ByLock Uygulaması

Teknik Raporu

İçindekiler

TANIMLAR ve KISALTMALAR

Ağ	:	Birden fazla sayıdaki bilgisayarın birbirlerine bağlanarak haberleşmesini sağlayan iletişim ortamı
Ağ Analizi	:	Bir yazılımın bilgisayar ağları üzerinde gerçekleştirdiği iletişimin incelenmesi ve yorumlanması işlemi
Ağ topolojisi	:	Bir ağı oluşturan bilgisayar ve diğer ağ bileşenlerinin yapılandırmasının tarifi
Alan adı (domain)	:	IP adreslerinin insanların hatırlayabileceği kelime ve harf gruplarıyla eşleştirilerek Internet üzerinde ilgili sunucuya erişim kolaylığı sağlayan adres
Android	:	Akıllı telefon ve tablet bilgisayarlarda çalışmak üzere tasarlanmış, geliştirilmesine Google'ın öncülük ettiği açık kaynaklı işletim sistemi
Asimetrik Şifreleme	:	Gizli ve açık olarak nitelendirilen iki adet anahtar barındıran, açık anahtar ile şifrelenen verinin yalnızca gizli anahtar kullanılarak deşifre edilebileceği şifreleme yöntemlerine verilen ad (Açık Anahtarlı Şifreleme)
Bulanıklaştırma	:	Yazılım üzerinde tersine mühendislik yapılmasını zorlaştırmak için yazılımın kaynak kodundan program haline dönüştürülmesi aşamasında karmaşıklık ilave etme yöntemlerine verilen ad
Censys.io	:	IPv4 adres sistemindeki tüm adresleri günlük olarak tarayıp elde edilen verinin sorgulanmasını sağlayan web arama motoru

DNS	:	Alan adlarının hangi IP adres(ler)ine karşılık geldiğinin sorgulanmasına yarayan çözümleme sistemi
Google Play	:	Android yüklü telefonlara yönelik geliştirilen uygulamaların sunulduğu resmi uygulama marketi
Hata Ayıklama	:	Yazılımları kontrollü bir biçimde adımlara bölerek çalıştırarak barındırdıkları hataları bulmak için kullanılan bir yöntem. Tersine mühendislik çalışmalarında yazılımın hangi işlemleri gerçekleştirdiğini takip etmek ve dolayısıyla işleyiş şekline dair detaylı bilgi elde etmek için kullanılmaktadır
HTTPS Güvenlik Protokolü	:	HTTP protokolü üzerinde uçtan uca şifreleme sağlayan protokol
IOS	:	Akıllı telefon ve tablet bilgisayarlarda çalışmak üzere Apple tarafından geliştirilen işletim sistemi
IP Adresi	:	Internet ağına doğrudan bağlanan her cihaza verilen, numaralardan oluşan benzersiz adres
IPv4	:	1 ile 255 değerleri arasındaki 4 adet sayı ile ifade edilen, teorik olarak 4 milyardan fazla adres sağlayabilen adresleme sistemi
ISS	:	İnternet Servis Sağlayıcı
Kaynak Kod	:	Yazılımın geliştirici tarafından yazıldığı, çalıştırılabilir bir programa dönüşmesi için belirli aşamalardan geçmesi gereken kodlar/yazılar bütünü.
Kriptografik Özet Fonksiyonu	:	Girdi olarak verilen değişken boyuttaki veriyi belirli boyuttaki bir özet değerine dönüştüren

		kriptografik matematiksel fonksiyonlara verilen ad. Bu fonksiyonlar verideki 1 bit değerinin değişmesi gibi küçük farklılıklarda bile özet fonksiyon çıktısında büyük ölçekli farklılıklara sebebiyet verecek ve aynı çıktıyı verecek girdileri bulmanın neredeyse imkânsız olacağı bir şekilde tasarlanır.
Log	:	Bilgisayar sistemlerinde gerçekleştirilen işlemlerin kayıtları
Parola/Anahtar	:	Bir sistemde yetki kontrolü yahut veri şifrelenmesi gibi amaçlar için kullanılmak üzere belirlenen, sembol (harf, sayı, bit vb.) dizisi.
Port	:	İnternet üzerinden bilgisayara ulaştırılan verinin bilgisayarda işleneceği uygulamayı bildiren numara
PTR	:	DNS sunucularında IP adresinden ilgili domain(ler)in sorgulanmasına olanak sağlayan kayıt tipi
ptrarchive.com	:	DNS sunucularındaki PTR kayıtlarını arşivleyerek geçmişe dönük arama yaptıran bir web arama motoru
Simetrik Şifreleme	:	Tek bir anahtar kullanılarak şifrelenen verinin yalnızca tekrar aynı anahtar kullanılarak deşifre edilebileceği şifreleme yöntemlerine verilen ad.
SSL	:	Internet üzerinde güvenli iletişim kurmayı sağlayan bir şifreleme protokolü (Secure Sockets Layer)
SSL Sertifikası	:	SSL protokolünde iletişimin tarafların birbirlerinin kimliğinden emin olması için kullanılan, genellikle iki tarafın ortak olarak güvendiği bir Sertifika Otoritesi tarafından verilmiş olan sertifika

Sunucu (Server)	:	İnternet üzerinde kendisine ulaşan istekleri değerlendiren ve yanıtlayan bilgisayar
Şifre	:	Şifreleme işleminde kullanılan yöntem ve yapıların her birine verilen ad
Şifreleme	:	Bir verinin bir parola/anahtar kullanılarak, yalnızca tekrar aynı parola/anahtar kullanılarak açılabilecek şekilde, matematiksel belirli yöntemler kullanılarak anlamsız hale getirilmesi.
Tersine Mühendislik	:	Bir uygulamanın derlenmiş hâlinden kaynak kodlarını ve/veya uygulamanın işleyiş yordamlarını elde etmeye yönelik olarak gerçekleştirilen teknik çalışma
TLS	:	Eski adı SSL olan bu şifreleme yönteminin adının açılımı dilimizde "Taşıma Katmanı Güvenliği" dir. TLS, İnternet gibi IP üzerine kurulmuş bilgisayar ağlarında iletişim kuran iki uç nokta arasında kriptografik şifreleme yaparak gerçekleştirilen iletişimin uçlar haricinde trafiğin geçtiği noktalarda anlamlandırılabilir bir şekilde olmamasını sağlar. (Transport Layer Security)
UML	:	Bir uygulamanın bileşen yapısını, çalışma şekillerini vb. grafikler şeklinde raporlamakta kullanılan modelleme standartı (Unified Modelling Language)
Uygulama Paketi	:	Bir uygulamayı oluşturan tüm dosyaları barındıran, ilgili işletim sistemi üzerine yüklenebilir durumdaki dosya
virustotal.com	:	Kullanıcılar tarafından kendisine gönderilen dosya, uygulama paketi ve internet adresleri üzerinde

		analizler yapıp sonuçlar üzerinde aramalar yapılmasını sağlayan web arama motoru
VPN	:	Aralarında yerel ağ kurulması imkânı bulunmayan bilgisayarlar arasında Internet üzerinden sanal olarak yerel ağ kurulmasını sağlayan, genellikle şifreleme ile bağlantının güvenliğini sağlayan protokollerin genel adı
whois.domaintools.com	:	İnternetteki alan adları ve IP adresleri üzerinde birçok analiz ve sorgulamalar yapmayı sağlayan web sitesi

1.GİRİŞ

Fetullahçı Terör Örgütü/Paralel Devlet Yapılanması FETÖ/PDY üyelerince, akıllı telefonlara yüklenen kriptolu bir haberleşme aracı olan "ByLock(ByLock: Chat and Talk)" adlı mobil uygulama üzerinden iletişim kurulduğuna dair bilgilerin istihbar olunması üzerine, konuyla alakalı kapsamlı bir çalışma yürütülmüştür. Bu kapsamda, gerek ByLock mobil uygulaması gerekse iletişim kurduğu uygulama sunucuları ayrıntılı teknik çalışmalara tabi tutulmuştur. Bu çalışmalarda uygulamanın teknik tasarımına, mimarisine, işleyişine, aynı işlevi gören uygulamalarla benzer ve farklı yönlerine, kullanıcı profiline ilişkin hususlar ele alınmıştır.

2. BYLOCK UYGULAMASI

2.1 Uygulamanın Özellikleri

Google Play'de 2014 yılının başlarında kullanıma sunulan ve 2016 yılının ilk aylarına kadar çeşitli versiyonlarla kullanımda bulunan ByLock uygulamasında;

- Kriptolu anlık mesajlaşma,
- Kriptolu sesli görüşme,
- Grup mesajlaşmaları,
- Dosya paylaşımı,
- E-posta iletimi,
- Arkadaş ekleme

özellikleri mevcuttur.

Arkadaş ekleme işlemi, anılan uygulamaya kayıt olurken kullanıcı tarafından belirlenen ve "Kullanıcı Adı (Kodu/Rumuzu)" olarak isimlendirilen şahsa özel kodun girilmesi suretiyle gerçekleştirilmektedir. Uygulama üzerinden telefon numarası veya "ad soyad" bilgileriyle arama yapılarak kullanıcı eklenmesine imkan bulunmamaktadır. Diğer taraftan, ByLock'da, muadil veya yaygın mesajlaşma uygulamalarında bulunan; telefon rehberindeki kişilerin uygulamaya otomatik olarak eklenmesi özelliği bulunmamaktadır.

Kullanıcıların birbirleriyle ByLock uygulaması üzerinden iletişime geçebilmeleri için tarafların birbirlerinin "Kullanıcı Adı/Kodu" bilgilerini bilmeleri ve her iki tarafın diğerini arkadaş olarak eklemesi gerekmektedir.

2.2 ByLock Uygulamasına Kayıt Olma İşlemi

Uygulamada gerçekleştirilen kullanıcı kayıt işlemi esnasında,

- Kullanıcıdan telefon numarası ya da e-posta adresi talep edilmediği,
- Sadece bir kullanıcı adı ve parola üretilmesinin istendiği,
- "SMS" mesajı ya da arama ile doğrulama yapılmadığı,
- Kullanıcı adı ve parola girildikten sonra, kullanıcıdan talep edilen bilgiler ile (ekranda rastgele parmak hareketleri yaptırılarak vb. yöntemlerle) bir kriptografik anahtar üretildiği

tespit edilmiştir.

2.3. ByLock Sürümleri

Uygulamanın, Android işletim sistemi üzerinde çalışan "1 serisi" ve "2 serisi" olarak adlandırılabilecek iki temel sürümü bulunmaktadır. 2 serisi aynı zamanda "ByLock++" olarak da adlandırılmış olup, Google Play'de farklı bir sayfadan yeni bir uygulama gibi sunulmuştur.

1 serisi sürümlerin en sonuncusu olan "ByLock 1.1.7" 2014 yılının Aralık ayında güncellendiği anlaşılmaktadır. Daha sonraki süreçte, ByLock++ (2 serisi) piyasaya sürülmüş, uygulama Google Play'den kaldırılana kadar bu sürüm kullanıma sunulmaya devam edilmiştir. Versiyonların yaklaşık tarihlerini gösteren ekran görüntüsü Ek-1'de, uygulamanın Google Play'den yaklaşık indirilme sayılarına ilişkin ekran görüntüsü Ek-2'de sunulmuştur.

2.4 ByLock Uygulamasını Global ve Ticari Anlık Mesajlaşma (Instant Messaging - IM) Uygulamalarından Ayıran Farklılıklar

Anlık mesajlaşma uygulamalarının çoğu, kullanıcılara **kolay kullanım** özelliği sunmaktadır. ByLock uygulamasında ise, uygulamayı kullanan şahıs, iletişim kurmak istediği şahsa ait "Kullanıcı Adı" bilgisine sahip değilse, bu kişi ile iletişim kuramamaktadır.

Anlık mesajlaşma uygulamaları, kullanıcılarına hızlı iletişim imkânı sunar. ByLock uygulamasını kullanan bir şahıs uygulamayı telefonuna indirdiğinde, rehberindeki diğer şahısların uygulamayı kullanıp kullanmadığını görememekte, şahıslar ile doğrudan iletişime geçememektedir.

Anlık mesajlaşma uygulamalarının çoğu, reklam vb. servisler ile uygulamanın olabildiğince çok kullanıcı tarafından kullanılmasını sağlamak suretiyle uygulamanın marka değerini ve kazancını arttırmayı hedeflemektedir. ByLock uygulamasında ise daha fazla kullanıcıya ulaşmak ve ticari bir değer haline gelmek yerine 'anonimlik' temelinde belirli bir kullanıcı sayısını aşmamak istendiği anlaşılmaktadır.

Anlık mesajlaşma uygulamalarında, şahıslar sosyal çevresiyle günlük ve çoğunlukla rutine dair iletişime geçmektedir. ByLock uygulamasındaki iletişim ağı ve içerikler incelendiğinde ise, örgütsel amaç ve temalı bir kullanım görülmektedir.

3. BYLOCK UYGULAMASINA YÖNELİK TEKNİK ÇALIŞMALAR

3.1 Dayanak ve Yöntem

1.11.1983 Tarihli Ve 2937 Sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununun 6 ncı maddesinin (d) bendinde; Milli İstihbarat Teşkilatının görevlerini yerine getirirken; gizli çalışma usul, prensip ve tekniklerini kullanabileceği (i) bendinde ise Milli İstihbarat Teşkilatı "dış istihbarat, millî savunma, terörle mücadele ve uluslararası suçlar ile siber güvenlik konularında her türlü teknik istihbarat ve insan istihbaratı usul, araç ve sistemlerini kullanmak suretiyle bilgi, belge, haber ve veri toplamak, kaydetmek, analiz etmek ve üretilen istihbaratı gerekli kuruluşlara ulaştırmak" yetkisiyle donatılmış bulunmaktadır.

Söz konusu kanuni yetkiye müsteniden Teşkilata özgü teknik istihbarat usul, araç ve yöntemleri kullanılmak suretiyle ByLock uygulamasına ait sunucular üzerindeki veriler ile uygulama sunucusunun ve IP adreslerinin satın alındığı e-posta adreslerinin içerikleri başta olmak üzere muhtelif veriler elde edilmiştir. Yine işbu rapor bünyesinde, kendi imkânlarının ifşa olmaması adına, eğer açık kaynaklı bir veri, veri tabanı ve araçlar üzerinden izah/teyit imkanı varsa, doğrulama amacıyla kullanılabilecek bir takım hususlara Teşkilatın kendi imkanlarına atıfta bulunulmadan yer verilmiştir.

Devletin teknik istihbarat faaliyetlerine ilişkin imkân ve kabiliyetlerin açığa çıkarılmaması ve istihbarata karşı koyma amacıyla, verilerin temin edilmesine ilişkin hassas yöntem, usul ve araçlara yer verilmemiştir. Bu amaçla, sadece raporun kapsamına girmesi gerektiği değerlendirilen hususlara değinilmiştir.

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.

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 görülmüştür. 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:**

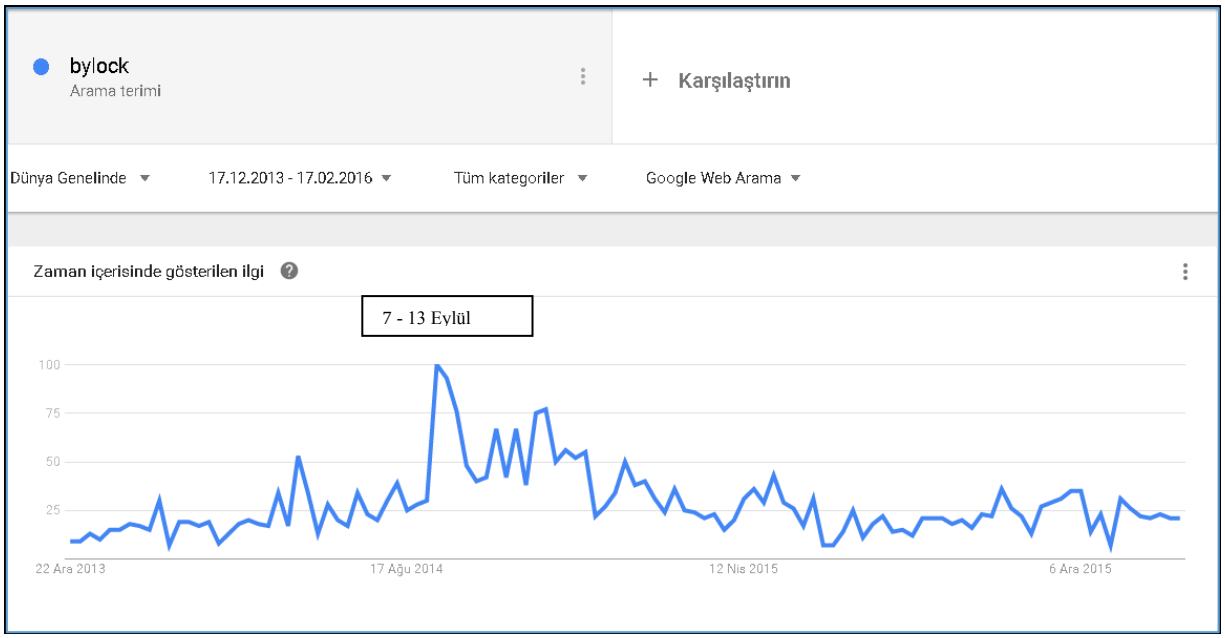
→ 46.166.160.137	→ 46.166.164.178	→ 46.166.164.181
→ 46.166.164.176	→ 46.166.164.179	→ 46.166.164.182
→ 46.166.164.177	→ 46.166.164.180	→ 46.166.164.183

'**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. ByLock hakkında elde edilen verilerin doğrulanması için 'censys.io' sitesinden örnek olarak 26 Ocak 2016 tarihine ait SSL/TLS protokolü için 443/TCP portlarına yönelik yapılan tarama verileri indirilmiş, bu veri üzerinde yapılan aramada ByLock sunucusu için hazırlanan TLS sertifikaları aranmıştır. Arama sonucunda yukarıda listelenen 9 adet IP adresine ait TLS sertifikaları bulunmuştur. Bulunan sertifikalardan birine ait ekran görüntüsü örnek olarak EK-3'de sunulmuştur. Söz konusu sertifikanın **"David Keynes"** adıyla oluşturulduğu görülmüştür.

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**. (Ek-4)

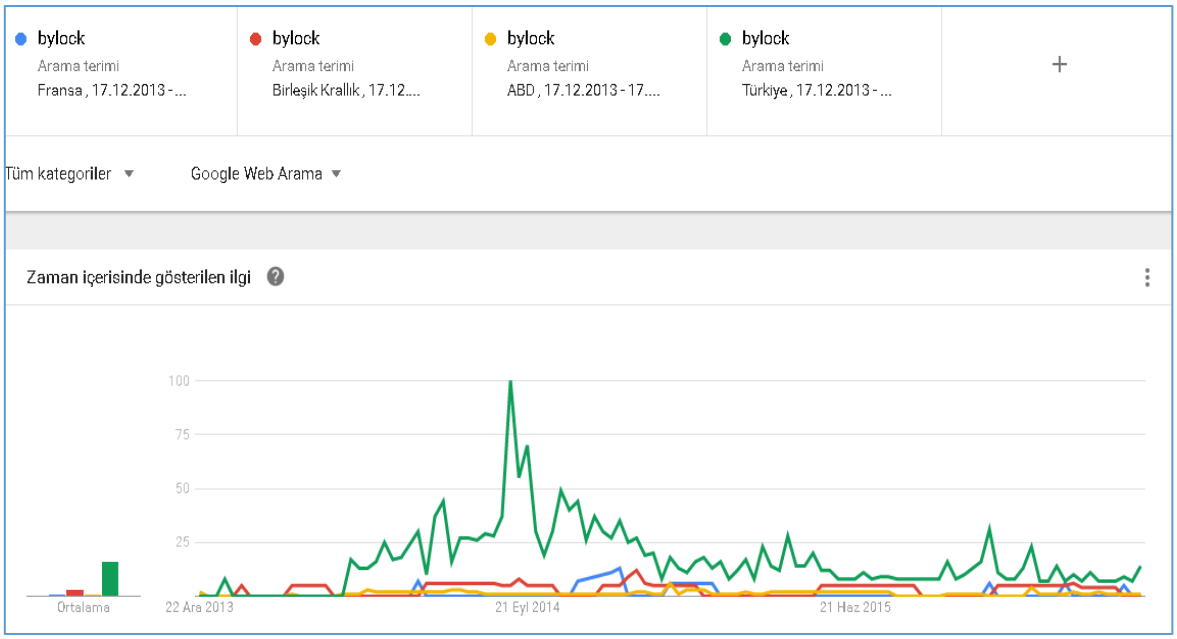
3.3 ByLock Uygulamasına İlişkin Açık Kaynak Tespitleri

15 Temmuz 2016 tarihinden öncesine dair olarak "ByLock" uygulamasına ilişkin açık kaynaklarda yürütülen muhtelif araştırmalar neticesinde; "ByLock" uygulamasının, Google Play ve Apple AppStore uygulama marketlerinden yayından kaldırılmasının ardından, uygulama kurulum dosyalarına erişimin, APK indirme siteleri üzerinde, hangi versiyonun hangi zaman aralığı için sunucu tarafından desteklendiği ve çalışır vaziyette olduğu ayrı bir çalışmanın konusu olmakla birlikte, devam ettiği tespit edilmiş olup arama motorlarında "ByLock" kelime aramalarına ilişkin istatistikler ve karşılaştırmalar aşağıda grafiksel olarak sunulmuştur:



"ByLock" Arama İstatistikleri (Türkiye)

17 Aralık 2013 ve 17 Şubat 2016 tarihleri arasında "ByLock" anahtar kelimesi kullanılarak yapılan Google aramaları incelendiğinde; aramaların 7 - 13 Eylül 2014 tarih aralığında tavan yaptığı, 2015 yılının başlarında inişe geçtiği ve sonraki süreçte de tekrar yükselişe geçmediği belirlenmiştir.



"ByLock" Arama İstatistikleri (Dünya)

"ByLock" uygulamasına ilişkin dünya genelinde yapılan aramalar incelendiğinde, Türkiye dışında Fransa, İngiltere ve ABD'nin yer aldığı tespit edilmiş olmakla birlikte anılan uygulamaya ilişkin aramaların neredeyse tamamının Türkiye kaynaklı olduğu, diğer ülkelerden yapılan aramaların da örgütün yabancı ülkelerdeki mensupları tarafından veya Türk kullanıcılar tarafından VPN bağlantısı ile gerçekleştirildiği değerlendirilmektedir.

APK indirme sitelerinde yer alan 500.000 - 1 milyon adet indirme istatistiklerinin, ne ölçüde doğru sayıyı ifade ettiği teyit edilememekte birlikte, bu rakamlara ulaşıldığı varsayılsa bile;

- Uygulamanın, cihazdan silinip tekrar yüklenmesi,
- İndirilip kullanıcı oluşturul(a)maması,
- Farklı bir cihaza kurulması

gibi hususlar bir arada değerlendirildiğinde, indirme sayılarının uygulama sunucusu üzerinde olduğu görülen 215.092 adet kullanıcı sayısıyla uyumsuz olmadığı değerlendirilmektedir. Nitekim tüm çalışmalarda bilinçli veya bilinçsiz 'indirme' değil

kullanma durumu irdelenmiştir. Dolayısıyla, muhtelif indirme rakamlarından ziyade, anılan uygulamaya 'kayıt olmuş' kullanıcıların esas alınması gerekmektedir.

Twitter'da, 15 Temmuz 2016 tarihi öncesinde "ByLock" uygulamasına ilişkin paylaşımlarda bulunan kullanıcıların büyük çoğunluğunun FETÖ/PDY lehine paylaşımlarda bulunduğu görülmüştür. Bu durum, kimliği tespit edilebilen hesap kullanıcılarının (gerçek kimliklerine bu rapor da yer verilmemiştir) FETÖ/PDY'ye müzahir şahıslar olduklarının, kamuoyuna yansımasında önce uygulamayı bildiklerinin ve yaygın şekilde kullandıklarının göstergesi olarak değerlendirilmiştir.

"ByLock" uygulamasına yönelik olarak yapılan açık kaynak çalışmalarında;

- Anılan uygulamanın 15 Temmuz 2016 tarihinden önce, belirli sayıda olmak üzere, Twitter dışındaki çok az platformda yer aldığı,
- Ekşi Sözlük, Uludağ Sözlük, İnci Sözlük gibi güncel konuların ve kavramların yoğun olarak paylaşıldığı ve tartışıldığı platformlarda, 15 Temmuz 2016 tarihinden öncesine ait herhangi bir bilgiye rastlanmamıştır.

Toplumda ve hatta teknik konularla ilgili insanlar arasından bilinirliği yok denebilecek seviyedeyken, istatistikler göz önünde bulundurulduğunda; diğer ülkelere kıyasla Türkiye'den kullanım değerlerinin açık farklı yüksek olması (diğer tüm ülkelerin toplamından çok daha fazla) uygulamanın amacı hakkında fikir veren en önemli unsurlar arasında görülmektedir.

3.4. Kriptografik Protokol Analizi ve Tersine Mühendislik Çalışması

3.4.1 Kriptografik Protokol Analizi

Çalışmanın bu bölümünde "ByLock" uygulamasının istemcisi ve sunucusu arasındaki haberleşme ağ analizi yapılmıştır. Yapılan bu analizle istemci ve sunucu arasındaki ağ trafiği "IP" paketi seviyesinde ele alınmış olup, bu paketlerin yapısı, kullanılan protokol katmanları, içerdiği verilerin tespiti ve bu verilerin şifreli olup olmadıklarının belirlenmesi amaçlanmıştır. Ağ analizi işlemi, burada yer verilen, uygulamanın 4 farklı sürümü üzerinde ayrı ayrı tekrarlanmıştır.

Uygulamanın ağ trafiği incelendiğinde bahse konu uygulamanın "TCP" katmanında şifreleme sağlayan "TLS" (Transport Layer Security) kriptografik protokolünü kullandığı tespit edilmiştir. Test ortamında, istemci tarafından gönderilen isteklerin ve sunucudan istemciye dönen cevapların çözümü "TLS" şifrelemesinin çözümlenebilmesiyle sağlanmıştır.

"ByLock" uygulamasının istemcisinin kayıt aşamasında "XML" biçiminde gönderdiği mesajın çözümlenmesi sonucunda mesaj içeriğinde,

- Kullanıcıya ait özel bir kayıt numarası,
- Kullanıcı adı,
- Kullanıcı parolasının kriptografik özet fonksiyonu (cryptographic hash function) çıktısı,
- Gizli anahtarın (private exponent) şifrelenmiş hali,
- Açık anahtarlı şifreleme (public key encryption) değişkeni olan taban değeri (modulus),
- Uygulamanın hangi işletim sistemi sürümünde çalışmakta olduğu,
- Kullanıcının bulunduğu saat dilimi,

bilgilerinin bulunduğu gözlemlenmiştir. Gözlemlenen mesaj yapısına dair fikir vermesi için içeriği kısıtlanmış olan bir mesaj örneği aşağıda sunulmuştur:

```
<?xml version="1.0" encoding="UTF-8"?>
<request id="">
     <userId>0</userId>
     <username>CIKARILMISTIR</username>
     <password>183B…6786</password>
     <privateExponent>Gg3g…9yx0=</privateExponent>
     <modulus>AJ8K…UJbk=</modulus>
     <edition>android</edition>
     <tzid>Europe/Istanbul</tzid>
     <audioV2>1</audioV2>
</request>
```

3.4.2 Tersine Mühendislik Çalışmaları

”ByLock” uygulamasının, “Android” işletim sisteminde çalışan ve burada yer verilen 4 farklı sürümünün kurulum dosyalarına yönelik statik ve dinamik tersine mühendislik analizleri gerçekleştirilmiştir.

3.4.2.1 Statik Analiz

“ByLock” uygulamasının kaynak kodlarını elde edebilmek amacıyla “Android” uygulamaları için geliştirilmiş bir disassembler yazılımı kullanılmıştır. Bu yazılım aracılığıyla “ByLock” uygulamasının ele alınan sürümlerinin “dalvik bytecode” biçiminde olan kaynak kodları (sadece akıllı telefonlar için derlenebilir ve anlaşılabilir kodlar) “smali” dosyaları halinde elde edilmiştir. Elde edilen bu “smali” kaynak kodları üzerinden analizler yapılmıştır. Söz konusu kaynak kodların incelenmesi sırasında “Android” uygulama geliştiricileri tarafından sıkça uygulanan bir yöntem olan bulanıklaştırma (obfuscation) yönteminin kullanıldığı gözlemlenmiştir. Bulanıklaştırma yöntemi ile kaynak kodlarda kullanılan sınıf isimleri, yordam isimleri, değişken isimleri gizlenerek, tersine mühendislik ile statik analiz yapacak kişinin daha çok zamanını alarak işi zorlaştırmak, karışıklık yaratmak aynı zamanda da uygulamanın kaynak kodlarının güvenliğini sağlamak amaçlanmıştır.

Kaynak kodların kurulum dosyasından elde edilmesi çalışması sonucunda bahse konu bulanıklaştırılmış kaynak kodları üzerinde yapılan incelemeler neticesindeki tespitler aşağıda sunulmuştur:

- “ByLock” uygulamasının, “androidsupport”, “android-filechooser” ve “googlegms” (sadece 1.1.6 sürümü için) kod kütüphanelerini kullandığı tespit edilmiştir.
- Uygulamanın 4 ayrı sürümüne dair “uygulama özelindeki (UÖ)” (Kod kütüphaneleri hariç diğer kodlar, uygulama özelindeki (UÖ) kodlar olarak adlandırılmıştır.) ve toplam kod dosyası sayısı ile kod satırı sayısı aşağıdaki tabloda sunulmuştur.

Sürüm Numarası	UÖ için Kod Dosyası Sayısı	Toplam Kod Dosyası Sayısı	UÖK için Kod Satırı Sayısı	Toplam Kod Satırı Sayısı
1.1.3	288	773	86885	214621
1.1.6	295	1560	88042	383325
1.1.7	288	773	87586	215329
2.0.0	287	772	74542	184400

Tablo - 4 ayrı sürüme dair UÖ ve toplam kod dosyası sayısı ile kod satırı sayısı

- Uygulamanın kaynak kodları içerisinde, Türkçe *"Dosya", "Posta"* ve *"Sesli Arama"* şeklinde ifadelerin bulunduğu görülmüştür (Ek-5).
- Uygulamada, mesajlaşmaya dair anlık bildirimlerin (push notification) iletimine dair kodların mevcut olduğu, lakin bu işlev için Google tarafından geliştirilen ve yaygın biçimde mobil uygulamalar tarafından kullanılmakta olan Google Bulut Mesajlaşması'ndan (Google Cloud Messaging – GCM) faydalanılmadığı görülmüştür.
- Uygulamanın 1.1.3 ve 1.1.7 sürümlerine ait kurulum dosyalarında sırasıyla;
  - "https://bylock.net:443/SHU-Server"
  - "https://46.166.164.181:443/App-Server"

  alan adlarının yer aldığı tespit edilmiştir.

- İki kullanıcı arasında iletilen verilerin **2048 bitlik** asimetrik "**RSA/ECB/OAEPWithSHA-1AndMGF1Padding**" kriptografik algoritması kullanılarak şifrelendiği belirlenmiştir. Söz konusu kriptografik algoritma bir tür açık anahtarlı/asimetrik şifreleme algoritması olup, biri gizli diğeri açık olmak kaydıyla iki adet anahtar kullanarak şifreleme yapmaktadır. Açık anahtar kullanılarak şifrelenen veriler gizli anahtar olmaksızın çözümlenememektedir.
- Asimetrik gizli anahtarın ise simetrik yapılı bir blok şifreleme algoritması olan "**AES/CBC/PKCS5Padding**" ile şifrelendiği gözlemlenmiştir.
- İstemci kaynak kodlarında yer alan kriptografik algoritmalara ilişkin bölümler Ek-6'de sunulmuştur.

- Uygulamaya kayıt ve iki kullanıcı arasındaki mesajlaşmaya ait kriptografik akış şeması Ek-7'da sunulmuştur.

3.4.2.2 Dinamik Analiz

"ByLock" uygulamasının statik analizinin yapılmasının ardından, uygulamanın burada yer verilen 4 ayrı sürümü, diğer bir tersine mühendislik yöntemi olan dinamik analiz ile incelenmiştir.

Uygulamaya kayıt esnasında, kullanıcının belirlemiş olduğu parolanın, "xml" mesajı içerisindeki "password" alanında "MD5" kriptografik özet algoritmasıyla, asimetrik gizli anahtarın (private exponent) ise "privateExponent" alanında şifreli olarak sunucuya iletildiği tespit edilmiştir.

Söz konusu şifreleme yönteminde;

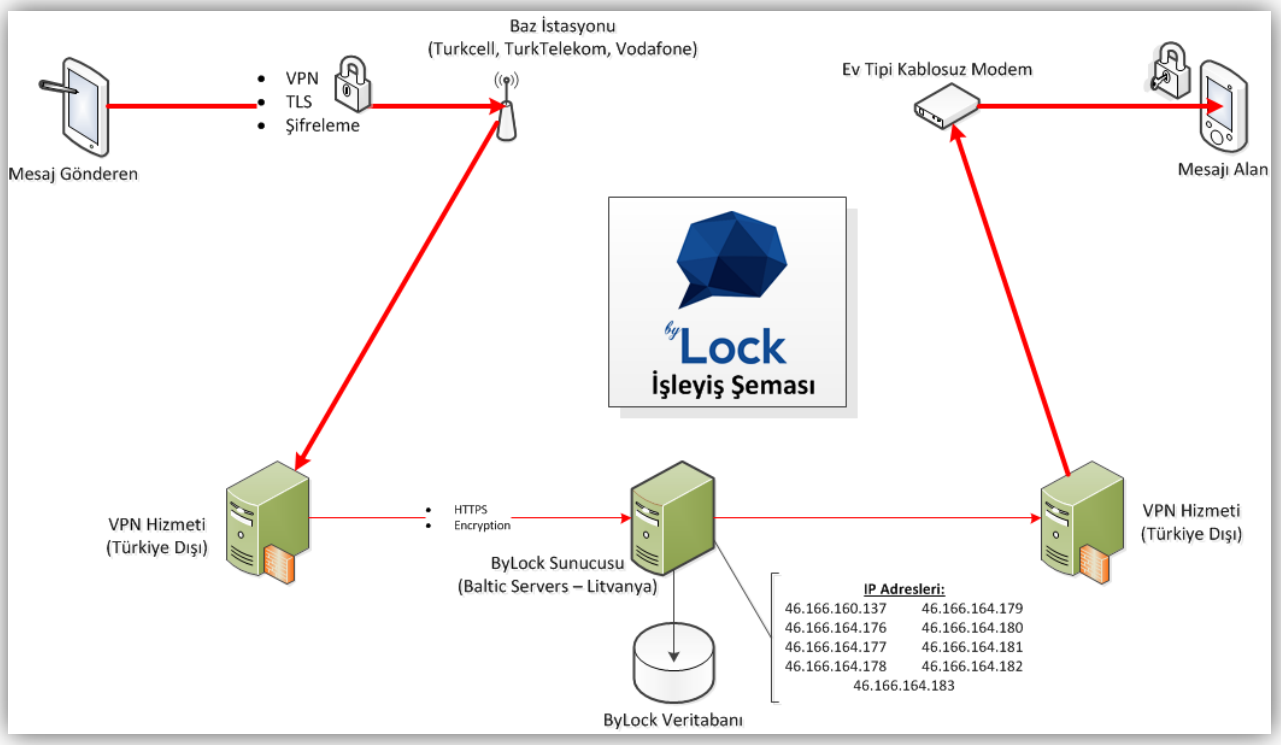
- Kayıt sırasında giriş ekranına girilen parolanın "SHA-256" kriptografik özet algoritmasından geçirildiği,
- Elde edilen 32 byte uzunluğundaki kriptografik özet değerinin 16 byte'lık iki parçaya ayrılarak kullanıldığı,
- Söz konusu kriptografik özet değerinin ilk 16 byte'lık kısmının "AES/CBC/PKCS5Padding" blok şifreleme algoritması için simetrik gizli anahtar (secret key) olarak, son 16 byte'lık kısmının ise başlangıç vektörü (initilization vector) olarak kullanılarak, istemci tarafında oluşturulan asimetrik gizli anahtarın (private key) şifrelendiği (Bahse konu asimetrik gizli anahtar her kullanıcı için özel olarak kayıt sırasında üretilerek haberleşmede kullanılmaktadır.),
- Şifrelenmiş olan bu çıktının "xml" formatlı mesajda "privateExponent" bölümünde yer aldığı

tespit edilmiştir.

3.5 Sunucuya Yönelik Teknik Çalışmalar

3.5.1 Uygulamanın İşleyiş Şeması

ByLock uygulaması ve uygulama sunucularında çalışan yazılımlara ilişkin işleyiş şemasına aşağıda yer verilmiştir:



3.5.2 Uygulama Sunucusunun Yazılım Modelleri

Yürütülen çalışmalar neticesinde, uygulama sunucusundaki yazılım detaylı incelemelere tabii tutulmuş ve söz konusu yazılıma ilişkin yazılım modelleri Ek-8'de sunulmuştur.

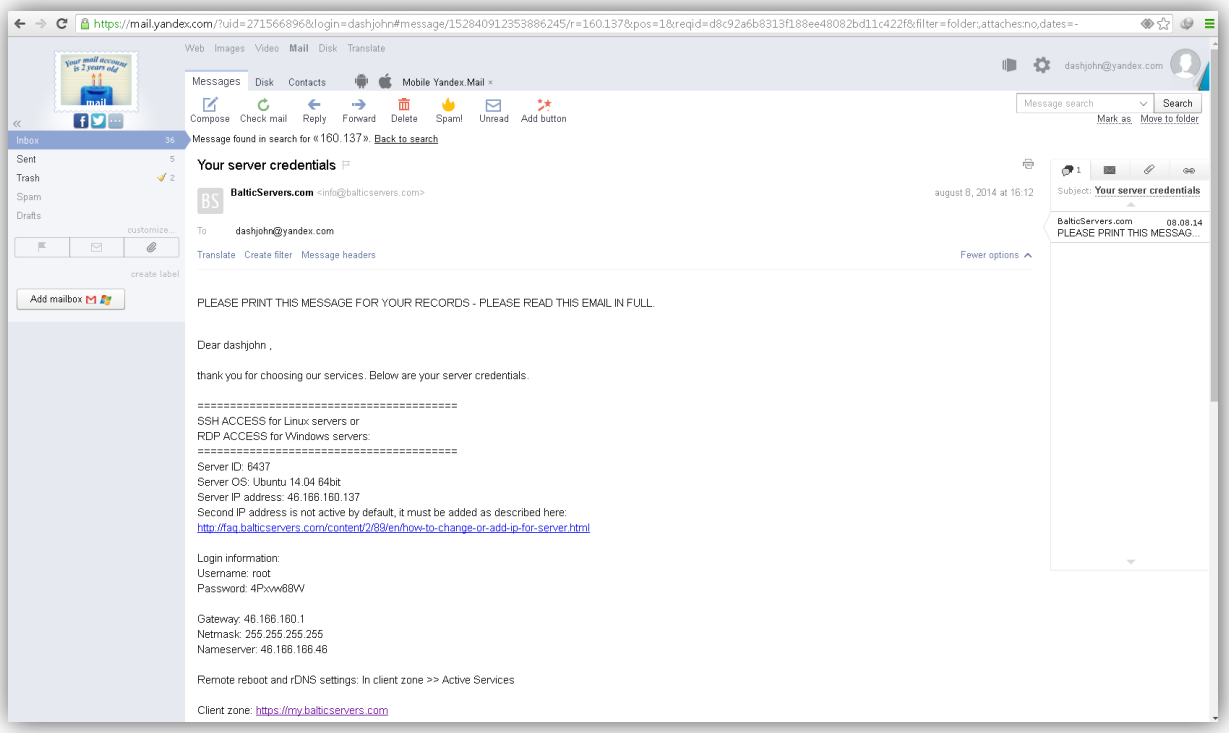
3.5.3 Uygulama Sunucusunda Çalışan Yazılımda Rastlanan Türkçe İfade

Sunucuda çalışan yazılımların kaynak kodları içerisinde, Türkçe olarak "Yetkiniz Yok" şeklinde bir ifadenin bulunduğu görülmüştür (Ek-9).

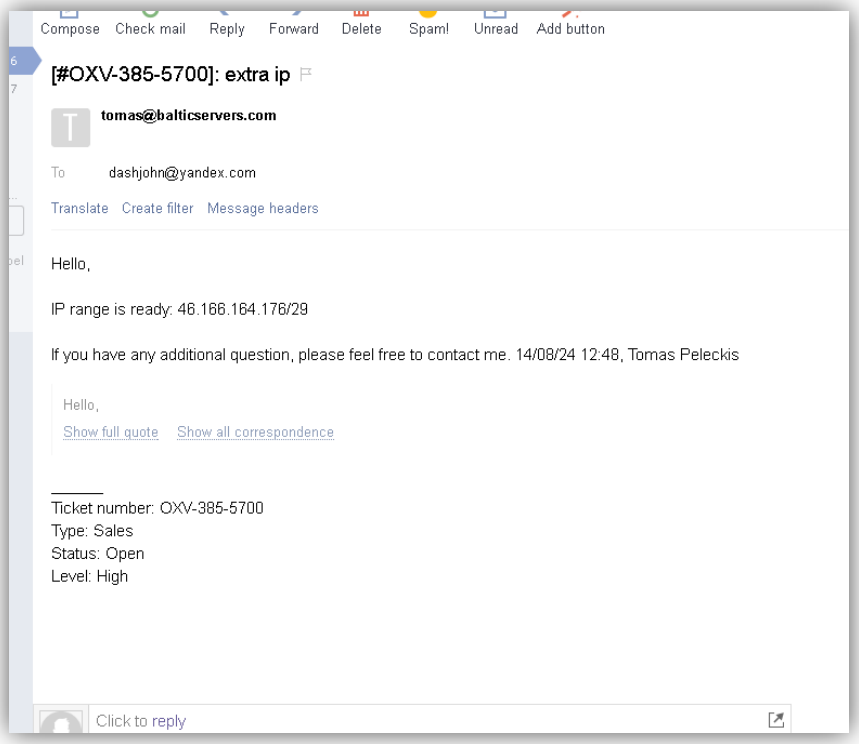
3.5.4 Uygulamanın Sunucusunu Yöneten Şahsın Faaliyetlerine Yönelik Tespitler

Uygulama sunucusunu yöneten şahsın, uygulamanın hizmet verdiği sunucuyu ve IP adreslerini kiralama yöntemi ile temin ettiği, söz konusu hizmetlere ait bedelleri aylık ve üç aylık aralıklarla ödediği, bu işlemleri dashjohn@yandex.com adlı elektronik posta adresi üzerinden gerçekleştirdiği 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 verilmiştr. 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.


Compose Check mail Reply Forward Delete Spam! Unread Add button

[#OXV-385-5700]: extra ip

tomas@balticservers.com

To dashjohn@yandex.com

Translate Create filter Message headers

Hello,

IP range is ready: 46.166.164.176/29

If you have any additional question, please feel free to contact me. 14/08/24 12:48, Tomas Peleckis

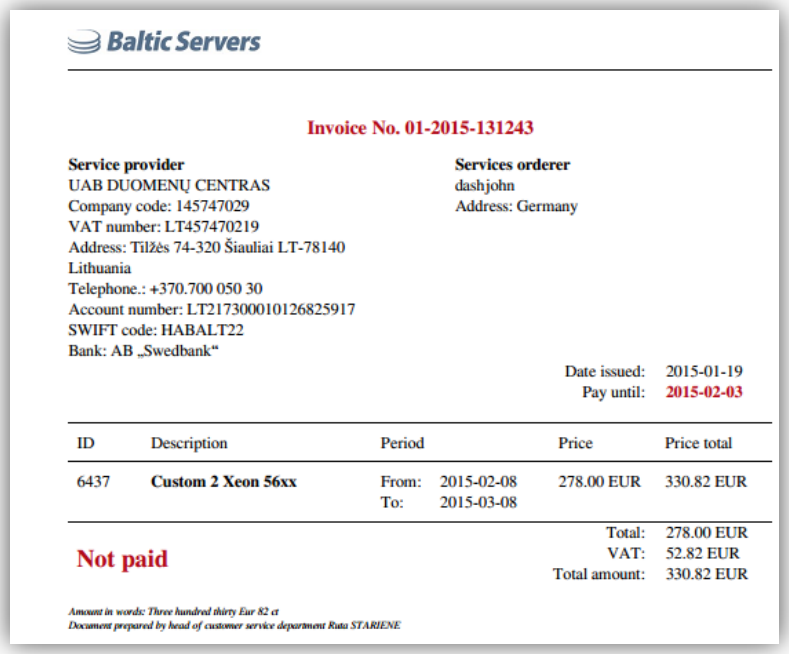
Hello,

Show full quote Show all correspondence

Ticket number: OXV-385-5700
Type: Sales
Status: Open
Level: High

Click to reply

ByLock uygulamasının hizmet verdiği sunucu ve ek IP adreslerinin aylık ve 3 aylık dönemlerde tahakkuk eden faturalara ilişkin elde edilen e-posta içeriklerine aşağıda yer verilmiştir:


Baltic Servers

Invoice No. 01-2015-131243

Service provider
UAB DUOMENŲ CENTRAS
Company code: 145747029
VAT number: LT457470219
Address: Tilžės 74-320 Šiauliai LT-78140
Lithuania
Telephone.: +370.700 050 30
Account number: LT217300010126825917
SWIFT code: HABALT22
Bank: AB „Swedbank"

Services orderer
dashjohn
Address: Germany

Date issued: 2015-01-19
Pay until: **2015-02-03**

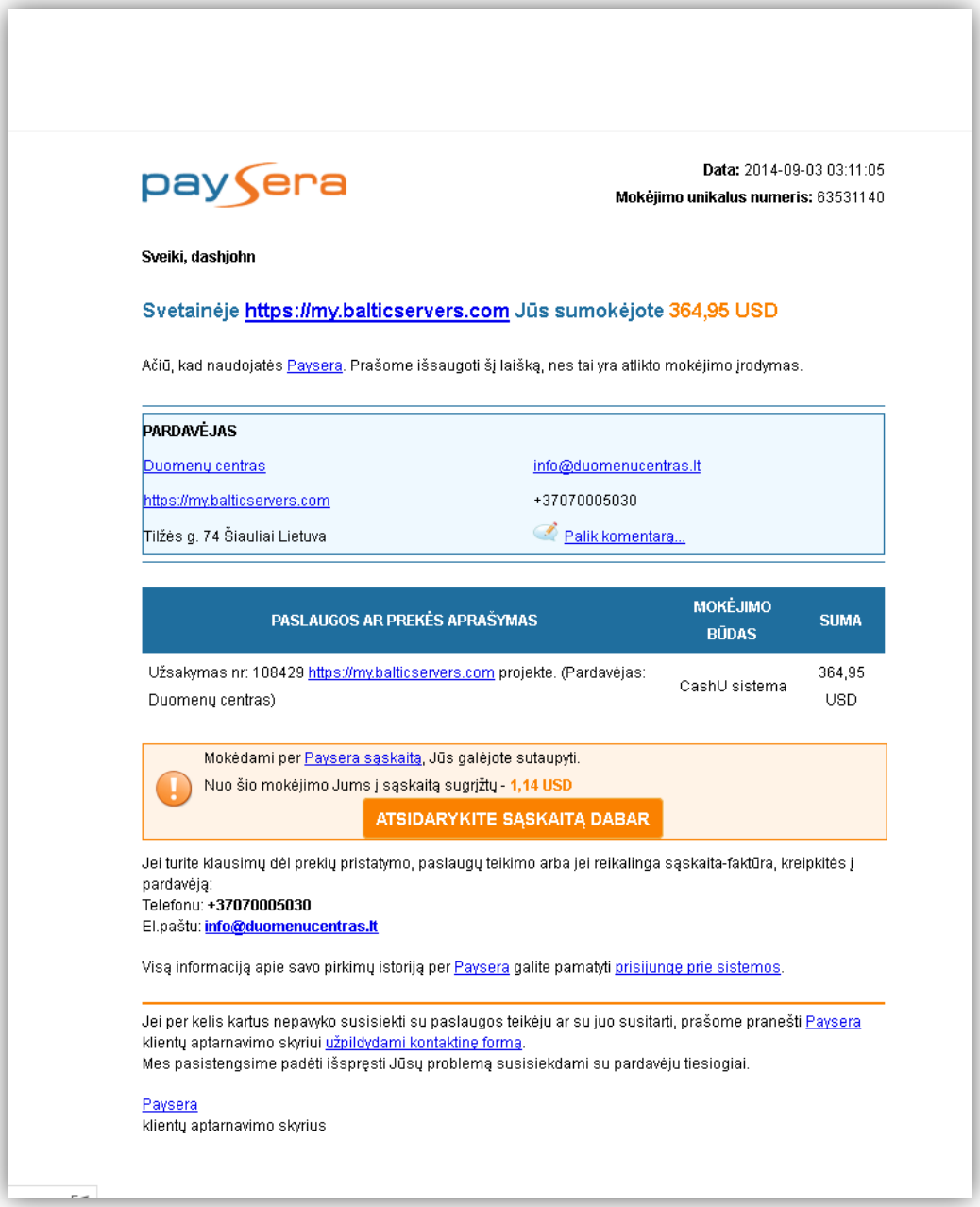
ID	Description	Period	Price	Price total
6437	**Custom 2 Xeon 56xx**	From: 2015-02-08 To: 2015-03-08	278.00 EUR	330.82 EUR

Not paid

Total: 278.00 EUR
VAT: 52.82 EUR
Total amount: 330.82 EUR

Amount in words: Three hundred thirty Eur 82 ct
Document prepared by head of customer service department Ruta STARIENE

Bahsi geçen ödemeler incelendiğinde sunucu ve IP adreslerinin 2016 yılı Şubat ayına kadar **dashjohn@yandex.com** e-posta adresi kullanılarak kayıt olunan anonimlik sağlayan "PaySera" ödeme sistemi vasıtası ile ödemelerinin yapıldığı tespit edilmiştir. Ödemelere ilişkin örnek bir e-posta içeriğine aşağıda yer verilmiştir:



paysera

Data: 2014-09-03 03:11:05
Mokėjimo unikalus numeris: 63531140

Sveiki, dashjohn

Svetainėje https://my.balticservers.com Jūs sumokėjote 364,95 USD

Ačiū, kad naudojatės Paysera. Prašome išsaugoti šį laišką, nes tai yra atlikto mokėjimo įrodymas.

PARDAVĖJAS

Duomenų centras	info@duomenucentras.lt
https://my.balticservers.com	+37070005030
Tilžės g. 74 Šiauliai Lietuva	Palik komentarą...

PASLAUGOS AR PREKĖS APRAŠYMAS	MOKĖJIMO BŪDAS	SUMA
Užsakymas nr: 108429 https://my.balticservers.com projekte. (Pardavėjas: Duomenų centras)	CashU sistema	364,95 USD

Mokėdami per Paysera sąskaitą, Jūs galėjote sutaupyti.
Nuo šio mokėjimo Jums į sąskaitą sugrįžtų - 1,14 USD
ATSIDARYKITE SĄSKAITĄ DABAR

Jei turite klausimų dėl prekių pristatymo, paslaugų teikimo arba jei reikalinga sąskaita-faktūra, kreipkitės į pardavėją:
Telefonu: **+37070005030**
El.paštu: **info@duomenucentras.lt**

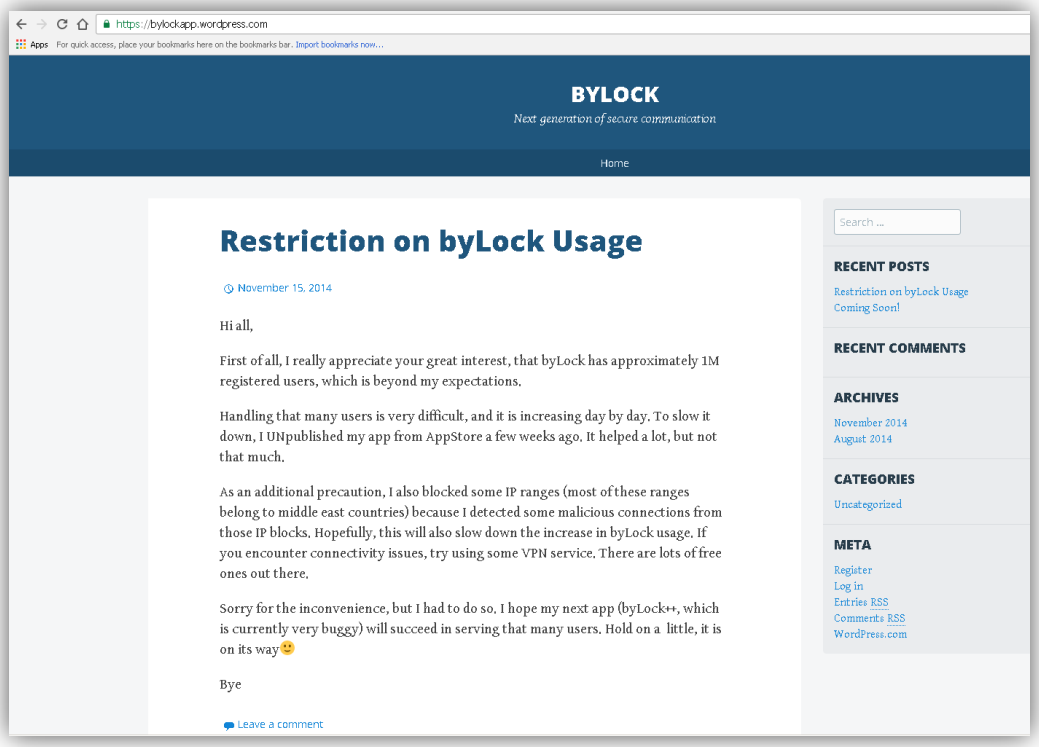
Visą informaciją apie savo pirkimų istoriją per Paysera galite pamatyti prisijunge prie sistemos.

Jei per kelis kartus nepavyko susisiekti su paslaugos teikėju ar su juo susitarti, prašome pranešti Paysera klientų aptarnavimo skyriui užpildydami kontaktinę formą.
Mes pasistengsime padėti išspręsti Jūsų problemą susisiekdami su pardavėju tiesiogiai.

Paysera
klientų aptarnavimo skyrius

3.5.5 Uygulama Sunucusuna Ortadoğu IP Adreslerinden Erişimin Engellenmesi

15.11.2014 tarihinde ByLock uygulama sunucusunun yöneticisi olduğu değerlendirilen şahıs, uygulama için açtığı "**bylockapp.wordpress.com**" adresli web sayfasında, Ortadoğu'dan gelen bazı IP adreslerinin uygulamaya erişimini engellediğini duyurmuştur. Uygulama sunucularına yönelik yürütülen teknik incelemeler neticesinde elde edilen bilgilerle, şahsın engelleme işlemini **17.11.2014** tarihinde yaptığı, fakat **15.11.2014** tarihinden önceki erişim log kayıtlarını veri tabanından sildiği tespit edilmiştir. Şahsın konuyla ilgili yazısının ekran görüntüsüne aşağıda yer verilmiştir:



Sunucudan elde edilen bilgiler doğrultusunda, bu engellemeye yönelik çalıştırıldığı tespit edilen komutlardan bir kısmı, örnek olarak aşağıda sunulmuştur:

```
root@hst-46-166-160-137:~#
iptables -N LOGGING
iptables -A INPUT -s 5.2.80.0/21 -j LOGGING
iptables -A INPUT -s 5.11.128.0/17 -j LOGGING
iptables -A INPUT -s 5.23.120.0/21 -j LOGGING
iptables -A INPUT -s 5.24.0.0/14 -j LOGGING
iptables -A INPUT -s 5.44.80.0/20 -j LOGGING
iptables -A INPUT -s 5.44.144.0/20 -j LOGGING
```

```
iptables -A INPUT -s 5.46.0.0/15 -j LOGGING
iptables -A INPUT -s 5.63.32.0/19 -j LOGGING
```

Söz konusu şahsın engellediği IP adres blokları Ek-10'da yer almaktadır.

Engelleme işlemine konu IP adreslerinin tamamına yakınının Türkiye IP adresleri aralığında olduğu, dolayısıyla şahsın, açıklamalarında Ortadoğu derken aslında özellikle Türkiye'den gelen bağlantıları engellemeye yönelik bir çalışmada bulunduğu anlaşılmıştır.

Söz konusu şahsın, IP adreslerini engellemesi neticesinde, Türkiye'deki kullanıcılarının Sanal Özel Ağ (Virtual Private Network - VPN) kullanımını şart koşarak kullanıcı tespitini engellemeye çalıştığı anlaşılmaktadır. Bu yöntem ile uygulamayı kullananların tespitinin önüne geçilmesini amaçlayan kurgusal başka bir tedbir alındığı değerlendirilmektedir.

Uygulama sunucusu yöneticisinin gerçekleştirdiği IP engellemesinin, Türkiye'deki kullanıcılarının uygulamaya erişimlerini engellemekten ziyade, kullanıcıların VPN kullanılması sonucunda gerçek IP adresleri ile sunucuya bağlanmalarının tespit edilmesini önlemeyi amaçladığı sonucuna varılmaktadır.

3.6. ByLock Uygulama Sunucusu Verileri

Yürütülen çalışmalar neticesinde, ByLock uygulama sunucusundaki veri tabanı dosyaları, sunucu yöneticisi tarafından girilen komutlar, sunucuda çalışan yazılım dosyaları elde edilmiştir. Ayrıca Türkiye'den sunucuya doğrudan bağlanmasını engelleyen yazılım içerisinde yer alan ve tamamına yakını Türkiye'ye ait olan IP adres blokları elde edilmiştir.

3.6.1 Sunucudan Elde Edilen Veri Tabanı Dosyaları

ByLock uygulamasına ait verilerin saklandığı **109 GB**'lık veri tabanı dosyası elde edilmiştir. Elde edilen verilerin incelemesine ilişkin detaylara aşağıda yer verilmiştir:

3.6.2 ByLock Uygulamasına Ait Veri Tabanı Deseni ve Özellikleri

Veri tabanı dosyaları üzerinde gerçekleştirilen çalışmalar neticesinde, aşağıdaki tablolar elde edilmiştir:

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

17 rows in set (0.00 sec)
```

Şekil 3.6.2.1: Uygulamaya ait tablo isimleri

Elde edilen tabloların veri yapıları ve/veya tablo içeriklerine ilişkin tespit edilen detay bilgilere aşağıda yer verilmiştir:

3.6.2.1 *"action" tablosu:*

```
MariaDB [appDb]> select * from action;
+----+-----------------------------------+-----------------+----------------+-----------------+-----------------+
| id | name                              | parameter1      | parameter2     | parameter3      | parameter4      |
+----+-----------------------------------+-----------------+----------------+-----------------+-----------------+
|  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 Deletion |               |                |                 |                 |
| 32 | Send Mail                         | User Id         | Mail Id        |                 |                 |
| 33 | Delete Mail                       | Mail Id         |                |                 |                 |
| 34 | Download Version                  | Version Id      |                |                 |                 |
| 35 | Upload Version                    | Version Id      |                |                 |                 |
+----+-----------------------------------+-----------------+----------------+-----------------+-----------------+
32 rows in set (0.00 sec)
```

Şekil 3.6.2.2: Action tablosunun alan adları ve özellikleri

Action tablosu, kullanıcıların uygulama etkileşimlerinin tutulduğu **"log"** tablosuyla ilişkilidir. Action tablosunda, **"log"** tablosundaki **"actionId"** değerine karşılık gelen **"işlem adı"** bilgisi tutulmaktadır. Örneğin; **actionid=3, kayıt olma işlemini, actionid=1** ise "**Add Friend** (Arkadaş Ekleme)" işlemini ifade etmektedir. Arkadaş ekleme işlemi sırasında **parameter1** değerine her kullanıcıya uygulama sunucusu tarafından atanan Userid kod numarası, **parameter2** değerine ise her kullanıcının kayıt olurken oluşturduğu "Kullanıcı Adı" **(nickname)** bilgilerinin girildiği görülmüştür. Uygulamayı kullanan şahısların yapmış oldukları kayıt olma, uygulamaya giriş yapma (Login), Çağrı gerçekleştirme, e-posta iletişimi dahil olmak üzere farklı işlemlerin hepsi için Action tablosundaki ilgili işlemin numarasına ve eklenecek değerlere göre bir log kaydı oluşturulmaktadır.

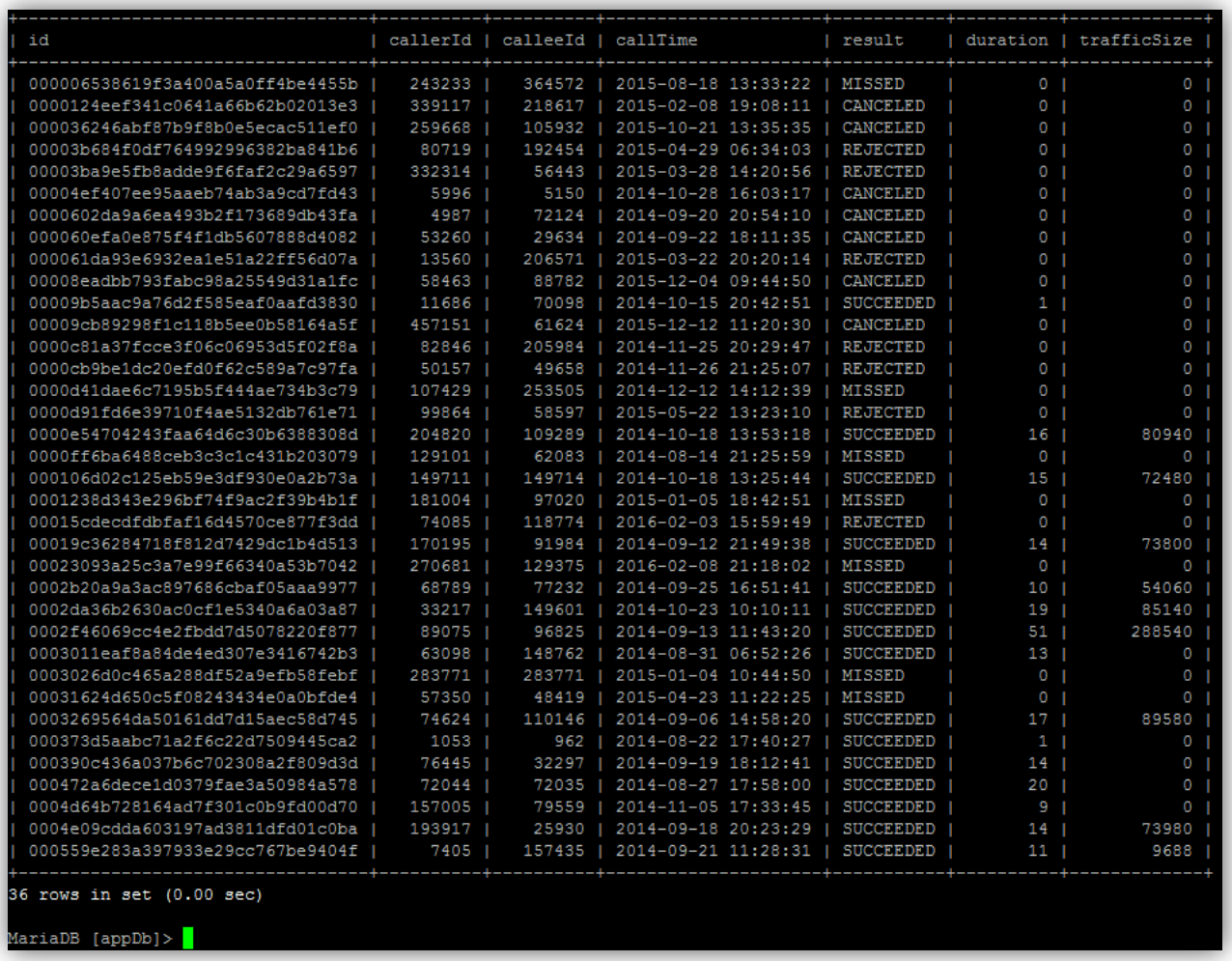
3.6.2.2 "attachment" tablosu:

```
MariaDB [appDb]> show columns in attachment;
+-----------+--------------+------+-----+---------+-------+
| Field     | Type         | Null | Key | Default | Extra |
+-----------+--------------+------+-----+---------+-------+
| id        | int(11)      | NO   | PRI | NULL    |       |
| mailId    | int(11)      | NO   | MUL | NULL    |       |
| fileId    | int(11)      | NO   | MUL | NULL    |       |
| filename  | text         | 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 3.6.2.3: attachment tablosunun alan adları ve özellikleri

Attachment (İlişik) tablosu, uygulamayı kullanan şahısların e-posta iletişimi sırasında yazdıkları metne ilave ettikleri dosya, resim vb. farklı formattaki içeriklerin isimlerinin saklandığı tablodur. Attachment tablosunda, 4.675 adet e-posta ekine ait isim bilgisinin kriptolu olarak saklandığı görülmüştür.

3.6.2.3 "call_history" tablosu:



id	callerId	calleeId	callTime	result	duration	trafficSize
000006538619f3a400a5a0ff4be4455b	243233	364572	2015-08-18 13:33:22	MISSED	0	0
0000124eef341c0641a66b62b02013e3	339117	218617	2015-02-08 19:08:11	CANCELED	0	0
000036246abf87b9f8b0e5ecac511ef0	259668	105932	2015-10-21 13:35:35	CANCELED	0	0
00003b684f0df764992996382ba841b6	80719	192454	2015-04-29 06:34:03	REJECTED	0	0
00003ba9e5fb8adde9f6faf2c29a6597	332314	56443	2015-03-28 14:20:56	REJECTED	0	0
00004ef407ee95aaeb74ab3a9cd7fd43	5996	5150	2014-10-28 16:03:17	CANCELED	0	0
0000602da9a6ea493b2f173689db43fa	4987	72124	2014-09-20 20:54:10	CANCELED	0	0
000060efa0e875f4f1db5607888d4082	53260	29634	2014-09-22 18:11:35	CANCELED	0	0
000061da93e6932ea1e51a22ff56d07a	13560	206571	2015-03-22 20:20:14	REJECTED	0	0
00008eadbb793fabc98a25549d31a1fc	58463	88782	2015-12-04 09:44:50	CANCELED	0	0
00009b5aac9a76d2f585eaf0aafd3830	11686	70098	2014-10-15 20:42:51	SUCCEEDED	1	0
00009cb89298f1c118b5ee0b58164a5f	457151	61624	2015-12-12 11:20:30	CANCELED	0	0
0000c81a37fcce3f06c06953d5f02f8a	82846	205984	2014-11-25 20:29:47	REJECTED	0	0
0000cb9be1dc20efd0f62c589a7c97fa	50157	49658	2014-11-26 21:25:07	REJECTED	0	0
0000d41dae6c7195b5f444ae734b3c79	107429	253505	2014-12-12 14:12:39	MISSED	0	0
0000d91fd6e39710f4ae5132db761e71	99864	58597	2015-05-22 13:23:10	REJECTED	0	0
0000e54704243faa64d6c30b6388308d	204820	109289	2014-10-18 13:53:18	SUCCEEDED	16	80940
0000ff6ba6488ceb3c3c1c431b203079	129101	62083	2014-08-14 21:25:59	MISSED	0	0
000106d02c125eb59e3df930e0a2b73a	149711	149714	2014-10-18 13:25:44	SUCCEEDED	15	72480
0001238d343e296bf74f9ac2f39b4b1f	181004	97020	2015-01-05 18:42:51	MISSED	0	0
00015cdecdfdbfaf16d4570ce877f3dd	74085	118774	2016-02-03 15:59:49	REJECTED	0	0
00019c36284718f812d7429dc1b4d513	170195	91984	2014-09-12 21:49:38	SUCCEEDED	14	73800
00023093a25c3a7e99f66340a53b7042	270681	129375	2016-02-08 21:18:02	MISSED	0	0
0002b20a9a3ac897686cbaf05aaa9977	68789	77232	2014-09-25 16:51:41	SUCCEEDED	10	54060
0002da36b2630ac0cf1e5340a6a03a87	33217	149601	2014-10-23 10:10:11	SUCCEEDED	19	85140
0002f46069cc4e2fbdd7d5078220f877	89075	96825	2014-09-13 11:43:20	SUCCEEDED	51	288540
0003011eaf8a84de4ed307e3416742b3	63098	148762	2014-08-31 06:52:26	SUCCEEDED	13	0
0003026d0c465a288df52a9efb58febf	283771	283771	2015-01-04 10:44:50	MISSED	0	0
00031624d650c5f08243434e0a0bfde4	57350	48419	2015-04-23 11:22:25	MISSED	0	0
0003269564da50161dd7d15aec58d745	74624	110146	2014-09-06 14:58:20	SUCCEEDED	17	89580
000373d5aabc71a2f6c22d7509445ca2	1053	962	2014-08-22 17:40:27	SUCCEEDED	1	0
000390c436a037b6c702308a2f809d3d	76445	32297	2014-09-19 18:12:41	SUCCEEDED	14	0
000472a6dece1d0379fae3a50984a578	72044	72035	2014-08-27 17:58:00	SUCCEEDED	20	0
0004d64b728164ad7f301c0b9fd00d70	157005	79559	2014-11-05 17:33:45	SUCCEEDED	9	0
0004e09cdda603197ad3811dfd01c0ba	193917	25930	2014-09-18 20:23:29	SUCCEEDED	14	73980
000559e283a397933e29cc767be9404f	7405	157435	2014-09-21 11:28:31	SUCCEEDED	11	9688

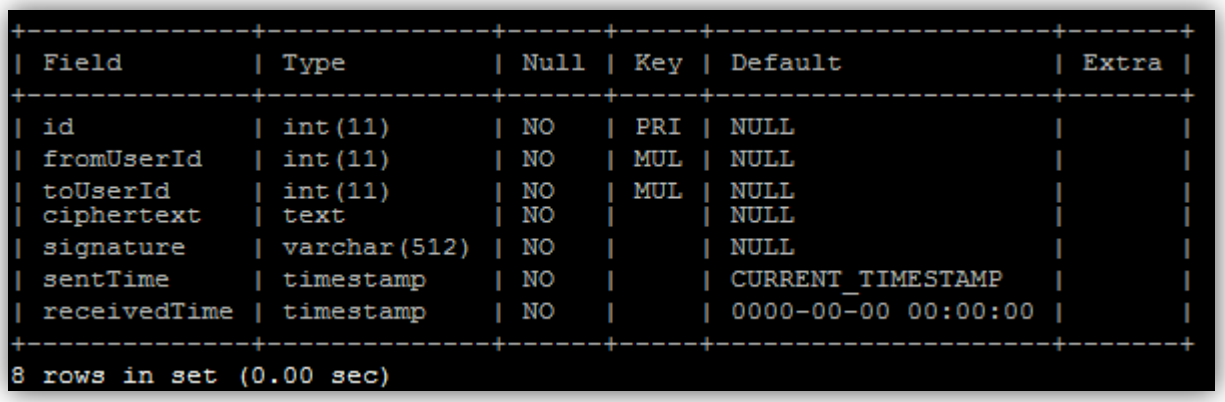
36 rows in set (0.00 sec)

MariaDB [appDb]>

Şekil 3.6.2.4: call_history tablosuna ait örnek kayıtlar

"call_history" tablosu, bütün **çağrı hareketlerine ilişkin** bilgilerin kayıt edildiği tablodur. Uygulamanın sesli çağrı özelliğiyle arama yapıldığında, yapılan çağrıya ilişkin **log** kaydı **"call_history"** tablosunda oluşmaktadır. **"call_history"** tablosunda, arayan_Id (callerId), aranan_Id (calleeId), arama_zamanı (callTime), aramanın başarılı olma durumu (result), görüşme süresi (duration) vb. bilgiler tutulmaktadır. **"call_history"** tablosundan elde edilen verilerde toplam **1.218.784** çağrı kaydı bulunmaktadır. Userid eşleştirilmesi yapılabilen şahıslara ait elde edilen çağrı hareketlerine ilişkin kayıtlardan, kimlerin, ne zaman ByLock uygulaması üzerinden sesli iletişim kurduğunun tespiti yapılabilmektedir.

3.6.2.4"chat" tablosu:



Field	Type	Null	Key	Default	Extra
id	int(11)	NO	PRI	NULL	
fromUserId	int(11)	NO	MUL	NULL	
toUserId	int(11)	NO	MUL	NULL	
ciphertext	text	NO		NULL	
signature	varchar(512)	NO		NULL	
sentTime	timestamp	NO		CURRENT_TIMESTAMP	
receivedTime	timestamp	NO		0000-00-00 00:00:00	

8 rows in set (0.00 sec)

Şekil 5: Chat tablosunun alan adları ve özellikleri

"Chat" tablosu, uygulama vasıtasıyla gerçekleştirilen mesajlaşmalara ait bilgilerin saklandığı tablo olup, uygulamanın sohbet özelliği kullanılarak gönderilen her bir mesaj için; **mesajı gönderen kullanıcı**, **mesajı alan kullanıcı**, **mesajın şifreli hali**, **imza, mesajın gönderilme zamanı** ve **mesajın karşı tarafta okunma zamanı** bilgilerinin **"chat"** tablosunda saklandığı görülmüştür. **"chat"** tablosundan elde edilen verilerde toplam **17.169.632** kayıt bulunmaktadır.

Elde edilen 17.169.632 adet mesajlaşma içeriğinin tamamı kriptolu olarak veri tabanında saklanmakta olup, gerçekleştirilen çalışmalar neticesinde 15.520.552 adet mesajlaşmaya ait içerikler çözümlenmiştir. Mesajların çözümlenme işlemi devam etmektedir. Veri tabanında kriptolu olarak tutulan ve çözümlenen mesaj içeriklerine ait örneklere aşağıda yer verilmiştir:

Mesaj İçeriği Örneği 1

fromUserId	toUserId	ciphertext	sentTime	receivedTime
363824	344436	17 Aralık operasyonunda görevli oldugumdan dolayı 08/12/2015 günü gözaltına alındım. O sabah namazdan sonra hanım kahvaltı hazırladı. Kahvaltı yaptıktan sonra kapının zili çaldı. Beklenen bir durumdu kapıyı açtığımda polisler gelmişti. Şubeye gitmemiz gerektiğini söylediler. Ben hazirlandim çocuk uyuduğu için uyandirmadan öptüm hanımla vedalasirken bana "seni Rabbime emanet ediyorum Ondan geri istiyorum" dedi. Rahat bir şekilde kapıdan çıkarken bende Allaha emanet olun dedim ve beni alarak istanbula götürdüler. Gözaltında olduğumuz son gece hic uyumadik. Geceyi namaz ve duayla geçirdik. Özellikle Muhterem Hocamiza bol bol dua ettim. Sabahleyin savcılığa sevk olduk ve ben dahil tüm arkadaşlarım serbest kaldık. Rabbim emanetini geri gönderdi. Ben yokken eşim yatak odasında hiç uyumamis. Oturma odasinda uyurken uyku ile uyanıklik arası kapının açıldığını duymuş. Baktığında Hocamızın başında beyaz takkesi ve uzerinde kol ağızları işlemeli olan cubbesiyle evimizin içerisinde dolaştığını , hanima baktiktan sonra yatak odasına doğru gittiğini görünce hanım uyanık bir şekilde ayağa kalkarak Hocamızın gittiği istikamete bakıyor ama göremiyor ve o esnada sabah ezanı okunmaya başlıyor. Biz hocamızın ağzından çıkan her heceden emindik. Allaha Şükürler olsun ki Hocamızda bizden eminmis evimizi denetlemeye gelmiş. Abilerim Rabbim bizlerle beraber inşallah. Bunu gözaltindayken daha iyi anladım. Ne olur duaya devam edelim.	2015-12-12 19:21:27	2015-12-13 01:34:05

Mesaj İçeriği Örneği 2

fromUserId	toUserId	ciphertext	sentTime	receivedTime
73605	201087	abi bizim reis umreye gitti	2016-01-23 22:29:42	2016-01-24 04:29:46
73605	201087	uygur bosandi	2016-01-23 22:29:59	2016-01-24 04:30:03
73605	201087	vali bey uygurun karisi paralelci oldugu icin bosandigini soylemis	2016-01-23 22:31:02	2016-01-24 04:33:29
73605	201087	ayrica uygur emniyete benim paralelci oldugumu soylemis	2016-01-23 22:32:14	2016-01-24 04:33:29
73605	201087	emniyettekiler bana soyledi	2016-01-23 22:32:33	2016-01-24 04:33:29
73605	201087	bassavci izne gutti	2016-01-23 22:33:27	2016-01-24 04:33:32
73605	201087	suleyman bassavcivekili oldu	2016-01-23 22:33:56	2016-01-24 04:34:01
73605	201087	yarin gelin abi	2016-01-23 22:34:25	2016-01-24 04:34:31
73605	201087	daha cok var abi de	2016-01-23 22:34:34	2016-01-24 04:34:39
73605	201087	bize mi abi	2016-01-23 22:34:55	2016-01-24 04:35:00
73605	201087	onu bana kom sube muduru anlatti	2016-01-23 22:35:33	2016-01-24 04:36:13
73605	201087	savci mehmet ustun celik e getirmisler evraki	2016-01-23 22:36:13	2016-01-24 04:36:25
73605	201087	o da bassavcu ile gorudup	2016-01-23 22:36:23	2016-01-24 04:36:28
73605	201087	iade etmis	2016-01-23 22:36:28	2016-01-24 04:36:34
73605	201087	kom sube muduru omer koparam odama gelip bana anlatti	2016-01-23 22:37:03	2016-01-24 04:37:07
73605	201087	ne yapalim diyor bu sekilde evrak iade edilmesi dogru mu diyor	2016-01-23 22:37:48	2016-01-24 04:38:25
73605	201087	abi bassavci ,mehmet demirag, uygur meydan ,hasan reis onumuzdeki hafta yoklat	2016-01-23 22:39:05	2016-01-24 04:39:10
73605	201087	izne ayrildilar	2016-01-23 22:39:15	2016-01-24 04:39:20
73605	201087	suleyman kendini ispat etmek istiyor	2016-01-23 22:40:01	2016-01-24 04:40:06
73605	201087	abi bilerek ayrilmis olabilirler	2016-01-23 22:40:49	2016-01-24 04:42:27
73605	201087	emniyetle aralari yok operasyon icin suleyman istekli diye biliyirum	2016-01-23 22:41:19	2016-01-24 04:42:27
73605	201087	ok abi ben yarin goruseyim	2016-01-23 22:43:22	2016-01-24 04:44:33
73605	201087	abi bizim arkadaslardan birine tutuklamaya sevk ederlerse ne yapali	2016-01-23 22:45:06	2016-01-24 04:45:47
73605	201087	m	2016-01-23 22:45:07	2016-01-24 04:45:47
73605	201087	ok abi	2016-01-23 22:46:26	2016-01-24 04:46:50
73605	201087	abi yargitaya basvurayim mi	2016-01-23 22:46:46	2016-01-24 04:47:23

Mesaj İçeriği Örneği 3

fromUserId	toUserId	ciphertext	sentTime	receivedTime
56827	2637	gorusmek uzere	2015-12-20 21:58:24	2015-12-21 04:37:16
56827	2637	engec cuma gelir zannedersem	2015-12-23 20:50:50	2015-12-24 02:50:55
56827	2637	nasil intibak ettiniz mi	2015-12-23 20:51:17	2015-12-24 02:51:50
56827	2637	tunxay bey nerelerde	2015-12-23 20:51:36	2015-12-24 02:51:50
56827	2637	ayni bolgede misiniz	2015-12-23 20:51:48	2015-12-24 02:51:53
56827	2637	irtibatiniz devam ediyor mu	2015-12-23 20:52:16	2015-12-24 02:52:22
56827	2637	tuncay bey kisa surecekmis gibi hareketbetmesin kendisine is vaksin oralarda	2015-12-23 20:52:53	2015-12-24 02:54:19
56827	2637	bu serefsizler devrilsrler bile sacalarin sonuclanmasi o kadar kisa surnez	2015-12-23 20:53:30	2015-12-24 02:54:19
56827	2637	o yuzden 2 yil minimum disarida kalacak sekilde hareketvetnek lazim	2015-12-23 20:53:56	2015-12-24 02:54:19
56827	2637	sizde de eger disari kesin olursa oyke gormek lazim	2015-12-23 20:54:18	2015-12-24 02:54:22
56827	2637	vevtayin istemek lazim bosta jalmak cok sikunti cunku	2015-12-23 20:54:35	2015-12-24 02:54:51
56827	2637	tesekkurler abi, simdilik bize ozel bir problem yok. cunku memleketin tumu bir problem sarmalinda zaten.	2016-01-02 07:13:24	2016-01-02 18:55:33
56827	2637	su bahsettiginiz firmalarda istihdam ile ilgili bir gelime oldu mu	2016-01-02 07:13:59	2016-01-02 18:55:33
56827	2637	sa abi, yeni rektorunuz hayirli olsun	2016-01-16 23:20:52	2016-01-17 05:33:14
56827	2637	sa abi yaşıyormusun	2016-01-26 12:14:54	2016-01-26 14:28:55
56827	2637	durumun nedir	2016-01-26 12:14:59	2016-01-26 14:28:55
56827	2637	yapabileceğimz bir şey var mı	2016-01-26 12:15:11	2016-01-26 14:28:55
56827	2637	ya bosanan bir arkadasim uygun bir aday cikar mi	2015-10-31 19:06:28	2015-11-01 00:06:38
56827	2637	hizmetten akrabayi taalukat da olabilir	2015-10-31 19:07:03	2015-11-01 00:07:16
56827	2637	bu arkadasim brukselde yasiyor	2015-10-31 19:07:25	2015-11-01 00:07:31
56827	2637	eskiden serrehberdi, proje islerine bakiyordu hizmet firmani kur oradan bize faydali ol dedi	2015-10-31 19:08:07	2015-11-01 00:08:15
56827	2637	simdi iyi bir isadami bruksel ve antalyada 2 oteli var	2015-10-31 19:08:31	2015-11-01 00:08:35
56827	2637	yillik 100 bin euroya yakin himmet veriyor	2015-10-31 19:08:57	2015-11-01 00:09:30
56827	2637	74 lu	2015-10-31 19:09:07	2015-11-01 00:09:30
56827	2637	sapsari 178 boy 80 kg	2015-10-31 19:09:28	2015-11-01 00:09:32
56827	2637	eski esi ile kaynanadan dolayi bosandi	2015-10-31 19:09:49	2015-11-01 00:09:53
56827	2637	bu surecte tiranci da olunca artik dayanamadi	2015-10-31 19:10:04	2015-11-01 00:10:10
56827	2637	2 cocuk var annede kalacak gibi	2015-10-31 19:10:23	2015-11-01 00:10:28
56827	2637	konya taskent	2015-10-31 19:10:36	2015-11-01 00:11:06
56827	2637	birebir tanidiginiz veya esinizin tanidigi varsa yoksa luzum yok ugrasmayin	2015-10-31 19:11:28	2015-11-01 00:11:38
56827	2637	bosanmis ama hizmeti bilen bir bayanda olabilir	2015-10-31 19:11:51	2015-11-01 00:12:08

Mesaj İçeriği Örneği 4

fromUserId	toUserId	ciphertext	sentTime	receivedTime
222716	277794	Tamam bekliyoruz	2016-02-04 23:31:07	2016-02-05 05:31:47
222716	277794	Tamam	2016-02-04 23:46:12	2016-02-05 05:46:28
222716	277794	tamam insallah	2016-02-17 02:20:18	2016-02-17 08:22:32
222716	277794	onlara soyle hemen baslasinlar	2016-02-17 02:20:52	2016-02-17 08:22:32
222716	277794	Hamzaby bylok kaydet size sorulari olacak	2015-11-22 11:40:32	2015-11-22 17:45:19
222716	277794	Hamzaby (22.11.2015 10:08): cizrede bocekle ilgili:::1- bocekleri tespit eden kimdi 2- kactane bocek vardi ve hepsi gsm mi 3-boceklere elle dokunan oldumu 4-en son emniyetten ne zaman geldiler 5- kamera goruntuleri varmi? 6- prizler ve puvatlar kontrol edilde baska bocek varmi ama kesinlikle elle dokunulmasa...	2015-11-22 11:41:05	2015-11-22 17:45:19
277794	222716	izmir daha heyete sunmamış bekleyin dedi sonra m.beylere haber verin dedi	2016-01-26 22:41:01	NULL
277794	222716	az önce msj	2016-02-04 23:45:04	2016-02-05 05:46:06
277794	222716	pztes. kesin cevap vereceğiz dediler	2016-02-04 23:45:27	2016-02-05 05:46:06
277794	222716	arkadaşlar izinde olduğu için karar veremiyorlarmış	2016-02-04 23:46:27	2016-02-05 10:55:26
277794	222716	pzts kesin dedi	2016-02-04 23:46:53	2016-02-05 10:55:26
277794	222716	izmir olumsuz oldu.	2016-02-10 00:28:00	2016-02-10 12:11:29
277794	222716	izmir m.beye blg diyor eşinede abla olur diyor	2016-02-17 02:16:36	2016-02-17 08:20:11
277794	222716	ilçede abi varmiş	2016-02-17 02:16:59	2016-02-17 08:20:11
277794	222716	bende olur dedim.	2016-02-17 02:17:18	2016-02-17 08:20:11
277794	222716	ben izmire olur diye yazdım. aderi açık değildi bana dönsün hemen gönderelim. inş	2016-02-17 02:24:05	2016-02-17 11:46:49

Mesaj İçeriği Örneği 5

fromUserId	toUserId	ciphertext	sentTime	receivedTime
4380	49	abi Bulent beyin vizesi ile ilgili alternatifler arasinda sığınmacı olarak müracaat düşünecek miyiz.	2015-12-16 18:45:52	2015-12-17 00:47:38
4380	49	tamam abi. inş	2015-12-16 18:52:07	2015-12-17 00:52:10
4380	49	abi Suat Gözütok hoca burada kampta daha önceki yillarda olduğu gibi bir yukarıya ziyaret talep ediyordu. ayrica Kamil Şatır abi de buralarda onun da talebi vardı	2015-12-26 19:29:09	2015-12-27 01:33:01
4380	49	tamam abi söylerim onlara inş	2015-12-26 19:34:10	2015-12-27 01:43:17
4380	49	abi remzi abi tamam dedi ama ödemeyi nasil yapacagiz diyordu.	2015-12-31 00:19:38	2015-12-31 06:27:08
4380	49	abi bir web sitesi falan varsa oradan bilgileri alabiliriz diyordu remzi abi.	2015-12-31 00:58:56	2015-12-31 07:19:32
4380	49	tamam abi	2015-12-31 01:26:23	2015-12-31 07:26:31
4380	49	abi biz bir şekilde getirtmeye çalişalim inş	2016-01-01 08:07:26	2016-01-01 14:33:23
4380	49	diger arkadaşla ilgili de ben bir goruseyim inş abi. arkadaşın sıkıntılı olduğunu biliyordum. zaten orada başka sıkıntılar da var.	2016-01-01 08:08:26	2016-01-01 14:33:23
4380	49	Estağfurullah abi.	2016-01-01 08:34:19	2016-01-01 14:34:49
4380	49	faruk bey halloldu demisti demişti abi.	2016-01-01 08:35:45	2016-01-01 14:35:50
4380	49	abi malum büyüğümüz daha önce, gelirken bir iki kisiyi de getirirsin demişlerdi m gecen ay iptal ettirmistik biletleri. bu ay nasıl yapalım. bir iki kişi ye soyleyeyim mim ne buyurursunuz	2016-01-04 19:00:47	2016-01-05 01:03:26
4380	49	abi siz bilirsiniz. daha sonra biz insanların gidisine mani oluyormusuz gibi olmasın diye soruyorum.	2016-01-04 19:05:50	2016-01-05 01:06:05
4380	49	ben isimleri tesbit edip size bildiririm inş abi. siz yine de bilet aldırmadan once sorar mısınız	2016-01-04 19:07:37	2016-01-05 01:07:43
4380	49	tamam abi inş.	2016-01-04 19:09:11	2016-01-05 01:09:20
4380	49	ARO	2016-01-04 19:09:15	2016-01-05 01:09:20
4380	49	Abi müsait misiniz	2016-01-07 08:29:32	2016-01-07 19:49:19
4380	49	bu Yalçın bey yarın yukarı gidiyormuş. bir şekilde ayarlamış. bizden de gizliyor	2016-01-07 08:31:12	2016-01-07 19:49:19
4380	49	işin garibi bizim burada muhasebe kayıtlarını takip eden mali heyetteki bir arkadaşı da yanına almış.	2016-01-07 08:32:29	2016-01-07 19:49:19
4380	49	bilemiyorum büyüğümüz ile görüşmek ona birşeyler söylemek mi istiyorlar	2016-01-07 08:33:27	2016-01-07 19:49:19
4380	49	haber vereyim diye düşündüm	2016-01-07 08:34:15	2016-01-07 19:49:19
4380	49	bu arkadaşlar zaten hala kendi aralarında görüşmelere devam ediyor.	2016-01-07 08:34:48	2016-01-07 19:49:19
4380	49	abi bizim burada diyoga bakan arkadaşımızın hanımı yeni baro sınavını kazanıp avukatlik hakkını kazandı. New York'ta yemin törenleri varmış. acaba gitmişken günü birlik bir ziyaret mümkün mü diye soruyorlardı.	2016-01-08 01:34:59	2016-01-08 07:35:15
4380	49	20 çarşamba veya 22 cuma	2016-01-08 01:36:28	2016-01-08 07:36:40
4380	49	persembe yemin toreni varmış	2016-01-08 01:36:41	2016-01-08 07:36:46
4380	49	tamam abi ARO. isimlerini Birol beye mi ileteyim	2016-01-08 01:48:37	2016-01-08 07:49:03
4380	49	tamam abi.	2016-01-08 01:49:36	2016-01-08 07:49:50
4380	49	abi aradı görüştük 11inde beraber olacağız inş.	2016-01-08 02:47:30	2016-01-08 09:22:00
4380	49	abi bu arada Yalçın bey tek geliyormuş. Diğer arkadaş izin alamamış şirketinden. arkadaş bizim hesapları falan almış o muhasebeciden. korkum borclar ile ilgili büyüğümüze bir şeyler söyleyip moral bozması	2016-01-08 02:50:08	2016-01-08 09:22:00
4380	49	İnş abi	2016-01-08 03:28:31	2016-01-08 09:28:59
4380	49	İnş abi	2016-01-09 01:48:21	2016-01-09 07:48:42
4380	49	Abi cüneyt bey geldi. green kartını devam ettirmek için sömestr tatilini kullanarak ailecek geldiğini ve kimse ile görüşmediğini söyledi. bir kaç gün kalıp döneceğim dedi (yarın NY taraflarına gelip oradan dönecekmiş) bilgi vereyim dedim.	2016-01-22 03:30:13	2016-01-22 09:53:28
4380	49	evet abi size soylemiştim avukat eşi ile birlikte günü birlik . tamam demiştiniz.	2016-01-22 18:45:40	2016-01-23 00:45:59
4380	49	bizim buranın diyalogcusu	2016-01-22 18:45:53	2016-01-23 00:46:46

Mesaj İçeriği Örneği 6

fromUserId	toUserId	ciphertext	sentTime	receivedTime
1382	8605	MFTH mühendislere baksn fatih abinin by lock eklersen...	2015-11-03 14:08:48	2015-11-03 20:09:07
1382	8605	rasim bey i fuat beyle senin de olduğun bir yerde (yemek) tanıştıralım..fatih abi de olacak...fuat beyle görüsecektiniz...	2015-11-03 14:10:13	2015-11-03 20:10:29
1382	8605	tmm	2015-11-03 14:11:01	2015-11-03 20:11:06
1382	8605	gönderdiğin miktar neydi...hamza beyle	2015-11-12 14:53:58	2015-11-12 22:28:48
1382	8605	ben bunu nereye demiştim...jrton düşmedi	2015-11-12 16:29:25	2015-11-12 22:32:52
1382	8605	17500 o başka bir yere idi	2015-11-12 16:34:19	2015-11-12 22:34:29
1382	8605	düşüneyim	2015-11-12 16:34:25	2015-11-12 22:34:29
1382	8605	tmm	2015-11-12 16:35:35	2015-11-12 22:36:13
1382	8605	evet..şimdi bilgisayarsızlık daha tedbirsizlik	2015-11-12 16:37:48	2015-11-12 22:38:07
1382	8605	birde kullandığınız parmak flsh dersiniz.,zaten yakup biliyor	2015-11-12 16:38:23	2015-11-12 22:38:44
1382	8605	benim için gerek yok...sen bilirsin...2 saate çıkmayı düşünüyorum	2015-11-12 16:39:42	2015-11-12 22:40:09
1382	8605	olur	2015-11-12 16:44:57	2015-11-12 22:47:04
1382	8605	yarın ile ilgili dosyalar ne zaman geliyor...	2015-12-02 14:31:59	2015-12-02 20:32:16
1382	8605	bekliyorum	2015-12-02 14:33:37	2015-12-02 20:33:50
1382	8605	niye...	2015-12-09 17:15:49	2015-12-09 23:37:20
8605	1382	/33+Q4DllkOKZcTbEdMHJsBELFPGyPWHsxTU171CLZ+Fb7HER781JLJo7QrnkRutYQAbxQA+E+N4B5xMONI8OVKQklWhW5IQH7sP8jwsPYiaRjb...	2015-12-15 12:26:42	2015-12-15 18:31:36
8605	1382	/zvuq40NP+J15mEnvPn9qzRJmPJIA4izvBhV02V/f2BRl2GUj/ZiiPgR1hsBKXVr4dKu/s9qVNYadQGZxi/Uj5c3s8wJkmjfz3tU+GOxJjFY6e355Cb0gcae...	2015-12-15 12:33:41	2015-12-15 19:36:15
8605	1382	/zgCG1DzGLroCqfh9Tz8dRa9u3s+v4ZWMrnItPn3kUEMjKRnLkzwZxkhYMq9gARfSMneIkHtA5t6rLsvlQDxK2q8OpRQgZmiYDkkzXcXP4Ltxp/c2bpf...	2015-12-15 22:32:36	2015-12-16 04:40:59
8605	1382	/2nR4j+D00QUSw+7NIBGauolrNk/G0ih4l8oAe3UFYnj8dsMWLrbV+HFTtEtG+AOL3r9RtlJVdzCWWN1x3vDP2Ge/I0WfheFMPXUTue2wpzd+NbHL...	2015-12-15 22:42:22	2015-12-16 04:42:31

Yukarıdaki mesaj içeriklerindeki son dört satır, henüz çözümlenmemiş mesaj örneğidir. (Çözümleme çalışmalarına devam edilmektedir.)

3.6.2.5 "client" tablosu:

```
+-------------+--------------+------+-----+-------------------+-----------------------------+
| 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 (0.00 sec)
```

Şekil 6: client tablosunun alan adları ve özellikleri

"client" tablosunun uygulama geliştiricisi tarafından gerçekleştirilen kısa süreli teknik çalışmalarda kullanıldığı değerlendirilmektedir.

3.6.2.6 "exception" tablosu:

```
MariaDB [appDb]> show columns in 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     | text        | NO   |     | NULL    |       |
+-------------+-------------+------+-----+---------+-------+
5 rows in set (0.00 sec)
```

Şekil 7: exception tablosunun alan adları ve özellikleri

Uygulama kullanıcılarının karşılaştıkları yazılımsal hataların **"exception"** tablosunda saklandığı görülmüştür. Tabloda uygulamanın kullanımı sırasında karşılaşılan problemlere ilişkin kayıtlar yer almaktadır.

3.6.2.7 "file" tablosu:

```
MariaDB [appDb]> show columns in 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 (0.00 sec)
```

Şekil 8: file tablosunun alan adları ve özellikleri

"file" tablosunda, kullanıcıların birbirleri ile paylaştıkları dosyalara ait bilgilerin yer aldığı görülmüştür.

3.6.2.8 "file_transfer" tablosu:

```
MariaDB [appDb]> show columns in 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         | text         | 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 (0.00 sec)
```

Şekil 9: file_transfer tablosunun alan adları ve özellikleri

"file_transfer" tablosunda, transfer edilen dosyanın hangi kullanıcı tarafından (fromUserId), kime gönderildiği (toUserId), dosyanın gönderilme ve iletilme zamanı gibi bilgilerin saklandığı görülmüştür (Dosya bilgileri şifreli bir şekilde tutulmaktadır).

3.6.2.9 "group_member" tablosu:

groupId	userId
24	59
24	522
24	528
24	533
24	619
24	836
24	3984
25	312
25	365
25	444
25	566
26	53
26	112
26	296
26	101683

Şekil 10: group_member tablosuna ait örnek kayıtlar

"group_member" tablosunda, uygulama üzerinde kullanıcılar tarafından oluşturulan gruplarda (groupId), hangi kullanıcıların (userId) hangi grupta bulunduğu bilgisi yer almaktadır. Oluşturulan gruplarda yer alan şahıslara ait "Userid (Kullanıcı kodu)" bilgisi bu tabloda tutulmaktadır. "GroupId" olarak adlandırılan numara ile "User_group" tablosundaki Id sütunu eşleştirildiğinde oluşturulan grup isimlerine dahil olan şahıslara ait bilgiler elde edilebilmektedir. "User" tablosundaki Userid ile "group_member" tablosundaki Userid bilgisi eşleştirilerek ise aynı grupta yer alan şahıslara ait "Kullanıcı adı" bilgisi de elde edilebilmektedir. Toplamda 187.629 kayıt bulunmaktadır.

3.6.2.10 "user_group" tablosu:

id	Userıd	name
10087	202603	1.sosyal ekip
5253	31687	ABILER
9827	1157	adli grup
28073	85680	ahmet talha
28281	111201	Balikesir
26694	1443	BAYAN IZDVC
26821	136433	BEDRIN ASLANLARI
28106	1756	bilecik heyeti
28151	26130	Bolge Bayan
27282	1020	Dergici

26205	235480	DERSHANE
2665	1560	devreler
9722	183441	DNSTY - GRB
12191	142211	drgrubuankara
26315	203536	esnaf
2298	3792	hkk
9915	200800	il disi ogrenciler
27860	127098	ilçe bblm
27073	343230	ilçe mdr
27455	53714	koordine
27719	107144	kordinasyon
27233	154395	LISE GM
51319	121260	Manisa
27074	343230	merkez md
28410	72453	merkezi müdür mesul
11688	87555	mudur+zumre
26697	59407	MüdürDisB
27271	48208	prizma
28146	2529	Samsun Unv
7391	755	ÜNIV GM
28521	46519	ILÇE MESULLER
11631	3904	ISTISARE

Şekil 16: user_group tablosuna ait örnek kayıtlar

"user_group" tablosunda, hangi grubun hangi kullanıcı tarafından oluşturulduğu ve grubun isminin saklandığı görülmüştür. **"user_group"** tablosundan toplam **31.886** kayıt bulunmaktadır. "user_group" tablosu ilişkili olduğu diğer tablolar ile beraber değerlendirildiğinde oluşturulan gruplara hangi Userid ye sahip şahısların dahil olduğu bilgisi elde edilebilmektedir.

3.6.2.11 "log" tablosu:

```
MariaDB [appDb]> select * from log2 limit 50;
+----+--------+----------+----------------------------------+---------------------+----------------+----------------+----------+
| id | userId | actionId | sessionId                        | eventTime           | parameter1     | parameter2     | parameter3
+----+--------+----------+----------------------------------+---------------------+----------------+----------------+----------+
|  1 | 112695 |        8 | f04cac0db3b50a7f32f02e9078c05b42 | 2015-12-11 00:27:49 | 63.141.217.112 | ios            | 1.3-1
|  2 | 268729 |        8 | 9ef6a66b539c26d8bedfe769622c187a | 2015-12-11 00:27:49 | 109.237.27.253 | android        | 0.8-24
|  3 | 486035 |        8 | ad1103f9e70d7487f0de72c363aa9e3b | 2015-12-11 00:27:50 | 46.165.250.77  | android        | 0.8-24
|  4 |  62583 |        8 | 1f1fc6443b99da21f985cd1fe6163f5b | 2015-12-11 00:27:50 | 95.90.236.57   | android        | 0.8-24
|  5 | 414878 |        8 | ae381682883b087ab5ec6e40fc3a3304 | 2015-12-11 00:27:50 | 41.237.216.23  | android        | 0.8-24
|  6 | 344793 |        8 | b31c01ecc52d452be5685e6200f80a8d | 2015-12-11 00:27:50 | 212.71.237.37  | android        | 0.8-24
|  7 | 452815 |        8 | 2648bdde8154c8196742dd96e3b7cce6 | 2015-12-11 00:27:50 | 50.118.197.80  | android        | 0.8-24
|  8 | 342848 |        8 | 6c958252cc3d568b88eb00b686e335e0 | 2015-12-11 00:27:50 | 107.181.182.187| android        | 0.8-24
|  9 |  93105 |        8 | 325977fac965b961822f5cc23671b900 | 2015-12-11 00:27:50 | 69.31.50.104   | android        | 0.8-24
| 10 | 440155 |        8 | c4b1fa4ae1011880c76dc11f34ea3006 | 2015-12-11 00:27:51 | 105.196.74.28  | android        | 0.8-24
| 11 | 127494 |        8 | 653803a0460432e8e7bc880263dcb956 | 2015-12-11 00:27:52 | 188.165.245.164| android        | 0.8-24
| 12 | 231797 |        8 | 6965e072eed87c3ba52f3a458bc86117 | 2015-12-11 00:27:52 | 188.226.164.216| android        | 0.8-24
| 13 | 147531 |        8 | f6a833c15b7bf9d09733e46d362e42f0 | 2015-12-11 00:27:52 | 119.81.230.144 | ios            | 1.3-1
| 14 |  50402 |        8 | 922b59f35a97f173082d79dfdc9b6928 | 2015-12-11 00:27:52 | 46.101.201.244 | ios            | 1.2-1
| 15 | 324769 |        8 | 308341350f7856b7c7556d1f0cc9213e | 2015-12-11 00:27:52 | 50.118.197.55  | android        | 0.8-24
| 16 | 124458 |        8 | a7be7f6e3b2587c9af5b2444d001a700 | 2015-12-11 00:27:52 | 176.58.115.86  | android        | 0.8-24
| 17 | 210287 |        8 | ff93329e4b5f37274254c285b64a7a49 | 2015-12-11 00:27:52 | 85.159.214.107 | android        | 0.8-24
| 18 |      0 |       22 |                                  | 2015-12-11 00:27:52 | zeyne10        | 37.187.56.223  | android
| 19 | 372087 |        8 | 848c5b2871c0cdbb45de856fefbb9a39 | 2015-12-11 00:27:52 | 209.95.44.197  | android        | 0.8-24
| 20 | 398604 |        8 | 04bc7b09b17ead3ff08809c138699ec2 | 2015-12-11 00:27:52 | 88.80.188.144  | android        | 0.8-24
| 21 | 226069 |        8 | c2b4e26fad4f6139170d7a600d6eb987 | 2015-12-11 00:27:53 | 192.95.46.78   | android        | 0.8-24
| 22 | 229330 |        8 | bcdafbb3040d68e648ff4a187cb87e41 | 2015-12-11 00:27:53 | 78.214.29.62   | android        | 0.8-24
| 23 | 196951 |        8 | 29bcc6bf6f85354aa42d54e99fa9646c | 2015-12-11 00:27:53 | 37.187.57.151  | android        | 0.8-24
| 24 | 362465 |        8 | ff014adc9c9dc21bfed0fd2d7d4205e3 | 2015-12-11 00:27:53 | 151.236.221.64 | android        | 0.8-24
| 25 | 117491 |        8 | 740e0f8a3509b1a828e329ff341b4a52 | 2015-12-11 00:27:54 | 37.187.3.107   | android        | 0.8-24
| 26 | 460015 |        8 | 4f02c85a266596ff4e8f7d79276dc155 | 2015-12-11 00:27:54 | 192.95.25.76   | android        | 0.8-24
| 27 | 405993 |        8 | 7987e5c7ca42f7c16710ef34d19e7222 | 2015-12-11 00:27:54 | 107.182.226.40 | android        | 0.8-24
| 28 | 486908 |        8 | fa1a741451a32c38dd40f83dd25432c6 | 2015-12-11 00:27:55 | 69.31.50.186   | android        | 0.8-24
| 29 |      0 |       22 |                                  | 2015-12-11 00:27:55 | tekturkiye     | 85.203.19.87   | android
| 30 | 113049 |        8 | b3431ae570bf710ace4ae251204105dd | 2015-12-11 00:27:55 | 206.190.151.208| android        | 0.8-24
| 31 | 456814 |        8 | 2fda9745a4915589fbe4b056c3319402 | 2015-12-11 00:27:55 | 185.14.184.166 | android        | 0.8-24
| 32 | 342211 |        8 | 0bdbefb15bc2f85fb9249aa30cdd2cbf | 2015-12-11 00:27:56 | 95.211.206.221 | android        | 0.8-24
| 33 | 397780 |        8 | e862d060bc59f55d047cb48c0b50f928 | 2015-12-11 00:27:57 | 178.32.117.4   | android        | 0.8-24
| 34 | 361703 |        8 | f368a3f51b181bc5682f3d6e10112848 | 2015-12-11 00:27:57 | 216.185.39.178 | ios            | 1.3-1
| 35 | 452231 |        8 | 6a68144a6c1b1c4d6b5d6b7f578a97a8 | 2015-12-11 00:27:57 | 107.182.229.11 | ios            | 1.3-1
| 36 | 440803 |        8 | acaf4d3c15a2f25e7da68e1991832bf0 | 2015-12-11 00:27:57 | 66.228.57.54   | android        | 0.8-24
| 37 |      0 |       22 |                                  | 2015-12-11 00:27:57 | muhammed27     | 107.191.108.233| android
| 38 | 123861 |        8 | c51d5fc584e83f09ce810cb6046918bf | 2015-12-11 00:27:58 | 37.139.12.233  | android        | 0.8-24
| 39 | 463240 |        8 | 08aba677f48d6039bdfb2744d0bdc0be | 2015-12-11 00:27:58 | 46.101.10.91   | android        | 0.8-24
| 40 | 274396 |        8 | 111abf7028e5b5f0562819b005ee591c | 2015-12-11 00:27:58 | 168.235.80.45  | android        | 0.8-24
| 41 | 210773 |        8 | 05bde1995013f7072d1dd75e42cca3e6 | 2015-12-11 00:27:58 | 46.165.250.77  | android        | 0.8-24
| 42 |      0 |       22 |                                  | 2015-12-11 00:27:58 | adnn43         | 107.182.226.87 | android
| 43 | 186503 |        8 | d3e1e05301aae365fa6319dca8f07a2a | 2015-12-11 00:27:58 | 104.238.169.118| android        | 0.8-24
| 44 | 104517 |        8 | 0332fca64078783c3450895a5abdfb92 | 2015-12-11 00:27:59 | 107.182.228.69 | android        | 0.8-24
| 45 | 134908 |        8 | 374721a978c83485083da3d78d986ab1 | 2015-12-11 00:28:00 | 188.166.68.163 | android        | 0.8-24
| 46 | 437265 |        8 | 60c0287e998cc57a1c9e87cd1eca5228 | 2015-12-11 00:28:00 | 188.166.48.118 | android        | 0.8-24
| 47 | 140051 |        8 | c4e006c28d8bcfabd039fbbb9b215ac1 | 2015-12-11 00:28:01 | 178.62.37.116  | android        | 0.8-24
| 48 | 108409 |        8 | 32d643d88eafff870dfdff8b56fe4d88 | 2015-12-11 00:28:01 | 188.165.28.83  | android        | 0.8-24
| 49 | 468051 |        8 | c5ddb3a799689b819f84c17e034830e7 | 2015-12-11 00:28:01 | 209.95.35.113  | android        | 0.8-24
| 50 | 140924 |        8 | 24ce40dab83f9c0ec71238c8edf7940e | 2015-12-11 00:28:01 | 50.115.126.118 | android        | 0.8-24
+----+--------+----------+----------------------------------+---------------------+----------------+----------------+----------+
50 rows in set (0.00 sec)

MariaDB [appDb]>
```

Şekil 11: log tablosuna ait örnek kayıtlar

"log" tablosunda, uygulamaya ait log kayıtları tutulmaktadır. Parametreler "parameter" alanlarında kayıtlı verilerin hangi anlama geldiği bilgisi, **"action"** tablosunda saklandığı görülmüştür. **"action"** tablosundaki **"id"** alanı ile bu tablodaki **"actionId"** alanı eşleştirilerek parameter alanlarında kayıtlı veriler anlamlandırılabilmektedir.

Uygulamaya giriş işlemi olan **"Login"** ile uygulamaya kayıt olma işlemi olan **"Register"** işlemlerinde, kullanıcılara ait IP adres bilgilerinin de **"log"** tablosuna

kayıt edildiği görülmüştür. Bu veriler şahıs tespit işlemlerinde kullanılmıştır. Log tablosu uygulamayı kullanan şahısların sunucuda bırakmış oldukları izler olarak görülmektedir.

3.6.2.12 "mail" tablosu:

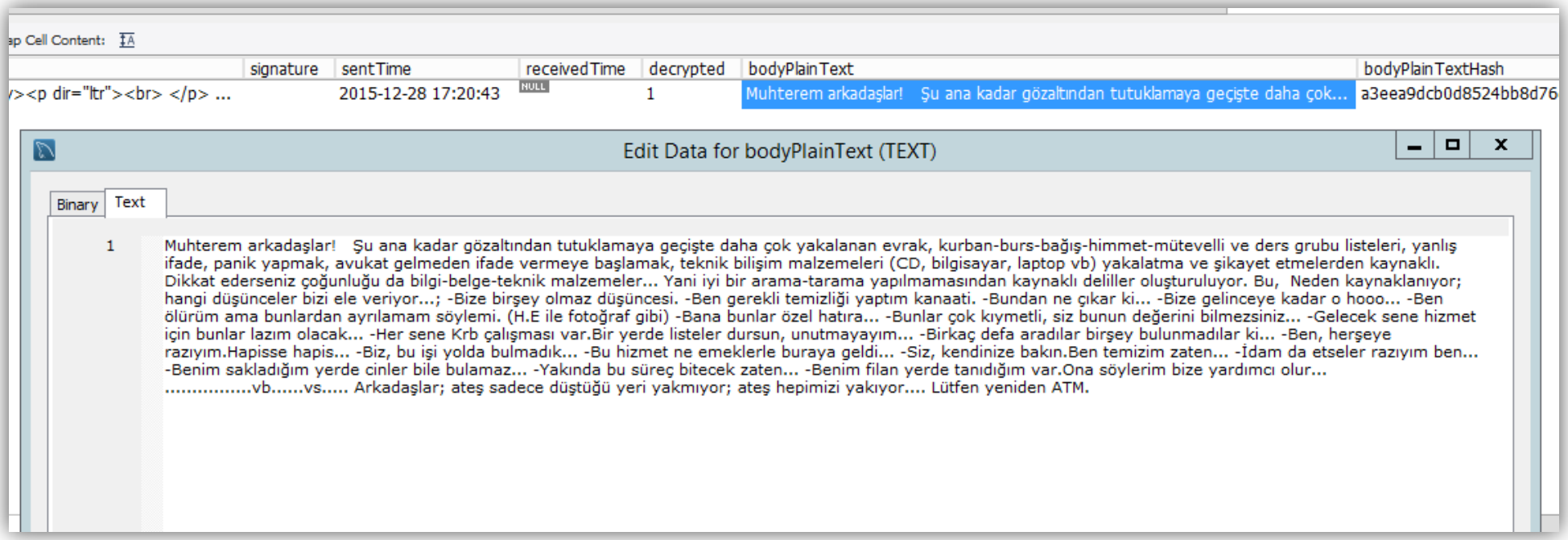
```
MariaDB [appDb]> show columns in mail;
+-----------------+--------------+------+-----+---------------------+-------+
| Field           | Type         | Null | Key | Default             | Extra |
+-----------------+--------------+------+-----+---------------------+-------+
| id              | int(11)      | NO   | PRI | NULL                |       |
| fromUserId      | int(11)      | NO   | MUL | NULL                |       |
| toUserId        | int(11)      | NO   | MUL | NULL                |       |
| otherRecipients | varchar(512) | YES  |     | NULL                |       |
| subject         | varchar(512) | YES  |     | NULL                |       |
| body            | text         | YES  |     | NULL                |       |
| signature       | varchar(512) | NO   |     | NULL                |       |
| sentTime        | timestamp    | NO   |     | CURRENT_TIMESTAMP   |       |
| receivedTime    | timestamp    | NO   |     | 0000-00-00 00:00:00 |       |
+-----------------+--------------+------+-----+---------------------+-------+
9 rows in set (0.00 sec)
```

Şekil 12: mail tablosunun alan adları ve özellikleri

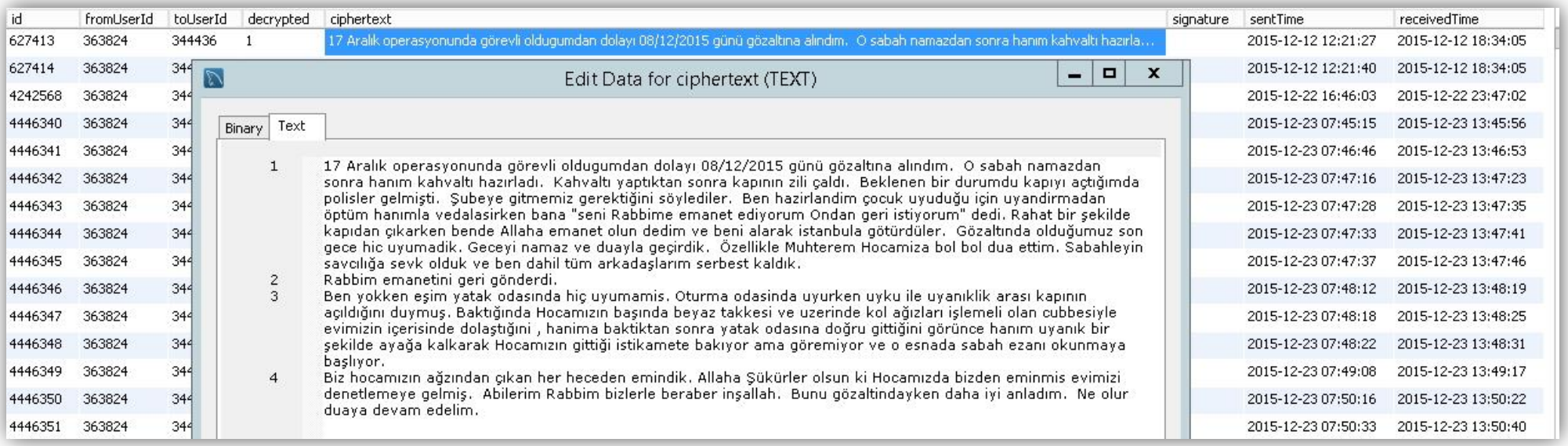
"mail" tablosu alan adları ve özellikleri ile **"chat"** tablosuna benzemektedir. Uygulamanın e-posta özelliği kullanılarak gönderilen her bir e-posta için; **e-postayı gönderen kullanıcı**, **e-postayı alan kullanıcı**, **e-postayı alan diğer kullanıcılar, konu, e-posta içeriğinin şifreli hali, imza, e-postanın gönderilme zamanı** ve **e-postanın gönderilen kişiye iletilme zamanı** bilgilerinin **"mail"** tablosunda saklandığı görülmüştür. Toplamda ulaşılabilen 3.158.388 adet e-posta içeriği kriptolu olarak bu tabloda saklanmaktadır. Gerçekleştirilen çalışmalar neticesinde 2.293.518 adet e-posta içeriği çözümlenmiştir. Çözümleme işlemi devam etmektedir.

"mail" tablosunda yer alan içeriklere ait örnek verilere aşağıda yer verilmiştir:

Eposta İçeriği Örneği - 1



Eposta İçeriği Örneği - 2



id	fromUserId	toUserId	decrypted	ciphertext	signature	sentTime	receivedTime
627413	363824	344436	1	17 Aralık operasyonunda görevli oldugumdan dolayı 08/12/2015 günü gözaltına alındım. O sabah namazdan sonra hanım kahvaltı hazırla...		2015-12-12 12:21:27	2015-12-12 18:34:05
627414	363824	344				2015-12-12 12:21:40	2015-12-12 18:34:05
4242568	363824	344				2015-12-22 16:46:03	2015-12-22 23:47:02
4446340	363824	344				2015-12-23 07:45:15	2015-12-23 13:45:56
4446341	363824	344				2015-12-23 07:46:46	2015-12-23 13:46:53
4446342	363824	344				2015-12-23 07:47:16	2015-12-23 13:47:23
4446343	363824	344				2015-12-23 07:47:28	2015-12-23 13:47:35
4446344	363824	344				2015-12-23 07:47:33	2015-12-23 13:47:41
4446345	363824	344				2015-12-23 07:47:37	2015-12-23 13:47:46
4446346	363824	344				2015-12-23 07:48:12	2015-12-23 13:48:19
4446347	363824	344				2015-12-23 07:48:18	2015-12-23 13:48:25
4446348	363824	344				2015-12-23 07:48:22	2015-12-23 13:48:31
4446349	363824	344				2015-12-23 07:49:08	2015-12-23 13:49:17
4446350	363824	344				2015-12-23 07:50:16	2015-12-23 13:50:22
4446351	363824	344				2015-12-23 07:50:33	2015-12-23 13:50:40

Edit Data for ciphertext (TEXT)

Binary | Text

1 17 Aralık operasyonunda görevli oldugumdan dolayı 08/12/2015 günü gözaltına alındım. O sabah namazdan sonra hanım kahvaltı hazırladı. Kahvaltı yaptıktan sonra kapının zili çaldı. Beklenen bir durumdu kapıyı açtığımda polisler gelmişti. Şubeye gitmemiz gerektiğini söylediler. Ben hazirlandim çocuk uyuduğu için uyandirmadan öptüm hanımla vedalasirken bana "seni Rabbime emanet ediyorum Ondan geri istiyorum" dedi. Rahat bir şekilde kapıdan çıkarken bende Allaha emanet olun dedim ve beni alarak istanbula götürdüler. Gözaltında olduğumuz son gece hic uyumadik. Geceyi namaz ve duayla geçirdik. Özellikle Muhterem Hocamiza bol bol dua ettim. Sabahleyin savcılığa sevk olduk ve ben dahil tüm arkadaşlarım serbest kaldık.

2 Rabbim emanetini geri gönderdi.

3 Ben yokken eşim yatak odasında hiç uyumamis. Oturma odasinda uyurken uyku ile uyanıklik arası kapının açıldığını duymuş. Baktığında Hocamızın başında beyaz takkesi ve uzerinde kol ağızları işlemeli olan cubbesiyle evimizin içerisinde dolaştığını , hanima baktiktan sonra yatak odasına doğru gittiğini görünce hanım uyanık bir şekilde ayağa kalkarak Hocamızın gittiği istikamete bakıyor ama göremiyor ve o esnada sabah ezanı okunmaya başlıyor.

4 Biz hocamızın ağzından çıkan her heceden emindik. Allaha Şükürler olsun ki Hocamızda bizden eminmis evimizi denetlemeye gelmiş. Abilerim Rabbim bizlerle beraber inşallah. Bunu gözaltindayken daha iyi anladım. Ne olur duaya devam edelim.

3.6.2.13 "roster" tablosu:

id	FromUserid	ToUserid	Nickname
1614883	25434	13690	yasin komser
369601	15882	88327	Albay
577245	170895	57572	albay133
1599444	349749	359042	zalbay
2127968	1185	467	yousuf albay
2369838	404376	378741	aalbay
1212882	121371	189573	yarbay
775159	8781	9891	4006 pilot karma
1372304	183366	84121	pilot abi
1809484	22189	402862	pilot3163
311151	852	46512	Fatih Yigit Komiser delikanlii
1209224	269043	152142	M.Akif Baskomiser
1223777	269043	1820	Ismail Baskomiser
1496338	248855	280030	Coskun komiserim
953721	54855	183982	ank900ara faik hsyk
1757555	151879	113586	tarsus fatih hsyk
1528960	202	343151	Halil Bey Kuvvet Asker
121697	48277	25921	farukhakim
2509336	472645	411050	savci20
2527154	513677	411050	savci
214579	50600	14396	Hakim a
369678	2019	14396	kayshakim
502138	153432	114772	hakim bey
838090	35441	25921	faruk hakim
1324263	211131	320752	Hakim Rakipi
1491175	347869	348172	Lukmanul hakim
2378077	27520	493923	hakim hoca

1963375	247967	111715	izmir krfz genel mudur hakki
2002545	247967	212333	sehzade mehmet ilk okulu muduru
2030074	247967	204116	aydinlik kolej muduru suleyman
2183272	247967	227925	afyon dersaneler genel muduru
2234374	247967	404312	yamanlar personel muduru
2284118	247967	258443	gaye koleji muduru
1459232	198273	91598	IZDIVAC MESULU
1485582	41937	221517	Bartin Mezun Mesulu
1548773	252699	157533	Ahmet tnzya mesul
1902440	61414	152800	Fatih-Avukat mesulu
2061472	103819	43229	Fatih hukuk izm mesul
2101795	15701	113492	Bornova iletisim k. mesulu
2433830	493512	431708	livane0808 Dr mesulü mrt
2494689	455475	415386	Tarik mesul
2515420	74717	234956	usak univ mesul
2553409	74717	102163	antalya 03 mesul
1015970	62153	107144	Burak Egitim Abi Sorumlusu
1287653	74717	96040	antalya mucahit lise sorumlu
2336240	402417	130327	Turgutlu sorumlusu elif
2402531	402417	424228	manisa sorumlusu Dicle hnm
2526470	402417	239789	denizli Sorumlusu ahsen hoca

Şekil 13: roster tablosuna ait örnek kayıtlar

"roster" uygulamaya ait rehber bilgilerinin saklandığı tablodur. Bu tabloda, hangi kullanıcının, hangi kullanıcıyı, uygulama rehberine (telefon rehberi değildir) hangi isimle kaydettiği bilgisinin saklandığı görülmüştür. ByLock uygulamasını kullanan şahıs, "Kullanıcı Adı" ile bir arkadaşını uygulamada ekledikten sonra, kendi rehberinde eklediği kişinin isim bilgisini yeniden düzenleyebilmektedir. (Örn. "Kullanıcı Adı" "100" olan kişi, "Kullanıcı Adı" "500" olan kişiyi rehberine ekledikten

sonra, rehberinde "500" kodlu kişinin adını "Orhan A" olarak kaydetmiştir). **"roster"** tablosundan elde edilen verilerde toplam **1.350.624** kayıt bulunmaktadır.

3.6.2.14 "setting" tablosu:

```
MariaDB [appDb]> 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 (0.01 sec)
```

Şekil 14: setting tablosuna ait örnek kayıtlar

"setting" tablosunda, uygulama sunucusu çalışırken kullanılan bazı teknik parametrik değerlerin saklandığı görülmüştür.

3.6.2.15 "user" tablosu:

```
MariaDB [appDb]> show columns in user;
+-----------------+-------------+------+-----+---------------------+-----------------------------+
| Field           | Type        | Null | Key | Default             | Extra                       |
+-----------------+-------------+------+-----+---------------------+-----------------------------+
| id              | int(11)     | NO   | PRI | NULL                |                             |
| username        | varchar(32) | NO   |     | NULL                |                             |
| plain           | varchar(32) | NO   | MUL | 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 |                             |
+-----------------+-------------+------+-----+---------------------+-----------------------------+
12 rows in set (0.00 sec)
```

Şekil 15: user tablosunun alan adları ve özellikleri

"user" tablosunda, Kullanıcı Adı, kullanıcı şifresi (**md5 kriptografik özeti**), **RSA Sertifika bileşenleri,** kullanıcının oluşturulma tarihi ve en son giriş yapma tarihi

gibi bilgilerin tutulduğu görülmüştür. Bu tabloda aynı zamanda kullanıcının kendine özel **RSA kriptografik anahtar setinin gizli anahtarı (privateExponent)** mevcuttur. **privateExponent** bileşeninin tabloda kriptolu bir şekilde saklandığı görülmüştür.

"user" tablosunda toplam 215.092 kayıt bulunmakta olup, uygulama kullanıcılarının kullandıkları parolalar kriptolu bir şekilde saklanmıştır. Gerçekleştirilen çalışmalar neticesinde 184.298 şahsa ait parola bilgisi çözümlenmiştir. User tablosunda yer alıp deşifre edilen verilere ilişkin örneklere aşağıda verilmiştir: ("**username**" bilgisi kullanıcı adına/koduna, "**plain**" bilgisi ise yürütülen çalışmalar neticesinde çözümlenmiş kullanıcı şifresine işaret etmektedir.)

Kullanıcı Adı/Kodu ve Çözümlenmiş Şifre Örneği – 1

username	plain
10001	qwertyuiopasdfghjkl"
bahadir5959	qazwsxedcrfvtgb1234$
umudumsun	qwertyuiop1234567890-
adem999	asdfghjkl1234567890*.
tlh34	poiuytrewq1234567890.
yusuf2763	qwertyuiop0987654321.
melih63	qwertyuiop.1234567890
ender63	1234567890qwertyuiop.
Ahmetahir26	0123456789987654321a.
sinan20	1234567890qwertyuiop.
serkan6363	qwertyuiop1234567890.
sinand	1234567890qwertyuiop.
akifaltnzde2	olmakyadaolmamak1234.
haktat	1234567890qwertyuiop.
incredible06	insansizhavaaraci2006
cihan6403	qwertyuiop1234567890.
istanbul61	istanbulistanbul2001.
adem2015	q1w2e3r4t5y6u7i8o9p0.
34talha34	qwertyuiop1234567890.
mcht2015	qwertyuiop.1234567890
13muhacir12	poiuytrewq1234567890.
serdar6342	qwertyuiop1234567890.
sinanecz	qwertyuiop0987654321.
ablak63	0987654321qwertyuiop.
05721537	1234567890987654321h*
ilkera	qwertyuiop1234567890.
fth63	qwertyuiopasdfghjkl1.
efekentli48	a123456789987654321z,
mustafabakir	qwertyuiop0987654321.
eczserdar	qwertyuiop0987654321.
fetih061453	poiuytrewq1234567890.
ismail2009	qwertyuiop0987654321.
mcebisli63	qwertyuiop1234567890!
cem05	1234567890@qwertyuiop
selo1	tedbirieldenbirakma.01
gazanfer0232	qaz[ç©ºæ ¼]wsx[ç©ºæ ¼]
haticeyurekdeler	aaaaaaaaaaaaaaaaaaaa1&
evren25	evrenartut@hotmail.com
gazanferr	qaz[ç©ºæ ¼]wsx[ç©ºæ ¼]
Nataniel	qwertyuiop1234567890@#$
lkmn34	asdfghjkl1234567890.....

Kullanıcı Adı/Kodu ve Çözümlenmiş Şifre Örneği – 2

username	plain
suleman	1234567890asdfghjkL
S1357	asdfghjkl.123456789
bedir313	fatihsultanmehmet7%
fatmaolmez	123456!@#fatmaolmez
S9876	asdfghjkl.123456789
neyzen19	asdfghjkl!@#$%&+?/.
Yildirim5252	Yildirim1234567890.
ibrahimtosun	i_tosun@hotmail.com
gonulkrdnz061	gonulkaradeniz@@@@@
zeynel78	123456789.kara.anka
smurat	Murat2008Murat2008.
Sierra	qwertyuioplmnbvcxza
smha	seni.seviyorum.1989
Aykut12	234567890asdfghjkl.
snh34	istanbulistanbul.34
Yildirim111	Yildirim1234567890.
kenan046	Bugunlerdegececek1.
cihangirdaloglu	cihangircihangir29.
tuyetlinh	tuyetlinh@gmail.com
camilabastiel	chocolate123456789.
500269	Yildirim1234567890.
Numan111	qweasd123.qweasd123
asdfghzxc	qawsedrftgyhuj1234.
Allim0671	qwertgfdsa1234554321
serdargul	serdar.gul1234567890
AYKUT12	1234567890asdfghjkl.
123123123123123123	1231231231231231a/
honda0101	123456789.poiuytrewq
ensaaaarrr0015	asdfghjkl.1234567890
newbutold	icisenidisibeniyakar
bydoktortarik	qawsedrftgyhujikolp.
Allim	1234567890poiuytrewq
akifaltnzde	olmakyadaolmamak123.
Davud44	Qazwsxedc1234567890.
davud500217	Qazwsxedc1234567890.
efendi	1234567890Asdfghjkl.
59bahadir	qazwsxedcrfvtgb1462$
59bahdir	qazwsxedcrfvtgb1452$
serdar63	1234567890asdfghjkl.
sanliurfa63	1234567890asdfghjkl.
imrance58	fatmacelik123456789.

3.7 ByLock Uygulamasına Ait İstatistiki Veriler

Tespit	**Sayı**
Uygulamaya Kayıt Olan Kullanıcı Sayısı	215.092
Parolası Çözümlenebilen Kullanıcı Sayısı (Çözümleme İşlemi Devam Etmektedir.)	184.298
Uygulamada Oluşturulmuş Toplam Grup Sayısı	31.886
Uygulamadaki Toplam Mesaj İçeriği (Gönderilen ve Alınan Bütün Mesajlar)	17.169.632
Çözümlenen Mesaj İçeriği (Çözümleme İşlemi Devam Etmektedir.)	15.520.552
Uygulama Verilerindeki Toplam E-Posta İçeriği	3.158.388
Çözümlenen E-Posta İçeriği (Çözümleme İşlemi Devam Etmektedir.)	2.293.518
Bylock Uygulamasında En Az 1 Kez Mesaj Atmış ve/veya Almış Şahıs Sayısı	60.473
Uygulamadaki Sesli Görüşmeyi Kullanan Şahıs Sayısı	78.165
Uygulamayı Sadece Sesli İletişim İçin Kullanan Şahıs Sayısı	46.799

Ayrıca çözümlenen şifrelere ilişkin istatistiki veriler Ek-11'de sunulmuştur.

4.DEĞERLENDİRME ve SONUÇ

ByLock uygulaması, tersine mühendislik, kripto analiz, ağ davranış analizi ve bağlantı kurulan sunucular tarafından cevap veren kodlar da dahil olmak üzere detaylarına yukarıda yer verilen ayrıntılı teknik çalışmalara tabi tutulmuş olup, aşağıda yer verilen sonuç ve değerlendirmelere ulaşılmıştır:

1- ByLock uygulamasının, güçlü bir kripto sistemiyle internet bağlantısı üzerinden iletişim sağlamak üzere, gönderilen her bir mesajın farklı bir kripto anahtarı ile şifrelenerek iletilmesine dayanan bir tasarıma sahip olduğu görülmüştür.

2- Uygulamayı geliştiren ve kullanıma sunan şahsın,

- Daha önce yaptığı işlere ilişkin referanslarının bulunmadığı,
- Sektördeki geçmişinin belirsizlik arz ettiği,
- Erişilebilir iletişim bilgilerinin bulunmadığı,
- Gerçekleştirilen iş ve işlemlere (sunucu ve IP kiralama) ait ödemelerin anonimlik içeren yöntemlerle (Paysera) gerçekleştirildiği,
- Kullanıcı sayısını artırmayı ve ticari değer haline gelmeyi hedeflemediği,
- Uygulamanın tanıtılmasına yönelik girişimlerin bulunmadığı

görülmüştür.

Diğer taraftan, uygulamanın Litvanya'da sunucu kiralanmak suretiyle kullanıma sunulması ve kiralama bedellerinin ise "Paysera" adlı anonimlik sağlayan ödeme sistemiyle gerçekleştirilmiş olması, **bu girişimin kurumsal ve ticari mahiyetinin bulunmadığını** teyit etmektedir.

Kaldı ki,

- Uygulamaya ait kaynak kodları içerisinde bir takım "Türkçe" ifadelerin yer alması,
- Kullanıcı adlarının, grup isimlerinin ve çözümlenen şifrelerin büyük çoğunluğunun Türkçe ifadelerden oluşması,
- Çözümlenen içeriklerin neredeyse tamamının Türkçe olması,

- Uygulama sunucusu yöneticisinin, Ortadoğu IP adreslerinden uygulamaya erişimi engellediğini belirtmesine rağmen, gerçekleştirilen engellemelerin tamamına yakının Türkiye IP adreslerine yönelik olması,
- Türkiye'den erişim sağlayan kullanıcılara ait kimlik bilgilerinin ve iletişimin gizlenmesini sağlamak amacıyla kullanıcıların uygulamaya erişimini, VPN vasıtasıyla gerçekleştirilmesine zorlanması,
- Bunun yanı sıra, ByLock'a ilişkin "Google" üzerinden gerçekleştirilen aramaların neredeyse tamamının Türkiye'deki kullanıcılar tarafından gerçekleştirilmesi ve uygulamaya Türkiye IP adreslerinden erişimin engellendiği tarih itibariyle uygulamaya yönelik "Google" aramalarında büyük bir artış olması,
- Ayrıca, ByLock'la ilişkili internet kaynaklı yayınların (sosyal medya, web siteleri vb.), çoğunlukla sahte hesaplar üzerinden FETÖ/PDY lehine paylaşımlarda bulunulması,
- İki yüz bini aşkın kullanıcı kitlesine sahip ByLock'un "15 Temmuz Darbe Girişimi" öncesinde ne Türk kamuoyu ne de yabancılar tarafından bilinmemesi/tanınmaması

hususları birlikte değerlendirildiğinde, **anılan uygulamanın global bir uygulama maskesi altında, FETÖ/PDY mensuplarının kullanımına sunulduğu** anlaşılmıştır.

3- Uygulamanın akıllı telefonlara yüklendikten sonra kullanılabilmesi için kullanıcı adı/kodu ve parolanın, akabinde cihaz üzerinde rastgele el hareketleriyle oluşturulan kullanıcıya özel güçlü bir kriptografik şifrenin belirlenmesi ve bu bilgilerin uygulama sunucusuna kriptolu olarak iletilmesi işlemleriyle, **kullanıcı bilgilerinin ve iletişimin güvenliğinin azami şekilde korunmasının amaçlandığı** görülmektedir.

Diğer taraftan, kullanıcı hesabı oluşturulması sırasında kişiye ait özel bir bilginin (telefon numarası, kimlik numarası, e-posta adresi vb.) talep edilmemesi, global ve ticari benzer uygulamalarda olduğu şekilde kullanıcı hesabını doğrulamaya yönelik bir işleyişin (sms şifre doğrulaması, eposta doğrulaması vb.) bulunmamasının esaslı

sebebinin, **anonimliğin sağlanması ve kullanıcı tespitinini zorlaştıracak önlemlerin kurgulanması**ndan kaynaklandığı değerlendirilmiştir.

4- Uygulama geliştiricisinin, otorite imzalı SSL sertifikası kullanmadığı, kendi oluşturduğu bir SSL sertifikasını kullandığı tespit edilmiştir. Ancak global ve ticari anlık mesajlaşma uygulamalarının "otorite imzalı SSL sertifikası" kullandığı, bununla kullanıcı bilgilerinin ve iletişim güvenliğinin sorumluluğunu ücreti mukabilinde bu otoriteye bıraktığı bilinmektedir. ByLock uygulamasında ise, uygulama geliştiricisinin, kullanıcılara ait bir takım bilgilerin sertifika otoritesine gitmesini istememesi nedeniyle "otorite imzalı SSL sertifikası"nı tercih etmediği değerlendirilmektedir. Uygulama geliştiricisinin sistem, işleyiş, kullanıcı güvenliği bakımından aldığı diğer önlemler de nazara alındığında, kullanıcılara ait haberleşme trafiğinin kendi uygulama sunucusu harici bir noktaya akışını engelleyen ilave bir önlem olarak tasarladığı görülmektedir.

5- Uygulamaya kayıt işleminin, sistemde kayıtlı kullanıcılarla iletişim kurmak için yeterli olmaması, iki kullanıcının haberleşmesi için her iki tarafın, çoğunlukla yüz yüze veya bir aracı (kurye, mevcut ByLock kullanıcısı üzerinden vb.) vasıtasıyla temin edilen kullanıcı adlarının/kodlarının eklemesinin gerekmesi; mesajlaşmanın, her iki kullanıcının da birbirini eklemesinden sonra başlatılabilmesi sebebiyle **haberleşmenin, sadece oluşturulan hücre tipine uygun şekilde gerçekleştirilmesine imkan verecek şekilde kurgulandığı** değerlendirilmiştir.

6- Uygulama üzerinden sesli arama, yazılı mesajlaşma, e-posta iletimi ve dosya transferi gerçekleştirilebilmektedir. Bununla, kullanıcıların **örgütsel mahiyetteki haberleşme ihtiyaçlarının, başka herhangi bir haberleşme aracına ihtiyaç duyulmadan gerçekleştirildiği** ve tüm iletişim sunucu üzerinden geçtiğinden oluşturulan grupların ve haberleşme içeriklerinin uygulama yöneticisinin denetim ve kontrollerinde olmasını sağladığı değerlendirilmiştir.

7- Gerçekleştirilen haberleşmenin, cihaz üzerinden **belirli sürelerde manuel işleme gerek duymaksızın otomatik olarak silinmesi**, kullanıcıların, haberleşme güvenliği bakımından silmeleri gereken verileri silmeyi unutsa dahi sistemin gerekli tedbirleri alacak şekilde tasarlandığını göstermektedir. Böylece ByLock

uygulamasının, **olası bir adli işlem neticesinde cihaza el konulması durumunda dahi uygulamada yer alan kullanıcı listesindeki diğer kullanıcılara ve uygulamadaki haberleşmelere ilişkin geçmiş verilere erişimi engelleyecek şekilde kurgulandığı** değerlendirilmiştir. Ayrıca, uygulamaya ait sunucu ve iletişim verilerinin, uygulama veri tabanında kriptolu olarak saklanmasının, kullanıcı tespitinin önlenmesi ve haberleşme güvenliği için alınan ilave güvenlik tedbiri mahiyetinde olduğu değerlendirilmiştir.

8- Kullanıcıların kendilerini gizlemek amacıyla;

- Çok uzun haneli parola belirlediği, örneğin çözümü tamamlanan veriler arasında **38 haneye varan parolaların yer aldığı** ve çözümü tamamlanan **parolaların yarısından fazlasının 9 hane ve üzerinde** karakter içerdiği,
- Belirli bir tarihten sonra uygulamanın Android Market veya Apple AppStore'dan indirilmesi yerine, kullanıcıların cihazlarına manuel olarak yüklendiği,
- Uygulamaya kayıt esnasında gerçek isimlerin "Kullanıcı Adı" olarak belirlenmediği,
- Haberleşme içeriklerinde ve uygulamadaki arkadaş listelerinde kişilerin gerçek bilgileri yerine örgüt içerisindeki kod adlarına yer verildiği

görülmüştür. Elde edilen ve çözümleme işlemleri tamamlanan **mesajlaşma içeriklerinin tamamına yakınının FETÖ/PDY unsurlarına ait örgütsel temas ve faaliyetleri içerdiği** ve örgüte ait jargonla örtüştüğü görülmüştür.

9- FETÖ/PDY unsurlarınca gerçekleştirilen 15 Temmuz 2016 askeri darbe girişimi sonrasında adli kontrol işlemlerine (gözaltı, tutuklama, yakalama vb.) tabii tutulan örgüt mensuplarının ifadelerinden, 2014 yılının başlangıcında FETÖ/PDY örgüt üyeleri tarafından örgütsel haberleşme aracı olarak kullanıldığı anlaşılmıştır.

Yukarıda izah edilen durumların hepsi birlikte değerlendirildiğinde, ByLock uygulamasının, global bir uygulama görüntüsü altında münhasıran **FETÖ/PDY terör örgütü mensuplarının kullanımına sunulduğu** sonucuna ulaşılmıştır.

5.EKLER

Ek-1: ByLock Uygulamasının Versiyon Tarihleri

Ek-2 ByLock Uygulamasının Google Play'den Yaklaşık İndirilme Sayısı

Ek-3: Bylock Sunucusuna Ait Sertifikanın Ekran Görüntüsü

Ek-4: ByLock Sunucusu IP Adreslerine İlişkin virustotal.com Sorgusu

Ek-5: Kaynak Kodlarda Geçen Türkçe İfadeler

Ek-6: İstemci Kaynak Kodlarında Geçen Kriptografik Algoritmalar

Ek-7: Kayıt ve İki Kullanıcı Arasındaki Şifreli Mesajlaşmaya Ait Akış Şeması

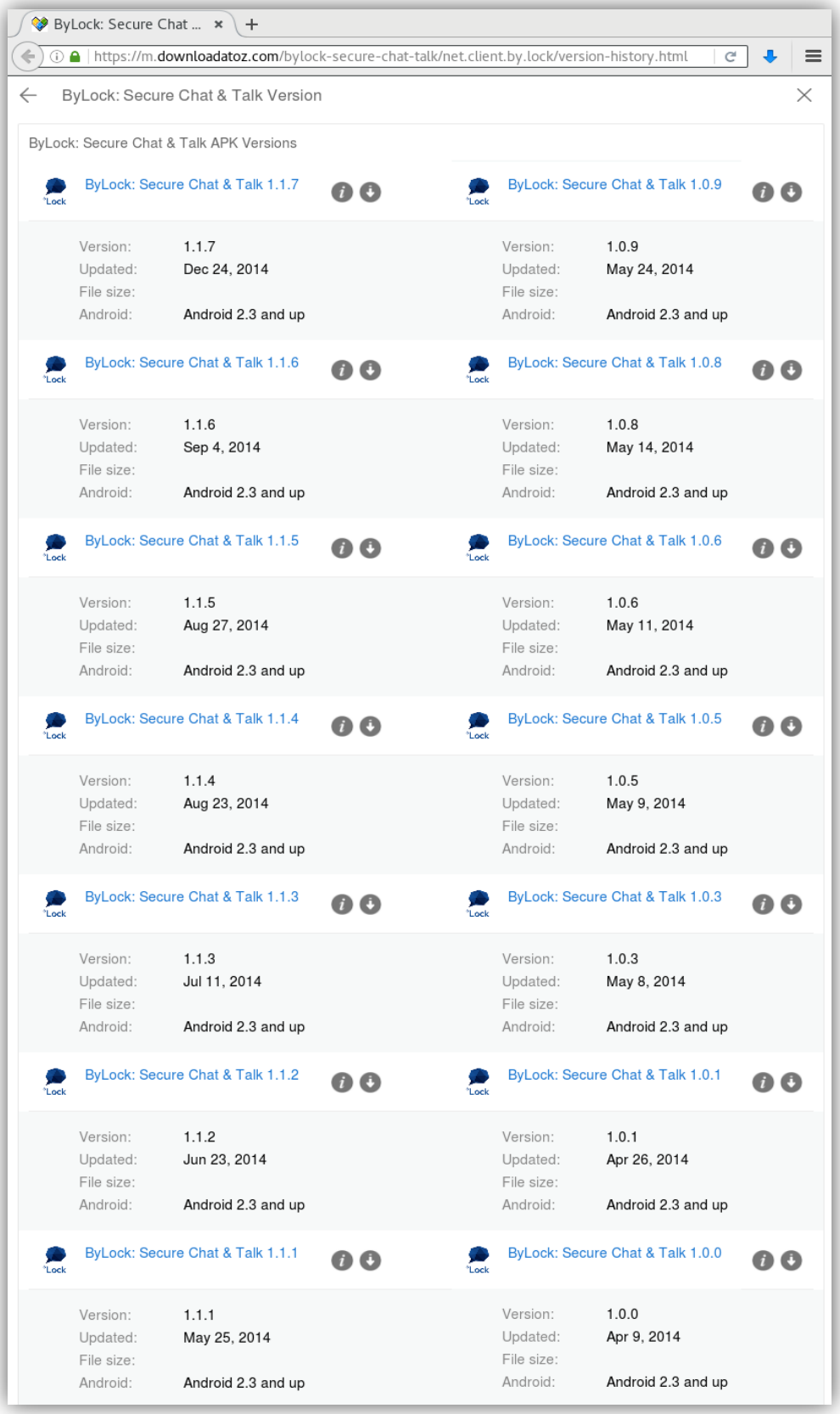
Ek-8: Uygulama Sunucusu Yazılım Modelleri

Ek-9: Uygulaman Sunucusunda Çalışan Yazılımda Rastlanan Türkçe İfade

Ek-10: Uygulama Sunucusunda Engellenen IP Adresleri Listesi

Ek-11: Çözümlenen Şifrelere İlişkin İstatistiki Veriler

Ek-1: ByLock Uygulamasının Versiyon Tarihleri



ByLock: Secure Chat ...

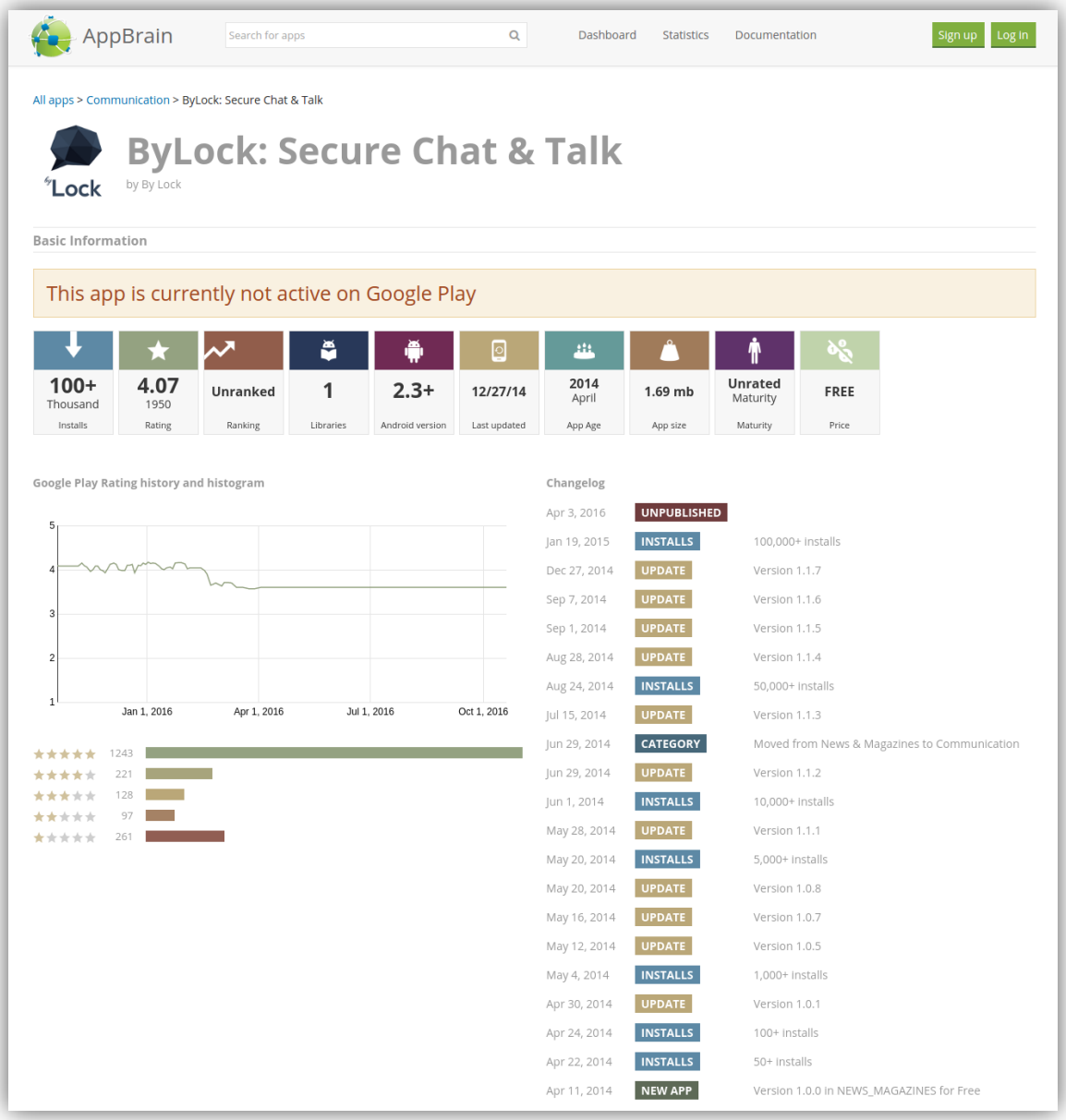
https://m.downloadatoz.com/bylock-secure-chat-talk/net.client.by.lock/version-history.html

ByLock: Secure Chat & Talk Version

ByLock: Secure Chat & Talk APK Versions

ByLock: Secure Chat & Talk 1.1.7		ByLock: Secure Chat & Talk 1.0.9	
Version:	1.1.7	Version:	1.0.9
Updated:	Dec 24, 2014	Updated:	May 24, 2014
File size:		File size:	
Android:	Android 2.3 and up	Android:	Android 2.3 and up
ByLock: Secure Chat & Talk 1.1.6		ByLock: Secure Chat & Talk 1.0.8	
Version:	1.1.6	Version:	1.0.8
Updated:	Sep 4, 2014	Updated:	May 14, 2014
File size:		File size:	
Android:	Android 2.3 and up	Android:	Android 2.3 and up
ByLock: Secure Chat & Talk 1.1.5		ByLock: Secure Chat & Talk 1.0.6	
Version:	1.1.5	Version:	1.0.6
Updated:	Aug 27, 2014	Updated:	May 11, 2014
File size:		File size:	
Android:	Android 2.3 and up	Android:	Android 2.3 and up
ByLock: Secure Chat & Talk 1.1.4		ByLock: Secure Chat & Talk 1.0.5	
Version:	1.1.4	Version:	1.0.5
Updated:	Aug 23, 2014	Updated:	May 9, 2014
File size:		File size:	
Android:	Android 2.3 and up	Android:	Android 2.3 and up
ByLock: Secure Chat & Talk 1.1.3		ByLock: Secure Chat & Talk 1.0.3	
Version:	1.1.3	Version:	1.0.3
Updated:	Jul 11, 2014	Updated:	May 8, 2014
File size:		File size:	
Android:	Android 2.3 and up	Android:	Android 2.3 and up
ByLock: Secure Chat & Talk 1.1.2		ByLock: Secure Chat & Talk 1.0.1	
Version:	1.1.2	Version:	1.0.1
Updated:	Jun 23, 2014	Updated:	Apr 26, 2014
File size:		File size:	
Android:	Android 2.3 and up	Android:	Android 2.3 and up
ByLock: Secure Chat & Talk 1.1.1		ByLock: Secure Chat & Talk 1.0.0	
Version:	1.1.1	Version:	1.0.0
Updated:	May 25, 2014	Updated:	Apr 9, 2014
File size:		File size:	
Android:	Android 2.3 and up	Android:	Android 2.3 and up

Ek-2: ByLock Uygulamasının Google Play'den Yaklaşık İndirilme Sayısı



Ek-3: ByLock Sunucusuna Ait Sertifikanın Ekran Görüntüsü

46.166.160.137

Identity: 46.166.160.137
Verified by: David Keynes
Expires: 08/21/2024

▾ **Details**

Subject Name

C (Country):	US
ST (State):	Oregon
L (Locality):	Beaverton
O (Organization):	Unknown
OU (Organizational Unit):	Unknown
CN (Common Name):	46.166.160.137

Issuer Name

C (Country):	US
ST (State):	Oregon
L (Locality):	Beaverton
O (Organization):	by Lock
OU (Organizational Unit):	CA
CN (Common Name):	David Keynes

Issued Certificate

Version:	3
Serial Number:	1B 8F A2 F4
Not Valid Before:	2014-08-24
Not Valid After:	2024-08-21

Ek-4: ByLock Sunucusu IP Adreslerine İlişkin virustotal.com Sorgusu

virustotal

46.166.160.137 IP address information

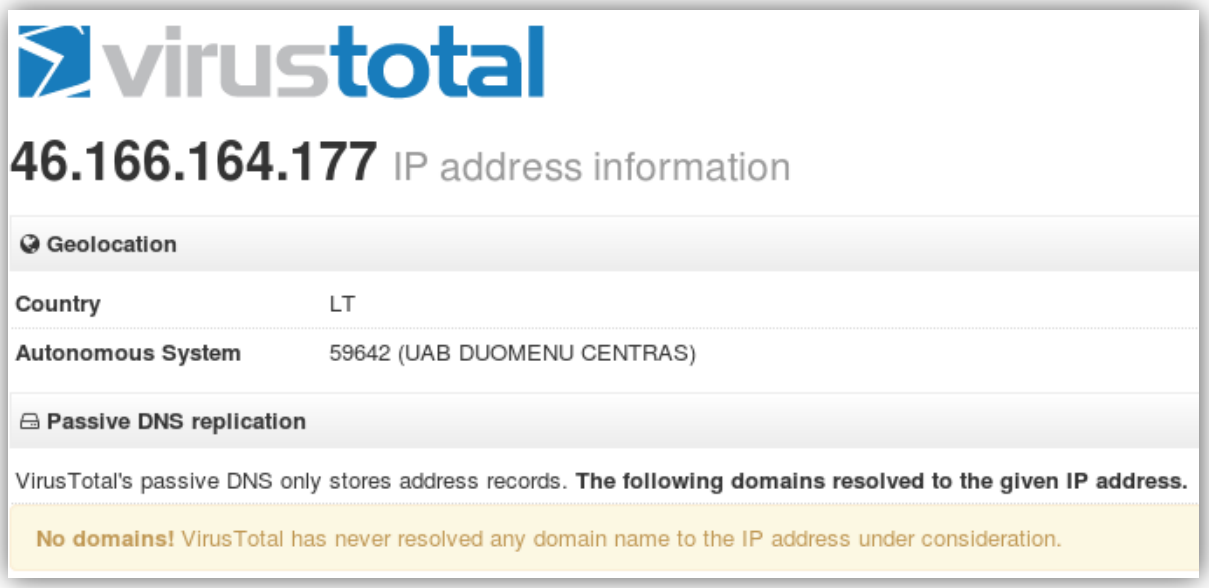
Geolocation

Country	LT
Autonomous System	59642 (UAB DUOMENU CENTRAS)

Passive DNS replication

VirusTotal's passive DNS only stores address records. **The following domains resolved to the given IP address.**

2016-02-19 bylock.net



virustotal

46.166.164.177 IP address information

Geolocation

Country	LT
Autonomous System	59642 (UAB DUOMENU CENTRAS)

Passive DNS replication

VirusTotal's passive DNS only stores address records. **The following domains resolved to the given IP address.**

No domains! VirusTotal has never resolved any domain name to the IP address under consideration.

Ek-5: Kaynak Kodlarda Geçen Türkçe İfadeler

```
.methodprotected a()Ljava/lang/String;
    .locals 3
    .prologue
    .line 35
new-instance v0, Ljava/lang/StringBuilder;
iget-object v1, p0, Lnet/client/by/lock/b/d;->i:Ljava/lang/String;
invoke-static                    {v1},                    Ljava/lang/String;-
>valueOf(Ljava/lang/Object;)Ljava/lang/String;
move-result-object v1
invoke-direct          {v0,          v1},          Ljava/lang/StringBuilder;-
><init>(Ljava/lang/String;)V
const-string v1, " (Dosya) ("
invoke-virtual          {v0,          v1},          Ljava/lang/StringBuilder;-
>append(Ljava/lang/String;)Ljava/lang/StringBuilder;
move-result-object v0
iget v1, p0, Lnet/client/by/lock/b/d;->a:I
int-to-long v1, v1
invoke-static {v1, v2}, Lnet/client/by/lock/f/j;->a(J)Ljava/lang/String;
move-result-object v1
invoke-virtual          {v0,          v1},          Ljava/lang/StringBuilder;-
>append(Ljava/lang/String;)Ljava/lang/StringBuilder;
move-result-object v0
const-string v1, ")"
invoke-virtual          {v0,          v1},          Ljava/lang/StringBuilder;-
>append(Ljava/lang/String;)Ljava/lang/StringBuilder;
move-result-object v0
invoke-virtual {v0}, Ljava/lang/StringBuilder;->toString()Ljava/lang/String;
move-result-object v0
return-object v0
.endmethod
```

```
 .methodprotected a()Ljava/lang/String;
     .locals 2
     .prologue
     .line 21
 new-instance v0, Ljava/lang/StringBuilder;
 iget-object v1, p0, Lnet/client/by/lock/d/m;->b:Ljava/lang/String;
```

```
 invoke-static                    {v1},                    Ljava/lang/String;-
>valueOf(Ljava/lang/Object;)Ljava/lang/String;
 move-result-object v1
 invoke-direct          {v0,          v1},          Ljava/lang/StringBuilder;-
><init>(Ljava/lang/String;)V
 const-string v1, " (Posta)"
 invoke-virtual          {v0,          v1},          Ljava/lang/StringBuilder;-
>append(Ljava/lang/String;)Ljava/lang/StringBuilder;
 move-result-object v0
 invoke-virtual               {v0},               Ljava/lang/StringBuilder;-
>toString()Ljava/lang/String;
 move-result-object v0
 return-object v0
 .endmethod
```

```
.methodprotected a()Ljava/lang/String;
    .locals 3
    .prologue
    .line 56
new-instance v1, Ljava/lang/StringBuilder;
const-string v0, "Sesli Arama"
invoke-direct          {v1,          v0},          Ljava/lang/StringBuilder;-
><init>(Ljava/lang/String;)V
iget-object v0, p0, Lnet/client/by/lock/a/c;->f:Lnet/client/by/lock/f/h;
invoke-virtual {v0}, Lnet/client/by/lock/f/h;->a()Ljava/lang/Object;
move-result-object v0
check-cast v0, Ljava/lang/String;
const-string v2, "CLOSED"
invoke-virtual {v0, v2}, Ljava/lang/String;->equals(Ljava/lang/Object;)Z
move-result v0
if-eqz v0, :cond_0
new-instance v2, Ljava/lang/StringBuilder;
const-string v0, " ("
invoke-direct          {v2,          v0},          Ljava/lang/StringBuilder;-
><init>(Ljava/lang/String;)V
iget-object v0, p0, Lnet/client/by/lock/a/c;->i:Lnet/client/by/lock/f/h;
invoke-virtual {v0}, Lnet/client/by/lock/f/h;->a()Ljava/lang/Object;
move-result-object v0
check-cast v0, Ljava/lang/String;
invoke-virtual          {v2,          v0},          Ljava/lang/StringBuilder;-
>append(Ljava/lang/String;)Ljava/lang/StringBuilder;
```

```
move-result-object v0
const-string v2, “)”
invoke-virtual {v0, v2}, Ljava/lang/StringBuilder;-
>append(Ljava/lang/String;)Ljava/lang/StringBuilder;
move-result-object v0
invoke-virtual {v0}, Ljava/lang/StringBuilder;->toString()Ljava/lang/String;
move-result-object v0
    :goto_0
invoke-virtual {v1, v0}, Ljava/lang/StringBuilder;-
>append(Ljava/lang/String;)Ljava/lang/StringBuilder;
move-result-object v0
invoke-virtual {v0}, Ljava/lang/StringBuilder;->toString()Ljava/lang/String;
move-result-object v0
return-object v0
    :cond_0
const-string v0, ““
goto :goto_0
.endmethod
```

Ek-6: İstemci Kaynak Kodlarında Geçen Kriptografik Algoritmalar

Kayıt sırasında girilen parolanın "MD5" kriptografik özeti için kullanılan fonksiyonları içeren "smali" dosyalarının 4 ayrı uygulama sürümüne ait kurulum paketleri içerisindeki yolları aşağıda sunulmuştur:

Sürüm Numarası	Dosya Yolları
1.1.3	smali\net\client\by\lock\c\i.smali
1.1.6	smali\net\client\by\lock\c\m.smali
1.1.7	smali\net\client\by\lock\c\i.smali
2.0.0	smali\net\client\bylockapp\two\c\i.smali

Tablo - Asimetrik gizli anahtarın şifrelenmesi için kullanılan kodları içeren dosyaların uygulamanın kurulum paketleri içerisindeki yolları

"MD5" kriptografik özet algoritmasının kullanımına ait kaynak kodların bir kısmına aşağıda yer verilmiştir:

```
.line 89
:try_start_0
const-string v1, "MD5"
invoke-static {v1}, Ljava/security/MessageDigest;-
>getInstance(Ljava/lang/String;)Ljava/security/MessageDigest;
:try_end_0
.catchLjava/security/NoSuchAlgorithmException; {:try_start_0 ..
:try_end_0} :catch_0
move-result-object v0
.line 93
:goto_0
invoke-virtual {v0}, Ljava/security/MessageDigest;->reset()V
.line 94
invoke-static {}, Lnet/client/by/lock/d/r;-
>i()Lnet/client/by/lock/d/r;
move-result-object v1
invoke-virtual {v1}, Lnet/client/by/lock/d/r;->k()Ljava/lang/String;
move-result-object v1
.line 95
invoke-virtual {v1}, Ljava/lang/String;->getBytes()[B
move-result-object v1
invoke-virtual {v0, v1}, Ljava/security/MessageDigest;->update([B)V
.line 96
new-instance v1, Ljava/math/BigInteger;
invoke-virtual {v0}, Ljava/security/MessageDigest;->digest()[B
move-result-object v3
```

Uygulama istemcileri arasındaki 2048 bitlik asimetrik "RSA/ECB/OAEPWithSHA-1AndMGF1Padding" algoritmasına dair fonksiyonları içeren "smali" dosyalarının 4 ayrı uygulama sürümüne ait kurulum paketleri içerisindeki yollarına aşağıdaki tabloda yer verilmiştir:

Sürüm Numarası	Dosya Yolları
1.1.3	smali\net\client\by\lock\d\f.smali
1.1.6	smali\net\client\by\lock\d\f.smali
1.1.7	smali\net\client\by\lock\d\f.smali
2.0.0	smali\net\client\bylockapp\two\d\f.smali

Tablo - Haberleşmenin şifrelenmesi için kullanılan kodları içeren dosyaların uygulamanın kurulum paketleri içerisindeki yolları

"RSA/ECB/OAEPWithSHA-1AndMGF1Padding" kriptografik algoritmasının kullanımına ait kaynak kodların bir kısmı aşağıda sunulmuştur:

```
invoke-static {v0}, Ljava/security/KeyFactory;-
>getInstance(Ljava/lang/String;)Ljava/security/KeyFactory;
move-result-object v0
iput-object v0, p0, Lnet/client/by/lock/d/f;-
>b:Ljava/security/KeyFactory;
    .line 52
const-string v0, "SHA1withRSA"
invoke-static {v0}, Ljava/security/Signature;-
>getInstance(Ljava/lang/String;)Ljava/security/Signature;
move-result-object v0
iput-object v0, p0, Lnet/client/by/lock/d/f;-
>d:Ljava/security/Signature;
    .line 53
const-string v0, "RSA/ECB/OAEPWithSHA-1AndMGF1Padding"
invoke-static {v0}, Ljavax/crypto/Cipher;-
>getInstance(Ljava/lang/String;)Ljavax/crypto/Cipher;
move-result-object v0
```

Asimetrik gizli anahtarı, "SHA256" kriptografik özet fonksiyonu ve "AES/CBC/PKCS5Padding" algoritması ile şifrelemek için kullanılan fonksiyonları içeren "smali" dosyalarının 4 ayrı uygulama sürümüne ait kurulum paketleri içerisindeki yollarına aşağıdaki tabloda yer verilmiştir:

Sürüm Numarası	Dosya Yolları
1.1.3	smali\net\client\by\lock\d\q.smali
1.1.6	smali\net\client\by\lock\d\q.smali
1.1.7	smali\net\client\by\lock\d\q.smali
2.0.0	smali\net\client\bylockapp\two\d\q.smali

Tablo - Asimetrik gizli anahtarın şifrelenmesi için kullanılan kodları içeren dosyaların uygulamanın kurulum paketleri içerisindeki yolları

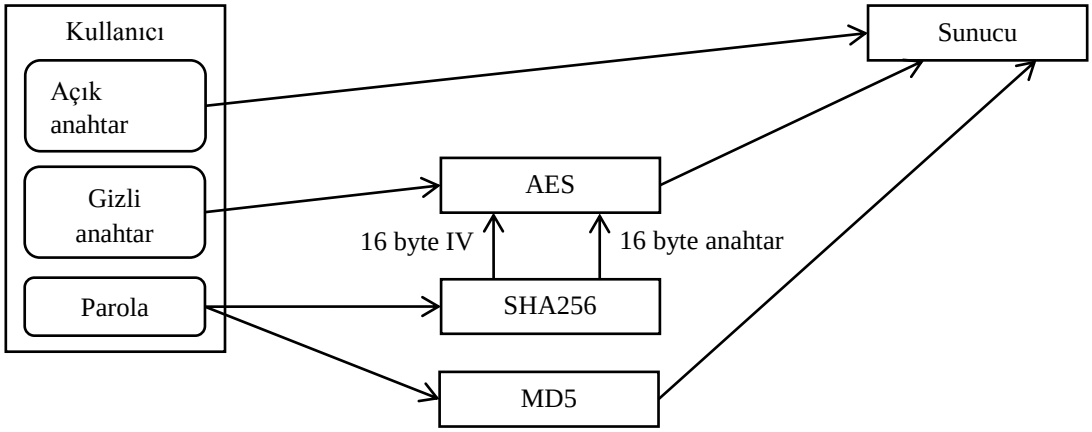
"SHA256" ve "AES/CBC/PKCS5Padding" kriptografik algoritmalarının kullanımlarına ait kaynak kodların bir kısmı aşağıda sunulmuştur:

```
.methodpublicconstructor<init>([B[B)V
    .locals 8
    .prologue
    .line 59
invoke-direct {p0}, Lnet/client/by/lock/d/f;-><init>()V
    .line 60
iput-object p2, p0, Lnet/client/by/lock/d/q;->f:[B
    .line 61
const/4 v1, 0x0
    .line 63
    :try_start_0
const-string v0, "SHA-256"
invoke-static {v0}, Ljava/security/MessageDigest;-
>getInstance(Ljava/lang/String;)Ljava/security/MessageDigest;
move-result-object v0
    .line 64
invoke-static {}, Lnet/client/by/lock/d/r;-
>i()Lnet/client/by/lock/d/r;
move-result-object v2
invoke-virtual {v2}, Lnet/client/by/lock/d/r;->l()Ljava/lang/String;
move-result-object v2
invoke-virtual {v2}, Ljava/lang/String;->getBytes()[B
move-result-object v2
invoke-virtual {v0, v2}, Ljava/security/MessageDigest;->update([B)V
    .line 65
invoke-virtual {v0}, Ljava/security/MessageDigest;->digest()[B
move-result-object v0
    .line 66
const-string v2, "AES/CBC/PKCS5Padding"
invoke-static {v2}, Ljavax/crypto/Cipher;-
>getInstance(Ljava/lang/String;)Ljavax/crypto/Cipher;
```

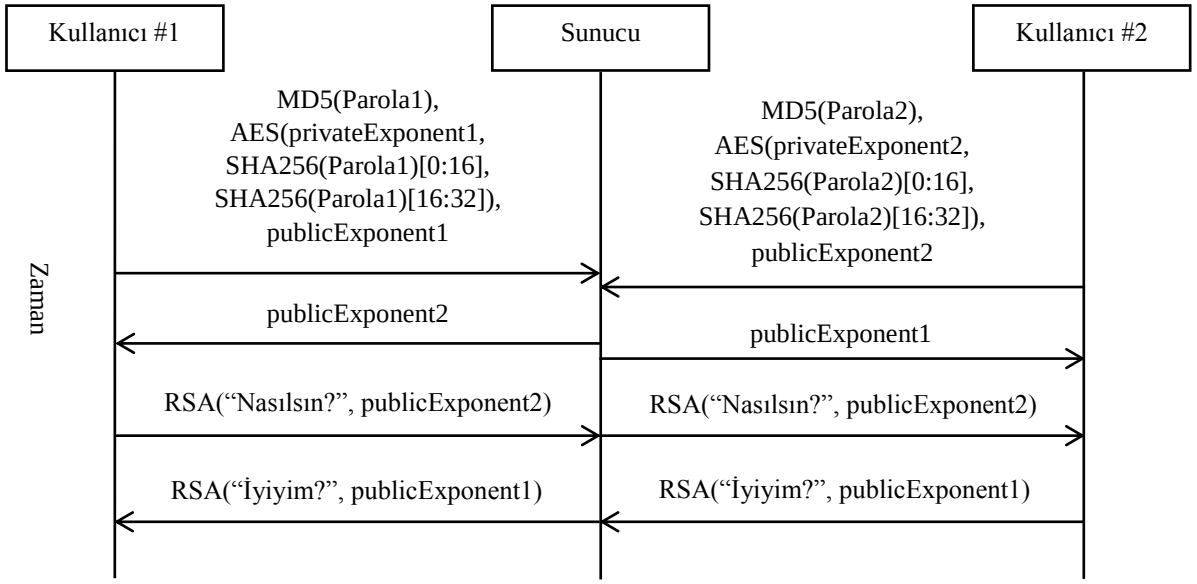
```
move-result-object v2
    .line 67
const/4 v3, 0x2
new-instance v4, Ljavax/crypto/spec/SecretKeySpec;
const/4 v5, 0x0
const/16 v6, 0x10
const-string v7, “AES”
invoke-direct {v4, v0, v5, v6, v7}, Ljavax/crypto/spec/SecretKeySpec;-
><init>([BIILjava/lang/String;)V
new-instance v5, Ljavax/crypto/spec/IvParameterSpec;
    .line 68
array-length v6, v0
add-int/lit8 v6, v6, -0x10
const/16 v7, 0x10
invoke-direct {v5, v0, v6, v7}, Ljavax/crypto/spec/IvParameterSpec;-
><init>([BII)V
```

Ek-7: Kayıt ve İki Kullanıcı Arasındaki Şifreli Mesajlaşmaya Ait Akış Şeması

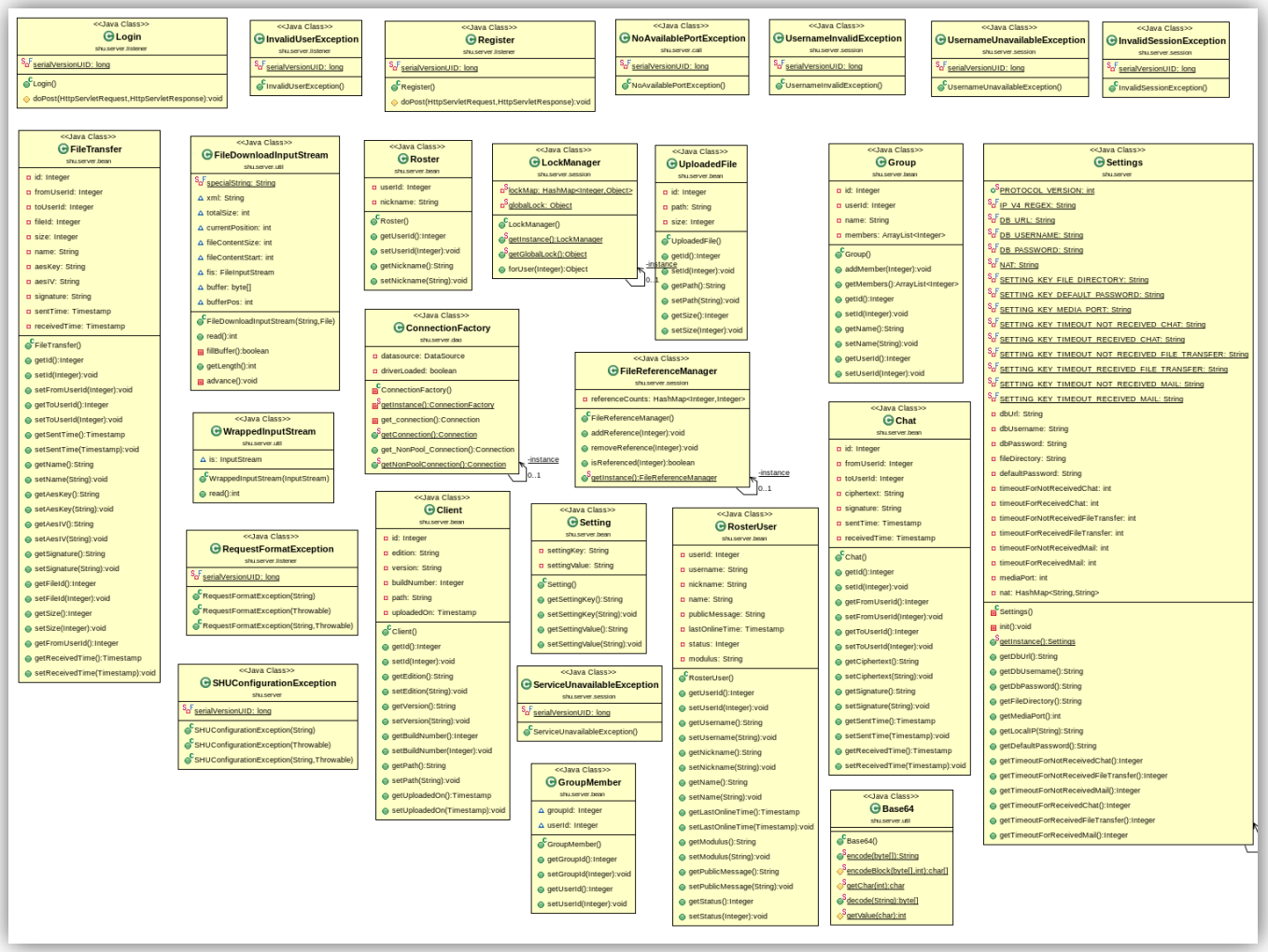
Kayıt olan kullanıcıdan sunucuya gönderilen kriptografik değişkenler/anahtarlar akış şeması:

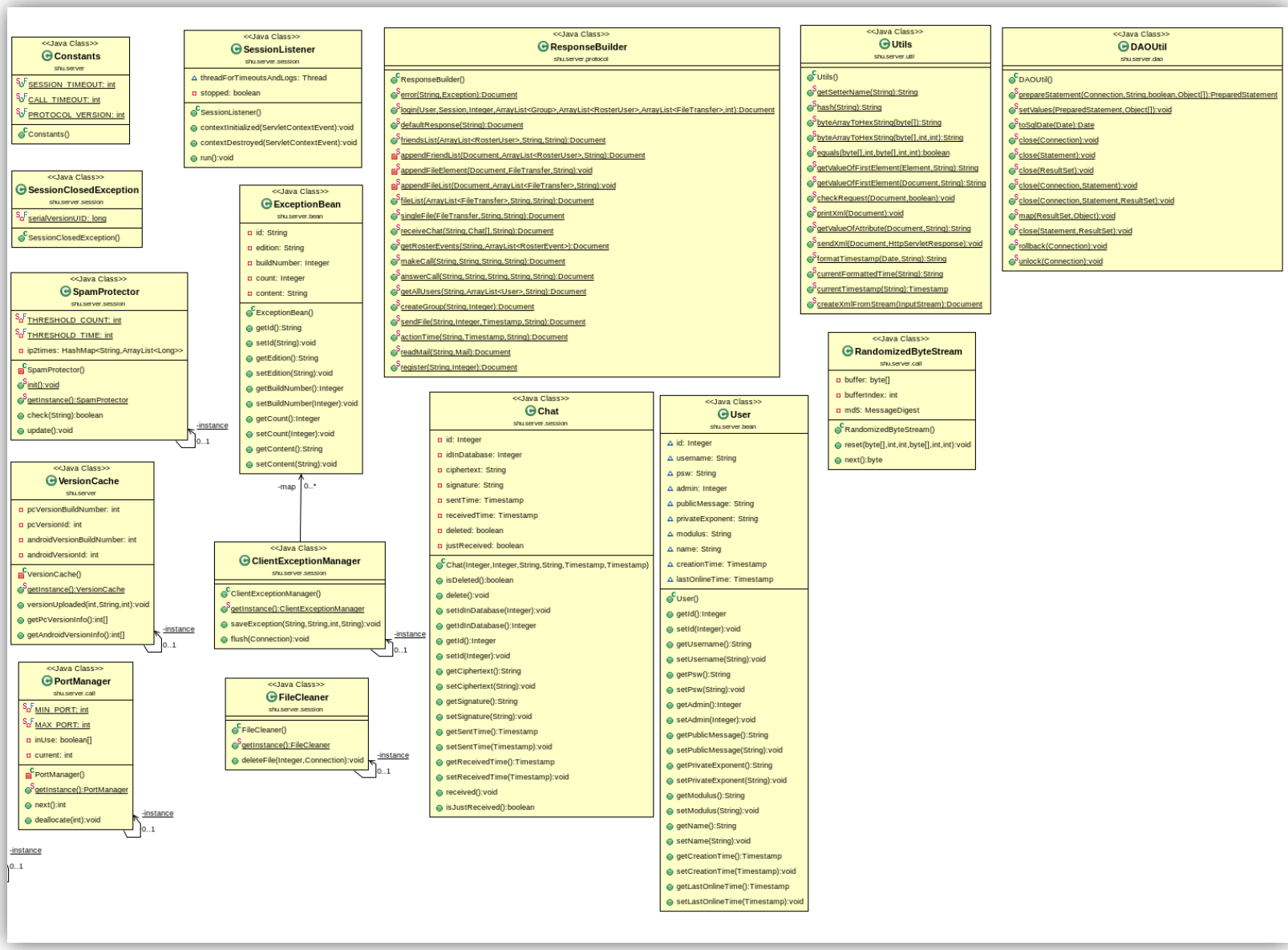


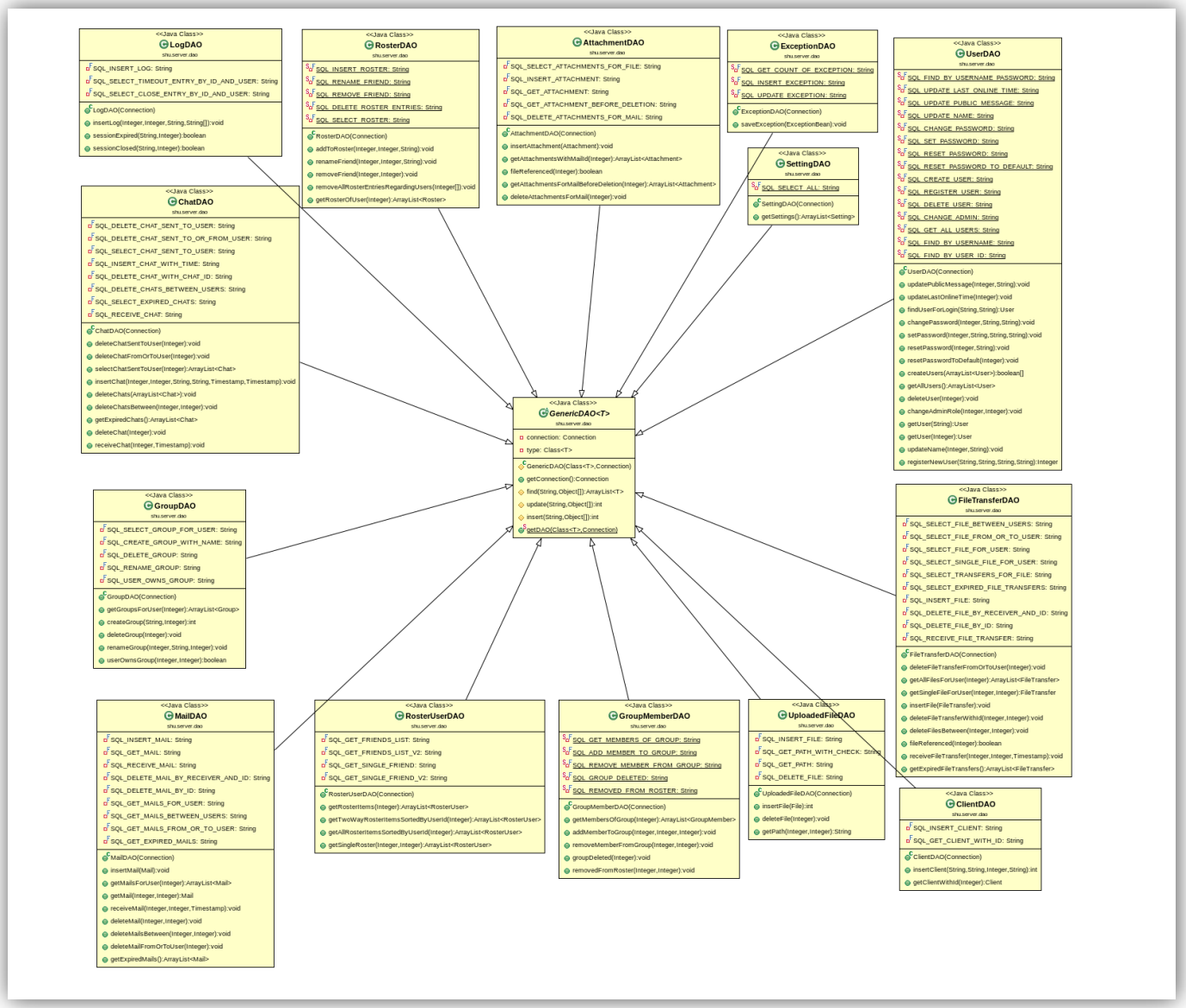
İki kullanıcı arasındaki şifreli mesajlaşmaya dair akış şeması:

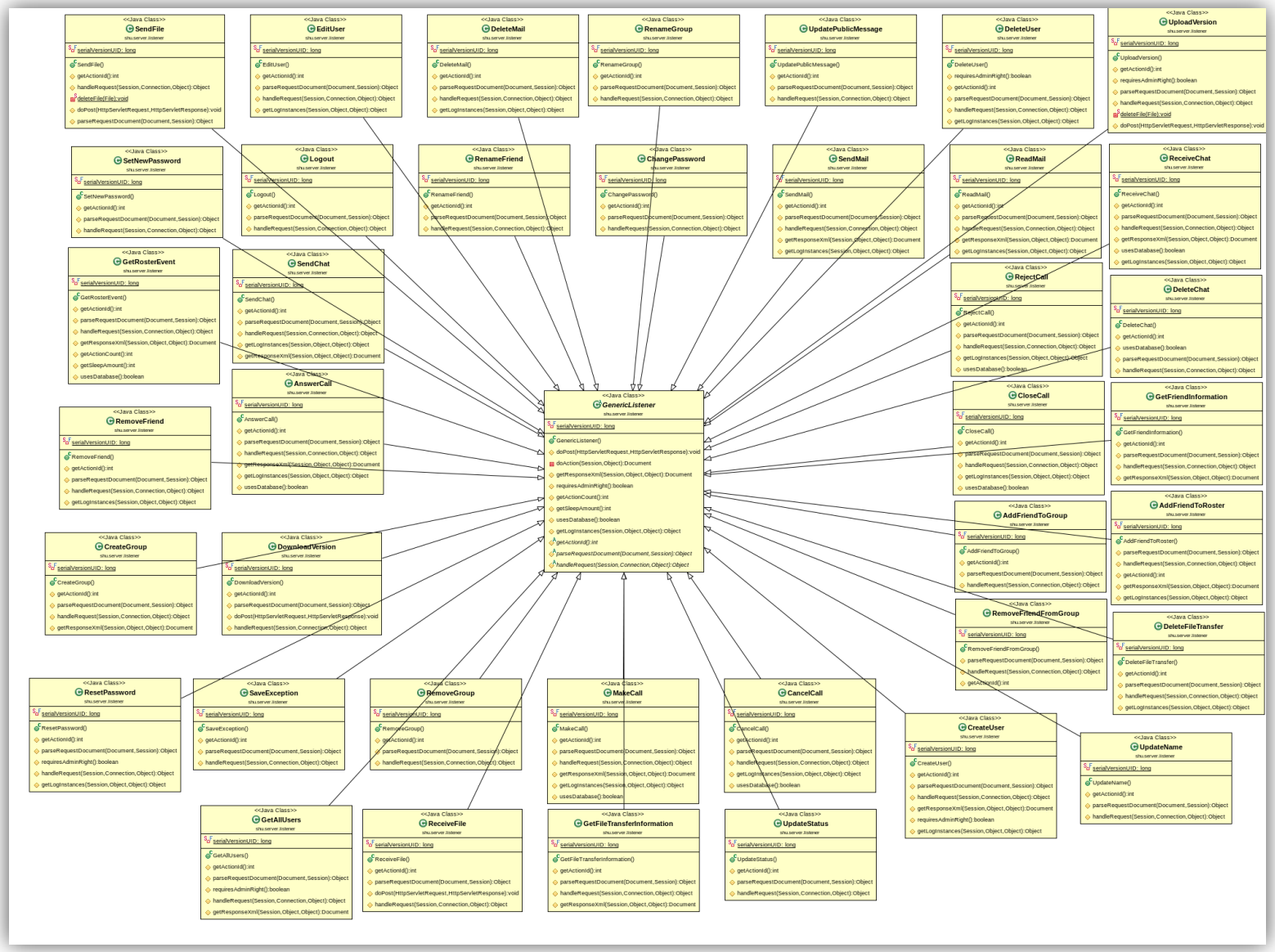


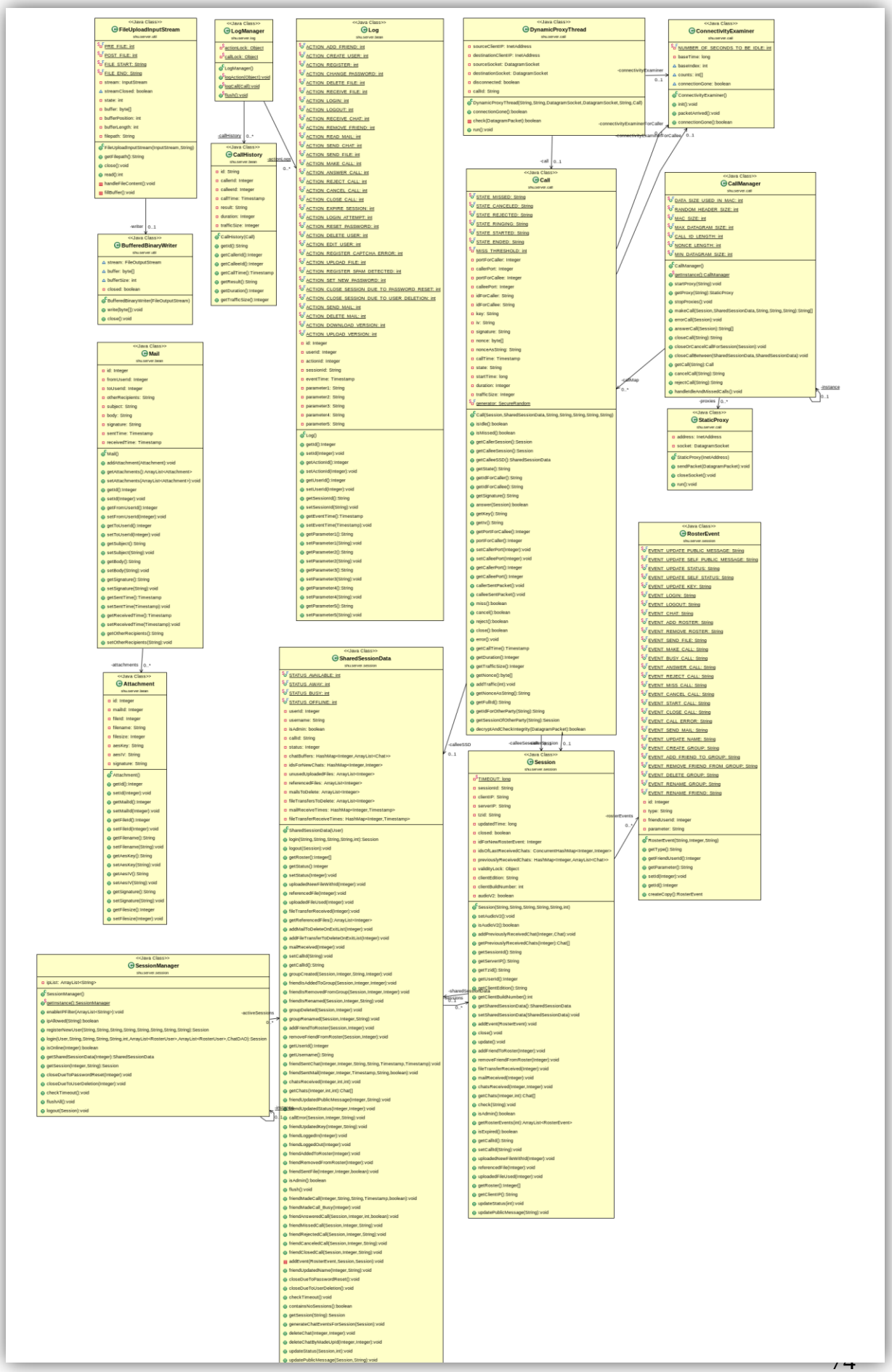
Ek-8: Uygulama Sunucusu Yazılım Modelleri




<<Java Class>>
Constants
shu.server
SESSION_TIMEOUT: int
CALL_TIMEOUT: int
PROTOCOL_VERSION: int
Constants()
<<Java Class>>
SessionListener
shu.server.session
threadForTimeoutsAndLogs: Thread
stopped: boolean
SessionListener()
contextInitialized(ServletContextEvent):void
contextDestroyed(ServletContextEvent):void
run():void
<<Java Class>>
ResponseBuilder
shu.server.protocol
ResponseBuilder()
error(String,Exception):Document
login(User,Session,Integer,ArrayList<Group>,ArrayList<RosterUser>,ArrayList<FileTransfer>,int):Document
defaultResponse(String):Document
friendsList(ArrayList<RosterUser>,String,String):Document
appendFriendList(Document,ArrayList<RosterUser>,String):Document
appendFileElement(Document,FileTransfer,String):void
appendFileList(Document,ArrayList<FileTransfer>,String):void
fileList(ArrayList<FileTransfer>,String,String):Document
singleFile(FileTransfer,String,String):Document
receiveChat(String,Chat[],String):Document
getRosterEvents(String,ArrayList<RosterEvent>):Document
makeCall(String,String,String,String):Document
answerCall(String,String,String,String,String):Document
getAllUsers(String,ArrayList<User>,String):Document
createGroup(String,Integer):Document
sendFile(String,Integer,Timestamp,String):Document
actionTime(String,Timestamp,String):Document
readMail(String,Mail):Document
register(String,Integer):Document
<<Java Class>>
Utils
shu.server.util
Utils()
getSetterName(String):String
hash(String):String
byteArrayToHexString(byte[]):String
byteArrayToHexString(byte[],int,int):String
equals(byte[],int,byte[],int,int):boolean
getValueOfFirstElement(Element,String):String
getValueOfFirstElement(Document,String):String
checkRequest(Document,boolean):void
printXml(Document):void
getValueOfAttribute(Document,String):String
sendXml(Document,HttpServletResponse):void
formatTimestamp(Date,String):String
currentFormattedTime(String):String
currentTimestamp(String):Timestamp
createXmlFromStream(InputStream):Document
<<Java Class>>
DAOUtil
shu.server.dao
DAOUtil()
prepareStatement(Connection,String,boolean,Object[]):PreparedStatement
setValues(PreparedStatement,Object[]):void
toSqlDate(Date):Date
close(Connection):void
close(Statement):void
close(ResultSet):void
close(Connection,Statement):void
close(Connection,Statement,ResultSet):void
map(ResultSet,Object):void
close(Statement,ResultSet):void
rollback(Connection):void
unlock(Connection):void
<<Java Class>>
SessionClosedException
shu.server.session
serialVersionUID: long
SessionClosedException()
<<Java Class>>
ExceptionBean
shu.server.bean
id: String
edition: String
buildNumber: Integer
count: Integer
content: String
ExceptionBean()
getId():String
setId(String):void
getEdition():String
setEdition(String):void
getBuildNumber():Integer
setBuildNumber(Integer):void
getCount():Integer
setCount(Integer):void
getContent():String
setContent(String):void
<<Java Class>>
SpamProtector
shu.server.session
THRESHOLD_COUNT: int
THRESHOLD_TIME: int
ip2times: HashMap<String,ArrayList<Long>>
SpamProtector()
init():void
getInstance():SpamProtector
check(String):boolean
update():void
-instance
0..1
<<Java Class>>
RandomizedByteStream
shu.server.call
buffer: byte[]
bufferIndex: int
md5: MessageDigest
RandomizedByteStream()
reset(byte[],int,int,byte[],int,int):void
next():byte
<<Java Class>>
VersionCache
shu.server
pcVersionBuildNumber: int
pcVersionId: int
androidVersionBuildNumber: int
androidVersionId: int
VersionCache()
getInstance():VersionCache
versionUploaded(int,String,int):void
getPcVersionInfo():int[]
getAndroidVersionInfo():int[]
-instance
0..1
-map
0..*
<<Java Class>>
ClientExceptionManager
shu.server.session
ClientExceptionManager()
getInstance():ClientExceptionManager
saveException(String,String,int,String):void
flush(Connection):void
-instance
0..1
<<Java Class>>
Chat
shu.server.session
id: Integer
idInDatabase: Integer
ciphertext: String
signature: String
sentTime: Timestamp
receivedTime: Timestamp
deleted: boolean
justReceived: boolean
Chat(Integer,Integer,String,String,Timestamp,Timestamp)
isDeleted():boolean
delete():void
setIdInDatabase(Integer):void
getIdInDatabase():Integer
getId():Integer
setId(Integer):void
getCiphertext():String
setCiphertext(String):void
getSignature():String
setSignature(String):void
getSentTime():Timestamp
setSentTime(Timestamp):void
getReceivedTime():Timestamp
setReceivedTime(Timestamp):void
received():void
isJustReceived():boolean
<<Java Class>>
User
shu.server.bean
id: Integer
username: String
psw: String
admin: Integer
publicMessage: String
privateExponent: String
modulus: String
name: String
creationTime: Timestamp
lastOnlineTime: Timestamp
User()
getId():Integer
setId(Integer):void
getUsername():String
setUsername(String):void
getPsw():String
setPsw(String):void
getAdmin():Integer
setAdmin(Integer):void
getPublicMessage():String
setPublicMessage(String):void
getPrivateExponent():String
setPrivateExponent(String):void
getModulus():String
setModulus(String):void
getName():String
setName(String):void
getCreationTime():Timestamp
setCreationTime(Timestamp):void
getLastOnlineTime():Timestamp
setLastOnlineTime(Timestamp):void
<<Java Class>>
PortManager
shu.server.call
MIN_PORT: int
MAX_PORT: int
inUse: boolean[]
current: int
PortManager()
getInstance():PortManager
next():int
deallocate(int):void
-instance
0..1
<<Java Class>>
FileCleaner
shu.server.session
FileCleaner()
getInstance():FileCleaner
deleteFile(Integer,Connection):void
-instance
0..1
-instance
0..1


LogDAO
shu.server.dao
SQL_INSERT_LOG: String
SQL_SELECT_TIMEOUT_ENTRY_BY_ID_AND_USER: String
SQL_SELECT_CLOSE_ENTRY_BY_ID_AND_USER: String
LogDAO(Connection)
insertLog(Integer,Integer,String,String[]):void
sessionExpired(String,Integer):boolean
sessionClosed(String,Integer):boolean
RosterDAO
shu.server.dao
SQL_INSERT_ROSTER: String
SQL_RENAME_FRIEND: String
SQL_REMOVE_FRIEND: String
SQL_DELETE_ROSTER_ENTRIES: String
SQL_SELECT_ROSTER: String
RosterDAO(Connection)
addToRoster(Integer,Integer,String):void
renameFriend(Integer,Integer,String):void
removeFriend(Integer,Integer):void
removeAllRosterEntriesRegardingUsers(Integer[]):void
getRosterOfUser(Integer):ArrayList<Roster>
AttachmentDAO
shu.server.dao
SQL_SELECT_ATTACHMENTS_FOR_FILE: String
SQL_INSERT_ATTACHMENT: String
SQL_GET_ATTACHMENT: String
SQL_GET_ATTACHMENT_BEFORE_DELETION: String
SQL_DELETE_ATTACHMENTS_FOR_MAIL: String
AttachmentDAO(Connection)
insertAttachment(Attachment):void
getAttachmentsWithMailId(Integer):ArrayList<Attachment>
fileReferenced(Integer):boolean
getAttachmentsForMailBeforeDeletion(Integer):ArrayList<Attachment>
deleteAttachmentsForMail(Integer):void
ExceptionDAO
shu.server.dao
SQL_GET_COUNT_OF_EXCEPTION: String
SQL_INSERT_EXCEPTION: String
SQL_UPDATE_EXCEPTION: String
ExceptionDAO(Connection)
saveException(ExceptionBean):void
UserDAO
shu.server.dao
SQL_FIND_BY_USERNAME_PASSWORD: String
SQL_UPDATE_LAST_ONLINE_TIME: String
SQL_UPDATE_PUBLIC_MESSAGE: String
SQL_UPDATE_NAME: String
SQL_CHANGE_PASSWORD: String
SQL_SET_PASSWORD: String
SQL_RESET_PASSWORD: String
SQL_RESET_PASSWORD_TO_DEFAULT: String
SQL_CREATE_USER: String
SQL_REGISTER_USER: String
SQL_DELETE_USER: String
SQL_CHANGE_ADMIN: String
SQL_GET_ALL_USERS: String
SQL_FIND_BY_USERNAME: String
SQL_FIND_BY_USER_ID: String
UserDAO(Connection)
updatePublicMessage(Integer,String):void
updateLastOnlineTime(Integer):void
findUserForLogin(String,String):User
changePassword(Integer,String,String):void
setPassword(Integer,String,String,String):void
resetPassword(Integer,String):void
resetPasswordToDefault(Integer):void
createUsers(ArrayList<User>):boolean[]
getAllUsers():ArrayList<User>
deleteUser(Integer):void
changeAdminRole(Integer,Integer):void
getUser(String):User
getUser(Integer):User
updateName(Integer,String):void
registerNewUser(String,String,String,String):Integer
SettingDAO
shu.server.dao
SQL_SELECT_ALL: String
SettingDAO(Connection)
getSettings():ArrayList<Setting>
ChatDAO
shu.server.dao
SQL_DELETE_CHAT_SENT_TO_USER: String
SQL_DELETE_CHAT_SENT_TO_OR_FROM_USER: String
SQL_SELECT_CHAT_SENT_TO_USER: String
SQL_INSERT_CHAT_WITH_TIME: String
SQL_DELETE_CHAT_WITH_CHAT_ID: String
SQL_DELETE_CHATS_BETWEEN_USERS: String
SQL_SELECT_EXPIRED_CHATS: String
SQL_RECEIVE_CHAT: String
ChatDAO(Connection)
deleteChatSentToUser(Integer):void
deleteChatFromOrToUser(Integer):void
selectChatSentToUser(Integer):ArrayList<Chat>
insertChat(Integer,Integer,String,String,Timestamp,Timestamp):void
deleteChats(ArrayList<Chat>):void
deleteChatsBetween(Integer,Integer):void
getExpiredChats():ArrayList<Chat>
deleteChat(Integer):void
receiveChat(Integer,Timestamp):void
GenericDAO<T>
shu.server.dao
connection: Connection
type: Class<T>
GenericDAO(Class<T>,Connection)
getConnection():Connection
find(String,Object[]):ArrayList<T>
update(String,Object[]):int
insert(String,Object[]):int
getDAO(Class<T>,Connection)
GroupDAO
shu.server.dao
SQL_SELECT_GROUP_FOR_USER: String
SQL_CREATE_GROUP_WITH_NAME: String
SQL_DELETE_GROUP: String
SQL_RENAME_GROUP: String
SQL_USER_OWNS_GROUP: String
GroupDAO(Connection)
getGroupsForUser(Integer):ArrayList<Group>
createGroup(String,Integer):int
deleteGroup(Integer):void
renameGroup(Integer,String,Integer):void
userOwnsGroup(Integer,Integer):boolean
FileTransferDAO
shu.server.dao
SQL_SELECT_FILE_BETWEEN_USERS: String
SQL_SELECT_FILE_FROM_OR_TO_USER: String
SQL_SELECT_FILE_FOR_USER: String
SQL_SELECT_SINGLE_FILE_FOR_USER: String
SQL_SELECT_TRANSFERS_FOR_FILE: String
SQL_SELECT_EXPIRED_FILE_TRANSFERS: String
SQL_INSERT_FILE: String
SQL_DELETE_FILE_BY_RECEIVER_AND_ID: String
SQL_DELETE_FILE_BY_ID: String
SQL_RECEIVE_FILE_TRANSFER: String
FileTransferDAO(Connection)
deleteFileTransferFromOrToUser(Integer):void
getAllFilesForUser(Integer):ArrayList<FileTransfer>
getSingleFileForUser(Integer,Integer):FileTransfer
insertFile(FileTransfer):void
deleteFileTransferWithId(Integer,Integer):void
deleteFilesBetween(Integer,Integer):void
fileReferenced(Integer):boolean
receiveFileTransfer(Integer,Integer,Timestamp):void
getExpiredFileTransfers():ArrayList<FileTransfer>
MailDAO
shu.server.dao
SQL_INSERT_MAIL: String
SQL_GET_MAIL: String
SQL_RECEIVE_MAIL: String
SQL_DELETE_MAIL_BY_RECEIVER_AND_ID: String
SQL_DELETE_MAIL_BY_ID: String
SQL_GET_MAILS_FOR_USER: String
SQL_GET_MAILS_BETWEEN_USERS: String
SQL_GET_MAILS_FROM_OR_TO_USER: String
SQL_GET_EXPIRED_MAILS: String
MailDAO(Connection)
insertMail(Mail):void
getMailsForUser(Integer):ArrayList<Mail>
getMail(Integer,Integer):Mail
receiveMail(Integer,Integer,Timestamp):void
deleteMail(Integer,Integer):void
deleteMailsBetween(Integer,Integer):void
deleteMailFromOrToUser(Integer):void
getExpiredMails():ArrayList<Mail>
RosterUserDAO
shu.server.dao
SQL_GET_FRIENDS_LIST: String
SQL_GET_FRIENDS_LIST_V2: String
SQL_GET_SINGLE_FRIEND: String
SQL_GET_SINGLE_FRIEND_V2: String
RosterUserDAO(Connection)
getRosterItems(Integer):ArrayList<RosterUser>
getTwoWayRosterItemsSortedByUserId(Integer):ArrayList<RosterUser>
getAllRosterItemsSortedByUserId(Integer):ArrayList<RosterUser>
getSingleRoster(Integer,Integer):ArrayList<RosterUser>
GroupMemberDAO
shu.server.dao
SQL_GET_MEMBERS_OF_GROUP: String
SQL_ADD_MEMBER_TO_GROUP: String
SQL_REMOVE_MEMBER_FROM_GROUP: String
SQL_GROUP_DELETED: String
SQL_REMOVED_FROM_ROSTER: String
GroupMemberDAO(Connection)
getMembersOfGroup(Integer):ArrayList<GroupMember>
addMemberToGroup(Integer,Integer,Integer):void
removeMemberFromGroup(Integer,Integer):void
groupDeleted(Integer):void
removedFromRoster(Integer,Integer):void
UploadedFileDAO
shu.server.dao
SQL_INSERT_FILE: String
SQL_GET_PATH_WITH_CHECK: String
SQL_GET_PATH: String
SQL_DELETE_FILE: String
UploadedFileDAO(Connection)
insertFile(File):int
deleteFile(Integer):void
getPath(Integer,Integer):String
ClientDAO
shu.server.dao
SQL_INSERT_CLIENT: String
SQL_GET_CLIENT_WITH_ID: String
ClientDAO(Connection)
insertClient(String,String,Integer,String):int
getClientWithId(Integer):Client


SendFile
EditUser
DeleteMail
RenameGroup
UpdatePublicMessage
DeleteUser
UploadVersion
SetNewPassword
Logout
RenameFriend
ChangePassword
SendMail
ReadMail
ReceiveChat
GetRosterEvent
SendChat
RejectCall
DeleteChat
AnswerCall
GenericListener
CloseCall
GetFriendInformation
RemoveFriend
AddFriendToGroup
CreateGroup
DownloadVersion
RemoveFriendFromGroup
DeleteFileTransfer
ResetPassword
SaveException
RemoveGroup
MakeCall
CancelCall
CreateUser
UpdateName
GetAllUsers
ReceiveFile
GetFileTransferInformation
UpdateStatus


FileUploadInputStream
LogManager
Log
DynamicProxyThread
ConnectivityExaminer
CallHistory
BufferedBinaryWriter
Call
CallManager
Mail
StaticProxy
Attachment
RosterEvent
SharedSessionData
Session
SessionManager

Ek-9: Uygulama Sunucusunda Çalışan Yazılımda Rastlanan Türkçe İfade

```
package shu.server.listener;

 import java.io.BufferedReader;
 import java.io.File;
 import java.io.IOException;
 import java.io.InputStream;
 import java.io.InputStreamReader;
 import java.nio.file.Files;
 import java.sql.Connection;
 import java.sql.SQLException;
 import java.util.Random;
 import java.util.StringTokenizer;
 import java.util.jar.JarFile;
 import java.util.zip.ZipEntry;
 import javax.servlet.ServletException;
 import javax.servlet.annotation.WebServlet;
 import javax.servlet.http.HttpServletRequest;
 import javax.servlet.http.HttpServletResponse;
 import javax.xml.parsers.ParserConfigurationException;
 import org.w3c.dom.Document;
 import org.xml.sax.SAXException;
 import shu.server.VersionCache;
 import shu.server.bean.Log;
 import shu.server.dao.ClientDAO;
 import shu.server.dao.ConnectionFactory;
 import shu.server.dao.GenericDAO;
 import shu.server.log.LogManager;
 import shu.server.protocol.ResponseBuilder;
 import shu.server.session.InvalidSessionException;
 import shu.server.session.Session;
 import shu.server.session.SessionClosedException;
 import shu.server.session.SessionManager;
 import shu.server.util.FileUploadInputStream;
 import shu.server.util.Utils;

 @WebServlet({"/UploadVersion"})
 public class UploadVersion
   extends GenericListener
 {
   private static final long serialVersionUID = 1L;

   protected int getActionId()
   {
     return 35;
   }

   protected boolean requiresAdminRight()
   {
     return true;
   }

   protected Object parseRequestDocument(Document requestDocument,
Session session)
     throws RequestFormatException
   {
     return null;
   }

   protected Object handleRequest(Session session, Connection
connection, Object requestParameter)
```

```
    throws SQLException, SessionClosedException
  {
    return null;
  }

  private static void deleteFile(File file) {
    try {
      Files.delete(file.toPath());
    } catch (Exception ex) {
      ex.printStackTrace();
    }
  }

  protected void doPost(HttpServletRequest request,
HttpServletResponse response)
    throws ServletException, IOException
  {
    String filename = System.nanoTime() + "-" + (new
Random().nextInt(9000) + 1000);
    FileUploadInputStream fuis = null;
    response.setCharacterEncoding("UTF-8");
    Integer userId = null;
    String sessionId = "";
    String edition = "";
    String version = "";
    int buildNumber = -1;
    String clientIP = request.getRemoteAddr();
    Document requestDocument = null;
    Session session = null;
    Connection connection = null;
    try {
      fuis = new FileUploadInputStream(request.getInputStream(),
filename);
    }
    catch (IOException e) {
      e.printStackTrace();
      return;
    }
    File uploadedFile = new File(fuis.getFilepath());
    try {
      requestDocument = Utils.createXmlFromStream(fuis);

      Utils.checkRequest(requestDocument, true);
      try
      {
        userId =
Integer.valueOf(Integer.parseInt(Utils.getValueOfFirstElement(reques
tDocument, "userId")));
      }
      catch (NumberFormatException|RequestFormatException
localNumberFormatException) {}
      sessionId = Utils.getValueOfAttribute(requestDocument, "id");

      session = SessionManager.getInstance().getSession(userId,
sessionId);
      if (session == null) {
        throw new InvalidSessionException();
      }
      session.check(clientIP);

      edition = Utils.getValueOfFirstElement(requestDocument,
"edition");

      if (!uploadedFile.exists()) {
```

```
          throw new RequestFormatException("fileContent does not
exist!");
        }

        JarFile jf = new JarFile(uploadedFile);
        ZipEntry versionEntry = jf.getEntry("VERSION");
        if (versionEntry == null) {
          jf.close();
          throw new RequestFormatException("VERSION file is
missing!");
        }
        InputStream versionInputStream =
jf.getInputStream(versionEntry);
        if (versionInputStream == null) {
          jf.close();
          throw new RequestFormatException("VERSION file cannot be
opened!");
        }
        br = new BufferedReader(new
InputStreamReader(versionInputStream));
        String versionAndBuildNumber = br.readLine().trim();
        br.close();
        StringTokenizer tokenizer = new
StringTokenizer(versionAndBuildNumber, "-");
        if (tokenizer.countTokens() == 2) {
          version = tokenizer.nextToken();
          try {
            buildNumber = Integer.parseInt(tokenizer.nextToken());
          }
          catch (NumberFormatException localNumberFormatException1)
{}
        }
        jf.close();

        if (buildNumber == -1) {
          throw new RequestFormatException("invalid version
information in VERSION file!");
        }
      } catch
(SAXException|ParserConfigurationException|InvalidSessionException
e) {
        e.printStackTrace();
        deleteFile(uploadedFile);
        return;
      } catch (RequestFormatException e) {
        Utils.sendXml(ResponseBuilder.error(sessionId, e), response);
        deleteFile(uploadedFile);
        return;
      }

      if (!session.isAdmin()) {
        Utils.sendXml(ResponseBuilder.error(sessionId, new
Exception("Yetkiniz Yok!")), response);
        deleteFile(uploadedFile);

        return;
      }

      int clientId = -1;
      try {
        connection = ConnectionFactory.getConnection();
        ClientDAO cDAO =
(ClientDAO)GenericDAO.getDAO(ClientDAO.class, connection);
```

```
        clientId = cDAO.insertClient(edition, version,
Integer.valueOf(buildNumber), uploadedFile.getAbsolutePath());
        VersionCache.getInstance().versionUploaded(clientId, edition,
buildNumber);
      } catch (SQLException e) {
        e.printStackTrace();
        deleteFile(uploadedFile);
        Utils.sendXml(ResponseBuilder.error(sessionId, e), response);
        if (connection != null) {
          try {
            connection.rollback();
          }
          catch (SQLException e1) {
            e1.printStackTrace();
          }
        }
        return;
      } finally {
        if (connection != null) {
          try {
            connection.close();
          }
          catch (SQLException e) {
            e.printStackTrace();
          }
        }
      }

      Log log = (Log)super.getLogInstances(session, null, null);
      log.setParameter1(clientId);
      LogManager.logAction(log);

      Utils.sendXml(ResponseBuilder.defaultResponse(sessionId),
response);
    }
  }
```

Ek-10: Uygulama Sunucusunda Engellenen IP Adresleri Listesi

IP Blokları	**Ülke**
5.2.80.0/21	Türkiye
5.11.128.0/17	Türkiye
5.23.120.0/21	Türkiye
5.24.0.0/14	Türkiye
5.44.80.0/20	Türkiye
5.44.144.0/20	Türkiye
5.46.0.0/15	Türkiye
5.63.32.0/19	Türkiye
5.104.0.0/20	Türkiye
5.159.248.0/21	Türkiye
5.176.0.0/15	Türkiye
5.226.192.0/18	Türkiye
5.229.0.0/16	Türkiye
5.250.240.0/20	Türkiye
5.255.0.0/18	Türkiye
24.133.0.0/16	Türkiye
31.3.0.0/21	Türkiye
31.6.80.0/20	Türkiye
31.7.32.0/21	Türkiye
31.25.168.0/21	Türkiye
31.44.192.0/20	Türkiye
31.140.0.0/14	Türkiye
31.145.0.0/16	Türkiye
31.155.0.0/16	Türkiye
31.169.64.0/19	Türkiye
31.176.0.0/17	Türkiye
31.177.128.0/17	Türkiye
31.186.0.0/19	Türkiye
31.192.208.0/21	Türkiye
31.200.0.0/17	Türkiye
31.206.0.0/16	Türkiye
31.207.80.0/21	Türkiye
31.210.32.0/19	Türkiye
31.210.64.0/18	Türkiye
31.210.152.0/21	Türkiye
31.214.129.0/24	Almanya
31.214.152.0/24	Almanya
31.223.0.0/17	Türkiye
37.1.144.0/21	Hollanda
37.9.200.0/21	Türkiye
37.34.0.0/19	Türkiye
37.58.16.0/21	Türkiye
37.72.48.0/20	Türkiye
37.75.8.0/21	Türkiye
37.77.0.0/19	Türkiye
37.122.136.0/21	Türkiye
37.122.224.0/20	Türkiye
37.123.0.0/18	Türkiye
37.123.96.0/21	Türkiye
37.130.64.0/18	Türkiye
37.131.248.0/21	Türkiye
37.140.208.0/21	Türkiye
37.148.208.0/21	Türkiye
37.152.72.0/21	Türkiye
37.154.0.0/15	Türkiye
37.202.48.0/21	Türkiye
37.205.0.0/21	Türkiye
37.218.192.0/20	Kıbrıs
37.230.104.0/21	Türkiye
37.235.72.0/21	Türkiye
37.247.96.0/20	Türkiye
37.247.112.0/21	Türkiye
46.1.0.0/16	Türkiye
46.2.0.0/16	Türkiye
46.17.128.0/21	Türkiye
46.20.0.0/20	Türkiye
46.20.144.0/20	Türkiye
46.28.232.0/21	Türkiye
46.30.176.0/21	Türkiye
46.31.112.0/21	Türkiye
46.31.144.0/21	Türkiye
46.45.128.0/18	Türkiye
46.104.0.0/16	Türkiye
46.106.0.0/16	Türkiye
46.154.0.0/15	Türkiye
46.182.64.0/21	Türkiye
46.196.0.0/15	Türkiye
46.221.0.0/16	Türkiye
46.234.0.0/19	Türkiye
46.235.8.0/21	Türkiye
46.245.160.0/21	Türkiye
46.252.96.0/20	Türkiye
46.254.48.0/21	Türkiye
62.29.0.0/17	Türkiye
62.108.64.0/19	Türkiye
62.244.192.0/18	Türkiye
62.248.0.0/17	Türkiye
77.72.184.0/21	Türkiye
77.73.216.0/21	Türkiye
77.75.32.0/21	Türkiye
77.75.216.0/21	Türkiye
77.79.64.0/18	Türkiye
77.92.96.0/19	Türkiye
77.92.128.0/19	Türkiye
77.223.128.0/19	Türkiye
77.245.144.0/20	Türkiye
78.40.224.0/21	Türkiye
78.111.96.0/20	Türkiye
78.135.0.0/22	Türkiye
78.135.4.0/22	Türkiye
78.135.8.0/21	Türkiye
78.135.16.0/20	Türkiye
78.135.32.0/19	Türkiye
78.135.64.0/18	Türkiye
78.160.0.0/11	Türkiye
79.98.128.0/21	Türkiye
79.99.176.0/21	Türkiye
79.123.128.0/17	Türkiye
79.170.168.0/21	Türkiye
79.171.16.0/21	Türkiye
80.93.208.0/20	Türkiye
80.251.32.0/20	Türkiye
80.253.240.0/20	Türkiye
81.6.64.0/18	Türkiye
81.8.0.0/17	Türkiye
81.21.160.0/20	Türkiye
81.22.96.0/20	Türkiye
81.91.112.0/20	Türkiye
81.212.0.0/14	Türkiye
82.145.224.0/19	Türkiye
82.150.64.0/19	Türkiye
82.151.128.0/19	Türkiye
82.222.0.0/16	Türkiye
83.66.0.0/16	Türkiye
84.17.64.0/19	Türkiye

84.44.0.0/17	Türkiye
84.51.0.0/18	Türkiye
85.29.0.0/18	Türkiye
85.95.224.0/19	Türkiye
85.96.0.0/12	Türkiye
85.119.32.0/21	Türkiye
85.119.64.0/21	Türkiye
85.153.0.0/16	Türkiye
85.158.96.0/21	Türkiye
85.159.64.0/21	Türkiye
85.159.72.0/21	Türkiye
85.235.64.0/19	Türkiye
86.108.128.0/17	Türkiye
87.251.0.0/19	Türkiye
88.224.0.0/11	Türkiye
89.19.0.0/19	Türkiye
89.106.0.0/19	Türkiye
89.107.224.0/21	Türkiye
89.145.184.0/21	Türkiye
89.252.128.0/18	Türkiye
90.158.0.0/15	Türkiye
91.93.0.0/16	Türkiye
91.102.160.0/21	Türkiye
91.109.208.0/21	Türkiye
91.151.80.0/20	Türkiye
91.191.160.0/20	Türkiye
92.42.32.0/21	Türkiye
92.43.80.0/21	Türkiye
92.44.0.0/15	Türkiye
92.61.0.0/20	Türkiye
92.63.0.0/20	Türkiye
93.89.16.0/20	Türkiye
93.89.64.0/20	Türkiye
93.89.224.0/20	Kıbrıs
93.91.64.0/20	Türkiye
93.93.24.0/21	Türkiye
93.94.192.0/21	Türkiye
93.94.248.0/21	Türkiye
93.95.176.0/21	Türkiye
93.155.0.0/17	Türkiye
93.182.64.0/18	Türkiye
93.184.144.0/20	Türkiye
93.186.112.0/20	Türkiye
93.187.64.0/21	Türkiye
93.187.200.0/21	Türkiye

93.190.120.0/21	Türkiye
93.190.216.0/21	Türkiye
94.46.0.0/21	Portekiz
94.46.32.0/21	Türkiye
94.54.0.0/15	Türkiye
94.73.128.0/18	Türkiye
94.78.64.0/18	Türkiye
94.79.64.0/18	Türkiye
94.101.80.0/20	Türkiye
94.102.0.0/20	Türkiye
94.102.64.0/20	Türkiye
94.103.32.0/20	Türkiye
94.120.0.0/14	Türkiye
94.138.192.0/19	Türkiye
94.199.32.0/21	Türkiye
94.199.200.0/21	Türkiye
94.235.0.0/16	Türkiye
95.0.0.0/12	Türkiye
95.65.128.0/17	Türkiye
95.70.128.0/17	Türkiye
95.128.56.0/21	Türkiye
95.130.168.0/21	Türkiye
95.142.128.0/20	Türkiye
95.173.0.0/19	Türkiye
95.173.160.0/19	Türkiye
95.173.224.0/19	Türkiye
95.183.128.0/17	Türkiye
109.228.192.0/18	Türkiye
109.230.196.0/24	Almanya
109.232.216.0/21	Türkiye
109.235.248.0/21	Türkiye
128.127.168.0/21	Türkiye
134.19.200.0/21	Türkiye
134.255.199.0/24	Almanya
141.196.0.0/16	Türkiye
146.185.96.0/19	Türkiye
149.0.0.0/16	Türkiye
149.140.0.0/16	Türkiye
151.135.0.0/16	Türkiye
151.250.0.0/16	Türkiye
159.20.64.0/19	Türkiye
159.20.112.0/21	Türkiye
159.146.0.0/17	Türkiye
159.253.32.0/20	Türkiye
159.253.80.0/21	Türkiye

176.30.0.0/16	Türkiye
176.33.0.0/16	Türkiye
176.40.0.0/14	Türkiye
176.53.0.0/17	Türkiye
176.54.0.0/15	Türkiye
176.88.0.0/14	Türkiye
176.216.0.0/14	Türkiye
176.220.0.0/16	Türkiye
176.227.0.0/17	Türkiye
176.232.0.0/15	Türkiye
176.234.0.0/15	Türkiye
176.236.0.0/16	Türkiye
176.237.0.0/16	Türkiye
176.238.0.0/15	Türkiye
176.240.0.0/16	Türkiye
178.18.192.0/20	Türkiye
178.20.224.0/21	Türkiye
178.22.8.0/21	Türkiye
178.132.48.0/21	Türkiye
178.210.160.0/19	Türkiye
178.211.32.0/19	Türkiye
178.211.192.0/19	Türkiye
178.233.0.0/16	Türkiye
178.240.0.0/13	Türkiye
178.250.88.0/21	Türkiye
178.251.40.0/21	Türkiye
185.3.56.0/22	Türkiye
185.4.68.0/22	Türkiye
185.4.208.0/22	Türkiye
185.4.224.0/22	Türkiye
185.5.176.0/22	Türkiye
185.7.0.0/22	Türkiye
185.7.80.0/22	İngiltere
185.7.176.0/22	Türkiye
185.8.12.0/22	Türkiye
185.8.32.0/22	Türkiye
185.8.128.0/22	Türkiye
185.9.36.0/22	Türkiye
185.9.156.0/22	Türkiye
185.9.220.0/22	Türkiye
185.11.12.0/22	Türkiye
185.11.212.0/22	Türkiye
185.11.248.0/22	Türkiye
185.12.108.0/22	Türkiye
185.12.224.0/22	Türkiye

185.13.56.0/22	Türkiye
185.14.20.0/22	Türkiye
185.14.64.0/22	Türkiye
185.14.172.0/22	Türkiye
185.15.40.0/22	Türkiye
185.15.196.0/22	Türkiye
185.16.236.0/22	Türkiye
185.17.112.0/22	Türkiye
185.17.136.0/22	Türkiye
185.19.80.0/22	Türkiye
185.19.92.0/22	Türkiye
185.21.4.0/22	Türkiye
185.21.204.0/22	Türkiye
185.22.56.0/22	Türkiye
185.22.100.0/22	Türkiye
185.22.160.0/22	Türkiye
185.22.184.0/22	Türkiye
185.22.248.0/22	Türkiye
185.23.72.0/22	Türkiye
185.24.80.0/22	İngiltere
185.24.124.0/22	Türkiye
185.25.100.0/22	Türkiye
185.26.68.0/22	Türkiye
185.26.144.0/22	Türkiye
185.28.0.0/22	Türkiye
185.28.60.0/22	Türkiye
185.28.132.0/22	Türkiye
185.28.160.0/22	Türkiye
185.29.120.0/22	Türkiye
185.29.192.0/22	Türkiye
185.32.12.0/22	Türkiye
185.33.60.0/22	Türkiye
185.33.108.0/22	Türkiye
185.33.128.0/22	Türkiye
185.33.232.0/22	Kıbrıs
185.34.128.0/22	Türkiye
185.35.20.0/22	Türkiye
185.40.72.0/22	Türkiye
185.40.84.0/22	Türkiye
185.42.172.0/22	Türkiye
185.43.228.0/22	Türkiye
185.44.192.0/22	Türkiye
185.46.40.0/22	Türkiye
185.46.52.0/22	Türkiye
185.48.24.0/22	Türkiye

185.48.180.0/22	Türkiye
185.48.212.0/22	Türkiye
185.49.44.0/22	Türkiye
185.49.68.0/22	Almanya
185.49.128.0/22	Türkiye
185.50.68.0/22	Türkiye
185.51.24.0/22	Kıbrıs
185.51.36.0/22	Türkiye
185.51.112.0/22	Türkiye
185.51.164.0/22	Türkiye
185.52.228.0/22	Türkiye
185.53.60.0/22	Türkiye
185.54.88.0/22	Türkiye
185.56.236.0/22	Türkiye
185.57.64.0/22	Türkiye
185.57.244.0/22	Türkiye
185.58.244.0/22	Türkiye
185.59.28.0/22	Türkiye
185.59.44.0/22	Türkiye
185.59.72.0/22	Türkiye
185.60.224.0/22	Türkiye
185.61.44.0/22	Türkiye
185.64.80.0/22	Türkiye
185.65.68.0/22	Türkiye
185.65.204.0/22	Türkiye
185.66.124.0/22	Türkiye
185.67.32.0/22	Türkiye
185.67.120.0/22	Türkiye
185.67.124.0/22	Türkiye
185.67.204.0/22	Türkiye
185.68.220.0/22	Türkiye
185.70.84.0/22	Türkiye
185.70.96.0/22	Türkiye
185.70.140.0/22	Türkiye
185.71.116.0/22	Türkiye
185.72.252.0/22	Türkiye
185.73.128.0/22	ABD
185.73.200.0/22	Türkiye
185.76.140.0/22	Türkiye
185.76.152.0/22	Türkiye
185.76.196.0/22	Türkiye
185.76.200.0/22	Türkiye
185.77.0.0/22	Türkiye
185.77.40.0/22	Türkiye
185.77.88.0/22	Türkiye

185.78.84.0/22	Türkiye
185.79.12.0/22	Türkiye
185.80.20.0/22	Türkiye
185.80.72.0/22	Türkiye
185.80.136.0/22	Türkiye
185.81.152.0/22	Türkiye
185.81.236.0/22	Türkiye
185.82.220.0/22	Türkiye
185.82.252.0/22	Türkiye
185.83.144.0/22	Türkiye
185.83.244.0/22	Türkiye
185.84.180.0/22	Türkiye
185.85.72.0/22	Türkiye
185.85.104.0/22	Türkiye
185.85.188.0/22	Türkiye
185.85.204.0/22	Türkiye
185.85.236.0/22	Türkiye
185.86.4.0/22	Türkiye
185.86.12.0/22	Türkiye
185.86.80.0/22	Türkiye
185.86.152.0/22	Türkiye
185.86.164.0/22	Türkiye
185.86.244.0/22	Türkiye
185.87.24.0/22	Türkiye
185.87.120.0/22	Türkiye
185.87.172.0/22	Türkiye
185.87.252.0/22	Türkiye
185.88.4.0/22	Türkiye
185.88.172.0/22	Türkiye
185.90.4.0/22	Türkiye
185.90.80.0/22	Türkiye
185.90.240.0/22	Türkiye
185.92.0.0/22	Türkiye
185.92.12.0/22	Türkiye
185.92.212.0/22	Türkiye
185.93.52.0/22	Türkiye
185.93.68.0/22	Türkiye
185.93.248.0/22	Türkiye
185.95.0.0/22	Türkiye
185.95.84.0/22	Türkiye
185.95.120.0/22	Türkiye
185.95.168.0/22	Türkiye
185.96.52.0/22	Türkiye
185.96.112.0/22	Türkiye
185.96.168.0/22	Türkiye

185.96.192.0/22	Türkiye
185.97.8.0/22	Türkiye
185.98.60.0/22	Türkiye
185.98.136.0/22	Türkiye
185.98.216.0/22	Türkiye
185.98.252.0/22	Türkiye
185.99.20.0/22	Türkiye
185.102.36.0/22	Türkiye
185.103.196.0/22	Türkiye
185.104.20.0/22	Türkiye
185.105.68.0/22	Türkiye
185.106.20.0/22	Türkiye
185.106.208.0/22	Türkiye
185.107.132.0/22	Türkiye
185.108.124.0/22	Türkiye
185.108.148.0/22	Türkiye
185.108.156.0/22	Türkiye
185.109.28.0/22	Türkiye
185.110.240.0/22	Türkiye
185.111.232.0/22	Türkiye
185.111.244.0/22	Türkiye
185.113.8.0/22	Türkiye
185.113.220.0/22	Türkiye
185.114.20.0/22	Türkiye
185.114.192.0/22	Türkiye
185.115.40.0/22	Türkiye
185.115.208.0/22	Türkiye
185.116.152.0/22	Türkiye
185.117.120.0/22	Türkiye
185.118.140.0/22	Türkiye
185.118.192.0/22	Türkiye
185.119.80.0/22	Türkiye
185.121.124.0/22	Türkiye
185.122.12.0/22	Türkiye
185.122.200.0/22	Türkiye
185.123.0.0/22	Türkiye
185.123.100.0/22	Türkiye
185.123.104.0/22	Türkiye
185.124.84.0/22	Türkiye
185.125.32.0/22	Türkiye
185.126.176.0/22	Türkiye
185.126.216.0/22	Türkiye
188.3.0.0/16	Türkiye
188.38.0.0/16	Türkiye
188.41.0.0/16	Türkiye
188.56.0.0/14	Türkiye
188.64.208.0/21	Türkiye
188.95.144.0/21	Türkiye
188.119.0.0/18	Türkiye
188.124.0.0/19	Türkiye
188.125.160.0/19	Türkiye
188.132.128.0/17	Türkiye
193.140.0.0/16	Türkiye
193.192.96.0/19	Türkiye
193.243.192.0/19	Türkiye
193.255.0.0/16	Türkiye
194.27.0.0/16	Türkiye
194.54.32.0/19	Türkiye
195.33.192.0/18	Türkiye
195.46.128.0/19	Türkiye
195.87.0.0/16	Türkiye
195.112.128.0/19	Türkiye
195.142.0.0/22	Türkiye
195.142.4.0/22	Türkiye
195.142.8.0/21	Türkiye
195.142.16.0/20	Türkiye
195.142.32.0/19	Türkiye
195.142.64.0/19	Türkiye
195.142.96.0/21	Türkiye
195.142.104.0/21	Türkiye
195.142.112.0/20	Türkiye
195.142.128.0/22	Türkiye
195.142.132.0/22	Türkiye
195.142.136.0/21	Türkiye
195.142.144.0/21	Türkiye
195.142.152.0/22	Türkiye
195.142.156.0/22	Türkiye
195.142.160.0/20	Türkiye
195.142.176.0/21	Türkiye
195.142.184.0/22	Türkiye
195.142.188.0/22	Türkiye
195.142.192.0/22	Türkiye
195.142.196.0/22	Türkiye
195.142.200.0/22	Türkiye
195.142.204.0/22	Türkiye
195.142.208.0/22	Türkiye
195.142.212.0/22	Türkiye
195.142.216.0/21	Türkiye
195.142.224.0/20	Türkiye
195.142.240.0/22	Türkiye
195.142.244.0/22	Türkiye
195.142.248.0/21	Türkiye
195.155.0.0/18	Türkiye
195.155.64.0/19	Türkiye
195.155.96.0/22	Türkiye
195.155.100.0/22	Türkiye
195.155.104.0/21	Türkiye
195.155.112.0/20	Türkiye
195.155.128.0/19	Türkiye
195.155.160.0/19	Türkiye
195.155.192.0/18	Türkiye
195.174.0.0/16	Türkiye
195.175.0.0/16	Türkiye
195.214.128.0/18	Türkiye
195.244.32.0/19	Türkiye
212.2.192.0/19	Türkiye
212.12.128.0/19	Türkiye
212.15.0.0/19	Türkiye
212.29.64.0/18	Türkiye
212.31.0.0/19	Türkiye
212.50.32.0/19	Türkiye
212.57.0.0/19	Türkiye
212.58.0.0/19	Türkiye
212.64.192.0/19	Türkiye
212.65.128.0/19	Türkiye
212.68.32.0/19	Türkiye
212.98.0.0/19	Türkiye
212.98.192.0/18	Türkiye
212.101.96.0/19	Türkiye
212.108.128.0/19	Türkiye
212.109.96.0/19	Türkiye
212.109.224.0/19	Türkiye
212.115.0.0/19	Türkiye
212.125.0.0/19	Türkiye
212.127.96.0/19	Türkiye
212.133.128.0/17	Türkiye
212.146.128.0/17	Türkiye
212.154.0.0/17	Türkiye
212.156.0.0/16	Türkiye
212.174.0.0/16	Türkiye
212.175.0.0/16	Türkiye
212.252.0.0/16	Türkiye
212.253.0.0/16	Türkiye
213.14.0.0/17	Türkiye
213.14.128.0/20	Türkiye

213.14.144.0/20	Türkiye
213.14.160.0/19	Türkiye
213.14.192.0/18	Türkiye
213.43.0.0/16	Türkiye
213.74.0.0/16	Türkiye
213.128.64.0/19	Türkiye
213.139.192.0/19	Türkiye
213.139.224.0/19	Türkiye
213.142.128.0/19	Türkiye
213.143.224.0/19	Türkiye
213.144.96.0/19	Türkiye
213.148.64.0/19	Türkiye
213.153.128.0/19	Türkiye
213.153.160.0/19	Türkiye
213.153.192.0/18	Türkiye
213.155.96.0/19	Türkiye
213.159.28.0/22	Türkiye
213.161.128.0/19	Türkiye
213.186.128.0/19	Türkiye
213.194.64.0/18	Türkiye
213.211.0.0/19	Türkiye
213.232.0.0/18	Türkiye
213.238.128.0/18	Türkiye
213.243.0.0/19	Türkiye
213.243.32.0/19	Türkiye
213.248.128.0/18	Türkiye
213.254.128.0/19	Türkiye
217.17.144.0/20	Türkiye
217.31.224.0/20	Türkiye
217.31.240.0/20	Türkiye
217.64.208.0/20	Türkiye
217.65.176.0/20	Türkiye
217.68.208.0/20	Türkiye
217.74.24.0/21	Türkiye
217.78.96.0/20	Türkiye
217.116.192.0/20	Türkiye
217.131.0.0/16	Türkiye
217.169.192.0/20	Türkiye
217.174.32.0/20	Türkiye
217.195.192.0/20	Türkiye
91.142.142.0/24	Türkiye
91.195.138.0/23	Türkiye
91.198.49.0/24	Türkiye
91.198.61.0/24	Türkiye
91.198.124.0/24	Türkiye
91.199.73.0/24	Türkiye
91.199.111.0/24	Türkiye
91.199.166.0/24	Türkiye
91.199.191.0/24	Türkiye
91.208.61.0/24	Türkiye
91.208.70.0/24	Türkiye
91.208.199.0/24	Türkiye
91.212.126.0/24	Türkiye
91.212.178.0/24	Türkiye
91.213.1.0/24	Türkiye
91.213.245.0/24	Türkiye
91.213.253.0/24	Türkiye
91.213.254.0/24	Türkiye
91.216.91.0/24	Türkiye
91.216.98.0/24	Türkiye
91.216.119.0/24	Türkiye
91.216.148.0/24	Türkiye
91.216.170.0/24	Türkiye
91.216.201.0/24	Türkiye
91.216.223.0/24	Türkiye
91.217.147.0/24	Türkiye
91.217.193.0/24	Türkiye
91.217.238.0/24	Türkiye
91.220.50.0/24	Türkiye
91.220.65.0/24	Türkiye
91.220.182.0/24	Türkiye
91.220.242.0/24	Türkiye
91.223.0.0/24	Türkiye
91.223.8.0/24	Türkiye
91.223.157.0/24	Türkiye
91.227.4.0/23	Türkiye
91.227.6.0/24	Türkiye
91.228.169.0/24	Türkiye
91.228.255.0/24	Türkiye
91.229.34.0/24	Türkiye
91.229.35.0/24	Türkiye
91.229.44.0/23	Türkiye
91.229.155.0/24	Türkiye
91.229.184.0/24	Türkiye
91.230.73.0/24	Türkiye
91.230.81.0/24	Türkiye
91.230.85.0/24	Türkiye
91.232.174.0/24	Türkiye
91.233.80.0/24	Türkiye
91.235.64.0/24	Türkiye
91.235.104.0/23	Türkiye
91.237.216.0/23	Türkiye
91.239.204.0/24	Türkiye
91.239.242.0/24	Türkiye
91.240.26.0/24	Türkiye
91.240.37.0/24	Türkiye
91.240.108.0/24	Türkiye
91.244.116.0/24	Türkiye
91.244.226.0/24	Türkiye
91.244.227.0/24	Türkiye
139.179.0.0/16	Türkiye
144.122.0.0/16	Türkiye
155.223.0.0/16	Türkiye
160.75.0.0/16	Türkiye
161.9.0.0/16	Türkiye
168.139.0.0/16	Türkiye
176.117.96.0/21	Türkiye
192.70.133.0/24	Hollanda
192.70.134.0/24	Hollanda
192.129.87.0/24	Türkiye
192.160.21.0/24	Türkiye
193.23.156.0/24	Türkiye
193.25.124.0/23	Türkiye
193.28.225.0/24	Türkiye
193.32.53.0/24	Türkiye
193.32.55.0/24	Türkiye
193.34.132.0/23	Türkiye
193.34.205.0/24	Türkiye
193.36.0.0/24	Türkiye
193.36.39.0/24	Türkiye
193.36.184.0/24	Türkiye
193.37.135.0/24	Türkiye
193.37.154.0/24	Türkiye
193.41.2.0/23	Türkiye
193.41.225.0/24	Türkiye
193.42.216.0/24	Türkiye
193.58.236.0/24	Türkiye
193.104.13.0/24	Türkiye
193.104.109.0/24	Türkiye
193.104.124.0/24	Türkiye
193.104.130.0/24	Türkiye
193.104.138.0/24	Türkiye
193.104.201.0/24	Türkiye
193.105.208.0/24	Türkiye
193.105.211.0/24	Türkiye

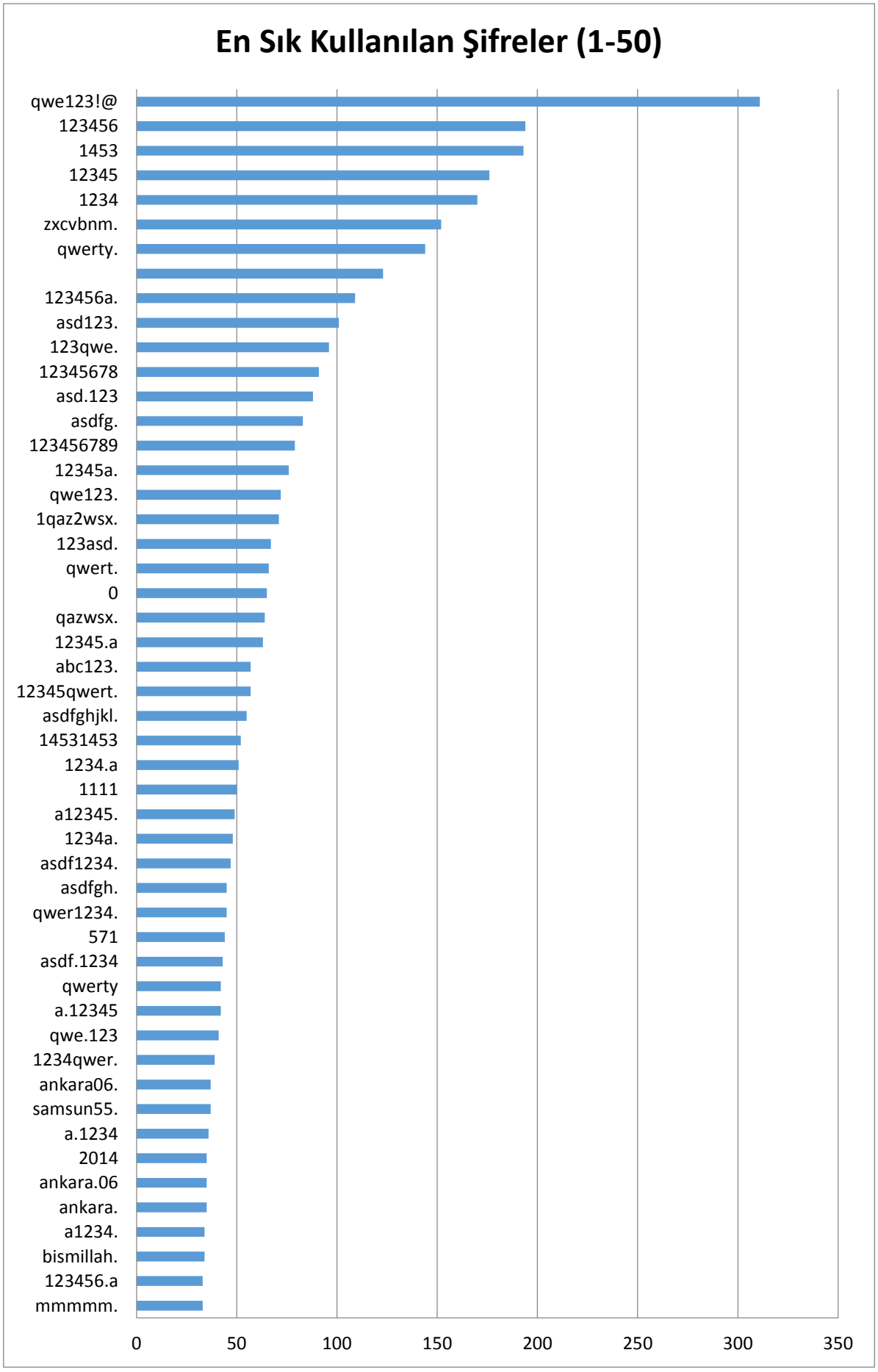
193.105.234.0/24	Türkiye
193.105.243.0/24	Türkiye
193.108.213.0/24	Türkiye
193.109.134.0/23	Türkiye
193.110.170.0/23	Türkiye
193.110.208.0/21	Türkiye
193.138.116.0/24	Türkiye
193.143.226.0/24	Türkiye
193.164.9.0/24	Türkiye
193.169.50.0/24	Türkiye
193.186.208.0/24	Türkiye
193.189.142.0/24	Türkiye
193.200.170.0/24	Türkiye
193.200.180.0/24	Türkiye
193.200.188.0/24	Türkiye
193.202.18.0/24	Türkiye
193.202.120.0/24	Türkiye
193.218.113.0/24	Türkiye
193.223.76.0/24	Türkiye
193.238.25.0/24	Türkiye
193.254.228.0/23	Türkiye
193.254.252.0/23	Türkiye
194.0.130.0/24	Türkiye
194.0.142.0/24	Türkiye
194.0.178.0/24	Türkiye
194.0.202.0/24	Türkiye
194.24.168.0/23	Türkiye
194.24.224.0/23	Türkiye
194.29.208.0/21	Türkiye
194.32.84.0/23	Türkiye
194.36.160.0/24	Türkiye
194.49.126.0/24	Türkiye
194.50.84.0/24	Türkiye
194.50.179.0/24	Türkiye
194.60.73.0/24	Türkiye
194.107.22.0/24	Türkiye
194.110.150.0/24	Türkiye
194.110.213.0/24	Türkiye
194.125.232.0/22	Türkiye
194.126.230.0/24	Türkiye
194.140.227.0/24	Türkiye
194.156.165.0/24	Türkiye
194.242.32.0/24	Türkiye
194.247.59.0/24	Türkiye
195.8.109.0/24	Türkiye

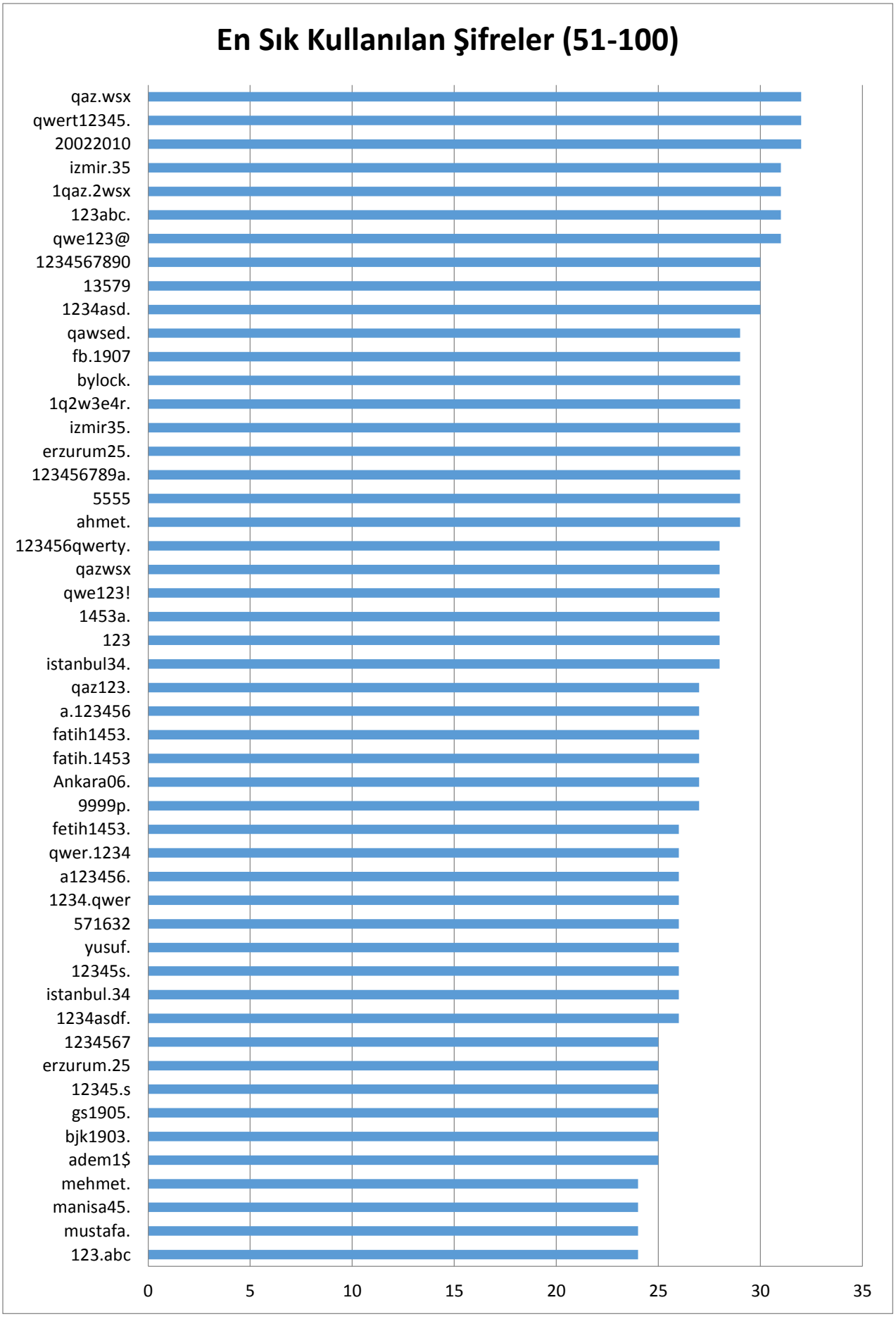
195.39.224.0/23	Türkiye
195.49.216.0/21	Türkiye
195.62.35.0/24	Türkiye
195.85.242.0/24	Türkiye
195.85.255.0/24	Türkiye
195.95.149.0/24	Türkiye
195.95.160.0/24	Türkiye
195.95.179.0/24	Türkiye
195.128.32.0/21	Türkiye
195.137.222.0/23	Türkiye
195.140.196.0/22	Türkiye
195.149.85.0/24	Türkiye
195.149.116.0/24	Türkiye
195.177.206.0/23	Türkiye
195.182.25.0/24	Türkiye
195.182.42.0/24	Türkiye
195.190.20.0/24	Türkiye
195.191.118.0/23	Türkiye
195.200.222.0/24	Türkiye
195.216.232.0/24	Türkiye
195.226.196.0/24	Türkiye
195.226.221.0/24	Türkiye
195.234.52.0/24	Türkiye
195.234.165.0/24	Türkiye
195.245.227.0/24	Türkiye

Ek-11: Çözümlenen Şifrelere İlişkin İstatistiki Veriler

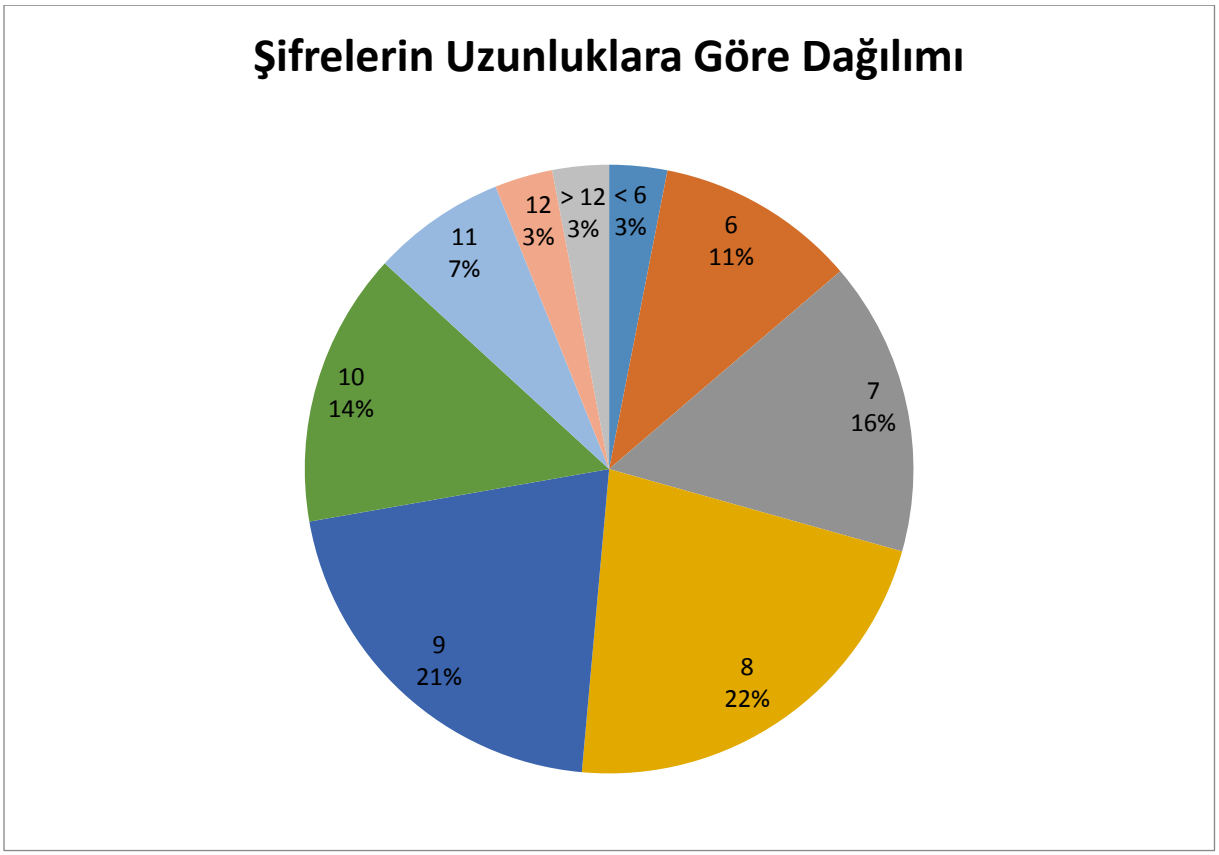
215.092 adet kriptografik MD5 özetinden yaklaşık %85'i çözülenmiş olup en sık görülen 50 şifreye aşağıda yer verilmiştir:

Sıra no:	**Şifre:**	**Sıra no:**	**Şifre:**
1	qwe123!@	**26**	asdfghjkl.
2	123456	**27**	14531453
3	1453	**28**	1234.a
4	12345	**29**	1111
5	1234	**30**	a12345.
6	zxcvbnm.	**31**	1234a.
7	qwerty.	**32**	asdf1234.
8		**33**	qwer1234.
9	123456a.	**34**	asdfgh.
10	asd123.	**35**	571
11	123qwe.	**36**	asdf.1234
12	12345678	**37**	a.12345
13	asd.123	**38**	qwerty
14	asdfg.	**39**	qwe.123
15	123456789	**40**	1234qwer.
16	12345a.	**41**	**samsun55.**
17	qwe123.	**42**	ankara06.
18	1qaz2wsx.	**43**	a.1234
19	123asd.	**44**	**ankara.**
20	qwert.	**45**	**ankara.06**
21	0	**46**	2014
22	qazwsx.	**47**	**bismillah.**
23	12345.a	**48**	a1234.
24	12345qwert.	**49**	mmmmm.
25	abc123.	**50**	123456.a


En Sık Kullanılan Şifreler (1-50)
qwe123!@
123456
1453
12345
1234
zxcvbnm.
qwerty.
123456a.
asd123.
123qwe.
12345678
asd.123
asdfg.
123456789
12345a.
qwe123.
1qaz2wsx.
123asd.
qwert.
0
qazwsx.
12345.a
abc123.
12345qwert.
asdfghjkl.
14531453
1234.a
1111
a12345.
1234a.
asdf1234.
asdfgh.
qwer1234.
571
asdf.1234
qwerty
a.12345
qwe.123
1234qwer.
ankara06.
samsun55.
a.1234
2014
ankara.06
ankara.
a1234.
bismillah.
123456.a
mmmmm.
0
50
100
150
200
250
300
350


En Sık Kullanılan Şifreler (51-100)
qaz.wsx
qwert12345.
20022010
izmir.35
1qaz.2wsx
123abc.
qwe123@
1234567890
13579
1234asd.
qawsed.
fb.1907
bylock.
1q2w3e4r.
izmir35.
erzurum25.
123456789a.
5555
ahmet.
123456qwerty.
qazwsx
qwe123!
1453a.
123
istanbul34.
qaz123.
a.123456
fatih1453.
fatih.1453
Ankara06.
9999p.
fetih1453.
qwer.1234
a123456.
1234.qwer
571632
yusuf.
12345s.
istanbul.34
1234asdf.
1234567
erzurum.25
12345.s
gs1905.
bjk1903.
adem1$
mehmet.
manisa45.
mustafa.
123.abc
0
5
10
15
20
25
30
35

Çözümlenen şifrelerin yaklaşık yarısının uzunluğu 9 karakterden fazladır. Şifre uzunluklarına göre dağılım grafiği aşağıda sunulmuştur:



En uzun şifre örnekleri:

- 1qaz2wsx3edc4rfv5tgb6yhn7ujm8ik,9ol.0p
- Selam.2010-Selam.2010-
- tedbirieldenbirakma.01
- qwertyuiop1234567890@#$
- asdfghjkl1234567890.....
- Pass.11111111111111111111
- olmakyadaolmamak123.
- Yahaf1z99.Yahaf1z99.