

**SİBER SUÇLARLA MÜCADELE ŞUBE MÜDÜRLÜĞÜ**  
**ADLİ BİLİŞİM BÜRO AMİRLİĞİ**  
**İMAJ (ADLİ KOPYA) ALMA VE İNCELEME RAPORU**

<b>RAPOR YAZIM TARİHİ</b>	11.09.2020
<b>TALEP EDEN BİRİM</b>	İstanbul Cumhuriyet Başsavcılığı Terör ve Örgütlü Suçlar Soruşturma Bürosu
<b>SORUŞTURMA NO</b>	İstanbul Cumhuriyet Başsavcılığının 08/11/2017 tarih ve 2017/83967 soruşturma sayılı yazısı
<b>KARARI VEREN MAKAM</b>	İstanbul 12. Sulh Ceza Hâkimliğinin 06/11/2017 tarihli ve 2017/4661 D. İş sayılı kararı
<b>ŞÜPHELİ</b>	Celal Yasin ÖZDEMİR (TC: [REDACTED])

“FETÖ/PDY Silahlı Terör Örgütüne Üye Olma” suçu ile ilgili olarak şüpheli Celal Yasin ÖZDEMİR (TC: [REDACTED]) isimli şahıstan elde edilen dijital materyallerin imajlarının (adli kopyalarının) alınması ve alınan imajlar üzerinde soruşturma kapsamında gerekli incelemelerin yapılarak tespit edilen hususlar doğrultusunda inceleme raporu tanzim edilmesi.

Adli bilişim incelemelerinde dijital materyalden, delil toplama, toplanan delilin anlamlandırılması ve incelenmesi aşamalarında bazı teknik ifadeler kullanılmaktadır. Öncelikle, bu ifadelerin ne anlama geldiğinin tarif edilmesinde fayda olacağı değerlendirilmektedir.

<b>İmaj (Adli Kopya)</b>	Dijital materyallerin alınan adli kopyasıdır.
<i>Delil materyalin türü, niteliği güvenlik parametreleri gibi özelliklerine göre imaj almanın farklı yöntemleri mevcuttur;</i>	
<b>Fiziksel İmaj</b>	Depolama alanının bütünü (tüm sektörler) dahil edilerek alınan imaj yöntemidir. Bu yöntemde delil içerisinde mevcut, silinmiş, ayrılmamış, artık ve kullanılmayan alanların tamamı incelenebilmektedir.
<b>Mantıksal İmaj</b>	Depolama alanının sadece mevcut alanının (göze görülebilen) imajının alınabildiği yöntemdir. Bu yöntem fiziksel imajın farklı sebeplerle alınamadığı durumlarda (RAID sistemler, şifrelenmiş sürücüler) uygulanabilmektedir.
<b>Dosya Sistemi</b>	Depolama alanında bulunan verilerin kısmi olarak imajının alındığı yöntemdir. Fiziksel veya mantıksal yöntemlerin uygulanmadığı veya kesin delilin bulunduğu alanın tespit edildiği durumlarda kısmi dosya sistemi imaj alınabilmektedir. Mantıksal bir imaj yöntemi olup silinmiş alan verilerini barındırmaz.
<b>Export (İçerik Çıkarma)</b>	İmaj içerisindeki klasör ve dosyaların okunabilir şekilde (formatta) dışarı aktarılmasıdır.
<b>Hash Değeri</b>	Veri bütünü kontrol etmek için geliştirilmiş tek yönlü şifreleme algoritması olup bir çeşit verinin parmak izidir. Birebir kopya neticesinde cihaz/program tarafından üretilen rakam ve harflerden oluşan 32/40 karakterli güvenlik anahtarıdır. Hash Değeri tüm dünyada

## GİZLİ

	<i>bilgisayar kriminalistiğinde kullanılmakta olup ilgili cihaz üzerindeki bir karakterin bile değişmesi durumunda HASH değeri değişmektedir. (MD5, SHA1, SHA256)</i>
<b>IMEI</b>	<i>IMEI, telefonlara verilen uluslararası bir güvenlik kodu, kimlik numarasıdır. Telefona dair tüm kayıtlar bu numara altında toplanır. IMEI numarası en az 14 karakterli bir numara olmalıdır. Aynı IMEI numarasının 15. karakteri bazı GSM işletmecileri kayıtlarında 0 (sıfır) olarak hazırlarında ise farklı bir numara olarak tutulabilmektedir. Bu nedenle IMEI numaralarına ait dökümler oluşturulurken ilk 14 karakteri uyan kayıtlar dikkate alınmaktadır.</i>
<b>ICCID</b>	<i>ICCID numarası, Türkçe'ye "Entegre Devre Kartı Kimliği" olarak çevirebileceğimiz 20 haneli bir numaradır. ICCID için cihazınıza takılı olan SIM kartın seri numarası diyebiliriz. İlk iki hanesi endüstriyel sektör numarasıdır ve Telekom sektörü için 89 kullanılır. Sonraki iki hane ise ülkenin uluslararası arama kodudur ve Türkiye için 90 kullanılır. Sonraki haneler ise operatörün belirlediği numaralardır.</i>
<b>PIN</b> <b>PUK</b>	<i>SIM kartın yetkisiz erişimin engellemesi amacıyla kullanıcı tarafından ürettiği 4 veya 5 haneli açılış şifresidir. SIM kartın unutulmuş/bilinmeyen PIN kodunu tespit etmek amacıyla geliştirilmiş 8 rakamlı açılış şifresidir.</i>
<b>UTC</b> <i>(Eşgüdümlü Evrensel Zaman)</i>	<i>Atomik olarak hesaplanan ve pek çok ülkede baz alınan bilimsel zaman dilimidir. UTC+0 olarak da kullanılır. Türkiye saat dilimi olarak kış saati (Ekim-Mart ayları arası) uygulamasında UTC+2, yaz saati (Mart-Ekim ayları arası) uygulamasında UTC+3 kullanılmaktadır. Dolayısıyla Türkiye'de kullanılan saat, kış saati uygulamasında UTC+0'dan iki, yaz saati uygulamasında üç saat ileridedir. 08/09/2016 tarihli 29825 sayılı Resmî Gazete' de yayımlanarak yürürlüğe giren 07/09/2016 tarihli 2016/9154 sayılı Bakanlar Kurulu Kararnamesine göre Türkiye'de yaz saati UTC+3 olarak kalıcı hale getirilmiştir. Rapora eklenen bilgi ve belgeler değerlendirilirken bu saat farklılıkları göz önüne alınmalıdır.</i>
<b>Mobil Cihazlarda İmaj (Adli Kopya) Alma Yöntemleri</b>	
<i>Mobil cihazlarda üç farklı şekilde imaj alma, diğer bir ifadeyle adli kopya yapılmaktadır. Bu adli kopya metotları; physical (fiziksel), logical (mantıksal) ve file system (dosya sistemi) şeklindedir.</i>	
<b>Physical (Fiziksel)</b>	<i>Mantıksal ve gelişmiş mantıksal çıkarımlar ile elde edilen mevcut ve gizlenmiş verilerin yanı sıra silinmiş verilerin de çıkarımının gerçekleştiği, cihaz belleğinin tamamının okunduğu çıkarım metodudur.</i>
<b>Logical (Mantıksal)</b>	<i>Cihaz üzerinde mevcut olan, cihazın manuel (el göz yordamıyla) incelendiğinde de görülebilen verilerin çıkarımının yapıldığı metottur.</i>
<b>File system (Dosya Sistemi)</b>	<i>Mantıksal çıkarım ile elde edilen verilerin yanı sıra cihaz üzerinde gizli olarak bulunan, cihazın manuel incelemesinde görülemeyecek dosyaların da çıkarımının yapıldığı metottur. Genellikle silinen verilere ulaşılması mümkün olmamaktadır.</i>
<i>Mobil cihazların incelemesinde silinmiş verilere de ulaşabilmek adına fiziksel imaj alınması daha uygun olmaktadır. Ancak mobil cihaz üreten şirketlerin müşterilerinin kişisel verilerinin güvenliğini sağlamak adına geliştirdikleri donanımsal ve yazılımsal güvenlik sistemleri nedeniyle zaman zaman inceleme yapılan mobil cihazlarda fiziksel imaj alınması mümkün olmamaktadır. Bu durumlarda alternatif (mantıksal ve dosya sistemi) imaj alma metotlarına başvurulmaktadır.</i>	
<i>En iyi içerik çıkarım metodu olan fiziksel imaj yapılmış olsa dahi, geri dönüşümü mümkün olmayacak şekilde silme işlemi (wipe) uygulanmış cihazlarda silme işleminden önceki verilere ulaşılması mümkün olmamaktadır.</i>	



Dijital materyallere yönelik imaj alma ve inceleme süreci aşağıda isimleri belirtilen adli bilişim cihazları ve adli bilişim yazılımları aracılığı ile uluslararası adli bilişim standartlarına uygun olarak tamamlanmıştır.

İmaj Alma Cihazları / Yazılımları	İnceleme Yazılımları
UFED 4PC (7.34.1.23)	UFED Physical Analyzer (7.35.2.16)

Celal Yasin ÖZDEMİR (TC: [REDACTED]) (ŞÜPHELİ)	1	Samsung marka J105F model 356502074438537 IMEI numaralı cep telefonu
	2	4.5G ibarlı 89902860395169119819 ICCID numaralı sim kart
	3	Sandisk marka 8 GB kapasiteli hafıza kartı

#### Anahtar Kelimeler:

İmaj dosyaları içerisindeki veriler incelendiği esnada, imaj dosyaları içerisindeki kayıtlı ve silinmiş veriler içerisinde bulunan video, resim, ses, doküman dosyaları ile e-mailler, internet kayıtları, sıkıştırılmış dosyalar incelenmiş, ayrıca imaj dosyaları içerisinde; " by-lock, bylock, by.lock, bylock++, bylockapp, net.client.by.lock, bylock.net, eagle, al.bts.eagle, cleanthemall, cocovoice, 46.166.16, sohbet-i canan, kakaotalk, cryptnote, falcon, morbeyin, org.herkul, cemaat, fetullah", com.fethullah.gulen, paralel", kripto", maklube, istişare grubu, haramzadeler, başçalan, fuat avni, yıldızkulis, düğüne çağır, köşk, himmet, bağış, mehdi, mesih, muhterem, sıfır olma, dünya imamı, kainat imamı, şakirt, şakirde, üst kurul, serrehber, belletmen, altın nesil, tazir, şefkat tokadı, zecr tokadı, tard olma, ümitçi, hocaefendi, hoca efendi, fethullah gülen, ışık evleri, fetih suresi, fetih okutma, fethetme, müteveli heyeti, müteveli toplantı, hizmet hareketi, hizmet, mahrem yerleri, mahrem hizmet, mahrem imam, takiyye, ikram, tedbir, ibni crkam evler, şarj evler, ağabey, abiler, ablalar, sohbet abisi, irşad ekseni, hizmet erleri, muhabbet fedaisi, adanmış ruh, cemaat zamanı, hususi evler, kutsal hoca payı, sadakat testi, parlatma, mahrem toplantı, beklenen nesil, kutsiler ordusu, gönül erleri, murakıp, talebe, refik, ümileri, mülahaza, firavun, deccal, yezit, tiran, herkul, özgürherkul, herkulnagme, rotahaber, aktifhaber, onyediyirmibes, on7yirmi5, zaman.com.tr, zaman gazetesi, samanyoluhaber, shaber, şubuhaber, haberdar, merkurhaber, küre.tv, yenyön, dünyatv, ırmaktv, sızıntı dergi, yağmur dergi, kimseyokmu, bankasya, bank asya, asya katılım, asyabes, fem dersane, körfez dersane, galebe, liste, pırlanta, dahhak, molla, polis, müdür, adil öksüz, dersane, iaşc, üstad, keyfiyet, müspet, müceddit, hidayet, irtibat, gönül eri, talibsiz dönem, karşı cephe, mansıp, mevki, irşad ufku, irşad ve müşid, hicret, hoşgörü, diyalog, huzur iklimi, kelimetullah, ikinci ilkler, insan-ı kamil, kamil insan, tahşidat, uhuvvet, şeriat, cihat, istişare, meşveret, başyüceler, istişare kurulu, nefis terbiyesi,

tecessüs, akabe, kuvvet dengesi, muvazene, imtihan, arama tarama, tarama mesulü, talebe mesulü, ümit mesulü, izdivaç mesulü, gözclü, serdoktor, gezici, Ergenekon, irticayla mücadele, 28 Şubat, zirve yayınevi, darbe planı, gizli tank, atabeyler, uyuyan hücre, 17/25 Aralık, 15 Temmuz darbe, mit turları, yasa dışı dinleme, kaynak holding, kayyum atama, nur evi, ışık evi, takkiye yapma, karşıt cephe, kalp insanı, ışık eri, ışık süvarisi, yargıcinadalet, nasilyapilir, aibm, ahim, avrupa insan hakları, aiök, avrupa işkenceyi önleme, gaybubet, eğitim danışmanı, pensilvanya, türkçe olimpiyat” kelime ve terim grupları ile aratılarak inceleme işlemi gerçekleştirilmiştir.

### **1- SAMSUNG MARKA J105F MODEL 356502074438537 IMEI NUMARALI CEP TELEFONU:**

Samsung marka J105F model 356502074438537 IMEI numaralı cep telefonun adli kopyasının (imajı) alınmasına yönelik gerekli teknik çalışmalar yapılmış ancak cep telefonun android sistem başlatılabilmesi için konulan Güvenlik kilit şifresi olduğu gözlenmiştir. Yine UFED 4 PC (7.34.1.23) ve diğer adli bilişim yazılımları ile çeşitli yöntemler denenmiş ancak Android sistem başlatma Güvenlik kilit şifresi olması sebebiyle imajın alınması ve incelenmesi mümkün olmamıştır. Cep telefonun da belirli sayıda şifre denemesi yapılması halinde cep telefonun kilitlenebileceği ve sıfırlama riski oluşabileceği değerlendirilmiştir.

Bahse konu cep telefonun android başlatma şifresinin öğrenilerek tarafımıza sunulması halinde gerekli imaj alma ve inceleme işlemlerin yapılabileceği değerlendirilmiştir.

### **2- 4.5G İBARELİ 89902860395169119819 ICCID NUMARALI SİM KART:**

#### **İmaj (Adli Kopya) Alma İşlemi:**

4.5G ibareli 89902860395169119819 ICCID numaralı sim kartın adli kopyası (imajı) UFED 4PC isimli adli bilişim yazılımı aracılığıyla alınmıştır. Alınan imaj iki kopya halinde Sandisk marka “İMAJ-A” ibareli 64 GB kapasiteli usb bellek ve Sandisk marka “İMAJ-B” ibareli 64 GB kapasiteli usb bellek içerisindeki “4.5G\_89902860395169119819\_SimKart” isimli klasör altına kaydedilmiştir.

#### **İnceleme İşlemi:**

4.5G ibareli 89902860395169119819 ICCID numaralı sim kartın alınan imajı UFED Physical Analyzer isimli adli bilişim yazılımı aracılığıyla soruşturma konusu dikkate alınarak incelenmiştir.

➤ Anahtar kelimeler eşliğinde yapılan inceleme sonucunda; soruşturma konusuyla ilgili olabileceği değerlendirilen herhangi bir veriye rastlanılmamıştır.

### **3- SANDİSK MARKA 8 GB KAPASİTELİ HAFIZA KARTI:**

#### **İmaj (Adli Kopya) Alma İşlemi:**

Sandisk marka 8 GB kapasiteli hafıza kartın adli kopyası (imajı) UFED 4PC isimli adli bilişim yazılımı aracılığıyla alınmıştır. Alınan imaj iki kopya halinde Sandisk marka “İMAJ-A” ibareli 64 GB kapasiteli usb bellek ve Sandisk marka “İMAJ-B” ibareli 64 GB kapasiteli usb bellek içerisindeki “Sandisk\_8GB\_HafızaKartı” isimli klasör altına kaydedilmiştir.

**İnceleme İşlemi:**

**Sandisk marka 8 GB kapasiteli hafıza kartın alınan imajı UFED Physical Analyzer isimli adli bilişim yazılım aracılığıyla soruşturma konusu dikkate alınarak incelenmiştir.**

➤ Anahtar kelimeler eşliğinde yapılan inceleme sonucunda; soruşturma konusuyla ilgili olabileceği değerlendirilen **herhangi bir veriye rastlanılmamıştır.**

**Rapor içeriğinde ayrıntılı özellikleri belirtilen dijital materyaller ile ilgili soruşturma konusu dikkate alınarak gerekli imaj (adli kopya) alma ve inceleme işlemleri tamamlanmıştır.**

**1- SAMSUNG MARKA I9190 MODEL 359904059077974 IMEI NUMARALI CEP TELEFONU:**

• İmaj üzerinde yapılan incelemelerde "Google Play" android market üzerinden indirilen uygulamaların bilgilerini tutan "Library.db" isimli veritabanı dosyasında Soruşturma konusu ile alakalı olabileceği değerlendirilen uygulamalara ait tanıtıcı isimler olduğu gözlenmiştir. Bahse konu uygulamaların "**alisafi.turkiye@gmail.com**" mail adresi ile Google Play android marketten indirildiği değerlendirilmiş ancak cep telefonu içerisinde yüklü olmadığı gözlenmiştir. Yani "**alisafi.turkiye@gmail.com**" mail hesabı üzerinden tarafıma tevdi edilen cep telefonu ya da aynı mail ile giriş yapılan başka bir cihaza uygulamaların indirilebileceği değerlendirilmiştir. Ayrıca bahse konu uygulamaların silinmiş olması sebebiyle tarih bilgilerine erişilmesi mümkün olmamıştır.

**2- 4.5G İBARELİ 89902860395169119819 ICCID NUMARALI SİM KART:**

• Anahtar kelimeler eşliğinde yapılan inceleme sonucunda; soruşturma konusuyla ilgili olabileceği değerlendirilen **herhangi bir veriye rastlanılmamıştır.**

**3- SANDISK MARKA 8 GB KAPASİTELİ HAFIZA KARTI:**

• Anahtar kelimeler eşliğinde yapılan inceleme sonucunda; soruşturma konusuyla ilgili olabileceği değerlendirilen **herhangi bir veriye rastlanılmamıştır.**

**Yapılan imaj (adli kopya) alma ve inceleme işlemlerine ait Şube Müdürlüğümüzce herhangi bir yedek tutulmamaktadır.**

  
348795  
Adli Bilişim Görevlisi



## MÜHÜR KAPATMA TUTANAĞI

İstanbul Cumhuriyet Başsavcılığı Terör ve Örgütlü Suçlar Soruşturma Bürosu tarafından 08/11/2017 tarih ve 2017/83967 soruşturma sayılı yazısı ile Şube Müdürlüğümüze gönderilen dijital materyaller ağız mühürlü delil poşetine konularak tarafınıza gönderilmiştir.

SN	DİJİTAL MATERYALLER	MÜHÜR BARKOD NO
1	Samsung marka J105F model 356502074438537 IMEI numaralı cep telefonu	SS20160066889M
2	4.5G ibareli 89902860395169119819 ICCID numaralı sim kart	
3	Sandisk marka 8 GB kapasiteli hafıza kartı	
6	Sandisk marka "İMAJ-A" ibareli 64 GB kapasiteli usb bellek	
7	Sandisk marka "İMAJ-B" ibareli 64 GB kapasiteli USB bellek	

İş bu mühür kapatma tutanağı tarafımızdan tanzimle birlikte imza altına alınmıştır. 20/09/2019  
Saat: 12:15

MÜHRÜ KAPATAN

348795

HAZIRUN

941098