

Content Search Made within the Disk Image of Phone Belonging to Taner KILIC And the Expert Opinion

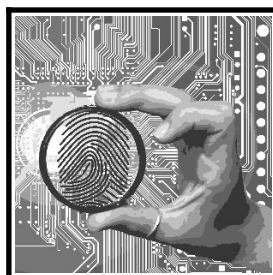
Dear Atty.,

This report is written following your request to detect whether the ByLock messaging application, which allegedly established connection over a line belonging to your client Taner Kilic, was installed to his phone, and whether there were traces of this application on the phone if the application was installed and removed.

The findings of examination, technical information and other important issues are submitted for your review in this report.

T. Koray Peksayar

B.Sc. in Mechanical Eng. – M.Sc. in Information Tech.
Information and Digital Forensic Expert – Chartered Judicial Expert
ITU M.Sc. Dip. No. 76-387



About the Expert

I was born in Istanbul in 1975. I completed the preparatory school, middle school and high school at Nişantaşı Anatolian High School. I graduated from Nişantaşı Anatolian High School Science-Mathematics branch.

I completed my undergraduate education at Istanbul University, Faculty of Engineering, and Department of Mechanical Engineering.

I received my graduate education on Information Technologies at Istanbul Technical University Informatics Institute.

I began to work on electronics, computers and network systems as an amateur in my middle school years, and at the end of my high school years I started to work as a professional.

During the last 3 years of my undergraduate education and during my graduate studies, I continued my professional work on computer and network systems. Within the scope of this time period, I have worked in more than one company, especially on web applications, network and intranet systems and information systems improvement.

As of 1998, I started working on software development, software performance, system performance, system reliability and system security.

During these studies I gained experience on many versions of the Windows operating system, popular application softwares and the undocumented modes and behaviors of these software.

Starting 1999, I have focused on Linux based operating systems as well as Windows based systems.

Since 2000, I have been developing services, products and solutions in my own company with the effective use of Linux and other UNIX based operating systems, telecommunication, software development, software performance, system performance, system reliability and system security.

Since 2003, I am a licensed amateur radio operator, I dabble in radios and volunteer in emergency communications.

Since 2010, I have been registered as a chartered judicial expert on the list of experts in First Instance Court of Istanbul Forensic Jurisdiction by means of being an independent scientist in the field of frequently used information and communication systems in order to provide help to the justice with the experience I have gained over many years and the scientific education I have taken.

I still continue my duty as a chartered judicial expert and I am registered at the First Instance Court of Istanbul Forensic Jurisdiction on the 230th page of the 2017 Criminal Expert List with the sequence number of 3852 and application number of 4269.

Among the subjects I served as a registered in the Istanbul Criminal Expert List, there are; computer technologies, information technologies, information technology communication, data processing, digital crimes, computer programming, computer software development, computer and security systems, CD / DVD analysis, digital evidence review, image processing and social media.

During my period of expertise which began in 2010, I was directly appointed as an expert by assize court, criminal court of first instance, civil court of first instance, juvenile court, civil court for intellectual and industrial property, labour and criminal court of peace that are established in Istanbul.

Since 2012, I have been involved in scientific examinations for various cases, which were demanded expert opinions by attorneys, and I have reported the findings of these examinations.

Among the above-mentioned cases, there are "Balyoz", "Ergenekon", "Poyrazköy", "Operation Cage Action Plan", "ÇYDD (Association for Supporting Contemporary Life)" and "Military Espionage and Blackmail" cases.

In particular, I am one of the first experts to detect the contradictions in digital evidences, technical irregularities and suspects of alteration after seizure in cases of "Balyoz", "Poyrazköy" and "ÇYDD".

All of my findings related to the "Balyoz" case were approved by Istanbul Technical University researchers (2nd time) who were appointed by Istanbul Anatolian 4th Assize Court and the trial was concluded in acquittance.

All of my findings of the "Poyrazköy" case consisting of the sub-cases of "ÇYDD", "Cage Action Plan" and "Assassination Attempt to Admirals" were investigated and approved by the researchers (3rd time) of Ministry of Justice Forensic Medicine Institution Department of Physical Principles Information and Technology Crime Branch who were appointed by the Istanbul Anatolian 5th Assize Court and the trial was concluded in acquaintance.

In both cases, allegation made against those who created fake evidences, and an investigation was ordered.

The reports and opinions I presented regarding "*Balyoz*" case are mentioned on page 24 of Constitutional Court decision with application number 2013/7800 dated 18/6/2014 and on pages 109, 392, 602, 657, 658, 730 and 739 of justified decision of Istanbul Anatolian 5th Assize Court dated 31/03/2015.

The reports and opinions I presented regarding "*Poyrazköy*" case are mentioned on pages 31 and 46 of justified decision of Istanbul Anatolian 5th Assize Court.

Disregarding the reports and opinions I presented on "*Ergenekon*" case and refusal of my speech on court by the court were considered among the justifications for judgement reversal on page 56 of the decision of Court of Cassation 16th Criminal Chamber dated 21/04/2016.

Scientific Examination and Expert Opinion

1. Purpose and Scope

This report is written on the digital forensics examination of the backup of Taner Kilic's phone, following your request to detect whether the ByLock messaging application, which allegedly established connection over a line belonging to your client Taner Kilic, was installed to his phone, and whether there were traces of this application on the phone if the application was installed and removed.

This report also presents issues, technical information, and other important aspects that were encountered during the examination.

Taking into consideration the necessity of possessing technical knowledge to understand the subject, details of technical information is presented in a plain language wherever possible.

Despite being a report to provide expert opinion, the examination in this report is conducted objectively in a manner equivalent to an expert witness report, and the technical information provided reflects the empirical reality.

Names of brands, models and software mentioned in this report are included to facilitate the understanding of the methodology followed in this report, and to facilitate the verification of the report when examined by other experts and they are not intended to serve any other purposes such as praising, promoting, or advertising a product or service.

2. General Information

2.1. Digital Evidence: Qualification of Electronically Stored Files as Documents

One of the most important debates in computer sciences regarding issues of information, consciousness and semanticity is that data does not always constitute meaningful information.

Digital data has to constitute a consistent whole with other similar data in the same environment in order to be considered as information.

Since a digital log is also a database, it can be assured that it contains meaningful information assuming this database is accessed under certain rules and conditions.

To give an example from accounting software, which keeps records on a database, comparing only the data on debits with the data on credits just gives the balance of payments for the period under examination.

A meaningful piece of information on balance of payments is only possible when this data is associated with the customer data.

Also, customer registration numbers solely do not contain any meaningful information. This data should be interpreted with an external data in order to reach a meaningful piece of information.

If the person operating this process is unknown, this again will distort the cohesion of meaning.

When the information indicating the user who entered a specific record is missing, this record and all relevant records would become invalid, as it would cause instability in the whole system, influencing meaningfulness of information.

Inconsistencies in data also occur when data-recording operations are made through breaching the system security using a vulnerability and obtaining the password, or saving data on a system where a user had already logged on.

As a result, in order to consider data as a meaningful piece of information, it must be consistent with similar data in the same environment, it must be stored on a stable and secure system, and this system must be accessible only through certain rules and conditions.

Digital information can be created using any system, by anyone, and indicating any time. Today, authenticity and validity of data is provided with digital signatures.

Therefore, in order to obtain meaning, the collected set of data should be able to answer the 5W1H questions: “Who? What? When? Where? Why? How?”

In other words, an explanation such as “which data is created when, on which system and database, in which form and type, in relation to which data, and by whom?” must be provided.

When the aforementioned conditions are fulfilled, it can be said that the recorded data contains meaningful information, and it ensures qualifications of being a document.

2.2. Source of Digital Data

The data stored in the digital environment can be generated as desired and misleading; It can be created in a way that it has been generated by any other person or persons to show a time, to contain desired information, to have desired content, to give the impression that it is created by the desired person.

It is stated in the 1st clause of the 134th article of Procedure Law No. 5271 with the title “Search of computers, computer programs and transcripts, copying and provisional seizure”;

“The judge or, in cases of peril in delay, the public prosecutor, may decide to locate, listen to or record the correspondence, through telecommunication or to evaluate the information about the signals of the suspect or the accused, if during an investigation or prosecution conducted in relation to a crime there are strong grounds of suspicion indicating that the crime has been committed and there is no other possibility to obtain evidence.”

Technical evaluation and the law article cited above present the significance of the causal relation of numerical evidence.

According to the law, investigation should be conducted on the “computer, software and logs owned by the suspect”.

Today, computer and other information technology systems vary and those systems interact with closed^[1] and open^[2] networks, rather than working standalone.

Therefore, ownership of the every digital data, even though it is known that computers has been used by the user, even though every digital data, should be able to be audited and its source should be able to be investigated.

For example; it is possible for an image file on a computer that is connected to the Internet to arise from an advertisement on a website.

On the systems connected to open computer networks, involuntary and unintentional situations may also occur.

As an example, an application software bug that is not and cannot be known by the user, might be discovered by a 3rd party and this software bug might be exploited using the vulnerability.

Another example of situations that arise outside of the user’s will is that malicious software runs on the system with other purposes than the visible function.

For example, a computer game or software works as a screen saver on a system, may allow this system to be controlled remotely, files to be downloaded and installed without user’s consent, by using a backdoor.^{[3][4]}

If the file subject to an examination is a file that is known to be connected to a computer system or is detectable if it is a readable and writeable file, then it is possible to find traces of this file, it is possible to come across to the traces and remarks of this software in the digital evidence examined.

Since the systems that are used to generate logs of read-only and archival^[5] files are IT devices, it is possible to have traces of such software or any other traces in these systems.

2.3. The Concept of Image

The image is the name given to the exact copy of a device or media that stores the data.

A complete copy of all the data in a device is saved into a digital file using image creation process.

1 Local network systems. Intranet and similar systems

2 As systems connected to the Internet

3 See also: “Steal this book II” 66th page of the free e-book written on Internet security

4 See also: News about Italian Hacking Team firm <http://www.hurriyet.com.tr/dunya/29497905.asp>

5 CD, DVD etc.

Technical cause of the necessity of image creation, before digital forensic analysis and during the digital evidence collection process, is to avoid the probability of any physical damage taken by the device, which stores the data.

2.4. Technical Details of Image Creation

Generally, when data is being copied from data storage media, the source data is read as write-protected and the original data is checked against the copy destination.

“Image creation” process can be achieved on computers using special write-protected devices or directly from source data storage media to the data storage medium, where copy is going to be taken on the devices, which specifically designed for this purpose.

After copying process original data should be checked against the copy data, in order to verify whether they are identical or not. Therefore, for detecting and verifying if every bits of the original evidence is identical to the copied data, hash values are obtained using cryptographic hash functions.

When obtained hash values are identical, it becomes verified that copy and original mediums are the same.

Hash values determined in the evidence collection process are also used to provide evidence integrity at later stages.

In order to ensure the integrity of evidence in digital forensics, it is necessary to ensure that the evidence does not change from the collection phase to the end of the examination phase.

Thus, the examiners will do the necessary examination on a copy of the original evidence, not the physical one. This subject is the most important digital forensics application of the immutability of evidence principle.

Before the examination, by calculating the hash value of the copy handed to them, experts should verify the equivalency of this value with the calculated value during the collection phase, in other words sameness of copy and original data.

If this audit is not concluded with equivalency, it will not be possible to conduct an examination because the integrity of the evidence cannot be achieved.

2.5. The Concept of Hash Value (Cryptographic Hash)

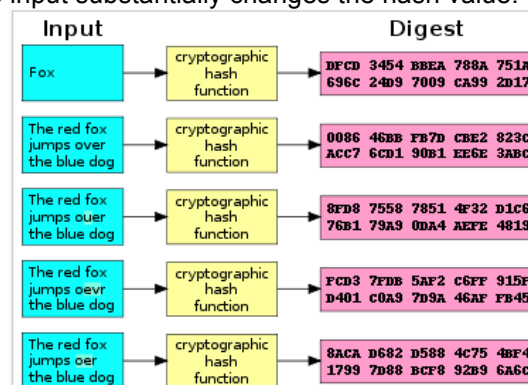
Cryptographic Hash^[6] Function is a hash function that provides various security features.

Cryptographic Hash Function converts the data to a bit series that has a certain length, (cryptographic) hash value.

In short, it makes the digital representation of a long data into a shorter data. This conversion changes its hash value^[7] in any case of modification.

For example, the generated hashes by a cryptographic hash function SHA1 for different inputs are represented in the graph below.

Even the tiniest alteration on the input substantially changes the hash value. This is called as avalanche effect.



Data that is to be hashed is named as “message”, hash value as “message hash” or also briefly “hash”.

⁶ Cited from Wikipedia's “Cryptographic Hash Function” article. https://tr.wikipedia.org/wiki/Kriptografik_%C3%B6zet_fonksiyonu

⁷ English: Hash value

An ideal cryptographic hash function should demonstrate four features below:

1. It should be easy to generate a hash for any message.
2. It should be difficult to create a message that corresponds to a hash.
3. It should be difficult to change the message in a way that hash will.
4. It should be difficult to find two different messages that have the same hash.

Cryptographic Hash Functions are commonly used in information technology areas such as digital signature, message verification code and other verification methods.

As other hash functions, they are also used to index data in hash tables, to find equivalent data, to detect duplicate data or uniquely identify files and provide data integrity.

In information-security contexts, cryptographic hash values are sometimes called “digital fingerprints”, “checksums”, and “hash values” even though all these terms stand for more general functions with rather different properties and purposes.

2.6. Use of Hash Value in Verification of File or Message Integrity

Verification of message integrity is one of the significant uses of secure hashes.

It is possible to figure out whether there is any change in a message or file by comparing calculated hashes before and after the delivery or any other event.

Most of the digital signature algorithms only verify the hash instead of verifying the whole message.

If the authenticity of the hash is preserved, it is accepted as a sufficient evidence for the authenticity of the message itself being preserved.

Immutability of the evidence is the primary consideration of digital forensic.

For digital forensic investigations, the image copies of the digital files and data storage devices are hashed and officially recorded, in order to ensure immutability.

By the requirement of aforementioned feature, cryptographic hash functions would generate different hash values when different sets of data are processed.

However, randomly and at low rates of probability, some cryptographic hash functions are known to be calculating same hash values for different data sets due to their working principles.

This case is known as “collision” and with the purpose of preventing this case in digital forensic practice, the most quickly found and fastest working 2 or more cryptographic hash functions are used and calculated hash values are recorded.

The most frequently used cryptographic hash functions are MD5 and SHA1 due to ease of use and pace.

2.7. Digital Data as Evidence, and Hash Value in Turkish Law

The most important article about protection and verification of data as evidence is the article 134 of the Criminal Procedure Law No. 5271 with the title “Search of computers, computer programs and transcripts, copying and provisional seizure”.

In this article;

“(1) Upon the motion of the public prosecutor during an investigation with respect to a crime, the judge shall issue a decision on the search of computers and computer programs and records used by the suspect, the copying, analyzing, and textualization of those records, if it is not possible to obtain the evidence by other means.

“(2) If computers, computer programs and computer records are inaccessible, as the passwords are not known, or if the hidden information is unreachable, then the computer and equipment that are deemed necessary may be provisionally seized in order to retrieve and to make the necessary copies. Seized devices shall be returned without delay in cases where the password has been solved and the necessary copies are produced.

“(3) While enforcing the seizure of computers or computer records, all data included in the system shall be

copied.

(4) In cases where the suspect or his representative makes a request, a copy of this copied data shall be produced and given to him or to his representative and this exchange shall be recorded and signed.

(5) It is also permissible to produce a copy of the entire data or some of the data included in the system, without seizing the computer or the computer records. Copied data shall be printed on paper and this situation shall be recorded and signed by the related persons."

Laws are recorded.

These sentences was modified with the clause (j) of the 1st paragraph in the 3rd article of "Decree Law on the Measures to be Taken in the Context of the State of Emergency and Regulation on the Arrangement of Some Institutions and Organizations" with no. 668, in 25/7/2016 as:

"Searches, copies and seizures regarding computers, computer programs and databases under Article 134 of the Law no. 5271 can be ordered by the public prosecutor as well, in cases where there is peril in delay.

Such orders shall be submitted to the competent judge for approval within five days. The judge shall announce the decision within ten days following the seizure; otherwise the seizure shall be automatically lifted.

In case the copying and backup process will take a long time, these tools and devices may also be seized. The devices seized shall be returned without delay once the process has been completed."

Also in Law No: 5070 on Electronic Signature, the requirements and actions to be taken to ensure the time of acquisition and immutability of digital data, is explained in the parts especially time stamping is discussed.

In the 3rd article of Electronic Signature^[8] Law^[9], electronic signature is defined as "Electronic data that are attached to another electronic data or has logical link with that electronic data and used for authentication purposes".

In the 3rd article of Electronic Signature Law, Timestamp^[10] is defined as: "A record signed electronically by the ECSP (Electronic Certificate Service Provider) for the purpose of verification of the exact time of creation, alteration, sending, receiving and/or recording of an electronic data".

Timestamps are used to prove that all kind of important electronic data such as documents and contracts existed before a certain time.

3. Regarding IMEI^[11] Numbers

The International Mobile Equipment Identity is a unique number to identify phones that are registered in the 3GPP standard family^[12] networks, iDEN networks, as well as some satellite phones.

It is usually found printed inside the battery compartment of the phone, but can also be displayed on-screen on most phones by entering *#06# on the dialpad, or alongside other system information in the settings menu on smartphone operating systems.

The IMEI is only used for identifying the device and has no permanent or semi-permanent relation to the subscriber.

An IMSI^[13] number identifies the subscriber instead - which is stored on a SIM card and can be transferred to any mobile device. However, many network and security features are enabled on subscriber's current device on purpose.

8 E-Signature Portal <http://www.e-imza.gen.tr/>

9 Law no: 5070 on Electronic Signature <http://www.tbmm.gov.tr/kanunlar/k5070.html>

10 Welcome Time Stamp (Article) <http://www.e-imza.gen.tr/index.php?Page=KoseYazisi&YaziNo=30&YazarNo=31>

11 International Mobile Device Identity

12 GSM, UMTS ve LTE

13 International Mobile Subscriber Identity

3.1. IMEI and Legislation

Many countries have accepted use of IMEI due to its efficiency in diminishing mobile phone theft.

For example; changing IMEI of a mobile phone or possessing any hardware capable of doing that is considered as crime according to mobile phones re-programming act in United Kingdom.

IMEI blocking is not the only approach in fight with mobile phone theft.

For example; mobile operators in Singapore are not required by the regulator to implement phone blocking or tracing systems, based on IMEI or any other method. The regulator has expressed its doubts on the effectiveness of this kind of system in the context of the mobile market in Singapore. Instead, mobile operators are recommended to take measures such as the immediate suspension of service and the replacement of SIM cards in case of loss or theft.

The existence of a formally allocated IMEI number range for a GSM terminal does not mean that the terminal is approved or complies with regulatory requirements.

The link between regulatory approval and IMEI allocation was removed in April 2000 through introduction of the European R&TTE Directive.

Since that date, IMEIs have been allocated by several regional administrators, which are acting on behalf of the GSM Association to the GSM terminal manufacturers without the need to provide evidence of approval.

Beside the IMEI number, IMSI and MSISDN^[15] can also identify a target of lawful interception^[14].

3.2. IMEI and Blacklists of Stolen Devices

When mobile equipment is stolen or lost, the owner can contact their local operator by requesting that it should be blocked from the operator's network, and the operator can be expected to do so if required by law in the operator's jurisdiction.

If the local operator possesses an Equipment Identity Register (EIR), it then may put the device IMEI into it, and can optionally communicate this to shared registries, such as the Central Equipment Identity Register (CEIR), which blacklists the device in switches of other operators that use the CEIR. With this blacklisting in place the device becomes unusable if the operator uses the CEIR, otherwise this practice would not work.

The CEIR blacklisting would be effective if the IMEI number is not easy to change.

However, this is not always the case: a phone's IMEI may be easy to change with special tools.

In addition, IMEI is an un-authenticated mobile identifier^[16]. Spoofed IMEI can hinder all efforts to track or target mobile devices for lawful interception.

3.3. Structure of IMEI and IMEISV^[17]

IMEI or IMEISV includes information on the origin, model, and serial number of the device. The structure of the IMEI/SV is specified in 3GPP TS 23.003^[20].

The model and origin comprise the initial 8-digit portion of the IMEI/SV, known as the "type allocation code"^[21] (TAC).

The remainder of the IMEI is manufacturer-defined, with a Luhn check digit at the end.

14 Locating, phone tapping etc.

15 Phone number. In format 905051234567 (Mobile Station International Subscriber Directory Number)

16 Unlike IMSI, verified by mobile network locally.

17 <http://www.gsma.com/newsroom/wp-content/uploads/2012/06/ts0660tacallocationprocessapproved.pdf>

18 15 decimal places: 14 digits plus a check digit

19 16 digits

20 GSM 02.16 / 3GPP 22.016 standard: <http://www.3gpp.org/Specs/22016-330.pdf>

21 TAC: Type Approval Code

As of 2004, the format of the IMEI is defined as “AA-BBBBBB-CCCCC-D”.

The IMEISV drops the Luhn check digit in favor of an additional two digits for the Software Version Number (SVN), making the format “AA-BBBBBB-CCCCC-EE”.

	AA	-	BB	BB	BB	-	CC	CC	CC	D or EE
Old IMEI	TAC				FAC	Serial number				(Optional) Luhn checksum
New IMEI	TAC									
Old IMEISV	TAC				FAC					
New IMEISV	TAC									Software Version Number (SVN).

Prior to 2002, the TAC was six digits long and was followed by a two-digit Final Assembly Code (FAC), which was a manufacturer-specific code indicating the construction location of the device.

From January 1, 2003 until April 1, 2004, the FAC code for all phones was 00. After April 1, 2004, the Final Assembly Code ceased to exist within the IMEI and the TAC was increased to eight digits in length.

For example, the old style IMEI code 35-209900-176148-1 or IMEISV code 35-209900-176148-23 tells us the following:

TAC	35-2099	Issued by the BAPT (code 35) with the allocation number 2099
FAC	00	Indicating the phone was made during the transition period when FACs were being removed
SNR	176148	Uniquely identifying a unit of this model
CD	1	Indicating that the phone is a GSM Phase 2 or higher
SVN	23	Identifying the revision of the software installed on the phone. 99 is reserved.

By contrast, the new style IMEI code 49-015420-323751 has an 8-digit TAC of 49-015420.

The new CDMA Mobile Equipment Identifier^[22] (MEID) uses the same basic format as the IMEI.

3.4. Check Digit Calculation

The last number of the IMEI is a check digit calculated using the Luhn algorithm, as defined in the IMEI Allocation and Approval Guidelines.

The Check Digit is calculated^[24] according to Luhn formula^[23].

The Check Digit is a function of all other digits in the IMEI. The Software Version Number (SVN) of a mobile device is not included in the calculation.

The purpose of the Check Digit is to help guard against the possibility of incorrect entries to the CEIR and EIR equipment.

The presentation of the Check Digit both electronically and in printed form on the label and packaging is very important. Logistics using bar-code reader and EIR/CEIR administration cannot use the Check Digit unless it is printed outside of the packaging, and on the ME IMEI/Type Accreditation label.

The check digit is not transmitted over the radio interface, nor is it stored in the EIR database at any point. Therefore, all references to the last three or six digits of an IMEI refer to the actual IMEI number, to which the check digit does not have place.

The check digit is validated in three steps:

1. Starting from the right, double every other digit except the last digit (which is the check digit) (e.g., $7 \rightarrow 2 \times 7 = 14$).
2. Sum the digits (e.g., $14 \rightarrow 1 + 4 = 5$).
3. Check if the sum is divisible by 10.

²² MEID

²³ Defined by ISO/IEC 7812 standard

²⁴ See also: GSM 02.16 / 3GPP 22.016 standard: <http://www.qtc.jp/3GPP/Specs/22016-330.pdf>

Conversely, one can calculate the IMEI by choosing the check digit that would give a sum divisible by 10. For the example IMEI 49015420323751?:

Order	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Meaning	Type Allocation Code								Serial Number						CD
IMEI	4	9	0	1	5	4	2	0	3	2	3	7	5	1	x
Double every other	4	18	0	2	5	8	2	0	3	4	3	14	5	2	x
Sum digits	4 + (1 + 8) + 0 + 2 + 5 + 8 + 2 + 0 + 3 + 4 + 3 + (1 + 4) + 5 + 2 + x = 52 + x														

To make the sum divisible by 10, we set x = 8, so the complete IMEI become 490154203237518.

3.5. IMEI and Legislation in Turkey


ICTA (Information and Communication Technologies Authority) has a database for IMEI numbers which can be queried via e-Government website ^{[25][26]}.

IMEI numaranızı, cihazınızın numara çevirme ekranına *#06# yazarak öğrenebilirsiniz.

Imei Sorgulama

IMEI No *

* Lütfen 15 haneli IMEI Numarasını giriniz!

Güvenlik Resmi * 

* Lütfen resimde gördüğünüz karakterleri yanında bulunan kutuya giriniz. Resmi okuyamıyorsanız, üzerine tıklayarak yeni bir tane oluşturabilirsiniz.

In some cases, IMEI numbers of some smart phone models are changed with IMEI numbers of old model phones. If this happens and there is more than one device using the same IMEI number, records of those IMEI numbers are also kept by ICTA.

An example of this case is depicted below:

IMEI	352558068271163
Durum	Bu IMEI numarasının başka cihazlara kopyalandığı tespit edilmiştir
Kaynak	--
Sorgu Tarihi	27/12/2016
Marka/Model	Üretici: Samsung Korea Pazar Adı: Samsung SM-G900F Model Bilgileri: Samsung SM-G900F

Bu IMEI numarasının başka cihazlara kopyalandığı tespit edilmiştir: It has been detected that this IMEI number has been copied to other devices

Durum: Status

Kaynak: Source

Sorgu Tarihi: Query Date

²⁵ IMEI Querying <https://www.turkiye.gov.tr/imei-sorgulama>

²⁶ Outputs of "IMEI inquiry" and "IMEI – MSISDN matching inquiry" on E-State system has "this inquiry is informative, not a precise record" warning. Therefore, it is necessary to ask the ICTA for precise records with the official request letter.

This database also keeps records on MSISDN matches of the IMEI numbers observed on network^[27]

IMEI numaranızı, cihazınızın numara çevirme ekranına ***#06#** yazarak öğrenebilirsiniz.

Imei Sorgulama

IMEI No *
* Lütfen 15 haneli IMEI Numarasını giriniz!

MSISDN No * Örn. 3122345678
* Lütfen 10 haneli Telefon Numarasını giriniz!

The mobile devices, which are imported or brought in with passengers, should be recorded to ICTA database in Turkey. Otherwise, the devices become out of service on the mobile networks of operators operating in Turkey.

Information on this subject can be found on the first page of IMEI registration service user's guide provided by Information and Communication Technologies Authority.

Things you should know

- The device should be brought **in with passenger** in order to be able to obtain this service.
- You should complete your registry within **120 days** starting your date of entry to the country
- No device should be brought in with passenger within last **two years**
- You should know **15-digit IMEI number** of your device. You can find out the IMEI number by dialing ***#06#**. Registration for devices containing more than one sim card can be registered using at most **three** IMEI numbers.

This registration requirement is regulated including the technical details under “*Communiqué Pertaining to the Registration of Devices with Electronic Identity Information* ^[29]” issued on Official Gazette with number 29058 and date of 12/07/2014.

In article 3 clause (f) of this communiqué:

“f) Technical controls: Checking whether the IMEI number has been previously listed on the white list prior to the transfer of the electronic identity information of the imported or manufactured device or of the device brought in with the passenger, checking whether the IMEI number has been identified as lost, stolen or altered electronic identity, TAC control, digit control or other relevant controls,”

According to below inquiries, ICTA – being the regulator of electronic communication in Turkey and obliged to store required logs – stores IMEI numbers on its database in 15 digits including the check digit and returns the IMEI numbers on queries in 15 digits including the check digit:

1. ICTA IMEI number query page,
2. ICTA IMEI number and MSISDN match query page,
3. ICTA IMEI Registration Service User's Guide,
4. Communiqué Pertaining to the Registration of Devices with Electronic Identity Information

²⁷ IMEI - MSISDN Matching Inquiry <https://www.turkiye.gov.tr/imei-msisdn-eslesme-sorgulama>

²⁸ http://www.mcks.gov.tr/Dosyalar/BTK_IME_Kayit_2017.pdf

²⁹ <http://www.mcks.gov.tr/tr/KonuDetay.php?BKey=32>

4. Examination of ByLock Application and the Information Gathered

ByLock is a mobile application that is defined as “a communication application that provides encrypted, secure and secret communication in military grade encryption standards between users” by its developer.

It is known that ByLock was developed for Android and iOS operating systems and published on Google Play and Apple App Store in the beginning of 2014, released by the individual, who introduces himself as David Keynes.

ByLock application cannot be found on Google Play and Apple App Store today. However, ByLock application package file can be found on various websites of software download.^[30]

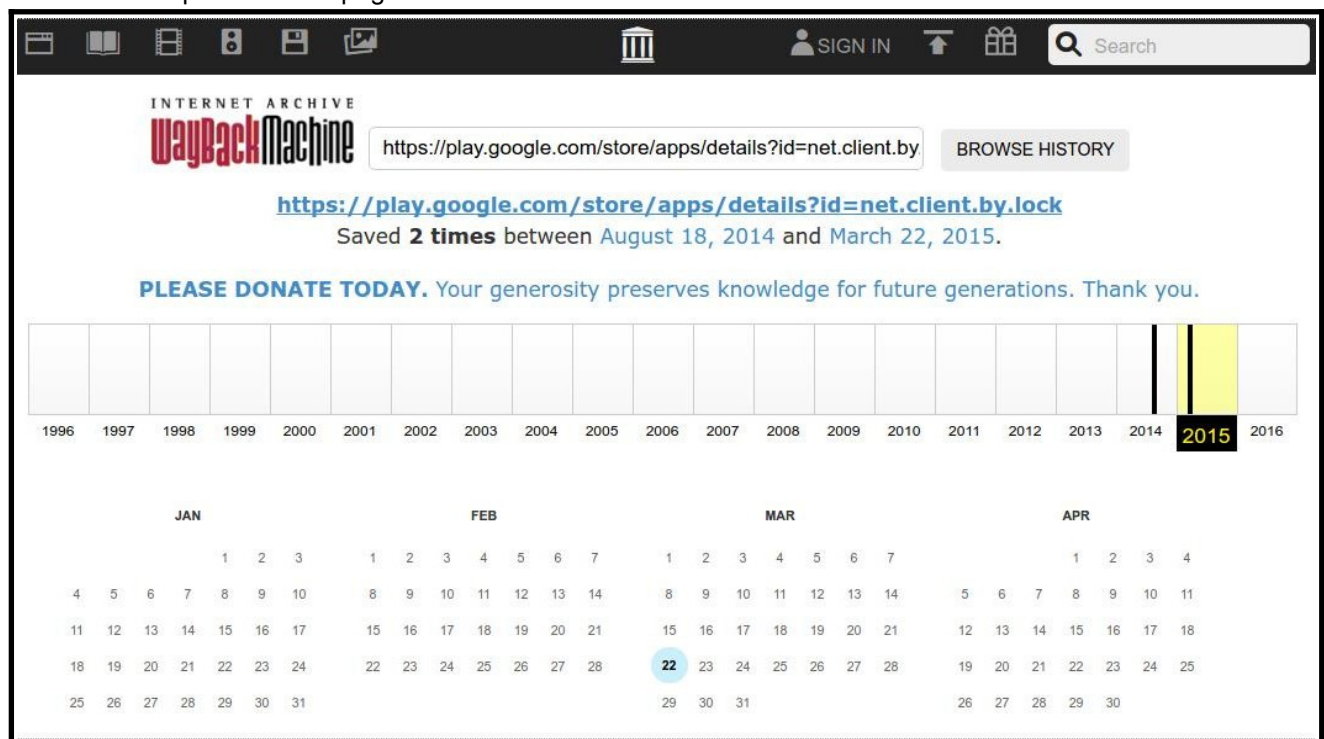
Android application package files with “apk” extension are zipped archive files. When the file is unzipped and the files inside are extracted, detailed information can be obtained about the application by searching words and meaningful arrays of letters using binary file editor within the file named as “classes.dex” which includes the main program codes.

0008:cb40	3b 00 29 4c 6a 61 76 61 78 2f 78 6d 6c 2f 74 72	;.)Ljavax/xml/tr
0008:cb50	61 6e 73 66 6f 72 6d 2f 73 74 72 65 61 6d 2f 53	ansform/stream/S
0008:cb60	74 72 65 61 6d 53 6f 75 72 63 65 3b 00 18 4c 6e	streamSource;..Ln
0008:cb70	65 74 2f 63 6c 69 65 6e 74 2f 62 79 2f 6c 6f 63	et/client/by/loc
0008:cb80	6b 2f 61 2f 61 3b 00 18 4c 6e 65 74 2f 63 6c 69	k/a/a;..Lnet/cli

From the screenshot above, the information can be obtained that the class name of the ByLock software is “net.client.by.lock”. Using this class name, the Google Play Store address of the application can be reached.

When the Google Play Store address^[31] is accessed, it can be observed that the application has been removed from the store.

When this address is searched on the website archive.org that saves backups of the websites, it is observed that the last back-up time of this page is 22/03/2015.^[32]



From the e-mail link in this backup, it can be found that the software developer uses “keynes97209@gmail.com” address.

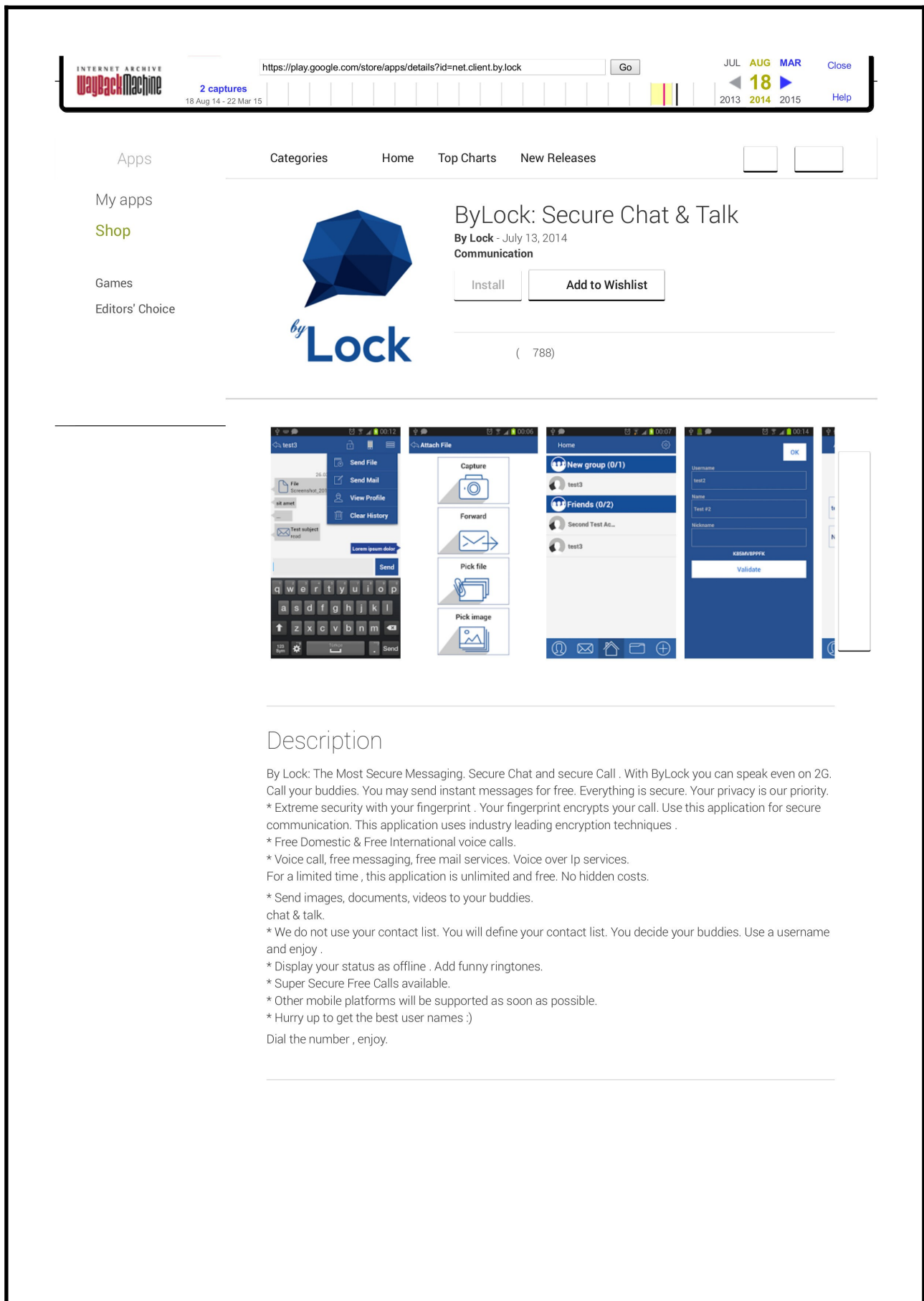
30 For example <https://apkpure.com/bylock-secure-chat-talk/net.client.by.lock>

31 <https://play.google.com/store/apps/details?id=net.client.by.lock>

32 <https://web.archive.org/web/20150322201135/https://play.google.com/store/apps/details?id=net.client.by.lock>

The screenshot of the backup on

"<https://web.archive.org/web/20150322201135/https://play.google.com/store/apps/details?id=net.client.by.lock>" is as below:



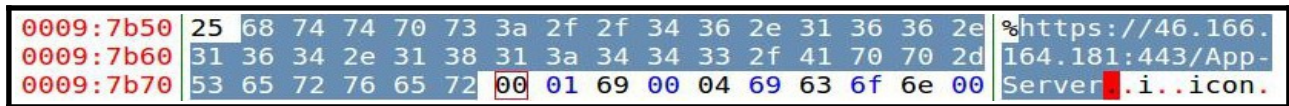
<https://web.archive.org/web/20150322201135/https://play.google.com/store/apps/details?id=net.client.by.lock>”;

©2014 Google Site Terms of Service Devices Terms of Sale Privacy Policy Developers Artists About Google

With the additional research conducted, it has been technically shown that the application was published on the early 2014 on application stores and stayed there as available for downloads until the first months of 2016 with different versions. Information on this discovery appears on the 9th page of the “technical report”^[33] that has no date and signature, prepared by MIT (National Intelligence Agency).

Because the application server has been offline since the beginning of 2016, it has been determined that the application was out of use starting from that date.

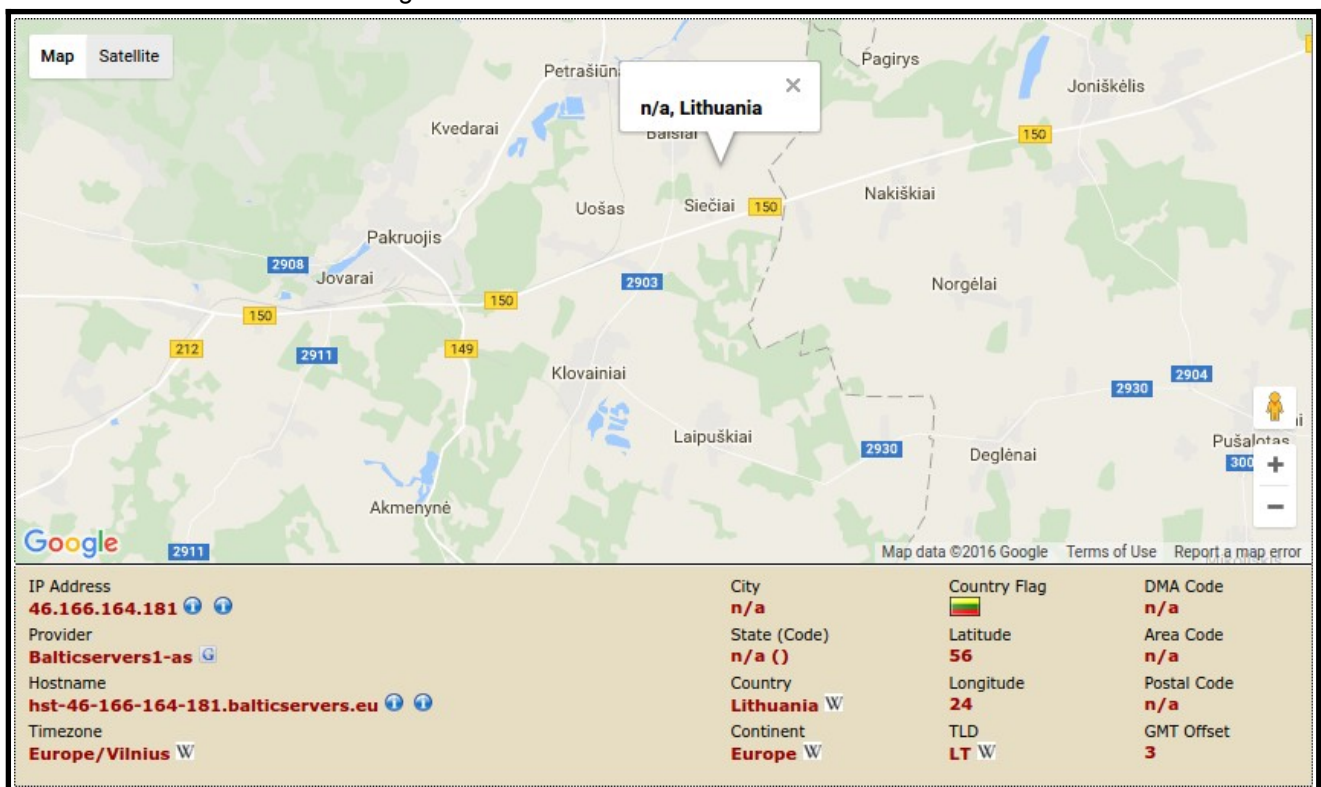
When words and meaningful arrays of letters are searched, in the file named “classes.dex”, the server address that connects the software to the external world is obtained.



From this image, the information of the server address that connects the software to the external world is obtained and that is “https://46.166.164.181/App-Server”.

When an examination on the IP 46.166.164.181^[34] that belongs to this address conducted, the outputs obtained are below:

1. The server is located in the Siečiai area, Lithuania,
2. The server is on the network “BalticServers”
3. The server is located in the Siečiai area, Lithuania,
4. The website of the hosting firm is “balticServers.eu”



33 Report sent to Ankara Public Prosecutor's Office as an appendix in the Ministry of Justice letter

34 According to the report sent to Ankara Public Prosecutor's Office as an appendix in the Ministry of Justice letter and prepared by National Intelligence Agency, it has been stated that ByLock application was establishing connection with the application server running on 46.166.160.137 and 46.166.164.181 IP addresses, depending on the application version on 443 port

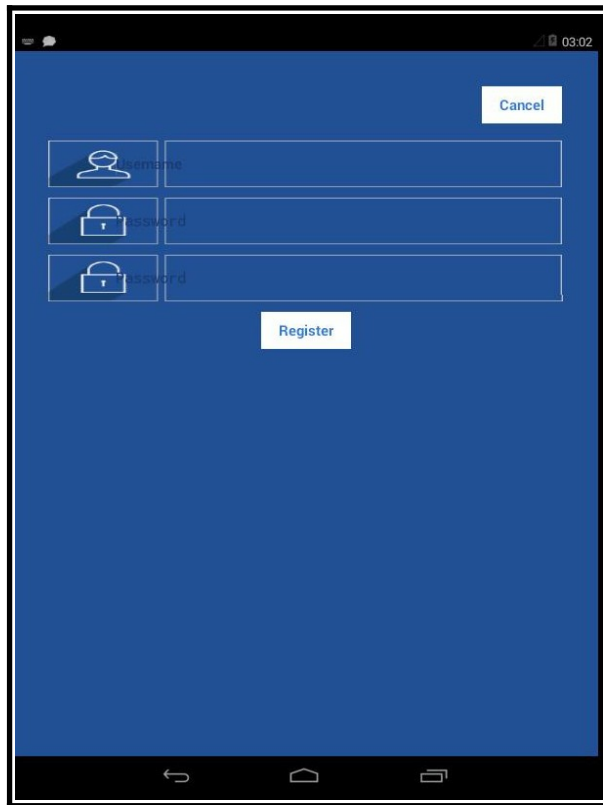
When the date information of the "classes.dex" file is gathered with the 'stat' command, it is reached that the version 1.1.7, which is known as the last version of the software, was compiled on 26/12/2014 at 20:38:06 (Turkish Local Time):

```
File: 'classes.dex'
Size: 736092      Blocks: 1440      IO Block: 16384  regular file
Device: 1dh/29d Inode: 3772282245  Links: 1
Access: (0664/-rw-rw-r-- )  Uid: ( 1000/  koray)   Gid: ( 500/ UNKNOWN)
Access: 2016-09-27 17:56:25.000000000 +0300
Modify: 2014-12-26 20:38:06.000000000 +0200
Change: 2016-10-10 23:05:11.261258110 +0300
Birth: -
```

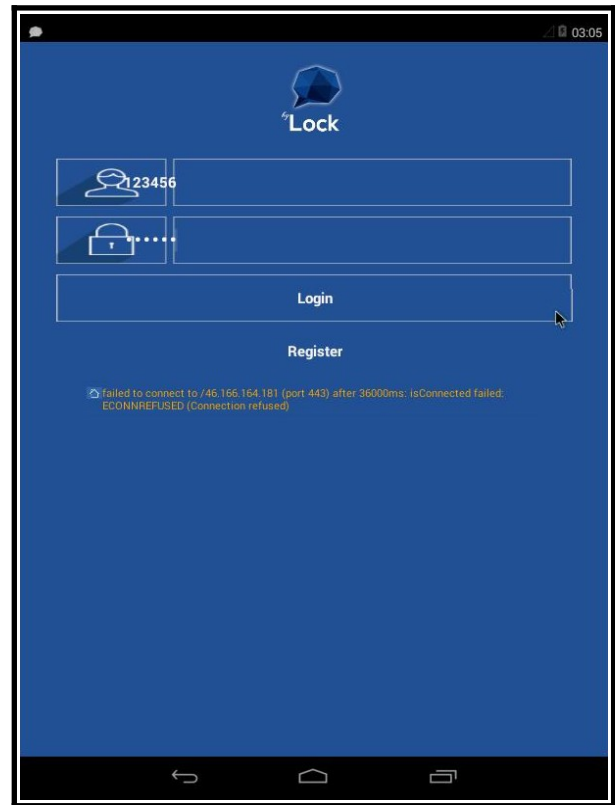
Using freely available dex2jar^[35] software that converts DEX files to JAVA archive (JAR) files and also freely available Java Decompiler GUI^[36] software that converts executable Java code to Java source code, the source code of the application has been obtained by myself.

With the examination conducted on the program code indicates that the application server runs on "<https://46.166.164.181/App-Server>" address, which can be found in "c/b.java" and "f/p.java" files under "net/client/by/lock" directory, performs various functions of the mobile application.

The screenshots below have been captured from the virtual machine that I have downloaded and installed in order to examine the application named ByLock:



User Login Screen



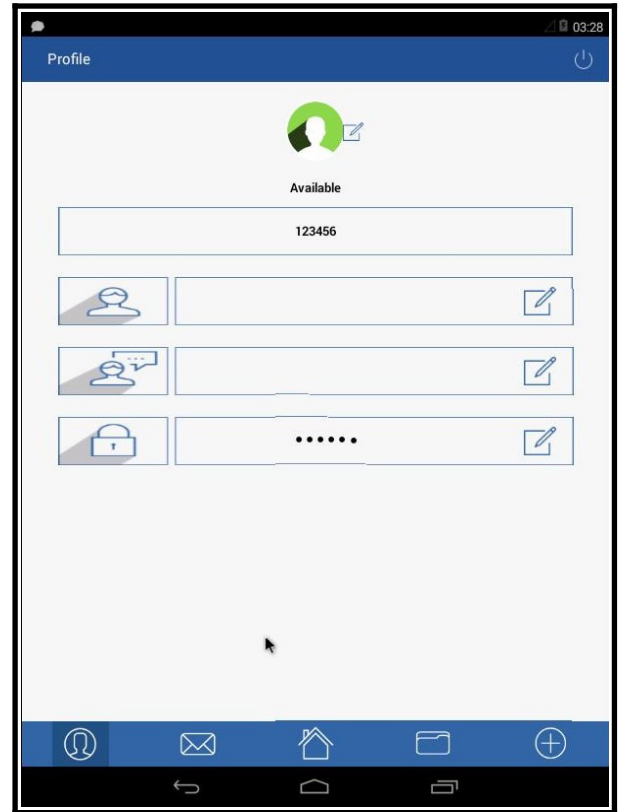
User Login Screen: Login failed, because the application server is not available.

³⁵ Dex2jar: <https://bitbucket.org/pxb1988/dex2jar/downloads>

³⁶ Java Decompiler GUI: <http://jd.benow.ca/#jd-gui-download>



Home Screen



User Information Edit Screen

Because of a software bug found on the application, the application runs in a way that the current user is logging in as if that user has been registered to the system properly although she/he has not.

During the examination conducted on the program code, "Sesli Arama" ("Voice Call") expression has been observed in "*net/client/by/lock/a/c.java*" file.

```
protected String a()
{
    StringBuilder localStringBuilder = new StringBuilder("Sesli Arama");
    if (((String)this.f.a()).equals("CLOSED")) {}
    for (String str = " (" + (String)this.i.a() + ")";; str = "") {
        return str;
    }
}
```

This finding indicates that the developer, who developed the application either speaks Turkish or the application might have been altered by individual(s) later.

ByLock application was registered to Apple App Store and Google Play stores by David Keynes, whose identity was questioned in some news^{[37][38]} published on press and it was claimed that David Keynes is actually Alpaslan Demir^[39], who is a former citizen of Republic of Turkey.

37 Hürriyet – İsmail Saymaz: There he is 'By Lock' David Keynes - <http://www.hurriyet.com.tr/iste-by-lock-david-keynes-40257030>

38 T24 – ByLock in ten questions with statements of David Keynes, patent holder - <http://t24.com.tr/haber/patent-sahibi-david-keynesin-ifadeleriyle-10-soruda-bylock,367450>

39 Takvim - Ergün Diler: That is David Keynes - <http://www.takvim.com.tr/yazarlar/ergundiler/2016/10/28/iste-david-keynes>

5. Commentary on ByLock Application and its Messaging System

5.1. An Overview of the Storyline of Detecting ByLock Users

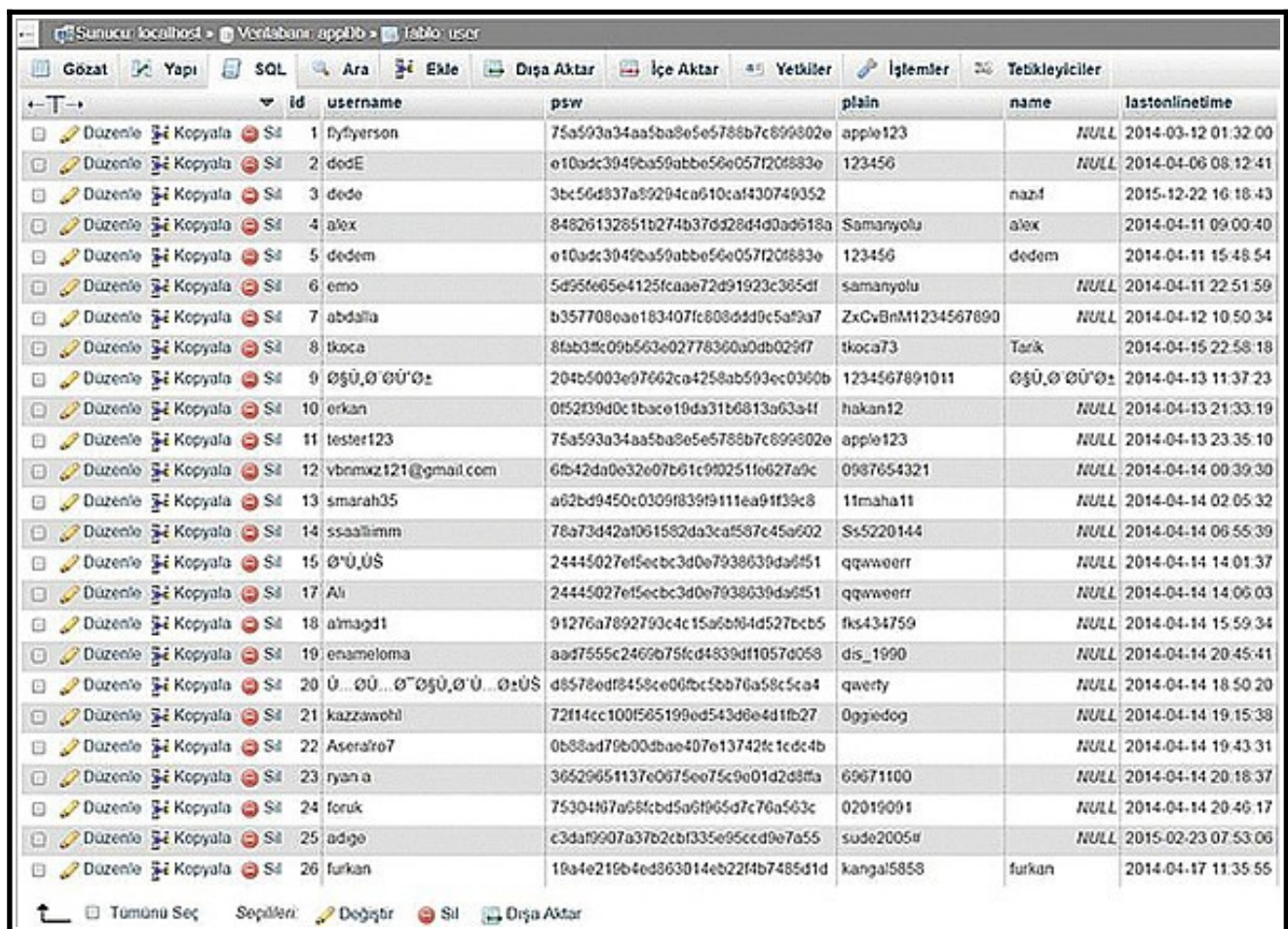
Based on the experience gained from judicial incidents related to information technologies and cases in the past years, I believe that alleged login to ByLock system incident should be able to be explained in details.

A detailed official statement containing technical details that can illuminate the experts working on this field, about ByLock and especially about the identification methods to show who ByLock users really are, is deficient.

The resources on this topic are some news published on press. These news are contradictory and some of them can be considered as “magazine news”.

I believe that the most respectable article among those publications is the article with the title: “Secret messaging through coup: ByLock”^[40] that has been written by Murat Yetkin and published on Hurriyet Newspaper on 13/09/2016.

One of the images^[41] that has been used in this article is the screenshot of the phpMyAdmin management software known by every individual, who uses MySQL and MariaDB database management systems is below:



	id	username	psw	plain	name	lastonlinetime
Düzenle Kopyala Sil	1	Byferson	75a593a34aa5ba8e5e5788b7c699802e	apple123	NULL	2014-03-12 01:32:00
Düzenle Kopyala Sil	2	dedE	e10adc3945ba59abbe56e057f20683e	123456	NULL	2014-04-06 08:12:41
Düzenle Kopyala Sil	3	dede	3bc56d837a99294ca610caf430749052		nazif	2015-12-22 16:18:43
Düzenle Kopyala Sil	4	alex	84826132851b274b37cd28d4d0ad618a	Samanyolu	alex	2014-04-11 09:00:40
Düzenle Kopyala Sil	5	dedem	e10adc3945ba59abbe56e057f20683e	123456	dedem	2014-04-11 15:48:54
Düzenle Kopyala Sil	6	emo	5d956e05e4125fcaae72d91923c365df	samanyolu	NULL	2014-04-11 22:51:59
Düzenle Kopyala Sil	7	abdalla	b357708eae183407fc808d4d9c5af9a7	ZxCvBnM1234567890	NULL	2014-04-12 10:50:34
Düzenle Kopyala Sil	8	tkoca	8fab33c09b563e02778360a0db029f7	tkoca73	Tarik	2014-04-15 22:58:18
Düzenle Kopyala Sil	9	ÖŞÜ,Ö'ÖÜ'Öz	204b5003e97662ca4258ab593ec0360b	1234567891011	ÖŞÜ,Ö'ÖÜ'Öz	2014-04-13 11:37:23
Düzenle Kopyala Sil	10	erkan	0f52f39d0c1bace10da31b6813a63af1	hakan12	NULL	2014-04-13 21:33:19
Düzenle Kopyala Sil	11	tester123	75a593a34aa5ba8e5e5788b7c699802e	apple123	NULL	2014-04-13 23:35:10
Düzenle Kopyala Sil	12	vbrmxz121@gmail.com	6fb42da0e32e07b61c900251f627a9c	0987654321	NULL	2014-04-14 00:39:30
Düzenle Kopyala Sil	13	smarah35	a62bd9450c0309f839f9111ea91f39c8	11maha11	NULL	2014-04-14 02:05:32
Düzenle Kopyala Sil	14	ssaa11mim	78a73d42a1061582da3ca587c45a602	Ss5220144	NULL	2014-04-14 06:55:39
Düzenle Kopyala Sil	15	Ö'Ü,ÜŞ	24445027ef5ecb3d0e7938639da651	qqweerr	NULL	2014-04-14 14:01:37
Düzenle Kopyala Sil	17	Ali	24445027ef5ecb3d0e7938639da651	qqweerr	NULL	2014-04-14 14:06:03
Düzenle Kopyala Sil	18	almagd1	91276a7892793c4c15a6b04d527bcb5	fls434759	NULL	2014-04-14 15:59:34
Düzenle Kopyala Sil	19	enameloma	aa07555c2460b75fc4d4839d11057d058	dis_1990	NULL	2014-04-14 20:45:41
Düzenle Kopyala Sil	20	Ü...ÜÜ...Ö'ÖÜ,Ö'Ü...ÖzÜŞ	d8578edf8458ce00fbc5bb76a58c5ca4	qwerty	NULL	2014-04-14 18:50:20
Düzenle Kopyala Sil	21	kazzawohl	72f11cc100f565199ed543d8e4d1fb27	Oggiedog	NULL	2014-04-14 19:15:38
Düzenle Kopyala Sil	22	Aseratro7	0b88ad79b00dbae407e13742fc1dc4b		NULL	2014-04-14 19:43:31
Düzenle Kopyala Sil	23	ryan a	36529651137e0675ee75c9e01d2d8fa	69671100	NULL	2014-04-14 20:18:37
Düzenle Kopyala Sil	24	foruk	7530467a68fcb45a61965d7c76a563c	02019091	NULL	2014-04-14 20:46:17
Düzenle Kopyala Sil	25	adgo	c3da1907a37b2cbf335e95cdd9e7a55	sude2005#	NULL	2015-02-23 07:53:06
Düzenle Kopyala Sil	26	furkan	19a4e216b4ed863014eb22f4b7485d1d	kangal5858	furkan	2014-04-17 11:35:55

According to this image, name of the examined database is “appDb” and database table is “user”.

It is obvious by the common programming principles that the data columns held in the table are “id” (user ID number^[42]), “username” (username), “psw” (encrypted password), “plain” (unencrypted password), “name” (name) and lastonlinetime (last connection time and date).

When we assume that the news are right, this image is not symbolic and shows the whole types of data stored about the users, it is concluded that related governmental bodies possess ByLock user database.

40 http://sosyal.hurriyet.com.tr/yazar/murat-yetkin_575/darbe-yolundaki-gizli-yazismalar-bylock_40222697

41 <http://i.hurim.com/i/hurriyet/98/603x436/57d6f5db67b0a911786c7397>

42 ID number increments by 1 when a user registers to the system. Neither Republic of Turkey ID number nor any other number.

However, information that cannot be inferred from this image is whether another data about the users are stored on database or not.

Another detail provided by other publications is that people allegedly using ByLock are identified with the analysis of this database; by grouping and sorting by priorities and by assigning color codes informing the institutions they work.

The information about how this analysis was conducted is deficient just as the points stated above.

It can be assumed that the information has been gathered from the "name" column in the ByLock user database.

In this case, as one remembers the information given in details on section "Digital Evidence: Qualification of Electronically Stored Files as Documents" such as;

"Since a digital log is also a database, it can be assured that it contains meaningful information assuming this database is accessed under certain rules and conditions."

and

"Digital information can be created using any system, by anyone, and indicating any time."

Therefore, in order to obtain meaning, the collected set of data should be able to answer the 5W1H questions: "Who? What? When? Where? Why? How?"

In other words, an explanation such as "which data is created when, on which system and database, in which form and type, in relation to which data, and by whom?" must be provided."

and answers these 6 questions regarding the logs recorded on ByLock database by both considering standard working structure of the system and by allowing the possibility that comes to mind, then two different paths arise:

1. What?
Logs on ByLock database
2. When?
 1. During the time period when the ByLock application server is online.
 2. When the ByLock application server is down.
3. Where?
 1. In Lithuania.
 2. At any place through remote access as being an Internet application.
4. Why?
 1. In order to keep record of people using ByLock application and enable reliable operation of the system.
 2. With any purpose. e.g. make some people seem to have been using ByLock.
5. Who?
 1. ByLock application itself
 2. Person / company developing ByLock system.
 3. People purchasing / taking over ByLock system.
6. How?
 1. Via ByLock application.
 2. Through any database management software.

In other words, these logs may be created in 2 different ways:

1. As normally expected (through usual operations of ByLock system):
ByLock application itself created them on ByLock database during when ByLock server was online and ByLock application was used on the server in Lithuania.
2. Considering ByLock system used by people with bad intentions:
Logs on ByLock database were created on the server in Lithuania and/or from anywhere through remote access since it is an internet application, while and/or afterwards the ByLock application server was online, using ByLock application and/or utilizing any database management software, by ByLock application itself and/or person/company who developed ByLock system and/or people who purchased/took over ByLock system.

The information obtained from the publications is that the most important evidence from the FETO / PDY investigations is that the ByLock software is installed on mobile phones of almost all the members and that they have been able to communicate with each other using this software.

It is well accepted through various concrete evidences that; ByLock was developed by people with bad intentions for their own communication purposes, however this service is also open for use of everyone.

When *“Since a digital log is also a database, it can be assured that it contains meaningful information if this database was assumed to be accessed under certain rules and conditions.”* sentence is interpreted together with the 2 paragraphs above, existence of a log recorded in the name of anyone is possible on an information technology system which turned out to be operated by people with bad intentions.

As principle of *“Digital data has to constitute a consistent whole with other similar data in the same environment in order to be considered as information.”* directs us, the logs can be accepted as accurate and valid if any other data related with the person who has his/her name on the record (i.e. IP address, the device used for access, etc.) and/or some other data that can only be known by the person who has his/her name on the record exists.

Criminal Procedure Law No. 5271, article no.134 regulating the subject of “Search of computers, computer programs and transcripts, copying and provisional seizure” explains on clause 1 that;

“Upon the motion of the public prosecutor during an investigation with respect to a crime, the judge shall issue a decision on the search of computers and computer programs and records used by the suspect, the copying, analyzing, and textualization of those records, if it is not possible to obtain the evidence by other means.”

When above quoted law article is interpreted with below mentioned principle, causality of digital evidence comes in sight;

“The data stored in the digital environment can be generated as desired and misleading; It can be created in a way that it has been generated by any other person or persons to show a desired time, to contain desired information, to have desired content, to give the impression that it is created by the desired person.”

According to the law, the valid search should be conducted on “computers, computer programs and computer logs used by the suspect”.

In other words, according to codes of Turkish Republic, digital evidence could only be collected from the information technology systems that belong to the person.

A log of the date and time at which users connect to the internet services is recorded by service providers as specified in the law No 5651 regarding Regulating Broadcasting in the Internet and Fighting Against Crimes Committed through Internet Broadcasting

These logs are delivered to Information and Communication Technologies Authority periodically and they are combined and stored at Information and Communication Technologies Authority.

At first glance, this may seem to conflict with Criminal Procedure Law No. 5271, however, through another viewpoint this implies that the internet service a person uses can be interpreted as an information technology system of his/her own and he/she can be hold responsible for the actions made using this system.

With specified justifications above, I think that the names collected from user database of ByLock system – which turned out to be operated by people with bad intentions – are not sufficient to form a causality link between real people and ByLock system.

5.2. Default Method for the Detection of ByLock Users

Components of ByLock system are as below:

1. User,
2. Smartphone establishes an Internet connection from the IP address that is assigned by the access provider.
3. ByLock mobile application installed on the smartphone
4. (As detected with this report and discussed in the “technical report” that has no date and signature by MIT - National Intelligence Agency-) Application server running on 46,166.160.137 and 46.166.164.181 IP addresses, depending on the application version (in the past) over 443 port (HTTPS)

⁴³ Abbreviated as ICTA - <http://www.btk.gov.tr/>

Connection and flow between those 4 elements are as follows:

1. The user installs the application on the phone he/she owns,
2. Smartphone establishes an Internet connection from the IP address that is assigned by the access provider.
3. It establishes a connection over port 443 (HTTPS) with the application server running on 46.166.160.137 or 46.166.164.181 IP addresses, depending on the application version, over port numbered 443 (HTTPS)
4. User record is created on ByLock system using ByLock application
5. User is logged in to ByLock system using ByLock application,
6. Messaging and other features are used, using the application

As observed, in order for a user to be referred as he or she was using the system by logging in, the user has to establish minimum 2 connections, where 1st is for user registration and 2nd is for logging in.

By assuming that the smartphone connected to the Internet directly using access provider, the following roadmap below might be a way to detect whether the individual uses ByLock or not:

1. Detection of whether ByLock application is installed on the smart phone or not,
2. If not installed, detection of any traces left when the application was uninstalled,
3. Verifying whether a connection was established (detection of communication) from the IP address assigned by the access provider to 46,166.160.137 or 46.166.164.181 over port number 443 (HTTPS) using ICTA's (Information and Communication Technologies Authority) logs.

However, this assumption is only valid for end-to-end direct connections.

With the complement research conducted, it has been discerned that several access providers do not provide end-to-end connection to their subscribers to avoid a set of technical difficulties.

This information was publicly shared first in an article on 20/10/2016 on Educators' Union website.

5.3. Examination of the Article Published on the Educators' Union Website

I was informed about an article^[44] published on 20/10/2016 on Educators' Union website at the early days of November 2016. This article also published as it is on some media.

Below is the quoted article in full length:

"Lately, 2,400 teachers were laid off from their jobs as part of the inquiries conducted by the Ministry of National Education after the FETO coup attempt. The justification for this laying off is using a message program, which is publicly known as 'Bylock'. The social witness testimonies are increasingly delivered to our union for some of the educators who were laid off indicating they are actually people who would never be connected with the terrorist organization of the FETO. As examples were increasing such as the fact that many educators are not related to the allegations in terms of social perception, some even do not have the ability to use this program, and there are no internet subscriptions registered to their address, as a union we issued a call under name of "ByLock uncertainty generates victims", mentioned about the need for a detailed technique investigation and a timely intervention to protect innocents with the aim of establishing justice.

Lately, the opinion that the educators who are dismissed from their jobs with justification of being the user of 'Bylock' are the victims of situations developed or occurred without their own consent is becoming more and more popular in the public opinion. In order to be included in the internet environment, it is known that the IP number which is uniquely allocated to the user by operators is sometimes allocated to more than one user and those many users can perform legal / illegal transactions at over the same IP, that's why the feeling of "damp and dry wood are mixed" grows stronger. When the job dismissal process is carried out, a situation in which the innocent and the victim are suffering from the same pangs occurs, thus generating the confusion in which "one can't tell the good people from the worthless". The difficulty of retraining for reorganization is severe to the conscience because of the belief that it is not possible to compensate for the reputation loss happened during this process.

There has been a consensus point where it is not found right that such technical issues without sufficient clarification should not be regarded as a single justification criterion for dismissals. In this phase, instead of just a transaction over IP, the 'log' records of the operators should be examined

44 <http://www.egitimbersen.org.tr/ebs/manset/3874/-bylock--mutlaka-aydinlatilmalidir>

and the technical examiner should accept it as the definitive evidence after reviewing all the records at the same time. Similarly, no actions should be taken on definite opinions regarding people before determining whether there is any abuse of his/her registered phone line which can be examined through signal from the base stations - indicating where the phone is used - and records of the 'HTS', and fully illuminating the direct non-criminal elements such as abuse of the internet subscriber line.

It is important to share with the people - on whom the actions were taken - the information about which of their actions or behaviors of his/her have justified this kind of actions to be taken, which actions of his/her considered as a crime in consequence of conducted investigation, which phone number of his/her is involved in the crime if there are more than one phone number registered in the name of the person.

Management of the process in a healthy and transparent manner and consideration of technical subjects after they are illuminated in all details are required to prevent the society's sense of justice from getting damaged."

The quotation of the article;

"In order to be included in the internet environment, it is known that the IP number which is uniquely allocated to the user by operators is sometimes allocated to more than one user and those many users can perform legal / illegal transactions at over the same IP"

is verified through verbal information obtained from access providers and mobile operators by means of the technical examination that I personally conducted.

Therefore, it is crystal clear that the flow explained on section "Default Method for the Detection of ByLock Users" might not be exact and accurate, and the detection of communication through only ICTA records may provide misleading result.

The reason behind that is explained in below.

5.4. IP Allocation and Connection Routing Methods of Internet Service Providers

Today, the most common communication rule^[45] that helps the Internet to exist is the 4th version of IP Protocol, abbreviated as IPv4. IP addresses under IPv4 family consist of 4 times 8'ers that are separated by "." This mathematical phenomenon limits the maximum number of IP addresses with the IPv4 by 232 in other words 4.294.967.296 (approximately 4.3 billions).

Some of those IP addresses (approximately 589 millions) are for special use, which are referred as "Private Internet Addresses", "Intranet addresses" and "Addresses not redirected to the Internet".

In closed networks, those types of addresses can be assigned to devices in a way that every device has a different address. However, it is not necessary for unconnected devices to have distinct IP addresses.

Remaining addresses that can be defined in IPv4 standard (approximately 3.7 billions), referred as "open Internet addresses" and "Internet-redirectable addresses", are open to public use. The devices that directly connected to the Internet must have distinct IP addresses.

Today, the number of subscribers of the Internet access providers increases logarithmically; although the numbers of the IP addresses they can assign to their subscribers remain the same. Especially the mobile operators fail to provide sufficient number of IP's to their subscribers.

Therefore, using a technique called Network Address Translation^[49] (NAT), it is provided for multiple users to access to the Internet, by:

1. Assigning subscribers the IP addresses that are not linked to each other, where they might be the same, and cannot be redirected on the Internet (meaning at no cost) and enabling subscribers to establish a connection with the access provider using IP protocol.
2. Translating connections established through those addresses into routable addresses via a device called router.

45 Protocol

46 Internet Protocol

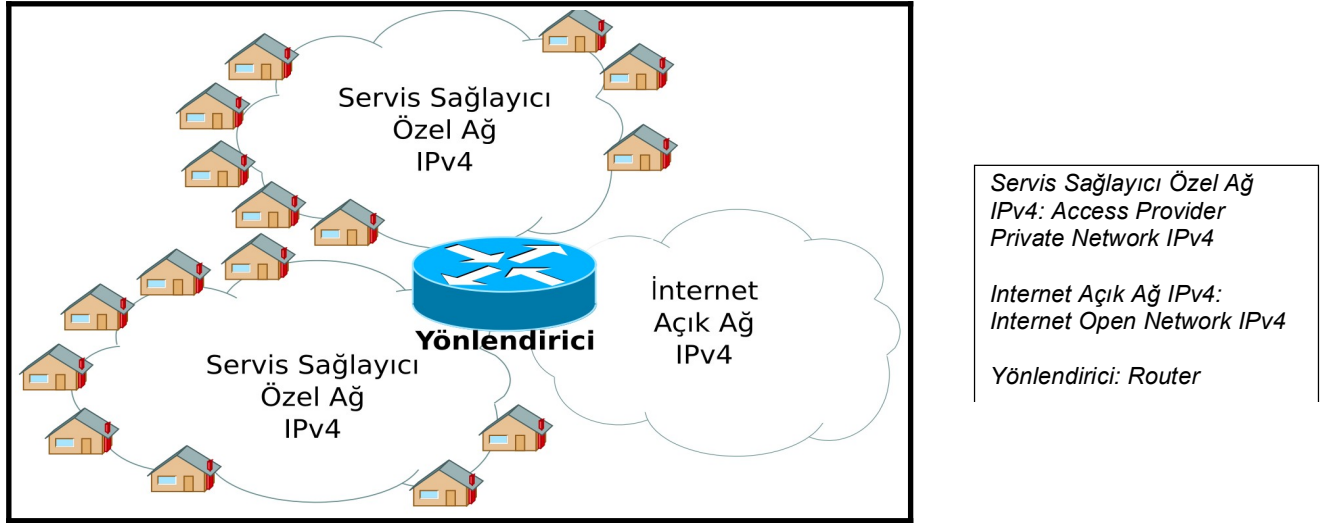
47 1 to 2 up to the 8th floor (2⁸) (1~255) (Octet)

48 For example: 212.54.78.45, 168.14.58.92

49 Network Address Translation(NAT)

The Internet side of this structure is referred as the external interface, whereas the side where subscribers establish connection to the access provider is referred as local interface.

A router between external and local interfaces alters and transmits the packages from local interface to external interface (the Internet).



Today, in order to be able to meet the number of subscribers by the large access providers, the Network Access Translation has been developed to a more advanced version. This technique is referred as Carrier Grade NAT ^[50] or Large Scale NAT ^{[51] [52]}. Using this technique, subscribers get separated into unconnected closed networks and assigned private IP addresses and enabled their connection to the Internet, which is an open network.

For example, on a network that has a private IP address range and defined with 172.16.0.0, 65534 IP addresses can be assigned to users and connection to the Internet can be established using routers.

In this way, hundreds of users are assigned with private IP addresses. The Internet connection request coming from those private IP addresses are converted to Internet connections with only 1 host that has the Internet IP knowledge.

Therefore, hundreds of users unrelated to each other, has the same IP addresses when they connect to a service on the Internet.

5.5. Large Scale NAT Technique and the Law No. 5651

Following definitions are provided in the 2nd article of, Law No. 5651 on Regulating Broadcasting in the Internet and Fighting Against Crimes Committed through Internet Broadcasting:

“d) Access: Getting an opportunity of use through connection to any Internet environment”

“e) Access provider: Any kind of real or legal persons or entities providing to their users access to Internet environment”

“g) Internet environment: The environment established on Internet which is open to public and not covered by communications and personal or corporate computer systems”

“Traffic data: The values related with any kind of access through Internet environment including the parties, time, period, the type of service used, the transferred data quantity and the connection points, etc.”

According to the 6th article and clause b of the very same law that regulates the obligations of access provider is:

“b) To retain all traffic data about the services that it provides for the period specified in the regulation - which cannot be less than six months and more than two years - and to maintain accuracy, integrity and confidentiality of such data”

It is clear that the access provider is obliged to keep the record of access to the area outside the personal or corporate computer systems for as long as 6 months or less and not more than 2 years to be determined in the regulation and to ensure the correctness, integrity and confidentiality of such information.

50 Carrier Grade NAT (CGN)

51 Large Scale NAT (LSN)

52 https://en.wikipedia.org/wiki/Carrier-grade_NAT

When Large Scale NAT is used, it is clear that logging only the connections established from the external interface of router and using only the logs obtained from the external interface as certain information, will be misleading, because thousands of subscribers will have the same IP address.

In order to avoid this misleading condition, a log should be kept for the IP address and port number which connection requests was sent to when the subscriber established connection with local interface and the router redirected it to the Internet, so that which user accessed to which service in reality can be detected.

5.6. Valid Method for the Detection of ByLock Users

It is clear that the detection of communication through only ICTA records may generate misleading result when the method interpreting that the flow explained on section “*Default Method for the Detection of ByLock Users*” might not be exact and accurate, the technical information detailed on section “*IP Allocation and Connection Routing Methods of Internet Service Providers*” and the opinions on section “*Large Scale NAT Technique and the Law No. 5651*” are taken into consideration.

Therefore, it is only possible to detect whether a person uses the system or not, by:

1. Detection of whether ByLock application is installed on the smart phone or not,
2. If not installed, detection of any traces left when the application was uninstalled,
3. Verifying if a connection was established from the IP address assigned by the access provider to 46.166.160.137 or 46.166.164.181 over port number 443^[53] on the date or date ranges on which the action was taken from ICTA's (Information and Communication Technologies Authority) logs.
4. Verifying if a connection was established from the IP address assigned by the access provider to 46.166.160.137 or 46.166.164.181 over port number 443^[53] on the date or date ranges on which the action was taken from the access provider's logs.

If the answer given to 3rd question is “yes” and if the answer given to 4th question is “no”; this indicates that access provider uses the Large Scale NAT technique and the subscriber actually did not commit the alleged act.

This is most likely because, in the time range when the subscriber was connected, another subscriber who the subscriber does not know and whose location was possibly close to him/her used the ByLock system.

If the answers to both questions are “yes”, this might indicate that the subscriber might have actually committed the alleged act.

Such situations might also be encountered when the Internet connection is shared via modem, wireless network or using mobile access point feature of the smart phones.

If the access provider is not capable of querying in logs using the IP addresses and ports given in the 4th clause and can answer the question only as “subscriber established an Internet connection on the given date range” without being capable of giving any details, it might be an indication of that the access provider does not log the connections established to the local interface of the router using the Large Scale NAT technique.

This case does not apply with the Law no. 5651, clause 6 and in reality it will be never found out which user established a connection to which service.

However, this communication detection report is likely to mislead when Internet connection is shared over a modem, over a wireless network, or using access point features of smartphones.

On the other hand, the points elaborated in quoted part of the article


“In this phase, instead of just a transaction over IP, the 'log' records of the operators should be examined and the technical examiner should accept it as the definitive evidence after reviewing all the records at the same time. Similarly, no actions should be taken on definite opinions regarding people before determining whether there is any abuse of his/her registered phone line which can be examined through signal from the base stations - indicating where the phone is used - and records of the 'HTS', and fully illuminating the direct non-criminal elements such as abuse of the internet subscriber line.”

are technically significant in terms of reality and judiciary.

⁵³ Standard port of the HTTPS protocol

Therefore, I believe that examination of the log records of the base stations and HTS logs that show where the phone was used by synchronizing the individuals' known physical locations, will result positively.

6. Examined Digital Material and the Method of Examination

Model	Samsung Galaxy Note 2
Rear Sticker	
Model	GT-N7100
IMEI Number	353627055929742
Operating System	Android 4.4.2
Baseband Version	N7100XXUFOA1
Backup Date	05/07/2017
Backup File Name	Taner_Kilic_Samsung_Galaxy_Note_2_GT-N7100_Yedek.ab
Backup File Size	8.191.781.886 byte
Backup File MD5 Hash Value	d9604d39113810f2f8af7d801fc0e5ae
Backup File SHA1 Hash Value	42516f812915f6fa794fec395eaa6cfd44458a38
Rootkit Activation Date	09/07/2017
Rootkit Activation Method	Odin and Chainfire Auto-Root patch (https://autoroot.chainfire.eu/)
Softwares installed and uninstalled	BusyBox SuperUSER
Raw Image File Name	Taner_Kilic_Samsung_Galaxy_Note_2_GT-N7100_Imaj.img
Raw Image File Size	15.758.000.128 byte
Raw Image File MD5 Hash Value	d7dae200d6117077011c9a98d936b759
Raw Image File SHA1 Hash Value	2b1084d5a5bb5fb98e5df52fbc94d00e8e2b709c

6.1. Pre-examination Preparation

Before the examination, an Android backup of the phone has been created by executing the 'adb' command.

To create a raw image, for gaining access to deleted files and to activate rootkit necessary patch has been applied.

The image has been created by executing BusyBox and dd commands. After creation of the image, rootkit has been deactivated, the patch applied has been removed and no other changes has been made on the phone's file system.

With the examination conducted, it has been observed that the image created provides the sufficient data about the usage process of the phone. It has been observed that image has 19 file system partitions. It has been noted that sector size is 512-byte.

Examination has been conducted on cache, system and userdata partitions with the details below.

Partition #	Partition Name	Initial Sector	Partition Function
15	CACHE	327680 (167772160 byte offset)	Buffer
16	SYSTEM	3129344 (1602224128 byte offset)	System
19	USERDATA	8486912 (4345298944 byte offset)	User

Before the examination;

1. The hash value of the smartphone with details provided has been obtained and their integrity has been verified.
2. The partitions in the image file have been mounted in directories as read-only (mount).
3. In directories on Ubuntu Linux operation system with `"find ./ -print0 | xargs -0 stat -c \"%n\",\"%w\",\"%x\",\"%y\",\"%z\""`
> `Zaman_Cizelgesi.csv` command
 1. File/Directory Name,
 2. Last Accessed Date,
 3. Last Edit Date on File Data,
 4. Last Edit Date on File System,Timelines that contains information about respectively every file and directories were obtained and saved into the file.

6.2. Examination of Phone Hardware

Eye-examination of the phone shows that the ByLock app is not installed on the device and the IMEI number of the phone is 353627055929742.

The IMEI number was verified from Information and Communication Technologies Authority (ICTA) IMEI Queries page on the E-State system, showing that the IMEI number is registered to ICTA, and the brand/model details are correct.



Hoş geldiniz, sunulan hizmetlerden faydalanmak için sisteme giriş yapmalısınız

türkiye.gov.tr

Hizmet Adı, Anahtar Kelime, Plaka No...

Bilgi Teknolojileri ve İletişim Kurumu

IMEI Sorgulama

Hizmet Listesine Geri Dön

Geri Yazdır

IMEI	353627055929742
Durum	IMEI NUMARASI KAYITLI
Kaynak	İthalat yoluyla kaydedilen IMEI
Sorgu Tarihi	10/07/2017
Marka/Model	Üretici: Samsung Korea Pazar Adı: Galaxy Note 2 GT-N7100 Model Bilgileri: Galaxy Note 2 GT-N7100

Bu hizmet Bilgi Teknolojileri ve İletişim Kurumu işbirliği ile e-Devlet Kapısı altyapısı üzerinden sunulmaktadır.

Bu işlem için yaklaşık 1 dakikanızı ayırmalısınız.

Bu işlem toplam 2 aşamalıdır. Şu anda 2. aşamadasınız.

Bu sorgulama bilgilendirme amaçlıdır, kesin kayıt değildir. İspat hukuku açısından geçerliliği bulunmamaktadır.

6.3. Examination Method

6.3.1. Examination of Timeline

The timeline containing the time information of all the files stored in the phone's image file has been examined. The aim of this examination was to obtain detailed information about the usage process of the phone.

6.3.2. Examination of Google Play Store Databases which contain the List of all Installed Applications on the Phone

In smartphones using Android operating system, the "com.android.vending/db" directory in the phone's image contains two SQLite database files named "library.db" and "package_verification.db", which include some records of all applications that were installed starting from the moment a user first sets up his/her Gmail account, and applications installed later.

When applications are deleted and even removed from Google Play Store, logs of these applications are stored in those databases.

The "localappstate.db" SQLite database file that is in the same directory, stores some log records of the software installed.

An example from a laboratory work conducted by myself that shows traces of ByLock application which were deleted from the phone, is below:

0000:f700	08 7a 65 6b 61 69 6b 6f 63 40 67 6d 61 69 6c 2e	.xyzzyzy@gmail.
0000:f710	63 6f 6d 03 03 63 6f 6d 2e 66 69 72 65 2e 77 61	com..com.fire.wa
0000:f720	6c 6c 70 61 70 65 72 73 0f 18 ba e8 11 06 f9 ef	llpapers..□□.□□
0000:f730	30 44 64 6f 59 66 57 75 63 32 30 69 59 72 32 6d	0DdoYfWuc20iYr2m
0000:f740	50 38 2d 55 68 4e 46 4d 6c 42 45 02 62 89 25 18	P8-UhNFMlBE.b.%.
0000:f750	31 01 01 31 09 09 06 00 43 08 08 00 00 00 00 00	1..1...C.....
0000:f760	8 08 08 00 00 01 08 7a 65 6b 61 69 6b 6f 63 40	□.....xyzzyzy @
0000:f770	67 6d 61 69 6c 2e 63 6f 6d 03 03 6e 65 74 2e 63	gmail.com..net.c
0000:f780	6c 69 65 6e 74 2e 62 79 2e 6c 6f 63 6b 9d 40 65	lient.by.lock.@e
0000:f790	55 59 f8 a5 0b 79 46 65 4c 53 43 39 70 71 67 77	UY□□.yFeLSC9pqgw
0000:f7a0	66 46 77 6e 37 67 56 74 6b 5a 75 70 42 76 4a 59	fFwn7gVtkZupBvJY
0000:f7b0	02 68 89 24 18 31 01 01 3d 09 09 06 00 43 08 08	.h.\$1..=...C..

6.3.3. Data Scan and the Retrieval of Meaningful Data

For a detailed examination, Bulk Extractor^[56] that was developed by Simson Garfinkel^[55], who works at National Institute of Standards and Technology of the United States of America as a senior engineer, has been chosen as a way of detailed scanning and reporting.

6.3.3.1. About the Bulk Extractor

Bulk Extractor is software that extracts meaningful data arrays by scanning disk images, files and directories independent from file system and file system structures.

Bulk Extractor is capable of retrieving meaningful data arrays from both corrupted and uncorrupted file systems, on corrupted file systems and data stored on deleted files also can be extracted as sound.

The results obtained are stored in text files, which store different types of data arrays (i.e. web addresses, phone numbers, barcodes, Ethernet MAC addresses, e-mail subjects, zip files). In those files search operations, processing can be carried out and queries can be run, using automated software.

Bulk Extractor also generates histograms to enable investigating occurrence frequency of the data strings' contents.

Those text files that represent all data arrays are indexed in a report named 'report.xml' file, which is in XML format. This report and the medium that examined data are stored (image, file or directory) can be opened using Bulk Extractor Viewer (BEViewer) and it can be displayed where the meaningful data is located in file.

55 <https://www.nist.gov/people/simson-garfinkel>

56 https://github.com/simonsong/bulk_extractor

Bulk Extractor is superior to other digital forensic tools with its speed and robustness. It can process data arrays asynchronously with an approach similar to artificial intelligence, instead of file system examination approach.

For example; the program processes the pages with each idle core by dividing the disk image into 16-megabyte pages.

Bulk Extractor uses various algorithms to identify compressed data, and decompress and process it whenever the data is found. In practice, it is common to have large amounts of compressed data from deleted partitions of a file system.

That compressed data is not identified and taken into account by other digital forensic softwares.

Some examples for those compressed data are installation files of the program^[57] and system libraries^[58].

Another advantage of Bulk Extractor feature that works independent from file systems and file systems structures is that it is capable of finding stored data in different types of storing units and in a file system that is not in open standards (commercial or hardware dependent).

In this way, Bulk Extractor (without the necessity of identification of file system) can process the data obtained from hard drives, SSD drives, optical storage media, camera cards, cell phones, network package records and any other digital media.

6.3.3.2. Retrieval of Meaningful Data with the Bulk Extractor

Android backup of the phone has been processed by activating all filters of Bulk Extractor^[59] and data arrays with different meanings found by the filters have been written into related text files by Bulk Extractor.

Bulk Extractor has saved the files discovered in archive files into related directories.

7. Examination

Following the information elaborated in the “Information Gathered and the Examination of ByLock App” section, traces that should be searched for in a system where ByLock is installed, or removed following a previous installation are listed below:

1. The word “Bylock”
2. The string “net.client.by.lock”
3. The string “net.client”
4. The string “.client”
5. The string “.client
6. The directory structure “net/client/by/lock”
7. The IP address “46.166.164.181”
8. The IP address “46.166.160.137”
9. Adjacent words “Sesli” and “Arama”
10. The e-mail address keynes97209@gmail.com

7.1. Sample Examination

It would be beneficial to give an example, in order to understand the main examination better. For example, a search applied to an extracted data that was extracted by Bulk Extractor from a Samsung Grand 2 mobile phone, data files that contains “keynes” content are observed:

57 Zip, Installation files similar to Install Shield, Microsoft CAB files, Android APK packages, Apple iOS IPA packages

58 DLL files of Microsoft systems, SO files of UNIX based systems

59 Command executed: bulk_extractor -e all -o cikti_dizini imaj_dosyasi

7.2. Examination by Data Scan

A data scan was made by,

1. Word and parameter search within the directory list obtained from the phone backup,
2. Word and parameter search within meaningful data series obtained from the phone backup using Bulk Extractor,
3. IP address scan on meaningful data series obtained from the phone backup using Bulk Extractor,
4. Word and parameter search within the phone backup, executing “strings” and “grep” commands,
5. Word and parameter search within the installed applications list of the applications database obtained from the phone backup.

The following non-case sensitive parameter combinations were used in the search operations:

- | | |
|----------------------------|------------------------|
| 1. ByLock | 14. https://46.166.164 |
| 2. Lock | 15. https://46.166 |
| 3. net.client.by.lock | 16. https://46 |
| 4. net/client/by/lock | 17. ttps://46 |
| 5. net.client | 18. tps://46 |
| 6. .client | 19. ps://46 |
| 7. net/client | 20. s://46 |
| 8. client | 21. ://46 |
| 9. lient | 22. //46 |
| 10. Sesli Arama | 23. /46 |
| 11. Sesli | 24. 46.166.164.181 |
| 12. keynes | 25. 46.166.164 |
| 13. https://46.166.164.181 | 26. 46.166 |

Following the scan, no evidence was found in the image of phone belonging to Taner KILIC, showing that ByLock was installed or removed after installation.

8.3. Examination of Google Play Store Databases which Contain the List of All Applications on the Phone

In smartphones using Android operating system, the “apps/com.android.vending/db” directory in the phone’s image includes two SQLite database files named “library.db” and “package_verification.db”, which include some records of all applications that were installed at the moment a user first sets up his/her Gmail account, and applications installed later.

The “localappstate.db” SQLite database in the same directory also stores some records of installed software. Even when an application is uninstalled from the phone, or even after it is removed from Google Play Store, records of this application leave traces in these databases in the phone, and in the “journals” which are a form of registry ensuring the consistency of these databases.

Following the scan, no evidence was found in the image of phone belonging to Taner KILIC, showing that ByLock was installed or removed after installation.

8.4. Examination of Timelines

A timeline including timestamps of all files recorded under the system and the user parts of the phone image was examined. Detailed information on the usage of the phone was obtained this way.

The timeline of the system section includes 3938 files and file/directory names, times of last access, times of last modification, and the last date of modification of the filing system.

The timeline of the user section includes 41188 files and file/directory names, times of last access, times of last modification, and the last date of modification of the filing system.

These timelines are provided with the phone image, in the form of an Excel file inside a DVD, in the annex of this report.

The investigation has shown that Samsung Galaxy Note 2 GT-N7100 phone was launched on the Turkish market in September 2012.

According to the data on the phone, it was detected that

1. The earliest date of use is 17/11/2012,
2. The latest date of use by the owner is 06/06/2017, at 16:44:03,
3. After that time, the phone was used
 1. on 12/06/2017, between 11:58:51 and 16:44:03,
 2. on 13/06/2017, between 00:40:04 and 16:42:01.

There is no sign of a reset to factory settings or a similar disruption during this time period. On the contrary, the phone was used regularly while it was on.

On 27/08/2014, the alleged date of crime, the phone was used between

1. 21:16:16 and 21:17:25,
2. 00:07:15 and 00:08:20.

During this period of use, the following files under the user directory was accessed:

1. /data/com.mosteknoloji.android.elfeneri/app_webview/Cache/776c223035b71c35_0
2. /data/com.mosteknoloji.android.elfeneri/app_webview/Cache/776c223035b71c35_1
3. /data/com.mosteknoloji.android.elfeneri/app_webview/Cache/776c223035b71c35_2
4. /data/com.google.android.gms/app_webview/Cache/dd1d0df83b0f21c6_0
5. /data/com.google.android.gms/app_webview/Cache/dd1d0df83b0f21c6_1
6. /data/com.google.android.gms/app_webview/Cache/dd1d0df83b0f21c6_2
7. /data/com.mosteknoloji.android.elfeneri/app_webview/Cache/8ea696993c998dd8_0
8. /data/com.mosteknoloji.android.elfeneri/app_webview/Cache/8ea696993c998dd8_1
9. /data/com.mosteknoloji.android.elfeneri/app_webview/Cache/8ea696993c998dd8_2
10. /data/com.google.android.gms/app_webview/Cache/d2d5a64ba0b19390_0
11. /data/com.google.android.gms/app_webview/Cache/d2d5a64ba0b19390_1
12. /data/com.google.android.gms/app_webview/Cache/d2d5a64ba0b19390_2
13. /data/com.mosteknoloji.android.elfeneri/app_webview/Cache/430863e8e1d8d068_0
14. /data/com.mosteknoloji.android.elfeneri/app_webview/Cache/430863e8e1d8d068_1
15. /data/com.mosteknoloji.android.elfeneri/app_webview/Cache/430863e8e1d8d068_2
16. /data/com.google.android.gms/app_webview/Cache/96a8b7584b69a337_0
17. /data/com.google.android.gms/app_webview/Cache/96a8b7584b69a337_1
18. /data/com.google.android.gms/app_webview/Cache/96a8b7584b69a337_2
19. /data/com.google.android.gms/app_webview/Cache/ea7f6123170a3a91_0
20. /data/com.google.android.gms/app_webview/Cache/ea7f6123170a3a91_1
21. /data/com.google.android.gms/app_webview/Cache/ea7f6123170a3a91_2

None of these files accessed are determined to be related to ByLock.

9. Conclusion

9.1. The Necessity of Determining Whether ByLock was Installed on the Phone

In order for an application to be precisely referred as it was installed on a phone, the traces of this application have to be searched on the phone's backup or image.

Today it is known that the application named ByLock leaves traces when installed on and uninstalled from the Apple iPhone, which runs on iOS operating systems and various brand and model phones run on Android operating systems and an example has been provided in the previous sections.

As it has been discussed in the "The Valid Method for the Detection of ByLock Users", detection of whether the messaging application in subject was downloaded and installed on the phone is only possible by;

1. Detection of whether ByLock application is installed on the smart phone or not,
2. If not installed, detection of any traces left when the application was uninstalled

The phone belonging to Taner KILIC was sent by judicial units to police department in charge following the Criminal Procedure Law No. 5271, Article 134: "Search of computers, computer programs and transcripts, copying and provisional seizure", image of the phone was created but has not been examined and no evidence has been obtained yet.

Following the examination, no evidence was found in the image of phone belonging to Taner KILIC, showing that ByLock was installed or uninstalled after installation.

9.2. The Necessity of Determining Whether ByLock was Used on the Phone

It has been observed that ByLock application was establishing a connection over port number 443 to application server with IP addresses 46.166.160.137 or 46.166.164.181, depending on the version of application.

As it has been detailed in the section "**Method for the Detection of ByLock Users**", it must be ascertained that the following flow has occurred in order for the individual to be referred that he or she was using this and similar systems:

1. The user installs the application on the phone he/she owns,
2. Smartphone establishes an Internet connection from the IP address that is assigned by the access provider.
3. It establishes a connection over port 443 (HTTPS) with the application server running on 46.166.160.137 or 46.166.164.181 IP addresses, depending on the application version,
4. User record is created on ByLock system using ByLock application
5. User is logged in to ByLock system using ByLock application,
6. Messaging and other features are used, using the application

As observed, in order for a user to be referred as he or she was using the system by logging in, the user has to establish minimum 2 connections, where 1st is for user registration and 2nd is for logging in.

As discussed in the section "**Method for the Detection of ByLock Users**" above, it is only possible to prove whether the alleged act was committed between the alleged date or date range, when the alleged connection established with the messaging system by obtaining:

1. Verifying if a connection was established from the IP address assigned by the access provider to 46.166.160.137 or 46.166.164.181 over port number 443[53] on the date or date ranges on which the action was taken from ICTA (Information and Communication Technologies Authority) logs.
2. Verifying if a connection was established from the IP address assigned by the access provider to 46.166.160.137 or 46.166.164.181 over port number 443[53] on the date or date ranges on which the action was taken from the access provider's logs,

from the detailed communication detection reports.

Those reports should be examined by taking the points, which discussed in the "**IP Assignment and Connection Routing Methods of Internet Service Providers**" and "**Method for the Detection of ByLock Users**" sections, into account

In some cases, connection logs of the requested IP addresses on a port number has been provided in the ICTA reports, the address visited (in other words, the type of the service utilized) and transmitted data amount might be missing.

Therefore, those reports with this entity do not apply with the law no. 5651 and cannot be considered as communication detection report.

For example, it will appear to be established a connection to ByLock server, although this is not an indication of usage of ByLock application;

1. When 1000's of websites are published on the same IP address using virtual web hosting method is considered; by taking into account that https://46.166.160.137 address might have been hosting one or more websites, when a connection established hosted on this IP address,
2. When https://46.166.160.137 is clicked that can be found on a website,
3. When the element known as "iframe" that is used to show a website within another website is used to show https://46.166.160.137,

On the 12th page of the "Technical Report of ByLock Application" prepared by MIT (National Intelligence Agency) "3.2 ByLock Application IP/Domain Name Analysis"

"Examination of network traffic of the application in subject, indicates that ByLock generally accessed to application server directly via IP address; however on some versions (For example, ByLock version 1.1.3), connection connecting to same server was established via "bylock.net" domain name."

On the 13th page of the very same report, it has been stated that:

"After detection of the IP Addresses, it was examined which domain name or name were matching those IP addresses between the date intervals ByLock was active. In this scope, it is been found out that only the IP address 46.166.160.137 among referred IP addresses was used with bylock.net domain name, between the dates 1 September 2015 – 9 October 2016. Research conducted on open sources also supports that condition. According to the analysis conducted on websites Virustotal.com, whois.domaintools.com, ptrarchive.com, no other domain name usage was observed in the period when the ByLock servers were active. (Appendix-4) "

On the 19th page of the very same report, it has been stated that:

*"In the installation files of versions of the application
Domain names are contained respectively in version 1.1.3 and 1.1.7;
- "https://bylock.net:443/SHU-Server"
- "https://46.166.164.181:443/App-Server"*

Version 1.1.3 is working by establishing a connection to "https://bylock.net:443/SHU-Server" URL. Following the quotation from the report, bylock.net domain name is associated with 46.166.160.137 IP address.

All application servers run on the addresses with word extension depending on their functions.

For example, version 1.1.7 of the application those addresses are identified in net/client/by/lock/f/p.java the source code and some are below and all source code is provided in appendix.

- User login: "https://46.166.164.181:443/App-Server/Login"
- Read Message: https://46.166.164.181:443/App-Server/ReadMail
- Send Message: "https://46.166.164.181:443/App-Server/SendMail"

Therefore, records in such reports are not indicators of connections established with IP address that relates to ByLock application.

It is defined in the 2nd article of the law no. 5651, Regulating Broadcasting in the Internet and Fighting Against Crimes Committed through Internet Broadcasting.

According to this article, the data that access provider is obliged to store, is defined as "The values related with any kind of access through Internet environment including the parties, time, period, the type of service used, the transferred data quantity and the connection points, etc." and it is clearly demanded that traffic to be stored.

The definitions made in the law no. 5651, Regulating Broadcasting in the Internet and Fighting Against Crimes Committed through Internet Broadcasting:

"d) Access: Getting an opportunity of use through connection to any Internet environment"

"e) Access provider: Any kind of real or legal persons or entities providing to their users access to Internet environment"

"g) Internet environment: The environment established on Internet which is open to public and not

covered by communications and personal or corporate computer systems”

“j) Traffic data: The values related with any kind of access through Internet environment including the parties, time, period, the type of service used, the transferred data quantity and the connection points, etc.”

According to the 6th article and clause b of the very same law that regulates the obligations of access provider is:
“b) To retain all traffic data about the services that it provides as specified in the regulations for the period specified in the regulation which cannot be less than six months and more than two years and to maintain accuracy, integrity and confidentiality of such data”

In case of deficiency of addresses that direct towards application functions and deficiency of network volume size (size of the data transferred), report cannot be referred as either precise or reliable.

Additionally, according to the explanation made by Suleyman Soylu, the Minister of Internal Affairs and news reported due to that explanation, access provider had some dysfunctionalities in their connection logging function, where reason is unknown, it is hard to refer to these records as reliable.

For this reason, these reports required to contain detailed traffic information in accordance with Law No. 5651; related to Internet access;

1. Sides (Source IP and destination IPs 46,166.160.137 and 46.166.164.181)
2. Connection time
3. Connection duration,
4. Type of service provided (Connected address),
5. Size of the data transferred
6. Connection port (Port number 443)

Based on the possibility that multiple users appear to be establishing the same connection at the same time because the access provider / operator uses a large-scale network address translation technique, I believe that the request from the ICTA (Information and Communication Technologies Authority) to determine the persons who are connected to the same or nearby base stations which seem to have established the same connection in the same hour-minute-second (same moment) at the date of the crime claim will also have a positive effect in reaching the material truth.

9.3. The Necessity of Determining the Continuity of ByLock Use

Given that, access to the Internet is not uninterrupted and not continuous, it is necessary to be able to determine at what time and at what intervals an action is being processed over the Internet.

That necessity is vital for crimes committed through Internet to be prevented instantly.

Recurrence and continuity of the action is significant, since the system in subject is used for interactional information transfer.

As it has been detailed in the section “*Default Method for the Detection of ByLock Users*”, it must be ascertained that the following flow has occurred in order for the individual to be referred that he or she was using this and similar systems:

1. The user installs the application on the phone he/she owns,
2. Smartphone establishes an Internet connection from the IP address that is assigned by the access provider.
3. It establishes a connection over port 443 (HTTPS) with the application server running on 46.166.160.137 or 46.166.164.181 IP addresses, depending on the application version,
4. User record is created on ByLock system using ByLock application
5. User is logged in to ByLock system using ByLock application,
6. Messaging and other features are used, using the application

As observed, in order for a user to be referred as he or she was using the system by logging in, the user has to establish minimum 2 connections, where 1st is for user registration and 2nd is for logging in.

However, in the case of accusation, only one date is specified although it is necessary to determine the followings;

1. Is this date installation date or messaging date,

2. Continuity of the action,
3. Other date ranges the action was committed

9.4. The Necessity of Establishing a Certain Causal Relationship between the Phone and the User

IMEI and phone numbers are determining elements for the mobile network connection made by phones.

ByLock messaging application can only be installed on mobile phones referred as “smart” running on Android and Apple iOS operating systems.

Connection to mobile phone network is not sufficient, in order for ByLock application system or as referred in trial documents “messaging network”, to operate. For this system to operate, Internet connection is essential.

IP address is the element that matches the connection with the user, in connections established with the Internet.

In order to be able to understand the event pattern and to ensure the connection of the certain causal link; how the alleged connection was matched to the phone number of the SIM card inserted in the device; the detection procedure must be explained together with the steps and technical reasons.

IP address is the element that matches the connection with the user, in connections established with the Internet.

Additionally, it is possible to use one IMEI number on different devices, because IMEI numbers can be defined on the devices with different IMEI numbers ^[60] using some tools.

For these reasons, it is not sufficient to state that the application was used on a phone that has a specific IMEI number.

It also might be necessary to query from ICTA whether IMEI number 353627055929742 was used on other devices other than this phone.

9.5. The Necessity of Determining the Use of Phone on the Date of Crime

The timeline of the system section includes 3938 files and file/directory names, times of last access, times of last modification, and the last date of modification of the file system.

The timeline of the user section includes 41188 files and file/directory names, times of last access, times of last modification, and the last date of modification of the file system.

The investigation has shown that Samsung Galaxy Note 2 GT-N7100 phone was launched on the Turkish market in September 2012.

According to the data on the phone, it was detected that;

1. The earliest date of use is 17/11/2012,
2. The latest date of use by the owner is 06/06/2017, at 16:44:03,
3. After that time, the phone was used:
 1. on 12/06/2017, between 11:58:51 and 16:44:03,
 2. on 13/06/2017, between 00:40:04 and 16:42:01.

There is no sign of a reset to factory settings or a similar disruption during this time period. On the contrary, the phone was used regularly while it was on.

On 27/08/2014, the alleged date of crime, the phone was used between:

1. 21:16:16 and 21:17:25,
2. 00:07:15 and 00:08:20.

During this period of use, none of the files under the user directory was accessed are determined to be related to ByLock.

⁶⁰ Also referred as Copying or Cloning

9.6. Retrieval of Other Records Regarding the Phone and the User

Therefore, I believe that examination of the log records of the base stations and HTS logs that show where the phone was used by synchronizing the individuals' known physical locations, by determining date or date intervals, is necessary.

Sincerely,
T. Koray Peksayar

B.Sc. in Mechanical Eng. – M.Sc. in Information Tech.
Information and Digital Forensic Expert – Chartered Judicial Expert
ITU M.Sc. Dip. No. 76-387

Appendices:

Appendix-1: Source code where the related functions are defined and used to access to addresses, in the ByLock application, version 1.1.7 (net/client/by/lock/f/p.java)

Appendix-2: USB Memory Stick
content:

1. Android backup of the Samsung Galaxy Note 2 GT-N7100 phone,
2. Disk Image of the Samsung Galaxy Note 2 GT-N7100 phone,
3. Timeline of the file system of Samsung Galaxy Note 2 GT-N7100 phone

Appendix-1: Source code where the related functions are defined and used to access to addresses, in the ByLock application version 1.1.7 (net/client/by/lock/f/p.java)

```
package net.client.by.lock.f;
```

```

public class p
{
    public static String A()
    {
        return H() + "/DeleteMail";
    }

    public static String B()
    {
        return H() + "/UpdateStatus";
    }

    public static String C()
    {
        return H() + "/UpdateName";
    }

    public static String D()
    {
        return H() + "/DeleteChat";
    }

    public static String E()
    {
        return H() + "/AddFriendToGroup";
    }

    public static String F()
    {
        return H() + "/RemoveFriendFromGroup";
    }

    public static String G()
    {
        return H() + "/Register";
    }

    private static String H()
    {
        return "https://46.166.164.181:443/App-Server";
    }

    public static String a()
    {
        return H() + "/Login";
    }

    public static String b()
    {
        return H() + "/Logout";
    }

    public static String c()
    {
        return H() + "/UpdatePublicMessage";
    }

    public static String d()
    {
        return H() + "/SendChat";
    }
}

```

```

public static String e()
{
    return H() + "/ReceiveChat";
}

public static String f()
{
    return H() + "/GetRosterEvent";
}

public static String g()
{
    return H() + "/AddFriendToRoster";
}

public static String h()
{
    return H() + "/GetFriendInformation";
}

public static String i()
{
    return H() + "/RenameFriend";
}

public static String j()
{
    return H() + "/RemoveFriend";
}

public static String k()
{
    return H() + "/SendFile";
}

public static String l()
{
    return H() + "/ReceiveFile";
}

public static String m()
{
    return H() + "/DeleteFileTransfer";
}

public static String n()
{
    return H() + "/GetFileTransferInformation";
}

public static String o()
{
    return H() + "/ChangePassword";
}

public static String p()
{
    return H() + "/MakeCall";
}

public static String q()
{
    return H() + "/AnswerCall";
}

public static String r()
{
    return H() + "/RejectCall";
}

```

```
public static String s()
{
    return H() + "/CancelCall";
}

public static String t()
{
    return H() + "/CloseCall";
}

public static String u()
{
    return H() + "/CreateGroup";
}

public static String v()
{
    return H() + "/RemoveGroup";
}

public static String w()
{
    return H() + "/RenameGroup";
}

public static String x()
{
    return H() + "/SetNewPassword";
}

public static String y()
{
    return H() + "/SendMail";
}

public static String z()
{
    return H() + "/ReadMail";
}
}
```