Journal of the Faculty of Engineering and Architecture of Gazi University 39:3 (2024) 1637-1647

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University

Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

Examination of MAC address records of phones connected to the macOS computer

Tümay Kurtca[1]*, Refik Samet[2]

[1]Department of Computer Forensics, Graduate School Of Informatics Engineering, Gazi University, 06500, Ankara, Türkiye
[2]Department of Computer Engineering, Faculty of Engineering, Ankara University, 06830, Ankara, Türkiye

Highlights:

- Analyze the MAC address records
- Identify the problems encountered during the analysis
- Detect MAC addresses by the suggested analysis method

Keywords:

- Digital Forensic
- MacOS
- MAC address
- iOS
- ANDROID

Article Info:

Research Article
Received: 05.07.2022
Accepted: 25.08.2023

DOI:

10.17341/gazimmfd.1140690

Acknowledgement:

The authors would like to thank The Gendarmerie Forensic Department for their support in this study.

Correspondence:

Author: Tümay Kurtca
e-mail: tkurtca@gmail.com
phone: +90 312 202 3801

Graphical/Tabular Abstract

In forensic content examination, it is important to support electronic devices such as personal computers and mobile phones with the detection of MAC addresses. However, as a result of the examinations made with forensic examine software, it has been observed that the MAC address records that have fallen into the operating system cannot always be detected completely. In this study, suggestions for examination have been made. The Table A below shows an example of this situation.

Table A. Results determined by the examiner software and the results determined after the suggested analysis method

MAC addresses of phones with iOS operating system with network connection via USB	Examine software results	MAC addresses detected by the suggested analysis method
98:00:C6:42:A5:03	3E:2E:FF:41:60:A0	98:00:C6:42:A5:03
B4:9C:DF:01:B3:DD		B4:9C:DF:01:B3:DD
3C:2E:FF:41:60:A0		3C:2E:FF:41:60:A0

Purpose:
The aim of this study is to analyze the MAC address records of the phones connected to a computer with MacOS, to identify the problems encountered during the analysis and to offer solutions to these problems.

Theory and Methods:
This article suggests a methodology consisting of the preparation of the working environment, the collection of data, the analysis of the data and the evaluation of the results. In accordance with this methodology, a total of ten different applications were used by phones with iOS and ANDORID operating systems.

Results:
Obtained results showed that the MAC address records falling to the operating system did not work correctly every time, the connection type affects the results, and there are multiple MAC address records for one phone. These results may mislead the court conclusion.

Conclusion:
When iOS devices make a network connection with macOS computer over Wi-Fi, the MAC address records that fall on the operating system are completely different, how to find the correct MAC address record that falls on the operating system when USB connection is established, and in which case more than one MAC address in the operating system records for ANDROID devices record has been shown.

Journal of the Faculty of Engineering and Architecture of Gazi University 39:3 (2024) 1637-1647

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University

Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

MacOS bilgisayara bağlanan telefonların MAC adresi kayıtlarının incelenmesi

Tümay Kurtca[1]*, Refik Samet[2]
[1]Gazi Üniversitesi, Bilişim Enstitüsü, Adli Bilişim Bölümü, 06500, Ankara, Türkiye
[2]Ankara Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, 06830, Ankara, Türkiye

ÖNEÇIKANLAR

- MAC adres kayıtlarını analiz etmek
- Analiz sırasında karşılaşılan sorunları belirlemek
- MAC adreslerini, önerilen analiz yöntemiyle tespit etmek

Makale Bilgileri
Araştırma Makalesi
Geliş: 05.07.2022
Kabul: 25.08.2023

DOI:
10.17341/gazimmfd.1140690

Anahtar Kelimeler:
Adli bilişim,
macOS,
MAC adresi,
iOS,
ANDROID,
kayıtlar

ÖZ

MAC adresleri sayesinde bir cihazın üretici firmasına, hangi ülkede kime satıldığına kadar tespitler yapılabilir. Cihazların MAC adresleri adli bilişim yazılımları ile tespit edilebilir. Fakat işletim sistemleri kendilerini sürekli geliştirmekte adli bilişim yazılımları da bu gelişimi daha çok Windows işletim sistemi üzerine yapmaktadır. Dolayısı ile adli bilişim yazılımları macOS için yeteriz kalmaktadırlar. Bu çalışmanın amacı, macOS üzerinde ağ bağlantısı sağlayan telefonların, MAC adresi kayıtlarını incelemek, inceleme esnasında karşılaşılabilecek sorunları belirlemek ve karşılaşılan bu sorunlara çözüm yolları sunmaktır. Hedeflenen bu amaçlara ulaşabilmek amacıyla, bu makalede çalışma ortamının hazırlanması, verilerin toplanması, verilerin analizi ve sonuçların değerlendirilmesi safhalarını kapsayan metodoloji önerilmektedir. iOS ve ANDROID işletim sistemine sahip telefonlar ile toplam on farklı uygulama, önerilen bu metodolojiye uygun olarak gerçekleştirilmiştir. Elde edilen sonuçlar; işletim sistemi kayıtları içerisinde tespit edilen MAC adreslerinin her defasında birebir doğru sonucu vermediğini, bağlantı türünün tespit edilen sonuçları etkilediğini ve bir telefon için birden fazla MAC adresi kaydı olduğunu göstermiştir.

Examination of MAC address records of phones connected to the macOS computer

HIGHLIGHTS

- Analyze the MAC address records
- Identify the problems encountered during the analysis
- Detect MAC addresses by the suggested analysis method

Article Info
Research Article
Received: 05.07.2022
Accepted: 25.08.2023

DOI:
10.17341/gazimmfd.1140690

Keywords:
Digital forensic,
macOS,
MAC address,
iOS,
ANDROID,
records

ABSTRACT

Thanks to the MAC addresses, determinations can be made to the manufacturer of a device, up to which country it is sold to. MAC addresses of the devices can be determined with forensic software. However, despite the continuous development of operating systems, the progress of forensic software remains insufficient in terms of Mac operating system (macOS). The aim of this study is to analyze the MAC address records of the phones connected to a computer with macOS, to detect the problems which occured during the analysis and to offer solutions to these problems. In order to achieve this goal, this article suggests a methodology consisting of the preparation of the working environment, the collection of data, the analysis of the data and the evaluation of the results. In accordance with this methodology, a total of ten different applications were used by phones with iOS and ANDROID operating systems. Obtained results showed that the MAC address records falling to the operating system did not work correctly every time, the connection type affects the results, and there are multiple MAC address records for one phone.

*Sorumlu Yazar/Yazarlar / Corresponding Author/Authors : *tumay.kurtca@gmail.com, samet@eng.ankara.edu.tr / Tel: +90 505 849 7161

1. Giriş (Introduction)

İnternet bağlantısı kurabilen cihazların ethernet kartlarına, bu kartları üreten firma tarafından yerleştirilen fiziksel kimliğe, ortam erişim kontrolü (media access control-MAC) adresi denilmektedir [1]. İnternet bağlantısı sağlayabilen her cihazın birbirinden farklı MAC adres bilgisi bulunmaktadır. Bu MAC adres bilgileri cihazın ethernet kartı değiştirilmediği sürece aynıdır. Her ağ bağdaştırıcısı cihaz özgü olarak, üretim süreci sırasında ağ donanımına gömülür veya aygıt yazılımında depolanır. Bu nedenle her akıllı cihazın; Wi-Fi ve Bluetooth gibi her biri kendi MAC adresine sahip birden çok MAC adresi bulunmaktadır [2]. MAC adresleri 48 bittir yani 6 adet oktetten (8 bit) oluşmakladır. Onaltılık sayı düzeninde 12 karakter ile ifade edilir. Fakat birkaç ağ türü 64 bit adresleme gerektirebilir. Bu durumda 48 bit MAC adresine sabit 16 bit "FFFE" değeri eklenir [3]. 48 bit adresleme için bakılacak olursa onaltılık sayı düzeninde 12 karakter ile ifade edilen karakterlerden ilk altısı cihaz üretici firmasını (organizasyona ait eşsiz kimlik/OUI) tanımlar [4]. Geriye kalan son altı karakter NIC (ağ arabirim denetleyicisi) ise, cihaz ait benzersiz adres olarak tanımlanır. Söz konusu benzersizlikten dolayı adli incelemelerde kişiye ait telefon, bilgisayar vb. dijital materyallerin MAC adres bilgilerinin tespiti önemlidir [5]. Günümüzde kullanılan birçok cep telefonu hücresel ağlar vasıtası ile veri kullanımı gerçekleştirmektedir [6], bu nedenle İnternet'e 7/24 nerede olursa olsun ulaşabilme kabiliyetine sahiptir [7]. Sabit modemlerin yer almadığı mekanlarda kullanıcılar genellikle telefondaki hücresel ağ bağlantısı sayesinde bilgisayar üzerinden İnternet'e erişim sağlarlar. Ancak mobil telefonların sağladığı bu kolaylıklar sayesinde internetin hayatımızın her alanına girmesi ile birlikte dijital alanda işlenen suçlar ve kötücül yazılımlar da artışlar meydana gelmiştir [8]. Bu artış dolayısı ile gerek tespit edilen açıklıklarla çok sayıda kötücül yazılım gerekse IP ve MAC adresleri tespit yöntemi geliştirilmiştir [9]. Yine dijital alanda işlenen suçlar dışında birçok olayda tespit edilen basit bir ağ bağlantısı ile olayın çözümüne ulaşılmıştır. Bilgisayarlar ile mobil cihazlar arasında bağlantı yapıldığı anda işletim sisteminde oluşan kayıtlardan elde edilen MAC adres bilgileri aracılığı ile kullanılan cihazı nereden kimi tarafından satın aldığına dair bilgilere erişilebilir [10]. Ancak incelemeler sırasında işletim sisteminde yer alan MAC adres bilgilerinin her defasında gerçek sonucu vermediği ve eksik MAC adresi bilgilerinin raporlandığı tespit edilmiştir.

Bu çalışmada macOS bilgisayara bağlanan telefonların MAC adresi kayıtlarının analiz edilmesi için öncelikle literatür taraması yapılmıştır. macOS'un El Capitan ve Yosemite sürümlerinde ağı hatırlama seçeneği aktif edilen bağlantılara ait verilerin "com.apple.airport.preferences.plist" dosyasında yer aldığından ve bu dosyanın hangi klasör yolu içerisinde olduğundan bahsedilmiştir [11]. Ağ trafiğinin analizi için MAC adres bilgilerinin gerekli olduğu ve bu bilgilerin "NetworkInterfaces.plist" dosyasında yer aldığı belirtilmiştir [12]. "netusage.sqlite" veri tabanı dosyasında cihazın bağlantı zamanı, bağlandığı ağ bilgilerinin bulunduğu ve bu veri tabanı ile ilgili genel bilgiler verilmiştir [13]. "com.apple.network.identification.plist" dosyasında ise kablosuz ağ geçmişini, servis seti tanımlayıcısı (service set identifier-SSID), gibi bilgilerin bulunduğuna değinilmiştir [14]. Ancak yaptığımız çalışmalarda bu "com.apple.network. identification.plist" isimli dosyanın, macOS'un yeni sürümlerinden biri olan Mojave sürümünde bulunmadığı görülmüştür. Bluetooth bağlantısı ile ilgili verilerin "com.apple.bluetooth.plist" dosyasında yer alabileceğinden bahsedilmiş [15] ancak kablosuz ve USB bağlantıları çalışma içerisinde yer almamıştır. "Mac Memorize" yazılımı ile uçucu hafıza incelemesi yapılarak Wi-Fi ağına ait parola tespit edilmiş ancak bu verinin ağ ile ilişkisi belirtilememiştir [16]. Adli bilişim incelemelerinde macOS ile ilgili yapılan çalışmalara bakıldığında büyük oranda hiyerarşik dosyalama sistemi (hierarchical file system-HFS) seçildiği, canlı incelemeler yapıldığı ve uçucu bellek analizleri gerçekleştirilerek veriler elde edildiği görülmüştür. macOS'un güncel sürümleri (apple dosyalama sistemine (apple file system-APFS) sahip sürümler) üzerinde ayrıntılı bir çalışmanın olmadığı görülmüştür. Bu sebeple bu çalışmada platform olarak macOS Mojave versiyonu seçilmiştir. Yapılan literatür taraması sonucu ağ ile ilgi veriler bulunduran dosyaların sadece dosya konumlarına yer verilmiştir. Bu dosyalardaki verilerin doğruluğu, dosyaların nasıl inceleneceği, raporlama aşamasında yanıltıcı bir durum olup olmadığı belirtilmemiştir.

Bilgi sistemlerine yönelik veya bilgi sistemleri kullanılarak işlenen suçlar ve gerçekleştirilen saldırılar işletim sistemleri üzerinde izler bırakmaktadır. Bu izler sayesinde MAC adreslerinin tespit edilmesi önem arz etmektedir. MAC adresleri sayesinde cihaz üretici firmasına, ülkeye ve cihazın kime satıldığına kadar tespitler yapılabilir. Fakat işletim sistemleri kendilerini sürekli geliştirmekte adli bilişim yazılımları da bu gelişimi daha çok Windows işletim sistemi üzerine yapmaktadır dolayısı ile macOS için yeteriz kalmaktadırlar. macOS ve Windows işletim sistemlerinin yapıları farklı olduğundan, Windows işletim sistemi üzerinde kullanılan adli bilişim yöntemleri macOS üzerinde kullanılamamaktadır [17]. Bu sebeple daha spesifik bir çalışma olabilmesi adına bu çalışmada platform olarak macOS seçilmiştir. Aynı zamanda literatür taramasında, macOS'un eski dosyalama sistemleri üzerinde çalışmalar yapıldığı görüldüğü için bu çalışmada macOS'un yeni dosyalama sistemine sahip Mojave sürümü seçilmiştir.

Bu çalışmada hedeflenen amaç; macOS bilgisayara bağlanan telefonların, MAC adresi kayıtlarını incelemek, inceleme esnasında karşılaşılan problemleri belirlemek ve karşılaşılan bu problemlere çözüm yolları bulmaktır. Hedeflenen amaca ulaşabilmek için bu makalede çalışma ortamının hazırlanması, verilerin toplanması, verilerin analizi ve sonuçların değerlendirilmesi aşamalarından oluşan bir metodoloji önerilmiştir. ANDROID ve iOS işletim sistemine sahip telefonlar aynı bilgisayara bağlanarak ve bağlantı türleri değiştirilerek çeşitli uygulamalar yapılmıştır. Uygulamaların ardından bilgisayarın kopyası alınarak, MAC adresi kayıtlarının düştüğü dosyalar incelenmiştir. İnceleme sonucunda telefonlar ile kurulan ağ bağlantısı türlerinin (kablosuz, USB) tespit edilen verileri etkilediği görülmüştür. Tespit edilen MAC adres bilgilerinin çoğunlukla gerçek MAC adres bilgilerini göstermemesin yanında bazı telefonlara ait birden fazla MAC adresi kaydı olduğu görülmüştür. Ayrıca alınan bir kopyanın dosya sisteminin görüntülenmesine ve verilerin işlenerek incelenmesine olanak sağlayan [18] uluslararası adli bilişim camiasında popüler olarak kullanılan adli bilişim yazılımı, Magnet AXIOM kullanıldığında raporlama aşamasında bağlanılan bütün iOS işletim sistemine sahip cihazları tespit edemediği görülmüştür. Bu durumunda CMK m. 134 uyarınca incelenmesi yapılan delilerin [19], mahkeme sonucunu yanıltabileceği değerlendirilmiştir. Söz konusu dosyaların nasıl inceleneceği ve doğru MAC adreslerinin ulaşılabilirliği gösterilmiştir.

Makale çalışmasının önerileri şunlardır; 1) Elde edilen sonuçlara göre düzenlenecek raporların dava sonucunu yanıltabileceği uyarısında bulunulmuştur. 2) Uygulamalarda kullanılan çeşitli marka-model cep telefonları ile tespit edilen MAC adresi kayıtlarının değerlendirmesi yapılmış olup inceleme aşamasında sadece adli bilişim yazılımına bağlı kalınmaması önerilmiştir. 3) iOS telefonlarla kablosuz ağ üzerinden bağlantı kurulduğunda bilgisayar içerisinde tespit edilen MAC adres bilgilerinin, cihazın kendi MAC adres bilgisinden tamamen farklı olduğu tespit edilmiş olup bu durum yargı makamına sunulacak olan raporda belirtilmelidir. Ayrıca bu makalede, iOS cihazların, bilgisayara USB üzerinden ağ bağlantısı sağlandığında doğru MAC adres bilgisinin nasıl bulunacağı ve ANDROID cihazlar

için işletim sistemi kayıtlarında hangi durumda birden fazla MAC adresi kaydı düştüğü gösterilmiştir.

Bu makalenin sonraki bölümleri sırasıyla şu şekilde düzenlenmiştir. macOS bilgisayara bağlanan telefonların MAC adreslerinin analizi için Bölüm 2'de metodoloji önerilmiştir. Önerilen metodoloji Bölüm 3'te gerçekleştirilmiştir. Bölüm 4'te öneriler ve sonuçlar sıralanmıştır.

2. macOS Bilgisayara Bağlanan Telefonların Mac Adresi Kayıtlarının İncelenmesi Metodolojisi
(The Methodology of Examining the Records of Mac Address of Phones Connected to macOS Computer)

Bu çalışmada önerilen metodoloji, çalışma ortamının hazırlanması, verilerin toplanması, verilerin analizi, sonuçların değerlendirilmesi olmak üzere 4 aşamadan oluşmaktadır.

2.1. Çalışma Ortamının Hazırlanması
(Preparation of Working Environment)

CMK 134'e göre bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı dijital materyaller üzerinde arama yapılmasına ve bu materyallerden kopya çıkartılıp inceleme yapılmasına hâkim tarafından karar verilir. Ancak olay yerinde şüphelilerin kullandığı tüm dijital materyaller bulunamayabilir. Örneğin arama sırasında bulunan bir telefon ve bir bilgisayara el konulabilir ancak şüpheli suç aracı olarak birden fazla telefon ve diğer dijital materyalleri kullanıyor olabilir. Bu materyaller kolluk kuvvetinin arama yaptığı yerde olmayabilir veya şüpheli tarafından gizlenmiş olabilir. Bu durumda el konulan bilgisayarın incelenmesi ile şüphelinin kullandığı diğer materyaller hakkında deliller elde edilebilir. Bu doğrultuda yapılan çalışmanın amacı ise macOS bilgisayarın işletim sistemi kayıtlarından ağ bağlantısı sağlanmış telefonlara ait MAC adreslerini tespit etmektir. Dolayısı ile CMK 134'e göre incelemeyi gerçekleştirecek olan adli bilişim uzmanında incelenecek materyal olarak sadece bilgisayar olduğu varsayılmalıdır. Bu sebeple çalışma ortamı için bilgisayar temin edilmelidir. Söz konusu bilgisayar delil niteliği taşıdığı için adli bilişim yazılımları ile imajı (kopyası) alınmalıdır. Ayrıca alınan kopya analiz edildiğinde tespit edilecek verilerin (MAC adres kayıtları) doğru olup olmadığını belirleyebilmek amacıyla MAC adres bilgilerine ulaşılabilen farklı işletim sistemi ile çalışan akıllı telefonlar ve bu uygulamaları yapabilmek için adli bilişim yazılımları (kopya alma ve inceleme) edinilmelidir.

2.2. Verilerin Toplanması (Data Collection)

- MAC adres bilgileri tespit edilmek istenen telefonların marka ve model bilgisi, MAC adresleri cihaz adı her telefonun ayarlar bölümünde yer almaktadır. Bu bilgiler toplanmalıdır.
- Bilgisayarın işletim sistemi üzerinde kayıt düşmesi için bilgisayar ile farklı işletim sistemine sahip telefonlar arasında, farklı ağ bağlantısı türleri (Wi-Fi/Wi-Fi Anımsatma/USB) kullanılarak ağ bağlantısı gerçekleştirilmeli ve ağ bağlantısı sağlanan telefonların hangi bağlantı türü ile bağlanıldığı not alınmalıdır.
- Gerçekleştirilen her ağ bağlantısından sonra bilgisayar kapatılmalı, bilgisayarın imajı (kopyası) alınmalıdır.

2.3. Verilerin Analizi (Data Analysis)

- Adli bilişim yazılımlarıyla, veri toplama kısmında alınan tüm kopyalar, incelenmelidir.
- Mevcut metodolojide kullanılan, MAC adresi kayıtlarının düştüğü dosyalardaki kayıtlar incelenmeli, bu dosyalarda geçen MAC adresleri ile telefonların veri toplama aşamasında elde edilen kendi MAC adresleri karşılaştırılmalıdır.

2.4. Sonuçların Değerlendirilmesi (Evaluation of the Results)

Veri Analiz aşamasında elde edilen bilgiler ışığında;

- Bilgisayarın alınan kopyaları incelenerek işletim sistemi kayıtlarından tespit edilen MAC adresleri ile veri toplama aşamasında elde edilen cep telefonların kendi MAC adresleri karşılaştırılmalıdır. Eğer farklılık söz konusu ise bu farklılığın tekrar edip etmediğine bakılmalıdır.
- İncelenen her kopyada, daha önce bağlanılan diğer telefonlara ait kayıt olup olmadığına bakılmalıdır. Eğer inceleme yazılımlarının verdiği sonuçlarda önceki telefonlara ait kayıt yok ise manuel olarak inceleme yapılmalıdır.
- Kullanılan aynı işletim sistemine sahip telefonlar için farklı sonuçlar çıkıyorsa bu sebebi tespit etmek için bağlantı türleri karşılaştırılmalıdır.
- Veri toplama aşamasında elde edilen MAC adresleri kopya içerisinde anahtar kelime olarak aratılmalı ve gerçek MAC adresinin tespit edilebilirliğine dair değerlendirme yapılmalıdır.

3. Önerilen Metodolojinin Uygulaması
(Application of the Proposed Methodology)

Bu bölümde, bir önceki bölümde önerilen metodoloji kullanılarak iOS ve ANDROID işletim sistemine sahip telefonlar ile toplam on farklı uygulama gerçekleştirilmiştir. Yapılan her uygulama için aşağıdaki adımlar uygulanmıştır.

- Çalışma Ortamının Hazırlanması; Öncelikle bilgisayarın işletim sistemini analiz etmek için Macbook Pro (A1707), iPhone, Samsung, Casper marka telefonlar temin edilmiştir. Kopya almak için BlackBag MacQuisition (Version 2019 SR-2) ve alınan kopyayı incelemek için Magnet AXIOM (Version 3.6.0.15906) yazılımları temin edilmiştir. BlackBag MacQuisition; MAC işletim sistemine sahip cihazlar için kopya alma işlemini destekleyen lisanslı bir adli bilişim yazılımıdır [20]. Magnet AXIOM ise "Examine" ve "Process" olmak üzere iki uygulamadan oluşur [21]. Bu yazılımlar, lisanslı olup alınan kopyanın içeriğini dosya sistemi görünümünde görüntüleyebilen ve araştırmacıların dosyaları manuel olarak işlemesine olanak tanıyan aynı zamanda otomatik veri işleme ve analiz yeteneğine sahiptirler [18].
- Verilerin Toplanması; Çalışma ortamının hazırlanması aşamasında temin edilen telefonların, ayarlarlar menüsündeki "Hakkında" kısmından telefon adı, marka, model bilgisi ve MAC adresleri not alınmıştır. Bilgisayarın işletim sistemi üzerinde kayıt düşmesi için ANDROID ve iOS işletim sistemine sahip telefonlar olmak üzere iki ana başlık altında uygulamalar yapılmıştır. Bölüm 3.1.'de verilen Tablo 1 ve Bölüm 3.2.'de verilen Tablo 8'de uygulamalarda kullanılan telefon, bağlantı türü ve tespit edilmek istenen Wi-Fi MAC adresleri yer almaktadır. Kullanılan telefonlar bir önceki uygulamada elde edilen sonuçları doğrulamak amacıyla ve aynı marka telefonun bağlantı türünün değiştirilmesi sonucunda değişen kayıtları görmek amacıyla seçilmiştir. Her uygulama başında telefonların neden seçildiği açıklanmıştır. Her gerçekleştirilen bağlantı sonrası bilgisayarın kopyası, BlackBag MacQuisition yazılımı ile alınmıştır.

- Verilerin Analizi; Verilerin toplanması aşamasında alınan kopya, Magnet AXIOM yazılımı ile incelenmiştir. MAC adresi kayıtlarının düştüğü aşağıda ayrıntıları verilen dosyalar her uygulama için analiz edilmiştir.
- "…\Library\Preferences\SystemConfiguration\com.apple.airport.preferences.plist; Bilgisayara anımsatılan Wireless ağ geçmişi ile ilgili bilgileri tutar [10].

- "…\private\var\networkd\netusage.sqlite"; Bu veri tabanı dosyasında cihazın bağlandığı ağ ve zaman bilgileri tutulmaktadır [12].
- "…\Library\Preferences\SystemConfiguration\com.apple.network.identification.plist**";** Kablosuz ağ geçmişini SSID, zaman, güvenlik tipi gibi değerlerin kaydını tutar [13]. Yapılan literatür taramasında araştırmaların macOS 10.14 versiyonundan daha eski versiyonları üzerinde yapıldığı görülmüştür. Fakat bu çalışmalarda yer alan "com.apple.network.identification.plist" isimli dosyanın uygulamalarda kullanılan Mojave sürümüne sahip bilgisayar içerisinde olmadığı görülmüştür.
- "…\Library\Preferences\SystemConfiguration\NetworkInterfaces.plist"; Ağ arayüzü ile ilgili bilgileri tutan dosyadır. İçerisinde bulunan "BSD" arayüz adını, "IOMACAddress" ise MAC adresi bilgisini tutar [22].

Yukarıda adı geçen dosyalardaki MAC adresleri ile veri toplama aşamasında elde edilen telefonların kendi MAC adresleri karşılaştırılmıştır.

- Sonuçların Değerlendirilmesi; yapılan analizler doğrultusunda değerlendirilen sonuçlar Bölüm 4.2'de sunulmuştur.

3.1. iOS Cep Telefonları ile Gerçekleştirilen Çalışmalar
(Practices Executed by Using IOS Mobile Phones)

Bu bölümde iOS telefonlar kullanılarak beş adet uygulama gerçekleştirilmiştir. Tablo 1'de gerçekleştirilen uygulamaların özeti, yani veri toplama aşamasında elde edilen veriler yer almaktadır. iOS telefonlar, macOS bilgisayar ile Wi-Fi üzerinden, veya doğrudan USB ile ya da iki seçenek bir arada iken ağ bağlantısı sağlayabilirler. Söz konusu bağlantı türleri ile gerçekleştirilen uygulamalarda elde edilen sonuçları teyit etmek ya da telefon modeli, bağlantı türü ve "Wi-Fi Ağını Anımsa" seçeneği değiştirilerek ortaya çıkan farklılıkları görmek amacıyla bir sonraki uygulamalar yapılmıştır. Telefonlar, tablodaki açıklama satırında olduğu gibi bilgisayara bağlanmış ve bilgisayarın kopyası alınmıştır. Alınan kopya veri analizinde belirtildiği gibi incelenmiş ve metodun son aşaması tamamlanarak sonuçlar değerlendirilmiştir.

3.1.1. iOS uygulama-1 (iOS application-1)

Tablo 1'in 1. satırında yer alan cep telefonu ile ağ bağlantısı gerçekleştirilmiştir. Daha sonra bilgisayarın kopyası alınmıştır. Kopyanın, Magnet AXIOM ile incelenmesi neticesinde; "com.apple.airport.preferences" isimli. plist uzantılı dosyada; ağ ismi ve MAC adres bilgisinin yer aldığı tespit edilmiştir. Ancak tespit edilen MAC adresinin tüm oktetleri, telefona ait gerçek MAC adresinden farklıdır (Tablo 2).

Tablo 2. "com.apple.airport.preferences.plist" dosyası yapı bilgileri
(Structure information of the "com.apple.airport.preferences.plist" file)

Ağ Adı (SSID)	NiHaT
Son Bağlantı Tarihi/Saati	22.08.2019 06:18
Güvenlik Modu	WPA2 Personal
MAC Adresi	*3a:fb:44:bc:bf:b5*
Durum	Active

Kopyanın, Magnet AXIOM ile ağ arayüzleri başlığı incelendiğinde ise 8 adet kaydın yer aldığı tespit edilmiştir. Ağ ismi iPhone olan telefona ait MAC adres bilgisinin, ilk oktet değerinin 9A olduğu ve geriye kalan tüm oktetlerin cihazın kendi MAC adresi ile aynı şekilde yer aldığı tespit edilmiştir. (Tablo 3).

Tablo 3. Yazılımın yapılar sekmesinde ki "Ağ-arayüzleri-macOS" bilgileri
(Network interfaces-macOS information in the structures tab of the software)

BSD.	MAC adresi	Ağ adı
en0	88:E9:FE:86:8C:31	Wi-Fi
en3	FA:00:4C:22:D6:05	Thunderbolt 3
en2	FA:00:4C:22:D6:00	Thunderbolt 2
en1	FA:00:4C:22:D6:01	Thunderbolt 1
en4	FA:00:4C:22:D6:04	Thunderbolt 4
en5	AC:DE:48:00:11:22	iBridge
en6	88:E9:FE:73:F2:DD	Bluetooth PAN
en7	*9A:*00:C6:42:A5:03	*iPhone*

Aynı zamanda kopya içerisinde bulunan "netusage.sqlite" veri tabanı dosyasının, Magnet AXIOM yazılımı ile incelenmesi sonucunda "ZNETWORKATTACHMENT" tablosunun "ZIDENTIFIER" sütunundaki değerin "NiHaT-3a:fb:44:bc:bf:b5" olduğu görülmüştür. Bu değere göre tespit edilen MAC adresinin telefona ait gerçek MAC adresinden farklı olduğu tespit edilmiştir.

Uygulama neticesinde; "NetworkInterfaces.plist" isimli dosyada uygulamada kullanılan telefonun ağ isminin (Nihat) yer almadığı ve MAC adresi birinci oktet değerinin "98" olması gerekirken "9A" (bu değerden iki bayt fazla) olduğu tespit edilmiştir. Diğer dosyalarda ise bulunan MAC adres bilgisinin, ağ bağlantısı sağlayan telefona ait gerçek MAC adres bilgisi ile aynı olmadığı tespit edilmiştir.

3.1.2. iOS uygulama-2 (iOS application-2)

Tablo 1'in 1. satırında gerçekleştirilen uygulama neticesinde ulaşılan verilerin doğrulanması maksadıyla, Tablo 1'in 2. satırında yer alan cep telefonu ile ağ bağlantısı gerçekleştirilmiştir. Daha sonra bilgisayarın kopyası alınmıştır. Kopyanın yapılan analizinde; "netusage.sqlite" isimli dosya içerisinde ve "com.apple.airport.preferences" isimli dosya içerisinde MAC adres

Tablo 1. iOS ile Yapılan Uygulamaların Özeti (Summary of Applications with iOS)

	Sıra No	Telefon Marka Model	Cihaz Adı	Bağlantı Türü	Wi-Fi MAC Adresi	Açıklama
iOS Uygulama 1	I1	iPhone A1778	NiHaT	USB & Wi-Fi	98:00:C6: 42:A5:03	"Wi-Fi Ağını Anımsa" seçeneği *aktif* edilmiştir.
iOS Uygulama 2	I2	iPhone A1688	Mürsel	USB & Wi-Fi	B4:9C:DF:01:B3:DD	"Wi-Fi Ağını Anımsa" seçeneği *aktif* edilmiştir
iOS Uygulama 3	I3	iPhone A1688	Salih İphone'u	Wi-Fi	58:E2:8F:CB:87:D4	"Wi-Fi Ağını Anımsa" seçeneği *pasif* edilmiştir
iOS Uygulama 4	I4	iPhone A1786	Yiphone	Wi-Fi	78:4F:43: 28:B3:7F	"Wi-Fi Ağını Anımsa" seçeneği *pasif* edilmiştir
iOS Uygulama 5	I5	iPhone A1901	Ömer	USB	3C:2E:FF:41:60:A0	Sadece USB üzerinden bağlantı sağlanmıştır.

kayıtları bulunmuştur. Ancak bulunan MAC adreslerinin, uygulamada kullanılan telefonun gerçek MAC adresi ile aynı olmadığı tespit edilmiştir. Kullanılan telefon ile USB üzerinden de ağ bağlantısı kurulduğundan "NetworkInterfaces" dosyasında yer alan kayıtlara yeni bir kaydın eklenmiş olması beklenmiştir. Ancak kopyanın, Magnet AXIOM ile incelenmesi sonucu Ağ arayüzleri başlığında yer alan kayıtlarda bir artış olmadığı ve halen sekiz adet olduğu tespit edilmiştir. Oluşan son kayıt incelendiğinde; MAC adres bilgisinin ilk oktet değerinin "B4" olması beklenirken "B6" olarak yer aldığı tespit edilmiştir (Tablo 4). Bir önceki uygulamada kullanılan (Tablo 1'in 1. satırında belirtilen) telefona ait herhangi bir veri bulunmadığı görülmüştür.

Tablo 4. Yazılımın yapılar sekmesinde ki "Ağ-arayüzleri-macOS" bilgileri
(Network interfaces-macOS information in the structures tab of the software)

BSD.	MAC adresi	Ağ adı
en0	88:E9:FE:86:8C:31	Wi-Fi
en1	FA:00:4C:22:D6:01	Thunderbolt 3
en2	FA:00:4C:22:D6:00	Thunderbolt 2
en3	FA:00:4C:22:D6:05	Thunderbolt 1
en4	FA:00:4C:22:D6:04	Thunderbolt 4
en5	AC:DE:48:00:11:22	iBridge
en6	88:E9:FE:73:F2:DD	Bluetooth PAN
en7	*B6:*9C:DF:01:B3:DD	*iPhone*

"NetworkInterfaces.plist" isimli dosyanın .plist editörü ile incelenmesi sırasında; "MatchingMACs" anahtarı içerisinde daha önce bağlantı kurulan telefonun MAC adres bilgisi olduğu tespit edilmiştir. Burada tespit edilen MAC adres bilgisinin ilk oktet değeri, gerçek MAC adresi değerinden iki bayt fazla olarak gözükmektedir (Tablo 5).

Uygulama neticesinde; "netusage.sqlite", "NetworkInterfaces" ve "com.apple.airportpreferences" isimli dosyalardaki kayıtlar ile iOS Uygulama-1 neticesinde ulaşılan veriler doğrulanmıştır. Alınan kopyanın, Magnet AXIOM ile incelenmesi sonucu ağ arayüzleri başlığı içerisinde USB ile bağlanılan tüm telefonlara ait kayıtlar yerine, bağlantı kurulan son telefona ait kaydın yer aldığı görülmüştür. Ancak "NetworkInterfaces.plist" isimli dosyanın plist editörü yardımıyla manuel incelenmesi sonucu, USB ile bağlantı gerçekleştirilen tüm iPhone telefonların MAC adres bilgilerine ulaşılabildiği görülmüştür.

3.1.3. iOS uygulama-3 (iOS application-3)

Tablo 1'in 3. satırında yer alan cep telefonu ile ağ bağlantısı gerçekleştirilmiştir. Bu uygulamada, "Wi-Fi Ağını Anımsa" seçeneğinin **pasif** edilmesi ile kurulan bağlantının sonuçlarını görmek amaçlanmıştır. Kurulan bağlantı sonrasında bilgisayarın kopyası alınmıştır. Kopyanın, Magnet AXIOM ile incelenmesi neticesinde; "netusage.sqlite" veri tabanı dosyasına ait "ZNETWORKATTACHMENT" tablosunun "ZIDENTIFIER" sütunundaki değerin "Salih iPhone'u-16:61:be:1c:00:48 olduğu görülmüştür. Ancak burada bulunan kaydın, uygulamada kullanılan telefona ait gerçek MAC adresi ile aynı olmadığı tespit edilmiştir.

Uygulama sonucunda; USB üzerinden ağ bağlantısı gerçekleştirilmediğinden dolayı "NetworkInterfaces.plist" içerisinde, ağ anımsama seçeneği pasif edildiğinden dolayı ise "com.apple.airport.preferences" plist dosyasında MAC adres bilgisi bulunmamıştır. Wi-Fi ağının anımsatılması veya anımsama seçeneğinin pasif edilmesi durumunda ise "netusage.sqlite" isimli dosya içerisinde yer alan MAC adres bilgisinin, telefona ait gerçek MAC adres bilgisi ile aynı olmadığı tespit edilmiştir.

3.1.4. iOS uygulama-4 (iOS application-4)

Bir önceki uygulama neticesinde ulaşılan tüm tespitler doğrulanmıştır.

3.1.5. iOS uygulama-5 (iOS application-5)

Sadece USB üzerinden ağ bağlantısı gerçekleştirildiğinde önceki uygulamalara göre herhangi bir farklılığın oluşup oluşmayacağının tespit edilmesi amacıyla Tablo 1'in 5. satırında yer alan telefon ile ağ bağlantısı gerçekleştirilmiştir. Daha sonra bilgisayarın kopyası alınmış ve alınan kopya Magnet AXIOM ile incelenmiştir. İnceleme sonucunda ağ ara yüzleri yapı başlığında kayıt sayısının artmadığı ve önceki uygulamalarda olduğu gibi yine sekiz adet olduğu tespit edilmiştir (Tablo 6).

Tablo 6. Yazılımın yapılar sekmesinde ki "Ağ-arayüzleri-macOS" bilgileri
(Network interfaces-macOS information in the structures tab of the software)

BSD.	MAC adresi	Ağ adı
en0	88:E9:FE:86:8C:31	Wi-Fi
en1	FA:00:4C:22:D6:01	Thunderbolt 3
en2	FA:00:4C:22:D6:00	Thunderbolt 2
en3	FA:00:4C:22:D6:05	Thunderbolt 1
en4	FA:00:4C:22:D6:04	Thunderbolt 4
en5	AC:DE:48:00:11:22	iBridge
en6	88:E9:FE:73:F2:DD	Bluetooth PAN
en7	*3E:*2E:FF:41:60:A0	*iPhone*

Önceki yapılan uygulamalarda olduğu gibi "NetworkInterfaces.plist" isimli dosyanın plist editörü ile incelenmesi sırasında; bağlanılan diğer iPhone telefonların MAC adresleri tespit edilmiştir (Tablo 7).

Uygulama neticesinde; sadece USB ile ağ bağlantısı sağlanmış da olsa Ağ arayüzleri yapı başlığında USB ile bağlanılan tüm telefonlara ait kayıtlar yerine, bağlantı kurulan son telefona ait kaydın yer aldığı görülmüştür. Böylece iOS Uygulama 2'de ulaşılan bilgiler doğrulanmıştır.

3.1.6. iOS cep telefonları ile gerçekleştirilen çalışmaların sonuçları (Results of executed by using IOS mobile phones)

- USB üzerinden bağlantı sağlanılması durumunda; "NetworkInterfaces.plist" isimli dosyada bulunan MAC adresi kaydı birinci oktet değerinin, telefonun gerçek Wi-Fi MAC adresi birinci oktet değerinden 2 bayt fazla olduğu tespit edilmiştir.
- "NetworkInterfaces.plist" dosyasında ağ adı iPhone olarak gözüken MAC adres değerinin ilk oktetinden iki bayt çıkartıldığında, kullanılan telefona ait gerçek MAC adres bilgisi bulunmuş olacaktır. Bulunan MAC adresinin ilk üç oktetinin MAC adresi denetleyici araçlarıyla sorgulanması sonucu satıcı firma ismi olarak Apple ile eşleşip eşleşmediği kontrol edilmelidir.

Tablo 5. "NetworkInterfaces.plist" dosyasına ait alt anahtarlar ve değerler (Subkeys and values of the "NetworkInterfaces.plist" file)

Kök Adı	Birincil alt anahtar adı	İkincil alt anahtar adı	Üçüncül alt anahtar adı	Üçüncül alt anahtar değerleri
root	Interfaces	[7]	IOMACAddress	*0xB6* 0x9C 0xDF 0x01 0xB3 0xDD
-	-	-	MatchingMACs	*0x9A* 0x00 0xC6 0x42 0xA5 0x03

- Magnet AXIOM ile ağ arayüzleri yapı başlığı incelendiğinde, USB ile bağlanılan tüm telefonlara ait kayıtlar yerine, bağlantı kurulan son telefona ait kaydın yer aldığı ve bağlantı sayısı artmasına rağmen kayıt sayısının artmadığı tespit edilmiştir. Ancak "NetworkInterfaces.plist" isimli dosyanın plist editörü yardımıyla incelendiğinde her bağlantı için bir kayıt bulunduğu görülmüştür.
- Wi-Fi üzerinden bağlantı sağlanması sonucunda; **"**netusage.sqlite" ve "com.apple.airport.preferences" dosyaları içerisinde bulunan telefonlara ait MAC adresi bilgilerinin, gerçek MAC adreslerini yansıtmadığı, tüm oktetlerin farklı olduğu tespit edilmiştir. İnceleme sonucunda yargı makamlarına sunulacak olan rapor içerisinde bu durum mutlaka belirtilmelidir. Wi-Fi üzerinden bağlantı sağlanması durumunda tespit edilemeyen MAC adres bilgileri, bilgisayarın alınan kopyası üzerinde anahtar kelime arama yöntemleri kullanılarak aratılmış ancak kopya içerisinde herhangi bir kayıt tespit edilememiştir.

3.2. ANDROID Cep Telefonları ile Gerçekleştirilen Çalışmalar (Practices Executed by Using ANDROID Mobile Phones)

Bu bölümde ANDROID telefonlar kullanılarak beş adet uygulama gerçekleştirilmiştir. Tablo 8'de gerçekleştirilen uygulamaların özeti, yani veri toplama aşamasında elde edilen veriler yer almaktadır. ANDROID telefonlar, macOS bilgisayar ile doğrudan USB üzerinden ağ bağlantısı gerçekleştirememektedir. Cep telefonun USB ile ağ bağlantısı gerçekleştirilebilmesi için ek yazılımlara ihtiyaç duyulmaktadır. Bu sebeple uygulamalarda kullanılan bağlantı türü sadece Wi-Fi olarak seçilmiştir. Uygulamalarda elde edilen sonuçları, teyit etmek ya da telefon modeli ve "Wi-Fi Ağını Anımsa" seçeneği değiştirilerek ortaya çıkan farklılıkları görmek amacıyla bir sonraki uygulama yapılmıştır. Telefonlar, tablodaki açıklama satırında olduğu gibi bilgisayara bağlanmış ve bilgisayarın kopyası alınmıştır. Alınan kopyalar, veri analizinde belirtildiği gibi incelenmiş ve metodun son aşaması tamamlanarak sonuçlar değerlendirilmiştir.

3.2.1. ANDROID uygulama-1 (ANDROID application-1)

Tablo 8'nin 1. satırında yer alan cep telefonu ile ağ bağlantısı gerçekleştirilmiştir. Daha sonra bilgisayarın kopyası alınmıştır. Kopyanın, Magnet AXIOM ile incelenmesi sonucu; imaj içerisinde yer alan "com.apple.airport.preferences.plist" dosyasında; A1 numaralı telefona ait MAC adresi kaydının 8C:45:00:09:E3:B8 olması gerekirken 8E:45:00:09:E3:B8 olduğu görülmüştür (Tablo 9).

Tablo 9. "com.apple.airport.preferences.plist" dosyası yapı bilgileri (Structure information of the "com.apple.airport.preferences.plist" file)

Ağ Adı (SSID)	AndroidAP
Son Bağlantı Tarihi/Saati	21.11.2019 06:19
Güvenlik Modu	WPA2 Personal
MAC Adresi	*8e:45:00:09:e3:b8*
Durum	Active

"netusage.sqlite" isimli veri tabanı dosyasına ait "ZNETWORKATTACHMENT" tablosunun "ZIDENTIFIER" sütunundaki değerin "AndroidAP-8e:45:00:09:e3:b8" olduğu görülmüştür.

Kopya içerisinde yer alan "NetworkInterfaces.plist" dosyasında herhangi bir değişiklik olmamıştır.

Uygulama neticesinde; "netusage.sqlite" ve "com.apple.airportpreferences" içerisinde tespit edilen MAC adres bilgisinin ilk oktet değeri "8C" olması gerekirken bu değerin iki bayt fazlası "8E" olduğu görülmüştür. iOS işletim sisteminde bu iki dosyadaki MAC adresi kayıtları telefonların kendi MAC adreslerinden tamamen farklı idi. "NetworkInterfaces.plist" dosyasında ise USB ile bağlanılmadığı için kullanılan telefon ile ilgili herhangi bir bilgi bulunmadığı görülmüştür.

3.2.2. ANDROID uygulama-2 (ANDROID application-2)

Tablo 8'nin 1.satırında gerçekleştirilen uygulama neticesinde ulaşılan verilerin doğrulanması maksadıyla Tablo 8'nin 2. satırında yer alan cep telefonu ile ağ bağlantısı gerçekleştirilmiştir. Daha sonra bilgisayarın kopyası alınmıştır. Kopyanın yapılan analizi sonucu elde edilen tespitler ile ANDROID Uygulama 1 sonucunda elde edilen tespitler eşleşmektedir. Ancak;

Tablo 7. "NetworkInterfaces.plist" dosyasına ait alt anahtar ve değerler (Subkey and values of the "NetworkInterfaces.plist" file)

Kök Adı	Birincil alt anahtar adı	İkincil alt anahtar adı	Üçüncül alt anahtar adı	Üçüncül alt anahtar değerleri
root	Interfaces	[7]	IOMACAddress	*0x3E* 0x2E 0xFF 0x41 0x60 0xA0
-	-	-	MatchingMACs	*0xB6* 0x9C 0xDF 0x01 0xB3 0xDD *0x9A* 0x00 0xC6 0x42 0xA5 0x03

Tablo 8. ANDROID ile Yapılan Uygulamaların Özeti (Summary of Applications with ANDROID)

	Sıra No	Telefon Marka Model	Cihaz Adı	Bağlantı Türü	Wi-Fi MAC Adresi	Açıklama
ANDROID Uygulama 1	A1	Samsung SM-G950F	AndroidAP	Wi-Fi	8C:45:0:09:E3:B8	"Wi-Fi Ağını Anımsa" seçeneği *aktif* edildi.
ANDROID Uygulama 2	A2	Samsung SM-G935F	Androids7	Wi-Fi	AC:5F:3E:CA:3C:1B	"Wi-Fi Ağını Anımsa" seçeneği *aktif* edildi.
ANDROID Uygulama 3	A3	Samsung SM-G610F	BASARAN	Wi-Fi	E0:AA:96:91:93:B0	"Wi-Fi Ağını Anımsa" seçeneği *pasif* edildi.
ANDROID Uygulama 4	A4	Samsung SM-A505F	Ahmet	Wi-Fi	A8:34:6A:E2:64:B2	"Wi-Fi Ağını Anımsa" seçeneği *pasif* edildi.
ANDROID Uygulama 5	A5	Samsung A510F	AndroidAP06	Wi-Fi	88:83:22: 38:E3:3C	Bir telefona ait birden fazla MAC adresi kaydı oluşmasının nedenini bulmak için yapılmıştır.

"netusage.sqlite" isimli veri tabanı dosyasına ait "ZNETWORKATTACHMENT" tablosunun "ZIDENTIFIER" sütununda birden fazla değer olduğu bu değerlerin sırasıyla "AndroidAP-8e:45:00:09:e3:b8", "AndroidAP-ae:5f:3e:ca:3c:1b" ve "Androids7-ae:5f:3e:ca:3c:1b" olduğu görülmüştür. Sonuç olarak ANDROID Uygulama 1'de bağlanan A1 numaralı telefona ait telefonun, kendi MAC adresi dışında bir adet daha MAC adresi kaydı olduğu ve oluşan bu kaydında A2 numaralı cep telefona ait olduğu *(ilk bayt değeri iki fazla olarak)* görülmüştür.

"com.apple.airport.preferences.plist" dosyasının analizinde de yukarıda ki tespitler teyit edilmekte olup sonuçlar Tablo 10'da sunulmuştur.

Tablo 10. "com.apple.airport.preferences.plist" dosyası yapı bilgileri
(Structure information of the "com.apple.airport.preferences.plist" file)

Ağ Adı (SSID)	AndroidAP
Son Bağlantı Tarihi/Saati	21.11.2019 06:19
Güvenlik Modu	WPA2 Personal
MAC Adresi	*8e:*45:00:09:e3:b8 *ae*:5f:3e:ca:3c:1b
Durum	Active

Uygulama sonucunda; uygulamada kullanılan telefon için; dosyalarda tespit edilen MAC adres kaydının ilk oktet değeri "AC" olması gerekirken bu değerin **i**ki bayt fazlası "AE" olduğu görülmüştür. ANDROID Uygulama 1'de elde edilen sonuçlar doğrulanmıştır. Ayrıca Samsung marka A2 numaralı telefonun bağlanılması sonucu, söz konusu dosyalarda daha önce bağlanılan Samsung marka A1 numaralı telefona ait kayıtların etkilendiği görülmüştür.

3.2.3. ANDROID uygulama-3 (ANDROID application-3)

Tablo 8'nin 3.satırıda yer alan cep telefonu ile ağ bağlantısı gerçekleştirilmiştir. Bu uygulamada "Wi-Fi Ağını Anımsa" seçeneği pasif edilmesi ile kurulan ağ bağlantısının sonuçlarını görmek amaçlanmıştır. Kurulan bağlantı sonrasında bilgisayarın kopyası alınmıştır. Kopyanın, Magnet AXIOM ile incelenmesi neticesinde; "netusage.sqlite" içerisinde bulunan MAC adres bilgisinin tespit edilmek istenen A3 numaralı telefona ait MAC adresi ile aynı olduğu görülmüştür (Tablo 11).

Tablo 11. "netusage.sqlite" dosyası bilgileri
(Information of "netusage.sqlite" file)

Ağ Adı	Bağlantı Türü	MAC Adresi
BAŞARAN	Wi-Fi	e0:aa:96:91:93:b0

Gerçekleştirilen ANDROID uygulama-3 neticesinde USB üzerinden ağ bağlantısı gerçekleştirilmediğinden dolayı "NetworkInterfaces.plist" içerisinde, ağ anımsama seçeneği pasif edildiğinden dolayı "com.apple.airport.preferences" isimli plist dosyasında herhangi bir kaydı bulunmamıştır. Ancak diğer uygulamalardan farklı olarak "netusage.sqlite" isimli dosyada bulunan MAC adresi kaydının, uygulamada kullanılan telefona ait gerçek MAC adresi kaydını ile aynı olduğu görülmüştür. Ayrıca ANDROID Uygulama 2'den farklı olarak A3 numaralı telefon ile bağlantı kurulmasının, daha önce bağlanan telefonlara ait kayıtları etkilemediği görülmüştür.

3.2.4. ANDROID uygulama 4 (ANDROID application 4)

Tablo 8'nin 3. satırında gerçekleştirilen uygulama neticesinde ulaşılan verilerin doğrulanması maksadıyla, Tablo 8'nin 4. satırında yer alan cep telefonu ile ağ bağlantısı gerçekleştirilmiştir. Daha sonra bilgisayarın kopyası alınmıştır. Kopyanın yapılan analizinde; uygulamada kullanılan telefonun MAC adres bilgisi A8:34:6A:E2:64:B2 olmasına rağmen "netusage.sqlite" isimli veri tabanı dosyasına ait "ZNETWORKATTACHMENT" tablosunun "ZIDENTIFIER" sütununda yer alan değerin AA:34:6A:E2:64:B2 olduğu görülmüştür. Diğer dosyalarda ise telefona ait herhangi bir kayıt bulunamamıştır.

ANDROID uygulama-4 sonucunda; bir önceki uygulamada, Wi-Fi Ağının anımsatılmaması durumunda tespit edilmek istenen MAC adresine ulaşılmıştı. Ancak bu deneyde Wi-Fi Ağı yine anımsatılmamış olmasına rağmen tespit edilmek istenen MAC adresi kayıtlarına ulaşılamamıştır. İşletim sistemi üzerinde tespit edilmek istenen MAC adresi kayıtlarına ulaşılıp ulaşılamamasının, Wi-Fi Ağının anımsatılması ile ilgisi olmadığı görülmüştür.

3.2.5. ANDROID uygulama 5 (ANDROID application 5)

ANDROID Uygulama 2'de, A2 numaralı telefon "Wi-Fi Ağını Anımsa" seçeneği aktif edilerek bağlantı kurulduktan sonra bilgisayarın alınan kopyası incelendiğinde "com.apple.airport.preferences.plist" ve "netusage.sqlite" isimli dosyalarda, daha önce ANDROID Uygulama 1'de bağlanılan A1 numaralı telefona ait MAC adresi kayıtlarının etkilendiği görülmüştü. *(A1 numaralı telefona ait telefonun kendi MAC adresi dışında bir adet daha MAC adresi kaydı vardı.)* Ancak bundan sonra yapılan uygulamaların hiçbirinde bu durumun oluşmadığı dikkat çekmiştir. ANDROID Uygulama 2'den sonra yapılan uygulamalarda "Wi-Fi Ağını Anımsa" seçeneği pasif hale getirilerek bağlantı kurulduğu için bu uygulamada "Wi-Fi Ağını Anımsa" seçeneği aktif edilmiştir. Böylece daha önceki uygulamalarda bağlanılan cep telefonlarına ait birden fazla MAC adresinin oluşup oluşmayacağının tespiti yapılmak istenmiştir. Tablo 8'nin ANDROID Uygulama 5 satırında tarif edildiği şekilde ağ bağlantısı sağlanmıştır. Gerçekleştirilen ağ bağlantısı sonrası bilgisayarın kopyası alınmıştır.

Kopyanın yapılan analizi neticesinde; "com.apple.airport.preferences.plist" dosyasının yapılan analizinde; daha önceden bağlantı sağlanan yine A1 numaralı telefona ait 3 adet MAC adres bilgisinin bulunduğu görülmüştür. Bu MAC adresi kayıtları incelendiğinde; ilk sırada olan kaydın telefonun kendi MAC adresi *(ilk oktet değeri iki fazla olarak)*, ikinci sırada olan kaydın A2 numaralı telefona ait MAC adresi *(ilk oktet değeri iki fazla olarak)* olduğu görülmüştür. Son olarak üçüncü sırada olan kaydın ise A5 numaralı telefona ait MAC adresi olduğu görülmüştür (Tablo 12).

Tablo 12. "com.apple.airport.preferences.plist" dosyası yapı bilgileri
(Structure information of the "com.apple.airport.preferences.plist" file)

Ağ Adı (SSID)	AndroidAP
Son Bağlantı Tarihi/Saati	21.11.2019 06:19
Güvenlik Modu	WPA2 Personal
MAC Adresi	*8e:*45:00:09:e3:b8 *ae*:5f:3e:ca:3c:1b 88:83:22:38:e3:3c
Durum	Active

"netusage.sqlite" veri tabanı dosyasına ait "ZNETWORKATTACHMENT" tablosunun "ZIDENTIFIER" sütununda yer alan değerin ise; daha önce bağlanılan A1 numaralı telefona ait, 2 adet kayıt olduğu ve kendisine ait MAC adresi kaydı olmadığı görülmüştür. Oluşan bu kayıtların A2 *(ilk oktet değeri iki fazla olarak)* ve A5 numaralı telefonlara ait olduğu görülmüştür.

ANDROID uygulama 5 sonucunda; A5 numaralı telefon bağlanıldığında, "com.apple.airport.preferences.plist" dosyasında daha önce bağlanılan Samsung marka A1 numaralı telefona ait kayıtların ANDROID Uygulama 2 sonucundaki gibi etkilendiği

görülmüştür. A5 numaralı telefon bağlanıldığında, "netusage.sqlite" dosyasında ise yine daha önce bağlanılan Samsung marka A1 numaralı telefona ait kayıtları etkilediği ancak com.apple.airport.preferences.plist" dosyasından farklı olarak A1 numaralı telefonun kendisine ait MAC adresi kaydı olmadığı görülmüştür.

3.2.6. ANDROID işletim sistemine sahip cep telefonları ile yapılan uygulamaların sonuçları
(Results of applications for mobile phones with ANDROID operating system)

- Birden fazla telefon ile bilgisayar arasında "Wi-Fi ağını anımsa seçeneği aktif" iken ağ bağlantısı gerçekleştirildiyse, "com.apple.airport.preferences.plist" ve "netusage.sqlite" isimli dosyalarında ilk bağlanılan telefona ait birden fazla MAC adresi kaydı olduğu görülmüştür. Yapılan uygulamalar sonucu bu durumun "Wi-Fi ağını anımsa seçeneği aktif" edilmesi ile ilgili olduğu anlaşılmıştır.
- "com.apple.airport.preferences.plist" dosyasında bir telefona ait birden fazla MAC adresi olduğunda ilk sırada olan MAC adresi o telefonun kendi MAC adresidir. Ancak buradaki MAC adresinin yine ilk oktet değerine dikkat edilmelidir.
- Veri analizi sırasında incelenen dosyalarda tespit edilen ANDROID işletim sistemine sahip telefonların MAC adresleri ya tamamen doğru olmakta ya da ilk oktet değeri telefonun gerçek MAC adres bilgisinin ilk oktet değerinden iki bayt fazla olmaktadır.
- Yapılan uygulamalarda tespit edilen MAC adresleri üretici firma ile MAC adresi eşleştiren veri tabanlarında sorgulatıldığı zaman herhangi bir üretici ile eşleşmiyorsa iOS işletim sistemine sahip telefonlarda olduğu gibi MAC adresleri ilk oktet değerinden iki bayt çıkartıldığında bir üretici ile eşleştiği ve cihazın kendi MAC adresi olduğu görülmüştür.

4. Sonuçlar ve Tartışmalar (Results and Discussions)

4.1. İnceleme Önerileri (Examination Suggestions)

- Alınan kopyanın, Magnet AXIOM ile raporlanması durumunda, "ağ arayüzleri" başlığı içerisinde **yalnızca** en son bağlanılan iPhone marka telefonun yer aldığı, önceki ağ bağlantısı sağlanan iOS işletim sistemine sahip telefonlara ait herhangi bir verinin bulunmadığı görülmüştür. Böyle bir incelemenin yanıltıcı sonuçlara neden olabileceği öngörülmelidir. Bu aşamada gerçek sonuçlara ulaşabilmek adına "NetworkInterfaces" isimli .plist dosyasını manuel olarak analiz edip "MatchingMACs" kısmında da daha önce iOS işletim sistemine sahip telefon ile bağlantı sağlayıp sağlamadığına bakılmalıdır.
- iOS için, "NetworkInterfaces" isimli plist dosyasında bulunan MAC adresinin ilk oktet değerinden iki bayt eksilttiğinde cihazın gerçek MAC adres bilgisine ulaşıldığı tespit edilmiştir. Örneğin uygulamada elde edilen MAC adres bilgisi "B6:9C:DF:01:B3:DD" ise ilk oktet olan B6'dan iki bayt eksilttiğinde ("B4:9C:DF:01:B3:DD") gerçek MAC adres bilgisine ulaşılabildiği görülmüştür. Görüldüğü üzere iPhone cihazlar, USB üzerinden ağa bağlandıkları durumda MAC adres bilgisi doğru bir şekilde tespit edilmektedir. iOS ile gerçekleştirilen son uygulama sonucunda toplamda üç tane iPhone ile USB aracılığı ile ağ bağlantısı sağlanmıştır. Söz konusu bağlantılar sonucunda elde edilmesi hedeflenen veriler, adli bilişim inceleme yazılımıyla elde edilen veriler ve çalışmamızda önerdiğimiz metodolojinin uygulanması ile elde edilen veriler Tablo 13'te sunulmuştur.

- Kopyanın, "…\Macintosh HD\private\var\db\lockdown\" dosya dizininde; USB kablo ile bağlantı sağlanan *(ağ bağlantısı sağlanmamış olsa bile)* her iPhone cihaz için plist dosyası yer almaktadır. [23] USB ile bağlanan iPhone cihazlarının gerçek MAC adreslerinin bu dosyada tutulduğu tespit edilmiştir. Buradan elde edilen MAC adres bilgisi ile "NetworkInterfaces" isimli plist dosyasından elde edilen MAC adresinin ilk oktet değerinden iki bayt eksiltilip elde edilen değer karşılaştırıldığında birebir aynı sonucu vermelidir.
- MAC adresinde yer alan ilk üç oktet, üretici firmayı belirlemek için kullanılmıştır. Elde edilen MAC adres bilgisinde yer alan ilk üç oktet internet ortamında sorgulandığında elde edilecek olan üretici firma adı, cihazın üretici firma adı ile karşılaştırılabilir. Örneğin; "NetworkInterfaces" isimli dosyada yer alan MAC adres bilgisinin ilk oktetinin "9A:00:C6" olduğu durumda, ilk oktet 9A değerinden iki bayt eksilttiğinde çıkan değer 98:00:C6 olacaktır. 98:00:C6 değeri internet ortamında MAC adres bilgisi ile üretici firma karşılaştıran veri tabanında sorgulanmıştır. Böylelikle üretici olarak karşımıza Apple firmasının çıktığı tespit edilmiş ve cihazın Apple 'a ait bir ürünü olduğu görülmüştür. İnceleme yazılımlarından elde edilen MAC adres bilgisi doğrudan raporlandığı takdirde uyuşmazlıklara sebebiyet vermektedir. Çünkü inceleme yazılımlarının tespit ettiği MAC adres bilgisini internet ortamında sorguladığımızda herhangi bir üretici firma adı ile eşleşmediği görülmüştür.
- macOS'a Wi-Fi aracılığı ile iPhone telefona bağlandığında macOS içerisinde yer alan "com.apple.airport.preferences.plist" ve "netusage.sqlite" isimli dosyalarda tutulan MAC adres bilgilerinin, telefonun gerçek MAC adresi ile aynı olmadığı tespit edilmiştir. iPhone telefonların gerçek MAC adres bilgileri anahtar kelime olarak aratılmış fakat herhangi bir sonuç elde edilememiştir. Adli bilişim inceleme yazılımları ile tespit edilen MAC adres bilgilerinin doğrudan rapora eklenmesi yerine bu durumun raporda belirtilmesi gerekmektedir.
- ANDROID işletim sistemine sahip telefonlar için "com.apple.airport.preferences.plist" dosyasında bir telefona ait birden fazla MAC adresi görülebilir. Bu durumda ilk sırada olan MAC adresinin telefonun kendi MAC adresi olduğu diğer MAC

Tablo 13. iOS telefonlar ile USB bağlantısı sağlanan uygulamalar sırasında (iOS uygulama1-2-5) adli bilişim yazılımı ile elde edilenler ve sunulan öneriler ile tespit edilen sonuçlar (The results obtained with the forensic software during the applications with USB connection with iOS phones (iOS application1-2-5) and the results obtained with the suggestions presented)

iOS ile USB bağlantısı sağlanan uygulamalar	Tespit edilmesi hedeflenen kayıtlar	İnceleme yazılımı ile tespit edilen kayıtlar	Önerilen analiz yöntemi bağlanılan tüm gerçek MAC adreslerine ulaşılabildi mi?
iOS uygulama-1	iOS uygulama-1'de kullanılan telefona ait gerçek MAC adresi	iOS uygulama-1'de kullanılan telefon MAC kaydı (ilk oktet farklı)	Evet
iOS uygulama-2	iOS uygulama-1-2'de kullanılan telefonlara ait gerçek MAC adresi	Sadece iOS uygulama-2'de kullanılan telefon MAC kaydı (ilk oktet farklı)	Evet
iOS uygulama-5	iOS uygulama-1-2-5'de kullanılan telefona ait gerçek MAC adresi	Sadece iOS uygulama-5'de kullanılan telefon MAC kaydı (ilk oktet farklı)	Evet

adreslerinin ise "Wi-Fi ağını anımsa seçeneği aktif" iken ağ bağlantısı gerçekleştirilen diğer telefonlara ait olduğu tespit edilmiştir. Yine burada MAC adreslerinin ilk oktet değeri dikkate alınmalıdır.

- İnceleme sonucu elde edilen MAC adres bilgisi mutlaka internet üzerinden MAC adres bilgileri ile üretici firmaları sorgulayan veri tabanı ile sorgulatılmalıdır. Sorgulama sonucu elde edilen MAC adresi bir üreticiye ait değilse raporda belirtilmelidir.

4.2. Sonuçlar (Conclusions)

İşletim sistemlerinde bulunan veriler arasından MAC adres bilgilerinin tespiti büyük önem arz etmektedir. Adli bilişim yazılımı ile yapılan incelemeler sonucunda; işletim sisteminde tespit edilen MAC adres bilgilerinin her defasında farklı sonuçlar verebildiği, bağlantının nasıl yapıldığının çıkan sonuçları değiştirdiği, bir telefon için birden fazla MAC adresi kaydının düştüğü tespit edilmiştir. Bu nedenle yapılan çalışma sonucunda iOS telefonlar Wi-Fi üzerinden bağlantı sağlandığı takdirde, MAC adres bilgisinin telefona ait gerçek MAC adres bilgisinden tamamen farklı olduğu ve bu durumun incelemelerde göz ardı edilmemesi gerektiği önerilmektedir. Ayrıca öneriler bölümünde USB ile bağlantı sağlandığı takdirde MAC adres bilgisinin doğrusunun nasıl bulunacağı sunulmuştur. ANDROID cihazlar için hangi durumda birden fazla MAC adresi kaydı düştüğü gösterilmiştir. USB veya Wi-Fi ağı üzerinden bağlantı gerçekleştirilen telefonlara ait MAC adres bilgisinin tespitine yönelik yapılacak incelemeler; yalnızca adli bilişim inceleme yazılımlarının sonuçlarına göre yapılır ve inceleme neticesinde çıkan bu sonuçlar rapora doğrudan eklenir ise yapılan bu incelemenin dava sonucunu yanıltabileceği görülmüştür. Akbal vd.'nin yaptıkları çalışmada bahsettikleri gibi; incelemeci adli bilişim yazılımlarının verdikleri sonuçlarla yetinmemelidir [24].

Bu çalışmada inceleme yazılımı olarak Magnet AXIOM kullanılmıştır. Magnet AXIOM yazılımı ile yapılan analizler sırasında iOS işletim sistemine sahip telefonlar eğer USB ile bağlandıysa sadece son bağlanılan telefonu göstermektedir. Daha önce USB ile bağlanan iOS işletim sistemine sahip telefon varsa Magnet AXIOM yazılımı ile raporlama aşamasında gözden kaçmaması için ne yapılması gerektiği bu çalışmada gösterilmiştir. İleriki çalışmalarda yapılan uygulamalar başka inceleme yazılımları ile ya da Windows/Linux ortamında gerçekleştirilebilir. macOS bilgisayar ile ANDROID işletim sistemine sahip bir telefonun USB üzerinden ağ bağlantısının sağlanması için ek yazılıma ihtiyaç duyulmaktadır, bu yazılımlar temin edilip ANDROID işletim sistemine sahip telefonlar için USB üzerinden bağlantı uygulamaları yapılabilir. ANDROID işletim sistemine sahip farklı marka telefonlar ve iPhone 6s aşağısı model telefonlar ile uygulamalar gerçekleştirilebilir. Ayrıca MAC adresi rasgele seçiminin adli bilişim incelemelerini nasıl etkilediği araştırılabilir. Teknolojinin ilerlemesiyle beraber internetin hayatımızın her alanında olması aynı zamanda kullandığımız cihazların saldırılara karşı savunmasız kalmasına neden olmaktadır. Bunun farkında olan cihaz geliştiricileri MAC adres rasgele seçimini kullanmaya başlamıştır. MAC adres rasgele seçimi cihazların gerçek MAC adresleri yerine geçici rasgele MAC adresleri ile ağa bağlanmalarını sağlayan bir gizlilik tekniğidir [25]. Fenske vd., yaptıkları çalışmada MAC adresi rasgele seçimini gerçekleştiren cihazlar arasında uygulamada farklılıkların olduğunu, cihazların kendi içlerinde tutarsızlıklarının olduğunu cihazların uyku ya da etkin durumlarının MAC adresi rasgele seçimini etkilediğini belirtmişlerdir [26]. Bu durumda ileriki çalışmalarda, aynı marka-model ve aynı/farklı işletim sistemi sürümlerine sahip cep telefonları temin edilerek, ağ bağlantısı sırasında telefonun etkin veya uyku durumunda olması göz önüne alınması ile çeşitli uygulamalar gerçekleştirilebilir.

Teşekkür (Acknowledgement)

Bu çalışmadaki desteklerinden dolayı Jandarma Kriminal Daire Başkanlığına teşekkür ederiz.

Kaynaklar (References)

1. Garg U., Verma P., Moudgil Y., Sharma S., MAC and Logical addressing, International Journal of Engineering Research and Applications (IJERA), 2 (3), 474-480,2012.
2. Longo E., Redondi a., Cesana M., Pairing Wi-Fi and Bluetooth MAC addresses through passive packet capture, In Conference on 2018 17th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net), 1-4. 10.23919/MedHocNet.2018.8407082.
3. Imam A.Y., Mac Address Routing Policy Over The Ip Network, 3, 8-11,10.33564/IJEAST.2019.v03i11.002, 2019.
4. Martin J., Rye E., Beverly R., Decomposition of MAC address structure for granular device inference, In Proceedings of the 32nd Annual Conference on Computer Security Applications (ACSAC '16) Association for Computing Machinery, New York-USA, 78–88, 2016.
5. Gedik D., Bilişim Suçlarında Ip Tespiti ile Ekran Görüntüleri Çıktılarının İspat Değeri, Bilişim Hukuku Dergisi 1 (1), 51-84, 2019.
6. Sarwar M., Soomro T.R., Impact of smartphone's on society, European journal of scientific research, 98 (2), 216–226, 2013.
7. Kim K., Min A.W., Gupta D., Mohapatra P., Singh J.P., Improving energy efficiency of Wi-Fi sensing on smartphones, Proceedings IEEE INFOCOM, Shanghai, 2930-2938, 2011.
8. Aslan Ö., Samet R., A Comprehensive Review on Malware Detection Approaches, IEEE Access, 8 (1-1), 6249-6271,2020.
9. Seo J.W, Lee S.J., A study on efficient detection of network-based IP spoofing DDoS and malware-infected Systems, SpringerPlus, 5 (1), 2016.
10. Blackman D., Szewczyk P., The challenges of seizing and searching the contents of Wi-Fi devices for the modern investigator, In 13th Australian Digital Forensics Conference, Edith Cowan University Joondalup Campus, Perth, Western Australia, 37-48, 2015.
11. Champlain college leahy center for digital investigation. Mac OS X Forensic Artifact Locations. https://www.champlain.edu/Documents/LCDI/Report_Mac%20Forensics.pdf. Yayın tarihi Kasım 12, 2015. Erişim tarihi Haziran 20, 2021.
12. Niranjan R., Mac OS Forensics, Practical Cyber Forensics, An Incident-Based Approach to Forensic Investigations, Editör: Karkal N.,Apress, New York, A.B.D., 101-133,2019.
13. Mac4n6. Network and Application Usage using netusage.sqlite & DataUsage.sqlite iOS Databases. https://www.mac4n6.com/blog/2019/1/6/network-and-application-usage-using-netusagesqlite-amp-datausagesqlite-ios-databases. Yayın tarihi 6 Haziran,2019. Erişim tarihi Haziran 20, 2021.
14. Rathod D.R., MAC OSX: iMessage, Face Time, Apple Mail Application Forensics, journal of ınformatıon, knowledge and research in computer engineering, 4 (2),1000-1003, 2017.
15. Maddu B., Rao P.V.R.D., OS X artifact analysis, International Journal of Recent Technology and Engineering (IJERA), 7 (6S), 26-32, 2019.
16. The Senator Patrick Leahy Center for Digital Investigation Champlain College. Mac RAM Analysis. https://www.champlain.edu/Documents/LCDI/archive/MAC_RAM_analysis-report.pdf .Yayın tarihi Haziran 17, 2012. Erişim tarihi Haziran 15, 2021.
17. Rathod D.R., MAC OSX Forenscis, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 6 (8), 1240-1243, 2017.
18. Salamh F., Mirza M., Hutchinson S., Yoon Y., Karabiyik U, What's on the Horizon? An In-Depth Forensic Analysis of Android and iOS Applications, IEEE Access. PP. 1-1. 10.1109/ACCESS.2021.3095562, 2021.
19. Özen M., Özocak G., Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134), Ankara Barosu Dergisi, 0 (0), 2015.
20. Christopher M., Marcus R., iPod Forensics, International Journal of Digital Earth (IJDE), 4, 2005.
21. Tadani A., Firdous K., Snapchat Analysis to Discover Digital Forensic Artifacts on Android Smartphone, Procedia Computer Science, 109, 1035-1040, 10.1016/j.procs.2017.05.421, 2017.

22. Information Security Group Royal Holloway University of London. Mac OS X Forensics Technical Report. https://www.royalholloway.ac.uk/isg/documents/pdf/technicalreports/2015/rhul-isg-2015-8.pdf .Yayın tarihi Mart 4, 2015. Erişim tarihi Haziran 10, 2021.

23. Tamma R., Skulkin O., Mahalik H., Bommisetty S., Data Acquisition from iOS Devices, Practical mobile forensics, Packt, Birmingham, UK, 61-88, 2018.

24. Akbal E., Yakut Ö.F., Dogan S., Tuncer T., Ertam F., A Digital Forensics Approach for Lost Secondary Partition Analysis using Master Boot Record Structured Hard Disk Drives, Sakarya University Journal of Computer and Information Sciences, 2021.

25. Martin J., Mayberry T., Donahue C., Foppe L., Brown L., Riggins C., Rye E., Brown D., A Study of MAC Address Randomization in Mobile Devices and When it Fails, Proceedings on Privacy Enhancing Technologies, 10.1515/popets-2017-0054, 2017.

26. Fenske E., Brown D., Martin J., Mayberry T., Ryan P., Rye E., Three Years Later: A Study of MAC Address Randomization In Mobile Devices And When It Succeeds. Proceedings on Privacy Enhancing Technologies, 164-181. 10.2478/popets-2021-0042, 2021.