutarlı olduğu gösterilirse, anlamlı borç bilgisinden bahsedilebilir.

Örneği genişleterek devam edecek olursak; muhasebe kayıtlarının sadece müşteri hesap numaralarından oluştuğunu düşünelim. Müşteri hesap numaralarının karşılığında hangi tarihlerde müşterilere banka üzerinden para transferi yapıldığı ve borçlandırıldığı belirtilmiş olsun. Sonrasında müşteri numaralarının kime ait olduğunu bankalara soralım ve bankaların verdiği müşteri isimlerini kullanarak tespit edilen kişilerden borçlarını ödemelerini talep edelim. Muhasebe verilerinin banka verileriyle kontrol edilmesi bizi bilgiye bir adım daha yaklaştırmakla birlikte, kişilerin doğru tespit edilmesi muhasebe kayıtlarının ve banka kayıtlarının bir arada doğru olmasına bağlıdır. Bankalar şayet aynı hesap numarasını birden fazla kişiye vermiş ise, kayıtları sağlıklı değilse elde edilen veri bir anlam ifade etmeyecektir.

Yalnızca, muhasebe veritabanı ve banka veritabanındaki müşteri hesap numaralarının tutarlı olması borçlanma işleminin doğru olduğunu da göstermez. Banka veritabanındaki transfer edilen para miktarı, transfer zamanı, transferi yapan kişi vb. bilgilerin de tutarlı olması gereklidir. Bu verilerden herhangi birindeki tutarsızlık bilgiye ulaşmamızı engelleyecektir.

Diyelim ki, muhasebe kayıtları ve banka kayıtları tamamen tutarlı; ancak borçlu olduğu iddia edilen kişi hayatında hiç o banka şubesine uğramamış ise, hesap kendi adına başkası tarafından açılmış ise ve bu durumun tespiti de mümkün ise bu kontrolün yapılması da zorunluluktur. Örnekler çoğaltılabilir. Özetle, ilgili tüm veriler tutarlı ve anlamlı ise bilgiden bahsetmek ve bilgi doğrultusunda işlem tesis etmek gereklidir ve hukuka uygun olandır.

Veritabanında birden fazla kayıt yöntemi varsa, yani muhasebe örneğinden devamla alacaklı kaydı, borçlu kaydı, banka hareketleri kaydı vb. farklı kayıtlar kendi içinde tutarlılık analizine tabi tutulmalıdır. Sonrasında iç tutarlılığı olduğu tespit edilen veriler dış verilerle birlikte tutarlılık analizine tabi tutulmalı ve birlikte yorumlanmalıdır.

Sayısal ortamlardaki veritabanlarında da sadece numaralar anlamlı bilgi içermemektedir. Bir işlemin kim tarafından yapıldığının belirli olmaması durumu da anlamsal bütünlüğün bozulmasına neden olacaktır. Bir kaydın kim tarafından girildiği bilgisi olmazsa, bu kayıt ve tüm bağlantılı/ilgili kayıtlar anlamsal bütünlük olmadığından geçersiz olacaktır ve sistemin bütününde kararsızlık oluşacaktır. Sistem üzerinde açıkların bulunması ve bu açıklardan faydalanarak güvenliğin aşılması veya zaten kullanıcı girişi yapılmış olan sisteme veri kaydedilmesi durumunda tutarsızlıklar oluşacaktır.

Dolayısıyla, verinin anlamlı bilgi olarak kabul edilebilmesi için aynı ortamda bulunan diğer benzer verilerle tutarlı olması, kararlı çalışan, güvenliği sağlanmış olan bir sistemde depolanması, bu sisteme belirli kurallar ve şartlarla erişimin sağlanıyor olması gereklidir. Sayısal ortamdaki verinin anlam kazanabilmesi için 5N1K olarak adlandırılan “Ne?, Nerede?, Ne Zaman?, Nasıl?, Neden?, Kim” sorularına; başka bir deyişle, “hangi veri, ne zaman, hangi sistemde ve veri depolama ortamında, ne şekilde ve tipte, hangi veri/verilerle ilişkili ve kim tarafından oluşturulmuştur?” sorularına cevap vererek açıklanabiliyor olmalıdır.

**Sayısal ortamda depolanan verilerin, 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 ve 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.**

Yukarıda sayılan kontroller ve iç tutarlılık analizlerinden sonra da dış verilerle tutarlılık analizi yapılmalıdır. Sayılan şartlar altında verilerin bilgi içerdiğinden bahsedilebilir ve belge niteliği taşıdığı söylenebilir.

**Yukarıda açıklanan tüm teknik hususlar ve örnekler ve ileride belirtilecek mevzuat ve değerlendirmeler esasında sayısal delilin illiyet bağının önemini ortaya koymaktadır. Sayısal verilerin delil olarak kullanılabilmesi illiyet bağının tam olarak kurulabilmesiyle mümkündür. Yukarıda sayılan ve ilerleyen bölümlerde değinilecek illiyet bağını kesebilecek hususlara azami özen gösterilmelidir.**

ByLock uygulamasına yönelik tespitlerin kullanıcıların cihazlarında yapılmadığı anlaşılmaktadır. Litvanya’da yer alan sunucudan elde edildiği anlaşılan veritabanı üzerinde Linux tabanlı çok sayıda kayıt (User ID, Group ID, IP, Sent Time, Received Time, Attachment vb.) tutulduğu anlaşılmaktadır. **Öncelikle, bu farklı kayıtların kendi içinde tutarlılık ve anlamlılık açısından yukarıda bahsedildiği şekilde analiz edilmesinin gerekli olduğu değerlendirilmektedir. Ancak iç tutarlılık analizinden sonra netleştirilen veriler dış verilerle birlikte değerlendirilmelidir.**

**ByLock veritabanının bir yöntemle elde edilmesinde de zaman damgasının gerekli olduğu değerlendirilmektedir. Tespit öncesi verilerin sunucuda var olduğunun ve veritabanının kopyalanması sonrası bir ilave olmadığının başka türlü ispatı mümkün değildir.**

Çeşitli somut kanıtlarla kabul gören temel bir olgunun ByLock uygulamasının kötü amaçlı kişilerce kendi haberleşme amaçları için geliştirildiği, ancak bunun aynı zamanda herkese açık bir hizmet olarak da sunularak örgüt üyelerinin perdelenmeye çalışıldığıdır. **Sayısal ortamda depolanan verilerin, 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 prensibiyle birlikte değerlendirildiğinde;** söz konusu kötü amaçlı kişilerce veritabanında **herhangi bir kimse adına kayıt açılması olasıdır. Geçmişte sözde dijital delillerle çok sayıda kişi ve aileyi mağdur etmiş bir örgütün bunu yapmayacağını düşünmenin ve veritabanını tamamen muteber kabul etmenin çok sayıda mağduriyete neden olabileceği değerlendirilmektedir.**

ByLock veritabanında iç tutarlılık analizi yapıldıktan ve tutarlı görülen IP adresleri belirlendikten sonra operatörlerden tarih-zaman aralığı ile istenen IP tahsis bilgilerinin, dolayısıyla gerçek kişi bilgilerinin doğru ve tutarlı olması da bir sonraki aşamadır. Rapor kapsamında açıklandığı şekliyle, operatörlerden alınan IP bağlantılı gerçek kişi bilgileri yeterince sağlıklı değildir. Özellikle, operatörlerin birden fazla kişiye aynı anda tahsis ettikleri ortak IP adreslerinin ayrıştırılmasına yönelik sağlıklı sistemleri olmadığı anlaşılmaktadır.   
  
Tüm bunlarla birlikte, ByLock uygulaması, uzunca bir süre Google Play Store ve nispeten kısa bir süre Apple AppStore uygulama mağazalarında yer almıştır. Uygulama mağazalarında bulunduğu için, herkes tarafından kurulmuş ve özellikle herhangi bir gerekçeyle iletişimlerini açıktan kurmak isteyen kişilerce kullanılmış olabilir. ByLock kurulum dosyaları halen yüzlerce internet sitesinde bulunmaktadır ve bugün dahi kolayca indirilip kurulması mümkündür; ancak sunucusu faal olmadığı için iletişim amaçlı kullanılması mümkün olmayacaktır.

IP üzerinden tespitlerde önemli problemlerin olduğu birçok siyasi tarafından da basın yayın organlarına ifade edilmiştir.

Ülkemizde, geçtiğimiz yıllarda kamuoyunda Ergenekon davası olarak bilinen yargılamada kararını açıklayan Yargıtay 16. Ceza Dairesi, dijital delillerle alakalı şu ifadeleri kullanmıştır:

“… *tamamı ‘dijital delil’ olarak adlandırılan,* ***suistimale müsait olan verilerin****,* “***Dijital delillere harici müdahalenin teknik olarak mümkün olması****, çoğu zaman kim tarafından hangi tarihte müdahale yapıldığının da belirlenememesi karşısında..."*

**Tespit edilen veri** g**üvenilir bilgi olarak değerlendirilse dahi, istihbari faaliyet kapsamında olduğu ve haricen delillendirilmedikçe idari ve adli süreçlerde kullanılamayacağı Emniyet Genel Müdürlüğü (doğrudan) ve MİT (dolaylı) tarafından ifade edilmiş,** adli ve idari işlemlerde kullanılması sorumluluğu her iki kurum ve operatörlerce doğrudan veya dolaylı kabul edilmemiştir. Nihai sorumluluk adli mercilere bırakılmıştır. Bu noktada rapor kapsamında Şekil 24 olarak Ek Bilginin hatırlatılması uygun olacaktır.   
  
 Öte yandan bir diğer önemli husus ise, Emniyet İstihbarat Başkanlığı tarafından 14/10/2016 tarihinde İçişleri Bakanlığı'na gönderilen "Bilgi Notu" ve bu bilgilendirme kapsamında yer alan bilgilerdir. Söz konusu "Bilgi Notu"na göre, "MİT tarafından ilk olarak 11 Ağustos 2016 tarihinde gelen listede Ad-Soyad, GSM numarası, Adsl abonelik bilgisi ve ID bilgilerine yer verilmektedir. 03 Eylül 2016 tarihinde gelen ikinci listede ise 18.074 kişinin kimlik bilgisine yer verilmiş, ID bilgilerine yer verilmeyen listede, tespitlerin IP üzerinden iz sürülerek yapıldığı anlaşılmıştır. İkinci liste ile ilgili olarak MİT ile yapılan görüşmelerde sunucuya bağlanan AVEA kullanıcılarının IP adreslerinde hatalar ile karşılaşıldığı, bu hataların AVEA'nın aynı baz istasyonu üzerinden internete bağlanan birden fazla aboneye aynı IP adresi ile hizmet vermesinden kaynaklandığı belirtilmiştir. AVEA'dan kaynaklanan bu hatadan dolayı ByLock isimli uygulamayı hiç kullanmamış kişilerin dahi kimlik bilgilerinin sunucudaki IP verileri ile eşleştiği, bu nedenle IP bağlantı sayısı düşük olanlarda (20 ve altı) yanlışlık olabileceği değerlendirilmektedir." denilmiştir.

ByLock sunucusuna erişim sağladığını iddia eden CGNAT sayısal değerleri hatalar içermektedir. BTK'dan gönderilen CGNAT dökümüne göre ByLock Sunucusuna ilk erişim sağladığı bağlantı kayıtları sayısal değerlerde aynı zaman diliminde birden fazla adet erişim gözükmesi maddi bir hata ve verilerin üst üste bindiği anlamına gelmektedir. Çünkü, bir şahıs aynı zaman diliminde aynı anda 2 farklı PORT'a erişim sağlayamaz.  
Aslında ByLock sunucusuna bağlanmış olsa dahi ki bu sayısal hatalar Bylock kullandığı iddia edilen kişilerin bağlantı yapmadığını, aksine operatörden kaynaklanan bir hatanın kurbanı olduğunu çok açık bir şekilde ifade etmektedir.   
  
Yukarıda yer alan tüm bu bilgi ve belgeler kapsamında bir kişinin ByLock kullanıcısı olduğuna yönelik iddianın somut ve maddi bir delile dönüşebilmesi için;  
  
 (1) **Kabul edilebilir olmalıdır**. Elde edilen delil dava sırasında hakim veya başka insanlar tarafından kabul edilebilir olmalıdır.

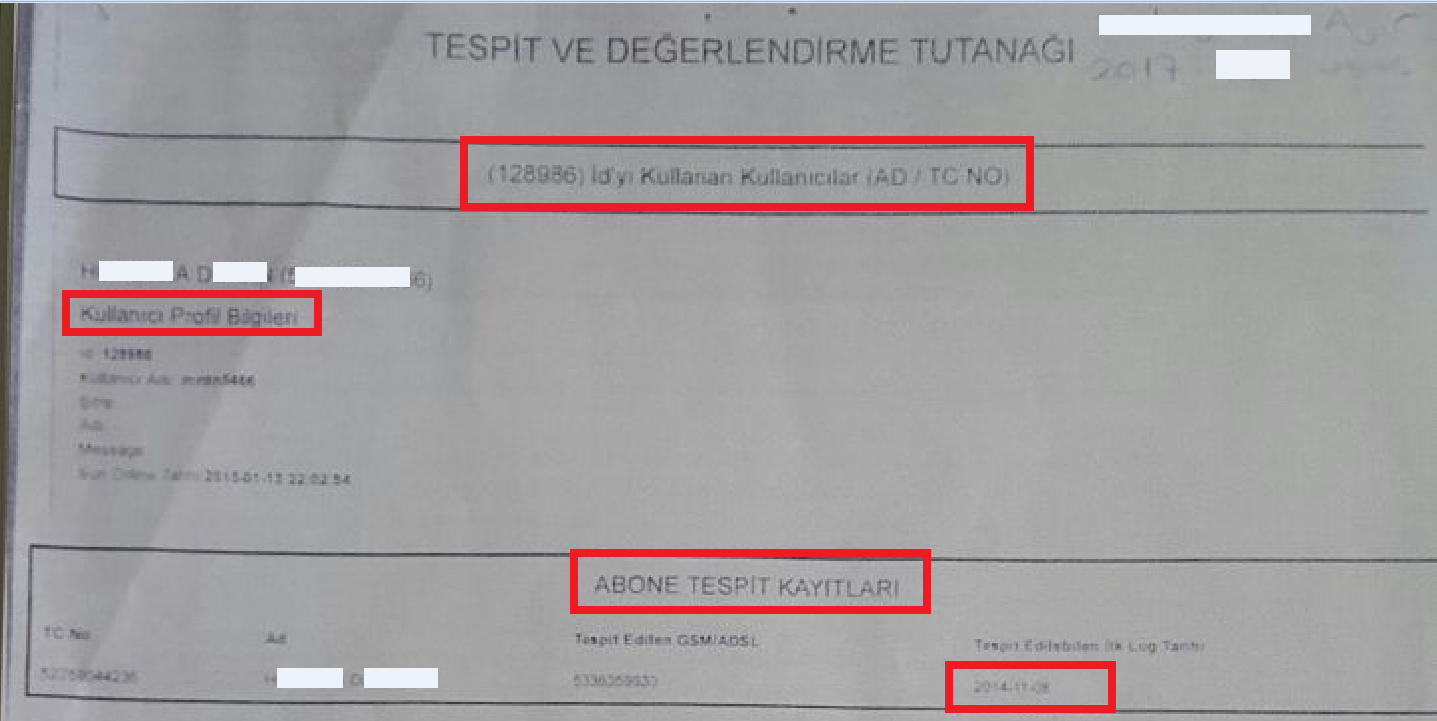
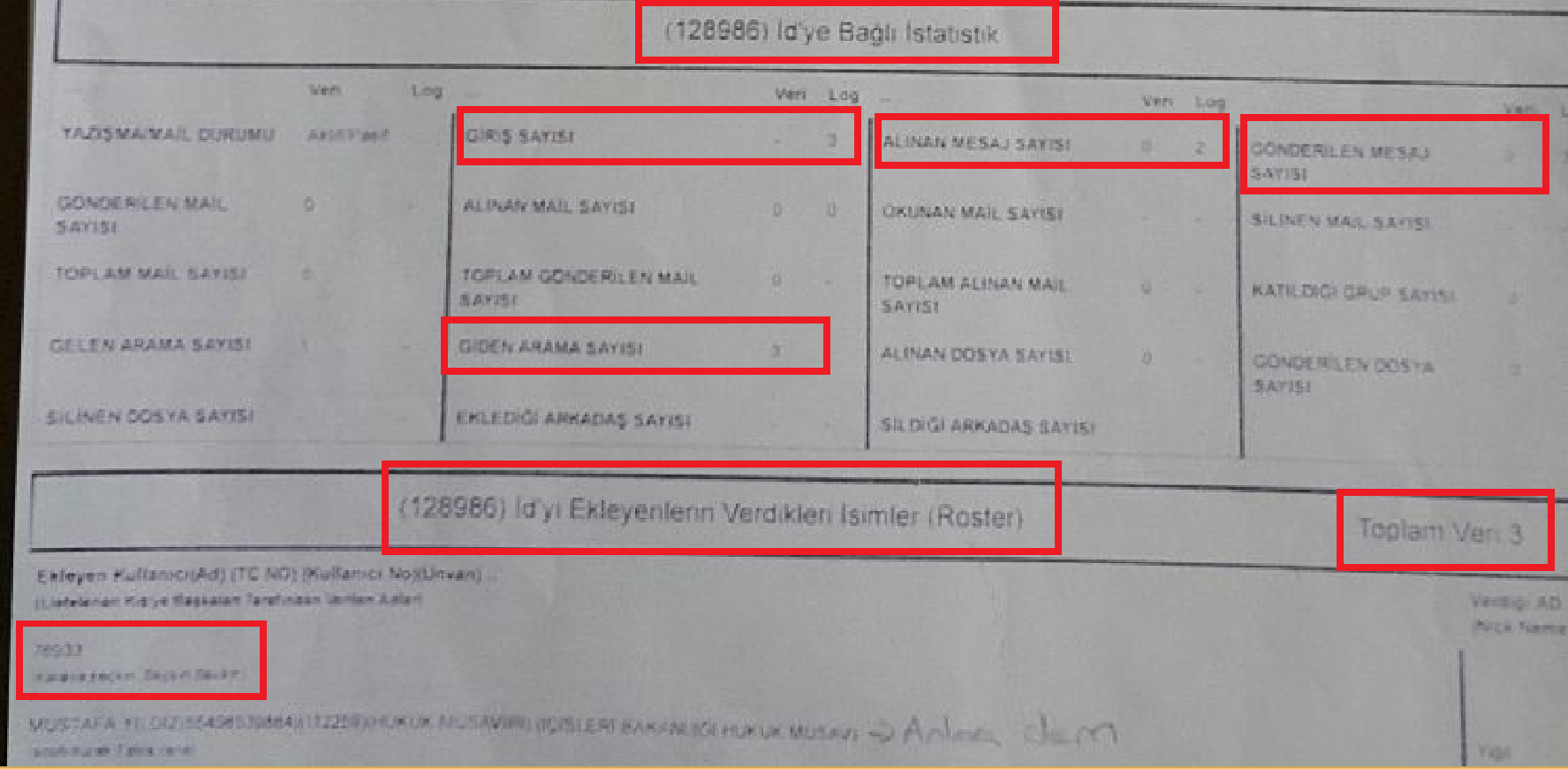
(2) **Gerçek ve aslına uygun olmalıdır.** Soruşturma veya kovuşturma altındaki konu ile ilgili doğrudan bir nedensellik bağı veya destekleyici mantıksal bağlar olması gerekir. Nedensellik bağı (illiyet rabıtası) aynı zamanda suçun kanun tanımında yer alan maddi unsurlarındandır ve meydana gelen netice ile fail arasındaki neden-sonuç ilişkisini ifade etmektedir. Adli kopya mahkemedeki dava konusu olayla ve faille ilgili ve bağlantılı olmalıdır.

(3) **Eksiksiz ve tam olmalıdır.** Elde edilebilen tüm deliller toplanmalıdır. Bu deliller yalnızca, failin suçlanmasına ilişkin değil, varsa suçsuzluğuna ilişkin olanları da kapsamalıdır. Nitekim 5271 sayılı Ceza Muhakemesi Kanunu’nun 170. maddesinin (4) ve (5) numaralı fıkralarına göre, iddianamede, yüklenen suçu oluşturan olaylar, mevcut delillerle ilişkilendirilerek açıklanmalı; iddianamenin sonuç kısmında, şüphelinin sadece aleyhine olan hususlar değil, lehine olan hususlarda ileri sürülmelidir. Sadece maddi olmamalıdır. Şüphelinin suçlu olduğunu veya suçsuz olduğunu kanıtlayan bir delil olmalıdır.

(4) **Güvenilebilir olmalıdır.** Delil güvenilir olmalıdır. Analiz için kabul edilmiş prosedürlere uygunluğundan ve doğruluğundan şüphe edilmemelidir.

(5) **İnanılabilir olmalıdır.** Delil, kanıtlama değerine sahip olmalıdır. Sanal yapıda olsa da, hakim veya taraflar tarafından açıkça anlaşılabilir ve inanılabilir olmalıdır.

(6) **Yasaya uygun olmalıdır.** Delil, yukarıdaki özelliklere sahip olsa da, yasaya uygun bir şekilde elde edilmemişse veya her ne kadar yukarıdaki özellikleri taşıyor olsa da yasaya uygun elde edilmediği için delil olarak değerlendirilemeyecektir. Örneğin 5271 sayılı CMK’nın 134. maddesine aykırı olarak bilgisayarlarda arama, kopyalama veya el koyma işlemi yapılmışsa, elde edilen verilerin mahkeme tarafından delil olarak kabul edilmeyeceği değerlendirilmektedir.

**“Sayısal verinin bilgi niteliği taşıyabilmesi için bulunduğu ortamdaki diğer benzer veriyle tutarlı bir bütün oluşturması gerekir**." prensibi doğrultusunda kayıtta adı görülen kişiye ait diğer bazı verilerin (IP adresi, erişim için kullanılan cihaz gibi) ve/veya sadece kayıtta adı görünen kişinin bilebileceği diğer bazı verilerin var olması halinde gerçek ve geçerli sayılabilir. Binlerce kişinin Bylock serverine erişim kaydı (CGNAT dökümleri) sadece **"Sinyal bilgisi"** ne yönelik olup, **"Sinyal tespiti/Bylock Serverine erişim"** yaptığı iddia edilip, Bylock Server'inde **"Sesli arama-alma, mail yollama-alma, mesaj yollama-alma vb"** işlemleri yaptığına yönelik her hangi bir **"log kaydı"** veya tespit tutanağı bulunmamaktadır.   
  
  
  
  
  
  
  
  
Yukarıda yer alan belgeler yine bir ByLock şüphelisine ait olup, kırmızı kutu içerisine alınan "id numarası, giriş sayısı, gönderilen-alınan mesaj bilgisi, gelen-giden arama, gelen-giden dosya vb." başlıklar altında şüpheliye ait olan ve ByLock'a erişim sağlayan telefon numarası, iletişim gerçekleştirdiği diğer ByLock kullanıcı bilgileri ve abonesi olduğu GSM servisine ait bilgiler yer almaktadır. Sadece BTK tarafından mahkemeye gönderilen GSM ve IMEI sorgusuna yönelik yapılan çalışmaya ait tespit kaydı bulunurken, yukarıda yer alan belgelerde belirtilen hususlara yönelik her hangi bir tespit bulunmamaktadır. **ByLock Serverine erişim bilgileri sadece sinyal bilgisi niteliğindedir**

**“3.2 ByLock Uygulaması IP/Alan Adı Analizi**

Söz konusu uygulamaya ait internet trafiğinin incelenmesi neticesinde, ByLock uygulamasının sunucu sistemine çoğunlukla doğrudan IP adresi üzerinden erişildiği, bazı sürümlerde ise (Örn. ByLock 1.1.3 sürümü) **“bylock.net”** alan adı üzerinden aynı sunucuya bağlanmak suretiyle iletişim kurulduğu görülmüştür.”,  
  
 Raporun 13. sayfasında: “Uygulamanın bağlandığı IP adreslerinin tespit edilmesi amacıyla farklı zamanlarda tekrarlanan testlerde, uygulamanın farklı sürümlerinin farklı birer IP adresine bağlandığı görülmüştür.   
  
 Uygulama sunucusunda geliştiricisinin uygulamaya özgü oluşturup imzaladığı bir sertifika (self-signed SSL certificate) ile HTTPS güvenlik protokolü kullanıldığı görülmektedir. Ayrıca tespit edilen sertifikaya yönelik çalışmalar neticesinde Litvanya’da sunucu kiralama hizmeti veren **"Baltic Servers"** isimli firmaya tahsisli 9 adet IP adresinin ByLock uygulamasının çeşitli sürümlerince kullanıldığı tespit edilmiştir:

**46.166.160.137**

**46.166.164.178**

**46.166.164.181**

**46.166.164.176**

**46.166.164.179**

**46.166.164.182**

**46.166.164.177**

**46.166.164.180**

**46.166.164.183**

**"censys.io"** isimli web sitesinde (söz konusu sitede tüm IPv4 adres uzayını kapsayan, geçmişe dönük çeşitli taramalar ve bunların sonuçlarına ait veriler sunulmaktadır) yayınlanan bilgiler kullanılarak çalışma teyit edilmiştir.

Tespit edilen IP adreslerinin incelenmesi kapsamında bu IP adreslerinin ByLock’un etkin olduğu tarihlerde hangi alan adı veya adları ile ilişkilendirildiği sorgulanmıştır. Bu kapsamda 1 Eylül 2015 – 9 Ekim 2016 tarihleri arasında anılan IP adreslerinden yalnızca 46.166.160.137 adresinin bylock.net alan adı ile kullanıldığı, diğer IP adreslerinin herhangi bir alan adı ile eşleşmediği bulgusuna ulaşılmıştır.   
  
 Açık kaynaklarda yapılan araştırmalardan çıkan sonuçlar da bu durumu destekler niteliktedir. **"virustotal.com, whois.domaintools.com, ptrarchive.com"** gibi web sitelerinde yapılan sorgulamalarda Bylock sunucularının aktif olduğu döneme ait başka bir alan adı kullanımına rastlanılmamıştır.  
  
  
 **“https://bylock.net:443/SHU-Server”**

**“https://46.166.164.181:443/App-Server”**

alan adlarının yer aldığı tespit edilmiştir.”,

“ByLock uygulamasının, "46.166.160.137" IP adresine sahip sunucu üzerinden hizmet sunduğu görülmüştür. Bahsi geçen sunucunun dashjohn@yandex.com isimli e-posta adresi kullanılarak kiralandığına dair e-posta içeriğine aşağıda yer verilmiştir. Bahsi geçen sunucunun, Litvanya’da hizmet veren "Baltic Servers" isimli firmanın kiraladığı sunuculardan biri olduğu görülmüştür.”

"Uygulama sunucusu yöneticisinin, uygulamayı kullananların tespitini nispeten zorlaştırmak amacıyla 8 adet ilave IP adresi (46.166.164.176, 46.166.164.177, 46.166.164.178, 46.166.164.179, 46.166.164.180, 46.166.164.181, 46.166.164.182, 46.166.164.183) kiralamıştır. Kiralanan IP adreslerine ilişkin elde edilen e-posta içeriğine aşağıda yer verilmiştir.” ifadeleri yer almaktadır.

MİT raporunun farklı sayfalarında görülen ifadeler arasındaki farklılıklar sebebiyle sistemin dönemsel olarak 9 adet IP adresi ile veya anılan 2 IP adresi ile çalıştığı konusu net olarak anlaşılamamaktadır." denilerek "46.166.164.181 ve 46.166.160.137" IP numaralarının ByLock Servirinin kullanımında olduğu diğer 7 IP numarasının ise teknik takibi zorlaştırmak amacıyla manipülatif olarak kullanıldığı belirtilmektedir.

Hemen hemen benzer tüm davalarda soruşturma savcıları ve mahkemeler, teknik destek alıp davalarını teknik verilerle neticeye ulaştırıken, bu kadar önemli davalarda Adli Bilişim uzmanı veya başkaca teknik konularda bilirkişiye başvurulmaması, neticede bir çok mağduriyetlerin doğmasına sebebiyet vermeye devam edecektir.