

# Akıllı Çocuk Saatleri

written by Mert SARICA | 1 September 2022

If you are looking for an English version of this article, please visit [here](#).

Bu hikaye, 4 Mayıs 2022 tarihinde Erman ATEŞ isimli bir okurumdan aldığım e-posta ile başladı. Bilinçli ve duyarlı bir baba olan Erman Bey göndermiş olduğu e-postada, akıllı çocuk saatlerinin bir çok ebeveyn tarafından haklı gerekçelerle tercih edilmeye başlandığını ancak yazılım, güvenlik ve mahremiyet açısından hem bir standarda tabi olmamaları hem de Instagram'da gördüğü bir mesaj nedeniyle tüm ebeveynler adına endişe duymaya başladığını ve bu nedenle de bu konuya mercek tutmamı rica etmişti. Instagram Dolandırıcıları, Arka Kapı Avı, Tuzak Sistem ile Hacker Avı blog yazılarımda olduğu gibi okurlarına her daim kulak veren bir güvenlik araştırmacısı olarak toplumsal fayda ve bilgi güvenliği farkındalığı adına bu konuya eğilmeye karar verdim.



Konu:

çocuklar için akıllı saatler

Mesajınız:

Merhaba Mert Bey,

Sizleri yıllardır ilgiyle takip ediyorum.

Ben 9 yaşında bir erkek çocuk babasıyım ve çocukların takip edilebildiği akıllı dijital saatlerin bir çok anne baba tarafından tercih edilmeye başlandığını görmekteyim. Nitekim cihazlar ve içlerindeki yazılımlar standartlara uyan ve lisans sahibi değiller genellikle.

Bazı instagram hesaplarında sadece belirli numaralardan aranması gerekirken herhangi birinin arayabildiği, sim kartın internet erişimi sağlaması vesilesiyle saate bağlanılarak ses ve video kaydı alınabilmesi gibi çeşitli endişelerin baş gösterdiğini görüyorum.

dijitalbaba orhan toker beyin instagram hesabı ve web sayfalarında bu konuyla ilgili birkaç paylaşım gördüm ve hem kendi ailem hem de birçok aile için endişelenmeye başladım.

bu konuda farkındalığı artırmak amacıyla sizlerin akıllı saatlerin güvenliği konusunda bir araştırma/değerlendirme bloğu yazmanızın mümkün olup olamayacağını sormak isterim (inaniyorum bu konuda size yazan ilk kişi ben değilimdir).

Teşekkürler, saygılar.

Erman

Aşağıdaki fotoğrafa bakıldığında akıllı çocuk saatleri gerçekten ebeveynler için çocuklarını gözetim altında tutmak için faydalanabilecekleri büyük bir teknolojik nimet mi ?



Yoksa ařađıdaki diđer bir fotođrafa bakıldıđında ebeveynlerin, kendilerinin ve çocuklarının mahremiyetini, özel hayatlarının gizliliđini istemeden de olsa tehlikeye attıkları, ortam dinlemeye imkan tanıyan saat görünümlü potansiyel casus bir cihaz mı ?



Bu sorulara yanıt bulmak için ilk olarak güvenlik arařtırmamda kullanmak üzere fiyat aısından uygun olan bir ocuk saati satın almaya karar verdim. Bunun için Hepsiburada, Trendyol gibi alıřveriř sitelerindeki Akıllı ocuk Saatleri kategorilerini incelemeye bařladım. En ok satılan, yorum ve deęerlendirme yapılan saatlere baktıktan sonra 1000'e yakın deęerlendirmesi olan bir marka ve modelde karar kılıp, satın aldım.

İlgili Kategoriler

Akıllı Çocuk Saati

Marka

Marka ara

- Alcatel
- TCL
- Smartbell
- Bilicra
- HANGAREX
- Fitbit
- RealFoni
- Phosfon

Renk



Fiyat

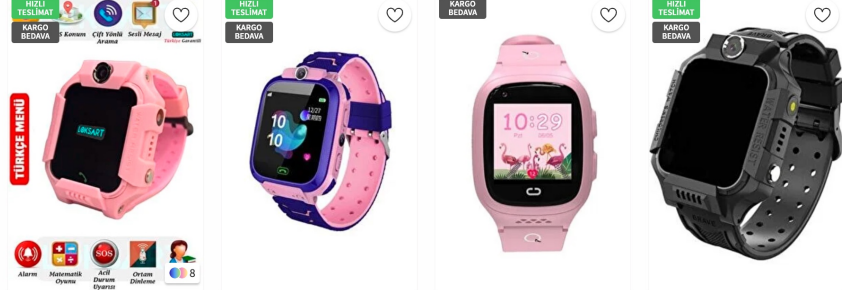
"Akıllı Çocuk Saati" araması için 673 sonuç listeleniyor

Önerilen

Hızlı Teslimat yapılan ürünleri göster.

Uygula

ÖNCEKİ ÜRÜNLERİ GÖSTER



Loksart Sim Kartlı Akıllı Çocuk Saat Fitbit Kız Çocuk Pembe Sim Kartlı Türkçe Menü İmei Kayıtlı Smartcel... Qfit Qfit Q4 4.5g Akıllı Çocuk Saati Pembe medigen Akıllı Çocuk Saati Sim Kartlı Konum Takip

Fiyat Aralığı

250 - 500 TL

Cinsiyet

Erkek Çocuk

Cinsiyet

Kız Çocuk

Temizle

Marka

Filtrele

Nabi

Nalan

Omni

Otto

Q12

Xinhang

Yohosport

Yukka

Intermax

Fiyat Aralığı

250 500

50 - 100 TL

100 - 250 TL

250 - 500 TL

500 - 750 TL

750 - 1000 TL

1000 - 1500 TL

1500 - 2000 TL

2000 - 2500 TL

2500 TL üzerinde

Marka Sharplace + Easytoy + Flameer + Xbazzar + StarWomen + Sunfay + Waysle +



LBS Konumlu Akıllı Çocuk Takip Saati Sim Kartlı Arama, Kamera, Göz Dileme... LBS Konumlu Akıllı Çocuk Takip Saati Sim Kartlı Arama, Kamera, Göz Dileme... LBS Konumlu Akıllı Çocuk Takip Saati Sim Kartlı Arama, Kamera, Göz Dileme... LBS Konumlu Akıllı Çocuk Takip Saati Sim Kartlı Arama, Kamera, Göz Dileme...

389,90 TL 389,90 TL 389,90 TL 489,90 TL

★★★★★ 1575 ★★★★★ 1575 ★★★★★ 1575 ★★★★★ 1575



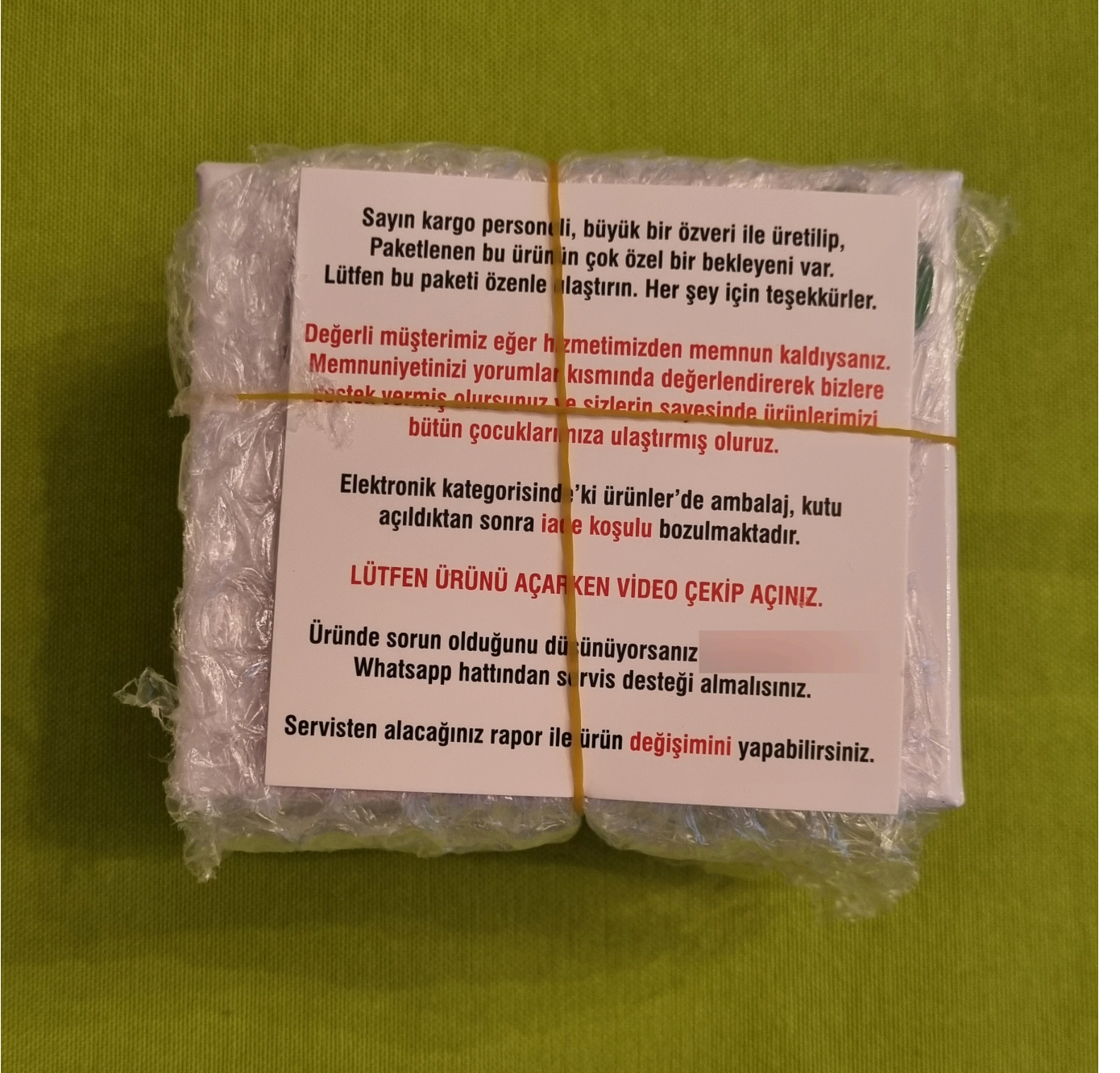
Smartbell Q539/2020 Sim Kartlı Akıllı Çocuk Saati - Pembe Smartbell Q539/2020 Sim Kartlı Akıllı Çocuk Saati - Mavi Kallow Z10 Akıllı Çocuk Takip Saati - Yeşil Kallow Z10 Akıllı Çocuk Takip Saati - Mor

385,00 TL 385,00 TL 390,00 TL 390,00 TL

Sepete ekle ★★★★★ 914 ★★★★★ 801 ★★★★★ 801



ÜRÜNÜ 2 SAAT BOYUNCA POWER BANK VEYA BİLGİSAYAR İLE ŞARJ EDİNİZ.  
AKSİ TAKDİRDE ÜRÜN GARANTİ KAPSAMI DIŞINDA KALACAKTIR.



Sayın kargo personeli, büyük bir özveri ile üretilip,  
Paketlenen bu ürünün çok özel bir bekleyeni var.  
Lütfen bu paketi özenle ulaştırın. Her şey için teşekkürler.

Değerli müşterimiz eğer hizmetimizden memnun kaldıysanız.  
Memnuniyetinizi yorumlar kısmında değerlendirerek bizlere  
destek vermiş olursunuz ve sizlerin sayesinde ürünlerimizi  
bütün çocuklarımıza ulaştırmış oluruz.

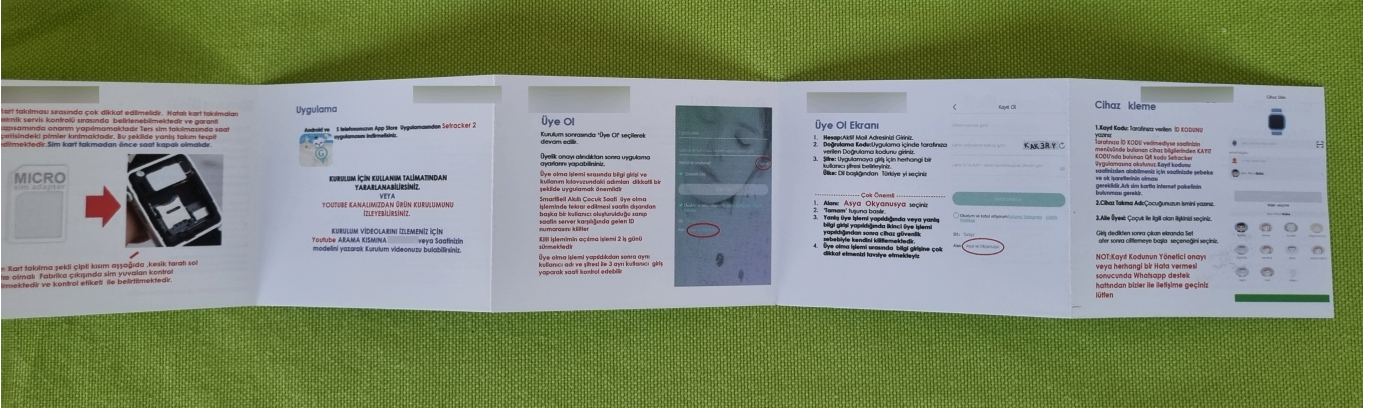
Elektronik kategorisindeki ürünler'de ambalaj, kutu  
açıldıktan sonra **iate koşulu** bozulmaktadır.

**LÜTFEN ÜRÜNÜ AÇARKEN VIDEO ÇEKİP AÇINIZ.**

Üründe sorun olduğunu düşünüyorsanız  
Whatsapp hattından servis desteği almalısınız.

Servisten alacağınız rapor ile ürün **değişimini** yapabilirsiniz.

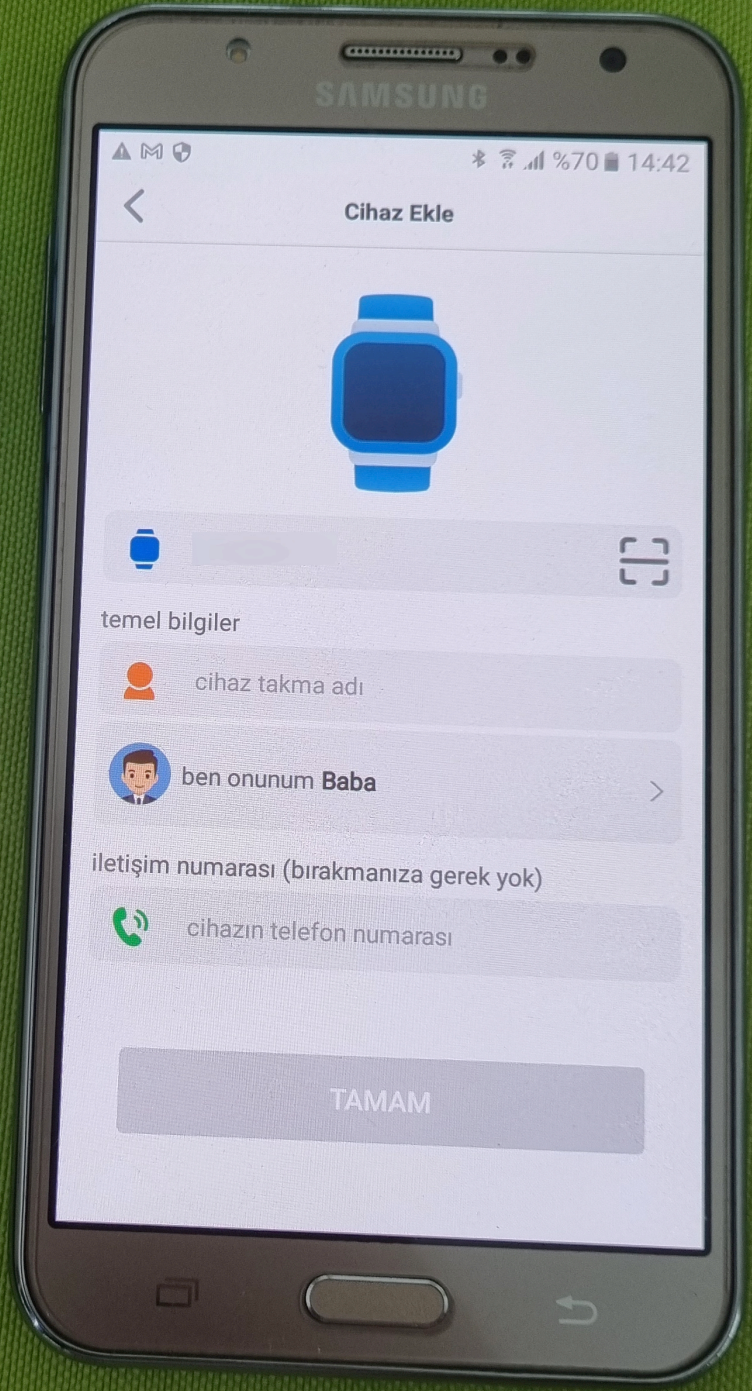
Saati kutusundan çıkarıp, kurulum kılavuzunu incelediğimde, saati uzaktan yönetebilmek için Çinli 3G Electronics isimli bir şirket tarafından geliştirilen Android veya iOS mobil uygulamasının kurulmasının gerektiği belirtiliyordu.



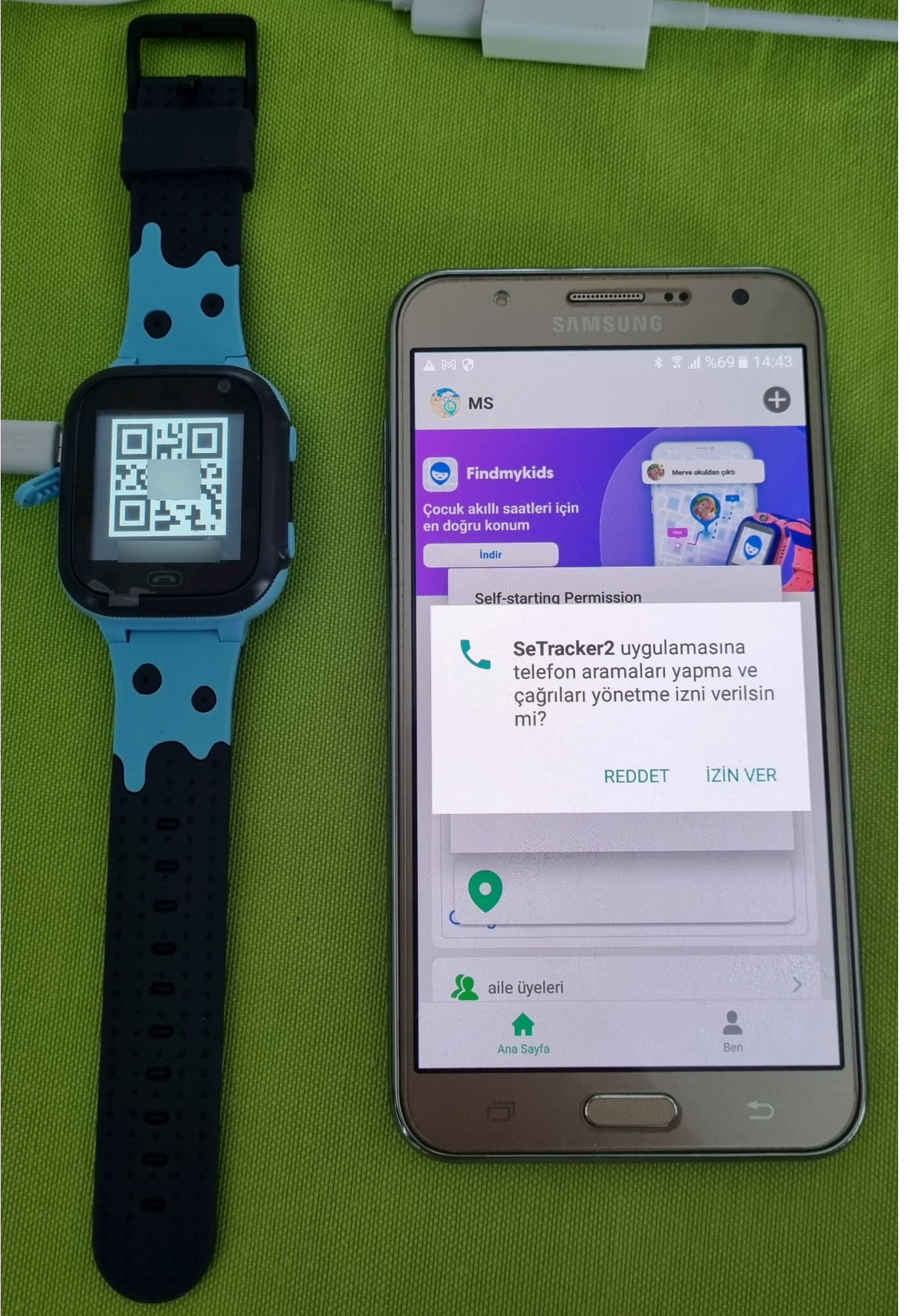
SeTracker2 isimli uygulamanın topladığı bilgilere baktığımızda lokasyon, ses ve görüntü kaydından, rehber, isim, cep telefonu ve e-posta adresine kadar kişiye özel, hassas, mahrem sayılabilecek bilgiler olduğunu gördüm.

Saate SIM kartı takıp, çalıştırdıktan sonra SeTracker2 uygulamasını açıp, kayıt oldum. Daha sonra uygulamaya ile saati eşleştirdikten sonra uygulamayı ve menü adımlarını incelemeye başladım.

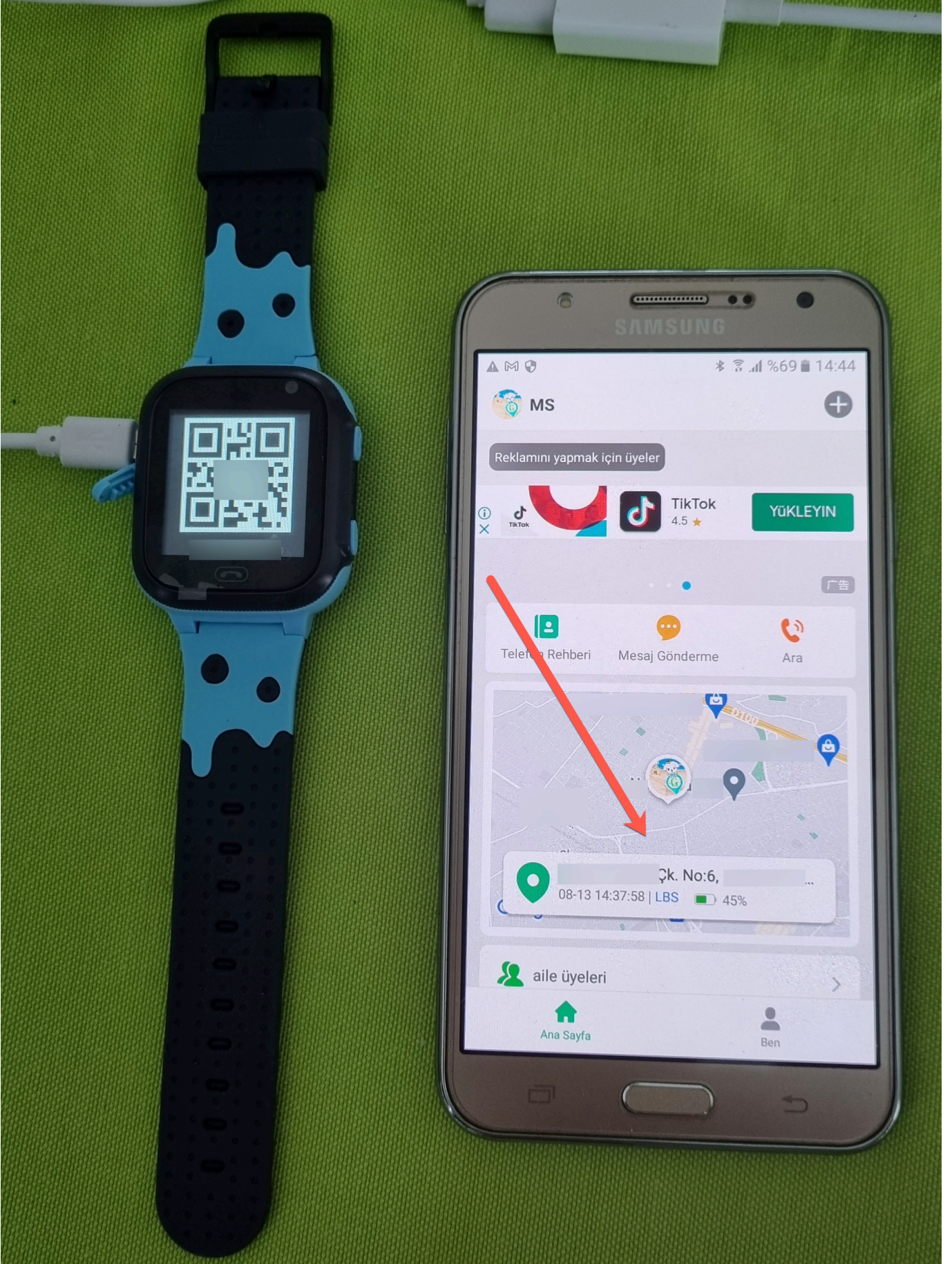


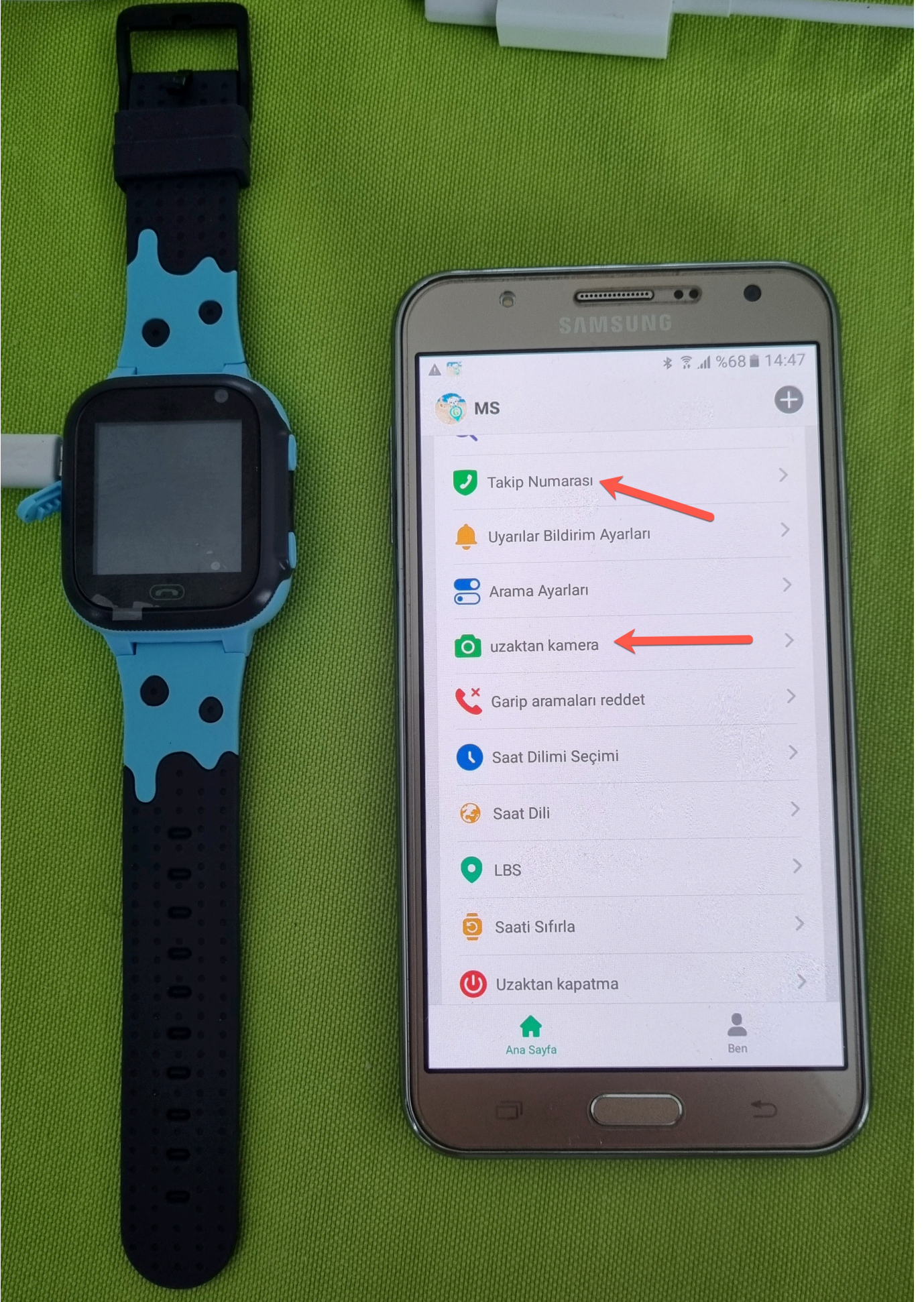


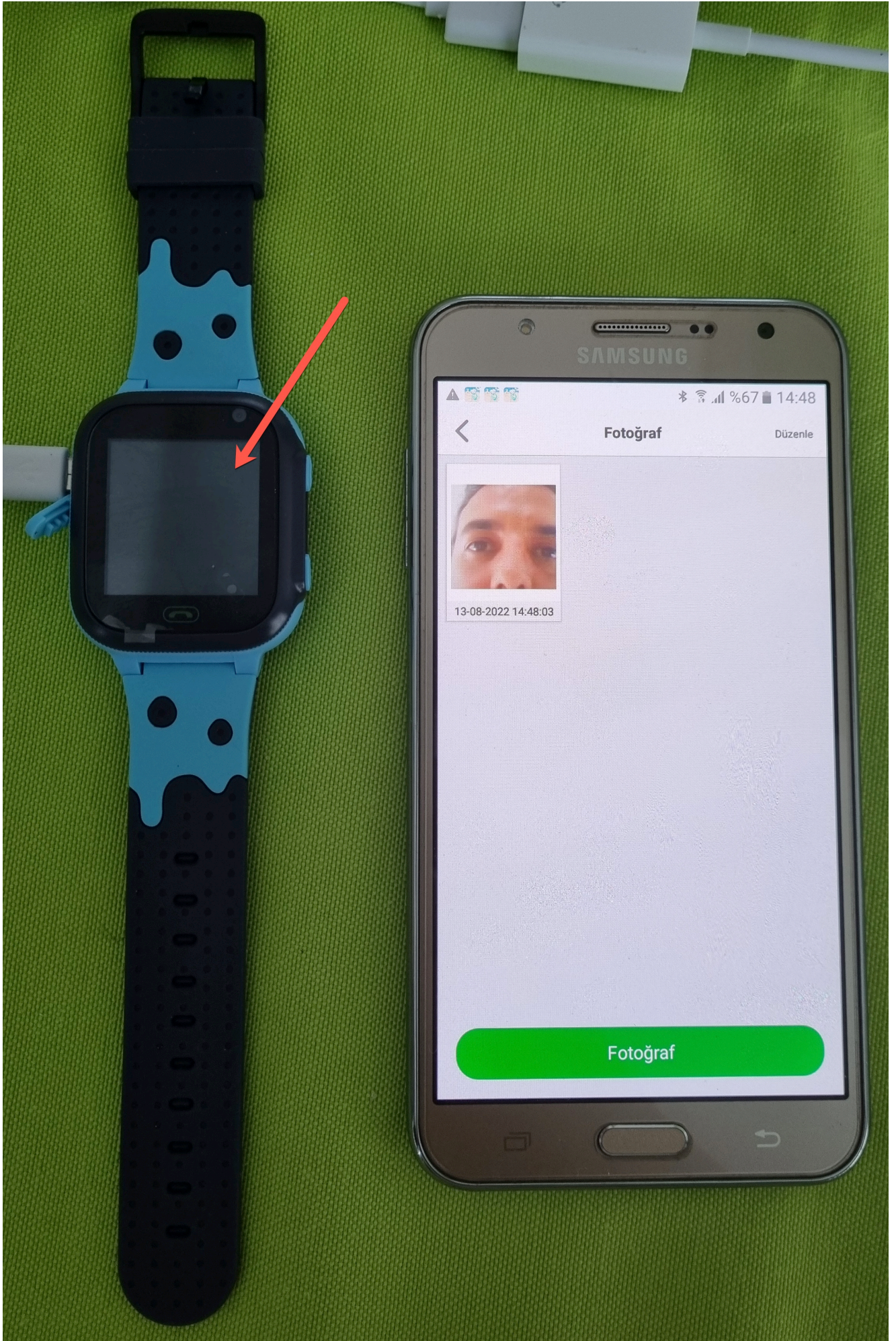




Uygulamada öncelikle dikkatimi çeken nokta, saatin harita üzerinden anlık olarak izlenebilmesi daha sonra ise Takip Numarası ve uzaktan kamera menü adımları oldu. Uzaktan kamera menüsü üzerinden saatteki kamera ile istediğiniz zaman fotoğraf çekilebiliyorsunuz. Bu esnada saat herhangi bir görsel veya işitsel bir uyarı oluşturmuyor. Takip numarası menüsü ile ise saatin girilen cep telefonu numarasını aramasını sağlayabiliyorsunuz ve saatteki mikrofon sayesinde de ortam dinlemesi yapılabiliyor. Bu esnada yine uzaktan kamera adımımda olduğu gibi telefon, ortam dinlemesi yapıldığına dair herhangi bir uyarı vermiyor.







“E ne güzel işte Mert, çocuğumuzu anlık olarak izleyebilir ve dinleyebiliriz” diye düşünüyor olabilirsiniz. Peki SeTracker2 uygulamasına giriş için kullandığınız e-posta adresinizi ve içinde özel karakter bile kullanarak güçlendiremediğiniz parolanızın bir an olsun art niyetli kişiler tarafından çalındığını veya tahmin edildiğini düşünelim. Art niyetli kişi, çocuğunuzun kolundaki saate uygulama üzerinden bağlanarak konumunu anlık olarak izleyebilir, fotoğrafını çekebilir, mesaj gönderebilir, gönderdiği mesajı silip geride iz bırakmayabilir, saatin belirttiği telefon numarasını aramasını sağlayarak ortam dinlemesi yaparak mahremiyetinizi, özel hayatınızın gizliliğini ihlal edebilir. Ayrıca art niyetli kişi tarafından gerçekleştirilen tüm bu işlemlerin iz kaydına (log) SeTracker2 uygulaması üzerinden ulaşma şansınızın olmadığını da altını çizeyim!

“Mert ben çok dikkatliyim, temkinliyim, kolay kolay dolandırıcıların ağına düşmem” de diyebilirsiniz. Aynı parolayı birden fazla web sitesine giriş esnasında kullanıyorsanız, o web sitelerinden biri çoktan hacklenmiş ve kullanıcı adınız/e-posta ve parolanız ele geçirilmiş olabilir. Çok Faktörlü Kimlik Doğrulaması (MFA) kullanmadığınız durumda (SeTracker2 uygulaması MFA desteklemiyor!) art niyetli kişilerin elde ettiği bu bilgilerle hesabınızın olduğu web sitelerine, mobil uygulamalara (SeTracker2 uygulaması gibi) rahatlıkla giriş yapılabileceğini unutmayın!

Çok faktörlü kimlik doğrulaması (MFA), kullanıcıların yalnızca bir paroladan daha fazla bilgi girmesini gerektiren, hesapta çok adımlı oturum açma sürecidir. Örneğin, kullanıcılardan parolanın yanı sıra e-posta adreslerine, cep telefonlarında gönderilen bir kodu (internet şubeye girişte olduğu gibi) girmeleri, mobil uygulamaya gönderilen bir isteği kabul etmeleri, gizli bir soruyu yanıtlamaları ya da parmak izlerini taratmaları istenebilir. İkinci bir doğrulama yöntemi, art niyetli kişilerin parolasını ele geçirildiği kullanıcıların hesaplarına yetkisiz erişmesini önlemeye yardımcı olmaktadır.

Bir diğer önemli konu ise ortam dinlemesi özelliğine sahip saatler kullanarak istemeden de olsa çocuğunuz üzerinden suç işliyor olabilirsiniz. Hukukçu olmasam da 5237 Sayılı Türk Ceza Kanunu'nun “Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması” başlıklı 133. maddesine dikkatinizi çekmek isterim:

(1) Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, iki yıldan beş yıla kadar hapis cezası ile



cezalandırılır.

(2) Katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan kişi, altı aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır.

(3) (Değişik: 2/7/2012-6352/80 md.) Kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri hukuka aykırı olarak ifşa eden kişi, iki yıldan beş yıla kadar hapis ve dörtbin güne kadar adli para cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.

Tahminimce başta Koş Mert Koş başlıklı blog yazım olmak üzere, güvenlik araştırmalarım aşına olanlarınızın bu yazımda tersine mühendislikle, statik ve dinamik kod analizi ile SeTracker2 uygulamasını analiz edip tespit ettiğim zafiyetlerin nasıl kötüye kullanılabileceğini göstermemi veya saatte keşfettiğim donanımsal bir zafiyet ile saatin nasıl casus bir cihaza dönüştürebildiğini görmeyi umuyorlardı. Tüm bu anlattıklarımın sonra bunca zahmete girmeden bu saatin, SeTracker2 uygulaması sayesinde art niyetli kişilere kötüye kullanım için davetiye çıkardığını, ebeveynler ve çocukları için büyük bir tehlike oluşturduklarını net olarak aktarabildiğimi düşünüyorum. :) Yine de uygulama ile ilgili teknik bilgi edinmek isteyenler var ise önceki yıllarda yapılmış olan çalışmalar için buraya ve de buraya göz atabilirler.

Umuyorum ki 2017 yılında Almanya'nın aldığı bu örnek karar gibi otoritelerimiz de benzer bir karar alarak, yasa dışı ortam dinlemesi yapma özelliğine sahip olan bu saat görünümlü potansiyel casus cihazların alışveriş sitelerinde satışını engelleyerek, ebeveynleri ve çocukları bu tür tehlikelerden korumak için önemli bir adım atarlar.

Bu bilgiler ışığında, ortam dinlemesi yapabilen akıllı çocuk saatleri kullanacaklara risklerini bilerek kullanmalarını tavsiye ettikten sonra siz sevgili okurlarımdan farkındalık yaratma adına bu yazıyı ebeveyn olan arkadaşlarınızla, dostlarınızla ve sevdiklerinizle paylaşmanızı önemle rica ederim.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

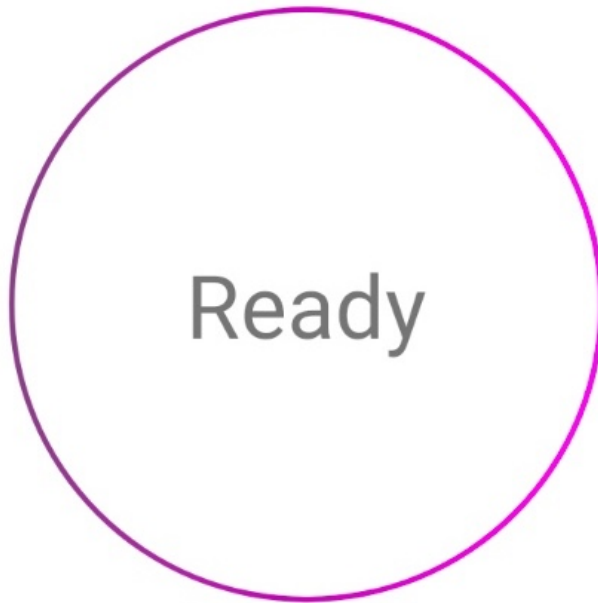
Not: Teknik okurlarım için de SeTracker2 uygulamasında SSL Pinning yönteminin kullanıldığını, HTTPS trafiğini analiz etmek için PCAPdroid isimli bir

Android uygulaması sayesinde basit bir şekilde trafiđi kayıt altına aldđımı ve daha sonrasında da Wireshark aracı ile analiz edebildiđimi de paylařayım.



STATUS

CONNECTIONS



## PCAP file

Create a PCAP file in device storage



## Target app



SeTracker2 (com.tgelec.setracker)



# ← Settings

Collector port  
1234

---

## Traffic inspection

### Block private DNS

Detect and possibly block private DNS to inspect DNS traffic. Disabling this can hinder traffic analysis



### Geolocation

Show country and ASN info by performing offline lookups

### TLS decryption

Decrypt the SSL/TLS traffic by performing mitm. This may now work with some apps, check out the user guide



### Block QUIC

Block QUIC connections to possibly fall back to decryptable TLS. Some apps may stop working



---

## Capture

### Capture as root

Allows PCAPdroid to run with other VPN apps



PCAPdroid\_15\_Aug\_08\_10\_30.pcap

ip.dst == 54.169.10.136 and http

No.	Time	Source	Destination	Protocol	Length	Info
31	2022-08-15 05:10:42.640911	10.215.173.1	54.169.10.136	HTTP	529	GET /app/public/S10APP/v2_getNoticeInfo?language=enUS&time...
78	2022-08-15 05:10:44.155382	10.215.173.1	54.169.10.136	HTTP	750	POST /app/public/S10APP/v2_new_userLogin2 HTTP/1.1 (applicat...
171	2022-08-15 05:10:45.354494	10.215.173.1	54.169.10.136	HTTP	645	GET /app/u9103038.580153.M80Q0808UFP68157495DR5J2I8JVFVH1L1666...
181	2022-08-15 05:10:45.426324	10.215.173.1	54.169.10.136	HTTP	645	GET /app/u9103038.580153.M80Q0808UFP68157495DR5J2I8JVFVH1L1666...
189	2022-08-15 05:10:45.433760	10.215.173.1	54.169.10.136	HTTP	634	GET /app/u9103038.580153.M80Q0808UFP68157495DR5J2I8JVFVH1L1666...
267	2022-08-15 05:10:46.002569	10.215.173.1	54.169.10.136	HTTP	575	GET /app/public/S10APP/v2_findAdInfo_new?language=enUS&flag=...
269	2022-08-15 05:10:46.015562	10.215.173.1	54.169.10.136	HTTP	660	POST /push/msg/bindUser HTTP/1.1 (application/x-www-form-ur...
419	2022-08-15 05:10:47.813877	10.215.173.1	54.169.10.136	HTTP	587	GET /app/public/S10APP/v2_new_findUserDeviceInfo?language=enL...
420	2022-08-15 05:10:47.813892	10.215.173.1	54.169.10.136	HTTP	587	GET /app/public/S10APP/v2_new_findUserDeviceInfo?language=enL...
423	2022-08-15 05:10:47.814177	10.215.173.1	54.169.10.136	HTTP	633	GET /app/u9103038.580153.FTVJ3JUB7DTCGMA0964GRVTKLN4FAFMT1666...
424	2022-08-15 05:10:47.814181	10.215.173.1	54.169.10.136	HTTP	677	GET /app/u9103038.580153.FTVJ3JUB7DTCGMA0964GRVTKLN4FAFMT1666...
427	2022-08-15 05:10:47.815374	10.215.173.1	54.169.10.136	HTTP	638	GET /app/u9103038.580153.FTVJ3JUB7DTCGMA0964GRVTKLN4FAFMT1666...
456	2022-08-15 05:10:48.750561	10.215.173.1	54.169.10.136	HTTP	689	GET /app/u9103038.580153.FTVJ3JUB7DTCGMA0964GRVTKLN4FAFMT1666...
473	2022-08-15 05:10:48.987693	10.215.173.1	54.169.10.136	HTTP	608	POST /S10APP/findFaceAuthInfo HTTP/1.1 (application/x-www-fc...
536	2022-08-15 05:10:51.566225	10.215.173.1	54.169.10.136	HTTP	719	GET /app/u9103038.580153.FTVJ3JUB7DTCGMA0964GRVTKLN4FAFMT1666...

File Data: 299 bytes

HTML Form URL Encoded: application/x-www-form-urlencoded

- Form item: "language" = "enUS"
- Form item: "appid" = "aaagg10006"
- Form item: "password" = "5f7b2e730cbbc2ca49428cfc0a19f249320e65fefbd6830299e24b0942745b7"
- Form item: "loginname" = "mert.sarica@gmail.com"
- Form item: "flag" = "70"
- Form item: "version" = "2.8.6"
- Form item: "isIPHONE" = "1"
- Form item: "timestampn" = "1669540243000"

01a0 30 30 36 26 70 61 73 73 77 6f 72 64 3d 35 66 37 0066pass word=5f7

01b0 62 32 65 37 33 30 63 62 62 63 32 63 61 34 39 34 b2e730cb bc2ca494

01c0 32 38 63 66 63 30 61 31 39 66 32 34 39 33 32 30 28cfc0a1 9f249320

01d0 65 36 35 66 65 66 62 64 36 38 33 30 32 39 39 65 e65fefbd 6830299e

Frame (750 bytes) | Decrypted TLS (688 bytes)

Text item (text), 74 bytes

Packets: 809 - Displayed: 15 (1.9%)

Profile: Default

PCAPdroid\_15\_Aug\_08\_10\_30.pcap

ip.dst == 54.169.10.136 and http

No.	Time	Source	Destination	Protocol	Length	Info
31	2022-08-15 05:10:42.640911	10.215.173.1	54.169.10.136	HTTP	529	GET /app/public/S10APP/v2_getNoticeInfo?language=enUS&time...
78	2022-08-15 05:10:44.155382	10.215.173.1	54.169.10.136	HTTP	750	POST /app/public/S10APP/v2_new_userLogin2 HTTP/1.1 (applicat...
171	2022-08-15 05:10:45.354494	10.215.173.1	54.169.10.136	HTTP	645	GET /app/u9103038.580153.M80Q0808UFP68157495DR5J2I8JVFVH1L1666...
181	2022-08-15 05:10:45.426324	10.215.173.1	54.169.10.136	HTTP	645	GET /app/u9103038.580153.M80Q0808UFP68157495DR5J2I8JVFVH1L1666...
189	2022-08-15 05:10:45.433760	10.215.173.1	54.169.10.136	HTTP	634	GET /app/u9103038.580153.M80Q0808UFP68157495DR5J2I8JVFVH1L1666...
267	2022-08-15 05:10:46.002569	10.215.173.1	54.169.10.136	HTTP	575	GET /app/public/S10APP/v2_findAdInfo_new?language=enUS&flag=...
269	2022-08-15 05:10:46.015562	10.215.173.1	54.169.10.136	HTTP	660	POST /push/msg/bindUser HTTP/1.1 (application/x-www-form-ur...
419	2022-08-15 05:10:47.813877	10.215.173.1	54.169.10.136	HTTP	587	GET /app/public/S10APP/v2_new_findUserDeviceInfo?language=enL...
420	2022-08-15 05:10:47.813892	10.215.173.1	54.169.10.136	HTTP	587	GET /app/public/S10APP/v2_new_findUserDeviceInfo?language=enL...
423	2022-08-15 05:10:47.814177	10.215.173.1	54.169.10.136	HTTP	633	GET /app/u9103038.580153.FTVJ3JUB7DTCGMA0964GRVTKLN4FAFMT1666...
424	2022-08-15 05:10:47.814181	10.215.173.1	54.169.10.136	HTTP	677	GET /app/u9103038.580153.FTVJ3JUB7DTCGMA0964GRVTKLN4FAFMT1666...
427	2022-08-15 05:10:47.815374	10.215.173.1	54.169.10.136	HTTP	638	GET /app/u9103038.580153.FTVJ3JUB7DTCGMA0964GRVTKLN4FAFMT1666...
456	2022-08-15 05:10:48.750561	10.215.173.1	54.169.10.136	HTTP	689	GET /app/u9103038.580153.FTVJ3JUB7DTCGMA0964GRVTKLN4FAFMT1666...
473	2022-08-15 05:10:48.987693	10.215.173.1	54.169.10.136	HTTP	608	POST /S10APP/findFaceAuthInfo HTTP/1.1 (application/x-www-fc...
536	2022-08-15 05:10:51.566225	10.215.173.1	54.169.10.136	HTTP	719	GET /app/u9103038.580153.FTVJ3JUB7DTCGMA0964GRVTKLN4FAFMT1666...

File Data: 299 bytes

HTML Form URL Encoded: application/x-www-urlencoded

- Form item: "language" = "enUS"
- Form item: "appid" = "aaagg10006"
- Form item: "password" = "5f7b2e730cbbc2ca49428cfc0a19f249320e65fefbd6830299e24b0942745b7"
- Form item: "loginname" = "mert.sarica@gmail.com"
- Form item: "flag" = "70"
- Form item: "version" = "2.8.6"
- Form item: "isIPHONE" = "1"
- Form item: "timestampn" = "1669540243000"

01a0 30 30 36 26 70 61 73 73 77 6f 72 64 3d 35 66 37 0066pass word=5f7

01b0 62 32 65 37 33 30 63 62 62 63 32 63 61 34 39 34 b2e730cb bc2ca494

01c0 32 38 63 66 63 30 61 31 39 66 32 34 39 33 32 30 28cfc0a1 9f249320

01d0 65 36 35 66 65 66 62 64 36 38 33 30 32 39 39 65 e65fefbd 6830299e

Frame (750 bytes) | Decrypted TLS (688 bytes)

Text item (text), 74 bytes

Packets: 809 - Displayed: 15 (1.9%)

Profile: Default