Fırat Üniversitesi Müh. Bil. Dergisi
32(1), 147-156, 2020

Android Cihazların Adli Bilişim Analizlerinde Parola Tespitine Bağlı Yeni Süreç Tanımlama Modelinin Geliştirilmesi

Ömer Faruk YAKUT [1] , Fatih ERTAM[2*]
[1] Adli Bilişim Bölümü, Teknoloji Fakültesi, Fırat Üniversitesi, Elazığ
[2] Adli Bilişim Bölümü, Teknoloji Fakültesi, Fırat Üniversitesi, Elazığ
[1]172144104@firat.edu.tr, *[2]fatih.ertam@firat.edu.tr

(Geliş/Received: 01/09/2019; Kabul/Accepted:06/02/2020)

Öz: Android işletim sistemin mobil işletim sistemi pazarına hâkim olması ile Android cihazlardan veri toplama yöntemi, mobil adli bilişim teknolojisi üzerine yapılan araştırmaların odak noktası olmuştur. Bununla birlikte, Android işletim sistemi sürümlerinin sürekli güncellenmesi ve güvenlik teknolojilerinin devreye alınması nedeniyle, mevcut veri toplama yöntemleri yeni Android mobil cihazları desteklememektedir. Bu sorunu çözmek için Android akıllı telefonların donanım ve yazılım güncelleme protokollerinin analizi ile özel kurtarma görüntüleri yüklemeye dayanan yeni adli kopya alma yöntemleri geliştirilmelidir. Ancak bu yöntemlerin yeni riskleri de beraberinde getirdiği bilinmeli ve işlemler sırasında gerekli önlemlerin alınması gerekmektedir. Bu çalışmada daha önce geliştirilen adli bilişim inceleme süreçlerine katkı yapabilmek için yeni bir süreç tanımlama modeli geliştirilmiştir. Bu amaçla mobil cihazların üzerindeki ekran izlerinden desen ve pin tespitine yönelik çalışmalar ile ilişkili yeni bir süreç model önerisi sunulmuştur. Geliştirilen model ile adli bilişim analizlerinin elde etme aşamasında şifreli olduğu için adli kopyası alınamayan mobil cihazların şifre ve pin tespitini mevcut yöntemlerin dışında tespit edilmesi amaçlanmıştır. Ayrıca çalışmanın analiz aşamasında ortaya çıkan şifrelenmiş verilerin şifrelerinin çözülmesine katkı sağlayacağı düşünülmektedir.

Anahtar kelimeler: Adli soruşturma modelleri, mobil adli bilişimi, Android cihazlar, mobil ekran izleri, şifre tespiti.

Developing a New Process Recognition Model Based on Password Detection in Forensic Analysis of Android Devices

Abstract: Android operating system dominates the mobile operating system market. The data collection method of Android devices is the focus of research on mobile forensic information technology. However, due to the constant updating of the Android system version and the introduction of security technologies, existing data collection methods do not support new Android mobile devices. To solve this problem, new forensic copying methods should be developed based on the analysis of the firmware update protocols of Android smartphones and uploading custom recovery images. However, it should be known that these methods bring new risks and necessary precautions should be taken during the transactions. In this study, a new process definition model has been developed in order to contribute to the forensic IT review processes developed previously. For this purpose, a new process model proposal related to the studies on pattern and PIN detection from screen traces on mobile devices is presented. With the developed model, it is aimed to determine the password and PIN detection of mobile devices that cannot be forensic copies since the forensic information analysis is encrypted at the stage of obtaining. In addition, it is thought that it will contribute to the decryption of the encrypted data generated during the analysis phase of the study.

Key words: Forensic investigation models, mobile forensics computing, android devices, mobile screen traces, password detection.

1. Giriş

Bilgisayar ve ağ teknolojilerinde yaşanan gelişmeler ile birlikte suçlular, adli bilişim yöntem ve tekniklerinin daha fazla farkına varmakta ve suçlarını işlemek için bilgisayar ve bilgisayar ağlarını daha karmaşık bir şekilde kullanmaktadır [1]. Bilgisayar aygıtları arasındaki farklı nitelikler nedeniyle adli bilişim kavramı "Bilgisayar Adli Bilişimi, Hafıza Adli Bilişimi, Multimedya Adli Bilişimi, Ağ Adli Bilişimi, Küçük Ölçekli Cihaz Adli Bilişimi veya Mobil Cihaz Adli Bilişimi" olarak farklı alt alanlara ayrılmıştır. Buna bağlı olarak her bir alt alanda dijital kanıt elde etmek için kullanılan yöntem, araçlar ve karşılaşılan zorluklarda farklılaşmaktadır.

Gelişen mobil cihaz teknolojisi getirdiği birçok kolaylık ve yenilik ile hayatın vazgeçilmez bir parçası olmayı başarmıştır. Dünya üzerinde cep telefonu kullanıcı sayısında meydana gelen artışa paralel olarak mobil cihaz teknolojisi büyük bir ivme kazanmıştır. "HootSuite" ve "We Are Social" in yayınladığı "Digital in 2019"

* Sorumlu yazar: fatih.ertam@firat.edu.tr , Yazarların ORCID Numaraları: [1] 0000-0001-7958-4499, [2] 0000-0002-9736-8068

raporlarına göre 5,112 milyar mobil cihaz kullanıcısı olduğu ve bu sayının toplam dünya nüfusunun %67 sini oluşturduğu belirtilmektedir [2].

Mobil cihaz teknolojisindeki devrim niteliğindeki donanım ve yazılım tabanlı gelişmeler bu cihazları kullanıcısının özel, kurumsal ve kamusal işlerinin büyük kısmını yürüttüğü ve takip ettiği taşınabilir bilgisayar haline gelmesine sebep olmuştur. Bu özellikleri ile kişisel bir bilgi kümesi barındıran mobil cihazlar siber saldırıların hedefi haline gelmeleri ve suç soruşturmalarında suç ile ilgili veri barındırma ihtimalleri taşımaları sebebiyle adli bilişimin konusu haline gelmiştir.

Cep telefonlarından veri toplanması son yıllarda daha önemli bir hale gelmiştir. Ancak bu kazanımı elde etmek akıllı cihaz teknolojisinin artmasıyla ve güvenlik açıklarının kapatılmasıyla gittikçe zor hale gelmektedir [3]. Bu durum adli kopya alma yöntemlerini ve adli kopya içerisindeki verilerin analiz süreçlerini olumsuz şekilde etkilemeye devam etmektedir.

Adli bilişim alanının dijital materyallerden adli kopya alma ve alınan adli kopyaları görüntüleme ve yorumlanması, pazarlanan yazılım uygulamaları ve adli araçlara tamamen bağımlıdır [4]. Adli araçların yeterlilikleri ile ilgili test işlemlerini gerçek ve tam anlamı ile gerçekleştirecek bir kurumun varlığı adli araç takımlarına duyulan güvene bir standart getirecektir. Bu konuda en dikkat çeken proje Ulusal Standartlar ve Teknoloji Enstitüsü'nün (NIST) Bilgisayar Adli Tıp Aleti Testi (CFTT) Projesi'dir. CFTT projesi 2000 yılından bu yana faaliyettedir. Disk görüntüleme, medya hazırlığı, dosya oyma ve anahtar terim görevlerini kapsayan, adli bilişim araçları takım performansını potansiyel olarak doğrulamak ve değerlendirmek için sağlam test metodolojileri oluşturmaya çalışmaktadır [5]. Ancak bu çalışmalarda elde edilen test sonuçları açıklanma süreci boyunca araçların test edilen versiyonlarının kullanılmaya devam edileceği, hatta ticari aracın bu süre zarfında yeni versiyona geçmiş olma ihtimallerinin de olduğu düşünülürse CFTT testi tarafından herhangi bir olumsuzluk tespit edilse dahi bu araçların kullanımının önüne geçemediğinden tam işlevsellik gösteremeyecektir [4]. Bu nedenle adli bilişim alanında daha etkin bir işleyişin gerçekleşebilmesi için devletler, kanun uygulayıcılar, akademik personeller ve bu alanda hizmet veren ticari işletmelerin organik bir ilişki içinde çalışmaları gerekmektedir [6].

Mobil cihaz teknolojisindeki gelişmeler ile birlikte sınırlı işlem ve bellek kaynaklarına sahip, farklı CPU mimarisi ile çeşitli güvenlikli işletim sistemi (OS) sürümlerine sahip mobil cihazların üretilmesi bu cihazların adli kopya edinimi ve analizini zorlaştırmaktadır. Mobil cihaz pazarındaki büyümenin devam etmesi üretici ve model çeşitliliğine neden olduğundan, profesyonel bir araştırmacının, mobil cihazlardan dâhili verileri toplamak için en uygun adli araçları seçmesi gerekmektedir [7]. Örneğin Windows mobil akıllı telefon için adli kanıt kurtarma tekniklerinin karşılaştırıldığı çalışmada mobil cihazda tutulan bilgilerin eksiksiz bir şekilde alınamadığı gibi farklı araçlar ile elde edilen bilgilerin çelişkili olduğu gösterilmiştir [8]. Ayrıca tüm adli araçların avantajlarının yanında dezavantajlarının da olduğu ve tek bir aracın tüm amaçlar için yeterli olmadığı bilinmelidir.

Mobil cihazlar geliştirilen uygulamalar sayesinde basit bir bilgisayarın yapabileceği işleri yapabilen sınırlı hafıza ve işlem gücüne sahip, mobil altyapılarını kullanabilen küçültülmüş bilgisayarlardır. Mobil cihazların çoklu işlem becerilerini gerçekleştirebilmek için Symbian, iOS, Android OS ve Windows Mobile şeklinde farklı işletim sistemleri geliştirilmiştir [9].

Android, Google liderliğindeki Özgür Yazılım Topluluğu (Open Handset Alliance) OHA, olarak bilinen bir grup şirket tarafından açık kaynak kodları ile oluşturulan mobil platformdur. Her ne kadar açık kaynak kodları ile yazılmış olsa da kodların küçük ve önemli kısımları Google tarafından saklı tutulmaktadır [12]. Android 2010 yılından sonraki beş yıldan daha az bir sürede mobil cihaz pazarında baskın işletim sistemi olma başarısı elde etti [10]. IDC tarafından yapılan araştırma sonuçlarına göre 2018 yılı verilerine göre Android işletim sisteminin pazar payı %85,1 seviyesine ulaşmıştır [11].

Android İşletim sistemi, aygıt sürücüleri, ağ altyapısı ve güç yönetimi gibi temel işlevleri desteklemeye yarayan Linux 2.6 tabanlı bir çekirdek üzerinde çalışır. Linux çekirdeği, yerel kütüphaneler, dalvik sanal makinesi (VM) , uygulama çerçevesi ve uygulamalar gibi katmanlardan oluşur [12]. 2019 yılının ilk çeyreğinden itibaren önde gelen uygulama mağazalarında indirilebilecek uygulamaların sayısına ilişkin verilere göre Android uygulama sayısı 2.1 milyon civarındadır [13] . Bu kadar çok uygulamanın olması Android uygulama geliştiricileri topluluğunun bir sonucudur. Dünya çapında 12 milyondan fazla mobil uygulama geliştiricisinin olduğu ve bunların yarısından fazlasının dikkatini Android işletim sistemine odakladığı tahmin edilmektedir [14]. Dolayısıyla halen popüler olan ve pazar payının büyük bir kısmına sahip işletim sistemine sahip akıllı telefonların dijital suç soruşturmalarında karşılaşılma ihtimalide artacaktır. Bu sebeple Android cihazların adli bilişim incelemelerinde yaşanan sorunlar ve kısıtlılıklara karşı üretilen çözüm yöntemleri, etki edeceği dava sayısı göz önüne alındığında daha önemli bir hal almaktadır.

Mobil cihaz teknolojisi gelişmeye ve değişmeye devam ettikçe, farklı tür mobil cihaz türleri ve güvenlik önlemlerine paralel olarak yeni mevcut kılavuzlar ve işlemler periyodik olarak gözden geçirilmeli ve ihtiyaca göre yeni yöntem ve modeller geliştirilmelidir.

2. Literatür Taraması

Adli bilişim süreçleri bilgisayar suçu ile ilgili kanıtların mahkemeye esas olmak üzere bütünlüğünü ve gözetim zincirini koruyarak düzgün bir şekilde sunulmasını sağlamak için oluşturulan bilimsel süreçleridir. Bu süreçlerin nihai amacı ise "neler oldu, kim dâhil oldu, ne zaman gerçekleşti, nerede gerçekleşti, neden oldu ve olay nasıl meydana geldi" sorularını cevaplayabilecek kanıtlar elde etmektir [15].

Literatürde, suç soruşturmalarında olayların yeniden inşasını kolaylaştırmak veya ilerletmek amacıyla dijital kaynaklardan elde edilen kanıtları bilimsel bir yol izleyerek gerçeğe uygun değerlendirilmesi için adli bilişim süreçleri ile ilgili birçok model geliştirilmiştir [16]. Ancak geliştirilen her model kendi alanı içerisindeki sorunlara çözüm üretmek için geliştirilmiştir. Suç soruşturmalarında kanıtların mahkemeye sunulma aşaması genelde kanıtları elde etme, koruma, analiz ve raporlama aşamalarından oluşmaktadır. Adli bilişim soruşturmaları için geliştirilen süreç modelleri de bu temel üzerinde geliştirilmektedir.

2.1 Kruse ve Heiser modeli (2001)

Lucent modeli olarak da bilinen bu model adli bilişim süreçlerini "Elde Etme (Acquire), Belgeleme (Authenticate) ve Çözümleme (Analyse) olarak üç aşamada ele almıştır. Ayrıca ilk harflerinden dolayı literatürde 3A modeli olarak da bilinmektedir. Bu model adli bilişim süreçlerini basit ve genel bir çerçeve ile ele almıştır.

2.2 ABD adalet bakanlığı modeli (USDOJ, 2001)

Dijital kanıtlarla ilişkili suç mahallinin soruşturma sürecini içeren ve acemi katılımcılar için bir rehber haline gelen bu model, daha sonra kolluk kuvvetleri ve diğer kurumlar tarafından dijital kanıtları güvence altına almak ve tanımlamak için de kullanılmıştır.

Bu modelin ilk aşaması, suç mahallinde kapsamlı bir araştırma süreci gerçekleştirdikten sonra kanıtların toplanmasıyla ilgilidir. İkinci aşama, önceki aşamadan toplanan kanıtları şeffaf bir şekilde bir araya getirmek ve kaynağını tanımlamak olan inceleme sürecini içermiştir. Üçüncü aşama, kanıtların kullanılabilirliği ile ilgili analizinin yapıldığı süreçtir. Son aşama ise önceki tüm aşamaların sonuçlarının raporlanması ve tüm süreçte toplanan bilgileri içerir[17]. Bununla birlikte, bu modelin tek kısıtlaması, belirsiz kalması ve düzgün bir şekilde açıklanmamasıdır.

2.3 DFRWS modeli (2001)

Dijital Adli Araştırmalar Çalıştayı tarafından yönetilen ilk büyük ölçekli konsorsiyumda, adli bilişim uzmanları, uygulayıcılar, güvenlik kurumları ve siviller tarafından "Tanımlama, Sunma, Toplama, İnceleme, Analiz Etme ve Raporlama" aşamalarından oluşan altı (6) basamaklı süreç olarak geliştirilmiştir. Bu model adli bilişim süreçlerinin standart ve tutarlı bir iskeletini oluşturmanın yanında teknik ve teknik olmayan kullanıcılar tarafından kolayca anlaşılabilir bir yapıya sahiptir. DFRWS modelinin tanımlama aşaması, bir olaya müdahale etmeden önce adli süreçleri organize etmek için olay öncesi hazırlığı dışarıda bıraktığı için yeterince geliştirilememiştir [18].

2.4 Soyut dijital adli tıp modeli (ADFM, 2002)

2002 yılında dijital adli soruşturma modelini daha da netleştirmek ve sadeleştirmek için DFRWS modeline kanıtları biriktirme konusundaki geleneksel yaklaşımı dâhil ederek yeni bir model geliştirilmiştir. Bu model "Tanımlama, Hazırlık, Yaklaşım Stratejisi, Muhafaza, Toplama, İnceleme, Çözümleme, Sunum ve Delilin İadesi" aşamalarından oluşmaktadır.

Bu modelin ilk aşaması, meydana gelen olayın türünü tanımlamak ve bu modelin amacına ulaşması için tüm yardımı sağlamaktır. İkinci aşama, bu adli modelin kalan aşamalarında kullanılacak yöntem ve prosedürler hakkında hazırlık yapmaktır. Ayrıca, kanıtları toplamak için gerekirse farklı arama emirlerinin hazırlanmasına da rehberlik eder. Üçüncü aşama, kanıt toplama sürecinin beşinci aşamasındaki benimsenecek yaklaşım ve süreçler geliştirmektir. Modelin dördüncü aşaması, potansiyel olarak ilgili delilleri içeren tüm bileşenleri ve cihazları

korumaktır. Cihazları ve bileşenleri içeren kanıtları sağlamlaştırdıktan sonra, fiziksel sahneyi kaydetmek ve prosedürlerin birleştirilmesi için beşinci toplama aşaması kullanılır. Altıncı aşama, işlenen suçun ilgili şüphelisini bulunmasıyla ilgilenen analiz aşamasıdır. Yedinci aşama, denetimin yapıldığı maddelerin önemini analiz etmektir. Sekizinci aşama analiz aşaması ve daha sonraki aşamada gelen sonuçların sunumunu içerir. Son ve dokuzuncu aşama, görevlerin yerine getirilmesinden sonra cihazları ve dijital kaynaklarını gerçek sahibine iade etme sürecini içerir. Tanımlanan bu modeldeki kusur veya boşluk, üçüncü aşamanın bir dereceye kadar ikinci aşamaya oldukça benzer olmasıdır [17].

2.5 Entegre dijital araştırma süreci (IDIP, 2003)

Entegre Dijital Araştırma Süreci olarak adlandırılan bu model adli bilişim araştırması yapmak ve kanıtları toplamak için adli uzmanlar için başka bir rehber haline geldi. Bu model "Hazırlık Aşaması, Dağıtım Aşaması, Fiziksel Suç İnceleme Aşaması, Dijital Suç İnceleme Aşaması ve Gözden Geçirme Aşaması" olmak üzere beş aşamada ele alınmıştır.

Hazırlık aşamasının amacı soruşturma sürecinin geri kalan aşamalarını hazırlanmaktır. İkinci aşama, adli uzmanlara olayı tespit etme ve ardından sertifikalandırma becerisi kazanabilecekleri bir sistem sağlar. Üçüncü aşama, olay yerindeki fiziksel delilleri toplamak, incelemek ve olay sırasında ortaya çıkan eylemlerin keskin gözlemini yapmakla ilgilidir. Dördüncü aşama üçüncü aşamaya benzer olarak fiziksel suç mahalli araştırma aşamasında elde edilen dijital kanıtların incelenmesi ve toplanmasıyla ilgilidir. Beşinci ve son aşama, dijital adli soruşturma sürecinin önceki aşamalarında yapılan tüm analizleri gözden geçirmektedir. Bu modelin ikinci aşamasında meydana gelen olayın belgelendirilmesi ile ilgilenmesi, modelin yaygın olarak kullanılmamasına neden olmuştur. Çünkü dijital suçu daha önce onaylamak imkânsızdır [19].

2.6 Geliştirilmiş dijital araştırma süreç modeli (EDIP, 2004)

Adli bilişim sürecini, IDIP 'dan farklı olarak yinelemeli olarak tasvir eder. Fiziksel ve dijital olay yeri inceleme aşamalarındaki aşamaları yeniden tanımlar. Dağıtım aşamasını yeniden tanımlar ve birincil (şüpheli) ve ikincil (mağdur) suç mahallindeki araştırmaları ayırt eder. Bu model "Hazırlık Aşaması, Dağıtım Aşaması, Geri İzleme Aşaması, Dinamit ve Gözden Geçirme Aşaması" olmak üzere beş (5) aşamada ele alınmıştır

EDIP modeli elektronik ve dijital olmayan teknolojiler için tutarlı ve standartlaştırılmış bir model oluşturmanın yanında gelecekteki dijital teknolojilere uygulanabilir bir çerçeve sunmaktadır. Bu avantajlarının yanında modelin ek alt aşamalarının bazı belirsizlikler içermesi ve bazı faaliyetlerinin birbirinin tekrarı durumunda olması, bu modelin dezavantajları arasında gösterilebilir [20].

2.7 Bilgisayar adli tıp saha triyaj süreç modeli (CFFTPM, 2006)

Bu model kısa bir sürede olay yerinde inceleme ve analiz yapabilmenin yanında araştırmacılara zamana duyarlı potansiyel psikolojik avantaj sağlamaktadır. Modelin odakları: "1. Hemen kullanılabilir kanıt bulun, 2. Akut risk altındaki mağdurları belirleyin, 3. Devam eden soruşturmayı yönlendirin, 4. Potansiyel masrafları belirleyin ve 5. Suçluların topluma yönelik tehlikelerini doğru bir şekilde değerlendirin" şeklindedir.

CFFTPM modeli "Planlama, Triyaj, Kullanıcı Kullanım Profilleri, Kronoloji Zaman Çizelgesi, İnternet Faaliyeti ve Vakaya Özgü Kanıtlar" aşamalarını içerir. Bu altı (6) aşama içerisinde yüksek bir sınıflandırma düzeyi ve her aşamada çeşitli alt görevleri vardır. Bu model hızlı bilgi edinme ve kritik durumlarda araştırma için avantaj sağlamanın yanında, Bu model sadece olay yerinde yapılan araştırma için uygundur. Soruşturma aşamasında sahne dışında ek çalışmalar yapılması gerektiğinde; kanıtlardan ödün verme olasılığı vardır [21].

2.8 Genel bilgisayar adli tıp soruşturma süreci modeli (GCFIPM, 2011)

GCFIPM modeli "Ön işlem, Edinme ve Koruma, Analiz, Sunum ve Son İşlem" aşamaları olmak üzere toplam beş (5) aşamadan oluşmaktadır. Ön işlem aşaması, soruşturmanın başlaması, gerçek zamanlı veri toplama, ilgili makamdan gerekli onayların alınması gibi yürütülen faaliyetleri ele alır.

Edinme ve Koruma aşamasında; tanımlama, toplama, taşıma, depolama ve koruma ile ilgili görevler yerine getirilir. Sonraki adım, adli soruşturmanın çekirdeği olarak kabul edilen analiz aşamasında; elde edilen veriler üzerinde suç kaynağı ve muhtemelen suçu işleyen kişinin tespiti ile ilgili analizler yapılır. Sunum aşamasında; analiz aşamasından elde edilen çeşitli sonuçların kolayca anlaşılan ve yeterli kabul edilebilir bir şekilde desteklenen bir formatta belgelenerek yetkililere raporlanmaktadır. Son olarak, soruşturmanın uygun şekilde

kapatıldığı son işlem aşaması sonrası hak sahiplerine gerekli dijital ve fiziksel kanıtlar verilerek soruşturma süreci gözden geçirilir.

Bu modelin çeşitli adli bilişim soruşturmalarına uygulanabilirliği ve yeni adli bilişim araştırma modelinin geliştirilmesi için iyi bir başlangıç noktası sağlayacak geniş bir çerçeve görevi görmesi avantajları arasında sayılabilir. Öte yandan bu modeldeki aşamalar, diğer modellerin aşamalarının gruplandırılması ile oluşturulmuştur. Sonuçta gruplandırılmış aşamalarda yinelenen faaliyetler ortaya çıkar. Genelleştirilmiş doğası nedeniyle bu modelin bir modelden ziyade bir yönerge çerçevesi olduğu düşünülmektedir [16].

2.9 Diğer modeller

2.9.1 Bulut bilişim için entegre kavramsal dijital adli model (2012)

Bulut ortamındaki adli soruşturmayla ilgili olarak, bu yeni teknoloji cezai faaliyetler için fırsatlar ve kolluk kuvvetlerine zorluklar getirmiştir. Bu çerçevenin diğer modellerden temel farkı, kanıt kaynağı tanımlama, koruma aşaması, inceleme ve analiz aşaması üzerinde uygulanan yineleme özelliğidir. Verilerin bulutta nasıl işlendiğinin merkezi olmayan doğası, araştırmacılar için yeni yıkıcı zorluklar yaratmaktadır [22].

2.9.2 Veri azaltma ve veri madenciliği modeli (2014)

Dijital soruşturmalarda karşılaşılan yeni zorluklar göz önünde bulundurarak adli soruşturma ve adli analizin toplama, azaltılmış depolama alanı, zamanında inceleme, istihbarat, araştırma, bilgi yönetimi, arşiv ve erişim gibi yedi gereksinimini listeler. Bu model dijital adli tıptaki en büyük zorluklardan birinin sürekli artan veri hacmi olduğuna dikkat çekmiştir. Modelin ana fikri, veri indirgeme yöntemini kullanarak verilerin bir alt kümesini elde etmektir. Ana odak noktaları; Triyaj cihazları ve ortamları, daha hızlı indeksleme, veri madenciliği veya istihbarat analizini kullanma potansiyeli sağlama, çapraz vaka analizi, geçmiş vaka verilerinin ve istihbarat analizinin araştırılmasını sağlamak olarak listelenebilir [23].

2.9.3 Nesnelerin interneti tabanlı dijital adli model (2015)

Nesnelerin İnternetinin (IoT) artan yaygınlığı adli bilişim için yeni sorunlar getiriyor. Bu alandaki analiz, muayene ve depolama gibi çeşitli korunması gereken formatların analizini ele almayı amaçlayarak IoT tabanlı araştırmayla ilgili standart bir prosedürü tanımlamaktadır [24].

2.9.4 Saha işleme modeli (2016)

Önerilen son modellerden biri dijital adli alanı çevreliyor. Saha işleme modeli dijital olmayan kanıtları eğitmeye odaklanmıştır. Olay yerinde araştırmanın erken aşamasını yürüten uzmanlar önce ilgili bilgileri analiz ettikten daha sonra laboratuvarda ayrıntılı analizi gerçekleştirmektedir. Yani, geleneksel laboratuvar tabanlı muayenenin bir dizüstü bilgisayar aracılığıyla sahnede yapılabilirliği ve bulut sistemi ile birleştirilmesi ile ilgilenmiştir [25].

2.9.5 D4I - Siber saldırıları incelemek ve araştırmak için dijital adli bilişim modeli (2020)

Siber saldırıların incelenmesi ve araştırılması için önerilen D4I çerçevesi sunulmaktadır. D4I mevcut dijital adli tıp süreçlerinin yerini almak üzere tasarlanmıştır. D4I çerçevesi, saldırının niteliğine, türüne ve karmaşıklığına bakılmaksızın adım adım ve yarı otomatik bir siber saldırı araştırması yöntemi sağlamaktadır. D4I'yi diğer dijital adli tıp süreçleriyle birlikte uygulama yeteneğini sınırlamadan NIST'in 4 aşamalı dijital adli bilişim sürecini kabul ederek düzenlemiştir [15].

2.10 Mobil cihazlar ile ilgili süreç modelleri

Mobil cihazların adli bilişim analizlerinde delillerin sağlıklı bir şekilde analiz edilmesine imkân tanıyan delil elde etme süreci "Veri girişi, Tanımlama, Hazırlama, İzolasyon, İşleme, Doğrulama, Raporlama, Sunum ve Arşiv" olmak üzere dokuz (9) aşamaya ayrılmıştır [26].

Mobil cihazlarda adli incelme süreci ise ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından hazırlanan Mobil Cihaz Adli İnceleme Kılavuzunda; Koruma, Elde Etme, İnceleme/Analiz ve Raporlama olarak Dört (4) aşamada ele alınmıştır [27].

Mobil cihaz inceleme süreçleri temel olarak birbirine benzerdir. Ancak kullanılan adli araç çeşitliliği ve farklı uygulamalar süreç aşamalarında bazı hatalara sebebiyet vermektedir. Bu nedenle bu hataları aza indireceği değerlendirilen temel iki süreç modeli ile bağlantılı farklı süreç model önerileri hazırlanmıştır [28] .

Mobil cihaz analizlerinin başarılı bir şekilde tamamlanabilmesi için mobil cihaz teknolojisindeki hızlı ilerleyiş karşısında temel süreç modellerinin de sürekli geliştirilmesi ve güncel tutulması gerekmektedir. Ayrıca farklı işletim sistemine sahip mobil cihazların farklılıkları göz önüne alınarak özel süreç modellerine ihtiyaç duyulmaktadır.

Bu çalışmanın ana katkıları aşağıdaki gibi verilebilir:

- Literatürde adli bilişim süreç modelleri incelenerek avantaj ve dezavantajları irdelenmiştir.
- Adli bilişim süreçlerinin uygulama alanındaki aksaklıkları tespit edilerek, mobil cihazların ekran izlerinden desen ve pin tespitine yönelik çalışmalar ile ilişkili yeni bir süreç model önerisi sunulmuştur.
- Mevcut güvenlik önlemleri ile bunlara karşılık geliştirilen yeni adli kopya alma yöntemlerine dikkat çekilmiş olup, bu güvenlik önlemlerini atlatmak için cihaz yonga setlerindeki benzerliklerden faydalanılarak ticari araçların desteklediği cihazlar ile desteklemediği cihazların adli kopyalarının alınabileceği süreçler ile ilgili yol haritası ve uygulama aşaması sunulmuştur.
- Mobil cihaz adli kopya formatlarındaki veri farklılıkları ve adli kopya formatları üzerinden yapılan analiz işlemlerindeki kelime aramalarının verdiği sonuçlar karşılaştırılarak, buna karşı alınacak önlemler temel süreçlere eklenmiştir.

3. Materyal ve Metot

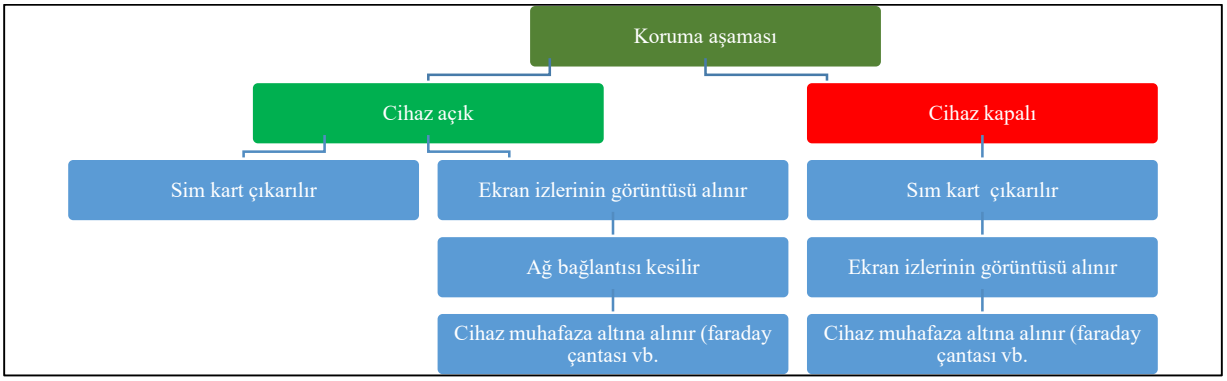
Geleneksel olarak, mobil adli bilişimi hem adli kopya alma hem de analiz aşamasında cihaz üreticisine veya modeline göre farklı özel prosedürler uygulanmasını gerektirir. Cep telefonları çok çeşitli veri yolları, ara yüz ve form faktörleri kullanmanın yanında benzersiz yazılım, bellek düzeni ve depolama teknikleri kullanmaktadır. Bu şaşırtıcı çeşitlilik, adli bilişim analizcilerini birçok kablo ve veri toplama tekniği içeren karmaşık kitlerle cihaz açıklarını sömürmek suretiyle adli kopya ve analiz aşamalarını gerçekleştirmeye mecbur bırakmıştır [12] .

Mobil cihaz adli inceleme süreç modelleri NIST tarafından hazırlanan mobil cihaz adli inceleme rehberinde de belirtilen “Koruma, Elde Etme, İnceleme/Analiz ve Raporlama” aşamaları ile bu aşamaların kendi içinde genişletilmiş formları olan “Veri girişi, Tanımlama, Hazırlama, İzolasyon, İşleme, Doğrulama, Raporlama, Sunum ve Arşiv” şeklinde ele alınmıştır. Önerilen model de ekran izlerinden parola tespit edilmesi ile ilgili çalışmalar ile ilişkili olarak adli bilişim temel süreçlerine alt süreçler dâhil edilmiş ve yeniden düzenlenmiştir.

3.1 Koruma aşaması süreç modeli

Dijital delillere el koyma aşamaları göz önene alınarak bu aşamada alınan önlemlerin, elde etme aşaması sürecini olumlu etkilemesi hedeflenmiştir. Gelişen mobil alt yapı, donanım ve yazılım teknoloji ile Android sürümlerindeki güvenlik açıklarının kapatılması, yeni koruma yöntemlerinin gelişmesini sağlamıştır. Bu nedenle mobil cihazların adli kopyasını almak giderek zorlaşmaktadır. Koruma aşamasında el koyma prosedürleri yerine getirilirken süreç şemasındaki hususlar yerine getirilmesi durumunda elde etme aşamasında bazı zorluklar kısmen de olsa aşılacağı değerlendirilmektedir.

- El Koyma Aşamasında; cihaz açık ya da kapalı olarak karşımıza çıkmaktadır. Her iki durumda ilk olarak cihaz üzerindeki ekran izlerini bozmadan ağ bağlantıları kesilmelidir. Sim kart çıkarılmalı, mümkün değilse ekran izleri alındıktan sonra cihaz uçak moduna alınarak, faraday çantası gibi izole bir ortamda muhafaza edilmelidir. Böylece cihaz uzaktan müdahale yöntemlerine karşı korunmuş olacaktır.
- Cihazın şifreli olup olmadığı kontrol edilerek varsa cihaz parolası devre dışı bırakılmalıdır. Ekran izlerinden tespit edilen olası şifre ve pin ’in tespit edilmesi, elde etme aşamasında en az mantıksal edinim sağlamamızı kolaylaştıracaktır.
- Olası şifre, pin vb. tespiti analiz aşamasında karşılaşılan şifreli dosya, doküman ve veri tabanlarının analiz süreçlerinde de şifre kırma aşmalarında kullanılabilmektedir.

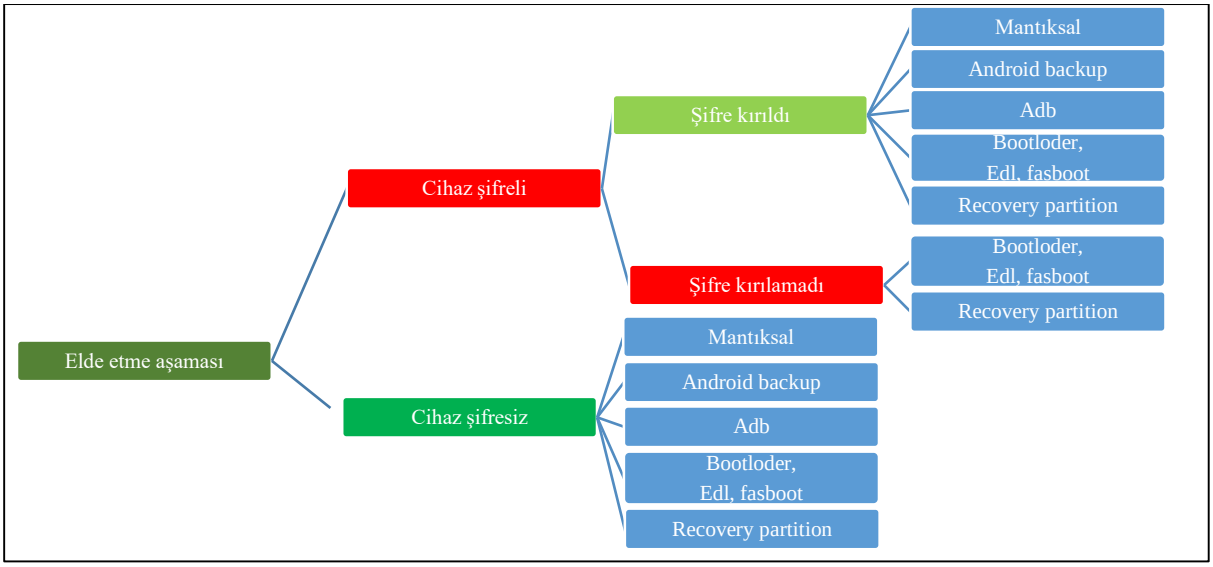


Şekil 1. Koruma aşaması süreç şeması

3.2 Elde Etme süreç modeli

Elde Etme aşaması süreç modelinde; temel alınan prensip cihazın fiziksel kopyasını almaktır. Ancak bazı soruşturmalarda bu yönteme gerek kalmadan cihazın belirli bölümlerindeki verilerin alınması yeterli olabilir. Her iki durumda cihazın fiziksel adli kopyasının alınması silinmiş verileri kurtarma ihtimalini arttıracaktır. Bazı silinmiş verilerin soruşturmanın seyrini ve karar sürecini değiştirebileceği göz önüne alındığında fiziksel adli kopya alınması önemli bir hal almaktadır.

Yeni nesil Android sürümler, cihaz yonga setleri ve güvenlik uygulamaları fiziksel adli kopya alınma sürecinde büyük sorunlara sebebiyet vermektedir. Fiziksel adli kopya alma süreci ile ilgili dikkat edilmesi gereken adımlar aşağıda sıralanmıştır. Adımlar anlatılırken ticari mobil adli araçları kullanılarak gerçekleştirilebilecek yöntemlerden ve araç yetenekleri baz alınmıştır. Elde etme aşamasında cihaz şifreli ve şifresiz olmak üzere iki türlü karşımıza çıkmaktadır. Cihazın şifresiz olduğu durumlarda yapılacak işlemler belli olduğundan şifreli cihazlara uygulanan aşağıdaki süreç, şifresiz cihazlar içinde uygulanabilmektedir.



Şekil 2. Elde etme aşaması süreç şeması.

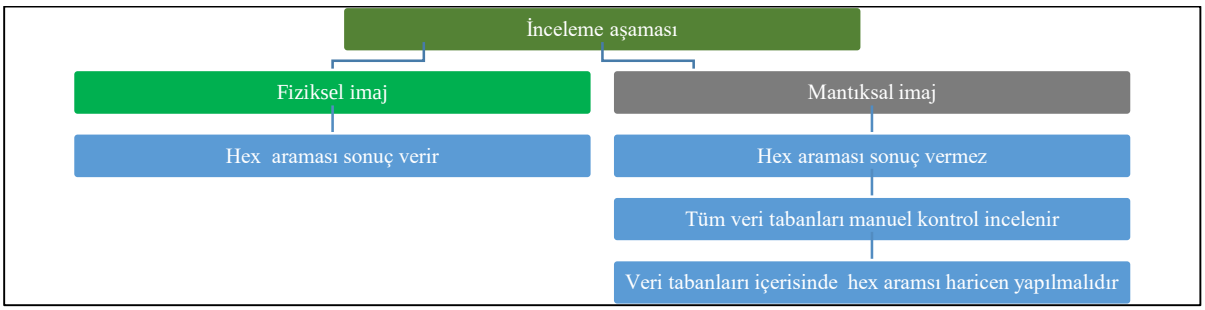
- Android cihazların hepsi veri alışverişini ADB (Android Debug Bridge) komut kütüphanesi komutları ile gerçekleştirmektedir. Bu komutun kullanılabilmesi için cihazın geliştirici seçeneklerinin açılarak USB hata ayıklama modülünün aktif edilmesi gerekir. Bu modül cihazlarda varsayılan olarak kapalı geldiğinden ve

açık olsa dahi cihaz ekranından bu modülün kullanılmasına onay verilmeden bu komutlar kullanılamayacaktır. Bu nedenle şifreli bir cihazın en düşük seviye mantıksal imajını almak mümkün değildir.

- Cihaz şifreli ise ticari mobil yazılımların kilit atlama ve devre dışı bırakma modülleri ile cihaz şifresi atlatılmaya çalışılır.
- Şifre atlatılamıyorsa yazılım güncelleme protokollerine dayanan fiziksel çıkarım yöntemleri olan Bootloader, EDL, Fastboot yöntemlerini destekleyen ticari mobil araç setleri kullanılabilir.
- Kullanılan adli araç elimizdeki şifreli cihazı Bootloader, EDL, Fastboot yöntemlerini desteklemiyorsa diğer yöntemlere geçmeden aynı yonga setini kullanan diğer cihaz modelleri tespit edilmelidir. Tespit edilen yeni modeller için mevcut adli aracın bu modeli destekleyip desteklemediği kontrol edilir. Desteklenen model varsa bu model üzerinden imaj alınmaya çalışılır. Aynı yonga setini kullanan cihaz listesini bulmak için, bu işi yapan web sitelerinden faydalanılabilir [29] . Yapılması gerek mevcut cihaz modelini web sitesinden aratarak yonga seti özelliğini seçmek, web sitesi aynı yonga setini kullanan cihazları bizim için sıralayacaktır.
- Bootloader, EDL, Fastboot yöntemlerini ile imaj alınamaması halinde özel kurtarma görüntüsü yükleme yöntemi ile fiziksel adli kopya alma yöntemi kullanılmalıdır. Ancak bu yöntem riskli bir yöntemdir. FRP kilidi gibi güvenlik yöntemleri risk oluşturmaktadır. Bazı modellerde bu yöntem uygulanırken cihazın fabrika ayarlarına dönmesi muhtemeldir. O yüzden ticari adli araçların bir kısmı bu yöntemi açık cihazlarda geliştirici seçeneklerden FRP kilidini kapattırarak uygulanmasını desteklemektedir.
- Cihaz Android sürümü Android 7 ve üst sürümlerden biri olması halinde yazılım güncelleme protokollerine dayanan fiziksel çıkarım yöntemleri ve özel kurtarma görüntüsü yükleme yöntemleri kullanılarak cihaz kapalı konumda alınan adli kopyalar şifreli geleceğinden veriler analiz aşamasında anlamlandırılamayacaktır.
- Android 7 ve üst versiyon telefonların fiziksel ve dosya sistemli imajları için UFED4PC tarafından Decryping Qualcomm, Decryping MTK, Decryping Bootloader gibi yöntemler geliştirilmiştir. Ancak bu yöntemler daha düşük sürümlerde uygulanması durumunda cihaz yazılımının çökmesi ve bozulması muhtemeldir.
- Ayrıca koruma aşamasında cihaz ürerindeki parmak izleri alınması durumunda izlerden tespit edilecek olası şifre ve pin'ler bu tarz cihazların imajları alınırken ve verilerin şifresi çözülürken kullanılabilir.

3.3 İnceleme aşaması süreç modeli

İnceleme aşaması süreç modelinde; temel alınan ana prensip elde edilen adli kopya formatı ve yapılacak analizin konusudur. Elde edilen adli kopyanın fiziksel kopya olması halinde hafıza erimlerinde yapılacak Hex aramaları sağlıklı sonuçlar verirken, mantıksal kopya formatlarında Hex araması sonuçları kesin sonuçlar olmamaktadır. Bu yüzden mantıksal adli kopya ile çalışıldığında edinilen veri tabanları ile geri görüntüleme günlükleri içerisinde ayrıca inceleme ve Hex araması yapılması sağlıklı bir analiz için gereklidir.

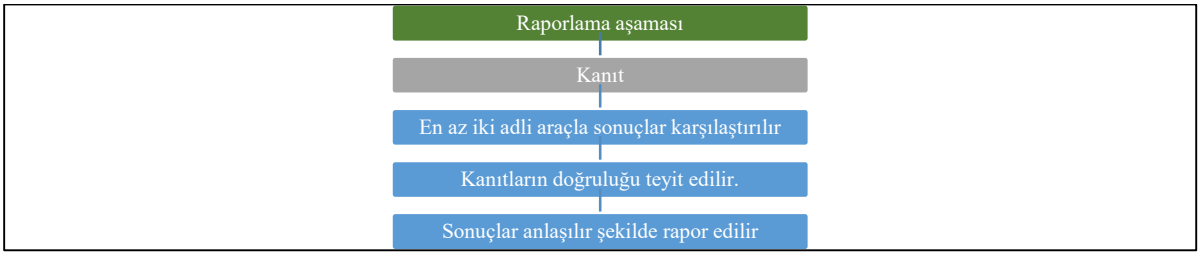


Şekil 3. İnceleme aşaması süreç şeması

3.4 Raporlama aşaması süreç modeli

Raporlama aşaması süreç modelinde; Temel alınan ana prensip analiz süreçlerinin insan ve adli araç faktörüne bağlı olduğu gerçeğidir. Adli araçlar temelde aynı prensiplerde çalışsa da kaynak kodları ve işleyiş farklılığı nedeniyle verileri anlamlandırma ve kurtarma işlemlerinde farklı performanslar sergileyebilmektedir. Bu nedenle

Raporlama sürecinde en az iki farklı adli araç ile kanıtlar ve veriler değerlendirmelidir Raporlama sürecinde en az iki adli araç seti ile veriler teyit edildikten sonra, kanıtların doğruluğu teyit edilmeli ve sonuçlar anlaşılır bir şekilde raporlanmalıdır.



Şekil 4. Raporlama aşaması süreç şeması

4. Sonuç

Bu çalışmada, Android mobil cihazların adli bilişim analizlerinde karşılaşılan zorluklar ve bunlara karşı uygulanacak yöntem ve süreç modellerinden bahsedilmiştir.

Adli bilişim analizlerinin temel amacı suç soruşturmalarına konu olan dijital materyalleri gizlilik, bütünlük ve kabul edilebilirlik kriterlerine uygun olarak toplanması, analiz edilmesi, raporlanması ve arşivlenmesidir. Mobil adli bilişim bu disiplin içerisinde temelde aynı amaca odaklanmıştır. Ancak mevcut marka, model ve işletim sistemi çeşitliliği ile kullanıcı verilerini korumaya yönelik geliştirilen güvenlik önlemleri ve şifreleme yöntemleri mobil adli bilişim analiz süreçlerini olumsuz etkilemektedir. Bu nedenle mobil adli bilişim analizlerinin sağlıklı bir şekilde yürütülmesi cihaza el konulma aşamasından raporlama aşamasına kadar geçen bütün süreçlerin takip edilmesi ile ilişkilidir. Bu temel prensipler ayrıca adli bilişim analizinde delil bütünlüğü ve kanıtların geçerliliklerinin sorgulanması ile ilgili geriye dönük eksiklikler ve ihmaller ilgili bilgilere ulaşmamıza imkân tanıyacağından süreç modellerinin takip edilmesi son derece önemlidir. Ancak temel süreç modellerinin mobil cihaz teknolojilerindeki gelişmeler karşısında genel bir çerçeve çizmenin ötesine geçmediğinden bu süreçlerin ayrıntılı olarak irdelenmesi ve yeni süreç modellerinin geliştirilmesi ihtiyacını doğurmaktadır.

Mobil cihaz kullanıcıların büyük bir kısmı mobil cihazlarını koruma önlemi olarak bir desen, pin, parmak izi, retina ve yüz tanıma gibi güvenlik önlemleri ile koruma altına almaktadır. Ancak yaygın olarak kullanılan yöntem desen ve pin ile oluşturulan şifreleme yöntemleridir. Mobil cihazların geniş ve dokunmatik ekranları kullanıcı parmak izlerini ve desenlerinin rahatlıkla alınabilmesine imkân tanımaktadır.

Bu izlerin başarılı bir şekilde alınarak analiz edilmesi ve şifre tespiti sayesinde mevcut yöntemler ile adli kopyası alınamayan mobil cihazların adli kopyalarını alınmasına imkân sağlayarak, durmuş olan mevcut temel süreçlerin kaldığı yerden devam etmesine imkân tanıyacaktır. Her ne kadar farklı cihaz üreticilerine ait mobil cihazlar farklı gibi gözükse de temelde aynı donanım üreticilerine ait donanımları ve yazılımları kullanmaktadırlar. Bu benzerlik adli kopya alma sürecinde herhangi bir model için desteklenen adli kopya alma yöntemi aynı yonga setini kullanan farklı bir mobil cihaz için desteklenebildiğinden mevcut ticari yazılımların desteklediği modellerden faydalanılarak desteklenmeyen cihazların adli kopyaları alınması mümkün olacaktır. Bu nedenle uygulamada sıkça kullanılan bu hususlarda temel süreçlere entegre edilmiştir.

Mobil cihaz üreticisi olan bazı markalar, belirli bir markanın altyapı ve donanım kaynaklarını kullanarak yeni bir marka oluşturmaktadır. Adli araç setleri asıl markaları desteklediği halde, kopya marka ile ilgili model desteği bulunmayabilir. Bu benzerlik sayesinde kopya markaya ait cihazın adli kopya alma sürecinde, adli aracın desteklediği markaların modellerinden faydalanılabilir. Pratik uygulamalarda bunun birçok kez faydası test edildiğinden bu yöntemlerde temel süreçlere entegre edilmiştir.

Adli bilişim analizlerinde gelinen noktada şifreleme yöntemleri ve güvenlik önlemleri şifre tespit yöntemleri ve bypass yöntemlerine olan ihtiyacı arttırmaktadır. Bu nedenle yukarıda koruma aşamasında bahsedilen ekran izlerinden şifre ve pin tespitine yönelik yapılan çalışmaların başarılı sonuçlar vermesi şifreli olduğu için mevcut araçlar ve yöntemlerle adli kopyası alınamayan mobil cihazlardan adli kopya alınmasına imkân sağlayacağı ve sürecin sorunsuz ilerlemesine imkân tanıyarak, adli makamların karar verme süreçlerini hızlandıracağı değerlendirilmektedir.

Yeni model önerisinde sunulan ve temel süreçlere entegre edilen tecrübeler tamamen durmuş olan yöntemleri yeniden devam ettirmesi bakımından benzersizdir. Bu nedenle önerilen modelin adli uzmanlara fayda sağlayacağı değerlendirilmektedir.

Kaynaklar

[1] Casey E. Handbook of Digital Forensics and Investigation. Handbook of Digital Forensics and Investigation. 2010. 1–17 p.

[2] Digital 2019: Global Internet Use Accelerates - We Are Social [Internet]. [cited 2019 Jul 28]. Available from: https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates

[3] Alendal G, Dyrkolbotn GO, Axelsson S. Forensics acquisition — Analysis and circumvention of samsung secure boot enforced common criteria mode. DFRWS 2018 EU - Proceedings of the 5th Annual DFRWS Europe. 2018;S60–7.

[4] Horsman G. Tool testing and reliability issues in the field of digital forensics. Digital Investigation. 2019;28:163–75.

[5] Guttman B, Lyle JR, Ayers R. Ten years of computer forensic tool testing. Digital Evidence and Electronic Signature Law Review. 2014;8(0):2019.

[6] Casey E. Editorial - A smörgåsbord of digital evidence. Digital Investigation. 2017;23:1–2.

[7] Yates M. Practical investigations of digital forensics tools for mobile devices. In: Proceedings of the 2010 Information Security Curriculum Development Annual Conference, InfoSecCD'10. 2010. p. 156–62.

[8] Grispos G, Storer T, Glisson WB. A comparison of forensic evidence recovery techniques for a windows mobile smart phone. Digital Investigation. 2011;8(1):23–36.

[9] Karataş G, Akbulut A, Zaim AH. Mobil Cihazlarda Güvenlik – Tehditler Ve Temel Stratejiler. İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi,. 2016;15(30):55–75.

[10] Barmpatsalou K, Damopoulos D, Kambourakis G, Katos V. A critical review of 7 years of Mobile Device Forensics. Vol. 10, Digital Investigation. 2013. p. 323–49.

[11] IDC - Akıllı Telefon Pazar Payı - İşletim Sistemi [Internet]. [cited 2019 Jun 15]. Available from: https://www.idc.com/promo/smartphone-market-share/os

[12] Vidas T, Zhang C, Christin N. Toward a general collection methodology for Android devices. In: DFRWS 2011 Annual Conference. 2011.

[13] • App stores: number of apps in leading app stores 2019 | Statista [Internet]. [cited 2019 Jun 16]. Available from: https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/

[14] Opasiak K, Mazurczyk W. (In)Secure Android Debugging: Security analysis and lessons learned. Computers and Security. 2019;82:80–98.

[15] Dimitriadis A, Ivezic N, Kulvatunyou B, Mavridis I. D4I - Digital forensics framework for reviewing and investigating cyber attacks. Array [Internet]. 2020;5(October 2019):100015. Available from: https://doi.org/10.1016/j.array.2019.100015

[16] O. K, Quayson E, Agyei O, Danso E. Survey of Digital Forensic Models and Proposed Thematic Scheme. International Journal of Computer Applications. 2017;169(11):41–5.

[17] Mushtaque K. Digital Forensic Investigation Models, an Evolution study. Journal of Information Systems and Technology Management. 2015;12(2).

[18] Lutui R. A multidisciplinary digital forensic investigation process model. Business Horizons. 2016;59(6):593–604.

[19] Bryant R, Bryant S. Policing digital crime. Policing Digital Crime. 2014. 1–258 p.

[20] Du X, Le-Khac NA, Scanlon M. Evaluation of digital forensic process models with respect to digital forensics as a service. European Conference on Information Warfare and Security, ECCWS. 2017;573–81.

[21] Rogers MK, Goldman J, Mislan R, Wedge T, Debrota S, Rogers MK, et al. Journal of Digital Forensics , Security and Law Computer Forensics Field Triage Process Model Computer Forensics Field Triage Process Model. 2006;1(2):1–21.

[22] Martini B, Choo KKR. An integrated conceptual digital forensic framework for cloud computing. Vol. 9, Digital Investigation. 2012. p. 71–80.

[23] Quick D, Choo KWR. Data reduction and data mining framework for digital forensic evidence: Storage, intelligence, review and archive. Trends and Issues in Crime and Criminal Justice. 2014. p. 1–11.

[24] Perumal S, Md Norwawi N, Raman V. Internet of Things(IoT) digital forensic investigation model: Top-down forensic approach methodology. In: 2015 5th International Conference on Digital Information Processing and Communications, ICDIPC 2015. 2015. p. 19–23.

[25] Hitchcock B, Le-Khac NA, Scanlon M. Tiered forensic methodology model for digital field triage by non-digital evidence specialists. In: DFRWS 2016 EU - Proceedings of the 3rd Annual DFRWS Europe. 2016. p. S75–85.

[26] Murphy CA. Developing Process for Mobile Device Forensics. 2012;1–9. Available from: http://www.mobileforensicscentral.com/mfc/documents/Mobile Device Forensic Process v3.0.pdf

[27] Ayers R, Brothers S, Jansen W. Guidelines on mobile device forensics. 2014; Available from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf

[28] Akalın U. Mobil Cihazlarda Adli Bilişim Çalişmalarina Yönelik Bir Model Önerisi. Gazi Üniversitesi; 2016.

[29] Samsung Exynos 7 Octa 7870 Chipset Kullanan Telefonlar - Epey [Internet]. [cited 2019 Jun 18]. Available from: