Journal of Medical Sciences 2021, 2(3) 67-77 **Araştırma Makalesi** / Research Article
https://doi.org/10.46629/JMS.2021.50

Discord Mesajlaşma Uygulamasının Mobil Cihazlarda Adli Bilişim Yönünden İncelenmesi

Digital Forensic Analysis of Discord Messaging Application on Mobile Devices

İsmail BARBAROS[1], Emel Hülya YÜKSELOĞLU[1]

İB: 0000-0001-5978-9008 **EHY:** 0000-0003-2009-6065

[1] İstanbul Üniversitesi-Cerrahpaşa, Adli Tıp ve Adli Bilimler Enstitüsü, İstanbul Türkiye

Öz

Amaç: Anlık mesajlaşma uygulamaları günümüzde yaygın olarak kullanılmaktadır. Bu uygulamaları kullanan kişiler suça maruz kalabileceği gibi kullanıcılar bu uygulamalarla suçta işleyebilmektedirler. Yaygın olarak mobil cihazlarda kullanılan anlık mesajlaşma uygulamalarından delil elde etmek için adli bilişim yazılımlarından faydalanılmaktadır. Her geçen gün yeni bir mesajlaşma uygulamasının geliştirilmesi adli bilişim uzmanlarının işlerini de zorlaştırmaktadır. Anlık mesajlaşma uygulamalarının yeni bir örneği olan Discord mesajlaşma uygulamasını kullanan mobil cihazlardan adli bilişim yöntemleri kullanılarak delil olabilecek hangi bulguların elde edilebileceği araştırılmıştır.

Gereç ve Yöntem: Araştırmamızda farklı işletim sistemlerine sahip iki mobil cihaza Discord mesajlaşma uygulaması yüklenmiştir. Bu uygulamalar aracılığıyla iki mobil cihaz arasında mesajlaşma, dosya alışverişi gerçekleştirilmiştir. Etkileşimler neticesinde her iki mobil cihazın adli kopyası alınarak adli bilişim yöntemleri ile incelenmiştir.

Bulgular: Her iki mobil cihazda da karşıdaki cihaz ile ilgili sınırlı bilgiye erişilebildiği tespit edilmiştir. Cihazlar arasında etkileşimi gösteren çeşitli bulgular tespit edilebilmiştir. Gönderilen bazı dosyaların sadece cihaz üzerinde değil Discord sunucuları üzerinden de tespit edilebildiği görülmüştür.

Tartışma ve Sonuç: Dinamik bir alan olan adli bilişimin teknolojik gelişmelere çabuk adapte olması gerekmektedir. Bu kapsamda incelenen Discord mesajlaşma uygulaması aracılığıyla işlenebilecek suçların tespitine yönelik adli bilişim yöntemleri ile deliller elde edilebileceği tespit edilmiştir. Discord mesajlaşma uygulaması ile ilgili literatürde çok fazla makale bulunmadığından bu çalışmanın adli bilişim uzmanlarının incelemelerine katkı sağlayacağı değerlendirilmektedir. Bu çalışmada tespit edilen bulguların bilgisayarlardan elde edilebilecek bulgularla karşılaştırılabileceği de öneri olarak sunulmuştur.

Anahtar Kelimeler: Adli bilimler, anlık mesajlaşma uygulaması, elektronik delil, adli bilişim

Abstract

Aim: Instant messaging applications are widely used in these days. People who use these applications can be exposed to crime as well as they can commit crimes with these applications. Forensic softwares are used to obtain evidence from instant messaging applications that are commonly used on mobile devices. The development of a new messaging applications every day makes work hard for forensic experts. In our study, what findings can be obtained by using forensic methods from mobile devices using Discord messaging application, which is a new example of instant messaging applications, was investigated.

Material and Methods: In our research, Discord messaging application was installed on two mobile devices with different operating systems. Messaging and file exchange between two mobile devices were carried out through these applications. As a result of the interactions, forensic images of both mobile devices were extracted and examined with forensic methods.

Results: It has been determined that limited information about the opposite device can be accessed on both mobile devices. Various findings indicating interaction between devices could be detected. It has been observed that some files which was sent through application can be detected not only on the devices but also on Discord servers.

Discussion and Conclusion: Digital forensic, which is a dynamic field of forensic sciences, needs to adapt quickly to technological developments. In this context, it has been determined that evidence can be obtained by digital forensic methods for the detection of crimes that can be committed through the Discord messaging application. Since there are not many articles in the literature about the Discord messaging application, it is considered that this study will contribute to the investigations of forensic experts. It is also suggested that the findings of this study can be compared with the findings that can be obtained from computers.

Key Words: Forensic Sciences, instant messaging applications, digital evidence, digital forensics

Sorumlu Yazar / Corresponding Author:İsmail BARBAROS
E-posta: ismailbrbrs@gmail.com, ismail.barbaros@ogr.iu.edu.tr

Giriş

İnternet teknolojisinin temelinde iletişim yer almaktadır. İnternet üzerinden en yaygın kullanılan iletişim yöntemi ise anlık mesajlaşma uygulamalarıdır. Önceleri sadece metin (yazı) gönderimi yapılabilen anlık mesajlaşma uygulamaları ile günümüzde farklı şekillerde de iletişim kurulabilmektedir. Artık kullanıcılar birbirleriyle sesli veya görüntülü arama da gerçekleştirebilmektedirler. Ayrıca metin yerine ses, resim, video, ofis dosyaları gibi formatlarda da dosyalar anlık mesajlaşma uygulamaları ile iletilebilmektedir.(1)

Kullanıcılar arasındaki anlık mesajlaşma isminden de anlaşılacağı gibi gerçek zamanlı olmaktadır. Yani herhangi bir anlık mesajlaşma uygulamasında mesaj yazan kişi gönder tuşuna bastığında karşı taraf bunu sohbet penceresinde çok kısa bir süre içerisinde görebilmektedir. Anlık mesajlaşma uygulamalarında genel olarak sohbet penceresinde önceki yazışmalar da görüntülenebilmektedir. Kullanıcılar metin mesajlaşmasında genellikle karşılıklı konuşmada olduğu gibi kısa cümleler kurabilirken uzun metinleri de gönderilebilmektedirler. Gönderilen veya alınan metin mesajları genellikle uygulamanın kurulduğu cihaz (bilgisayar veya mobil cihaz) üzerinde bir veri tabanında saklanmaktadır. Ayrıca gönderilen çeşitli formatlardaki dosyalar da ayrı klasörlerde veya veri tabanında saklanabilmektedir.

Görüntülü ve sesli arama, dosya gönderip alabilme özellikleri bu uygulamaların farklı amaçlarda kullanılmasını da sağlamaktadır.

Özellikle 2020 yılında ortaya çıkan küresel salgın nedeniyle ön plana çıkan ve artan iletişim ihtiyacı ile bu uygulamalar bireysel kullanımın ötesinde amaçlar için de kullanılmaya başlanmıştır. İnsanların ruh sağlığı için düzenli olarak gittikleri terapilerin telefonla yada çevrimiçi olarak anlık mesajlaşma ve sosyal medya uygulamaları üzerinden gerçekleştirildiği örneklerle karşılaşılmıştır.(2) Sağlık alanında bilgilendirme broşürleri, sağlık videoları, egzersiz programları whatsapp vb. mesajlaşma uygulamaları üzerinden paylaşılmış (2), hastaların dermatolojik şikâyetleri görüntülü konuşma ve paylaşılan resimler üzerinden görsel muayene ile teşhis edilmeye çalışılmıştır.(3) Uzun süren karantina tedbirlerinin eğitim faaliyetlerini de engellemesi çevrimiçi teknolojilerin bu alanda kullanımını da artırmıştır. Eğitimciler ve öğretmenler ilk şoku atlattıktan sonra eğitimin durmaması için öğrencilerinin ilgisini canlı tutacak yaratıcı çözümler üretmişlerdir. Çoğu ülkede yüz yüze eğitim yerini geçici olarak çevrimiçi eğitime bırakmıştır. Farklı çevrimiçi uygulamaların (Skype, Zoom, Hangouts vb.) yanında Whatsapp, Discord gibi anlık mesajlaşma uygulamalarının da kullanıldığı bilinmektedir. (4)

Discord, video oyunu oyuncularının arasındaki iletişimi iyileştirmek için 2015 yılında geliştirilmiş bir iletişim platformudur. Kullanıcılarına sesli ve görüntülü konuşma ile metin mesajlaşması imkanı tanımakta, çeşitli formatlardaki dosyaları oluşturdukları gruplarda paylaşabilmelerini sağlamaktadır. Farklı işletim sistemlerinde (bilgisayar ve mobil cihazlar) kurulabilen bu uygulama ile kullanıcılar sadece oyun değil farklı konularda topluluk oluşturup ilgi alanları hakkında sohbet edip, paylaşım yapabilmektedirler. (5)

Yaygın olarak kullanılmaya başlanan bu uygulamalar, diğer bilişim teknolojileri gibi suç işlemekte veya suça yardımcı olarak kullanılabilmekte, suçluların kendi aralarında rahatça iletişim kurmalarını sağlayabilmektedir. (6) Yasadışı malzeme (silah, uyuşturucu vb.) dağıtımı/pazarlanması, hakaret, propaganda amaçlı eğitimler verilmesi, terör eylemlerinin planlanması, siber zorbalık, telif haklarına aykırı dosya paylaşımında bulunulması bunlardan bazılarıdır.

Adli bilimlerin temel amacı suçu aydınlatmak için gerekli delillerin tespiti ve mahkemeye sunulması olarak özetlenirse, anlık mesajlaşma uygulamaları da işlenmiş bir suçu aydınlatabilecek delilleri barındırabildiğinden bu disiplinin ilgi alanına girmektedir. Çalışmamızın amacı, anlık mesajlaşma uygulamalarından biri olan Discord uygulamasından mobil cihazlar üzerinde adli bilişim yöntemleri kullanılarak hangi delillerin elde edilebileceğinin tespit edilip, iki farklı mobil işletim sisteminde (IOS ve Android) elde edilebilecek delilleri karşılaştırmaktır.

Yaptığımız literatür çalışmasında bu uygulamalardan delil elde edilmesi ile ilgili çeşitli çalışmalar yapıldığı görülmektedir. Yayınlardan birinde (7) anlık mesajlaşma uygulamaları üzerinde yapılan yazışmalardan faile ulaşılıp ulaşılamayacağı, yazışmalardan elde edilebilecek delillerin neler olduğu ve bu yazışmaların nasıl sınıflandırılabileceği üzerine çalışıldığı, ikisinde (8 ve 9) anlık mesajlaşma uygulamalarının mobil cihazlarda yaygınlaşmasıyla popülerlik kazanan örneklerinden delil elde edilme yöntemlerinin incelendiği görülmüştür. Uygulama marketlerinden indirilme sayısı artan uygulamalar adli bilişim yazılımı üreticilerini de yazılımlarını bu uygulamalardan delil elde edebilecek şekilde geliştirme-

lerine neden olmaktadır. Adli bilişim yazılımlarının tespit edebildiği delillerin karşılaştırıldığı bir çalışmada, önde gelen adli bilişim yazılımlarının gençler arasında yaygın kullanılan anlık mesajlaşma uygulamalarından delil elde edip edemediği ve elde ettikleri delillerin karşılaştırılması konu edilmiştir. (10)Çalışmamıza konu olan Discord uygulamasından delil elde edilmesi ile ilgili yapılan yayınlar incelendiğinde ise, birinde (11) Windows işletim sistemi kurulu bilgisayarlar üzerinde Discord uygulamasının analiz edildiği, diğerinde (12)farklı işletim sistemine (Windows, Linux ve MacOS) sahip bilgisayarlarda Discord uygulamasının incelendiği görülmüştür. Bu çalışmalar bilgisayarlar üzerinde yapıldığı için farklı işletim sistemlerine sahip mobil cihazlarda da bu incelemelerin yapılması gerektiği değerlendirilmiştir. Mobil cihazlar üzerinde daha önce yapılan çalışmalar araştırıldığında, (11)'de aktarılan (13)'de android mobil cihazlar üzerinde Discord uygulamasının adli bilişim yönünden incelemesinin yapıldığı belirtilmiş olmakla birlikte, bu makalenin Kore alfabesinde yazılmış olması detaylı bir inceleme yapılmasını engellemiş; ancak yine de makalede sadece android işletim sistemi üzerinde inceleme yapıldığı tespit edilmiştir. Android telefonların haricinde IOS işletim sistemine sahip Apple marka mobil cihazlarda da inceleme yapılmasının bu alandaki boşluğu doldurmak için gerekli olduğu değerlendirilmiştir.

Yöntem

Adli bilişim incelemeleri gerçekleştirilirken Amerikan Ulusal Standartlar ve Teknoloji Enstitüsünün genel kabul görmüş 4 aşamalı (Delilin korunması, birebir kopyasının alınması, incelenip analiz edilmesi ve raporlanması) adımları izlenmiştir. (14)

Testlerde Tablo 1'de görülen farklı işletim sistemlerine sahip iki adet mobil cihaz kullanılmıştır.

Delilin korunması aşamasında iki telefon üzerinden paylaşımlar yapıldıktan sonra telefonlar kapatılmıştır. İncelemeler birebir kopya (imaj) üzerinden yapılmıştır.

İmaj alma, inceleme ve analiz için Windows 10 işletim sistemi kurulu MSI marka bir bilgisayar kullanılmıştır. Mobil cihazların birebir kopyaları UFED 4 PC adli bilişim yazılımı ile alınmış ve UFED Physical Analyzer adli bilişim yazılımı ile incelenmiştir. (Tablo 2)

Tablo 1 Test telefonları

Marka	Model	İşletim Sistemi
Apple	A1586	IOS
Samsung	A310F	Android (Rooted)

Tablo 2

Marka	Model	Versiyon
Cellebrite	**UFED** 4PC	7.44.0.80
Cellebrite	UFED PA	7.44.1.3

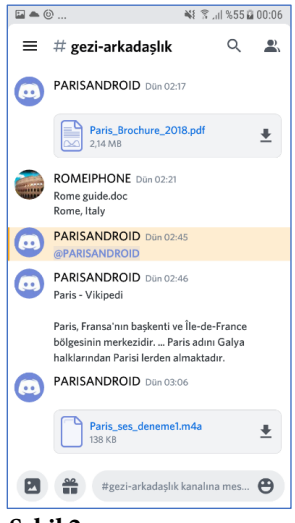
Discord uygulamasının IOS işletim sistemi yüklü cihaza Apple uygulama marketi Appstore'dan 70.0(25025) versiyonu, android işletim sistemi yüklü cihaza Google Playstore üzerinden 70.7(1519) versiyonu yüklenmiştir. Uygulamaya girmek için cep telefonu ya da elektronik posta adresi ile kullanıcı oluşturmak gerekmektedir. Tablo 3'te belirtilen e-posta adresleri ile kullanıcılar oluşturulmuştur.

Tablo 3

Kullanıcı	E-posta Adresi	İşletim Sistemi
PARASANDROİD	paris4321@mail.com.tr	Android
ROMEIPHONE	rome9876@mail.com.tr	IOS

Iphone'daki kullanıcı ile "ROMEIPHONE'un sunucusu" isimli bir sohbet odası (sunucu) kurulmuştur. Metin yazışmaları için gezi-arkadaşlık isimli bir sohbet kanalı kurulmuştur. (Şekil 1)

Şekil 1



Şekil 2

Her iki kullanıcı ile karşılıklı metin mesajları gönderilmiş, resim, ses ve video dosyaları paylaşılmıştır. ***Şekil 2***

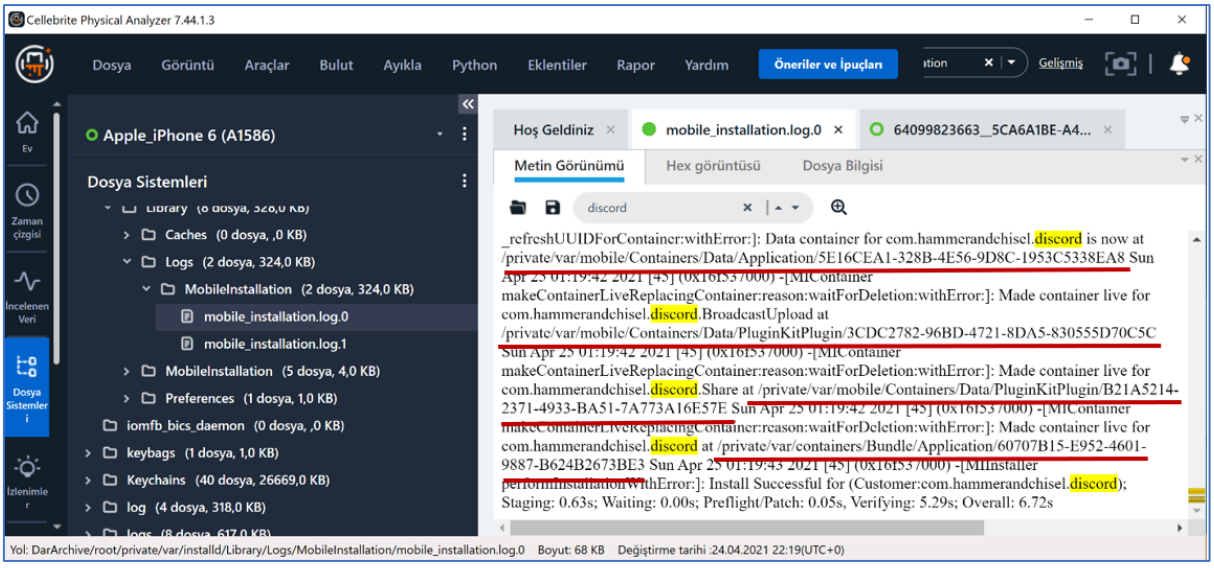
Bulgular

Her iki cihazın birebir kopyaları UFED 4PC yazılımı ile alındıktan sonra UFED Physical Analyzer yazılımı ile incelenmiştir.

Adli bilişim yazılımı ile yapılan ilk incelemede Discord uygulamasına ait sohbet mesajlarının otomatik olarak ortaya çıkarılmadığı görülmüştür. Manuel olarak yapılan incelemede uygulamaları kurduktan sonra oluşan dosyalar detaylı incelenmiş, anahtar kelime arama yöntemi ile kullanıcı adları ve sohbet mesajları araştırılmıştır.

IOS işletim sisteminde tespit edilenler

IOS işletim sistemine sahip cihazın birebir kopyası üzerinde yapılan incelemede; uygulama kurulduktan sonra "mobile_installation.log" dosyası içerisinde Discord uygulamasının kurulduğu klasörlerin isimlerinin yer aldığı görülmüştür. Log içerisinde uygulamanın kurulduğu saat (UTC+3 eklenmeli) bilgisi de yer almaktadır. (Şekil-3)



Şekil 3

Bu klasörlerin içerisinde bulunan dosyaların ayrıntılı incelemesinde,

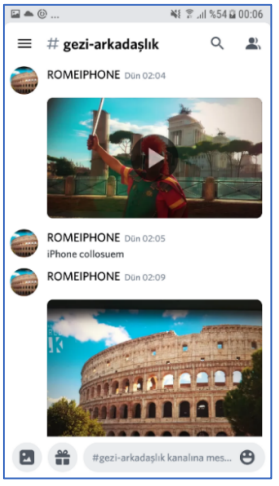
DarArchive/root/private/var/mobile/Containers/Data/Application/5E16CEA1-328B-4E56-9D8C-1953C5338EA8/Library/Caches/com.hammerandchisel.discord/fsCachedData/0C1F625C-C650-4E9A-8237-B450CEB0700C

klasör yolu altında bulunan 0C1F625C-C650-4E9A-8237-B450CEB0700C isimli dosyada iki kullanıcı arasında "gezi-arkadaşlık" kanalında yapılan konuşmaların kaydedildiği tespit edilmiştir. Şekil 4'te görülen yapıda; mesajın gönderildiği kanal numarası, "835662297668583428l" mesajı gönderen kullanıcı "PARISANDROID", kullanıcı tanımlama numarası "835642093522649129" mesaj içeriği ve mesajın gönderildiği zaman bilgisi "25.04.2021 02:46" bulunmaktadır. Kanalda bir dosya paylaşılmışsa Şekil 5'te görüldüğü şekilde ek (attachment) olarak paylaşılmaktadır.

Şekil 4

Şekil 5

Gönderilen dosyanın adı, boyutu ve bir web adresi ile gönderilmektedir. (Şekil 5) Bu web adresi bir internet tarayıcıya kopyalanıp adrese gidildiğinde belirtilen dosyaya erişilebildiği tespit edilmiştir. Bu şekilde herhangi bir kısıtlama olmadan web adresindeki bilgiler ile dosyaya internet üzerinden erişim sağlanabilmektedir.

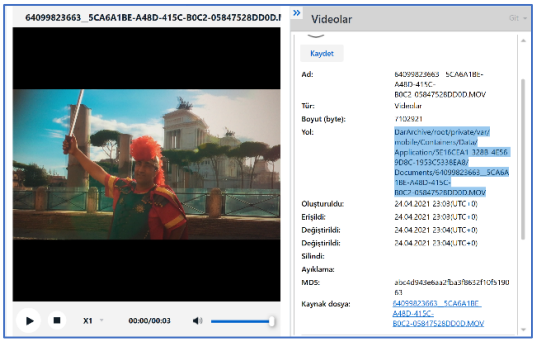


Şekil 6

Kanal üzerinden gönderilen (Şekil 6) daki resim ve video dosyalarına

DarArchive/root/private/var/mobile/Containers/Data/Application/5E16CEA1-328B-4E56-9D8C-1953C5338EA8/Documents

klasörü altından erişilebildiği tespit edilmiştir. Şekil 7

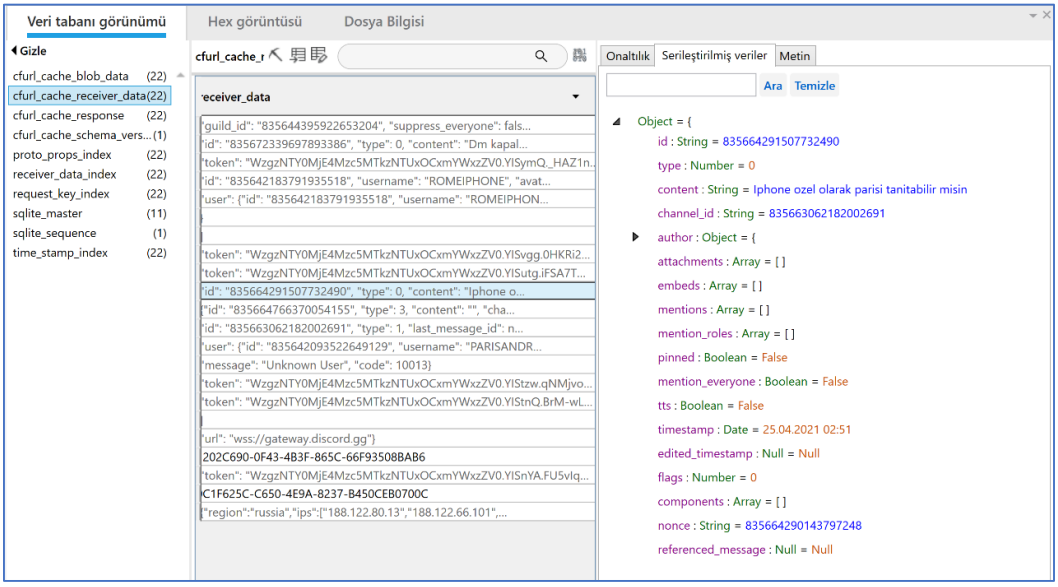


Şekil 7

DarArchive/root/private/var/mobile/Containers/Data/Application/5E16CEA1-328B-4E56-9D8C-1953C5338EA8/Library/Caches/com.hammerandchisel.discord/

Klasör yolu altında bulunan "Cache.db" dosyası içerisinde yapılan incelemede, her iki kullanıcının arasında geçen Şekil 8'deki "Direkt Mesaj-DM" mesajlaşmalarının bulunduğu görülmüştür. (Şekil 9)

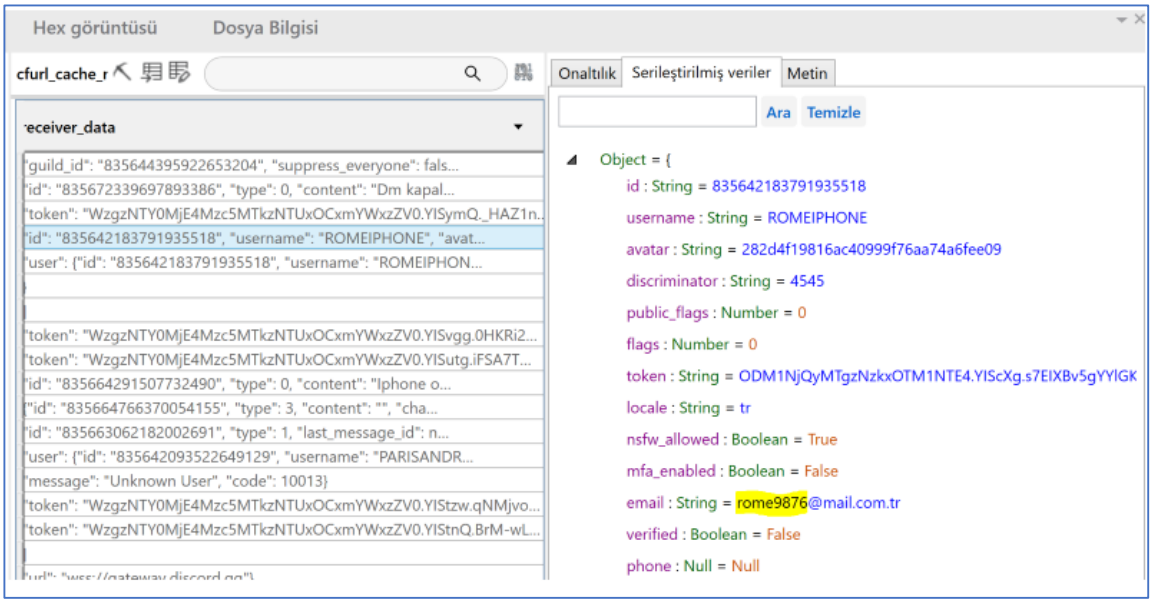
Şekil 8



Şekil 9

"Cache.db" veritabanı dosyasında sunucuyu kuran iphone cihazdaki kullanıcı "ROMEIPHONE"un uygulamaya kaydolurken kullandığı e-posta adresi "rome9876@mail.com.tr" tespit edilmiştir. (Şekil 10)

"Direkt Mesajlaşma - DM" kanalı (channel_id:835663062182002691) üzerinden yapılan sesli aramaların başlangıç ve bitiş zamanlarının da "Cache.db" veritabanına kaydedildiği tespit edilmiştir. Şekil 8'deki arama zamanı 02:53 ve arayan ve aranan kullanıcıların isimleri Şekil 11'de görülmektedir.



Şekil 10

Şekil 10, IOS işletim sistemi üzerinde yapılan incelemede karşı tarafta bulunan "PARISANDROID" kullanıcısının e-posta adresi "paris4321@mail.com.tr" tespit edilememiştir.


```
[{"id" : "835664766370054155",
        "type" : 3,
        "content" : "",
        "channel_id" : "835663062182002691",
        "author" : {"id" : "835642093522649129",
            "username" : "PARISANDROID",
            "avatar" : null,
            "discriminator" : "1040",
            "public_flags" : 0},
        "attachments" : [],
        "embeds" : [],
        "mentions" : [{"id" : "835642183791935518",
                "username" : "ROMEIPHONE",
                "avatar" : null,
                "discriminator" : "4545",
                "public_flags" : 0}],
        "mention_roles" : [],
        "pinned" : false,
        "mention_everyone" : false,
        "tts" : false,
        "timestamp" : 2021-04-25T02:53:26,
        "edited_timestamp" : null,
        "flags" : 0,
        "components" : [],
        "call" : {"participants" : [
                "835642093522649129",
                "835642183791935518"],
            "ended_timestamp" : 2021-04-25T02:54:36}
```


Şekil 11

Android işletim sisteminde tespit edilenler

Android cihaz üzerinde yapılan incelemede karşı tarafta bulunan "ROMEIPHONE" kullanıcısının e-posta adresi tespit edilememiştir. Ancak "PARISANDROID" kullanıcısının e-posta adresi

USERDATA(ExtX)/Root/data/com.discord/files/

klasör yolu altında "STORE_USERS_ME_V12" dosyası içerisinde tespit edilmiştir. (Şekil 12)


```
..com.discord.models.us
er.MeUse.....paris4321
@mail.com.t.............
............PARISANDROI
.
```


Şekil 12

İki kullanıcının arasında geçen mesajlaşmalar, (Şekil 13, Şekil 14) gönderilen dosyaların isimleri ile bu dosyalara erişim için kullanılabilecek olan ve daha önce bahsedilen web adresi bilgisinin,

USERDATA(ExtX)/Root/data/com.discord/files/

Klasörü altındaki

"STORE_MESSAGES_CACHE_V29" isimli dosyaya kaydedildiği görülmüştür. (Şekil 15, Şekil 16)


```
2021-04-24T23:47:36.461
000+00:0.............
.......104.............
..........PARISANDROI..
..............Android
dogrudan yanit verdigim
 mesa..................
..............841834723
65843251.........2021-0
4-24T23:50:09.872000+00
:0.....................
.454...................
....ROMEIPHON..........
.......Iphone ozel olar
ak parisi tanitabilir m
isi...................
............83566429014
379724.........2021-04-
24T23:51:32.987000+00:0
.....................1
04.....................
```


Şekil 13

Şekil 14


```
Paris_ses_deneme1.m4...
...https://media.discor
dapp.net/attachments/83
5644492274204763/835668
108584026112/Paris_ses_
deneme1.m4a.......https
://cdn.discordapp.com/a
ttachments/835644492274
204763/8356681085840261
12/Paris_ses_deneme1.m4
a.........104..........
.............PARISANDRO
I.....................
.....................
....84183887640526848..
.......2021-04-25T00:06
:43.111000+00:0........
```


Şekil 15


```
...............ROMEIPH
ON.....................
.....................
.............2021-04-24
T23:09:41.117000+00:0..
...............Paris_B
rochure_2018.pd......ht
tps://media.discordapp.
net/attachments/8356444
92274204763/83565580357
3633094/Paris_Brochure_
2018.pdf........https:/
/cdn.discordapp.com/att
achments/83564449227420
4763/835655803573633094
/Paris_Brochure_2018.pd
f.........104..........
```


Şekil 16

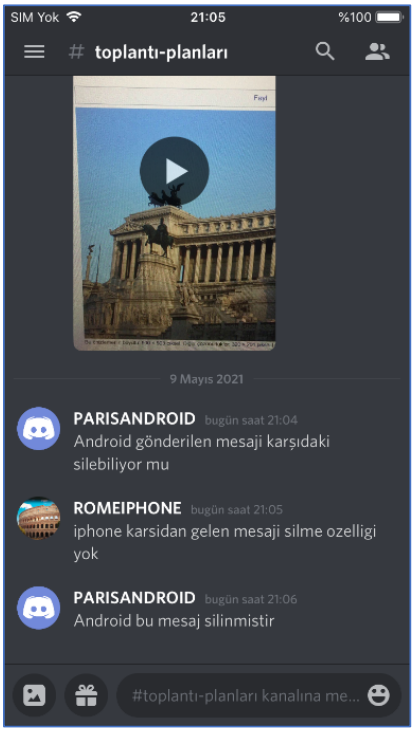
Şekil 11'deki arama bilgilerine android işletim sistemindeki

USERDATA(ExtX)/Root/data/com.discord/files/

dosyalar altında ulaşılamamıştır.

Silinmiş Mesajların Tespit Edilmesi

Silinmiş mesajların cihazlar üzerinde tespit edilip edilemeyeceğine yönelik yapılan incelemelerde, gönderilen metin mesajlarından, pdf uzantılı adobe reader ve jpg uzantılı resim dosyalarından bazıları silinmiştir. Silinen bu dosyaların tespit edilmesine yönelik inceleme yapılmıştır.



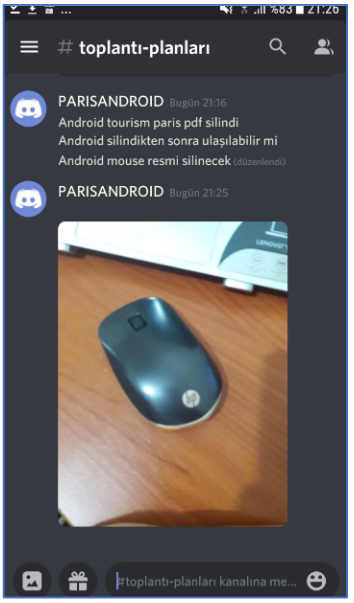
Şekil 17

Şekil 17'de görülen ekran görüntüsünde "PARISANDROID" kullanıcısının saat 21:06'da göndermiş olduğu "Android bu mesaj silinmiştir" mesajı "PARISANDROID" kullanıcısı tarafından silinmiştir. Silinen bu mesaj hem Android (Şekil 18), hem de IOS (Şekil 19) işletim sistemindeki cihazlarda tespit edilememiştir. Aşağıda görüldüğü gibi her iki işletim sisteminde mesajların tutulduğu dosyalar incelendiğinde 21:06'daki (Zaman dilimine UTC +3 eklenmeli) silinen mesajdan önceki ve sonraki mesajlar görüntülenebildiği halde silinen bu mesaja ulaşılamamıştır.

Şekil 18

Şekil 19

Silinen metin mesajından sonra sohbet esnasında paylaşılan dosyalardan (doküman, resim vb.) silinmiş olanları ile ilgili yapılan incelemede Şekil 20'deki resim "PARISANDROID" kullanıcısı tarafından "toplantı-planları" sohbet kanalında paylaşılmıştır.



Şekil 20

Telefonun kamerası ile çekilen 20210509_211719.jpg dosya isimli bu resmin tespiti için her iki cihazın birebir kopyalarında dosya isminden türetilen anahtar kelimeler aratılmıştır.

Android işletim sistemine sahip cihazda

USERDATA(ExtX)/Root/data/com.discord/files/

klasörü altındaki

STORE_MESSAGES_CACHE_V30

dosyası içerisinde bu ismin geçtiği ve paylaşım yapılırken iletilen web adresinin tespit edilebildiği görülmüştür. (Şekil 21)

IOS işletim sistemine sahip cihazda da

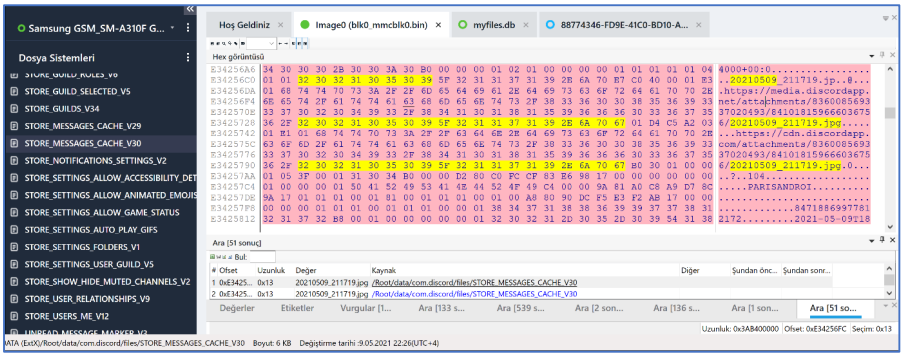
DarArchive/root/private/var/mobile/Library/UserNotifications/com.hammerandchisel.discord/

klasörü altındaki

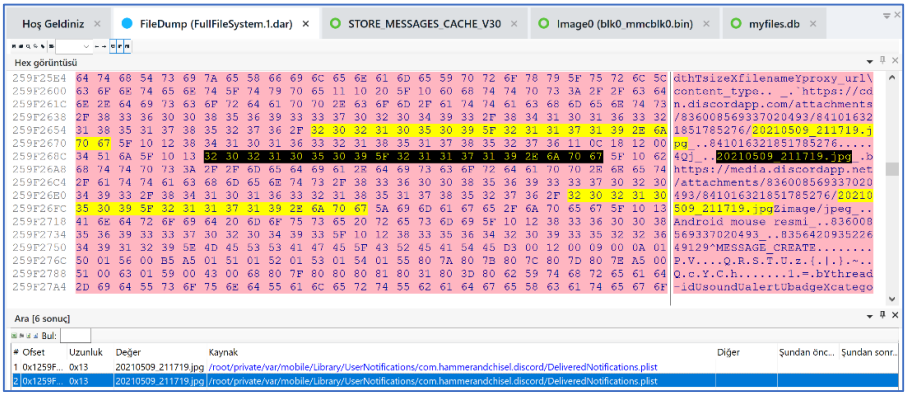
DeliveredNotifications.plist

dosyası içerisinde bu ismin geçtiği ve paylaşım yapılırken iletilen web adresinin tespit edilebildiği görülmüştür. (Şekil 22)

Mesajın içeriğindeki web adresi bir internet tarayıcıya kopyalanıp ilgili resme ulaşmak istenildiğinde herhangi bir parola şifre sormadan erişilebilir olduğu görülmüş, ancak ne kadar süre erişilir olacağına yönelik inceleme



Şekil 21



Şekil 22

yapılmamıştır. (**Şekil 23**)

https://media.discordapp.net/attachmen

ts/836008569337020493/841016321851785276/20210509_211719.jpg

Şekil 23

Tartışma ve sonuç

Adli bilimlerin en dinamik alanlarından biri olan adli bilişim yeni teknolojilere ve trendlere hızlı bir biçimde adapte olmak zorundadır. Suçlular yeni çıkan her türlü uygulamayı kendi menfaatleri için kullanabilmektedir. Bu kadar hızlı gelişen bir alanda adli bilişim uzmanlarının iş yükünü azaltacak olan adli bilişim yazılımı üreticileri maalesef bu hıza ayak uyduramamaktadır. Kullanıcılar arasında yeni bir uygulama popüler hale gelince bilgisayar veya mobil cihazlardan bu uygulama ile ilgili elde edilebilecek deliller adli bilişim yazılımları tarafından otomatik olarak tespit edilememektedir. Bu sebeple yeni uygulamalarla ilgili adli bilişim alanında ne kadar çok inceleme/deney yapılıp akademik yayın hazırlanırsa alanda çalışan uzmanların işi o kadar kolaylaşacaktır.

Adli bilişim yazılımlarının henüz otomatik olarak delil tespit edemediği bir uygulama ile ilgili eksikliği gidermek amacıyla hazırlanmış olan çalışmamızda, literatürde az sayıda yayın hazırlanmış olan Discord mesajlaşma uygulaması, mobil cihazlarda adli bilişim yöntemleri ile incelenmiştir. İki farklı işletim sisteminde de tespit edilen verilere bakıldığında IOS işletim sistemine sahip cihazlarda Android işletim sistemine sahip cihazlara göre daha fazla veri elde edilebildiği görülmüştür.

IOS işletim sisteminde dosya adlarının yanında dosyaların kendilerine de cihaz üzerinden ulaşılabilmiştir.

Her iki işletim sisteminde farklı dosya ve klasör yapısı mevcut olup, elde edilebilen verilerde de farklılıklar bulunmaktadır. Kullanıcılara ait e-posta adresleri sadece kendi cihazlarında tespit edilebilmiş, karşıdaki cihazı kullanan kullanıcının e-posta bilgisi bulunamamıştır. Kullanıcı adları ve uygulamanın otomatik olarak belirlediği kullanıcı tanımlama numaraları her iki işletim sisteminde de tespit edilebilmiştir. Metin mesajları dışında gönderilen ve alınan farklı formatlardaki dosyaların isimleri her iki cihazda da tespit edilebilirken dosyaların kendisi, discord uygulamasına ait klasörler altında IOS cihazda tespit edilebilmiş, uygulamanın içerisinden kamera aracılığıyla çekilen resimler dışında Android cihazda dosyalar tespit edilememiştir.

Uygulamanın diğer popüler anlık mesajlaşma uygulamaları gibi (whatsapp, telegram vb.) metin mesajlarını şifreli olarak saklamaması nedeniyle delil elde edebilmenin nispeten kolay olduğu görülmüştür. İleride uygulamaya bir şifreleme özelliği eklenirse bunun da tekrar analiz edilmesi faydalı olacaktır.

Discord uygulaması kullanılarak mesajlaşma, dosya paylaşımı yoluyla işlenebilecek suçlarda suçun tespitine ve delillendirilmesine yönelik olarak sadece eldeki cihazlar değil, Discord sunucularından da delil elde edilebildiği görülmüştür. Silinmiş dosyalarda aynı şekilde uygulama üzerinden paylaşılıp silinmiş olsalar da belli bir süre daha mesaj geçmişinden elde edilen web adresi aracılığıyla dosyaya erişilebilmektedir. Bu durum adli bilişim uzmanları tarafından değerlendirilmesi gereken bir husus olarak görülmektedir.

Bundan sonra yapılabilecek çalışmalarda mobil cihazlarda tespit edilebilen verilerle bilgisayarlarda kurulu uygulama veya bilgisayardan internet tarayıcısı ile uygulama hesabına girilerek yapılacak mesajlaşmalarda elde edilebilecek veriler karşılaştırılabilir.

Received Date/Geliş Tarihi: 18.05.2021
Accepted Date/Kabul Tarihi: 07.07.2021

Kaynaklar

1. Choi Y. (2017) Mobile Instant Messaging Evidence in Criminal Trials. Cathol Univ J Law Technol.;26(1):3.
2. Ifdil I, Fadli RP, Suranata K, Zola N, Ardi Z. (2020) Online mental health services in Indonesia during the COVID-19 outbreak. Vol. 51, Asian Journal of Psychiatry.
3. Jakhar D, Kaul S, Kaur I. (2020) WhatsApp messenger as a teledermatology tool during coronavirus disease (COVID-19): from bedside to phone-side. Clin Exp Dermatol. 45(6):739–40.
4. Oliveira Dias DM de, Albergarias Lopes DR de O, Teles AC. (2020) Will Virtual Replace Classroom Teaching? Lessons from Virtual Classes via Zoom in the Times of COVID-19. J Adv Educ Philos. 04(05):208–13.
5. Vladoiu M, Constantinescu Z. (2020) Learning during COVID-19 pandemic:

Online education community, based on discord. Proc - RoEduNet IEEE Int Conf. 2020-Decem:19–24.

6. Steiner R. An instant chat app promising criminals 'worry free secure communication' was hacked by police — here's how 746 gangsters were arrested.; Availablefrom:https://www.marketwatch.com/story/an-instant-chat-app-promising-criminals-worry-free-secure-communication-was-hacked-by-uk-police-heres-how-746-gangsters-were-arrested-2020-07-02. 21 Nisan 2021
7. Orebaugh A, Allnutt J. (2009) Classification of Instant Messaging Communications for Forensics Analysis. Int J Forensic Comput Sci. 22–8.
8. Akbal E, Doğan S, Baloğlu I. (2018) Android İşletim Sisteminde Whatsapp Uygulamasının Adli Bilişim Açısından İncelenmesi. Bilişim Teknol Derg. 11(2):147–56.
9. Chang MS, Chang CY. (2018) Forensic analysis of LINE messenger on android. J Comput. 29(1):11–20.
10. Billups K. New and Emerging Mobile Apps Among Teens - Are Forensic Tools Keeping Up? Available from:https://hammer.purdue.edu/articles/thesis/New_and_Emerging_Mobile_Apps_Among_Teens_-_Are_Forensic_Tools_Keeping_Up_/12249845/1; 25 Nisan 2021
11. Moffitt K, Karabiyik U, Hutchinson S, Yoon YH. (2021) Discord Forensics: The Logs Keep Growing. 2021 IEEE 11th Annu Comput Commun Work Conf CCWC 2021. 993–9.
12. Motylinski M, MacDermott A, Iqbal F, Hussain M, Aleem S. (2020) Digital Forensic Acquisition and Analysis of Discord Applications. Proc 2020 IEEE Int Conf Commun Comput Cybersecurity, Informatics, CCCI 2020.
13. Shin S, Park E, Kim S, Kim J. (2020) Artifacts Analysis of Slack and Discord Messenger in Digital Forensic. J Digit Contents Soc. 21(4):799–809.
14. Ayers R, Jansen W, Ayers R. (2014) Guidelines on Mobile Device Forensics. NIST Spec Publ. 1(1).