KARAR DESTEK SİSTEMLERİNİN MOBİL CİHAZ ADLİ BİLİŞİMİ SÜREÇLERİNE UYGULANMASINA YÖNELİK BIR ÖNERİ ÇALIŞMASI

Furkan Yılmaz*[1] ve Hüseyin Çakır[2]

[1] Gazi Üniversitesi, Bilişim Enstitüsü Adli Bilişim ABD, Ankara
[2] Gazi Üniversitesi Eğitim Fakültesi Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, Ankara
furkanyilmaz89@hotmail.com, hcakir@gazi.edu.tr

ÖZET

Bu çalışmada, diğer dijital materyal türlerine göre nicelik ve nitelik açıdan daha ön plana çıkan mobil cihaz adli bilişimi üzerinde durulmuştur. Karar destek sistemlerinin mobil cihaz süreçlerine entegresi için iş akışına ilişkin sorular ve kurallar çıkartılmıştır. Türkiye'de adli bilişimde karşılaşılan sorunlar ele alınarak, mobil cihaz adli bilişimi ile ilgilenen personelin karşılaştığı problemlerle ilgili en hızlı, en doğru ve en verimli şekilde karar destek sistemleri aracılığıyla çözüme ulaşmasını sağlayacak bir model önerisi sunulmuştur. Bu model önerisi ile yüksek iş hacmine sahip ve kamu sektöründe ya da özel sektörde faaliyet gösteren adli bilişim laboratuvarlarının mobil cihaz adli bilişimine ilişkin süreçlerini en etkili şekilde hızlandırarak, zaman ve maliyet açısından tasarruf sağlamaları öngörülmektedir. Mobil cihaz adli bilişimi uygulayıcısı olan personele katkı sağlaması, potansiyel riskleri azaltması, süreci hızlandırması ve hukukilik çerçevesinde delil bütünlüğünün korunması beklenmektedir.

Anahtar Kelimeler— adli bilişim, adli bilişim laboratuvarı, karar destek sistemleri, mobil cihazlar, mobil cihaz adli bilişimi

A Proposal Study on the Application of Decision Support Systems to Mobile Forensics Processes

ABSTRACT

In this study, it is presented a model proposal in which the digital forensics applications, which is a method of obtaining evidence that is frequently used in actual criminal investigations, is proposed for law enforcement units to accelerate the process in the most efficient and effective way due to the volume problem; mobile device forensics is emphasized in terms of quantity and quality compared to other types of digital materials. Questions and rules regarding the workflow have been drawn up to integrate decision support systems into mobile forensics processes. By handling the problems in digital forensics in Turkey, a model proposal is presented to the personnel who work in mobile forensics to get the solution in the fastest, most accurate and most efficient way through the decision support systems. With this model proposal, it is foreseen that digital forensics laboratories, which have huge backlog and operate in the public or private sector, will accelerate the processes related to mobile device forensic computing in the most effective way and save time and cost. It is expected to contribute to the mobile forensic personnel, reduce potential risks, accelerate the process and protect the integrity of evidence within the framework of legality.

Keywords— decision support systems, digital forensics, digital forensic laboratory, mobile devices, mobile forensics

I. GİRİŞ (INTRODUCTION)

Çağımızda teknolojinin ve internetin günlük yaşamın vazgeçilmez bir parçası haline gelmesinin sonucunda, kişilerin yaşamlarına ilişkin en önemli bilgiler dijital olarak tutulmaya başlanmıştır. Artık suç soruşturmalarında ve kovuşturmalarında en önemli bulgular, dijital materyallerden elde edilmekte, hatta adli bilişim işlemlerine yetki veren Ceza Muhakemesi Kanunu (CMK) Madde 134'te "…somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması halinde …" ifadesi olmasına ragmen keşif araması haline gelmiş durumdadır. Bununla birlikte sahip olunan dijital veri depolama birimleri çeşitlenmekte niceliksel ve niteliksel büyüme göstermektedir. Bu durumun tabii sonucu olarak bir suç dolayısıyla hakkında soruşturma yapılan şüpheliden elde edilen dijital materyaller: kişisel bilgisayarı, tableti, cep telefonu, sim kat, hafıza kartı, harici harddiski, USB bellek, CD/DVD vb. şeklinde çeşitlenmekte, bunların delil olarak analiz edilmesi gerekmektedir. Doğal olarak her geçen gün artan veri hacimlerinden kaynaklanan ve aynı zamanda çeşitli işletim sistemleri, dosya formatları vb. barındıran artan sayıda ve türdeki kaynakları inceleme ve analiz için standart tekniklerden yoksun olmanın sonucu olarak çeşitli sorunlar meydana gelmektedir [1].

Özellikle cep telefonları gibi mobil cihazların, kişinin sürekli yanında taşıması ve en mahrem anlarına dahi tanıklık ediyor olmasından dolayı diğer dijital materyallere göre suça konu bulguları taşıma ihtimali daha yüksektir.

Bu noktada adli bilişim faaliyetleri devreye girmekte; ancak oluşan bu dijital delil yığını tüm dünyada olduğu gibi (İrlanda Ulusal Polisi tarafından hazırlanan rapora göre dijital materyalin raporlanıp inceleme süresi 4 yılı aşmıştır [2].) Türkiye'de de önemli bir duruma gelmektedir. Hatta Türkiye'de 2018 yılında Kasım ayına kadar incelenen dijital material sayısı yaklaşık 630 bin olmuş, Avrupa kıtasının yıllık inceleme sayısıyla neredeyse denk olması Türkiye'deki durumun ciddiyetini daha da net ortaya koymaktadır [3].

Ayrıca Türkiye'de adli bilişim faaliyetlerine yetki veren temel mevzuat olan CMK'da ilgili madde metni 2005 yılında yürülüğe girmiştir. Her ne kadar madde metninde günümüze kadar bazı ufak değişiklikler yapılmış olsa da, mevcut ihtiyaçları karşılamamakta ve uygulamaya ilişkin bir çok soru işareti barındırmaktadır.

Bu çalışmayla ülkemiz mevzuatı içerisinde gün geçtikçe artan çeşitliliği, hızla değişen teknolojisi, karşılaşma sıklığı ve içinde barındırdığı veriler ile adli bilişim alanında önemli bir zorluk olarak karşımıza çıkan mobil cihazlardan delil elde etme aşamasında karar destek sisteminin uygulanmasına ait pragmatik, yapısal ve disiplinler arası bir yaklaşım ile bir model önerisi oluşturulacaktır.

Kolluk kuvvetleri tarafından uygulanabilecek ulusal bazda mobil cihazlara ilişkin detaylı ve net bir iş akışı bulunmamaktadır. Bu model sayesinde mobil cihaz adli bilişimi ile ilgilenen personelin, en doğru kararı en kısa sürede vermesi ve bunun sonucu olarak maliyet ve zaman tasarrufu sağlanması hedeflenmektedir. Mobil cihaz adli bilişimi uygulayıcısı olan personele katkı sağlaması, potansiyel riskleri azaltması, süreci hızlandırması ve hukukilik çerçevesinde delil bütünlüğünün korunması beklenmektedir.

II. PROBLEM (PROBLEM)

Dijital deliller yapısı gereği çok hassas olduklarından dolayı tüm süreç dikkatle ve belli prosedürlere uyularak icra edilmelidir. Dellilerin karartılması ya da zarar görmesine sebebiyet verecek uygulamalar, adli makamların delillerin reddi kararına yol açmaktadır [4].

Türkiye'de adli bilişim faaliyetleri yürütülürken bazı sorunlarla karşılaşılmaktadır. Farklı sebeplerle ortaya çıkan sorunlar dijital delilin geçerliliği konusunda şüphe uyandıracağından, bu sorunların çözülmesi gerekmektedir. Başlar, bu sorunları; adli bilişim sürecine ilişkin potansiyel riskler, ağ trafiği analizi delillerinin sorunları, mobil cihazlara ilişkin sorunlar, adli bilişim ilke ve standartlarının belirlenememesi, laboratuvarların yetersizlikleri, uygulayıcı eğitimsizliği, hukuka aykırıllk halleri olmak üzere yedi başlık altında saymıştır [5].

Ülkemizde uluslararası standartlara önem verilmektedir; ancak dijital delilin elde ediliş sürecine ilişkin işlemlerin nasıl olacağıyla ilgili düzenlemelerin olmaması, henüz elde ediliş aşamasında geri dönülmeyecek hasarlara zemin hazırlamaktadır [6]. Yapısı gereği hassas olan dijital verilerin, elde edildiği ilk andan itibaren delil zincirinin oluşması gerekmektedir. İmaj alma işlemlerindeki eksiklik, inceleme ve raporlama aşamasında ortaya konan delilleri görlgelemektedir.

Bir diğer problem ise, bilişim sistemlerinin gittikçe artan kapasitelerinin büyüklüğüdür. Şöyle

ki, delil olarak kullanılabilecek veri, elde edilen tüm sistemdeki verinin on binde biri kadar düşük seviyededir. Bu açıdan her türlü verinin değil, sadece yargılama konusu olayla ilgili, faili ve fiili ispat edecek verinin elde edilmesi gerekmektedir [7]. Bu da artan iş yüküne sebep olmakta, oluşan bu yığınları eritebilmek için daha akıcı süreçlerin oluşturulması ihtiyacı doğmaktadır.

Adli bilişim faaliyetini yerine getiren kolluk ve bilirkişilerin yeterince eğitilemesi de adli bilişim süreçleri açısından sorun teşkil etmektedir. Adli bilişim alanında görev alan personel, her bir dijital delilin farklılıklarını bilmesi gerekir [8]. Ayrıca bu personel, bilişim sistemleriyle ilgili ileri düzey bilgiye sahip, bunu koruyacak şekilde teknolojiyi takip eden ve gerekli hukuki bilgiyi haiz olmaları gerekmektedir [9]. Uzman personel eksikliği neticesinde veri elde etme imkanının olmadığı, manyetik alan etkisinden soyutlanmadan taşındığı, veri bütünlüğünü korumaya yönelik tedbirler alınmadan işlemlerin yapıldığı görülmektedir [10]. Gelinen noktada kolluk birimlerinde dahi adli bilişim personeli sayısı binlere ulaşmışken, bu sayıda personeli aynı nitelikte eğitmek ve aynı nitelikte iş ve işlemleri icra etmesini sağlamak da diğer bir problemdir.

Çeşitliliği gün geçtikçe artan mobil cihazlarla ilgili olarak, mobil cihaz adli bilişim süreçlerinde veri çıkarımına ilişşkin standardizasyon eksikliği görülmektedir [11]. Ayrıca mobil cihazlardaki ve mobil işletim sistemlerindeki çeşitlilik kesinlik barındıran bir standartlaşmanın önündeki en büyük engeldir. Mobil cihazlardan en fazlaya veriyi elde etme yöntemi olan fiziksel imaj alma işlemine ilişkin uygulanan teknikler pahalı, çok fazla teknik bilgiyle zaman istemektedir [11].

Ceza muhakemesi hukuku kapsamında yapılan adli bilişim faaliyetleri özünde temel hak ve özgürlüklere müdahale niteliği taşıdığından, yapılan işlemlerin hukukiliği önem arz etmektedir. Teknik açıdan ne kadar mükemmel bir çalışma ortaya konsa da, hukukiliğindeki problem elde edilen veriyi delil hukuku açısından geçersiz kılınmasına sebep olacaktır. Ceza Muhakemesi Kanunu Madde 134, adli bilişim faaliyetleri açısından temel mevzuat uygulamayla ilgili bir çok boşluğu barındırmakta ve uygulayıcılar bu alanları nasıl doldurcağı konusunda yeterli bilgiye sahip değillerdir.

III. SINIRLILIKLAR (LIMITATIONS)

Mobil cihazlar yapısı gereği çok çeşitlidir. Bu çeşitlilik adli bilişim uygulamalarını olumsuz etkilemektedir. Üretici firmaların, işletim sistemlerinin, kullanılan donanımlar ve hafıza çiplerinin çeşitlenmesi, adli bilişim için standart uygulama oluşturmayı zorlaştırmaktadır. Hatta piyasadaki bazı cihazların herhangi bir adli bilişim yazılımıyla dahi desteklenmediği görülmektedir.

Mobil cihaz adli bilişiminin amacı veriye ulaşmak iken, üretici firmaların veriyi cihazda kriptolu olarak tutma eğiliminde oldukları bilinmektedir. Bu da mobil cihaz adli bilişiminde fiziksel imaj almak için kullanılan bazı yöntemleri işlevsiz kılmaktadır.

İlk müdahale süreçleri ele alınırken, olay yerinin mobil cihaz dışındaki unsurları göz ardı edilmiştir. Olay yerleri için karşılacak senaryoların ve uyulacak prosedürler çalışma kapsamı dışında tutularak, mobil cihazlar için uygulanması gereken adımlara odaklanılmıştır.

Mobil cihaz adli bilişimi için ilk müdahale ve imaj alma aşamalarından sonra inceleme ve raporlama aşamaları gelmektedir. Ancak bu çalışmada başarılı şekilde imaj almak için bir model oluşturulduğundan, bu aşama sonrası yapılması gerekenler de çalışma kapsamı dışında tutulmuştur.

Personelin, modelde bahse konu işlemleri de nasıl uygulayacağını biliyor olması gerekmektedir. İşlemi yapacak mobil cihaz adli bilişimi uygulayıcısının konudaki bilgi eksiliğine ragmen işlem yapma ihtimali ve bu işlemler sonucunda delililn zarar görmesi ihtimali göz ardı edilmiştir

Mobil cihazların imajının alınabilmesi için gerekli olan yazılım, donanım ve uzmanlık konusunda çokça seçenek mevcuttur. Hatta uygulanabilecek yöntemler için teknolojik açıdan bir sınır koymanın da mümkün olmadığı değerlendirilmektedir. Bu sebeple modelin başarılı şekilde işlemesi için gerekli olan yazılım, donanum ve uzmanlık için Türkiye'de adli bilişim faaliyeti yürüten bir kolluk biriminin haiz olduğu kaynaklar esas alınmıştır.

IV. ADLİ BİLİŞİM (DIGITAL FORENSICS)

Digital Forensics Research Workshop (DFRWS), adli bilişimi suç teşkil ettiği tespit edilen olayların yeniden canlandırılmasını kolaylaştırmak veya ilerletmek veya planlanan operasyonları aksattığı görülen yetkisiz eylemlerin tahmin edilmesine yardım etmek amacıyla dijital kaynaklardan elde edilen dijital delillerin korunması, toplanması, doğrulanması, tanımlanması, analizi, yorumlanması, dokümantasyonu ve sunumuna

yönelik bilimsel olarak türetilmiş ve kanıtlanmış yöntemlerin kullanılması olarak tanımlamaktadır [12]. Literatür'de de adli bilişime için bir çok tanım bulunmaktadır.

"Adli Bilişim, bilişim sistemleri ve üzerinde bulunan depolama ünitelerinin, herhangi bir suçu işlemede veya yasaklanmış bir faliyette kullanılıp kullanılmadığını tespit etmek amacıyla yapılan çalışmaların tümüdür." [13].

"Adli Bilişim (Computer Forensics – Bilgisayar Kriminalistiği) bilimi; suçun aydınlatılabilmesi için bilimsel metotlar kullanılarak, çeşitli varyasyonlardaki dijital medyalar üzerinde bulunan, suçla ilgili dijital delillerin bozulmadan ve zarar görmeden anlaşılabilir bir şekilde adalet önüne sunulmaya hazır hale getirilmesini sağlayan ve başlı başına bilimsel teknik prensiplerin uygulandığı bir delil inceleme sürecinin bütünüdür" [14].

"Adli Bilişim en basit tanımıyla, bir yargılama esnasında kullanılabilecek potansiyel delillerin belirlenmesi için bilgisayar araştırma ve analiz tekniklerinin kullanılmasıdır. Bilgisayardaki verilerin korunması, tanılanması, çıkarılması, dökümü ve yorumunu içerir ancak bunun yanında hukuki kurallar, süreçler, delillerin bütünlüğü gibi konulara da riayet ederek bulunan veriler hakkında rapor yazılmasını da kapsar" [15].

"Adli Bilişim, bilişim sistemlerine iletilen, işlenen ve/veya depolanan dijital verinin adli talimat üzerine elde edilerek bulgu olarak tespit edilmesinden, raporlanarak delil olarak değerlendirilmesi amacıyla mahkemeye sunulmasına kadar geçen süreçte delil zinciri her aşamada uygulanarak gerçekleştirilen multidisipliner (çoklu disipinli) ve interdisipiliner (disiplinler arası) halde işletilen teknik ve hukuki adımlar ile işlemler bütünüdür [16].

Her türlü veri depolayan, ileten veya işleyen bilişim sistemleri üzerinde, yazılım veya donanım kullanılarak verilerin ortaya çıkartılması, kurtarılması, analiz edilmesi ve ilgili makamlara sunulması amacıyla yürütülen ilk müdahale, muhafaza, adli kopya alma, inceleme, raporlama ve benzeri faaliyetlerin her biri veya bütünü olarak tanımlanabilir.

Adli soruşturmalarda bu faaliyetlere yetki veren temel mevzuat soruşturmalarla sınırlı olmak üzere Ceza Muhakemesi Kanununun 134. maddesidir. Başlığındaki "bilgisayar, bilgisayar programları ve kütükleri" ifadesinin mobil cihazları karşılayıp karşılamadığı bile zamanında tartışma konusu olmuş olan bu maddeyi uygulayanlar çok iyi bilirler ki; adli bilişim faaliyetlerinin uygulanmasına ilişkin ihtiyaçları karşılamamaktadır.

V. MOBİL CİHAZ ADLİ BİLİŞİMİ (MOBILE FORENSICS)

Adli bilişim bazı alt dallara ayrılmaktadır. Bunlar temelde dört ana başlık altında toplamak mümkündür. Bunlar bilgisayar adli bilişimi (computer forensics), mobil cihaz adli bilişimi (mobile forensics), ağ adli bilişimi (network forensics) ve bulut adli bilişimidir (cloud forensics) [17].

Telefon, tablet, gps cihazları gibi elde kullanılması mümkün olan son kullanıcı düzeyindeki bilgisayar sistemleri olarak tanımlayabileceğimiz mobil cihazlardan yazılım veya donanım kullanılarak içindeki verilerin ortaya çıkartılması, kurtarılması, analiz edilmesi ve ilgili makamlara sunulması amacıyla yürütülen ilk müdahale, muhafaza, adli kopya alma, inceleme, raporlama ve benzeri faaliyetlerdir.

Mobil cihazlar üzerinde adli bilişime konu olabilecek donanım bileşenleri, öncelikle verinin depolandığı donanımlardır. Bunlar hafıza çipi, hafıza kartı ve sim karttır. Somut olayın konusuna göre wi-fi, bluetooth gibi kablosuz bağlantılar da delil kaynağı haline gelebilir [18].

Mobil cihazlar kişilere ait arama kayıtları, mesajlar, e-postalar, resimler, videolar, müzikler, ses dosyaları, sosyal medya hesapları, yüklü uygulamalar, konumlar, dökümanlar, wi-fi bağlantıları gibi hassas bilgileri barındırmaktadır.

5.1. Cihaza İlk Müdahale

Suça konu cihaz muhafaza altına alınmadan önce Ceza Muhakemesi Kanununu Madde 134 uyarınca hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından verilmiş kararın varlığı teyit edilmelidir.

Muhafaza altına alınan cihazın, ilk önce marka, model, imei numarası gibi ayırt edici özellikleri ve kim tarafından kullanıldığı bilgisiyle beraber not alınır. Buna müteakip fiziksel bir hasarının olup olmadığı ve cihazın açık olup olmadığı kontrol edilir.

Cihaz açıksa kapatılmaz ve şifreli olup olmadığı teyit edilir, şifreli ise olay yerinde temin cihetine gidilir. Ayrıca cihazın dış bağlantılarını kesmek için faraday çantası kullanılır ya da uçak moduna alınır. Cihazda bulunan sim kart ve hafıza kartı gibi aparatların da marka, operatör, seri numarası,

ICCID gibi ayırt edici özellikleriyle beraber tespiti yapılır. Cihaz ve aparatlarıyla beraber fotoğrafı çekilir. Eğer dıştan görünen fiziksel arızası varsa, fotoğraflar arızanın belli olacağı şekilde de çekilir.

5.2. İmaj Alma

Dijital delil niteliğindeki bir veri depolama biriminin veya dosya içeriğinin veri bütünlüğü korunarak, adli bilişim yöntemleriyle bire bir (bit-to-bit) kopyalanması işlemidir. Veriyi elde etmek için uygulanan yöntemler gerektirdiği teknik bilgi ve maliyet açısından sınıflandırmaya Şekil 1'deki gibi tutulmaktadır [19].

Şekil 1. Mobil Cihaz Adli Bilişimi Araçları Sınıfladırması [19]

5.2.1. Manuel İnceleme

Kullanıcı arayüzü kullanılarak ulaşılan bilgilerin kaydedilmesi sürecini içerir [19]. Bu yöntem adli bilişim araçları arasında en az teknik bilgi gereksinimi olan yöntemdir. Cihazın çalışıyor olması ve şifresiz, şifresi biliniyor ya da şifresinin bir şekilde aşılmış olması gerekmektedir. Her ne kadar en temel ve en sınırlı yöntem gibi gözükse de bazı adli bilişim yazılımlarının anlamlandırmadığı uygulamaların veritabanlarına erişme imkanı sağlamaktadır.

5.2.2. Mantıksal imaj alma

Bir çok mobil cihaz adli bilişimi yazılımının sunduğu en fazla sayıda mobil cihazı destekleyen hızlı bir ayıklama yöntemidir. Orta düzey teknik bilgiyle ve temel düzeyde bir eğitimle mantıksal çıkarım yapmak mümkündür [19]. Bir kaynak cihazdan ayıklanabilecek veri türleri olan arama kayıtları, telefon defteri, SMS'ler, takvim etkinlikleri, çoklu ortam dosyaları (resimler, videolar, ses dosyaları) ve uygulama verileri gibi verilerinin elde edilmesidir. Çoğu durumda, kilitli cihazlar için mantıksal ayıklama mümkün değildir.

Mantıksal seviyede veri elde etmenin literatürde dosya sistemli çıkarım (file-system extraction) olarak da geçen yöntemle alınacak bir imajda, mantıksal bir uzantı ile görünmeyecek gizli sistem dosyalarına da erişilebilmektedir. Sistemde yüklü bulunan ya da kullanıcı tarafından sonradan yüklenen uygulamaların çoğu bu yöntemle ayıklanan veritabanı dosyalarında saklanmaktadır. Parolalara, uygulama verilerine, telefon defteri girdilerine, arama kayıtlarına, mesajlara ve kullanıcıya tahsis edilmiş alanlardaki verilere ulaşılabildiğinden, cihazın yedeğini alma (backup) işlemi niteliğinde olarak değerlendirilmektedir.

5.2.3. Fiziksel imaj alma

En geniş ve kapsamlı ayıklama yöntemidir. Mobil cihazın hafıza çipinin kart üzerindeyken verisinin elde edilmesini kapsayan ve ileri düzey uzmanlık gerektiren yöntemdir [19]. Ayrılmış alan dahil olmak üzere mobil cihaz üzerinde "bit to bit" yöntemi ile binary seviyesinde veriye erişilmesidir. Raw formatta alınan bu imaj sayesinde silinmiş alandaki verilere de ulaşılabilmektedir. Alınan veri binary yapıda olduğundan dolayı, maliyeti ne kadar düşük olsa da gerektirdiği uzmanlık düzeyi yüksektir [20].

Ancak her ne kadar maliyetinin düşük olduğu düşünülse de, veriyi elde etmek mobil cihazların marka, model hafıza çipi gibi bileşenlerinin çeşitliliğinden dolayı geniş ar-ge ihtiyacı oluştumaktadır. Veriyi anlamlandırma konusunda da benzer şekilde kullanılan mobil uygulamaların farklı yazılım dilleriyle, farklı veri tabanlarını kullanması ya da farklı algoritmalar kullanmasından dolayı çeşitliliği benzer bir zorluk olarak karşımıza çıkmaktadır. Teoride uzmanın veriyi fiziksel düzeyde elde edip anlamlandırsa dahi, mobil cihazların günümüzde geldiği noktadan dolayı pratikte lisanslı mobil cihaz yazılımı olmazsa olmaz haline gelmiştir.

5.2.4. Chip-off

Adli bilişimde uygulamada son seçenek olarak kullanılan yöntemlerden biridir. Kart üzerindeki kalıcı veri tutan hafıza çipinin sökülerek, özel donanımlarla iletişim kurulması ve binary düzeyinde veriye ulaşılmasıdır. Bu yöntemle cihazda bütünsel olarak neler olup bittiğinin daha iyi bir resmini verir [21]. Ancak yeni gelişen teknoloji ile yeni model Android işletim sistemine sahip cihazlarda veriler cihazın kendisine ait bir şifreleme algoritması ile tutulduğundan dolayı anlamlandırma konusunda sıkıntılar yaşanmaktadır. Aynı şekilde iOS işletim sistemine

sahip cihazlar da veriler şifreli tutulduğu için chip-off işleminde başarılı sonuçlar elde edilememektedir. Bu yöntemin diğer bir zorluğu da bellek çipinin, kontrollerdan ayrı çipler olması durumunda, hafıza çipindeki verinin decrypt (şifresinin çözülmesi) edilemesidir.

5.2.5. Mikro düzeyde okuma

Mikro düzeyde okuma yöntemleri, yüksek güçlü mikroskop vasıtasıyla çipte bulunan fiziksel kapıların durumunu görüntülemek için kullanılmasıdır [19]. Bu görüntüleme neticesinde 0 ve 1'lere dönüştürülerek, tüm veri çipindeki her bir bitin çıkartılması amaçlanmaktadır. Bu bitleri bir araya getirerek dosya sistemine, dosyaların üstverilerine ve veri alanlarına erişilmesi hedeflenmektedir. Piyasada bulunabilecek en düşük kapasiteli telefonun 32 GB olduğunu düşünürsek, tüm bitlerin okunması için bu işlemin 270 milyar kez yapılması gerekmektedir. Bu sebeple gerektirdiği donanımlar ve emek açısından en pahalı yöntemdir. Dünyada bu yöntemin uygulandığı laboratuvarların olduğu bilinmektedir; ancak Türkiye'de uygulandığına ilişkin bir veri bulunmamaktadır.

5.3. Kullanılan Yöntemler

5.3.1. Kullanılan yazilimlar

Mobil cihaz adli bilişiminde dünya genelinde sıklıkla kullanılan yazılımlar aşağıda belirtilmiştir [22].

XRY: 1984 yılından beri İsveç'te bulunan MSAB firmasına ait mobil cihaz incelemelerinde kullanan dünya genelinde kabul görmüş bir çözümdür. Dronelar da dahil olmak üzere yaklaşık 25.000 farklı cihazı destekleyen XRY yazılımı, MTK, Spreadtrum, Coolsand & Infineon gibi Çin menşeili telefonlarda kullanılan çip setler için uygun çözümlerden biridir. Literatürde XRY ismiyle genel olarak anlamlandırılmasına rağmen bu ürün XRY ve XAMN olarak iki farklı fonksiyona sahiptir. XRY yazılımı cihazdan verinin çıkartılmasında; XAMN ise çıkartılan verinin analiz edilmesinde kullanılan yazılımdır. Mobil cihaz adli bilişiminde önemli olan cihazlardan verinin elde edilmesi süreci olduğu için bu firmanın XRY ürünün ön plana çıkması da kaçınılmazdır. Ayrıca Türkçe dil desteğini bulunması Türk adli bilişim incelemecileri için tercih sebebidir [23].

UFED: 1999 yılında İsrail'de kurulan Cellebrite şirketinin en bilinen mobil cihaz inceleme ve imaj alma yazılımı olan UFED, dünya çapında da kullanılan bir yazılımdır. 2018 yılında Forensic 4:Cast tarafından verilen "En iyi mobil adli bilişim donanımı" ödülünü UFED Touch2 ile, "En iyi mobil adli bilişim yazılımı" ödülünü ise UFED 4PC ve UFED Physical Analyzer (PA) ürünleri ile kazanmıştır [24].

UFED Touch ürünü sahada bu yazılımı kullanmamıza imkân veren bir donanımdır. Bu sayede olay yerinde imaj alma ve çıkarım yapma imkânı sunan bu cihazla arama kayıtları, resim, video gibi soruşturma açısından önem arz eden verilere anında ulaşma imkânınız olacaktır.

UFED 4PC ürünü ise kullanılan özel kitlerle mobil cihazların normal bilgisayarlar vasıtasıyla imajının alınmasını sağlarken; UFED PA ürünü ise alınan imajın anlamlandırılması ve incelenmesi için kullanılan ürünüdür.

Magnet Axiom: 2009 Yılında Kurulan Magnet Forensics firmasının ürünü olan Axiom, ilk olarak piyasaya IEF (Internet Evidence Finder) olarak çıkmıştır. İnternet kalıntılarını analiz etme konusundaki başarısı ile oldukça popüler hale gelmiş ve daha kapsamlı olan Axiom ürününü 2016 yılında piyasaya sürmüştür. Axiom hem bilgisayarlarda hem de mobil cihazlarda analiz imkanı sağlamaktadır.

Axiom, gelişmiş kazıma ve üçüncü parti uygulamalar için kapsamlı desteği sayesinde daha fazla silinmiş, kodlanmış ve şifreli veriye ulaşılmaktadır. Öte yandan diğer mobil adli bilişim yazılım kitleri ile chip-off ve J-tag gibi yöntemlerle alınan imajları desteklemektedir.

Magnet Acquire isimli aracıyla da mobil cihazların imajları alınabilmektedir. Ayrıca bu alınan imajlar Cellebrite'ın UFED ürünüyle ve Guidance Software'in Encase ürünüyle de analiz edilebilmektedir [25].

Oxygen Forensic Detective: Oxygen Software şirketi, 2000 yılında bilgisayardan mobil telekomünikasyona yazılım şirketi olarak kurulmuştur. Rus menşeili bu şirketin merkezi Amerika Birleşik Devletleri'ndedir.

Diğer mobil adli bilişim yazılımlarından farklı olarak, Jet-Imager ismini verdikleri modülle Android cihazlar için en hızlı fiziksel çıkarım seçeneğini sunmaktadır. %25'e varan süre avantajı sağlayan bu yöntem ile 16 GB bir telefonun imajı 5 ila 7 dakika arası sürmektedir. Ayrıca LG cihazlara özel olarak, bazı modellerinde tek klik ile ekran kilidini aşma özelliğini desteklemektedir. Bunun için ilave kablo veya araca ihtiyaç duymayan yöntem,

sadece standart USB kablosuna ihtiyaç duymaktadır. Hem Android hem de iOS işletim sistemine sahip cihazlar için, yüklü olan casus yazılımları tespit eden Oxygen Forensic Detective, casus yaılımların log ve konfigürasyon dosyalarını prosesleme imkanın sahiptir. Bu sayede konfigürasyon verisi, kullanılan servisler, uygulamanın kullanıcı adı, data transferinde kullanılan cell ID gibi bilgilere ulaşabilmektedir [26].

Paraben: 2001 yılından beri Amerika Birleşik Devletleri Merkezli bu firma, mobil cihazlar, akıllı telefonlar, bilgisayarlar, eposta, oyun sistemleri ve bulut adli bilişimi üzerine çözümler üretmektedir. Mobil cihaz adli bilişimi ile ilgili E3:DS ürünü bulunmaktadır. E3:DS ürünü, mantıksal imaj alma, fiziksel imaj alma, Çin menşeili cihaz desteği, bulut desteği, veri analizi, uygulama anlamlandırması ve kilitli cihazların kilidini aşma özelliklerine sahiptir [27].

Mobiledit: 1991 yılında kurulan Compelson firması, mobil cihaz adli bilişimi ile ilgili çalışmalarına 1996 yılında başlamıştır. 20 yılı aşkın süredir bu alanda kolluk kuvvetlerine, askeri kuvvetlere ve soruşturmalara destek olmaktadır. MOBILedit Forensic, MOBILedit Forensic Express, Sim Cloning Tool ve Camera Ballistics, ürünlerine sahip olan MOBILedit, mobil cihazlarda kullanılan yazılımları veri çıkarımı yapma, rehber, mesajlar, takvim, hatırlatıcılar, notlar, şifreler, uygulama verileri gibi birçok bilgiye ulaşılmasını sağlamaktadır [28].

Blackbag: Blackbag Technologies firması adli bilişim alanında Apple cihazlarına ilişkin sunduğu çözümlerle öne çıkmaktadır. Bu firmanın mobil cihaz adli bilişimi üzerine olan araçları, Blacklight ve Mobilyzedir. Blacklight hem Mac hem de Windows işletim sistemleri üzerinde çalışan kapsamlı incelemeyi sağlayan bir yazılımdır. Bu yazılımlar Windows, iOS ve Android işletim sistemine sahip cihazlardan bilinen internet kalıntıları, backup dosyaları gibi veri yapıları, sanal imajlar ve Windows registry dosyaları gibi verileri analiz edebilmektedir [29]. Mobilyze aracı ise, iOS ve Android cihazlarından imaj alma, triyaj yapma ve raporlama özelliklerine sahiptir.

Andriller: Andriller yazılımı Android cihazların şifrelerini aşmasıyla ön plana çıkmış bir mobil cihaz inceleme yazılımıdır. Mobil cihazlardan veri çıkarımı yapabilmekte, bunu yaparken bazen root işlemiyle bazen de root işlemi olmaksızın veriyi çıkartabilmektedir. Ayrıca Whatsapp uygulamasının kriptolu veritabanlarını aşabilmekte, Android backup dosyalarını çıkartabilmektedir [30].

Katana Forensics: Birleşik Devletler menşeili Katana Forensics firmasının mobil cihaz adli bilişimi ile ilgili ürünleri bulunmaktadır. Bunlar Lantern Triage ve Lantern 4'tür. Lantern Triage, mobil cihazlar için bir triyaj yazılımı olup, olay yerinde veri çıkarımı fonksiyonu vardır. Adnroid ve iOS işletim sistemli cihazlarından çıkarım özelliği sayesinde dosya sistemleri, mesajlar, bulut verisi, harita verisi, geolokasyon verileri ile çağrı kayıtları gibi bilgileri sunmaktadır. Lantern 4 ürünü ise mobil cihazlar için bir imaj alma ve analiz yazılımıdır. iOS ve Android cihazlarda mantıksal, iOS cihazlarda fiziksel çıkarım özelliklerine sahiptir. Dosya sistemi, dosya imza bilgisi, anahtar kelime araması gibi özelliklere de sahip olan bu yazılım Mac cihazlarda çalışabilmektedir [31].

5.3.2. Teknik yöntemler

Mobil cihaz adli bilişiminde bazı zorluklarla karşılaşılmaktadır. Veriye normal yöntemlerle ulaşılamama sorununu gündeme getirmektedir. Bu verinin normal yöntemlerle elde edilememesi fiziksel müdahaleyi de gerekli kılan Chip-off, JTAG, rooting ve jailbreak gibi ileri düzey teknik yöntemlerin uygulanmasını gerektirmektedir" [16].

Cihazlarla yukarıda sayılan araçlarla iletişim kurulamaması halinde, cihaza bazı teknik müdahalelerin yapılması gerekebilir. Sıklıkla yapılan teknik müdahaleler aşağıdaki gibidir.

Tamir: Cihaz ile arıza sebebiyle iletişim kurulamadığı durumlarda, teknik müdahalelerle ile cihazın arızasının tespiti, onarılması, eski haline getirilmesi süreçleridir. Bu yöntem diğer yöntemlere göre daha az maliyetli ve veri güvenliği açısından daha az risklidir.

Chip-off: Kart üzerindeki kalıcı veri tutan hafıza çipinin sökülerek binary düzeyinde veriye ulaşılmasıdır. Yöntem olarak çipi karta bağlayan bacakları ısıtılarak, kart ile bağlantısı kesilmektedir. Sökülen çipin pin-outu çıkartılarak ve veri yolları temizlenerek uygun apparat vasıtsaıyla bilgisayara gösterilmektedir. Bu şekilde fiziksel imaj alınmış olmaktadır. Ancak yeni gelişen teknoloji ile Apple cihazlardan sonra, Android işletim sistemine sahip cihazlarda veriler cihazın kendisine ait bir şifreleme algoritması ile tutulduğundan dolayı anlamlandırma problemleri chip-off yönteminin etkinliğini azalmıştır. Hafıza çipinin, kontrollerdan ayrı durumda board

üzerinde olması da, chip-off'u etkileyen bir diğer unsurdur.

J-tag: (Joint Test Action Group) İşlemcilerin kart üzerinden sökülmeden, kart üzerindeki j-tag pinleri üzerinde lehimleme işlemi yapılarak veriye erişilmesi işlemidir. Adli bilişim standartlarına uygun olarak Android cihazlarda anakart üzerinden test uçlarına lehimlemeler yapılarak j-tag işlemi yapılmaktadır. Fakat yeni gelişen teknoloji ile yeni model Android işletim sistemine sahip cihazlarda veriler cihazın kendisine ait bir şifreleme algoritması ile tutulduğundan dolayı anlamlandırma konusunda sıkıntılar yaşanmaktadır. Bunlar dışında diğer Android cihazlarda anakart üzerinde yol kopukluğu vb. gibi fiziksel bir arıza olmaması durumlarında cihazın anakartı üzerine lehimlemeler yapılarak veri alışverişi mümkün olabilmektedir.

ISP: (in system programming) çipin sisteme kurmadan önce programlanmasını gerektirmek yerine, bazı programlanabilir mantık aygıtlarının, mikro denetleyicilerin ve diğer gömülü aygıtların tam bir sistemde kurulurken programlanabilmesidir. Yeni model ufs çip diye tabir ettiğimiz çiplerde j-tag işlemini desteklemediği onun yerine ISP yönteminin kullanıldığı bilinmektedir

Root: Telefon, tablet gibi Android cihazların verisine ulaşmak için kök klasörüne erişim sağlanması işlemidir.

VI. KARAR DESTEK SISTEMI (DECISION SUPPORT SYSTEMS-DSS)

Karar destek kavramı ilk olarak Carnegie Teknoloji Enstitüsü'nde 1950'li yıllarda gerçekleştirilen teorik organizasyonel karar verme çalışmaları ve Massachusetts Institute of Technology (MIT) tarafından 1960'lı yıllarda etkileşimli bilgisayar sistemlerinde gerçekleştirilen çalışmalar sonucunda ortaya çıktığı bilinmektedir [32].

Gorry ve Scott Morton'a göre ise karar destek sistemi bireylerin enteklektüel kaynakları ile bilgisayarların karar iyileştirme yeteneklerini birleştiren ve yarı-yapısal problemlerle ilgilenen yönetim düzeyindeki karar alması gerekenler için bilgisayara tabanlı olarak destek sağlayan sistemler olarak vurgulanmıştır [33].

Karar destek sistemleri için yapılan en genel tanımlardan biri Gökçen tarafından "yönetici konumundaki karar vericilerin karar vermelerinde yardımcı olan sistemlerdir. Diğer bir deyişle, verilmesi gereken kararlarla ilgili veriyi daha iyi anlayarak, daha etkin karar seçeneklerini oluşturma, alternatifleri belirleme ve değerlendirme işlevlerinde destek sağlayan ve doğru karar verme olasılığını artıran sistemlerdir" şeklinde yapılmıştır [34].

Karar destek sistemleri genel olarak karar verici uzman kişilerin kararlarını vermede daha etkin ve verimli olmalarını sağlamak amacıyla geliştirilmiş olan bilgisayar destekli araçlar veya yazılımlar olarak tanımlanabilir [35].

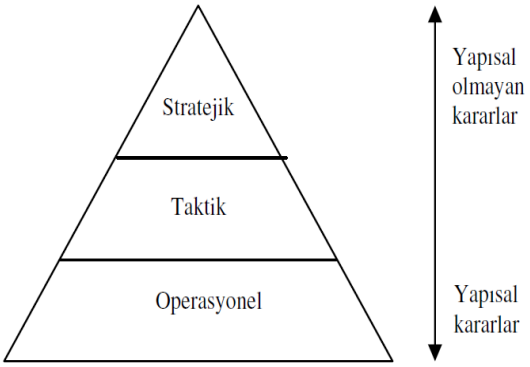
Karar Destek Sisteminde; "Karar" kelimesi, problem çözümünü; "Destek", karar verme sürecinde, bilgisayar ve yazılım teknolojileri kullanımıyla karar vericilerin desteklenmesini; "Sistem"; insan-makine arasındaki etkileşim ve bunun dizayn ve tanımlanmasını ifade etmektedir [32].

Tüm organizasyonların faaliyetinde sıklıkla kapsamlı veya basit kararlar alması gerekmektedir. Bunlar yatırım yapma-yapmama, kapasite artırma-azaltma, işçi alma-çıkarma, çalışma saatlerini artırma, ürün yelpazesini artırma-azaltma, üretim teknolojilerini değiştirme-değiştirmeme gibi faaliyetleri içerir. Bu kararları vermek her zaman kolay değildir ve bu kararlardan sonra her zaman doğru sonuçlar elde edilmeyebilir [36].

Karar verme süreci, stratejik, taktik ve operasyonel seviyelerde olabilir. Bunlar karar verecek yöneticinin seviyesine göre şekillenir. Yöneticilerin seviyelerine ve problemlerin niteliğine göre yapısal, yarı-yapısal ve yapısal olmayan kararlar şeklindedir. Şekil 1'de gösterildiği üzere yönetim seviyelerine göre karar tipleri alt kademeye doğru indikçe yapısal olmayandan yapısala doğru bir geçiş olmaktadır [37].

Karar destek sistemleri kullanılırken sıklıkla kullanılan algoritmalar aşağıdaki şekilde sıralanabilir [38]:

- Genetik Algoritmalar
- Doğrusal Programlama
- Yapay Sinir Ağları (YSA)
- Uzman Sistemler (US)
- Bulanık Önermeler mantığı
- Zaman Serileri
- Bayes Algoritması
- Analitik Hiyerarşi Prosesi (AHP)



Şekil 2. Yönetim Seviyelerinde Karar Tipleri [37]

Mobil cihaz adli bilişiminde karar destek sisteminin uygulanması bir uzmandan alınan bilgilerin karmaşık problemi çözmek için kullanılması mahiyetinde olacağı için yukarıda sayılan algoritmalardan uzman sistemler kullanılması daha uygun olmaktadır.

VII. MOBİL CİHAZ ADLİ BİLİŞİMİ VE KARAR DESTEK SİSTEMLERİ (MOBILE FORENSICS AND DSS)

Adli inceleme yapan tüm uzmanlar, kendilerini bekleyen artan iş yığını, büyük miktarda delil ve veri yığını problemiyle karşı karşıyadır [39]. Mobil cihaz adli bilişimi sürecinde, uzman sistemler yaklaşımıyla yapısal kararların ele alınması hedeflenmektedir. Yapısal kararlar, tanımlanmış kararlar olarak da belirtilebilirler. Yapısal kararlarda, sorunların çok iyi tanımlanmasının yanında, belirlilik seviyesi yüksek olması ve karar verici için öznel bir esneklik söz konusu değildir. Bu tip kararlar için bireyden bağımsız bilgisayar tarafından da alınabilen kararlar denilebilir [37]. Bu sayede ileri derece uzmanlık ve tecrübe isteyen bu süreçlerin uzman sistemler yardımıyla, bu süreçte yeni başlamış olan adli bilişim personelleri için hem karar alma süreçlerini hızlandırması hem de en doğru karara hata yapmadan ulaşması hedeflenmektedir.

Literatürde, adli bilişim iş akışına ilişkin kural koyma çalışmaları yapılmıştır. Effiong, çalışmasında adli bilişime ilişkin bütün süreci ele alan bir yapı ortaya koymuştur. Süreçler adım adım ele alınmıştır. Bu çalışmada bilgisayarlar üzerin yoğunlaşılmış ve adımlar genel nitelkikte olup daha yüzeysel olduğu görülmüştür [12].

Mobil cihazlar üzerine Faheem vd. tarafından yapılan çalışmada mobil cihaz adli bilişimi koruma, elde etme, inceleme, analiz ve raporlama olarak beş adımda ele elınmıştır. Bu adımlar daha genel nitelikte olup, doğrudan uygulayıcı için yol gösterici olarak görülmesi mümkün olmamaktadır. Ayrıca bu çalışma da mobil cihaz adli bilişiminde very çıkarımına ilişkin standardizasyon eksikliği ve mobil cihazlardan veriyi elde etmeye yönelik tekniklerin zorluğu ile maddi ve zaman yönünden maliyeti de vurgulanmıştır. Bu çalışmada mobil bulut verileri üzerine de yoğunlaşılmış; ancak mobil cihaz adli bilişimine ilişkin adımlar genel nitelikte kalmış ve mobil cihaz adli bilişiminde uygulamadli alt düzey problemler göz ardı edilmiştir [11].

Al Mutawa vd., tarafından yapılan adli bilişime yönelik model önerisi olan çalışmada ise, adli bilişim süreçlerinin davranışsal delil analizi konu alınmıştır. Buradaki model önerisinde ise laboratuvar ortamındaki inceleme, analiz ve raporlama süreçlerine odaklanılmıştır [40]. Post-mortem yani olay yeri sonrası olan sürece odaklanılarak, adli bilişim personeli için yapılan hataların telafisinin olmadığı ilk müdahale süreçleri göz ardı edilmiştir.

NIST (National Institute of Standard and Technology) tarafından hazırlanan mobil cihaz adli bilişimi için rehberde de mobil cihaz teknolojisi ve adli bilişim süreçleri baştan sona detaylı ele alınmıştır. Mobil cihaz adli bilişimiyle ilgilene herkesin başvurması gereken nitelikteki bu çalışmada, mobil cihaz incelemede kullanılan araçların çalışma prensipleri dahil, bir çok önemli noktaya değinilmiştir. Mobil cihaza müdahaleye ilişkin oluşturulan karar ağacı diyagramında cihazın durumuna ilişkin kilitli olup olmadığı ve batarya durumu gibi sınırlı bazı unsurlar dile getirilmiştir. Çalışmada da belirtildiği üzere bu diyagram başlangıç niteliğindedir. Detaylara girilmemiş problemler için uzmandan destek alınması gerektiği şeklinde çözümler önerildiği görülmüştür [19].

Akalın, mobil cihaz inceleme sürecine yoğunlaşarak bir model önerisi geliştirmiştir. Bu modelde literatürün genelinde yer alan koruma, elde etme, inceleme-analiz ve raporlama aşamaları üzerinden oluşturmuştur. Bu aşamaları toplamda on dokuz alt adımda ele almış ve alt adımların gerçekleşmesine dair kontrol listeleri oluşturmuştur. Ayrıca iki farklı adli bilişim yazılımıyla mobil cihaz incelemesine de yer verilmiştir. Detaylara girilen bu çalışmada da mobil cihaz adli bilişiminin en önemli problemlerinden olan imaj alma safhasında karşılaşılan engellere girilmemiş ve çözümler sunulmamıştır [20].

Mobil cihaz adli bilişiminin uygulanmasına ilişkin Türkiye'deki en kapsamlılardan sayılabilecek eserde Doğanay, zorluklar ve delil zincirine odaklanmıştır. Ancak mobil cihazlardan delil elde edilmesine ilişkin bir iş akışına yer vermiştir. Bu iş akışı her ne kadar diğer çalışmalara göre detaylı bir çıktı vermiş olsa da, adli bilişim uygulayıcısı için yapılması gerekenleri saymış ancak hangi sorunların nasıl çözüleceğine ilişkin detaylar yüzysel kalmıştır [41].

Anlaşıldığı üzere adli bilişime ilişkin çıkarılan modeller, daha yüksek seviyedeki süreçlere odaklanmıştır ve alt seviyedeki temel ilkelerle ilgili fazla detaya yer verilmemiştir. Ayrıca yapılan çalışmalar laboratuvar ortamında yürütülen adli bilişim süreçlerine ele alınmış ve olay yerindeki süreçler ve hukuki süreçler mevzuat ülkeden ülkeye farklılık gösterdiği için göz ardı edildiği görülmüştür. Bunlara ilave olarak mobil cihaz adli bilişiminin en önemli problemlerinden olan imaj almayla ilgili olarak mobil cihazların kendi içinde barındırdığı zorluklardan dolayı detaylı bir süreç modeli ortaya konulamadığı görülmüştür.

Bu çalışmada pragmatik, yapısal ve disiplinler arası bir yaklaşım ile mobil cihazların imaj alınmasına en önemli faktörler belirlenerek, hukuki açıdan karşılaşılan sorunların çözümünü de barındıran bir model önerisi geliştirilmiştir. Karar destek sistemiyle de mobil cihaz adli bilişim uygulayıcılarının cihaza ilk müdahale aşamasından başlayarak bir soru-kural diyagramı çıkartılmıştır.

7.1. Mobil Cihaz Adli Bilişiminde Soruların Belirlenmesi

Mobil cihaz adli bilişimi; cihaza ilk müdahale, imaj alma ile inceleme ve raporlama olmak üzere üç temel aşamada ele alınmıştır. Sorular belirlenirken mobil cihazlar üzerine çalışan adli bilişimcinin durumu net bir şekilde ortaya koyması, bunları detaylandırması ve varsa sorunları belirlenmesi hedeflenmiştir. Bu sorular özellikle Türkiye Cumhuriyeti mevzuatına göre hareket eden kolluk birimlerini yönlendirecek şekilde tasarlanmıştır. Model, pratikte mobil cihazların genelinde adli bilişim faaliyeti uygulayan kolluk birimlerine fayda sağlayacak adımları içerecek şekilde tasarlanmış olup sorular ve açıklamaları aşağıda verilmiştir.

7.1.1. Cihaza ilk müdahale

Cihaza ilk müdahale aşaması suça konu olduğu değerlendirilen bulgunun tespitiyle başlamaktadır. Cihaz tespitinden sonra olay yerine giden adli bilişim personelinin yetkileri de dahil olmak üzere kontrol etmesi gereken hususları da barındıran bir soru-cevap süreci ortaya konulmaya çalışılmıştır. Sorulara yetkinin olup olmadığının kontrolüye başlanıp, cihazın fiziksel durumunun tespiti ile devam edilmektedir. Bir sonraki aşama olan imaj alma işlemi için gerekli tedbileri alacak şekilde son verilmektedir. Oluşturulan diagram Şekil 2 ve Şekil 3'te gösterilmiştir.

1. Bir soruşturma kapsamında mı hareket ediliyor?

Türkiye'de adli bilişim açısından temel yetki veren mevzuat olan Ceza Muhakemesi Kanunu Madde 134'te belirtildiği üzere bu tedbir yalnızca soruşturma aşamasında uygulanmaktadır. Bu sebeple soruşturma kapsamında ve hakim kararı olmadan kişilerin temel hak ve özgürlüklerini barındıran alana müdahale Türk Ceza Kanununa göre sorumluluk doğurabilmektedir.

2. Adli bir soruşturma mı?
3. İdari bir soruşturma mı?
4. Yetkili makamlarca verilmiş bir karar var mı?

Soruşturmanın adli bir soruşturma olması durumunda hakim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından verilmiş karar olması gerekmektedir. Bu kararlar olmadan yapılan arama TCK Md. 120'ye göre Haksız arama suçunu oluşturabilecektir.

5. Verilen kararda arama yapılacak yere, aramanın konusuna ve şüpheliye ilişkin bilgiler uyuşuyor mu? (CMK md. 116 vd. ve CMK md. 134)
6. Kamuya ait bir cihaz mı?

İdari soruşturma kapsamında yalnızca kamuya ait cihazlara ilişkin adli bilişim incelemesi yapılabilirken, kişilere ait cihazlarda adli bilişim incelemesi yapabilmek için bir adli soruşturma kapsamında karar alınmış olması gerekmektedir.

7. Yetkili müfettiş veya denetim yetkisine sahip amir tarafından verilmiş bir karar var mı?
8. Adli bilişim dışında farklı bir kriminal analize ihtiyaç var mı?

Deliller üzerinde parmak izi, DNA analizi gibi çalışmalara ihtiyaç duyulacak olursa adli bilişim faaliyetlerine başlamadan önce ilgili birimle irtibata geçilerek gerekli önlemlerin alınması gerekmektedir.

9. Cihazın gözle görülen bir fiziksel arızası var mı?

Cihazdaki arızanın olay yerinde tespiti ileride oluşacak ihtilafların, delil karartma gibi şüphelerin ortadan kaldırılması için önem arz etmektedir.

10. Cihaz sıvı içinde mi?

Cihazın sıvı içinde olması durumunda içerideki akımı kesmek için engellemek amacıyla bataryanın sökülmesi gerekmektedir.

11. Sıvı tahrip edici bir sıvı mı?

Sıvı tahrip edici sıvıysa cihazı korumak için bir an önce o sıvıdan arındırmak gerekmektedir. Tahrip edici sıvı olmayan durumlarda oksitlenmeyi başlatmamak için mevcut sıvıyla muhafaza edilmesi gerekmektedir.

12. Cihaz açık mı?

Cihazın açık olması durumunda saat, tarih, kullanıcı gibi bazı bilgilerin kontrölü ve uçucu verilerin alınması gerekir. İlk önce uçucu verilerin kayda alınması önem arz etmektedir [41]. Cihazın açık halde laboratuvar ortamına nakli için powerbank gibi güç kaynağı ile desteklenmeli ve şarjın bitmesi durumuyla karşılaşılmasını engelleyici tedbirlerin alınması gerekmektedir.

13. Ekipman içerisinde faraday çantası var mı?

Mobil cihazlar yapısı gereği kablosuz iletişime açık olduğundan radio frekanslarını keserek, dışarıdan gelecek delil karartmaya ilişkin sinyalleri engellemek amacıyla faraday çantası kullanılması gerekmektedir. Faraday çantasının bulunmadığı durumlarda cihazın uçak moduna alınması da bir diğer çözümdür.

14. Cihaz içerisinde sim kart ve hafıza kartı gibi başka aparatlar var mı?

Cihaz içerisindeki diğer aparatların mutlak surette tespit edilmesi gerekmektedir. Daha sonradan ortaya çıkan sim kart ve hafıza kartları aidiyetle ilgili şüphe doğurabilmektedir.

15. Bu aparatları çıkartmak için bataryayı sökmek gerekiyor mu?
16. Cihaz evrensel bağlantı portlarına mı sahip?

Cihazın standartlar portlar dışında farklı, nadir bulunan veri ya da güç portuna sahip olması ara kabloları bulma konusunda ileride farklı sıkıntılara sebebiyet vermektedir. Adli bilişim incelemesi yapılması için cihazla iletişim kurulması en temel unsurlardan biridir.

7.1.2. İmaj alma

Cihaza ilk müdahale aşamasından sonra geçilen mobil cihazlar için imaj alma aşaması genellikle olay yerinde değil de laboratuvar ortamında gerçekleşirilmektedir. İmaj alma aşaması otuz dört sorudan oluşmakta ve bu sorularla cihazın içindeki anlamlı veriye ulaşılması hedeflenmektedir. Bu aşamada sorulan sorularla sırasıyla cihazın çalışıp çalışmadığı, varsa arızası, arızanın nasıl giderilebileceği, imajın nasıl alınabileceği tespit edilmesi amaçlanmaktadır.

1. Cihaza ait bilgilerin tespiti tam ve eksiksiz yapılmış mı?

Bu adım cihaza ilk müdahale eden, el koyan kişiyle laboratuvar ortamındaki uzmanın farklı kişi olması durumunda delil zincirinin korunması için önem taşımaktadır.

2. Cihaz açılıyor mu?

Cihazın açılmaması durumunda, eletriksel zararların meydana gelmemesi için içindeki elektrik enerjsini kontrollü şekilde deşarjı gerekmektedir.

3. Batarya var mı?

Bataryanın olup olmadığına göre, cihazın çalıştırılması için gereken yöntem değişmektedir. Batarya varsa osiloskop ile kontrolü gerekirken, yoksa farklı bir güç kaynağı ile enerji sağlanması gerekmektedir.

4. Sim kart olmadan açılan modellerden mi?

Bazı eski telefonların sim kart olmadan farklı bir fonksiyon barındırmamasından dolayı, sim kartsız çalışmama özellikleri mevcuttur. Bu engelin, sim kart klonlanarak aşılması mümkündür.

5. Cihaz ile normal yollardan iletişim kuruluyor mu?

Cihaz ile normal yollardan iletişim kurulması halinde, imajı alınabilir. İletişim kurulmaması halinde çözümü için adımlar atılması gerekmektedir.

6. Cihaz şifreli mi?

Cihazın şifresi olması durumunda şifreyi aşmaya yönelik işlemler yapılabilmekte iken, cihazın şifresi olmadığı halde iletişim kurulamaması halinde arıza olup olmadığına yönelik tespitlerin yapılması gerekmektedir.

7. Cihaza şifre kırma atağı yapılabiliyor mu?

Eğer cihaza şifre kırma atağına müsait olan bir cihazsa, hatalı denemeler neticesinde kendini wipelama riski de göz önüne alınarak bu işlem gerçekleştirilir. Ancak cihazın kendini tamamen silmesi olmayı, ileride şifrenin farklı yollardan

temini yoluyla aşılması imkanını da kapatacağından, bu hususa ayrıca önem gösterilmesi gerekmektedir.

8. Cihazın bootloader ile fiziksel imajı alınabiliyor mu?

Bootloader yöntemiyle cihazın kullanıcı arayüzüne ve buradaki şifreyle karşılaşmadan veriye erişilmesi mümkün olmaktadır.

9. Root işlemi ile imajı alınabiliyor mu?

Eğer cihazın şifresinin aşılması yönetici hakları elde edilince mümkün ise, cihazdaki yönetici haklarını elde etmek için root işlemi uygulanması gerekmektedir.

10. İmajı alınmasına rağmen başlangıç kriptosu var mı?

İmaj alındıktan sonra başlangıç şifrlemesi mevcutsa, veri kaybı riski olmadan atak yapılabilir. Çünkü imaj alma işlemi gerçekleştirildiğinden, asıl cihaza ilişkin delili bütünlüğü zaten sağlanmış durumdadır.

11. Cihazın arızası var mı?

Cihazın arızası varsa cihazın arızasının tespiti ve sonrasında giderilmesine yönelik işlemler yapılmalıdır.

12. Arıza bağlantı portlarında mı?

Arızanın bağlantı portlarında olması durumunda lehimleme ile giderilmesi çalışılmalıdır.

13. Lehimleme ile arıza giderildi mi?

Lehimleme ile de bağlantı kurulamadıysa, bunun çözümü portu değiştirmekten geçmektedir.

14. Arıza ekranda mı?

Ekran arızası durumunda ekranın çalışır hale getirilmesi çok müümkün olmadığından, yerine sağlam ekran takılarak cihazla iletişim kurulmaya çalışılması gerkemektedir.

15. Arıza board üzerinde mi?

Bileşenleri elinde tutan ve bunlar arasındaki iletişimi sağlayan kartın arızalı olması durumunda arızanın tespitine yönelik çalışma gerekir.

16. Board üzerindeki arıza tespit edilebiliyor mu?

Eğer kart üzerindeki arıza tespit edilemiyorsa, çözümü için başkaca yapılacak işlem bulunmamaktadır.

17. Kısa devre mi?

Kısa devre olması durumunda, kısa devrenin bulunduğu yer lehimlenerek, elektrik devresnin tamamlanması sağlanmalıdır.

18. Yanmış mı?

Eğer kart üzerinde yanma neticesinde bir tahribat oluşmuş ise, veriye ulaşmak için hafıza çipine odaklanılması gerekmektedir.

19. Hafıza çipi sağlam mı?

Hafıza çipinde de bir arıza veya hasar durumu varsa veriye ulaşılması pratikte imkansız hale geldiği söylenebilir. Bundan sonra yapılacak başkaca işlem bulunmamaktadır.

20. Arıza giderildi mi?

Eğer sayılan yöntemlerle arıza giderildiyse, cihazın verisine ulaşılıp ulaşılmadığının kontrolü ve ardından imajı alınması aşamasına geçilmesi, eğer arıza giderilememişse yapılan işlemler raporlanarak tutanak altına alınıp işlemin sonlandırılması gerekmektedir.

21. Cihazdaki veri kriptolu olarak mı tutuluyor?

Cihazın hafıza çipindeki veri kriptolu olarak tutulmuyorsa, chip-off işlemiyle çipi sökülerek, çiple iletişim kurularak verinin ham hali elde edilir. Bu şekilde cihazın fiziksel imajı alınmış olmaktadır.

22. Yapılan işlemler neticesinde arıza giderilerek veriye ulaşıldı mı?

Her ne kadar arıza giderilse de cihaz içindeki veriye ulaşılamadıysa, yapılan işlemler raporlanarak tutanak altına alınıp işlemin sonlandırılması gerekmektedir.

23. Adli bilişim yazılımları ile fiziksel imajı alınabiliyor mu?

Mobil cihaz adli bilişimin en temel hedefi sayılabilecek olan fiziksel imaj alındıysa işlemler tamamlanmış anlamına gelmektedir.

24. Adli bilişim yazılımları ile dosya sistemli ya da mantıksal imajı alınabiliyor mu?

Eğer fiziksel imaj alınamadıysa daha az miktarda ve daha yüzeysel veriye ulaşılmasını sağlayan diğer imaj alma yöntemleri denenir.

25. Adli bilişim yazılımında cihazın modeli destekleniyor mu?

Adli bilişim yazılımlarının imaj alma yöntemleri ve destekleri cihazdan cihaza değiştiğinden, destek verilen cihaz olmaması durumunda android

işletim sistemlerinin genel (generic) niteliklerinden imaj alma yönteminin denenmesi gerekmektedir.

26. Destekleyen farklı bir yazılım mevcut mu?

Her ne kadar adli bilişimde kullanılan yazılımların çoğu NIST gibi standartları haiz de olsa, tüm çözümleri kapsayan bir ürün bulunmamaktadır. Bu sebeple alternative yazılımların desteklerinin kontrol edilmesi gerekmektedir.

27. Cihaz piyasada sıkça bulunmayan Çin menşeili telefonlardan mı?

Cihazın piyasada bilinmeyen Çin menşeili bir cihaz olması, bu tip cihazlara özgü özel yazılımlara yoğunlaşılmasını gerektirmektedir.

28. İmajı alınması gereken SIM kart var mı?

Sim kart, da her ne kadar telefonun doğrudan bir parçası olmasa da bütünleyici parçası olup içerisinde veri barındırdığından imajı alınması gerekmektedir.

29. Pin veya Puk koruması var mı?

Şifreli olan sim kartların hatalı girilmesi durumunda kendini bloklamasından dolayı atak yapılamadığından, pin veya puk koruması imajı engelleyici unsurlardandır.

30. Pin veya Puk şifreleri elde mi?

Şifreli olması halinde şifrelerin temin edilmesi, olay yerindeyken tespitinin yapılması önem arz etmektedir.

31. Sim kart yerli bir operatöre mi ait?

Şifrelerinin olmaması durumunda, ülke egemenlik sınırları içerisindeki operatörlerden CMK Md. 134 kapsamında talebi yapılmalıdır.

32. İmajı alınması gereken hafıza kartı var mı?

Hafıza kartları da belirli bir kapasiteye sahip olduğundan kimi zaman cihazla birlikte kimi zaman tek olarak imajının alınması ve içerisindeki veriye erişilmesi gerekmektedir.

33. Hafıza kartı cihaz tarafından korumalı mı?

Bazı cihaz modellerinde üzerinde takılı bulunan hafıza kartını korumaya alarak, başka cihazla çalışmasını engelleyebilir. Bu durumlarda hafıza kartının imajı, cihaza takılı vaziyette olarak cihazla birlikte alınması gerekmektedir.

34. İmaj alındı mı?

Cihazın imajı alındıktan sonra, hash (veri özeti) değeri hesaplatılır, bu zamana kadar ki tüm işlemler tutanak altına alınır.

7.2. Mobil Cihaz Adli Bilişimden Kuralların Belirlenmesi

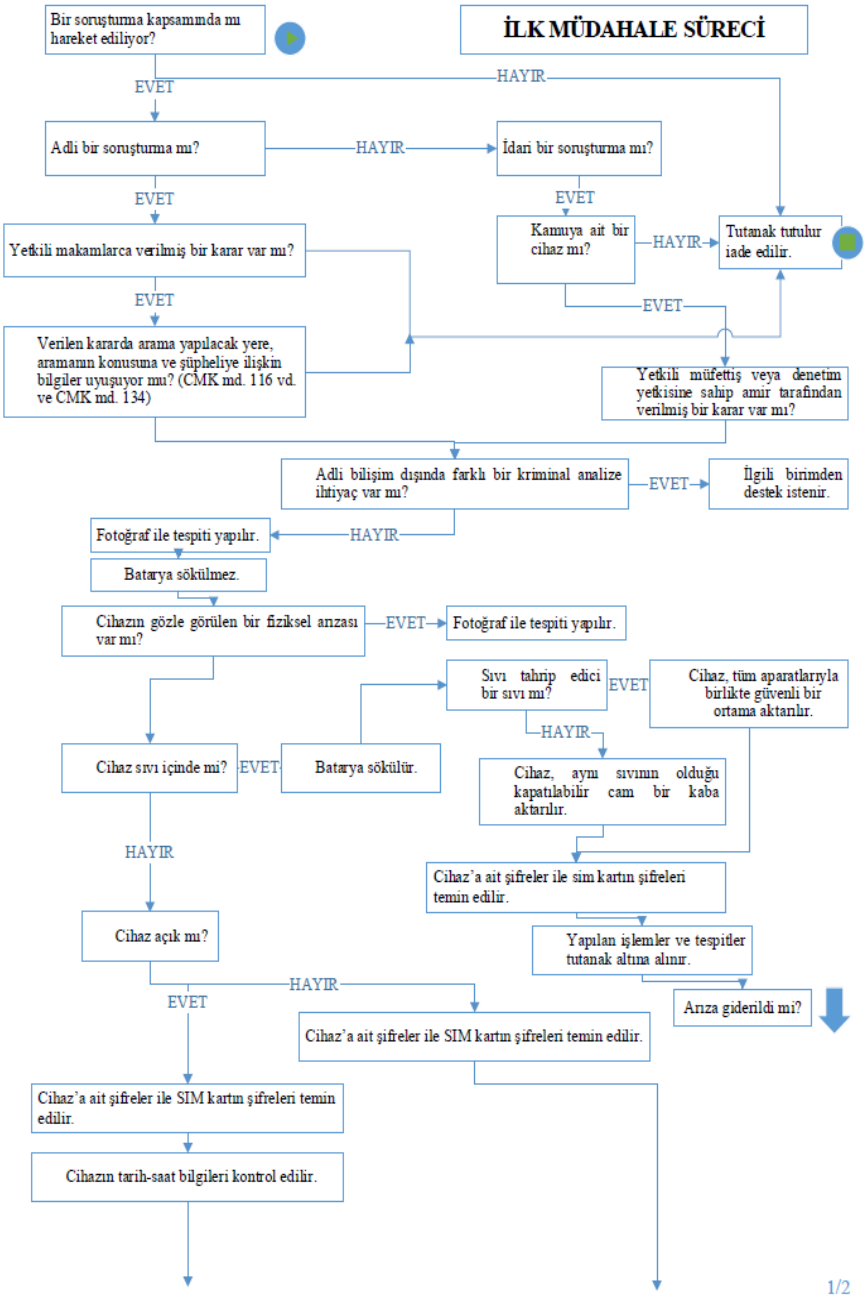
Uygulanacak kurallar belirlenirken günümüz şartlarındaki Türkiye Cumhuriyeti mevzuatı ve mevcut imkanlar dikkate alınmıştır. Adli bilişim personeline yapılacak işlemi nasıl gerçekleştireceği veya yukarıda sayılan yöntemlerin nasıl uygulanacağı değil, hangi işlemin en uygun olduğu yönünde tavsiye verecek şekilde planlanmıştır. Uygulanacak yöntemlerin detayları personelin kendi uzmanlığı olup, bunların bilgisayar sistemlerine aktarılmasına ilişkin bir öneri bulunmamaktadır.

Bu süreçler cihaza ilk müdahale ve imaj alma aşamalarından oluşmaktadır. Bütün süreçte toplamda 49 farklı soruyla mobil cihaz adli bilişimi süreçleri ele alınmış, bu sorular karşısında uygulanacak kurallar da iki farklı şekilde belirlenmiştir. Bu kuralların nasıl uygulanacağı konunun uzmanları tarafından belirlenecektir. Bu diyagramın belirlenmesinde kolluk kuvvetlerinin uygulamaları esas alınmıştır.

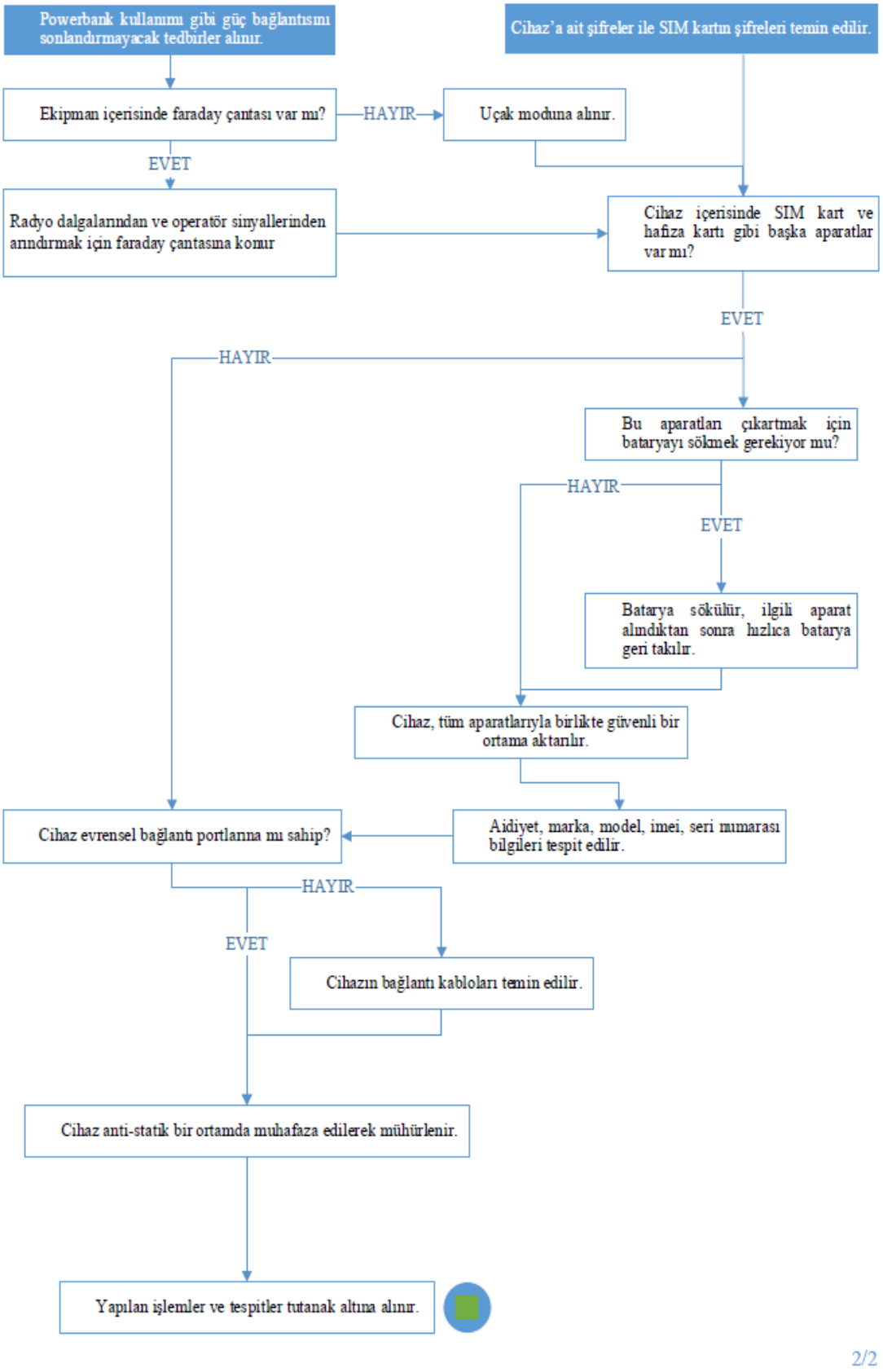
Mobil cihazların yapısı gereği, diyagramın iş akışının doğrusallığı sürekli olarak devam edememiştir. Bu sebeple bazı işaretler ile diyagramın uygulanabilir hale getirilmesi amaçlanmıştır. Bu kapsamda, soru-kural diyagramı içerisinde kullanılan mavi daire içerisindeki yeşil üçgen ile, önceki sorulardan ve verilmiş kurallardan bağımsız olarak sorulması gereken soruyu, mavi daire içerisindeki yeşil dikdörtgen ile, bu aşamadan sonra devam edilecek bir adımın olmadığı belirtilmiştir. Yatay mavi ok işareti ile o sorunun diyagramdaki daha önceki veya daha sonraki bir adımda sorulduğunu ancak soruya cevabın burada olduğu, yukarı ok işareti ile bu soruya cevabın daha yukarıdaki bir aşamada verildiği, aşağı ok işareti ile bu soruya cevabın daha aşağıdaki bir aşamada verildiği tanımlanmıştır.

7.2.1. Cihaza ilk müdahale

Cihaza ilk müdahale aşamasında sorulan on altı farklı soru için on yedi farklı kural tanımlanmıştır. Yetkilerin kontrolü sonucunda yapılacak işlemler, karşılaşılan duruma göre yapılacak işlemler ve ilk müdahale süreci tamamlandığında yapılacak işlemler Şekil 3 ve Şekil 4'te sıralanmıştır.



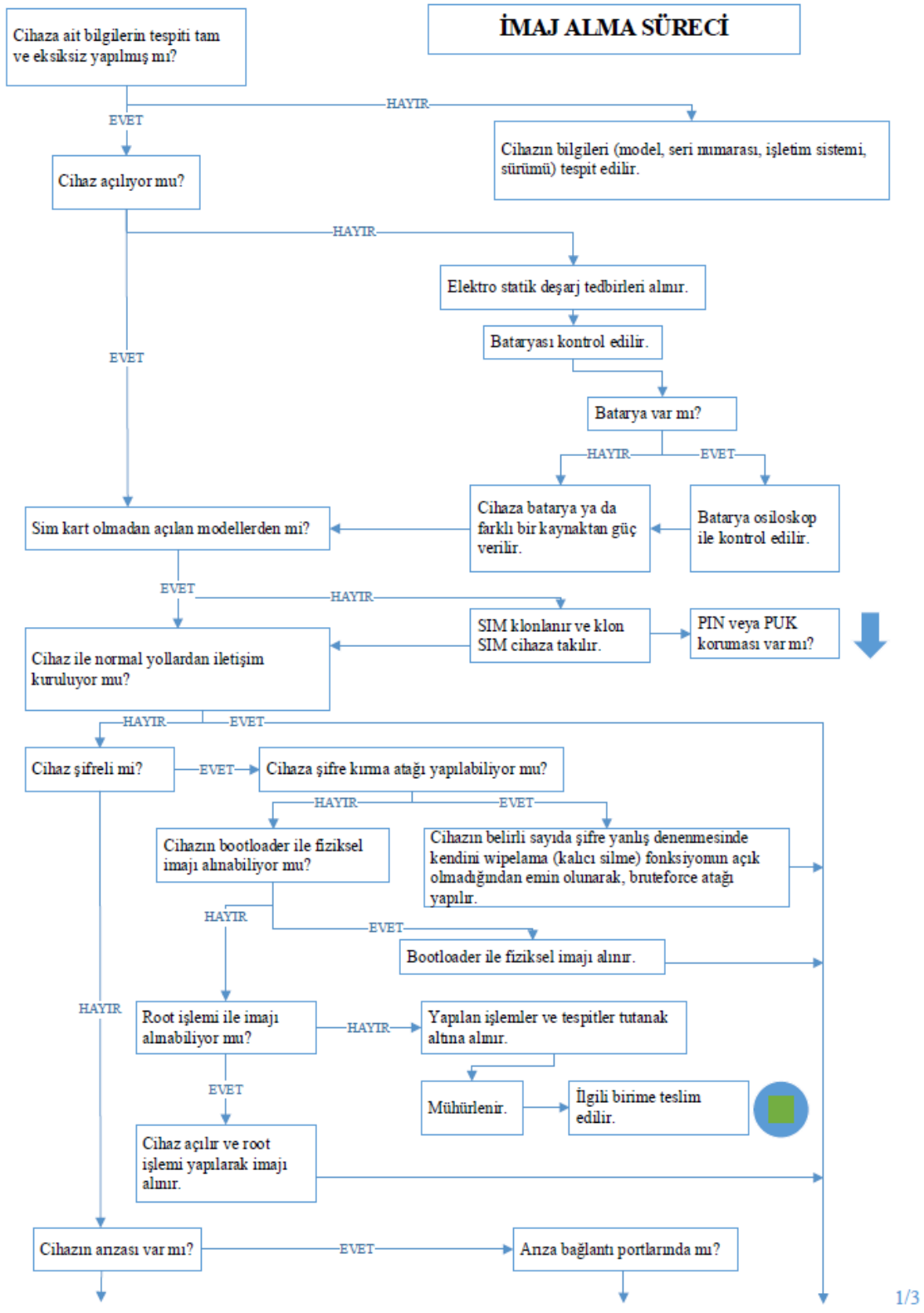
Şekil 3. Cihaza ilk müdahale süreci-1



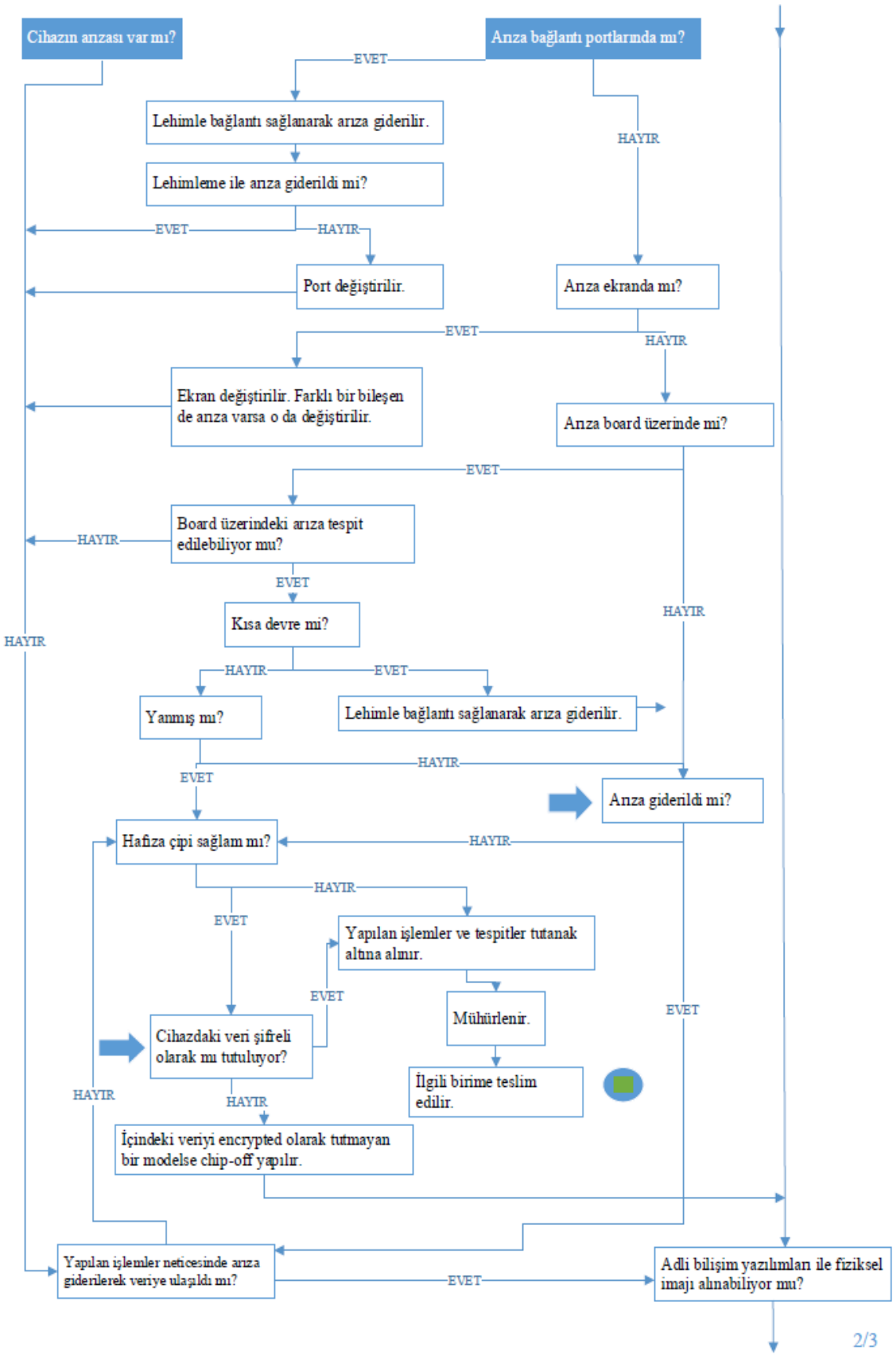
Şekil 4. Cihaza ilk müdahale süreci-2

7.2.2. İmaj alma

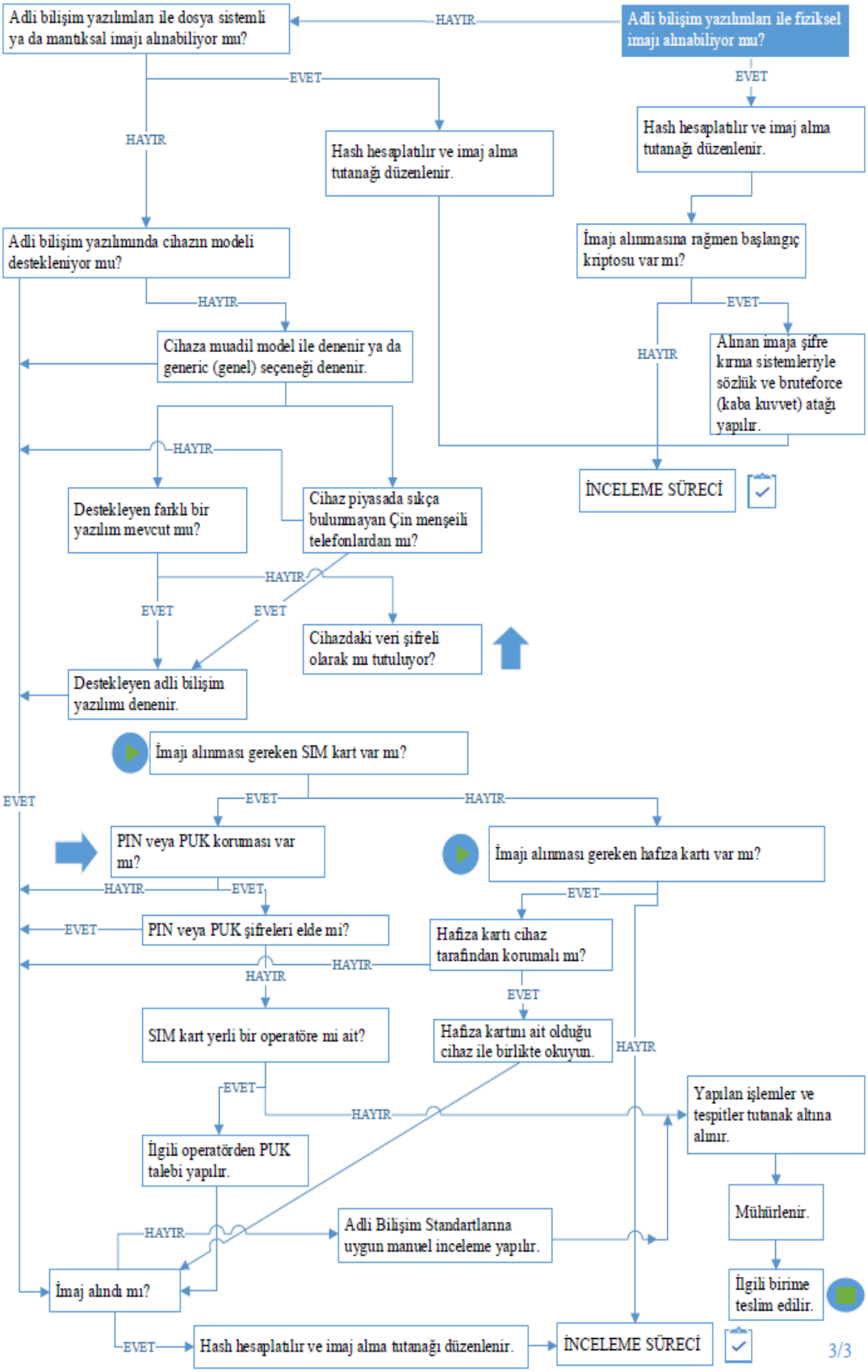
İmaj alma aşaması için hazırlanan otuz dört soruya 30 farklı kural belirlenmiştir. Bu aşama adli bilişimin en önemli adımı sayılabilir ve bu aşamada cihazın içindeki anlamlı veriye ulaşılması hedeflenmektedir. İmaj almaya ilişkin diyagramlar Şekil 5, Şekil 6 ve Şekil 7'de belirtilmiştir.



Şekil 5. İmaj alma süreci -1



Şekil 6. İmaj alma süreci -2



Şekil 7. İmaj alma süreci - 3

Bir karar destek siteminin uygulanması modeli olarak gün geçtikçe artan çeşitliliği, hızla değişen teknolojisi, karşılaşma sıklığı ve içinde barındırdığı veriler ile adli bilişim alanında önemli bir zorluk olarak karşımıza çıkan mobil cihazlardan delil elde etme aşaması ele alınmıştır.

Bu süreçler cihaza ilk müdahale ve imaj alma aşamalarından oluşmaktadır. Bütün süreçte toplamda 50 farklı soruyla mobil cihaz adli bilişimi süreçleri ele alınmış, bu sorular karşısında uygulanacak kurallar da 3 farklı şekilde belirlenmiştir. Bu kuralların nasıl uygulanacağı konunun uzmanları tarafından belirlenecektir. Bu diyagramın belirlenmesinde kolluk kuvvetlerinin uygulamaları esas alınmıştır.

VIII. MODELİN DOĞRULANMASI (VERIFICATION OF THE MODEL)

Modelin geçerliliği için, kamu kurumları, üniversite ve özel sektörden adli bilişim uzmanlarından modelin değerlendirilmesi istenmiştir. Modelin genel olarak geçerliliği ile ilk müdahale ve imaj alma aşamaları için ayrı ayrı değerlendirmeler gerçekleştirilmiştir.

8.1. İlk müdahale aşamasının değerlendirilmesi

İlk müdahale aşamasıyla ilgili olarak uzmanların hukuki açıdan bir problem olmadığı, uygulanacak adımların yeterli olduğu, cihazın imaj alınması sürecine etki edecek unsurlara yeterince önem verildiği, cihazın delil bütünlüğünü korumaya ilişkin unsurlara yeterince önem verildiği yönünde görüş birliğine vardıkları anlaşılmıştır.

İlk müdahale aşamasındaki potansiyel hataları azaltması ve ilk müdahale sürecini hızlandır beklendiği belirtilmiştir. İlk müdahale süreçlerinin uygulanabilmesi için daha fazla ayrıntıya gerek olmadığı yönünde hakim görüş oluşmuştur. Bir uzman, ayrıntılara ilişkin özellike adli bilişim işlemlerine yeni başlamış personelin kullanımı için video, resim vb. içeren ek bir dökümantasyon olmasının faydalı olacağını belirtmiştir.

8.2. İmaj alma aşamasının değerlendirilmesi

Hukuki açıdan ele alındığında bir problem teşkil etmeyeceği belirtilmiştir. Model önerisinde belirtilen imaj alma işleminde uygulanacak adımların yeterli olduğu belirtilmiştir. Cihazın imaj alınması sürecine etki edecek unsurlar ile cihazın delil bütünlüğünü korumaya ilişkin unsurlara yeterince önem verildiği yönünde görüş birliğine varıldığı anlaşılmıştır. Bu model önerisinin imaj alma aşamasındaki potansiyel hataları azaltması ve imaj alma sürecini hızlandıracağının beklendiği belirtilmiştir.

İmaj alma süreçlerinde uygulanabilmesi için daha fazla ayrıntıya gerek olmadığı yönünde hakim görüş oluşmuştur. Bir uzman, imaj alma sürecinin ayrıntılara ilişkin uzman olmayan personelin kullanımını kolaylaştıran görsel yönden desteklenmiş ek bir dökümantasyon olmasının faydalı olacağını belirtmiştir.

İmaj alma aşamasında uygulanacak adımların yeterli olduğu görüşünde de olsa, bir uzman imajı alınacak cihazın işletim sistemleri sürümlerinin de kontrol edilmesi gerektiği belirtmiştir. Ayrıca rooting gibi ileri düzey yazılımsal müdahalelerin sürece dahil edilmesinin faydalı olacağı görüşünü bildirmiştir. İmaj alma işleminin başarısız olması durumunda işlemlerin sonlandırılması yoluna gidilmekteyken; son bir yöntem olarak cihazın adli bilişim standartlarına göre manuel inceleme ile delil tespiti yapılabileceği de belirtlmiştir.

8.3. Modelin genel değerlendirilmesi

Uzmanların genel görüşü mobil cihaz adli bilişim süreçlerini yansıtıldığı ve başarılı şekilde karar verme süreçlerinin anlaşıldığı yönündedir. Diyagramın anlaşılırlığı ile ilgili de genel görüş olumlu olmakla birlikte, bazı uzmanlar daha anlaşılır hale getirilmesinin faydalı olacağını belirtmiştir.

Önerilen modelin mobil cihaz adli bilişimi uygulayıcısına katkı sağlayacağı konusunda görüş birliği bulunmaktadır. Ancak her seviyede mobil cihaz adli bilişimi uygulayıcısı için yeterli sadelikte olmadığını vurgulamışlardır. Bazı işlemlerin uygulanabilmesi için temel düzeydeki mobil cihaz adli bilişimi uygulayıcısı için eğitim verilmesinin gerekebileceği vurgulanmıştır. Ayrıca temel düzeydeki mobil cihaz adli bilişimi uygulayıcısı için resim veya video gibi bazı görsellerle dökümantasyonun takviye edilmesinin faydalı olacağı görüşü de bir uzman tarafından sunulmuştur.

8.4. Değerlendirme

Modelin mobil cihaz adli bilişimine katkı sağlayacağı anlaşılmıştır. Ancak bunun daha sağlıklı işlemesi için uzmanlardan gelen öneriler değerlendirilmiştir. Bu kapsamda belirtilen modelin anlaşılırlığı, uygulayacak personelin yeterliliği, imaj alınamama durumunda manuel inceleme yapılabileceği, işletim sistemi sürümlerinin de kontrol edilmesi gerektiği ve

rooting işlemlerinin de belirtilmesi gerektiği konularında öneriler gelmiştir.

Modelin anlaşılırlığı ile ilgili olarak diyagram mobil cihaz adli bilişimi faaliyeti işinin doğası gereği çok fazla bağlantı barındırmaktadır. Bu bağlantıların ilişkisi kimi zaman doğrusal olmadığından farklı işaretlerle bu ilişki kurulmaya çalışılmıştır. Ancak bu öneriye istinaden diyagramın doğrusal akışı dışındaki iş akışlarını tanımlamakta kullanılan işaretlere ilişkin açıklmaya ilave olarak yer verilmiştir.

Uygulayacak personelin yeterliliği ile ilgili olarak ise, personelin bu işlemleri yerine getirmesi için belirli bir teknik bilgi birikimine sahip olması gerektiği aşikardır. Ancak personelin yetiştirilmesi, gereken eğitimin nitelikleri bu çalışmanın konusu olmadığından, personelin eğitimi göz ardı edilmiştir. Bu işlemleri uygulayacak personelin yeterli teknik bilgi birikimini haiz olduğu kabul edilmiştir.

İmaj alınmama durumunda manuel inceleme yapılabileceği önerisi ile ilgili olarak; çalışma ilk müdahale ve imaj alma aşamalarıyla sınırlı olarak yapılmıştır. Manuel inceleme işlemi, imaj alma sonrası gerçekleştirilen inceleme ve raporlama alanlarında kaldığı değerlendirildiğinden çalışmanın başında göz ardı edilmiştir. Ancak öneriyle tekrar değerlendirilmiş ve manuel inceleme işlemi esası itibariyle bir inceleme işlemi olsa da, imaj alma işleminin başarısız olması durumunda başvurulan bir yöntem olduğundan, imaj alma işlemini yürüten personelin de bu işlem esnasında dikkate alması gereken bir adımdır. Bu sebeple adli bilişim standartlarına uygun olarak manuel incelemenin yapılması gerektiği modele işlenmiştir.

İşletim sistemlerinin kontrol edilmesi ve rooting işleminin uygulanması önerisiyle ilgili olarak, bu işlemler mobil cihaz adli bilişimi açısından önem arz etmektedir. Ancak imaj alma işleminde kullanılan mobil cihaz adli bilişimi yazılımları, imaj alma işlemlerini gerçekleştirirken işletim sistemlerini, çip setlerini, yazılımın root atılması ihtiyacı gibi unsurları değerlendirildiğinden bu hususlar, mobil cihaz adli bilişim yazılımlarının desteği altında çözüme kavuşturulmasının gerektiği beklenmektedir. Ayrıca desteklenen sürümler ve root ihtiyacı yazılımların güncellemelerine göre değişiklik gösterebileceğinden, model önerisinin genel geçer niteliğini olumsuz etkileme ihtimalinden dolayı bu önerilere ilave olarak yer verilmemiştir.

IX. SONUÇLAR (CONCLUSIONS)

Genel olarak karar verici uzman kişilerin kararlarını vermede daha etkin ve verimli olmalarını sağlamak amacıyla geliştirilmiş olan bilgisayar destekli araçlar veya yazılımlar olarak tanımlanabilen karar destek sistemlerinin [19] adli bilişim alanında mobil cihaz adli bilişim sürecinde nasıl entegre olabileceğine ilişkin bir çalışma gerçekleştirilmiştir.

Bu çalışmayla gün geçtikçe artan çeşitliliği, hızla değişen teknolojisi, karşılaşma sıklığı ve içinde barındırdığı veriler ile adli bilişim alanında önemli bir zorluk olarak karşımıza çıkan mobil cihazlardan delil elde etme aşamasında karar destek sisteminin uygulanmasına ait bir model önerisi sunulmuştur. Mobil cihaz adli bilişiminde en sık karşılaşılan durumlara ilişkin hazırlanan soru-kural akış diyagramı ile mobil cihaz adli bilişimi ile ilgilenen personelin, en doğru kararı en kısa sürede vermesi ve verdiği kararları sonuçlarıyla birlikte kaydederek, sistemin daha efektif hale getirilmesi amaçlanmıştır.

Bu kapsamda mobil cihaz adli bilişimine ilişkin 50 farklı soru oluşturulmuş ve bu sorular karşısında uygulanacak kurallar geliştirilmiştir. Sorular cihaza ilk müdahale ve imaj alma aşamalarına ayrılarak sorulmuştur. Özellikle cihaza ilk müdahale aşaması diğerlerinden farklı olarak olay yerinde uygulanması gereken protokolleri kapsamaktadır. Bu sebeple aşamalara ayrıştırabilen bu soru-kural akış diyagramı, teknik birimler dışında olay yerinde delillere el koyan kolluk birimleri tarafından da özellikle cihaza ilk müdahale aşaması uygulanabilmesi mümkündür.

Bu model önerisinin doğrulanmasıyla ilgili olarak, üniversitelerde, kamu kurumlarında ve özel sektörde görev yapan adli bilişim uzmanlarıyla görüşmeler gerçekleştirilmiştir. Bu modelin mobil cihaz adli bilişimi süreçlerini yansıttığı, karar vermeyle ilgili süreçlerin anlaşıldığı, mobil cihaz adli bilişimi uygulayıcısı için katkı sağlayacağını belirtmişlerdir. İlk müdahale ve imaj alma süreçlerini hızlandırmasının ve potansiyel hataların azaltılmasının beklendiği konusunda görüş bildirilmiştir. Ayrıca Türkiye'deki adli bilişim uygulamasında karşılaşılan sorunlardan olan hukukilik ve delil bütünlüğü konularına gereken önemin verildiği de vurgulanmıştır.

Uzmanların üzerinde durduğu unsurlardan biri de tecrübeli personelin süreci rahatça işletebileceği iken, yeni başlayan personelin resim veya video

gibi görsellerle desteklenmesinin ve modelin anlaşılırlığının artırılmasının faydalı olacağıdır. Ayrıca temel düzeydeki mobil cihaz incelemecisinin bazı iş ve işlemler uygularken eğitimlerle desteklenmesi gerektiği yönünde görüş bildirilmiştir. Ancak personelin eğitimi bu çalışmanın konusu olmadığından, bu öneriler göz ardı edilmiştir.

Ancak anlaşılır hale getirilmesiyle ilgili açıklamalar eklenmiş ve manuel inceleme yapılmasıyla ilgili olarak da model önerisinde yer verilmiştir. İmaj alınamaması durumunda adli bilişim standartlarına uygun manuel inceleme yapılmasına ilişkin diyagrama bir adım eklenmiştir.

Teknik açıdan ihtimallerin binlerce olduğu mobil cihaz adli bilişimi süreçlerinde, anlaşılır bir model sunulabilmesi için bazı unsurlar göz ardı edilmiştir. Olay yeriyle ilgili mobil cihazın dışındaki unsurlar bu süreç dışında tutulmuştur. Ayrıca yazılımsal işlemlerle ilgili olarak adli bilişim yazılımlarının sunduğu imkanlarla sınırlı kalınmıştır. Box cihazları gibi üçüncü parti yazılımlarla cihazın tüm admin haklarına erişilip cihazın her türlü sistem alanına erişilmesi mümkünken, önerilen modelde uzmanın adli bilişim yazılımının sunduğu kadarıyla rooting işlemini gerçekleştirmesi öngörülmüştür. Ayrıca modeli uygulayacak personelin, modelde bahse konu işlemleri de nasıl uygulayacağını biliyor olması gerekmektedir. İşlemi yapacak mobil cihaz adli bilişimi uygulayıcısının konudaki bilgi eksiliğine ragmen işlem yapma ihtimali de göz ardı edilmiştir.

Özetle bu önerilen modelin, yüksek iş hacmiyle adli bilişim faaliyeti yapan kamu veya özel laboratuvarlarda uygulanması halinde maliyet ve zaman tasarrufu sağlanması hedeflenmektedir. Ayrıca olay yerinde delil toplayan kolluk görevliler ve bilirkişiler için de kullanılmasının hem ülke geneli adli bilişim açısından iş ve işlemlerin standarda kavuşmasına hem de belirlenmiş kurallar sayesinde olası potansiyel riskleri azaltmaya ve sorunlar karşısında hızlı çözüm üretebilmesine fayda sağlayacaktır.

KAYNAKLAR (REFERENCES)

[1]. M. Scanlon and M. T. Kechadi. “Digital Evidence Bag Selection for P2P Network Investigation”. In Proceedings of the 7th International Symposium on Digital Forensics and Information Security (DFIS-2013), pages 307–314. Springer, Gwangju, South Korea, 2014.

[2]. D. Lillis, et al. “Current Challenges and Future Research Areas for Digital Forensic Investigation”. arXiv preprint arXiv:1604.03850, 2016.

[3]. “Soylu, incelenen dijital materyal sayısını açıkladı: 2018'de, ortalama 45 binden, 631 bin 233'e yükseldi” [Online]. Available: https://t24.com.tr/haber/soylu-incelenen-dijital-materyal-sayisini-acikladi-2018de-ortalama-45-binden-631-bin-233e-yukseldi,749982 Yayın Tarihi: 16.11.2018 Erişim Tarihi: 06.12.2020

[4]. K. Say, “Bilişim Suçlarında Olay Yeri İncelemesinin Hukuki Boyutu”, L. Bayram (ed.), Ses Görüntü ve Data İncelemeleri içinde (251-260), Adalet Yayınevi, Ankara, 2008, s. 259.

[5]. Y. Başlar, “Adli Bilişim Sürecinde Karşılaşılan Sorunlar ve Çözüm Önerileri”. 2019.

[6]. İ. Çiçek, “Ülkemizde Adli Bilişim Laboratuarı Kurulumu ve Bilişim Suçlarıyla Mücadeleye Katkıları”, Yayınlanmamış Yüksek Lisans Tezi, Haliç Üniversitesi Fen Bilimleri Enstitüsü, 2008, s. 14.

[7]. O. Değirmenci, “Ceza Muhakemesinde Sayısal (Dijital) Delil”, Seçkin Yayıncılık, Ankara, 2014, s. 121.

[8]. K. Say, “Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi”, Yayınlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, 2006.

[9]. Ş. Sağıroğlu, M. Karaman, “Adli Bilişim”, Teletapi Haberleşme ve Bilişim Teknolojileri Dergisi, 2012, S. 203, s. 67.

[10]. Ö. Özbey, “Adli Bilişim ve Sayısal Deliller (5271 sayılı CMK’nın 134. maddesi)”, Yargıtay Dergisi, 2010, C. 36, S. 3, ss. 61-126

[11]. M. Faheem, M. T. Kechadi, N. Le-Khac, “The State of the Art Forensic Techniques in Mobile Cloud Environment: A Survey, Challenges and Current Trends”, International Journal of Digital Crime and Forensics, Vol. 7, Issue 2, Pg.1-19, April 2015

[12]. E. Ndarake, “Computer Forensics Investigation (Step by step guide)”, 2013 https://baixardoc.com/documents/computer-forensics-investigation-techniques-effiong-effiong--5c9d2edf8ef6d Yayın Tarihi: 2013 Erişim tarihi: 20.04.2021

[13]. T. Henkoğlu, “Adli bilişim: Dijital delillerin elde edilmesi ve analizi”, Pusula, 2014.

[14]. A. H. Ekizer, Adli Bilişim. Erişim adresi: https://www.ekizer.net/adli-bilisim-computerforensics/ , 2014. Yayın Tarihi: 2014 Erişim Tarihi: 18/4/2021

[15]. H. Aydoğan, “Adli Bilişimde Yeni Elektronik Delil Elde Etme Yöntemleri” Yayınlanmamış Yüksek Lisans Tezi, Ankara, Polis Akademisi Güvenlik Bilimleri Enstitüsü, 2009.

[16]. H. A. Doğanay, "Mobil Adli Bilişiminin Önemi Bağlamında Hukuki Süreç ve Delil Zinciri Kavramı ile Yeni Nesil Mobil Cihazların İncelenmesinde Karşılaşılan Güncel Zorlukların Değerlendirilmesi", Yayınlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi Sağlık Bilimler Enstitüsü, 2019.

[17]. I. L. Lin, H. C. Chao, ve S. H. Peng, "Research of digital evidence forensics standard operating procedure with comparison and analysis based on smart phone". In 2011 International Conference on Broadband and Wireless Computing, Communication and Applications (pp. 386-391), 2011.

[18]. H. Çakır ve M. S. Kılıç, "Mobil Cihazların İncelenmesi" Adli Bilişim ve Elektronik Deliller 1. Baskı, Ankara, 2014, 373-409.

[19]. W. Jansen, R. Ayers, ve S. Brothers, "Guidelines on Mobile Device Forensics". NIST Special Publication 800-101 Revision 1, Springfield, VA, USA, 2014.

[20]. U. Akalın, "Mobil Cihazlarda Adli Bilişim Çalişmalarina Yönelik Bir Model Önerisi" Gazi Üniversitesi Yayınlanmamış Yüksek Lisans Tezi, 2016.

[21]. A. Zareen, S. Baig, "Mobile Phone Forensics Challenges, Analysis and Tools Classification", in the Proceedings of the 2010 International Workshop on Systematic Approaches to Digital Forensic Engineering, May 2010, pp. 47-55, 2010.

[22]. "The Digital Investigator's Resource for Mobile Device Forensic Information" [Online]. Available: https://www.mobileforensicscentral.com/mfc/products_software.asp Erişim Tarihi: 03.12.2020

[23]. "XRY" [Online]. Available: https://www.msab.com/products/xry/ Yayın Tarihi: 2020 Erişim Tarihi: 03.12.2020]

[24]. "Cellebrite" [Online]. Available: https://www.cellebrite.com/en/home/ Yayın Tarihi: 2020 Erişim Tarihi: 02.12.2020

[25]. "Magnet Forensics" [Online]. Available: https://www.magnetforensics.com/axiom-smartphone/#leader Erişim Tarihi: 02.12.2020

[26]. "Oxygen Forensics" [Online]. Available: https://www.oxygen-forensic.com/en/products/oxygen-forensic-detective Erişim Tarihi: 02.12.2020

[27]. [27] "Paraben Corporation" [Online]. Available: https://paraben.com/ Yayın Tarihi: 2020 Erişim Tarihi: 02.12.2020

[28]. "MOBILEdit" [Online]. Available: https://www.mobiledit.com/mobiledit Yayın Tarihi: 2020 Erişim Tarihi: 02.12.2020

[29]. "BlackBag Technologies" [Online]. Available: https://www.blackbagtech.com/software-products.html Yayın Tarihi: 2020 Erişim Tarihi: 02.12.2020

[30]. "Andriller" [Online]. Available: https://www.andriller.com/ Yayın Tarihi: 2020 Erişim Tarihi: 02.12.2020

[31]. "Katana Forensics" [Online]. Available: https://katanaforensics.com/lantern.php Yayın Tarihi: 2020 Erişim Tarihi: 02.12.2020

[32]. B. Bilgen, "Kurumsallaşma Üzerine Bir Karar Destek Sistemi Oluşturulması -Türk İnşaat Sektöründe Örnek Uygulama (Kural Tabanlı Kds Modeli)" Yayımlanmamış Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, İstanbul Teknik Üniversitesi, İstanbul, 2011.

[33]. E. Turban, Decision Support Systems and Expert Systems: Management Support Systems, 2nd ed., Macmillan Publishing Company, 6-30, 105-131, New York, 1990.

[34]. H. Gökçen, "Yönetim Bilgi Sistemleri", Palme Yayıncılık, Ankara, 2007.

[35]. E. Güvenç, "Zeki Karar Destek Sistemi Kullanılarak Muğla Sıtkı Koçman Üniversitesi Uzaktan Eğitim Öğrencilerinin Ders Performanslarının Değerlendirilmesi" Yayımlanmamış Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, Muğla Sıtkı Koçman Üniversitesi, Muğla, 2018.

[36]. M. A. Tokaylı, "Zaman Pencereli Araç Rotalama Problemi İçin Karar Destek Sistemi," Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, Gazi Üniversitesi, Ankara, 2005.

[37]. Türkiye Bilişim Derneği (TBD), Kamuda Karar Destek Sistemlerinin Kullanımı ve Bir Model Önerisi, Kamu Bilgi İşlem Merkezleri Yöneticileri Birliği, Kamu Bilişim Platformu XII, Antalya, 2010.

[38]. N. Demirci, Karar Destek Sistemlerinin Bir Durum Çalışmasına Uygulanması. Yayımlanmamış Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, Trakya Üniversitesi, Edirne, 2012.

[39]. N. M. M. Noor, A. F. Ghazali and Y. M. Saman "Decision Support Systems for Forensic Science in Crime Investigation" International Journal of Digital Content Technology and its Applications, 2013, 7.16: 26.

[40]. N. A. Mutawa, J. Bryce, Virginia N.L. Franqueira, A. Marrington, J. C. Read, Behavioural Digital Forensics Model: Embedding Behavioural Evidence Analysis into the Investigation of Digital Crimes Digital Investigation, Volume 28, Pp 70-82, 2019.

[41]. H. A. Doğanay, "Mobil Cihaz Adli Bilişiminde Karşılaşılan Güncel Zorluklar ve Delil Zinciri", Legem Yayıncılık, 2020.