K. K.
24.07.17
Ali Rıza TEMEL
Yazı İşleri Müd.

BİLİRKİŞİ RAPORU

ANKARA CUMHURİYET BAŞSAVCILIĞINA
(Anayasal Düzene Karşı İşlenen Suçlar Soruşturma Bürosu)

Soruşturma No	:	**2016/104109**
Görevlendirilme Nedeni	:	ByLock programı ile ilgili Internet üzerindeki açık kaynaklar üzerinden araştırma yapılmak suretiyle; - ByLock isimli programın ne olduğu, - Kimler tarafından kullanıldığı, - Halen kullanımda olup olmadığı, - Kriptolu iletişim yapılmasına olanak sağlayıp sağlamadığı hususlarının araştırılarak rapor düzenlenmesi istenilmiştir.
	:	ByLock Veri tabanı dosyasına ait Imaj kopyasının bulunduğu 1 adet Seagate Marka Z9A4E51C seri nolu 1TB image diski içerisindeki dosyaların incelenerek, dosya içeriklerinin raporlanması
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.

ByLock ile ilgili açıklamalardan önce kullanılan teknolojiler ile ilgili çeşitli terimlerin açıklanması gerekmektedir.

1.1.VoIP (Voice over IP)

VoIP konusunda ön bilgi, alt protokoller olan TCP/UDP, RTP ve Java Media Framework ile kriptolama konuları teorik olarak ayrıntılı olarak anlatılmıştır.

Voice over IP veya IP üzerinde ses, günümüz dünyasında yaygın olarak kullanılan bir haberleşme teknolojisidir. VoIP, temel olarak, sesli bir iletişim kurmak için telefon ağının yerine, bilgisayar ağının kullanılması anlamını taşıyor. Özellikle 1990'li yılların baslarında yaşanan

bilgisayar ağları ve ağ bileşenlerindeki teknolojik gelişimle birlikte, mevcut telefon şebekesi mimarisi üzerinde yapılan geliştirme çalışmalarıyla, anahtar devreli telefon sistemleri üzerinden sağlanan ses haberleşmesi, zamanla IP tabanlı altyapılar üzerinden gerçekleştirilmeye başlamıştır.

VoIP (Voice over Internet Protocol), oldukça geniş bir konu olmasına rağmen özünde ses sinyallerinin bir IP kaynak noktasından hedef IP noktasına kabul edilebilir standartlarda iletilmesidir. Bu anlamda VoIP, bir telefon görüşmesi yapmak için telefon ağının yerine, bilgisayar ağının kullanılması anlamına geliyor. Bir kurumda bir bilgisayar ağı ve bir de telefon ağı varsa, VoIP bu iki ağın birleştirilmesini sağlıyor. Böylece hem zaman açısından hem de maliyet açısından büyük bir tasarruf sağlanmış oluyor. İkinci olarak, internet erişiminin olduğu ortamda, telefon görüşmeleri ISS'in (Internet Servis Sağlayıcı) sağladığı ağ üzerinden yapılabilir. Standart telefonların sağladığı özelliklere ilave olarak IP ve bilgisayar dünyasının sağladığı içerik zenginliği ile birlikte, sesli konferans ya da video konferans yapılmasını da mümkün kılar.

VoIP teknolojisinde, iletilen ses verileri dosya seklinde düşünülebilir. IP ağı üzerinden iletilen her turlu veri küçük IP paketlerine dönüştürülerek ağ üzerinden iletilir. VoIP uygulaması, diğer anlamda IP telefon veya yazılım telefonu, analog konuşmayı sayısal sinyallere çevirir ve IP paketlerine dönüştürür. Oluşturulan IP paketleri ethernet kablosu üzerinden IP ağına iletilirler.

Her aşaması oldukça genişletilebilecek bir konu olan VoIP, iki IP noktası arasında ses iletişimi gerçekleştirirken aşağıdaki adımları takip eder.

1. Konuşmayı oluşturan analog sesler, kullanılan bilgisayarın ses kartıyla ses kodlayıcı tarafından (Voice encoder) sayısal sinyale çevrilir.
2. Bu sayısal sinyal IP paketlerine bölünür ve gideceği yere, sıraya bakılmaksızın, sürekli bir sinyal olmadan, gönderilir.
3. IP paketleri IP Şebekesi boyunca bireysel olarak iletilirler.
4. Alıcı tarafta bulunan bir Jitter, paket Şebekenin oluşturduğu herhangi bir gecikmeyi dengeleyerek, düzgün ve kesintisiz ses çıkışını kod çözücü (Decoder) üzerinden sağlar

Mevcut VoIP çözümlerinin hemen hepsi merkezi bir sunucu (server) kullanmaktadır. Sunucu aracılığıyla sinyalleşmeyi gerçekleştiren kullanıcılar (client) arasında RTP iletişimi başlar ve sunucu çağrının her aşamasını kontrol eder.

Ses paketlerinin iletiminde, paketlerin ulaşımının analog ses sinyalleriyle senkronizasyonun sağlanması son derece önemlidir. Paketlerin doğru zamanda ve doğru sırada oynatılması gerekir. Gerçek zamanlı iletişimde, gecikmenin mümkün mertebe minimize edilmelidir. IP Şebekeleri en-

iyi dağıtım (best-effort service) ilkesine göre çalıştığından böyle bir garanti yoktur. Benzer olarak kayıp paket sayıları özellikle yığılma zamanlarında artabilmektedir. Veri iletişimi yapılmadan önce, iki parti arasında bağlantı kurulur, veri değiş-tokuşu yapılır, sonra bağlantı sonlandırılır. Veri paketleri gönderildiği sırayla hedef noktaya ulaşır. Yığılma ve kayıplara karsı tanımlanmış mekanizmaları vardır. Tüm bu güzel özelliklerine rağmen TCP, VoIP uygulamaları açısından bazı dezavantajlar içermektedir. TCP, esasında kayıp paketlerin tekrar iletilmesine dayanmaktadır. Bu paketlerinin sırasının korunmasıyla birlikte güvenilir bir iletim sunarken, paketlerin iletimine gecikme (delay) eklemektedir. Oysa gerçek zamanlı iletişimde, ciddi bir gecikmedense kabul edilebilir seviyede bir kayıp tercih edilir. Yığılma ve kayıp kontrol mekanizmaları faydalı özellikler olarak düşünülebilir ancak uygulama seviyesinde bunlar üzerinde çok az nüfuz söz konusudur. TCP uygulamadan bağımsız olarak, kaybedilen bir paketin tekrar gönderilmesi uzun sayılabilecek bir süre alabilir ve böylece paket iletimini tıkayabilmektedir.

VoIP uygulamalarında, TCP'nin bir diğer dezavantajı da aynı anda bir paketin birden fazla noktaya iletilmesi (multicast) esnasında görülmektedir. IP, multicasting konusunda efektif dağıtım metodu sunarken, TCP bunu desteklemez. Her bir IP noktası ile ayrı ayrı TCP bağlantısı kurarak bunu yapar ve bu da netice olarak daha fazla band genişliği demektir.

Güvenilir bir protokol olan TCP, birçok kompleks özelliğine rağmen, VoIP uygulamalarında, nispeten oldukça basit bir protokol olan UDP tercih edilir. Kayıp paketlerin tekrar gönderilmesi için beklememesi UDP için TCP ye göre önemli bir avantajdır. Aynı zamanda, UDP, IP multicasting özelliklerinden de faydalanarak band genişliği konusunda tasarruf sağlar. Proje kapsamında yazılan uygulama da ses iletişimi için UDP yi kullanmaktadır. Ancak UDP de senkronizasyon, yığılma ve kayıp kontrol gibi özellikler olmadığından bunların dengelenebilmesi için UDP'ye bazı eklentiler yapmak gerekmektedir. Bu da aslında RTP (Real-time Transport Protocol)'nin görevidir.

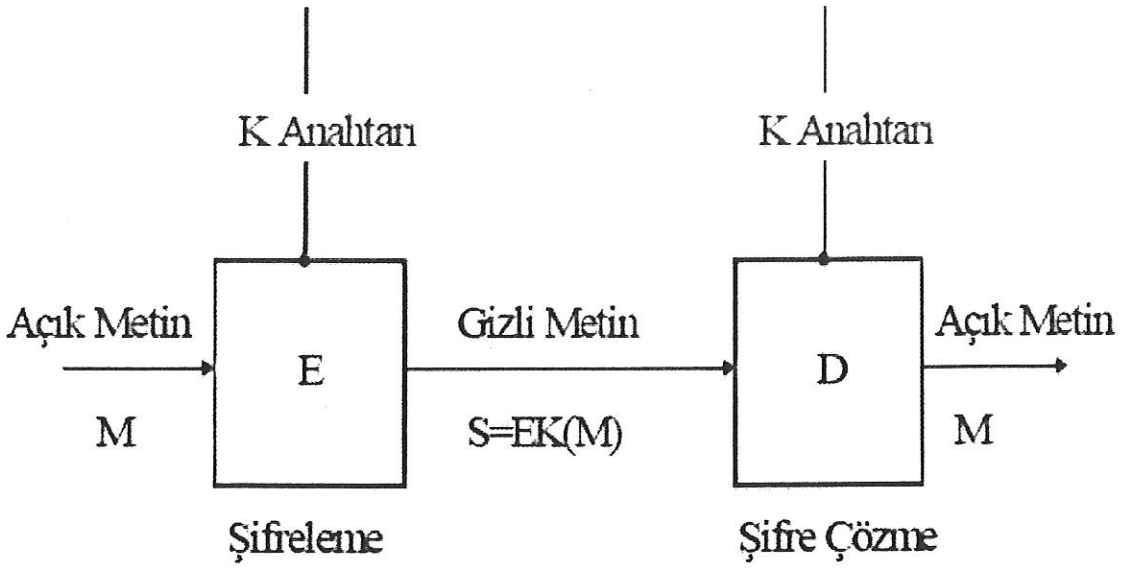
VoIP uygulamalarının birçoğu ilgili partilerle anlaşmanın sağlanması ve oturumun başlaması için sinyalleşme protokolleri kullanır. Baskın olarak kullanılan protokol Session Initiation Protocol (SIP)'dır. Bunun yanında oldukça popüler olan, XMPP gibi, başka IETF protokolleri de vardır. Bu protokoller yalın VoIP uygulamalarının yanında, video konferans, multimedia çözümleri, anlık mesajlaşma, kullanıcının mevcut durumu (presence), online oyunlar gibi çok geniş bir kullanım alanına sahiptir.

1.2. Kriptoloji

Kriptoloji, Yunanca krypto's (saklı) ve lo'gos (kelime) kelimelerinin birleştirilmesinden oluşturulmuştur ve iletişimde gizlilik bilimi olarak değerlendirilmektedir. Ticari ilişkilerde, devlet işlerinde, askeri işlerde ve personel ilişkilerinde güvenli iş çalışması yapmak büyük bir sorundur. Sistemler arası bağlantılarda ya da herhangi iki nokta arasındaki haberleşmede verinin güvenli bir şekilde gittiğinden emin olmak gerekir. Bunun sağlanması ise gönderilen çeşitli taşıma protokolleri (TCP, UDP, ATM, vs) RTP kontrol protokolü (RTCP) gerçek zamanlı taşıma protokolü (RTP) RTP arayüzü ve uygulamaları ile veri şifrelenir. Böylece açık haberleşme kanalları kullanılarak verinin güvenli bir şekilde ulaştırılması sağlanır. İletişimde, açık bir haberleşme kanalı kullanılıyorsa gizli tutulmak istenen bilginin yetkisiz bir kişi tarafından dinlenebileceği veya haberleşme kanalına girip (araya girme) veriyi bozabileceği ya da değiştirebileceği (yanlış verinin gönderilmesi) düşüncesi her zaman için önemli bir problem oluşturur.

Kriptoloji esas olarak iki bölüme ayrılır: Kriptografi (Şifreleme) ve kriptoanaliz (Şifre çözme). Gönderilmek istenen orijinal mesaj açık mesaj ve bu mesajın şifrelenmiş hali şifreli mesaj olarak adlandırılır. Şifreleme, askeri ve diplomatik iletişimde (haberleşmede) güvenliği sağlamak için bin yıldır kullanılmaktadır. Ancak bugün artık özel sektörde de gereksinim duyulmaktadır. Sağlık hizmetleri, finansal işler (örneğin: kredi oranları) gibi konularda bilgisayarlar arasındaki haberleşmede açık kanallar kullanılarak yapılmaktadır. Bu açık kanalların kullanılması sırasında yukarıda sayılan işlerin güvenli ve gizli bir şekilde yapılabilmesi için şifrelemeye gerek duyulmaktadır.

Bir mesajın anlaşılabilirliğini gizlemek amacı ile iki yöntem uygulanabilir. Bunlardan birincisi mesajın belirli bir yöntem uyarınca kısaltılması, diğeri ise belirli bir teknikle mesajın anlaşılamaz bir biçime dönüştürülmesidir. Bunlardan ilkine stenografi, diğerine ise kriptografi denir. Verinin orijinal biçimindeki haline açık metin denir. Dönüştürülmüş biçimine ise şifrelenmiş metin veya gizli metin denir. Dönüştürme işlemine şifreleme veya kriptolama diyoruz. Dönüştürülmüş metnin ters işlem sonucu açık metin halinin elde edilmesine ise şifre veya kripto çözme denir. M açık metni, E ve D simgeleri de kriptolama ve kripto çözme işlemlerini temsil ettiğinde, gizli metin S, S = EK(M) olarak gösterilir. Gizli metinden açık metnin elde edilmesi amacı ile kripto çözme işlevinde kullanılması, M = EK(S) olarak gösterilir. Her iki ifadede kullanılan K, kripto anahtarını temsil etmektedir.



Şekil 1.2.1 Şifreleme ve Şifre Çözme İşlemleri

Burada K anahtarını kullanmanın amacı, eğer M açık metni sadece E kripto işlevi ile şifrelenirse gizliliği sağlayacak olan tek parametrenin kripto algoritması olması ve iletişim güvenliğini arttırmak için alıcı tarafın her yeni kripto işlevi için farklı bir kripto algoritmasını bilmesinin gerekmesidir. Eğer mesajın şifrelendiği E işlevi kaybolacak olursa yeni bir algoritma tasarlanmak durumundadır. Bu durumda zaman kaybı da göz önüne alınacak olursa bu oldukça pahalı bir yöntemdir. Bunun yanı sıra K anahtarı mesajın kripto algoritması bilinse de ikinci bir güvenlik parametresi olduğundan iletişim güvenliğini arttırmaktadır.

1.3.AES Algoritması

AES (Advanced Encryption Standard; Gelişmiş Şifreleme Standardı), elektronik verinin şifrelenmesi için sunulan bir standarttır. Amerikan hükûmeti tarafından kabul edilen AES, uluslararası alanda da şifreleme (kripto) standardı olarak kullanılmaktadır. DES'in (Data Encryption Standard - Veri Şifreleme Standardı) yerini almıştır. AES ile tanımlanan şifreleme algoritması, hem şifreleme hem de şifreli metni çözmede kullanılan anahtarların birbiriyle ilişkili olduğu, simetrik-anahtarlı bir algoritmadır. AES için şifreleme ve şifre çözme anahtarları aynıdır.

AES, ABD Ulusal Standart ve Teknoloji Enstitüsü (NIST) tarafından 26 Kasım 2001 tarihinde US FIPS PUB 197 kodlu dokümanla duyurulmuştur. Standartlaştırma 5 yıl süren bir zaman zarfında tamamlanmıştır. Bu süreçte AES adayı olarak 15 tasarım sunulmuş, tasarımlar güvenlik ve performans açısından değerlendirildikten sonra en uygun tasarım standart şifreleme algoritması olarak seçilmiştir. Federal hükûmetin Ticaret Müsteşarı'nın onayının ardından 26 Mayıs 2002

tarihinde resmî olarak etkin hâle gelmiştir. Hâlihazırda birçok şifreleme paketinde yer alan algoritma Amerikan Ulusal Güvenlik Teşkilatı (NSA - National Security Agency) tarafından çok gizli bilginin şifrelenmesinde kullanımı onaylanan kamuya açık ilk şifreleme algoritmasıdır.

AES hakkında önemli bir nokta AES'in şifreleme standardının ismi olmasıdır. Ancak pratik kullanımda AES, standartta belirtilen şifreleme algoritmasının yerine geçecek şekilde kullanılmaktadır.

1.4. Anlık Mesajlaşma (Instant Messenger)

(IM) aynı anda çevrimiçi (online) olan kişiler arasında eş zamanlı iletişim sağlayan, ses, dosya ve görüntü aktarımına olanak veren yazılımların genel adıdır. **Anlık mesajlaşma**, bir bilgisayar programı sayesinde, üye olarak, listenize eklediğiniz kişilerle gerçek zamanlı görüşme olanağıdır. Kullanılan programın özelliğine bağlı olarak görüntülü ve sesli görüşme olanağı, ses, dosya ve görüntü aktarımı da yapılabilir. En bilinen anında mesajlaşma programları ICQ, Yahoo Messenger, MSN Messenger'dır, Smart (Akıllı) Telefonlarında ise Whatsapp, Skype, Viber, Line gibi örnekler verilebilir.

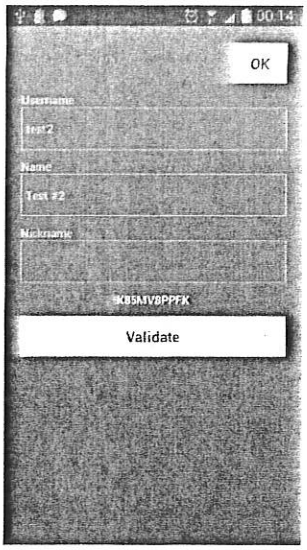
2. ByLock

ByLock Internet erişimi olan mobil cihazlar ve mobil cihaz özelliklerine sahip diğer sistemler kullanılarak yazılı mesaj (chat) yapılması, dosya alınıp gönderilmesi, e-posta alınıp gönderilmesi ve sesli arama (voip) yapılmasına olanak sağlayan mobil uygulamadır. Uygulama bu hali **Anlık Mesajlaşma (Instant Messenger)** uygulaması olarak değerlendirilebilir.

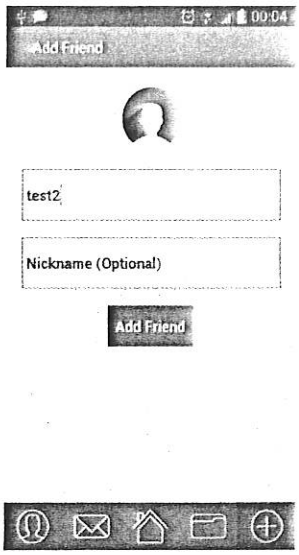
ByLock programı ile ilgili olarak raporun düzenlendiği dönem içerisinde sunucularının aktif olmamasından dolayı, söz konusu program hakkında Internet üzerindeki açık kaynaklardan (herkes tarafından herhangi bir izin gerektirmeden erişim sağlanabilen yerlerden) araştırmalar yapılarak aşağıdaki bilgiler elde edilmiştir.

Internet üzerindeki açık kaynaklardan elde edilen verilere göre programın ekran görüntülerinin aşağıdaki gibi olduğu tespit edilmiştir.

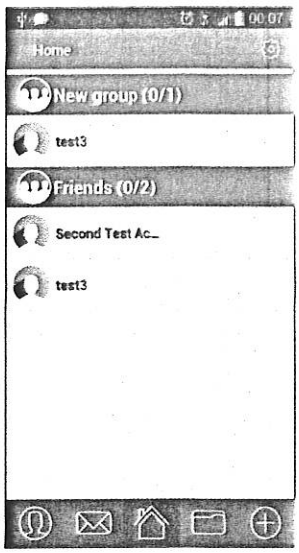
Şekil 2.1 (**byLock** Logosu)



(a) (Onaylama Ekranı)



(b) (Arkadaş Ekleme Ekranı)

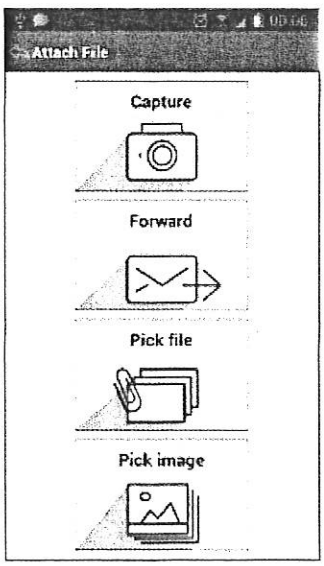


(c) (Grup Ekranı)

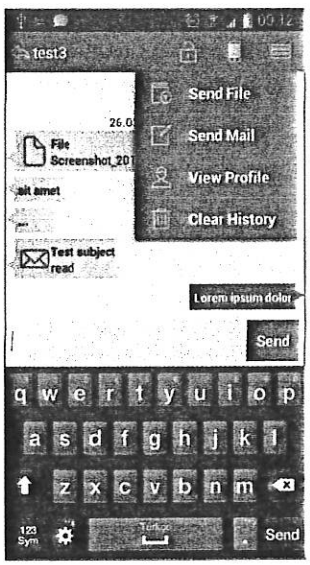
Şekil 2.2 "byLock görümleri"

"byLock" programının bir doğrulama sisteminin bulunduğu, bu doğrulama işleminde "**Username=Kullanıcıadı**", "**Name=İsim**" ve "**Nickname=Takmaad**" olarak (3) adet bilginin girilmesi gerektiği anlaşılmaktadır. Doğrulama işleminin hangi amaçla yapıldığı, doğrulama kodunun nereye gönderildiği ekran görüntüleri üzerinden belirleme olanağı bulunmamaktadır.

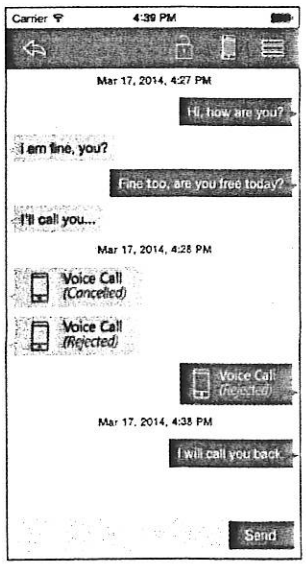
"Add Friend" (Arkadaş Ekleme) bölümünde iletişim kurulmak istenilen kişinin "**UserName= Kullanıcı Adı**" bilgisinin girilerek "**byLock**" uygulaması kullanan kişiler arasından arama yapılarak bu kullanıcılar ile iletişim kurulduğu anlaşılmakta, ekran görüntülerinde grup oluşturma ekranının olduğu görülmektedir.



(d) (Dosya Ekleme Ekranı)



(e) (Yazışma Ekranı)



(f) (Yazışma Ekranı)

Şekil 2.2 "byLock görünümleri"

Arkadaş listesine eklenen kişiler ile bire bir (P2P) iletişim kurulabileceği gibi grup oluşturularak grup içerisinde mesajlaşma yapılabilmektedir. **"byLock"** üzerinden kurulan iletişimlerde sohbet yapılması, dosya gönderilmesi, resim gönderilmesi, mail gönderilmesi, sesli görüşmeler yapılmasına olanak sağladığı görülmektedir. *(Değerlendirmeler Internet kaynakları üzerinden elde edilen ekran görüntülerine dayanılarak yapılmıştır.)*

Yapılan araştırmalarda https://apkdot.com/apk/by-lock/bylock/bylock-1-1-7/ ve http://apk-dl.com/bylock-secure-chat-talk link adreslerinde **"byLock"** programının Android Uygulama Paket (*.apk) dosyasına ait 1.1.7 versiyonun siteye yüklenmiş olduğu görülerek söz konusu uygulama dosyası belirtilen konumlardan indirilerek üzerinde çalışmalar yapılmıştır.

URL adresi	: https://apkdot.com/apk/by-lock/bylock/bylock-1-1-7/
Filename	: net.client.by.lock-1.1.7-17_APKdot.com.apk
Version	: 1.1.7 (17)
Uploaded	: August 14, 2015 GMT+0300
File size	: 1.77 MB (1772140 bytes)
Min. Android version	: 2.3 and up
MD5sum	: 84fddf10a23f4f25b5212232b73cd557
SHA1sum	: cac87620162e211b4fb02719a244b8127610cb7e
Downloads	: 9037

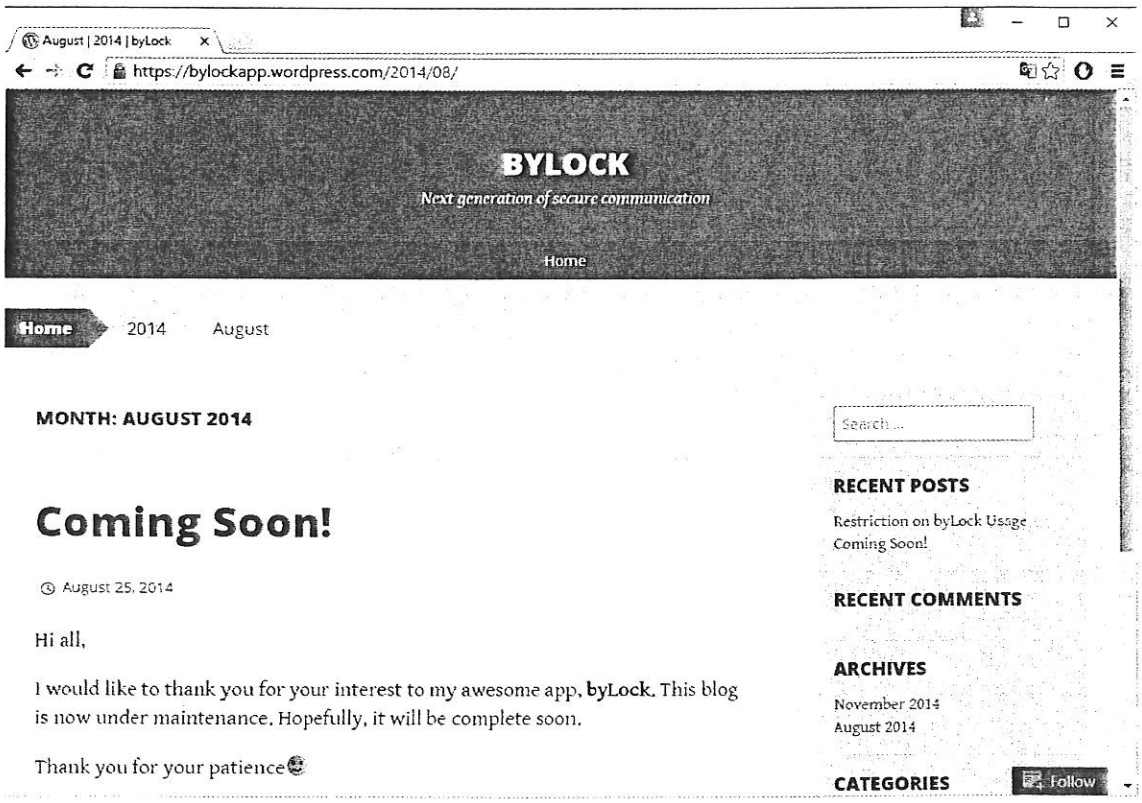
Şekil 2.3 (byLock 1.1.7 versiyonunun İndirildiği Web Sitesi)

URL Adresi	: http://apk-dl.com/bylock-secure-chat-talk
Download ByLock	: Secure Chat & Talk 1.1.7 Latest Version APK File
Uygulama Adı	: ByLock: Secure Chat & Talk 1.1.7
Package Name	: net.client.by.lock
Katagori	: İletişim
Geliştirici	: By Lock
Version	: 1.1.7
Yayın Tarihi	: 26 Aralık 2014
File Size	: 1.7M
Gerekli Android Ver.	: 2.3 and up
Geliştirici website	: https://bylockapp.wordpress.com/
E-Posta	: **keynes97209@gmail.com**

Şekil 2.4 (byLock 1.1.7 versiyonunun İndirildiği Web Sitesi)

http://apk-dl.com/bylock-secure-chat-talk isimli sitede https://bylockapp.wordpress.com/ isimli blogun ve keynes97209@gmail.com e-posta adresinin **"byLock"** programının geliştiricisi olarak görünen kişiye ait olduğunun belirtilerek görülmüştür.

https://bylockapp.wordpress.com/ blog sayfasına erişim sağlandığında halen yayında olduğu, 2014 Ağustos ve 2014 Kasım aylarında (2) iki yayın yapıldığı görülmüş, yapılan yayınlar aşağıda sunulmuştur. **keynes97209@gmail.com** e-posta adresine Internet üzerinde yapılan açık kaynak araştırmalarında **"byLock"** programı ile ilgili yapılan açıklamalar içerisinde geçtiği görülmüş başkaca bir tespit yapılamamıştır.



Şekil 10 (https://bylockapp.wordpress.com/2014/08 tarihli yayın)

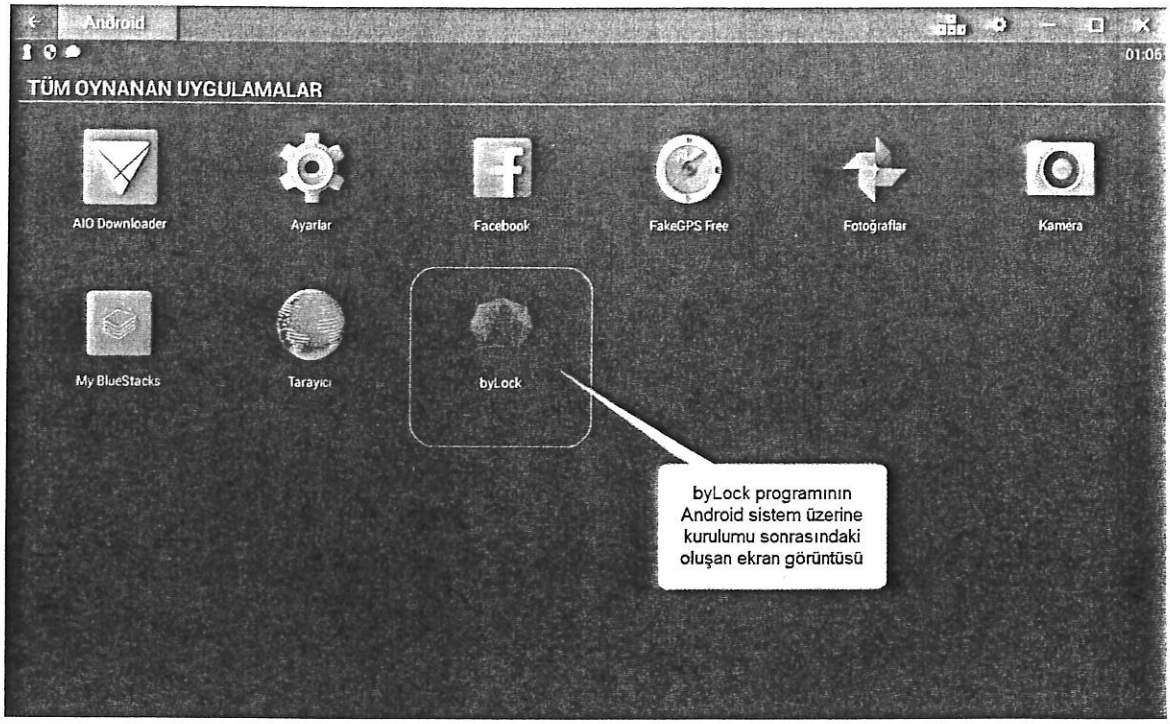
25 Ağustos 2014 tarihinde blog üzerinden "ÇOK YAKINDA" şeklinde bir haber yayınlandığı, bu yayında "byLock uygulamasına gösterilen ilgiden dolayı teşekkür ederiz, blog bakım altında..." şeklinde içerik olduğu görülmüştür.

Şekil 2.5 (https://bylockapp.wordpress.com/2014/11 tarihli yayın)

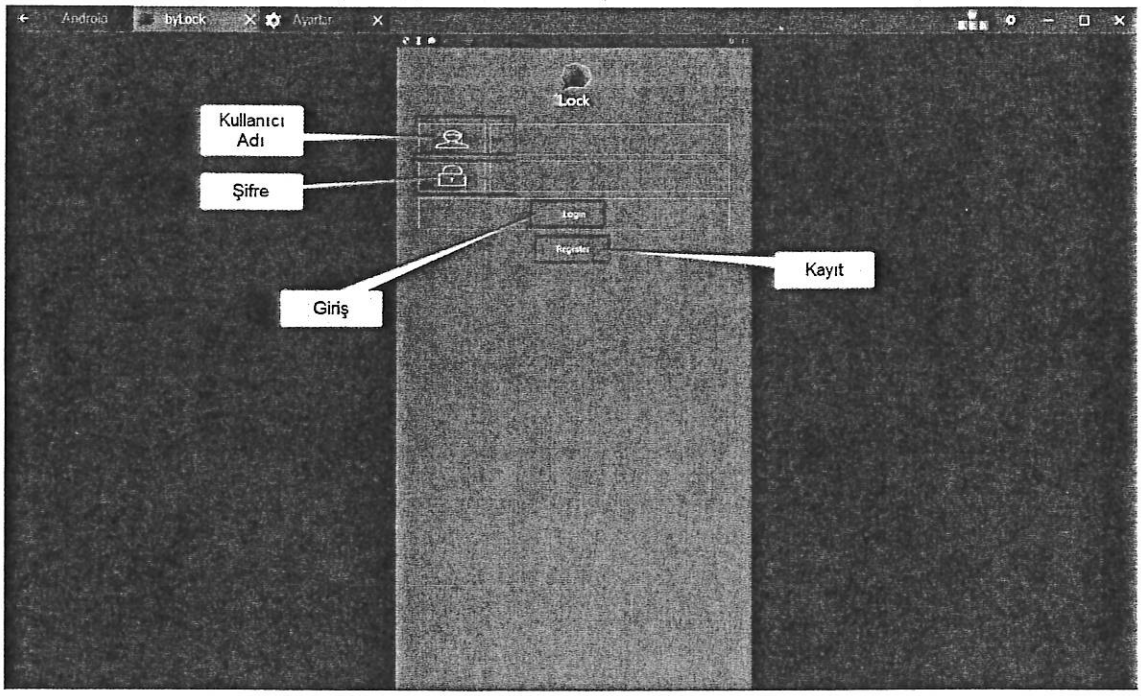
Aynı blog sayfasında 15 Kasım 2014 tarihinde ikinci bir haber yayınlandığı, bu haber içeriğinde ise özetle, uygulamanın AppStore üzerinden de yayınlandığını, bazı IP bloklarının engellendiğini, bu nedenle VPN üzerinden kullanımının önerildiği belirtilmiştir.

Blog sayfasında başkaca bir bilginin olmadığı, Wordpress.com isimli sitenin ücretsiz blog hizmeti veren yurt dışı kaynaklı bir site olduğu bu nedenle söz konusu içeriği oluşturan kullanıcı ile ilgili bilgi toplanamamıştır.

http://apk-dl.com/bylock-secure-chat-talk ve https://apkdot.com/apk/bylock/bylock/bylock-1-1-7/ link adreslerinden programın **v1.1.7** versiyonu indirilerek **Sanal Android** emulator uygulaması olan ve Windows işletim sistemi üzerinde üzerinde çalışabilen **BlueStacks** programı üzerine **test amaçlı olarak kurulumu gerçekleştirilerek test ortamı oluşturulmuştur.** ByLock programına ait Android Uygulama Paket (*.apk) dosyasının **v1.1.7** versiyonu kurulduğunda Şekil.13'deki ikonu ile kurulduğu ve kullanıma hazır hale geldiği,

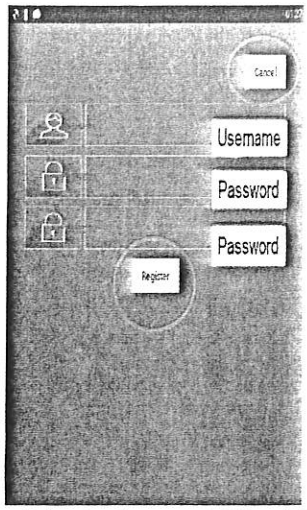


Şekil 2.6 (BlueStack üzerine kurulu byLock uygulaması)



Şekil 2.7 (byLock çalıştırıldığında ilk açılan ekran)

"byLock" programı Adroid platformda ilk çalıştırıldığında ekranda giriş ekranının açıldığı, ekranda "**Username**" ve "**Password**" girişi yapılmasının istenildiği, giriş butonunun hemen altında ise kayıtlı olmayan kullanıcılar için kayıt (**Register**) butonunun bulunduğu görülmüştür. "**Register**" butonuna tıklandığında aşağıda ekran görüntüsü alınmıştır.

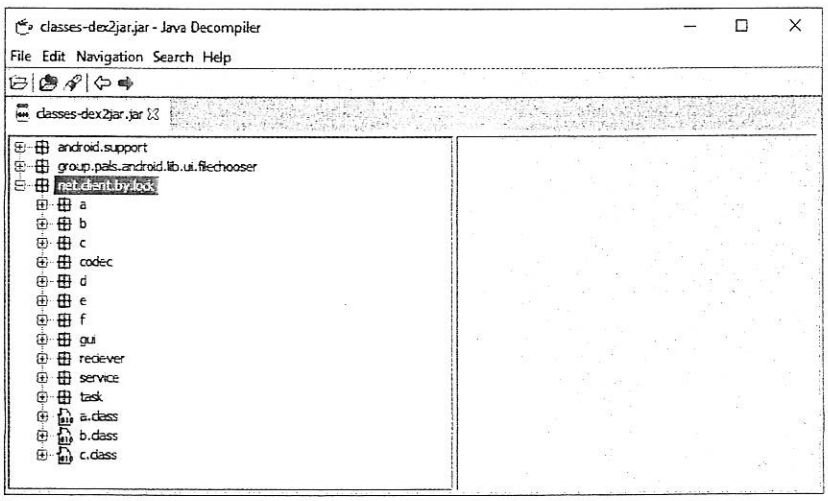


Şekil 2.8 (byLock Register butonuna tıklandığında alınan görüntü)

Kayıt ekranında "**Username**" yani kullanıcı adının belirlenmesini, sonrasında ise şifre belirlenmesi istenmektedir.

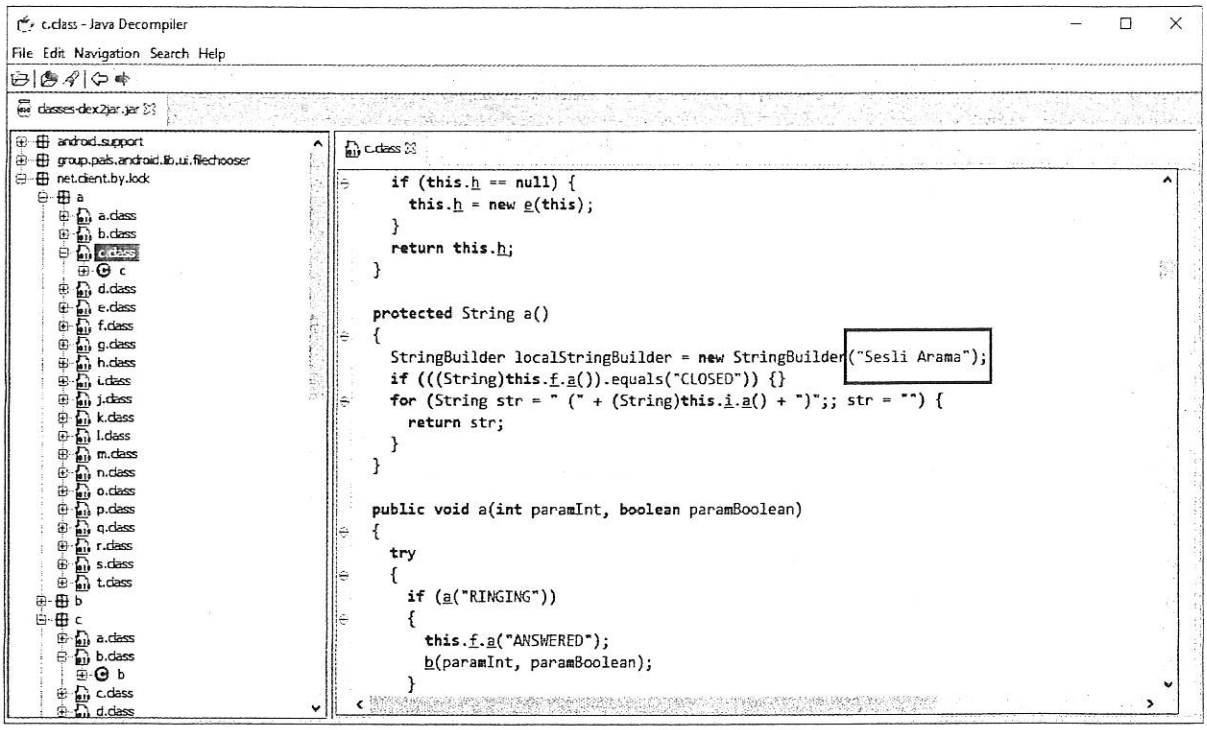
Kullanıcı adı bölümüne herhangi bir karakter, sayı, harf veya sembol girişi yapılabildiği, **Password** kısmına ise en az **(6) karekter** uzunluğunda, **harf, rakam ve sembollerden** oluşan en az (6) karakter uzunluğunda bir şifrenin girilmesi gerekmektedir. Bu işlemden sonda **Register** butonuna tıklandığında kayıt işlemleri başlamaktadır. İşlemin nasıl tamamlandığı veya devamında hangi prosedürlerin çalıştığı "**byLock**" uygulaması sunucusuna erişim sağlanamadığından detaylandırılamamıştır.

"byLock" uygulamasının indirilen ***.apk** dosyası **Java Decompiler 1.4.1** yazılımı kullanılarak kodları üzerinde inceleme yapılmıştır.

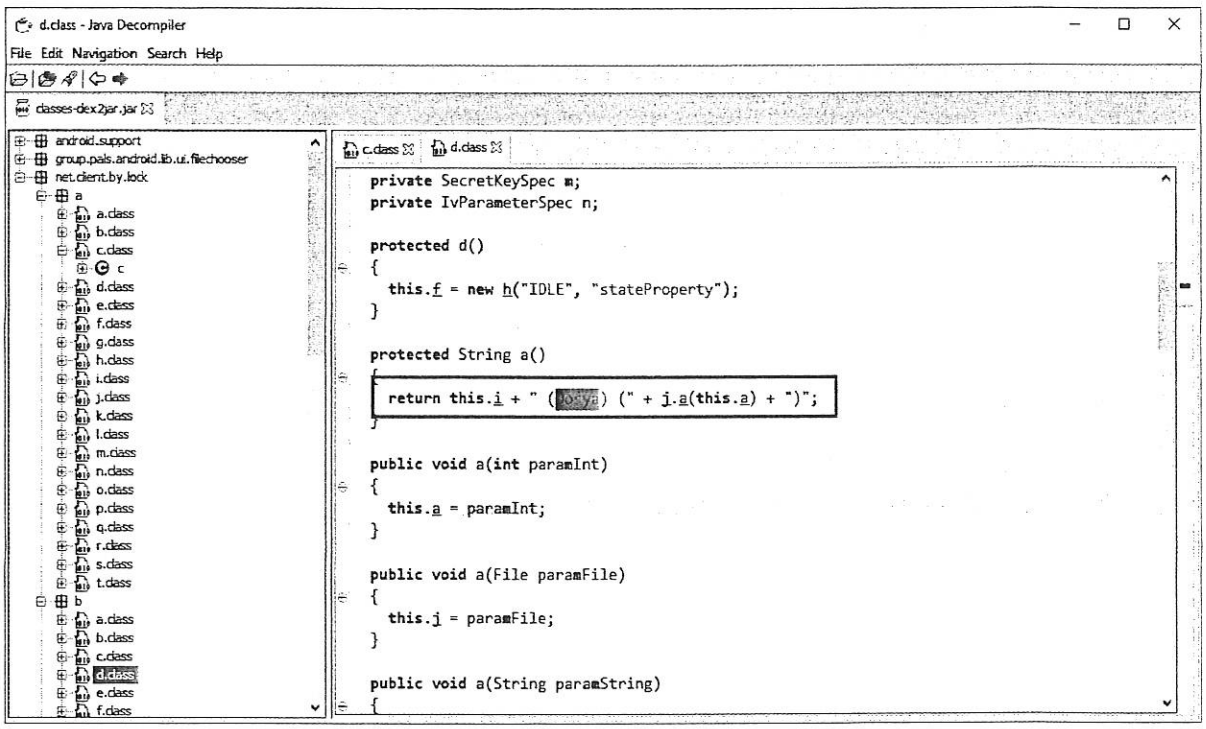


Şekil 2.9 (Classes dosyası **Java Decompiler 1.4.1 ile görüntüsü**)

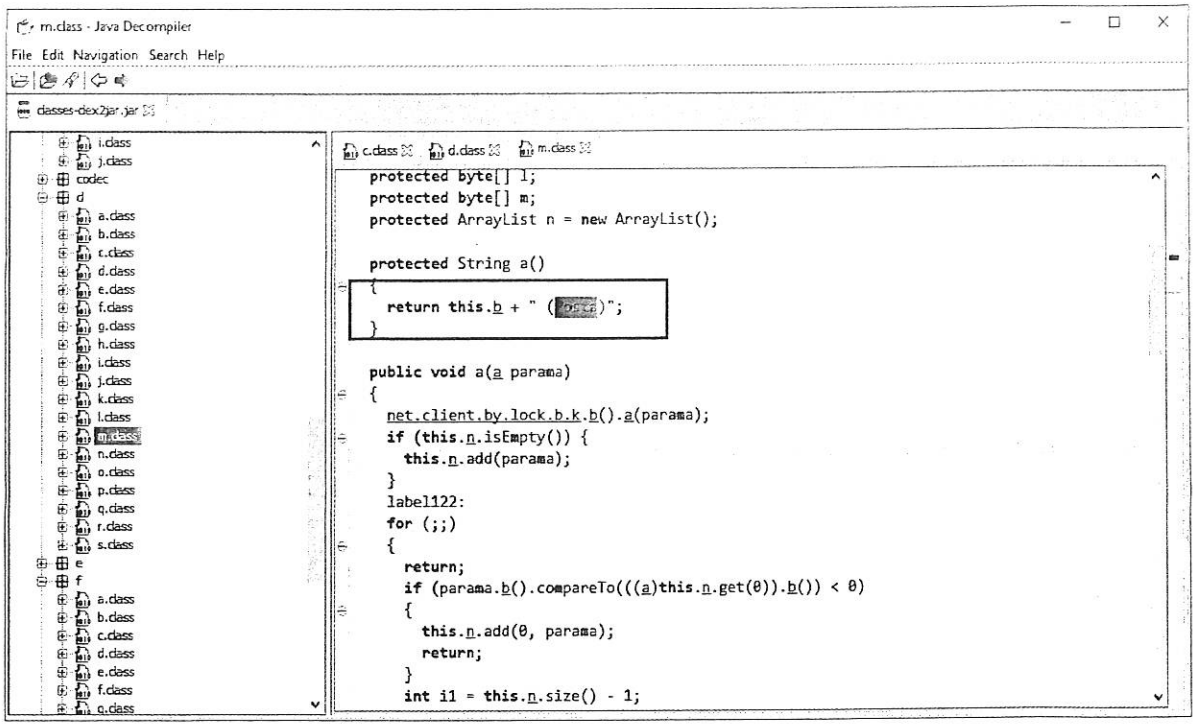
"byLock" uygulamasına ait Android Uygulama Paket (*.apk) dosyasına ait kodların incelenmesi esnasında bazı verilerin Türkçe olarak girildiği görülmüştür. Türkçe karakter içeren kodlar aşağıda listelenmiştir.



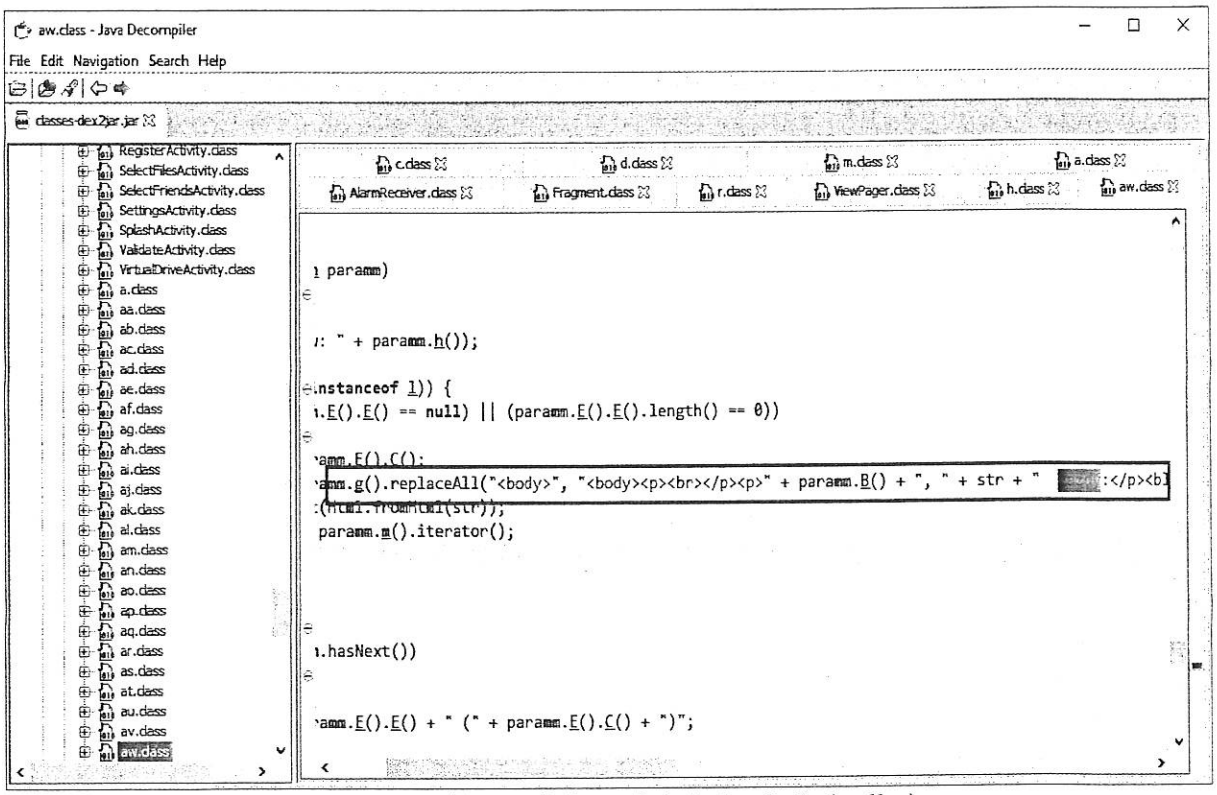
Şekil 2.10 ("**Sesli Arama**" ibaresinin bulunduğu kodlar)



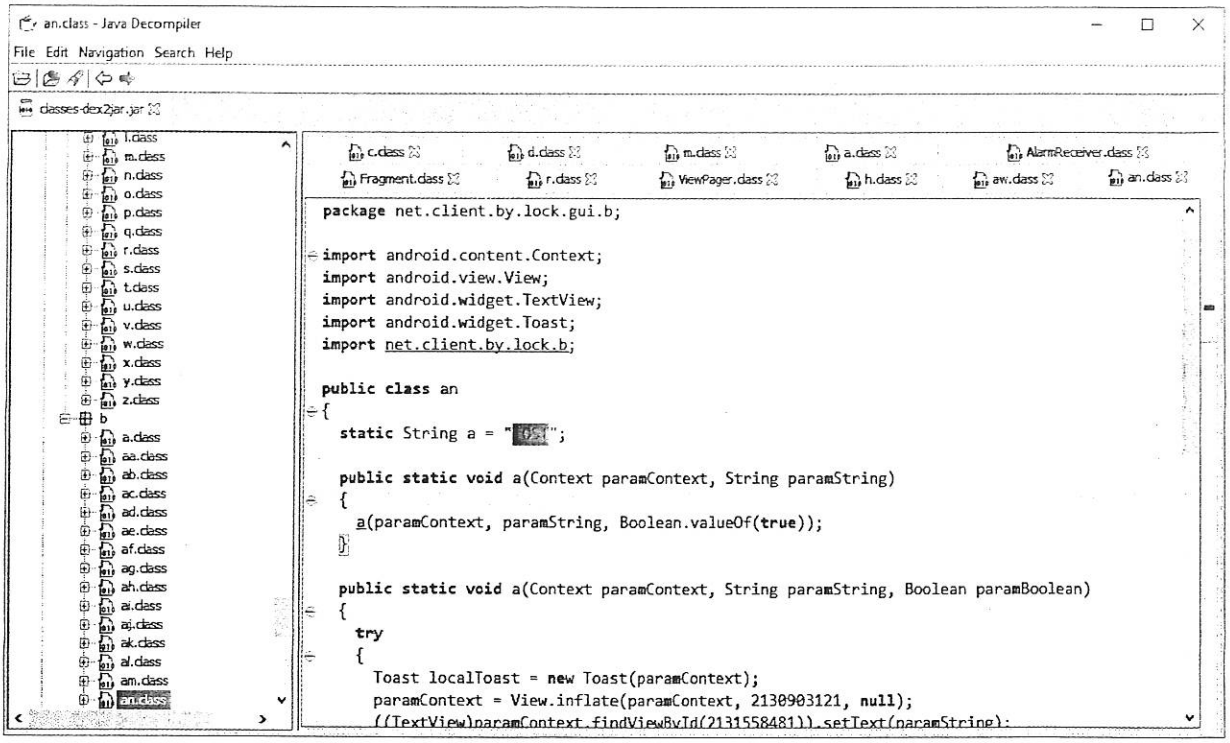
Şekil 2.11 ("**Dosya**" ibaresinin bulunduğu kodlar)



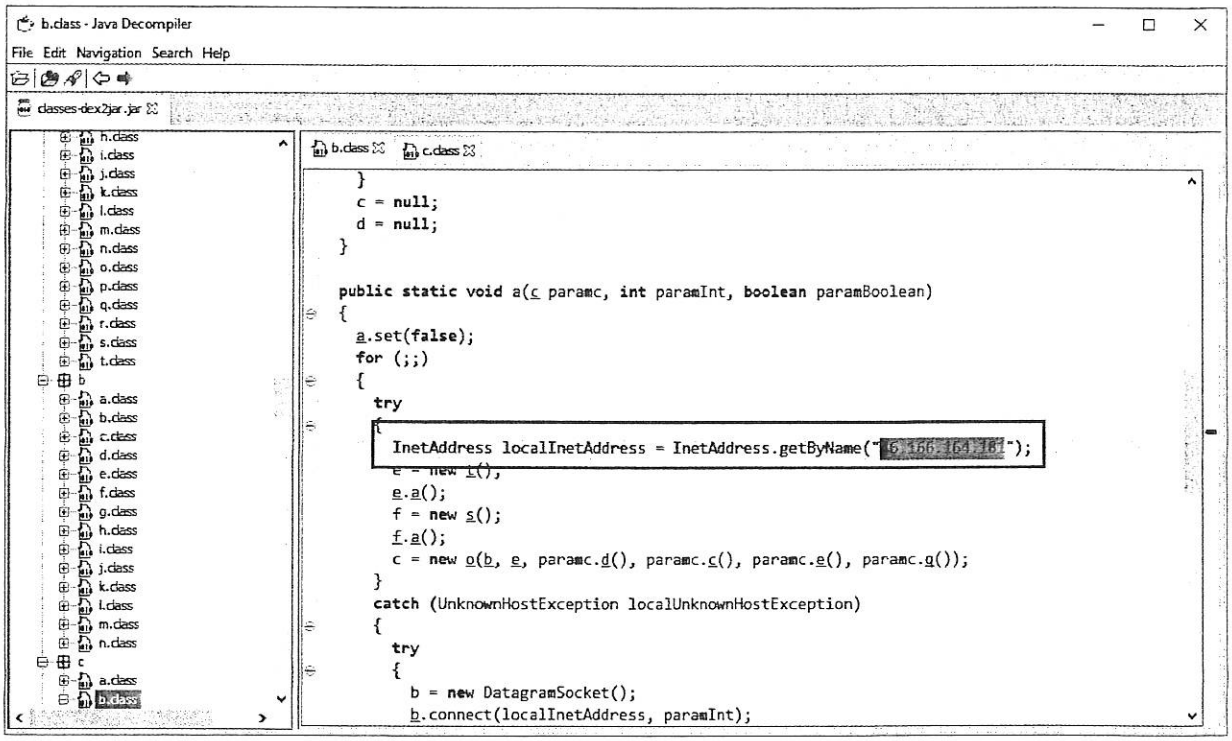
Şekil 2.12 ("**Posta**" ibaresinin bulunduğu kodlar)



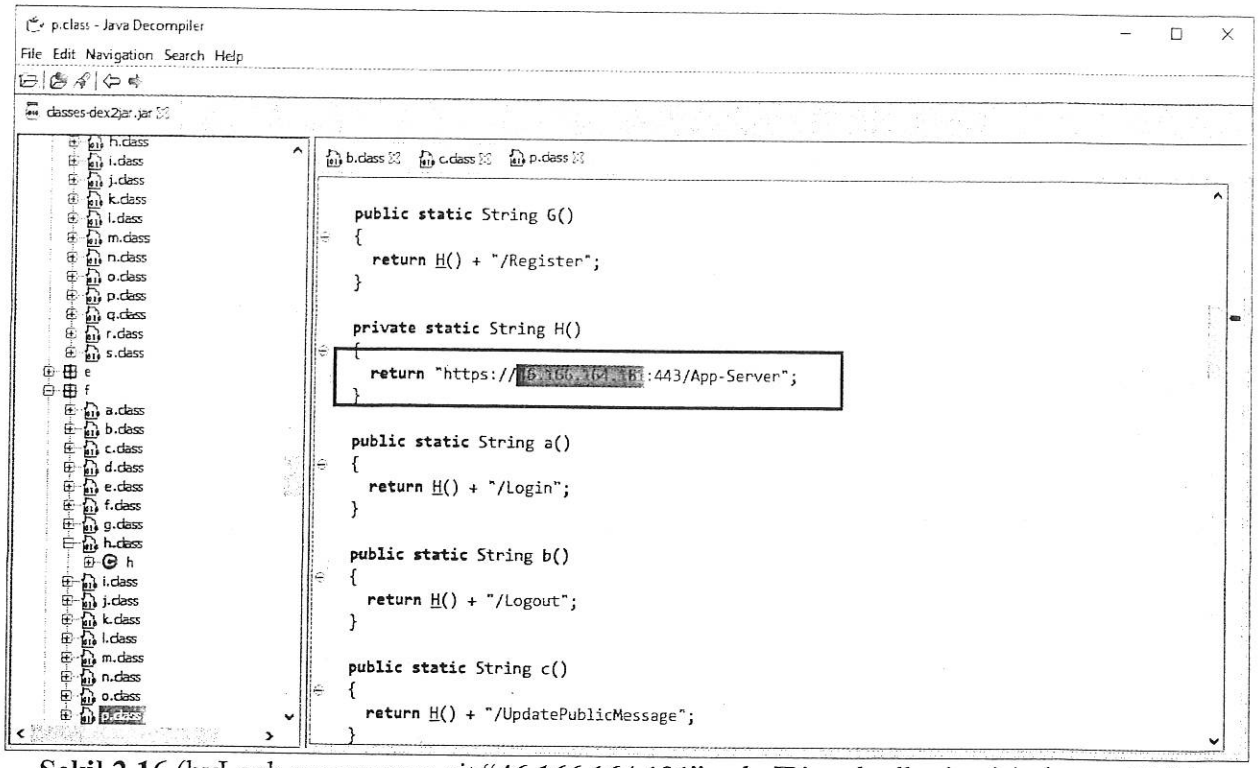
Şekil 2.13 ("**yazdı**" ibaresinin bulunduğu kodlar)



Şekil 2.14 ("**TOST**" ibaresinin bulunduğu kodlar)

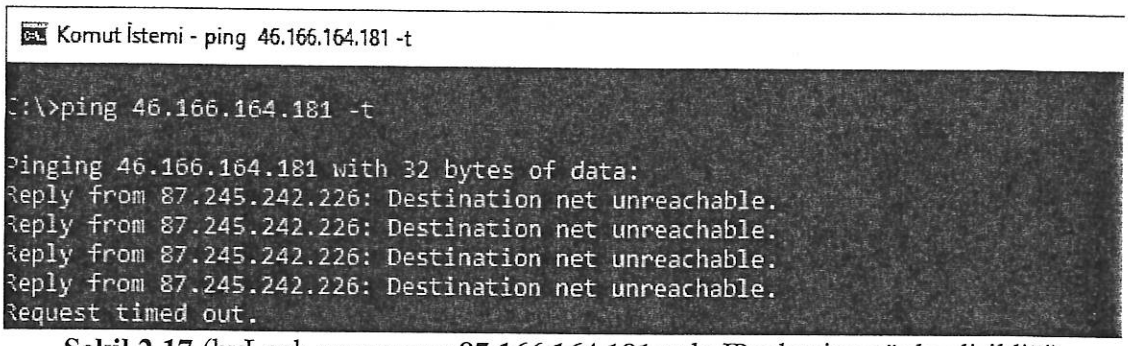


Şekil 2.15 (byLock sunucusuna ait "**46.166.164.181**" nolu IP'nın kodlar içerisinde yer aldığı)



Şekil 2.16 (byLock sunucusuna ait "**46.166.164.181**" nolu IP'nın kodlar içerisinde yer aldığı)

byLock sunucusuna ait **46.166.164.181** nolu IP adresinin App-Server (Uygulama Sunucusu) olarak kullanıldığı, 443 nolu PORT üzerinden sunucuya erişim sağlandığı görülmektedir. https://46.166.164.181:443/App-Server 'a erişim sağlanmak istenildiğinde sunucusunun kapalı olduğu ve uygulamanın sunucuya erişim sağlayamadığı görülmüştür.



Şekil 2.17 (byLock sunucunun **87.166.164.181** nolu IP adresine yönlendirildiği)

"byLock" sunucusuna ait uygulama kodları arasında tespit edilen **46.166.164.181** nolu IP adresinin yanıt vermediği, ping atıldığında **87.245.242.226** nolu IP adresine yönlendirdiği, bu IP adresinin de yanıt vermediği görülmüştür. **(Şekil 2.17)**

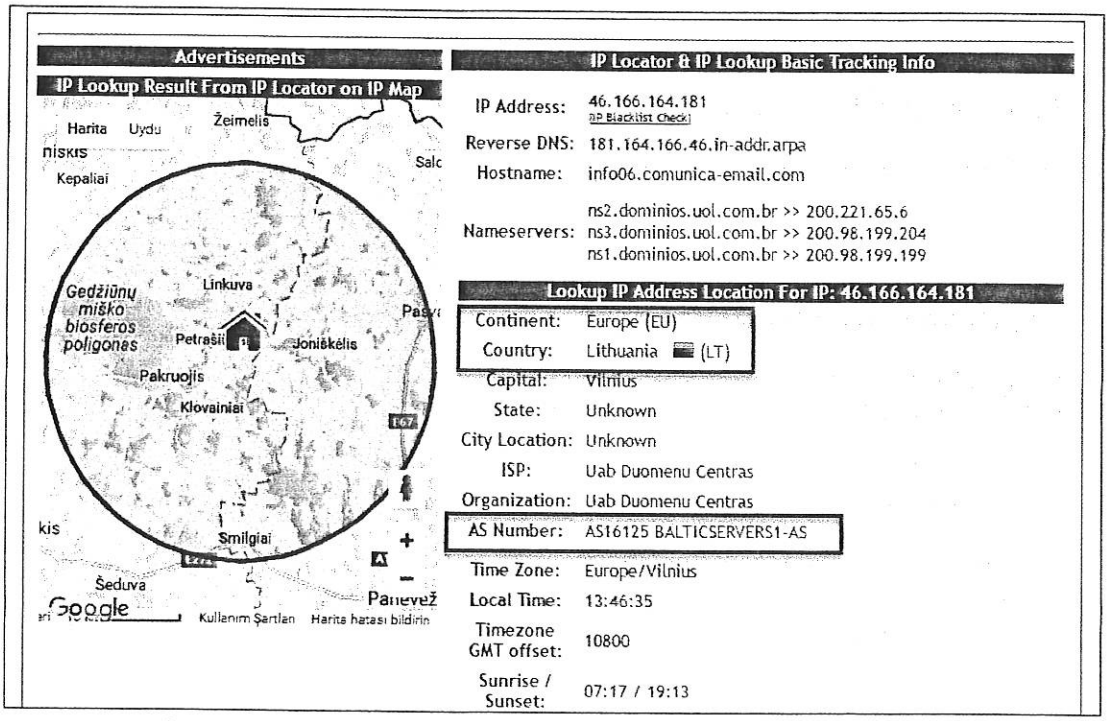
Whois.domaintools.com sitesi üzerinden yapılan sorgulamalarda **46.166.164.176 - 46.166.164.183 Aralığında olan 46.166.164.176, 46.166.164.177, 46.166.164.178, 46.166.164.179, 46.166.164.180, 46.166.164.181, 46.166.164.182 ve 46.166.164.183** nolu IP numaralarının AS16125 BALTICSERVERS1-AS üzerine 29 mayıs 2011 tarihinde kayıt edildiği görülmüştür.

IP Information for 46.166.164.181

IP Location	Lithuania Siauliai Uab Cherry Servers
ASN	AS16125 BALTICSERVERS1-AS , LT (registered Mar 29, 2011)
Resolve Host	hst-46-166-164-181.balticservers.eu
Whois Server	whois.ripe.net
IP Address	46.166.164.181

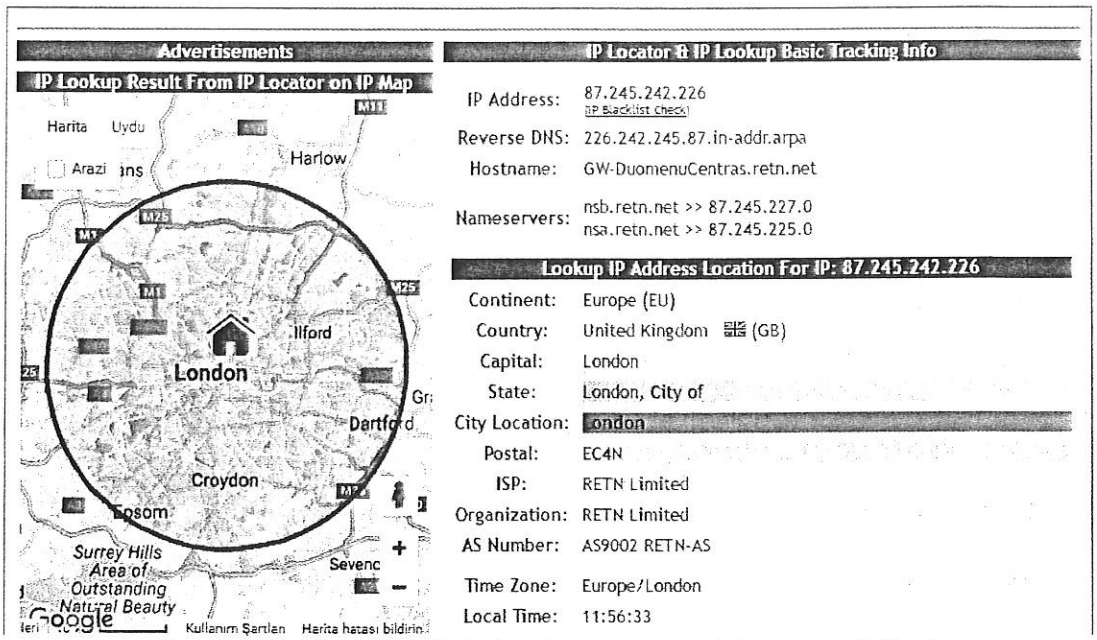
Abuse contact for **'46.166.164.176 - 46.166.164.183'** is ' andreizalop@mail.com

Sunucunun Lokasyon bilgilerine bakıldığında ise Litvanya üzerinden yayın yaptığı internet üzerindeki açık kaynaklardan anlaşılmıştır.



Şekil 2.18 (46.166.164.181 nolu sunucunun lokasyon bilgileri)

Yönlendirme yapılan 87.245.242.226 nolu IP adresinin ise İngiltere kaynaklı IP grubuna ait olduğu ve Lokasyon bilgilerinin Londra olduğu görülmektedir.



Şekil 2.19 (87.166.164.181 nolu sunucunun lokasyon bilgileri)

byLock ile ilgili olarak yapılan araştırmalarda programın **"David Keynes"** isimli bir kişi tarafından yazıldığı, https://bylockapp.wordpress.com/ blog sayfasının ve keynes97209@gmail.com eposta adresinin uygulamayı geliştiren kişiye ait olduğunu çeşitli web sitelerinde referans olarak gösterildiği görülmüştür.

Internet araştırmalarında "David Keynes" ve "byLock" programı ile ilgili uygulamanın yazıldığı ve piyasaya sürüldüğü konusunda **ticari şirket bilgisi veya detaylı şahıs bilgisine ulaşılamamıştır.**

byLock.apk dosyası içerisinde yer alan **BYLOCK.RSA** Sertifika dosyası Windows İşletim Sistemi olan bir bilgisayara yüklenmek suretiyle ayrıntılarına bakıldığında aşağıdaki bilgileri ulaşılmıştır.

Sertifikalar

Verilen	Veren	Süre Sonu	Hedeflenen amaçlar	Kolay Ad
David Keynes	David Keynes	11.08.2041	<Tümü>	<Yok>

Şekil 2.20 (Sertifika Bilgileri)

Alan	Değer
Verilen	David Keynes
Veren	David Keynes
Geçerlilik	**26.03.2014 – 11.08.2041**
Sürüm	V3
Seri No	53 32 9a c2
İmza Algaritması	sha1RSA
İmza karma Algoritması	sha1
Sertifikayı Veren	CN = David Keynes OU = Application CA O = by Lock L = Beaverton S = Oregon C = US
Geçerlilik başlangıcı	26 Mart 2014 Çarşamba 12:15:46
Geçerlilik sonu	11 Ağustos 2041 Pazar 12:15:46
Konu	CN = David Keynes OU = Application CA O = by Lock L = Beaverton S = Oregon C = US
Ortak Anahtar	RSA (2048 Bits) 30 82 01 0a 02 82 01 01 00 9b c3 99 24 5b 14 f2 5b 59 3c ea d0 fd 66 d7 9d db ca 91 92 5a 6c c0 6c 38 33 d9 be 4c 8c 72 14 e4 0f 9f 78 f5 74 14 44 87 fb dc d3 38 31 e7 8d d9 37 19 ff a8 67 6d 9d bb 37 3e 21 42 1d c2 9e b6 c2 37 13 2a 7f cf 3a 0d 51 b8 0e 26 d8 d6 ee cf 4b 57 16 a1 49 40 b7 1a be 33 c3 67 4a 9c 6a d8 af 33 8b 3a 97 1a 1b ff 78 e0 00 7b 0b 39 77 ab 8c 04 17 56 88 62 f8 2a 17 06 95 ea f7 8a 45 64 56 ca 58 a6 e0 1f 3d c9 09 35 6e e5 ff ac 67 fc 0f ae 25 9f 44 1c b4 6b ca 99 2c a7 b7 ad 42 b1 e3 54 be 60 d6 a7 b7 df 44 25 ff d4 8d 55 f2 a4 20 71 b3 ce 19 77 9c de d7 8f 26 53 64 aa 42 0a 0b 5e dc 4e ab ba 22 df 21 5f b3 f0 a2 76 a1 d6 e1 07 50 60 f8 48 c9 5f 6e 9f ca 31 da 70 d6 93 c2 8c 1b 68 4b f5 b7 cd cd db 10 b5 ec 58 54 1a af 83 90 af 97 f1 5e e0 09 11 da c6 47 2e 4d 02 03 01 00 01
Ortak Anahtar Parametreleri	05 00
Parmak izi algoritması	Sha1
Parmak izi	c8 57 8b 48 2f 69 aa 0c 1f 17 09 fb 81 5b 64 66 ea 41 bc 96

Şekil 2.21 (Sertifika Detayları)

Sertifika bilgilerinin 26 Mart 2014 Çarşamba 12:15:46'da kullanılmaya başlanıldığı, 11 Ağustos 2041 Pazar 12:15:46'ya kadar geçerli olduğu tespit edilmiştir.

Bylock programına ait *.apk dosyasının kaynak kod incelemelerinde programın AES256 algoritmasına göre şifreleme yaptığına ilişkin kodlara rastlanılmış olup, örnek kodlar aşağıda sunulmuştur.

----------net.client.by.lock ----------

a/c.class

```
public static c a(net.client.by.lock.d.c paramc, byte[] paramArrayOfByte1, byte[]
paramArrayOfByte2)
  {
    paramc = new c(paramc, true, "CALLING", false);
    paramc.a(new SecretKeySpec(paramArrayOfByte1, "AES"));
```

```
    paramc.a(new IvParameterSpec(paramArrayOfByte2));
    return paramc;
  }
  public void a(IvParameterSpec paramIvParameterSpec)
  {
    this.b = paramIvParameterSpec;
  }
  public void a(SecretKeySpec paramSecretKeySpec)
  {
    this.a = paramSecretKeySpec;
  }
   public void a(byte[] paramArrayOfByte)
  {
    this.n = paramArrayOfByte;
  }
```

Şekil 2.22 (AES Kullanımına ilişkin örnek Kodlar Uygulama içerisinden yapılan aramalarda AES algoritmasına göre şifreleme işlemi yapıldığı)

```
//************************ SecretKeySpec ************************

public k(DatagramSocket paramDatagramSocket, s params, SecretKeySpec
paramSecretKeySpec, IvParameterSpec paramIvParameterSpec, byte[]
paramArrayOfByte)
  {
    this.a = paramDatagramSocket;
    this.b = params;
    this.c = paramSecretKeySpec;
    this.d = paramIvParameterSpec;
    this.e = paramArrayOfByte;
    this.g = new Speex();     //**************** speex is a free codec for free speech
http://www.speex.org/
    this.h = 3212;
    this.i = 0;
    this.j = 0;
    this.l = new i();
    try
    {
      this.m = MessageDigest.getInstance("MD5");
      this.n = Cipher.getInstance("AES/CBC/PKCS5Padding");
      this.n.init(2, paramSecretKeySpec, paramIvParameterSpec);
      this.f = new l(this);
      return;
    }
```

Şekil 2.23 (Uygulama tarafında veri sıkıştırma işlemi için Speex Codec kullanıldığını gösterir bölüm)

```
********** package net.client.by.lock.d;**********
.....
private void c()
  {
   if ((this.b == null) || (this.d == null) || (this.c == null)) {}
   try
   {
    this.b = KeyFactory.getInstance("RSA");
    this.d = Signature.getInstance("SHA1withRSA");
    this.c = Cipher.getInstance("RSA/ECB/OAEPWithSHA-1AndMGF1Padding");
    return;
   }
   catch (NoSuchAlgorithmException localNoSuchAlgorithmException)
   {
    j.a("Error in initializing byLockKeyPair", localNoSuchAlgorithmException);
    this.b = null;
    this.d = null;
    this.c = null;
    return;
   }
   catch (NoSuchPaddingException localNoSuchPaddingException)
   {
    j.a("Error in initializing byLockKeyPair", localNoSuchPaddingException);
    this.b = null;
    this.d = null;
    this.c = null;
   }
.....
```

Şekil 2.24 (RSA/ECB/OAEPWithSHA-1AndMGF1Padding)

```
    this.m = MessageDigest.getInstance("MD5");
    this.n = Cipher.getInstance("AES/CBC/PKCS5Padding");
    this.n.init(1, paramSecretKeySpec, paramIvParameterSpec,
net.client.by.lock.d.r.i().a());
    this.o = new j();
    this.l = new r(this);
    return;
```

Şekil 2.25 (RSA/ECB/OAEPWithSHA-1AndMGF1Padding)

```
**********package net.client.by.lock.d;**********
import java.math.BigInteger;
import java.security.InvalidAlgorithmParameterException;
import java.security.InvalidKeyException;
import java.security.KeyFactory;
import java.security.KeyPair;
import java.security.KeyPairGenerator;
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;
import java.security.PrivateKey;
import java.security.Signature;
import java.security.SignatureException;
import java.security.spec.InvalidKeySpecException;
import java.security.spec.RSAKeyGenParameterSpec;
import java.security.spec.RSAPrivateKeySpec;
import java.util.ArrayList;
import java.util.Iterator;
import javax.crypto.BadPaddingException;
import javax.crypto.Cipher;
import javax.crypto.IllegalBlockSizeException;
import javax.crypto.NoSuchPaddingException;
import javax.crypto.spec.IvParameterSpec;
import javax.crypto.spec.SecretKeySpec;
import net.client.by.lock.f.j;

public final class q
  extends f
{
  private PrivateKey e;
  private byte[] f;

  public q()
  {
    try
    {
      Object localObject = KeyPairGenerator.getInstance("RSA");
      ((KeyPairGenerator)localObject).initialize(new RSAKeyGenParameterSpec(2048, RSAKeyGenParameterSpec.F4), r.i().a());
      localObject = ((KeyPairGenerator)localObject).genKeyPair();
      this.e = ((KeyPair)localObject).getPrivate();
      this.a = ((KeyPair)localObject).getPublic();
      c();
      e();
      return;
    }
    catch (NoSuchAlgorithmException localNoSuchAlgorithmException)
    {
      for (;;)
      {
        j.a("SelfKey", localNoSuchAlgorithmException);
      }
    }
    catch (InvalidAlgorithmParameterException localInvalidAlgorithmParameterException)
    {
      for (;;)
      {
        j.a("SelfKey", localInvalidAlgorithmParameterException);
      }
```

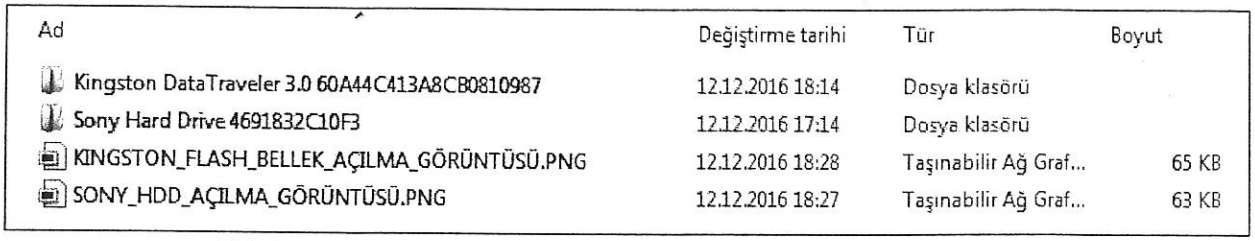
Şekil 2.26 (AES256 ile anahtarın üretimi)

Kaynak kodların incelenmesi sonucunda bir birleri ile haberleşen iki uçtaki kullanıcı arasındaki verilerin **2048** bitlik asimetrik **"RSA/ECB/OAEPWithSHA-1AndMGF1Padding"** kriptografik algoritması kullanılarak şifrelendiği, kullanılan algoritmanın açık anahtarlı/asimetrik şifreleme algoritması olduğu, biri gizli olmak üzere iki anahtar kullanılarak şifreleme yaptığı, açık anahtar kullanılarak şifrelenen verilerin gizli anahtar kullanılarak çözümlenebildiği görülmüştür.

3. Seagate Z9A4E51C seri nolu 1TB Sabit Diskin İncelenmesi

Ankara C.Başsavcılığının 13/12/2016 tarih ve 2016/104109 soruşturma nolu dosyası kapsamında 13/12/2016 tarihli teslim tesellüm tutanağı ile tarafımıza "byLock" Programına ait verilerin içerisinde bulunduğu Seagate marka 1 adet **Z9A4E51C** seri nolu 1TB kapasiteli sabit disk teslim edilmiştir.

İncelenen diskin image diski olduğu ve disk yazma korumalı olarak bilgisayar bağlandığında ekran görüntüleri bulunan içeriklerin yer aldığı görülmüştür.



Ad	Değiştirme tarihi	Tür	Boyut
Kingston DataTraveler 3.0 60A44C413A8CB0810987	12.12.2016 18:14	Dosya klasörü	
Sony Hard Drive 4691832C10F3	12.12.2016 17:14	Dosya klasörü	
KINGSTON_FLASH_BELLEK_AÇILMA_GÖRÜNTÜSÜ.PNG	12.12.2016 18:28	Taşınabilir Ağ Graf...	65 KB
SONY_HDD_AÇILMA_GÖRÜNTÜSÜ.PNG	12.12.2016 18:27	Taşınabilir Ağ Graf...	63 KB

Şekil 3.1 (Seagate marka Z9A4E51C seri nolu sabit disk içeriği)

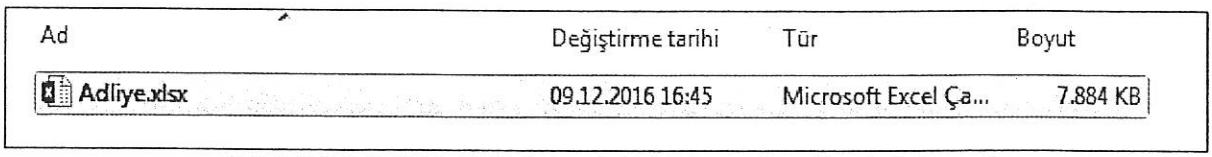
3.1. Kingston DataTraveler 3.0 60A44C413A8CB0810987

Imaj Dosya Adı	KINGSTON_MARKA_8GB_KAPASITELI_FLASH_BELLEK
Olay Numarası	ACBS_2016_104109
Imaj Oluşturan	SSM
Imaj Notu	MILLI_ISTIHBARAT_TESKILATI_TARAFINDAN_GONDERILEN_KINGSTON_MARKA_DATATRAVELER_MODEL_DTIG48GB04570700A00LF5V0S7455704_IBNARELI_SARI_BEYAZ_RENKLI_FLASH_BELLEK
Toplam Kapasite	7.751.073.792 Bytes (7,2 GB)
Toplam Sektör Sayısı	15.138.816
Md5 Hash	bfb9b514143ee745da5b275cb50919d6
SHA1 Hash	0e40b1613fb9af46b8b5359a70418e949351a632

Partitions/Bölüm

Name	Id	Type	Start Sector	Total Sectors	Size
	0c	FAT32X	8.064	15.130.752	7,2 GB

3.1.1.YAPILAN İNCELEME SONUCU:



Ad	Değiştirme tarihi	Tür	Boyut
Adliye.xlsx	09.12.2016 16:45	Microsoft Excel Ça...	7.884 KB

Şekil 3.1.1.1 (Usb Bellek içerisindeki yer alan (1 adet) dosya)

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.

3.2. SONY_MARKA_bBW3DEK69121056_IBARELI_HARICI_HDD olarak etiketlenen disk

MATERYALE AİT ÖZELLİKLER

İmaj Dosya Adı	SONY_MARKA_bBW3DEK69121056_IBARELI_HARICI_HDD
Dosya Numarası	ACBS_2016_104109
İmaj Alan	SSM
İmaj Notu	MILLI_ISTIHBARAT_TESKILATI_TARAFINDAN_GONDERILEN_SONY_MARKA_bBW3DEK69121056_IBARELI_HARICI_HDD
MD5	32e17a8f36e426f4af83cce32a0f5087
SHA1	8a58d21e32ccc80f873446e8cea046fcf9aec4f1
Total Size	1.000.204.883.968 Bytes (931,5 GB)
Total Sectors	1.953.525.164

Partitions/Bölüm

Name	Id	Type	Start Sector	Total Sectors	Size
	07	NTFS	2.048	1.953.519.616	931,5 GB

3.2.1. YAPILAN İNCELEME SONUCU

Sony Hard Drive 4691832C10F3 olarak etiketlenen diske ait Imaj verilerinin doğrulaması yapılmış, HASH değerlerinin doğrulandığı, Diskin içerisinde ibdata1 ve md5checksum.txt olarak iki adet dosyanın yer aldığı görülmüştür.

Ad	Değiştirme tarihi	Tür	Boyut
md5checksum.txt	26.10.2016 15:19	Metin Belgesi	1 KB
ibdata1	26.10.2016 15:13	Dosya	113.789.140 KB

Şekil 3.2.1.1 (Sony Hard Drive 4691832C10F3 seri nolu Harddisk İçeriği)

Dosya Adı	**ibdata1**
Mantıksal Boyutu	116.520.079.360
Son Erişim Tarihi	26/10/2016 15:18:49
Son Yazma Tarihi	26/10/2016 15:13:22
MD5	1173d7a09195cf0274ce24f0d69ede96
SHA1	e8cae63538d7a20ddfcb4c4ec49e552f4342e75c
Dosya Yolu	SONY_MARKA_bBW3DEK69121056_IBARELI_HARICI_HDD\media/e5a15e1f-844d-4b49-a747-c64ae055ead1\ibdata1

Şekil 3.2.1.2 (Sony Hard Drive 4691832C10F3 seri nolu Harddisk İçeriği)

Disk içerisinde yer alan **md5checksum.txt** içerisinde yer alan hash değerinin doğrulaması yapılmış ve aynı değere ulaşılmıştır.

3.2.1.1."ibdata1"

"ibdata1" MySQL veri tabanına ait kayıtların yer aldığı veri tabanı dosyasıdır. Şayet innodb türü engine (motor) tercih edildiğinde *.ibd uzantılı dosya oluşturulmaktadır. **MySQL** veri tabanının yapılandırma dosyasında **"innodb_file_per_table"** parametresi eklenmemiş ise veri tabanı dosyası tek bir **ibdata1** dosyası olarak büyük bir dosya olacaktır. "**innodb_file_per_table**" parametresi eklenmesi halinde veri tabanı ***.ibd** uzantılı veri tabanı dosyalarının oluşacaktır.

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.

```
mysql> select * from SYS_TABLES;
+---------------------------------+----+------------+------+--------+---------+--------------+-------+
| NAME                            | ID | N_COLS     | TYPE | MIX_ID | MIX_LEN | CLUSTER_NAME | SPACE |
+---------------------------------+----+------------+------+--------+---------+--------------+-------+
| appDb/action                    | 13 |          7 |    1 |      0 |       0 |              |     0 |
| appDb/attachment                | 41 |          7 |    1 |      0 |       0 |              |     0 |
| appDb/call_history              | 15 |          7 |    1 |      0 |       0 |              |     0 |
| appDb/chat                      | 40 |          7 |    1 |      0 |       0 |              |     0 |
| appDb/client                    | 17 |          6 |    1 |      0 |       0 |              |     0 |
| appDb/exception                 | 18 |          5 |    1 |      0 |       0 |              |     0 |
| appDb/file                      | 43 |          3 |    1 |      0 |       0 |              |     0 |
| appDb/file_transfer             | 42 |         10 |    1 |      0 |       0 |              |     0 |
| appDb/group_member              | 21 |          2 |    1 |      0 |       0 |              |     0 |
| appDb/log                       | 45 |         10 |    1 |      0 |       0 |              |     0 |
| appDb/mail                      | 44 |          9 |    1 |      0 |       0 |              |     0 |
| appDb/roster                    | 24 |          4 |    1 |      0 |       0 |              |     0 |
| appDb/setting                   | 25 |          2 |    1 |      0 |       0 |              |     0 |
| appDb/user                      | 26 |         10 |    1 |      0 |       0 |              |     0 |
| appDb/user_group                | 27 |          3 |    1 |      0 |       0 |              |     0 |
```

SYS_FOREIGN	11	-2147483644	1	0	0		0
SYS_FOREIGN_COLS	12	-2147483644	1	0	0		0
wordpress/wp_commentmeta	33	4	1	0	0		0
wordpress/wp_comments	34	15	1	0	0		0
wordpress/wp_links	35	13	1	0	0		0
wordpress/wp_options	36	4	1	0	0		0
wordpress/wp_postmeta	37	4	1	0	0		0
wordpress/wp_posts	38	23	1	0	0		0
wordpress/wp_terms	30	4	1	0	0		0
wordpress/wp_term_relationships	32	3	1	0	0		0
wordpress/wp_term_taxonomy	31	6	1	0	0		0
wordpress/wp_usermeta	29	4	1	0	0		0
wordpress/wp_users	28	10	1	0	0		0

28 rows in set (0,00 sec)

Şekil 3.2.1.1.1 (ByLock uygulamasına ait appDb içerisindeki tablo)

"appDb" olarak adlandırılan veri tabanının **"byLock"** programına ait verileri içerdiği anlaşılmış, tablolar aşağıda listelenmiştir.

Tables_in_appDb
action
attachment
call_history
chat
client
exception
file
file_transfer
group_member
log
mail
roster
setting
user
user_group

5 rows in set (0,00 sec)

Şekil 3.2.1.1.2 (ByLock uygulamasına ait appDb içerisindeki tablo)

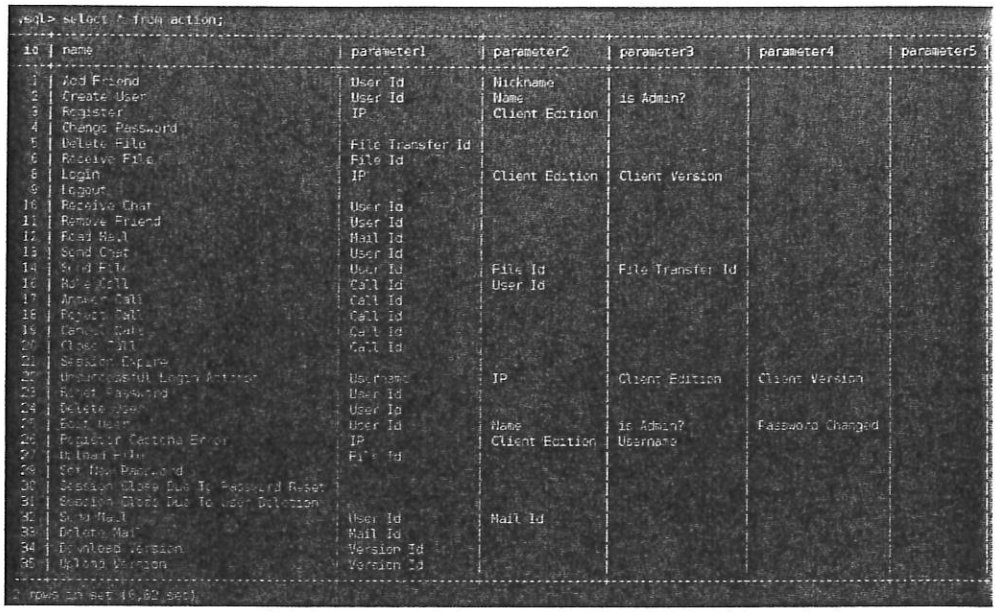
"appDb" isimli veri tabanı içerisinde **(15)** adet tablonun yer aldığı görülmüş, tablo içerikleri ve veri yapısı aşağıda detaylı olarak açıklanmıştır.

a) Action Tablosu

Field	Type	Null	Key	Default	Extra
id	int(11)	NO	PRI	NULL	
name	varchar(64)	NO		NULL	
parameter1	varchar(64)	NO		NULL	
parameter2	varchar(64)	NO		NULL	
parameter3	varchar(64)	NO		NULL	
parameter4	varchar(64)	NO		NULL	
parameter5	varchar(64)	NO		NULL	

Şekil 3.2.1.1.3 (Action tablo yapısı)

"action" tablosu içerisinde toplam (32) adet kayıt bulunduğu ve "**log**" tablosundaki oluşan uygulama loglarının **"action"** tablosundaki parametrelere göre oluştuğu anlaşılmıştır.



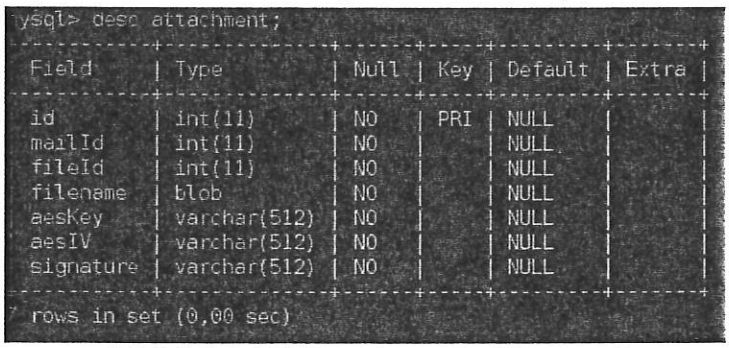
id	name	parameter1	parameter2	parameter3	parameter4	parameter5
1	Add Friend	User Id	Nickname			
2	Create User	User Id	Name	is Admin?		
3	Register	IP	Client Edition			
4	Change Password					
5	Delete File	File Transfer Id				
6	Receive File	File Id				
8	Login	IP	Client Edition	Client Version		
9	Logout					
10	Receive Chat	User Id				
11	Remove Friend	User Id				
12	Read Mail	Mail Id				
13	Send Chat	User Id				
14	Send File	User Id	File Id	File Transfer Id		
16	Make Call	Call Id	User Id			
17	Answer Call	Call Id				
18	Reject Call	Call Id				
19	Cancel Call	Call Id				
20	Close Call	Call Id				
21	Session Expire					
22	Unsuccessful Login Attempt	Username	IP	Client Edition	Client Version	
23	Reset Password	User Id				
24	Delete User	User Id				
25	Edit User	User Id	Name	is Admin?	Password Changed	
26	Register Captcha Error	IP	Client Edition	Username		
27	Upload File	File Id				
29	Set New Password					
30	Session Close Due To Password Reset					
31	Session Close Due To User Direction					
32	Send Mail	User Id	Mail Id			
33	Delete Mail	Mail Id				
34	Download Version	Version Id				
35	Upload Version	Version Id				

2 rows in set (0,02 sec)

Şekil 3.2.1.1.4 (**"action"** tablosundaki kayıtlar)

Tablo içerisindeki kayıtlar incelendiğinde Örneğin **"log"** tablosunda **"1"** değeri görüldüğünde bir kullanıcının arkadaş eklediği, **"2"** değeri görüldüğünde Yeni bir kullanıcının oluştuğu, **"24"** değeri görüldüğünde kullanıcının silindiği, **"25"** değeri görüldüğünde kullanıcı bilgilerinde düzenleme yapıldığı anlaşılmış, içerikler **Şekil 39'da** sunulmuştur.

b) Attachment Tablosu



```
mysql> desc attachment;
+-----------+--------------+------+-----+---------+-------+
| Field     | Type         | Null | Key | Default | Extra |
+-----------+--------------+------+-----+---------+-------+
| id        | int(11)      | NO   | PRI | NULL    |       |
| mailId    | int(11)      | NO   |     | NULL    |       |
| fileId    | int(11)      | NO   |     | NULL    |       |
| filename  | blob         | NO   |     | NULL    |       |
| aesKey    | varchar(512) | NO   |     | NULL    |       |
| aesIV     | varchar(512) | NO   |     | NULL    |       |
| signature | varchar(512) | NO   |     | NULL    |       |
+-----------+--------------+------+-----+---------+-------+
7 rows in set (0,00 sec)
```

Şekil 3.2.1.1.5 ("attachment" tablo yapısı)

"attachment" tablosu mail gönderilmesi sırasında bir dosyanın gönderilmesi durumunda kullanıldığı, tablo içerisinde "**mail**" tablosuna ait **mailId**, file tablosuna ait **fileId, filename** gibi bilgilerin de yer aldığı görülmüştür.

c) call_history Tablosu

```
mysql> desc call_history;
+-------------+-------------+------+-----+-------------------+-----------------------------+
| Field       | Type        | Null | Key | Default           | Extra                       |
+-------------+-------------+------+-----+-------------------+-----------------------------+
| id          | varchar(32) | NO   | PRI | NULL              |                             |
| callerId    | int(11)     | NO   |     | NULL              |                             |
| calleeId    | int(11)     | NO   |     | NULL              |                             |
| callTime    | timestamp   | NO   |     | CURRENT_TIMESTAMP | on update CURRENT_TIMESTAMP |
| result      | varchar(16) | NO   |     | NULL              |                             |
| duration    | int(11)     | YES  |     | NULL              |                             |
| trafficSize | int(11)     | YES  |     | NULL              |                             |
+-------------+-------------+------+-----+-------------------+-----------------------------+
7 rows in set (0,29 sec)
```

Şekil 3.2.1.1.6 (call_history tablo yapısı)

Call_history tablosu ile uygulama içerisindeki sesli aramalara ilişkin kayıtların tutulduğu görülmektedir. Tablo yapısı incelendiğinde **"id"** yapılan aramalar ile ilgili tablo id numarası, **"callerId"** arama yapan kullanıcının User tablosundaki ID numarasını, **"celleeId"** aranan kullanıcının User tablosundaki ID numarasını, **"callTime"** arama zamanını **"result"** arama durumunu, **"duration"** arama süresini, **"trafficSize"** oluşan trafiğin data cinsinden boyutunu ifade etmektedir.

Call_history tablosu içerisinde toplam **1.219.016** adet kayıt bulunduğu tespit edilmiş olup, örnek kayıtlar aşağıda sunulmuştur.

```
mysql> select * from call_history limit 5;
+----------------------------------+----------+----------+---------------------+----------+----------+-------------+
| id                               | callerId | calleeId | callTime            | result   | duration | trafficSize |
+----------------------------------+----------+----------+---------------------+----------+----------+-------------+
| 0000005386619f3a40ca5a0ff4be4455b |   243283 |   364572 | 2015-08-18 12:33:22 | MISSED   |        0 |           0 |
| 0000124eef341c0641a66b62b02019a3 |   339117 |   218617 | 2015-02-08 18:08:11 | CANCELED |        0 |           0 |
| 000036245abf87b9fab0e5eeac511ef0 |   259668 |   105932 | 2015-10-21 12:35:35 | CANCELED |        0 |           0 |
| 00003b684f0df76499299638bba841b6 |    80719 |   192454 | 2015-04-29 05:34:03 | REJECTED |        0 |           0 |
| 00003be9e5fb8addeaf6faf2c29a6597 |   332314 |    56443 | 2015-03-28 13:20:56 | REJECTED |        0 |           0 |
+----------------------------------+----------+----------+---------------------+----------+----------+-------------+
5 rows in set (0,00 sec)
```

Şekil 3.2.1.1.7 (call_history tablosu örnek veriler)

d) chat Tablosu

```
mysql> desc chat;
+--------------+--------------+------+-----+---------------------+-----------------------------+
| Field        | Type         | Null | Key | Default             | Extra                       |
+--------------+--------------+------+-----+---------------------+-----------------------------+
| id           | int(11)      | NO   | PRI | NULL                |                             |
| fromUserId   | int(11)      | NO   |     | NULL                |                             |
| toUserId     | int(11)      | NO   |     | NULL                |                             |
| ciphertext   | blob         | NO   |     | NULL                |                             |
| signature    | varchar(512) | NO   |     | NULL                |                             |
| sentTime     | timestamp    | NO   |     | CURRENT_TIMESTAMP   | on update CURRENT_TIMESTAMP |
| receivedTime | timestamp    | NO   |     | 0000-00-00 00:00:00 |                             |
+--------------+--------------+------+-----+---------------------+-----------------------------+
7 rows in set (0,00 sec)
```

Şekil 3.2.1.1.8 (**chat** tablo yapısı)

"chat" tablosu uygulama içerisindeki yazılı iletişim kurulmak için kullanılan bölüm olduğu, chat tablosunda "**fromUserId**" mesajı yazan kişiye ait user tablosundaki ID numarasını, **toUserId**" kendisine mesaj yazılan kişiye ait user tablosundaki ID numarasını, "**ciphertext**" mesaj

içeriğini, "**signature**" imzayı, "**sendtime**" gönderilme zamanını, "**receivedTime**" ise mesajın ulaştığı zamanı gösterdiği görülmüştür. **"chat"** tablosunda **17.169.650** adet kayıt bulunduğu tespit edilmiştir.

e) client Tablosu

```
mysql> desc client;
+-------------+--------------+------+-----+-------------------+-----------------------------+
| Field       | Type         | Null | Key | Default           | Extra                       |
+-------------+--------------+------+-----+-------------------+-----------------------------+
| id          | int(11)      | NO   | PRI | NULL              |                             |
| edition     | varchar(32)  | NO   |     | NULL              |                             |
| version     | varchar(32)  | NO   |     | NULL              |                             |
| buildNumber | int(11)      | NO   |     | NULL              |                             |
| path        | varchar(256) | NO   |     | NULL              |                             |
| uploadedOn  | timestamp    | NO   |     | CURRENT_TIMESTAMP | on update CURRENT_TIMESTAMP |
+-------------+--------------+------+-----+-------------------+-----------------------------+
6 rows in set (0,94 sec)
```

Şekil 3.2.1.1.9 (client tablo yapısı)

client tablosunda uygulamanın versiyonları ile ilgili alanların olduğu değerlendirilmiş ancak tablo içerisinde herhangi bir kayıt tespit edilememiştir.

f) exception Tablosu

```
mysql> desc exception;
+-------------+-------------+------+-----+---------+-------+
| Field       | Type        | Null | Key | Default | Extra |
+-------------+-------------+------+-----+---------+-------+
| id          | varchar(64) | NO   | PRI | NULL    |       |
| edition     | varchar(16) | NO   |     | NULL    |       |
| buildNumber | int(11)     | NO   |     | NULL    |       |
| count       | int(11)     | NO   |     | NULL    |       |
| content     | blob        | NO   |     | NULL    |       |
+-------------+-------------+------+-----+---------+-------+
5 rows in set (0,22 sec)
```

Şekil 3.2.1.1.10 (exception tablo yapısı)

Exception tablosu uygulama kullanılırken oluşan hatalara ait kayıtların yazıldığı tablo olduğu değerlendirilmiştir. Tablo içerisinde **445** adet kayıt bulunduğu tespit edilmiştir.

g) file Tablosu

```
mysql> desc file;
+-------+---------------+------+-----+---------+-------+
| Field | Type          | Null | Key | Default | Extra |
+-------+---------------+------+-----+---------+-------+
| id    | int(11)       | NO   | PRI | NULL    |       |
| path  | varchar(1024) | NO   |     | NULL    |       |
| size  | int(11)       | NO   |     | NULL    |       |
+-------+---------------+------+-----+---------+-------+
3 rows in set (1,02 sec)
```

Şekil 3.2.1.1.11 (file tablo yapısı)

"file" tablosu bylock uygulamasındaki dosya yüklenmesi için kullanılan tablo olduğu değerlendirilmiştir. Tablonun alan adlarına bakıldığında **"id"** tablo içerisinde primary (birincil)

index değerini, "**path**" dosyanın uygulama sunucu üzerindeki yerini, "**size**" ise dosyanın boyutunu göstermektedir.

```
mysql> select * from file limit 5;
+------+-----------------------------------------------------------------------+---------+
| id   | path                                                                  | size    |
+------+-----------------------------------------------------------------------+---------+
|  406 | /mnt/disk1-2tb/bL-files/2015/12/11/15/01/1268801304386516-3925        | 2150384 |
|  463 | /mnt/disk1-2tb/bL-files/2015/12/11/16/03/1271623968487787-8999        | 5038240 |
| 1709 | /mnt/disk1-2tb/bL-files/2015/12/12/22/02/1377745561692340-3101        | 1685232 |
| 1944 | /mnt/disk1-2tb/bL-files/2015/12/13/06/01/1408871234468102-8674        | 1314832 |
| 2002 | /mnt/disk1-2tb/bL-files/2015/12/13/10/03/1422503594622638-5462        | 2001120 |
+------+-----------------------------------------------------------------------+---------+
5 rows in set (0,57 sec)
```

Şekil Şekil 3.2.1.1.12 ("**file**" tablosu alan adları ve özellikleri)

"**file**" tablosunda **38.546** adet kayıt bulunduğu, tablo içerisindeki kayıtlara göre kullanıcılar tarafından yüklenen dosyaların sunucu üzerindeki "**disk1-2tb**" olarak adlandırılan alanda depolandığı anlaşılmaktadır.

h) "file_transfer" Tablosu

```
mysql> desc file_transfer;
+--------------+-----------+------+-----+---------------------+-----------------------------+
| Field        | Type      | Null | Key | Default             | Extra                       |
+--------------+-----------+------+-----+---------------------+-----------------------------+
| id           | int(11)   | NO   | PRI | NULL                |                             |
| fromUserId   | int(11)   | NO   |     | NULL                |                             |
| toUserId     | int(11)   | NO   |     | NULL                |                             |
| fileId       | int(11)   | NO   |     | NULL                |                             |
| name         | blob      | NO   |     | NULL                |                             |
| aesKey       | varchar(512) | NO |     | NULL                |                             |
| aesIV        | varchar(512) | NO |     | NULL                |                             |
| signature    | varchar(512) | NO |     | NULL                |                             |
| sentTime     | timestamp | NO   |     | CURRENT_TIMESTAMP   | on update CURRENT_TIMESTAMP |
| receivedTime | timestamp | NO   |     | 0000-00-00 00:00:00 |                             |
+--------------+-----------+------+-----+---------------------+-----------------------------+
10 rows in set (0,01 sec)
```

Şekil 3.2.1.1.13 ("**file_transfer**" tablo yapısı)

"**file_transfer**" tablosu bylock uygulamasını kullananlar tarafından file tablosuna yüklenen dosyaların kendi aralarında göndermelerini sağladıkları tablo olduğu değerlendirilmektedir. Tablo yapısına göre "**fromUserId**" dosyayı gönderen kişiye ait user tablosundaki ID numarasını, "**toUserId**" dosya gönderilen kişiye ait user tablosundaki ID numarasını, "**fileId**" file tablosundaki ID numarasını **"name"** dosya adını, **"aesKey"** ve **"aesIV"** anahtarları, "**signature**" imzayı, "**sendtime**" gönderilme zamanını, "**receivedTime**" ise mesajın ulaştığı zamanı gösterdiği görülmüştür.

i) "group_member" Tablosu

```
mysql> desc group_member;
+---------+---------+------+-----+---------+-------+
| Field   | Type    | Null | Key | Default | Extra |
+---------+---------+------+-----+---------+-------+
| groupId | int(11) | NO   | PRI | NULL    |       |
| userId  | int(11) | NO   | PRI | NULL    |       |
+---------+---------+------+-----+---------+-------+
2 rows in set (0,00 sec)
```

Şekil 3.2.1.1.14 (group_member tablo yapısı)

"group_member" tablosunda **"groupId"** ve **"userId"** olmak üzere iki adet alan bulunduğu, **"groupId"** bylock içiresinde oluşturulan grupların ifade ettiği, **"userId"** ise oluşturulan gruplara eklenen kullanıcıları ifade ettiği anlaşılmıştır.

```
mysql> select * from group_member limit 10;
+---------+--------+
| groupId | userId |
+---------+--------+
|       1 |     28 |
|       1 |     63 |
|       1 |     98 |
|       1 |    528 |
|       1 |    566 |
|       1 |    662 |
|       2 |     84 |
|       2 |    100 |
|       2 |    159 |
|       2 |    161 |
+---------+--------+
10 rows in set (0,00 sec)
```

Şekil 3.2.1.1.15 (**"group_member"** tablosu örnek veriler)

"group_member" tablosuna ait **(10)** adet kayıt listelenmiştir. Kayıtlara bakıldığında **groupId** numarası "1" olan grupta 6 adet kullanıcının yer aldığı görülmüştür. Yapılan çalışmalarda **group_member** tablosu içerisinde **208.424** adet kayıt bulunduğu, bir kullanıcının birden fazla gruba dâhil olduğu, groupId numarası (1) olan grupta userId numarası 28, 63, 98, 528, 566, 662 ID nolu kullanıcıların yer aldığı görülmüştür.

j) **"log" Tablosu**

```
mysql> desc log;
+------------+--------------+------+-----+-------------------+-----------------------------+
| Field      | Type         | Null | Key | Default           | Extra                       |
+------------+--------------+------+-----+-------------------+-----------------------------+
| id         | int(11)      | NO   | PRI | NULL              |                             |
| userId     | int(11)      | NO   |     | NULL              |                             |
| actionId   | int(11)      | NO   |     | NULL              |                             |
| sessionId  | varchar(128) | NO   |     | NULL              |                             |
| eventTime  | timestamp    | NO   |     | CURRENT_TIMESTAMP | on update CURRENT_TIMESTAMP |
| parameter1 | varchar(64)  | YES  |     | NULL              |                             |
| parameter2 | varchar(64)  | YES  |     | NULL              |                             |
| parameter3 | varchar(64)  | YES  |     | NULL              |                             |
| parameter4 | varchar(64)  | YES  |     | NULL              |                             |
| parameter5 | varchar(64)  | YES  |     | NULL              |                             |
+------------+--------------+------+-----+-------------------+-----------------------------+
8 rows in set (0,24 sec)
```

Şekil 3.2.1.1.16 (**"log"** tablo yapısı)

"**log**" tablosunda "**user**" tablosunda kayıtlı kullanıcıların program içerisindeki işlemlere ait uygulama loğlarının yer aldığı, "**log**" tablosundaki kayıtların "**action**" tablosunda belirtilen görülmüş, tablo içerisinde **138.174.968** adet kaydın bulunduğu tespit edilmiş, örnek kayıtlar aşağıda sunulmuştur.

id	userId	actionId	sessionId	eventTime	parameter1	parameter2	parameter3	parameter4	parameter5
1	112695	8	f64ca60dt3b50a7f32f02e9078c05b42	2015-12-11 00:27:49	63.141.217.112	ios	1.3-1	NULL	NULL
2	268729	8	9ef6a66b559c26d8bedfe769522c187e	2015-12-11 00:27:49	109.237.27.253	android	0.8-24	NULL	NULL
3	466035	8	ad1103f9e70d7487f0de72c363aa9e3b	2015-12-11 00:27:50	46.165.250.77	android	0.8-24	NULL	NULL
4	62583	8	1f1fc6443b99da21f965cd1fe6163f5b	2015-12-11 00:27:50	95.90.236.57	android	0.8-24	NULL	NULL
5	414878	8	ae3b1682683b687a69ec0e40fc3a3304	2015-12-11 00:27:50	41.237.216.23	android	0.8-24	NULL	NULL

rows in set (0.00 sec)

Şekil 3.2.1.1.17 (log örnek veriler)

"**log**" tablosu içerisinde yer alan kayıtlara göre "ios" ve "andoid" cihazlardan gelen bir kısım log kayıtlarının bulunduğu görülmüştür.

k) mail tablosu

```
mysql> desc mail;
+---------------+--------------+------+-----+---------------------+-----------------------------+
| Field         | Type         | Null | Key | Default             | Extra                       |
+---------------+--------------+------+-----+---------------------+-----------------------------+
| id            | int(11)      | NO   | PRI | NULL                |                             |
| fromUserId    | int(11)      | NO   |     | NULL                |                             |
| toUserId      | int(11)      | NO   |     | NULL                |                             |
| otherRecipients | varchar(512) | YES |     | NULL                |                             |
| subject       | varchar(512) | YES  |     | NULL                |                             |
| body          | blob         | YES  |     | NULL                |                             |
| signature     | varchar(512) | NO   |     | NULL                |                             |
| sentTime      | timestamp    | NO   |     | CURRENT_TIMESTAMP   | on update CURRENT_TIMESTAMP |
| receivedTime  | timestamp    | NO   |     | 0000-00-00 00:00:00 |                             |
+---------------+--------------+------+-----+---------------------+-----------------------------+
rows in set (0,01 sec)
```

Şekil 3.2.1.1.18 ("mail" tablo yapısı)

"**mail**" tablosu "**chat**" tablosu ile benzerlik göstermektedir. "**mail**" tablosunda "**fromUserId(gönderen), toUserId(alan), otherRecipients(diğer alıcılar), subject (konu), body (mesaj metni)**" gibi alanların bulunduğu görülmektedir. Mail tablosunda **3.758.351** adet kayıt bulunduğu tespit edilmiştir.

l) roster tablosu

```
mysql> desc roster;
+------------+-------------+------+-----+---------+-------+
| Field      | Type        | Null | Key | Default | Extra |
+------------+-------------+------+-----+---------+-------+
| id         | int(11)     | NO   | PRI | NULL    |       |
| fromUserId | int(11)     | NO   |     | NULL    |       |
| toUserId   | int(11)     | NO   |     | NULL    |       |
| nickname   | varchar(32) | NO   |     | NULL    |       |
+------------+-------------+------+-----+---------+-------+
4 rows in set (0,01 sec)
```

Şekil 3.2.1.1.19 (roster tablosu alan adları ve özellikleri)

"roster" tablosu bylock uygulaması içerisinde programı kullanın kişinin kendi rehberini oluşturması için kullandığı bölüm olduğu görülmüştür. Bir kullanıcı bylock üzerindeki bir kişiyi kendi listesine kayıt ettiğinde bu şahsa isim verebildiği görülmektedir.

```
mysql> select * from roster limit 10;
+----+------------+----------+----------+
| id | fromUserId | toUserId | nickname |
+----+------------+----------+----------+
|  3 |          5 |        4 | alex     |
|  4 |          4 |        5 |          |
|  5 |          6 |        5 |          |
|  6 |          5 |        6 |          |
|  7 |         19 |       24 | foruk    |
|  8 |         24 |       19 |          |
| 12 |         29 |       27 |          |
| 13 |         27 |       29 |          |
| 30 |         34 |       28 | Orhan A  |
| 31 |         28 |       34 | 2B.Yunus |
+----+------------+----------+----------+
10 rows in set (0,00 sec)
```

Şekil 3.2.1.1.20 ("roster" tablosu örnek veriler)

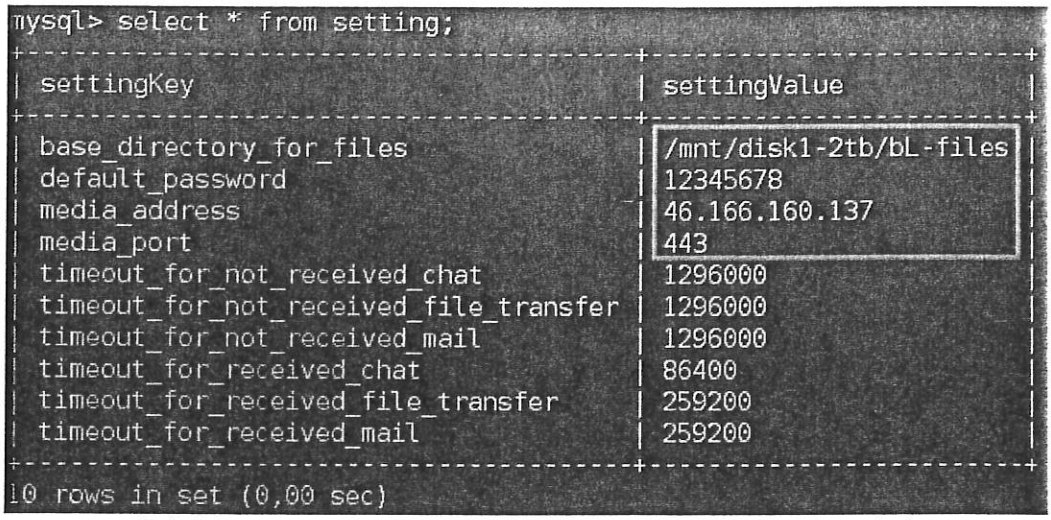
Örnek kayıtlar incelendiğinde fromUserId=3 (User tablosundaki ID numarası 3 olan kullanıcı), toUserId=4 (User tablosundaki ID numarası=4 olan kullanıcıyı) "alex" ismi ile kayıt altına aldığını göstermektedir. Yapılan çalışmalarda **"roster"** tablosuna ait **1.705.659** adet kayıt tespit edilmiştir.

m) setting Tablosu

```
mysql> desc setting;
+--------------+--------------+------+-----+---------+-------+
| Field        | Type         | Null | Key | Default | Extra |
+--------------+--------------+------+-----+---------+-------+
| settingKey   | varchar(64)  | NO   | PRI | NULL    |       |
| settingValue | varchar(1024)| NO   |     | NULL    |       |
+--------------+--------------+------+-----+---------+-------+
2 rows in set (0,03 sec)
```

Şekil 3.2.1.1.21 (setting tablo yapısı)

"setting" (ayarlar) tablosu üzerinde (2) adet alan bulunduğu görülmüştür. setting tablosundaki kayıtlar incelendiğinde aşağıdaki sonuçlar elde edilmiştir.



```
mysql> select * from setting;
+---------------------------------------+-------------------------+
| settingKey                            | settingValue            |
+---------------------------------------+-------------------------+
| base_directory_for_files              | /mnt/disk1-2tb/bL-files |
| default_password                      | 12345678                |
| media_address                         | 46.166.160.137          |
| media_port                            | 443                     |
| timeout_for_not_received_chat         | 1296000                 |
| timeout_for_not_received_file_transfer | 1296000                |
| timeout_for_not_received_mail         | 1296000                 |
| timeout_for_received_chat             | 86400                   |
| timeout_for_received_file_transfer    | 259200                  |
| timeout_for_received_mail             | 259200                  |
+---------------------------------------+-------------------------+
10 rows in set (0,00 sec)
```

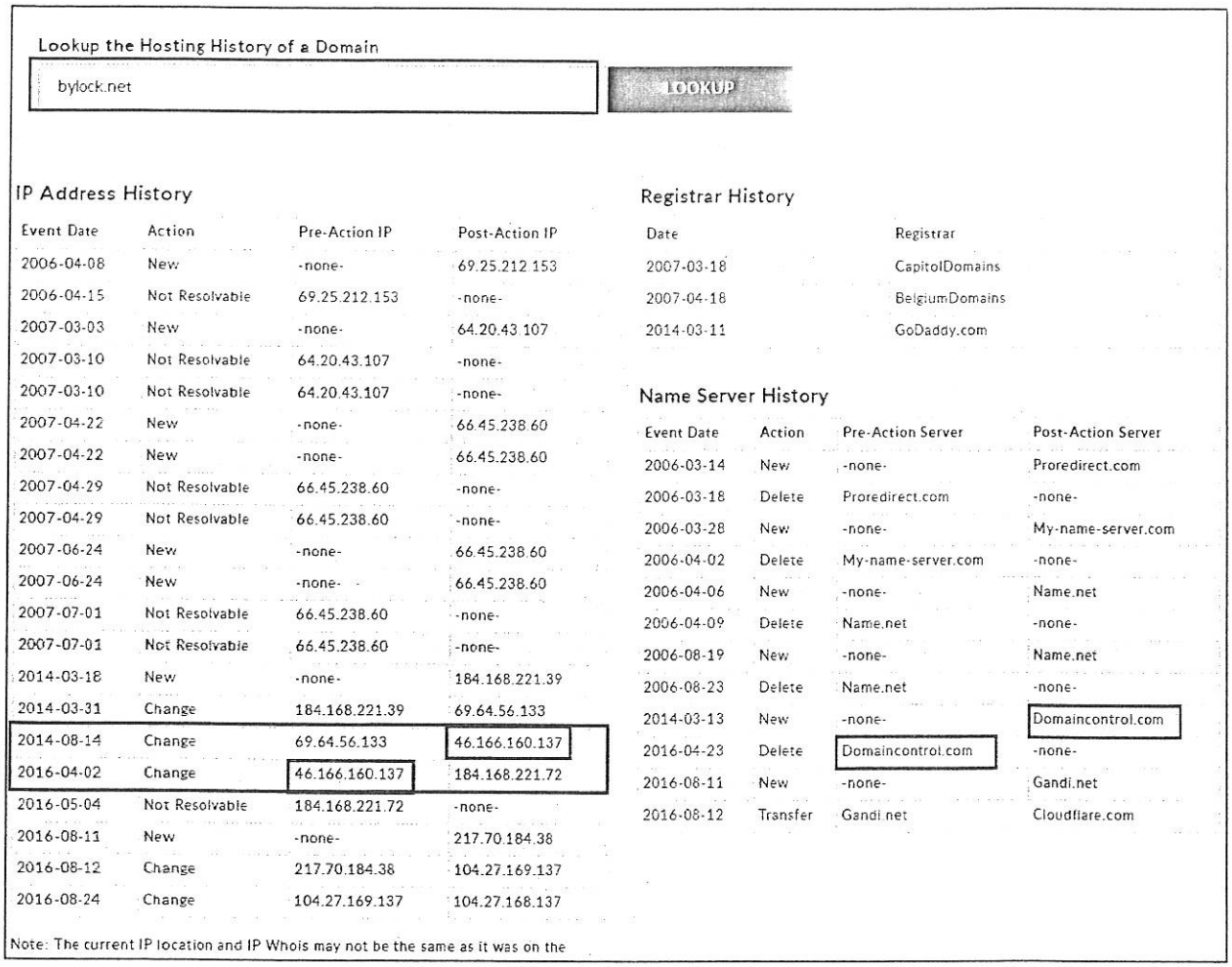
Şekil 3.2.1.1.22 (**"setting"** tablosu içeriğinde yer alan kayıtlar)

"setting" (ayarlar) tablosu içerisinde (10) adet kayıt bulunduğu tesit edilmiş, kayıtlar incelendiğinde bylock programına ait kullanım esnasındaki çeşitli ayarların burada yer aldığı görülmüştür.

Base_directory_for_files	Yüklenen dosyaların aktarılacağı sunucu üzerinde dosya yolunun burada gösterildiği
default_password	Ön tanımlı şifrenin **12345678** olarak belirlendiği
media_adres **media_port**	Media adres olarak **46.166.160.137** nolu IP adresinin **ve 443** nolu PORT bilgisinin belirtildiği görülmüştür

Şekil 3.2.1.1.23 (setting tablosunda yer alan kayıtlar)

46.166.160.137 nolu IP adresi ile ilgili olarak Internet üzerindeki açık kaynaklar (www.whois.domaintools.com) kullanılmak suretiyle yapılan araştırmalarda **14/08/2014** tarihinden itibaren **"bylock.net"** tarafından kullanılmaya başlanarak **02/04/2016** tarihine kadar kullanıldığı tespit edilmiştir. (Şekil 58)



Lookup the Hosting History of a Domain

bylock.net

LOOKUP

IP Address History

Event Date	Action	Pre-Action IP	Post-Action IP
2006-04-08	New	-none-	69.25.212.153
2006-04-15	Not Resolvable	69.25.212.153	-none-
2007-03-03	New	-none-	64.20.43.107
2007-03-10	Not Resolvable	64.20.43.107	-none-
2007-03-10	Not Resolvable	64.20.43.107	-none-
2007-04-22	New	-none-	66.45.238.60
2007-04-22	New	-none-	66.45.238.60
2007-04-29	Not Resolvable	66.45.238.60	-none-
2007-04-29	Not Resolvable	66.45.238.60	-none-
2007-06-24	New	-none-	66.45.238.60
2007-06-24	New	-none-	66.45.238.60
2007-07-01	Not Resolvable	66.45.238.60	-none-
2007-07-01	Not Resolvable	66.45.238.60	-none-
2014-03-18	New	-none-	184.168.221.39
2014-03-31	Change	184.168.221.39	69.64.56.133
2014-08-14	Change	69.64.56.133	46.166.160.137
2016-04-02	Change	46.166.160.137	184.168.221.72
2016-05-04	Not Resolvable	184.168.221.72	-none-
2016-08-11	New	-none-	217.70.184.38
2016-08-12	Change	217.70.184.38	104.27.169.137
2016-08-24	Change	104.27.169.137	104.27.168.137

Note: The current IP location and IP Whois may not be the same as it was on the

Registrar History

Date	Registrar
2007-03-18	CapitolDomains
2007-04-18	BelgiumDomains
2014-03-11	GoDaddy.com

Name Server History

Event Date	Action	Pre-Action Server	Post-Action Server
2006-03-14	New	-none-	Proredirect.com
2006-03-18	Delete	Proredirect.com	-none-
2006-03-28	New	-none-	My-name-server.com
2006-04-02	Delete	My-name-server.com	-none-
2006-04-06	New	-none-	Name.net
2006-04-09	Delete	Name.net	-none-
2006-08-19	New	-none-	Name.net
2006-08-23	Delete	Name.net	-none-
2014-03-13	New	-none-	Domaincontrol.com
2016-04-23	Delete	Domaincontrol.com	-none-
2016-08-11	New	-none-	Gandi.net
2016-08-12	Transfer	Gandi.net	Cloudflare.com

Şekil 3.2.1.1.24 (46.166.160.137 nolu IP verileri)

"setting" tablosunda gönderilen **mail, chat ve dosya** transferlerinde zaman aşımı sürelerinin de kontrol edildiği görülmüştür. Burada **"chat", "file transfer" ve "mail"** gönderilmesi halinde ulaştığında ve ulaşmadığındaki zaman aşımı süresinin belirlendiği tespit edilmiştir.

timeout_for_not_received_chat	1296000 (360 saat) 15 Gün
timeout_for_not_received_file_transfer	1296000 (360 saat)15 Gün
timeout_for_not_received_mail	1296000 (360 saat) 15 Gün
timeout_for_received_chat	86400 (24 Saat) 1 gün
timeout_for_received_file_transfer	259200 (72 Saat) 3 Gün
timeout_for_received_mail	259200 (72 Saat) 3 Gün

Şekil 3.2.1.1.25 (Zaman aşımı süreleri)

n) user Tablosu

```
ysql> mysql> desc user;
+-----------------+-------------+------+-----+---------------------+-----------------------------+
| Field           | Type        | Null | Key | Default             | Extra                       |
+-----------------+-------------+------+-----+---------------------+-----------------------------+
| id              | int(11)     | NO   | PRI | NULL                |                             |
| username        | varchar(32) | NO   |     | NULL                |                             |
| psw             | varchar(32) | NO   |     | NULL                |                             |
| admin           | int(11)     | NO   |     | NULL                |                             |
| publicMessage   | varchar(64) | YES  |     | NULL                |                             |
| privateExponent | varchar(512)| YES  |     | NULL                |                             |
| modulus         | varchar(512)| YES  |     | NULL                |                             |
| name            | varchar(32) | YES  |     | NULL                |                             |
| creationTime    | timestamp   | NO   |     | CURRENT_TIMESTAMP   | on update CURRENT_TIMESTAMP |
| lastOnlineTime  | timestamp   | NO   |     | 0000-00-00 00:00:00 |                             |
+-----------------+-------------+------+-----+---------------------+-----------------------------+
0 rows in set (0,00 sec)
```

Şekil 3.2.1.1.26 (user tablo yapısı)

"user" tablosunda **"id"** bylock içerisinde yer alan "UserId" no, kullanıcı adı (username), psw (md5 kriptolu olarak şifre), kullanıcı durumu admin veya user olarak, (program içerisinde 3 adet admin kullanıcısının yer aldığı diğer kullanıcıların standart user olarak görüldüğü), oluşturulma tarihi, son online tarihi gibi bilgilerin bulunduğu görülmüştür.

Yapılan inceleme sonucunda toplam **246.206** adet kayıt bilgisine ulaşılmıştır.

o) user_group tablosu

```
ysql> desc user_group;
+---------+--------------+------+-----+---------+-------+
| Field   | Type         | Null | Key | Default | Extra |
+---------+--------------+------+-----+---------+-------+
| id      | int(11)      | NO   | PRI | NULL    |       |
| userId  | int(11)      | NO   |     | NULL    |       |
| name    | varchar(128) | NO   |     | NULL    |       |
+---------+--------------+------+-----+---------+-------+
3 rows in set (0,00 sec)
```

Şekil 3.2.1.1.27 (user_group tablo yapısı)

Tablo yapısı incelendiğinde **"id"** user_grup tablosunun tablo birincil index değerini, **"userId"** tablo içerisindeki oluşturulan grubun hangi kullanıcı tarafından oluşturulduğu, **"name"** ise gruba verilen ismi ifade etmektedir. User_group tablosuna ait örnek kayıtlar incelendiğinde hangi kullanıcının (userId) hangi grubu oluşturduğu ve gruba verdiği isim görülmektedir.

```
ariaDB [appDb]> select * from user_group limit 10;
+----+--------+-----------------+
| id | userId | name            |
+----+--------+-----------------+
|  1 |     42 | 1               |
|  2 |     42 | 2               |
|  3 |    204 | vira bismillah  |
|  6 |     28 | 1.HY            |
| 12 |     42 | temsil          |
| 16 |    362 | devre           |
| 17 |    362 | karakol         |
| 18 |    362 | idb             |
| 19 |    362 | es dost akraba  |
| 23 |     42 | YY              |
+----+--------+-----------------+
10 rows in set (0.00 sec)
```

Şekil 3.2.1.1.28 (user_group tablosuna ait örnek veriler)

Yapılan inceleme sonucunda toplam 32.880 adet kayıt bilgisine ulaşılmıştır.

"**ibdata1**" dosyası içerisindeki ham veriler üzerinde **Linux Centos ve Debian** işletim sistemleri içerisinde "**Percona Data Recovery (percona-data-recovery-tool-for-innodb)** ve **TwinDB Data Recovery (undrop-for-innodb)**" araçları kullanılmak suretiyle kurtarma işlemleri yapılarak elde edilen verilere ait kayıt sayıları **Şekil 3.2.1.1.29** içerisinde sunulmuştur.

SN	TABLO ADI	KAYIT SAYILARI
1	action	32
2	attachment	11.827
3	call_history	1.219.016
4	chat	17.169.650
5	client	0
6	exception	445
7	file	38.546
8	file_transfer	9546
9	group_member	208.424
10	log	138.174.968
11	mail	3.758.351
12	roster	1.705.659
13	setting	10
14	user	246.206
15	user_group	32.880

Şekil 3.2.1.1.29 (Veri Tabanı üzerinde yapılan kurtarma işlemi soncunda elde edilen veriler)

Kayıtlar EK-2'du sunulan (1) adet Sandisk marka B161025474V SDCZ71-064G USB Bellek içerisine aktarılmış, USB Bellek Windows Bitlocker ile şifrelenerek, şifresi ayrı bir kapalı zarf içinde haricen sunulmuştur.

4. SONUÇ VE DEĞERLENDİRME

ByLock programı ile ilgili Internet üzerindeki açık kaynaklardan ve programın Android Uygulama Paket (*.apk) dosyası üzerinde araştırma ve incelemeler yapılmıştır.

Programın genel yapısı itibariyle yazılı mesaj gönderimi ve alımı, sesli arama, mail gönderimi, program içerisinden fotoğraf çekilmesi, gönderilmesi veya cep telefonu içerisindeki bir dosyanın programa eklenerek diğer kullanıcılara gönderilmesi, grup oluşturulması ve grup içi mesajlaşma gibi özeliklerinin mevcut olduğu görülmüştür

Programın ekran görüntülerine göre kayıt işlemi (**Register**) sonrasında birde onaylama (**Validate**) işlemi yapıldığını, onaylama işlemi sırasında **kullanıcı kimliğinin** belirlenmesi veya

kayıtlı kullanıcının kimliğini ortaya çıkartabilecek türden bir doğrulama sisteminin olmadığı, cep telefonu (SMS - KOD) veya e-posta üzerinden yapılan bir doğrulama yapısının olmadığı görülmüştür.

Programın Android Uygulama Paket (*.apk) dosyasına ait Java Decompiler uygulaması ile kaynak kodlar incelendiğinde verinin kriptolanması için AES256 algoritmasının kullanıldığı, verinin doğrulanması için ise (özet almak için) MD5 Hash algoritmasının kullanıldığı görülmüştür. Ayrıca aktarılan verinin sıkıştırılması için ise SPEEX codec algoritmasının kullanıldığı tespit edilmiştir.

"byLock" programını, uygulamayı kullanan kişi veya kişiler arasında, kendi kimliklerini belirleyici herhangi bir ibareyi kullanmaksızın (Telefon Numarası, IMEI numarası, doğrulama kodu e-posta vb.) Internet erişimi olan mobil cihazlarda kriptolu olarak kişiden kişiye veya grup içerisinde yazışma **(chat)** yapılmasına, dosya alınıp gönderilmesine, e-posta alınıp gönderilmesine ve sesli arama **(voip)** yapılmasına olanak sağlayan mobil iletişim aracı olduğu değerlendirilmiştir.

"byLock" veri tabanına ait raporun ilgili bölümlerinde detayları yazılı olan veri tabanı dosyası (ibdata1) incelenmiştir. MySQL INNODB (engine) motoru kullanılarak işletilen bu veri tabanının ilk incelemesinde yapısının bozuk olduğu görülmüştür. Veri tabanı dosyasının içerdiği nesnelere erişmek için kurtarma (recover) işlemine tabi tutulmuştur. Çeşitli yöntemler kullanılarak elde edilen veriler tablo 63'de liste halinde sunulmuş olup, MySQL dump *.sql dosyası olarak EK-2'de sunulan (1) adet Sandisk marka B161025474V SDCZ71-064G ibareli USB Bellek içerisinde Hash değerleri ile aktarılarak rapor ekinde sunulmuştur.

Arz olunur. 12/07/2017

BİLİRKİŞİ HEYETİ

Yrd. Doç. Dr. Baha ŞEN
Öğretim Üyesi

Rafet ÖNGÖÇMEN
Adli Bilişim Uzmanı

EKLER:
EK-1 Seagate Marka Z9A4E51C seri nolu 1TB IMAJ diski (1 adet)
EK-2 Sandisk marka B161025474V SDCZ71-064G (1 adet)
EK-3 Dosya Hash Listesi (1) Sayfa

Ankara C.Başsavcılığı Soruşturma No: 2016/104109

Sandisk marka B161025474V SDCZ71-064G USB Bellek içerisine aktarılan dosya listesi ve dosya hash değerleri

Filename	MD5	SHA1	SHA-256
action_export.sql	2523a35d361dca7fe186dc159c87e197	f02d62e4bbb707b984b3bd884cc8d5020d6b27c5	dfb9d85b0a8c9e4fec2272fbe643cffd4b2cc81a590bf84c407a5dd398122a08
attachment_export.sql	cc5f99f246b99d31172dd58f61ce6087	fef32fd5fa036b92c5c6167c68ee131fbd83cbd1	ff55d399d9e99df2fea9ee2378f17eefd49a63967f2e442a91a73e39ded16c3a
call_history_export.sql	16e6b02327a81bed9a567b7f0a3a5ba0	687ce53e387eb10f343a958f32c1b0660034417e	4b926811250455f399483df3776354a00fd4fa201e65628373fa9f6710f149a2
chat_export.sql	aae365413df3b3b947210846b2df09bd	0dfdc180f0db6a7eefbea802076c52e4787dae6b	633837bac28d70e3083005942fdb009d8ac608b0d7226ff1a726d2ed5f4b12eb
client_export.sql	64e2051eed918082b3189fa380a72503	698e46a630a4c35a26e5ebfbe710c9d0cd51a030	4b56538a2d76ffedc992c330d57767fe320169e495a9c7c43af07389d03284d4
exception_export.sql	8691e72f8aec4538db6c562d857ff008	5f181673e187af65e16405676bf2197b06714dc4	cf974704d5e95007ddecd0a93b386a8944b02ef7b7db43a9bb3702fabfa01b49
file_export.sql	958e5a1bdd739097aa29ef03115876ec	bb59b73220782c6ef51ceaa020a71ffc21cb1bb2	e3305b1bb0fa0e0c71d7311034500786dda9e63113c2e17e39ae5a4e08ca8323
file_transfer_export.sql	82d0c8d4a6f13b111b53eac45541daa1	301e2b9842e4746726d81c95a14e4dfffde50e6e	a20df7742a3eae6f16af9ec32a8e9c19d91db7a6dee2d4398fbc340c9d095f86
group_member_export.sql	0db7b0570d90b37e7402f0cce0443c31	d2bd386818965f642cb366e916ed8b1a16d8c8eb	38e58dd316ea5c83c46fc0310cac5e4767cff24b2386f422a251ee4e9b0a43b9
log_export.sql	926c87f7288a2deb5bd8576c6fb56767	d9b55ee976af09e337343bb2a4f5ab7568b1c97f	a716812cc4684528d7f4766eaa95822ae0dfc67f18397906351b3a9676297bfe
mail_export.sql	51131871444038291d5e5fd7a9790ac2	a3518fb882ce7e61f03f14ce52ab45997c311a1f	d5f7a95317272deab7f9749feda89c43c81d9618fd2d44a8e8a5057738ec6f56
roster_export.sql	ff45ccc620c5915124c107d75764a29a	3f312449c021f95aafa9a22f42b6009d71e14b54	59be2847215576121ab4c200300dee962972bbb6f315489eef96c7f024b96238
setting_export.sql	33e7eaf714104e22a7e4445b4a0124c2	67446cc0aee879d71cb4fcdb50e304eac98fa2ba	a85365ef560548ddcdf03814dbbc0f36bd361d0a781039df221bfd1db86a63d8
user_export.sql	7ad8bdafc853dc5702fa0ca78dd5cec7	604329abc978cbc08521377b593a07f1484ecacc	2cdc63afdb4349fce17162bec2527c893953315bfdb5ce8f144b4c307e8ab2a7
user_group_export.sql	e7f919ff15edd6476255b65f7940e6af	138b8e093157c544a2da9000380bc445ac457863	52e9f3dc4902a09f25d92eefd6694396804be24051cef9902a8afa1f3cc902ac