ARAŞTIRMA MAKALESİ

ADLİ TIP DERGİSİ
TURKISH JOURNAL OF FORENSIC MEDICINE

Geliş: 22.05. 2025
Kabul: 24.04.2026

Mobil Cihazlarda Son Etkinleştirme Tarihinin Tespit Edilmesi ve Adli Bilişim Açısından Önemi

Detecting Last Activation Date on Mobile Devices and Importance from a Digital Forensics Perspective

Adnan Keçe[1], Mehmet Pala[1], Enes Damar[1], Hasan Tunay[1], Bilal Aman[1]

[1] Adli Bilişim İhtisas Dairesi, Adli Tıp Kurumu, İstanbul, Türkiye

Öz

Amaç: Sıfırlama tarihinin önem arzettiği adli vakalarda adli bilişim uzmanlarının tutarlı ve güvenilir raporlar oluşturması gerekmektedir. Bu çalışma, adli bilişim incelemelerinde Android ve iOS işletim sistemine sahip mobil cihazlarda son etkinleştirme tarihinin güvenilir bir şekilde tespit edilmesini amaçlamaktadır.

Yöntem: Araştırma kapsamında android ve iOS işletim sistemlerine sahip mobil cihazlar fabrika ayarlarına sıfırlanmış ve sıfırlama işleminden sonra cihazların dijital kopyaları alınarak incelenmiştir. Hem Android hem de iOS platformlarındaki sistem ve kullanıcı veritabanı dosyalarının oluşturulma, değiştirilme ve erişim tarihleri ayrıntılı olarak analiz edilmiştir. Ayrıca bu dosyaların sıfırlama işleminden hemen sonra yeniden oluşturulma süreçleri incelenmiş ve dosyaların zaman damgaları karşılaştırılmıştır.

Bulgular: Android cihazlarda özellikle "SetupWizardPrefs.xml", "Google Service Framework" ve "Google Mobile Service" gibi sistem dosyaları; iOS cihazlarında ise, "sms.db", "call_history.db" ve "AddressBook.sqlitedb" gibi dosyaların sıfırlama işlemi sonrasında yeniden oluşturulduğu görülmüştür. Bu dosyaların zaman damgaları son etkinleştirme tarihini belirlemede güvenilir bir referans noktası olarak değerlendirilebilmektedir.

Sonuç: Android ve iOS cihazlarında, fabrika ayarlarına döndürme işlemi sonrası oluşturulan dosyaların zaman damgaları, adli bilişim incelemelerinde son etkinleştirme tarihinin tespiti için önemli kanıtlar sunmaktadır. Bu çalışmada elde edilen bulgular sıfırlama tarihiyle yüksek oranda (dakika bazında) tutarlılık gösterdiği gözlemlenmiştir. Ayrıca her cihazın ve işletim sisteminin kendine özgü veri yapısının dikkate alınması, inceleme sürecinde hata payını en aza indirmeye yardımcı olacaktır.

Anahtar Kelimeler: Adli Bilişim, Son etkinleştirme tarihi, Android, IOS, Dijital Delil, Zaman Damgalar

Abstract

Objective: In forensic cases where the reset date is of significant importance, forensic experts need to produce consistent and reliable reports. This study aims to reliably determine the last activation date on mobile devices with Android and iOS operating systems in forensic examinations.

Method: In the research, mobile devices with Android and iOS operating systems were reset to factory settings, and digital copies of the devices were taken and examined after the reset process. The creation, modification, and access dates of system and user database files on both Android and iOS platforms were analyzed in detail. Additionally, the processes of re-creation of these files immediately after the reset were examined, and the timestamps of the files were compared.

Results: On Android devices, system files such as "SetupWizardPrefs.xml", "Google Service Framework", and "Google Mobile Service" were found to be re-created after the reset process; on iOS devices, files such as "sms.db", "call_history.db", and "AddressBook.sqlitedb" were similarly re-created. The timestamps of these files can be considered a reliable reference point for determining the last activation date.

Conclusion: On Android and iOS devices, the timestamps of files created after the factory reset process provide significant evidence for determining the last activation date in forensic examinations. The findings from this study have observed a high degree of consistency (at the minute level) with the reset date. Additionally, considering the unique data structure of each device and operating system will help minimize the margin of error during the examination process.

Anahtar Kelimeler: Digital Forensics, Last activation date, Android, iOS, Digital evidence, Timestamps

Nasıl Atıf Yapmalı: Keçe A., Pala M., Damar E., Tunay H., Aman B.. Mobil Cihazlarda Son Etkinleştirme Tarihinin Tespit Edilmesi ve Adli Bilişim Açısından Önemi. Adli Tıp Dergisi 2026;40(1):(45-50) https://doi.org/10.61970/adlitip.1703850.

Sorumlu Yazar: Enes Damar, Adli Bilişim İhtisas Dairesi, Adli Tıp Kurumu, İstanbul, Türkiye
E-posta: enes.damar@adalet.gov.tr

GİRİŞ

Günümüz teknolojileri, mobil cihazları hem yüksek işlem kapasitesine sahip bir bilgisayar kadar akıllı ve hızlı, hem de bir cüzdan kadar küçük ve taşınabilir hâle getirmiştir. Bu özellikleri sayesinde mobil cihazlar, bireylerin günlük yaşamlarının ayrılmaz bir parçası hâline gelmiştir (1). Mobil cihazlar aracılığıyla yalnızca iletişim kurmakla kalmamakta; fotoğraf, video ve ses kaydı oluşturma veya izleme, uygulama yükleme ve kullanma, sosyal ağlara bağlanma, belge düzenleme ve paylaşma, konum bilgisi iletme ve internet üzerinde gezinme gibi çok çeşitli kişisel faaliyetler gerçekleştirilebilmektedir (2).

Mobil cihazların diğer teknolojik aygıtlardan ayrılan en önemli özelliklerinden biri, genellikle tek kullanıcıya ait olması ve kişisel bir aygıt olarak kabul edilmesidir (3). Aktif olarak kullanılan mobil cihazlar; arama geçmişi, konum bilgileri, mesajlar, fotoğraflar gibi kullanıcıya ait hassas veriler barındırmakta ve bu nedenle adli incelemelerde önemli bir bilgi kaynağı olarak değerlendirilmektedir (4,5).

Bununla birlikte, olası bir adli soruşturma ihtimali karşısında şüpheliler, cihazlarını fabrika ayarlarına döndürerek hızlı ve kolay biçimde sıfırlama yoluna gidebilmektedir (6). Bilişim teknolojilerinin günlük yaşamda yoğun olarak kullanılması, dijital ortamda işlenen suçların da çeşitlenmesine yol açmıştır (7). Bu suçlar arasında; kimlik hırsızlığı, kişisel bilgilerin yetkisiz erişimle ele geçirilmesi, taciz, çevrimiçi zorbalık, uyuşturucu ve silah ticareti ile sosyal mühendislik gibi yöntemlerle bilgi sızdırma yer almaktadır. Söz konusu suç tiplerindeki artış, adli bilişim çalışmalarının önemini daha da artırmaktadır (8).

Teknolojinin gelişmesi, dijital ortamda işlenen suçların hem uygulanma hem de yorumlanma süreçlerini karmaşık hâle getirmiştir (9). Bu nedenle, dijital delillerin incelenmesi belirli prosedürler dâhilinde yürütülmelidir.

Årnes ve arkadaşları, adli bilişimi; suç teşkil eden olayların çözümünü kolaylaştırmak amacıyla dijital kaynaklardan elde edilen kanıtların incelenmesine yardımcı olan disiplinler arası bir bilim dalı olarak tanımlamışlardır (10). Ayrıca, belirli bir olay veya suç hipotezini destekleyebilecek ya da çürütebilecek güvenilir bilgileri içeren her türlü dijital veriyi "dijital kanıt" olarak ifade etmişlerdir.

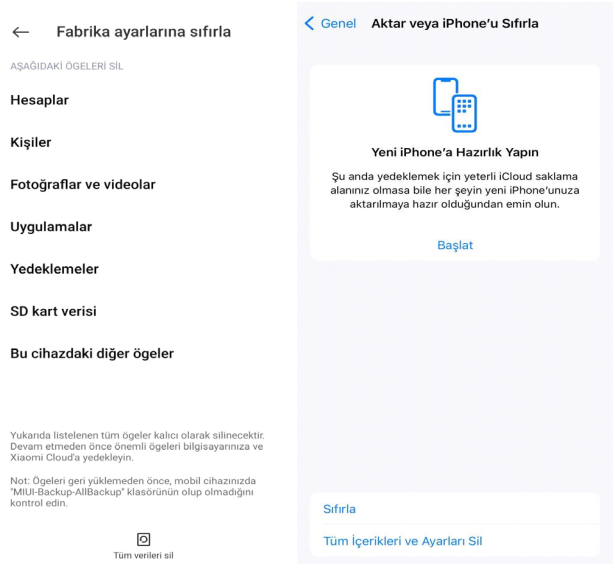
Dijital ortamda kullanılan cihazlar arasındaki teknik farklılıklar, adli bilişim alanında çeşitli alt disiplinlerin gelişmesine yol açmıştır. Bunlardan biri de Mobil Cihaz Adli Bilişimidir. Bu alanda yapılan incelemeler; cep telefonları, tabletler, SIM kartlar ve Android veya iOS işletim sistemine sahip taşınabilir cihazlar üzerinde yoğunlaşmaktadır (11). İnceleme kapsamı, olayın niteliğine göre kullanıcı verileri ile sistem verilerini birlikte veya ayrı ayrı kapsayabilmektedir (12).

Bu çalışmada, Android ve iOS işletim sistemine sahip mobil cihazların son sıfırlanma tarihini belirlemek amacıyla, farklı sürümlere sahip cihazlar üzerinde gerçekleştirilen testlerin sonuçları değerlendirilmiştir.

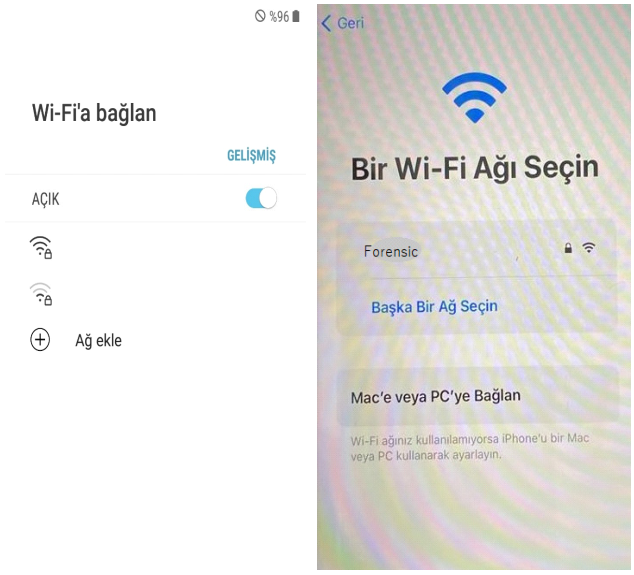
GEREÇ VE YÖNTEM

Bu çalışmada, mobil cihazların etkinleştirme tarihini belirlemek amacıyla cihazlardan elde edilen dijital kopyalar ayrıntılı biçimde analiz edilmiştir.

Mobil cihazlarda fabrika ayarlarına döndürme işlemi, ayarlar menüsünde yer alan sıfırlama seçenekleri veya kurtarma bölümü aracılığıyla gerçekleştirilebilmektedir. Bu çalışmada, her iki işletim sistemine sahip test cihazları fabrika ayarlarına döndürülmüş, kurulum süreçleri tamamlanmış ve elde edilen bulgular değerlendirilmiştir. Kullanıcılar tarafından en sık tercih edilen sıfırlama yöntemi, Şekil 1'de görüldüğü üzere, cihazın kendi



Şekil 1. Android sıfırlama menüsü ve iOS sıfırlama menüsü



Şekil 2. Android kurulum ekranı ve iOS kurulum ekranı

sıfırlama menüsü aracılığıyla yapılmaktadır.

Android ve iOS işletim sistemlerinde, sıfırlama sonrası cihazın yeniden kullanılabilmesi için Kurulum Sihirbazı tamamlanmak zorundadır. Bu sihirbaz; dil seçimi, Wi-Fi bağlantısı, hüküm ve koşulların onaylanması, tarih-saat ayarı, cihaz isminin belirlenmesi ve cihaz koruma seçeneklerinin yapılandırılması gibi adımları içermektedir. Yapılan bu ayarlar, cihaz içerisindeki ilgili sistem ve veritabanı dosyalarına kaydedilmektedir (17).

Sıfırlama işlemi sonrasında, bazı sistem ve veritabanı dosyaları kurulum aşamasında yeniden oluşturulmakta veya güncellenmektedir (15,16). Bu dosyaların oluşturulma, değiştirilme ve son erişim tarihleri, cihazın son etkinleştirilme zamanı hakkında kritik ipuçları sağlamaktadır. Kurulum sihirbazında Wi-Fi bağlantısı ve diğer başlangıç ayarlarının yapılması, özellikle Wi-Fi ile ilişkili sistem dosyalarının etkinleştirme tarihine dair önemli bilgiler sağlamaktadır. Şekil 2'de, Android ve iOS işletim sistemine sahip cihazlarda Wi-Fi ve diğer ayarların yapılandırıldığı ekran görüntüleri yer almaktadır.

Şekil 3. Android kurulum sonrası ve iOS kurulum sonrası genel görünüm

Kurulum işlemi tamamlandığında, cihazın önyüklü uygulamalarına ait genel görünüm Şekil 3'te sunulmuştur.

Burada; arama, SMS, internet tarayıcı, müzik,

e-posta, saat ve takvim gibi temel uygulamaların kurulum aşamasında otomatik olarak yüklendiği gözlemlenmiştir. Kurulum sonrası oluşan sistem ve veritabanı dosyalarının zaman damgalarını incelemek amacıyla, tüm cihazların dijital kopyaları alınmış ve analiz edilmiştir.

BULGULAR

Bu çalışmada, Android ve iOS işletim sistemine sahip mobil cihazlar üzerinde gerçekleştirilen testler sonucunda elde edilen bulgular, ayrı başlıklar altında değerlendirilmiştir. Analizlerde öncelikli olarak, sıfırlama sonrası ilk açılışta çalışan Kurulum Sihirbazı ayarlarının saklandığı dosyalar ile kurulum aşamasında yüklenen temel uygulamalara ait dosyalar incelenmiştir.

Android İşletim Sistemine Ait Bulgular

Android işletim sistemine sahip cihazlarda fabrika ayarlarına döndürme işlemi üç farklı yöntemle gerçekleştirilebilmektedir:

Yöntem 1: Cihazın ayarlar menüsünden "Fabrika ayarlarına dön" seçeneğinin kullanılması.

Yöntem 2: Cihazın recovery bölümünden wipe data/factory reset komutunun uygulanması.

Yöntem 3: Üçüncü taraf yazılımlar (ör. TWRP) aracılığıyla telefon belleğinin tamamen silinmesi (wipe işlemi).

Kurulum aşamasında Android cihazlarda SetupPrefWizard.xml isimli bir konfigürasyon dosyası oluşturulmaktadır. Bu dosyanın oluşturulma tarihi, son etkinleştirme zamanının tespitinde kritik bir göstergedir. Nitekim Cellebrite UFED adli bilişim inceleme yazılımı da son etkinleştirme tarihini belirlerken bu dosyanın zaman damgasını referans almaktadır. Android 6.0 sürümünün altında ise com.google.android.setupwizard klasörünün oluşturulma tarihi de kullanılabilmektedir. Ancak Android sürümlerindeki değişiklikler, bu dosyalara erişim imkânını her zaman garanti etmemektedir. Bu nedenle, son etkinleştirme tarihinin güvenilir şekilde belirlenebilmesi için birden fazla dosyanın zaman damgasının karşılaştırılması gerekmektedir.

Yapılan incelemeler sonucunda, sıfırlama işlemi uygulanmış cihazlardan elde edilen dijital delil kopyaları üzerinde bazı veritabanı dosyalarının "Oluşturulma Tarihi" meta verisinin, olayın gerçekleşme zamanı ile uyumsuz biçimde sabit bir zaman damgası içerdiği tespit edilmiştir.

Bu durumun temel nedeni, söz konusu dosyaların cihazın ilk kurulum aşamasında, henüz ağ tabanlı zaman senkronizasyonu (NITZ/NTP) gerçekleşmeden önce oluşturulmuş olmasıdır. Bu aşamada cihaz, geçerli zaman bilgisine sahip olmadığından, dosya sistemi işlemlerinde varsayılan bir zaman damgası kullanmaktadır. Bu varsayılan değer, sistem saatinin sıfırlandığı durumlarda bilişim sistemleri için evrensel bir başlangıç noktası olan 01 Ocak 1970 "Unix Epoch" tarihi olabildiği gibi, metinde örneklendiği gibi 01.01.2020 gibi daha ileri bir tarihin kullanıldığı durumlarda ise Android işletim sisteminin o sürümünün derlendiği ve yazılıma sabitlendiği "build time" değerini yansıtmaktadır.

Dolayısıyla, cihazın 2023 veya 2024 gibi daha ileri bir tarihte yeniden kurulması durumunda dahi, bu dosyalara ait "Oluşturulma Tarihi" bilgisinin değişmeyerek bu varsayılan değerlerden birini koruması mümkündür. Bu nedenle, adli bilişim analizlerinde zaman çizelgesi oluşturulurken, bu tür dosyaların "Oluşturulma Tarihi" verisinin tek başına güvenilir bir kanıt olarak değerlendirilmemesi; diğer zaman damgaları (örneğin "Değiştirme Tarihi") ile birlikte bütüncül bir yaklaşımla yorumlanması büyük önem taşımaktadır.

Tablo 1. Android veritabanı

Veritabanı	Oluşturma Tarihi	Değiştirme Tarihi
celander.db	1.01.2020 00:04:30(UTC+3)	8.08.2024 10:26:40(UTC+ 3)
gass.db	1.01.2020 00:04:15(UTC+3)	8.08.2024 10:38:33(UTC+3)
google_account_history.db	8.08.2024 10:23:36(UTC+3)	8.08.2024 10:23:36(UTC+3)
googlesettings.db	1.01.2020 00:03:58(UTC+3)	8.08.2024 10:38:09(UTC+3)
library.db	8.08.2024 10:23:40(UTC+3)	8.08.2024 10:27:08(UTC+3)
localappstate.db	1.01.2020 00:04:03(UTC+3)	8.08.2024 10:38:33(UTC+3)
SetupWizard_Prefsxml	8.08.2024 10:25:46(UTC+3)	8.08.2024 10:25:46(UTC+3)
WifiConfigStore.xml	8.08.2024 10:21:44(UTC+3)	8.08.2024 10:21:44(UTC+3)

iOS İşletim Sistemine Ait Bulgular

iOS cihazlarda sıfırlama işlemi iki farklı yöntemle gerçekleştirilebilmektedir:

Yöntem 1: Cihaz ayarları içerisinden, "iPhone'u Aktar veya Sıfırla" menüsünde yer alan "Tüm İçerikleri ve Ayarları Sil" seçeneğinin kullanılması.

Yöntem 2: Cihazın kurtarma moduna alınarak, iTunes üzerinden "Güncelle" seçeneği ile sıfırlama yapılması.

Sıfırlama sonrasında iOS cihazlar da Kurulum Sihirbazı aracılığıyla yeniden yapılandırılmaktadır. Örneğin, iPhone 4 model cihazlarda sıfırlama sonrası sistem tarafından .obliterated adlı, boyutu sıfır byte olan bir dosya oluşturulmaktadır.

Testler, iOS cihazlarda da Android'e benzer şekilde, sıfırlama sonrası oluşturulan veya değiştirilen sistem ve veritabanı dosyalarının etkinleştirme tarihinin belirlenmesinde kullanılabileceğini göstermiştir. Bu dosyaların adları iOS sürümüne göre farklılık gösterebilmekle birlikte, genel işlevleri benzerdir. Etkinleştirme tarihi tespitinde yararlanılabilecek bazı temel dosyalar tablo 2'de gösterilmiştir.

Tablo 2. IOS Veritabanı

Veritabanı	Oluşturma Tarihi	Değiştirme Tarihi
sms.db	11.08.2024 10:50:42(UTC+3)	11.08.2024 10:55:12(UTC+3)
AdressBook.sqlitedb	11.08.2024 10:52:22(UTC+3)	11.08.2024 10:56:47(UTC+3)
call_history.db/CallHistory.storedata	11.08.2024 10:50:35(UTC+3)	11.08.2024 10:52:38(UTC+3)
voicemail.db	11.08.2024 10:49:57(UTC+3)	11.08.2024 10:53:28(UTC+3)
notes.sqlite/NoteStore.sqlite	11.08.2024 10:48:44(UTC+3)	11.08.2024 10:49:51(UTC+3)

TARTIŞMA VE SONUÇ

Mobil cihazların sıfırlanma veya etkinleştirilme tarihinin doğru biçimde belirlenmesi, hukuki ve teknik açıdan kritik bir öneme sahiptir. Bu çalışmada elde edilen bulgular, tek bir kaynağa dayalı tespitlerin yetersiz kalabileceğini, güvenilir bir sonuca ulaşmak için en az üç farklı veritabanından elde edilen zaman damgalarının karşılaştırılması gerektiğini ortaya koymuştur.

Cihazların ayarlar menüsünde bulunan "Fabrika ayarlarına dön" seçeneği, kullanıcı tarafından yüklenmiş tüm uygulamaları, medyaları ve ayarları silerek cihazı varsayılan duruma getirmektedir. Ancak,örneğin Android cihazlarda, kullanıcıların şifre değişiklikleri gibi işlemler de keychain dosyasının değiştirilme tarihini etkileyebilmektedir. Bu durum, dosya değişim zamanının yalnızca fabrika ayarlarına döndürülme işleminden mi, yoksa kullanıcı tarafından yapılan başka bir işlemden mi kaynaklandığının net olarak ayırt edilmesini

güçleştirmektedir.

Buna karşın, kullanıcılar tarafından değiştirilemeyen sistem dosyalarına ve veritabanlarına dayalı tespitler daha güvenilir sonuçlar sunmaktadır. Özellikle, kurulum süreci sırasında zorunlu olarak çalışan Kurulum Sihirbazı, arka planda yeni dosyaların oluşturulmakta ve bu dosyalar etkinleştirme tarihinin belirlenmesinde kritik ipuçları barındırmaktadır. Örneğin, yaygın olarak kullanılan adli bilişim analiz araçlarında, etkinleştirme tarihinin belirlenmesinde SetupWizardPrefs.xml dosyasının oluşturulma zamanı referans alınmaktadır.

Son etkinleştirme zamanının kesin olarak tespit edilebilmesi için, kullanılan dosya ve veritabanlarının oluşturulma tarihleri mümkün olduğunca aynı yıl/ay/gün/saat/dakika aralığında olmalıdır. Bu bağlamda, adli bilişim uzmanlarının yazılımların otomatik sunduğu tarihleri raporlamadan önce mutlaka kendi tespitlerini yapmaları ve en az üç farklı bulguyu karşılaştırarak değerlendirmeleri gerekmektedir.

Bildirimler

Bu çalışma daha önce herhangi bir yüksek lisans ya da doktora tezinde kullanılmamıştır.

Çıkar çatışması

Yazarlar arasında herhangi bir çıkar çatışması bulunmamaktadır.

Finansal destek

Bu çalışma herhangi bir kurum ya da kuruluş tarafından maddi olarak desteklenmemiştir.

KAYNAKLAR

1. Kukulska-Hulme A, Pettit J, Bradley L, Carvalho AA, Herrington A, Kennedy DM, et al. Mature students using mobile devices in life and learning. Int J Mob Blended Learn. 2011;3(1):18–52.

2. Halvey M, Keane MT, Smyth B. Time based patterns in mobile-internet surfing. In: Grinter R, Rodden T, Aoki P, Cutrell E, Jeffries R, Olsen G, editors. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. New York (NY): ACM; 2006. p. 31–34.

3. Cameron D. The rocket in your pocket: how mobile phones became the media by stealth. In: Second Joint Journalism Education Association/ Journalism Education Association of New Zealand Conference; 2006 Dec; Auckland, New Zealand. p. 4–7.

4. Laurila JK, Gatica-Perez D, Aad I, Bornet O, Do TMT, Dousse O, et al. The mobile data challenge: big data for mobile computing research. IEEE Pervasive Comput. 2012;11(2):24–31.

5. Doherty EP. Digital forensics for handheld devices. Boca Raton (FL): CRC Press; 2013.6. Schwamm R. Effectiveness of the factory reset on a mobile device [dissertation]. Monterey (CA): Naval Postgraduate School; 2014.

7. Felka P, Mihale-Wilson C, Hinz O. Mobile phones and crime: the protective effect of mobile network infrastructures. J Quant Criminol. 2020;36(4):933–956.

8. Dweikat M, Eleyan D, Eleyan A. Digital forensic tools used in analyzing cybercrime. J Univ Shanghai Sci Technol. 2021;23(3):367–379.

9. Smith R. Crime in the digital age: controlling telecommunications and cyberspace illegalities. London: Routledge; 2018.

10. Årnes A, editor. Digital forensics. Hoboken (NJ): John Wiley & Sons; 2017.

11. Ahmad N, Boota MW, Masoom AH. Comparative analysis of operating system of different smart phones. J Softw Eng Appl. 2015;8(3):114–126.

12. Nigrini MJ. Forensic analytics: methods and techniques for forensic accounting investigations. Hoboken (NJ): John Wiley & Sons; 2020.

13. Ayers R, Brothers S, Jansen W. Guidelines on mobile device forensics (draft). NIST Spec Publ. 2013;800-101.

14. Ambler SW, Sadalage PJ. Refactoring databases: evolutionary database design. Boston (MA): Pearson Education; 2006.

15. Shukla U, Mandal B, Kiran KVD. Perlustration on mobile forensics tools. In: Proceedings of the Third International Conference on Computer Networks and Inventive Communication Technologies (ICCNCT 2020); 2021; Singapore. p. 845–856.