International Journal of Innovative Engineering Applications

Journal homepage: https://dergipark.org.tr/ijiea

FORENSIC ANALYSIS OF CRIMES COMMITTED ON LIVE BROADCAST PLATFORMS ACCESSED VIA WEB BROWSERS

***Nursena Atalay*[1], *Aytuğ Boyacı*[*2]**

[1]*Department of Digital Forensics Engineering, Fırat University, Elazig, Turkey*
[2]*Department of Computer Engineering, Air Force Academy, National Defense University, Istanbul, Turkey*

Abstract

Original scientific paper

Live broadcast platforms are expressed as platforms that allow watching the online broadcast stream, which can be recorded simultaneously and broadcast in real time. Platforms are usually realized by the broadcaster speaking in real time and the audience participating in the chat section of the platform. The use of live broadcast platforms takes place through web browsers and mobile environments. According to the Criminal Procedure Law, which we encounter in the digital environment or in daily life, there are many types of crimes whose provisions are quite severe. The crimes committed and the rates of punishment vary according to the type and size of the crime. Many crimes can be committed in real time via live broadcast platforms that can be accessed via internet browsers and mobile media. Based on the detection of crime in live broadcast streams over internet browsers, in this study, forensic examination of broadcasts made from Periscope, YouTube, Facebook and Twitch live broadcast platforms over Google Chrome, Mozilla Firefox and Microsoft Edge internet browsers, and the findings for the detection of crime were revealed.

Keywords: *Digital forensics, digital evidence, live broadcast platforms, social media.*

WEB TARAYICILAR ARACILIĞI İLE ERİŞİM SAĞLANAN CANLI YAYIN PLATFORMLARINDA İŞLENEN SUÇLARIN ADLİ ANALİZİ

Özet

Orijinal bilimsel makale

Canlı yayın platformları, eş zamanlı olarak hem kayıt altına alınabilen hem de gerçek zamanlı olarak yayınlanan çevrimiçi yayın akışının izlenmesine olanak sağlayan platformlar olarak ifade edilmektedir. Platformlar genellikle yayını yapan kişinin gerçek zamanlı olarak konuşması ve platformun sohbet bölümüne izleyicilerin katılması ile gerçekleşmektedir. Canlı yayın platformlarının kullanımı, web tarayıcılar ve mobil ortamlar üzerinden gerçekleşmektedir. Dijital ortamda ya da günlük hayatta karşımıza çıkan Ceza Muhakemesi Hukukuna göre hükmü oldukça ağır olan birçok suç türleri bulunmaktadır. İşlenen suçlar ve cezalandırma oranları suçun türü ve boyutuna göre farklılık göstermektedir. İnternet tarayıcıları ve mobil ortamlar aracılığı ile erişilebilen canlı yayın platformları üzerinden de gerçek zamanlı olarak birçok suç işlenebilmektedir. İnternet tarayıcıları üzerinden canlı yayın akışlarında suçun tespitine dayalı olarak bu çalışmada, Google Chrome, Mozilla Firefox ve Microsoft Edge internet tarayıcıları üzerinden Periscope, YouTube, Facebook ve Twitch canlı yayın platformlarından gerçekleştirilen yayınların adli incelemesi gerçekleştirilerek suçun tespitine yönelik olarak elde edilen bulgular ortaya konmuştur.

Anahtar Kelimeler: *Adli bilişim, canlı yayın platformları, elektronik delil, sosyal medya.*

1 Giriş

Kişisel canlı yayın teknolojileri, günlük hayatta birçok kişinin ilgi alanına göre çeşitli kategorilere sahip olan ve bu kategorilerde yayıncı olarak, canlı yayın açma ve izleyici olarak, canlı yayın akışına katılabilme imkânı sağlayan uygulamalardır. Canlı yayın platformları hem kişisel alanda hem de kamusal alanda iletişim kurma potansiyelini yüksek oranda arttırmaktadır. Bu uygulamalar dünya genelinde teknolojinin ve sosyal ağların gelişimi ile doğru orantılı bir şekilde yaygınlaşmıştır [1]. Kullanıcı oturumu açarak canlı yayın açma ya da canlı yayın akışına izleyici olarak katılabilme yeteneğine sahip olan bu uygulamalar arasında Periscope, Twitch, Facebook ve Youtube gibi yaygın kullanılan uygulamalar yer almaktadır. Yaygın olarak kullanılan platformlara kullanıcılar, kullanıcı oturumu açarak ya da kullanıcı oturumu açmaksızın erişim sağlayabilmektedir.

* Corresponding author.
E-mail address: aytugboyaci@hho.msu.edu.tr (A. Boyaci)
Received 20 May 2022; Received in revised form 24 November 2022; Accepted 02 December 2022

Doi: https://doi.org/10.46460/ijiea.1117692

Canlı yayın akış platformlarının kullanımı suça konu olabilecek hususları da beraberinde getirmektedir. Platformların yaygınlaşması ile birlikte gerçekleşen çocuk istismarı, telif hakkı ihlali, taciz vb. gibi suç unsurlarında ciddi artış gözlemlenmektedir [2]. Ceza muhakemesi kuralları gereğince işlenen suçların türüne ve şiddetine göre ceza hükümleri değişmektedir. Bazı ceza muhakemelerince canlı yayın platformları üzerinde işlenen suçların cezalandırılma hükmüne yönelik olarak kanun ve yasalar üzerinde değişikliğe gidilmiş ve ağır maddeler ile yeniden yapılandırılmıştır [3]. Canlı yayın platformlarına, mobil cihazlar üzerinden erişim sağlanabildiği gibi internet tarayıcıları üzerinden de erişim sağlanabilmektedir. İnternet tarayıcısı üzerinden yapılan canlı yayınlar ile ilgili suç unsuru analizi yayın yapılan mobil cihaz ya da bilgisayar üzerinde ki önbellek incelemeleri ile gerçekleştirilmektedir. Kullanıcının internet aktiviteleri bilgisayar ya da mobil cihazın geçici belleğinde ve kullanılan web tarayıcının geçici depolama alanlarında tutulmaktadır. İlgili alanların analizi ile canlı yayın platformlarında yapılmış olan aktivitelere tespit edilebilmektedir [4].

Bu çalışmada, internet tarayıcıları üzerinden canlı yayın akışlarında suçun tespitine yönelik olarak Google Chrome, Mozilla Firefox ve Microsoft Edge internet tarayıcıları aracılığı ile erişim sağlanan Periscope, YouTube, Facebook ve Twitch canlı yayın platformunun adli inceleme ve analizi "gerçekleştirilerek delil niteliği taşıyan veriler sunulmuştur.

1.1 Motivasyon

Canlı yayın platformları, teknolojinin ve sosyal medyanın gelişimine bağlı olarak mobil ortam ve internet tarayıcıları aracılığı ile yaygın olarak kullanılmaktadır. Canlı yayın platformlarının kullanımının artması ile birlikte yapılan canlı yayınların suç unsuru barındırıp barındırmadığı ile ilgili çalışmalar da yoğunlaşmıştır [5]. Platformlar üzerinden yapılan canlı yayınların mobil uygulama ya da web istemcisi üzerinde takip edilmesi için kullanılan yayın mekanizmaları çoğu zaman istemcinin ve kullanılan cihazın geçici bellek alanında işlenmektedir. İnternet tarayıcıları aracılığı ile erişim sağlanan sosyal medya uygulamalarına yönelik olarak yapılan analizler genel olarak ön bellek incelemesi ve internet artifekt incelemesi ile gerçekleşmektedir. Canlı yayın uygulaması adli inceleme ve araştırma kapsamında incelenen internet tarayıcıları üzerinden yapılan inceleme ve araştırmalarda tarayıcı internet artifektleri ve ön bellek incelemeleri ile suçların aydınlatılma yoluna gidilmektedir. Ön bellek ve internet artifektleri incelemesi ile resim, video vb. medya verileri, kullanıcı geçmişi, canlı yayın içeriği, yorumlar ve durum simgeleri gibi veriler elde edilebilmektedir. Suçun aydınlatılmasında delil niteliği taşıyan bu kalıntıların elde edilmesi kullanılan canlı yayın platformuna ve erişim sağlanan tarayıcı türüne göre değişiklik göstermektedir. Bu yüzden suça konu olan durumun istemciler üzerindeki analizinde elde edilecek olan kanıt niteliği taşıyabilecek en küçük bilgi bile son derece önem kazanmaktadır [6].

1.2 Araştırma Kapsamı

Çalışmada yaygın kullanılan Periscope, Twitch, Facebook ve Youtube platformlarından gerçekleştirilen canlı yayınların kullanıcı web tarayıcılarının ön bellek alanları ve internet artikfekt izleri üzerinde adli analiz yapılmıştır. Gerçekleştirilen canlı yayınların izleri sık kullanılan Google Chrome, Mozilla Firefox ve Microsoft Edge tarayıcıları için analiz edilerek elde edilen bulgular ortaya konmuştur.

Yapılan analiz sonucu canlı yayının suç unsuru barındıran yayının ilgili cihaz ile gerçekleştirip gerçekleştirilmediğinin tespitine yönelik bulgular elde edilmeye çalışılmıştır. Adli için açık kaynaklı Autopsy yazılımı ve Magnet Forensic adli inceleme yazılımı kullanılmıştır.

1.3 İlgili Çalışmalar

Teknolojinin gelişimine bağlı olarak çeşitli sosyal medya vb. uygulamalar mobil ya da bilgisayar erişimi ile yaygın olarak kullanılmaktadır. Yaygın olarak kullanılan bu uygulamalardan biri de canlı yayın uygulamalarıdır. Canlı yayın uygulamaları, günden güne kullanımı artan, izleyici olarak katılım sağlanabilen ya da canlı yayın açabilmeye imkân sağlayan uygulamalardır. Sosyal medya türünde ki uygulamaların kullanım sayısının artışına bağlı olarak, sosyal medya üzerinden işlenen suçlarında sayısının oranında artış olduğu görülmektedir [7]. Canlı yayın platformlarının adli incelemesine yönelik olarak gerçekleştirilen literatür taramasında problemin güncelliği ve canlı yayın uygulamaları üzerinde adli inceleme alanında yapılan çalışmaların yetersiz olduğu görülmektedir. Çalışma ile ilgili literatür aşağıda verilmiştir.

Graeme Horsman tarafından yapılan çalışmada çalışmada, canlı yayın platformlarında çocuk istismarı soruşturması ve incelemesi üzerine teknik ve yasal alanda olan zorlukların incelemesini gerçekleştirmiştir ve çalışmada örnek olay incelemesi olarak Periscope uygulaması kullanılmıştır [8]. Patrick Verleg çalışmasında bir tarayıcının önbelleğini kullanıcının kişisel bilgisini saklamak için kullanılıp kullanılamayacağını belirlemek amacıyla tarayıcı ön bellek incelemesi yapmıştır [9]. Philip Ndubueze, yüksek teknoloji suçlarının değişen dinamiklerini ve bu gelişmenin geleneksel polislik politika ve uygulamalarına nasıl meydan okuduğunu analizini yapmış olduğu çalışmada ortaya koymuştur [10]. Kunwadee Sripanidkulchai ve arkadaşları tarafından yapılan çalışmada ise geniş kapsamlı bir içerik dağıtım ağından canlı akış verileri incelenmiştir. İncelenen verilerin bugüne kadar internet'teki çalışılmış olan en kapsamlı canlı yayın verileri olduğunu iddia etmektedirler [11]. Zhicong Lu ve arkadaşları tarafından sunulan çalışmada, bazı canlı yayın platformlarının kullanımının araştırılması ve çalışma kapsamında çeşitli ropörtaj verilerine ulaşılması amaçlanmıştır. Yapılan çalışmalar sonucunda elde edilen veriler, yayınlanan farklı içerik kategorilerini ve bu içeriğin farklı boyutlarının izleyicileri nasıl etkilediğini ortaya koymuştur [12].

1.4 Makale Organizasyonu

Canlı yayın platformlarının adli inceleme ve analizi üzerine gerçekleştirilen çalışma 4 alt bölümden oluşmaktadır. Birinci bölüm, canlı yayın platformları hakkında genel bilgi ve araştırma kapsamında gerçekleşen motivasyon ve uygulamalardan bahsetmektedir. İkinci bölüm adli incelemesi yapılan dört adet canlı yayın platformu uygulamasının ve ön bellek incelemesinin nasıl yapıldığına yönelik olarak inceleme yöntem ve metodolojisinden bahsetmektedir. Üçüncü bölüm, canlı yayın uygulamalarına erişim sağlanan üç farklı internet tarayıcısı test ve bulgular sonuçları ile birlikte internet tarayıcıları arasında adli inceleme sonuçlarına yönelik olan karşılaştırma tablosunu içermektedir. Dördüncü bölümde, farklı internet tarayıcıları ile erişim sağlanan farklı canlı yayın platformlarının adli inceleme ve araştırma sonucu elde edilen sonuçlar açıklanmıştır.

2 Yöntem ve Metodoloji

Çalışmada Periscope, YouTube, Facebook ve Twitch canlı yayın platformlarının adli analizinin yapılabilmesi için öncelikle her bir platform için sanal bilgisayar kullanılmıştır. Her sanal bilgisayar için 4GB bellek alanı ve 2GB depolama alanı oluşturulmuştur. Her sanal bilgisayar üzerinde Google Chrome, Mozilla Firefox ve Microsoft Edge internet tarayıcıları yapılandırmaları gerçekleştirilmiş ve canlı yayın platformlarda kullanıcı oturumları açılarak canlı yayın yapılması sağlanmıştır. Çalışmada canlı yayın platformların kullanımı canlı yayın sahibi ve canlı yayın izleyicisi olarak iki farklı şekilde gerçekleştirilmiştir. Farklı internet tarayıcıları aracılığı ile kullanılan farklı canlı yayın platformlarının üzerinde gerçekleştirilen eylemler sonrasında sanal olarak oluşturulan bilgisayarların FTK Imager adli kopya alma programı aracılığı ile imajları alınmıştır. Her bir sanal bilgisayar Magnet ve Autopsy adli inceleme programları ile analiz edilmiştir. Adli inceleme sonucu, incelemesi yapılan imaj dosyalarında internet tarayıcıları üzerindeki bulgular, bilgisayar erişim verileri analiz edilmiş, tarayıcılar üzerinden erişilebilen bulgular ve canlı yayın platformları üzerinden erişilebilen bulgular ışığında internet tarayıcılarından ve platformlardan elde edilebilen bulgular kategorik olarak karşılaştırılarak çalışmanın test ve bulgular kısmında paylaşılmıştır.

2.1 Periscope

Periscope, kullanıcıların video içeriği yayınlayıp ya da hali hazırda yayında olan video akışlarına izleyici olarak katılabilecekleri bir canlı yayın hizmeti sunan canlı yayın uygulamasıdır. Platforma mobil ortamlar aracılığı ile erişim sağlanabildiği gibi internet tarayıcıları aracılığıyla da erişim sağlanabilmektedir. Periscope uygulaması üzerinde gerçekleşen canlı yayın akışlarına kullanıcı girişi yapmaksızın pasif olarak erişim sağlanabilmektedir. Canlı yayın açmak için aktif olarak kullanıcı oturumu açılması gerekmektedir [13].

2.2 Youtube

Youtube, kullanıcıların çeşitli video içerikleri izleyebileceği ve kullanıcı oturumu açtıktan sonra kişisel kanal adı verilen ortam üzerinden kendi içeriklerini paylaşabilmesine olanak sağlayan sosyal medya platformudur. Youtube platformu üzerinden paylaşılan içeriklere erişebilmenin yanında kullanıcı oturumu açılmadan canlı yayınlara erişilebilmektedir. Kullanıcı oturumu açıldığı taktirde erişilen canlı yayın akışlarına yorumlar ile aktif katılım sağlanabilmektedir. Kullanıcı oturumu açan her Youtube kullanıcısı platform üzerinden canlı yayın başlatabilmektedir [14].

2.3 Facebook

Facebook, kişiler arası aktif olarak iletişim sağlamak amacıyla kullanılan durum güncellemesi, video resim vb. medya paylaşımı yapmak, paylaşımlara yorum yapabilmek ve kullanıcılar arasında anlık sohbet imkânı sağlayan sosyal medya platformudur. Facebook platformu da kullanıcılarına canlı yayın içerikleri paylaşabilme imkânı sunmaktadır. Kullanıcı oturumu açan her kullanıcı platform üzerinde canlı yayın başlatabilmektedir. Canlı yayın içeriğini takip eden kullanıcıların oturum açma zorunluluğu bulunmamaktadır [15]. Facebook platformu da diğer canlı yayın platformlarında olduğu gibi kullanıcılar ile canlı yayın arasında interaktiviteye olanak sağlamakta, canlı yayın akışı sırasında yorum ve simge ifadeleri ile kullanıcıların canlı yayına katkı sunması mümkün olabilmektedir [16].

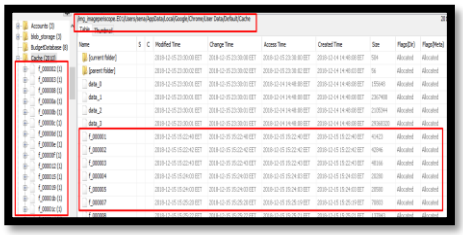
2.4 Twitch

Twitch platformu kullanıcıların aktif olarak giriş yaparak video içeriği yayınlayabildiği, aktif ya da pasif olarak yayında olan video akışlarına izleyici olarak katılım saplayabildiği canlı yayın platform uygulamasıdır. Platform erişimi IOS ve Android tabanlı mobil uygulamalar ile yapılabildiği gibi bilgisayar aygıtlarında standart bir web tarayıcısı aracılığıyla sağlanabilmektedir [17]. Twitch platformu da diğer canlı yayın platformları ile benzer şekilde yorum bölümü kısmında aktif olarak yorum yapabilme ve durum simgesi bırakabilme imkânı sağlamaktadır [18].

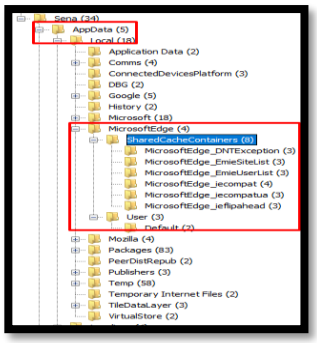
2.5 İnternet Tarayıcı Ön Belleği

İnternet tarayıcı ön belleği internet sitelerinin daha hızlı yüklenmesi amacıyla oluşturulmuş olan geçici depolama yapılan alan olarak tanımlanmaktadır [19]. Tarayıcı ön belleği, uygulama sunucusundan talep edilen içerik ile ilgili dosyaların bilgisayar hafızasına kaydederek, tekrar internet sunucusuna bağlanıp oradan indirmek yerine yerel hafızadan dosyaların çağrılmasına olanak tanımaktadır [20]. Ön bellek alanında uygulamaya ait yazı stillerini barındıran CSS dosyası, uygulamaya ait metin dili dosyası (Html), çeşitli güvenlik kontrolleri için ve hareketli menüler oluşturabilmek için kullanılan ve istemci tarafında çalışan script (js) dosyaları, uygulam içinde barındırılan resim ve müzik (Jpeg, Png, Mp4 vb.) gibi medya dosyaları, indirilebilir dosya içerikleri (Docx, Pdf, Zip vb.) tutulmaktadır. İnternet tarayıcılarının adli

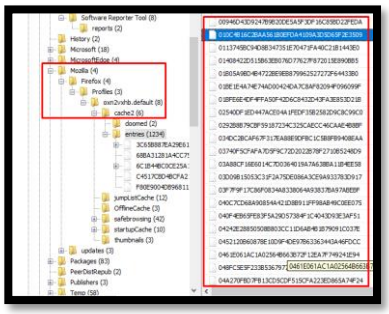
incelemeleri yapılırken genel olarak internet kalıntıları ve ön bellek analizi önemli bulgulara erişilebilmeye olanak sağlamaktadır [21]. İncelemesi yapılan tarayıcı ön bellekleri ile daha önce tarayıcı üzerinde gerçekleşmiş video izleme, resim, durum simgeleri, yorum sohbetleri vb. etkinliklere erişim sağlanabilmektedir. Internet tarayıcıları ön bellek dosyalarını farklı şekillerde isimlendirerek farklı dosya konumlarında saklamaktadırlar [22]. Tarayıcıların kullanımı ile aktif olarak kaydedilen ön bellek dosyaları kaydedilen dosyanın resim, video vb. türüne göre farklı mantıklar ile isimlendirilerek ve sıralanarak kaydedilmektedir. Google Chrome tarayıcısı ön bellek dosya dizimi Şekil 1, Microsoft Edge tarayıcısı ön bellek dosya dizimi Şekil 2, Mozilla Firefox tarayıcısı ön bellek dosya dizimi Şekil 3 ile gösterilmektedir.



Şekil 1. Google Chrome tarayıcı ön bellek dosya dizimi.



Şekil 2. Microsoft Edge tarayıcı ön bellek dosya dizimi.



Şekil 3. Mozilla Firefox tarayıcı ön bellek dosya dizimi.

3 Test ve Bulgular

Bu çalışmada, Periscope, Twitch, Youtube ve Facebook canlı yayın platformlarının Google Chrome, Mozilla Firefox ve Microsoft Edge internet tarayıcıları üzerindeki bulguları analiz edilmiştir. Oluşturulan sanal makineler üzerinde canlı yayın platformlarına internet tarayıcıları üzerinden giriş yapılmış, kullanıcı olarak canlı yayın izleme, yayın için yorum yapma gibi platformun özellikleri kullanılmıştır. Yine canlı yayın platformlarında canlı yayın yaparak yapılan canlı yayına ait internet tarayıcılarındaki bulguların analiz edilmesi hedeflenmiştir. Oluşturulan sanal makinelere ait imaj dosyaları Ftk imager adli kopya alma programı ile alınmıştır. İmajlar üzerinde bulgulara erişebilmek için Magnet ve Autopsy adli inceleme yazılımları kullanılmıştır. Farklı tarayıcılar üzerinden kullanımı gerçekleşen canlı yayın uygulamalarının incelemeleri, tarayıcı ön bellek ve internet kalıntılarının incelemesi ile gerçekleşmiştir. İncelemesi yapılan adli kopyalardan, delil niteliği taşıyacak ses, video, resim vb. medya verileri, canlı yayın esnasında gerçekleşen durum yorum ve durum simge bilgileri gibi bilgilere erişilmiştir. Adli incelemesi gerçekleşen farklı canlı yayın platformları ve farklı tarayıcıların inceleme sonuçları karşılaştırmaları bir şekilde sunulmuştur.

3.1 Google Chrome İnternet Tarayıcısına Ön Bellek Analizinden Elde Edilen Bulgular

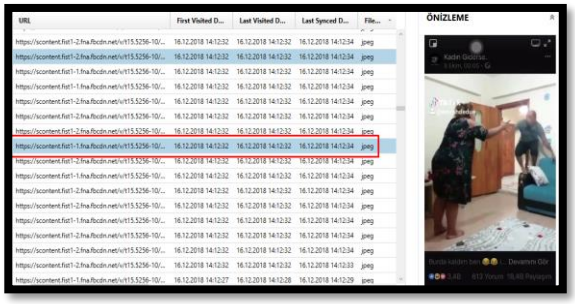
Canlı yayın platformları için gerçekleştirilen analiz için oluşturulan sanal makinede Windows 10 işletim sistemi kullanılmıştır. Google Chrome internet tarayıcısı üzerinden Facebook, Twitch, Youtube ve Periscope platformlarına öncelikli olarak kullanıcı oturumu açmadan erişim sağlanmış ve platformlar üzerindenden canlı yayın erişimleri sağlanmıştır. Yine aynı platformlarda kullanıcı oturumu açılarak canlı yayınlara erişim sağlanmış, canlı yayınlara platform üzerinden yorum, beğeni gibi aktiviteler gerçekleştirilmiştir. Platform üzerinden üçüncü aşamada ise bir canlı yayın başlatılmış, canlı yayına kullanıcıların erişimi sağlanmıştır. Üç uygulama içinde ayrı ayrı imajlar alınarak üç farklı durum için Google Chrome internet tarayıcısı üzerindeki bulguların analizi yapılmıştır. Adli analiz sonucunda, izlenilmiş olan canlı yayınların, kısa videolar şeklinde canlı yayın içerik bilgisi, erişim tarih ve saat bilgilisi, canlı yayın başlık bilgisi, yayın sırasında gerçekleşen yorum ve simge bilgileri, canlı yayın izlenme sayısı, canlı yayına erişim sağlayan kullanıcı bilgisi, link adres bilgisi gibi canlı yayın uygulamasında gerçekleşen etkinlikler ile ilgili bulgulara erişilebilmiştir. Google Chrome tarayıcısı üzerinden elde edilen delil niteliği taşıyan bulgular Şekil 4, Şekil 5, Şekil 6 ve Şekil 7'de gösterilmiştir. Şekil 4'te Youtube canlı yayın platformunun Google Chrome internet tarayıcısından erişimi sonucu elde edilen bulgular gösterilmektedir. Şekilde de görüldüğü gibi canlı yayına erişim zamanı kullanıcı bilgileri, canlı yayın erişim linki gibi kanıt niteliği taşıyabilecek bulgulara erişilebildiği görülmüştür.

Name	Date Created...	Value	Count	Kaynak
email	21.12.2018 16:00:23	deniz_demir_2327@gmail.com	1	youtube_image
email	21.12.2018 16:00:44	deniz.demir.2327@gmail.com	1	youtube_image
46432_92990pi_46432_92990	21.12.2018 17:32:42	deiz	1	youtube_image
46432_92998pi_46432_92998	21.12.2018 17:32:42	+00000000004552500	1	youtube_image
46432_92994pi_46432_92994	21.12.2018 17:32:42	Student	1	youtube_image
46432_93000pi_46432_93000	21.12.2018 17:32:42	Firat University	1	youtube_image
46432_92992pi_46432_92992	21.12.2018 17:32:42	demir	1	youtube_image
46432_92996pi_46432_92996	21.12.2018 17:32:42	deniz.demir.2327@gmail.com	1	youtube_image

Şekil 4. Youtube canlı yayın platformu kullanıcı hesap bilgileri.

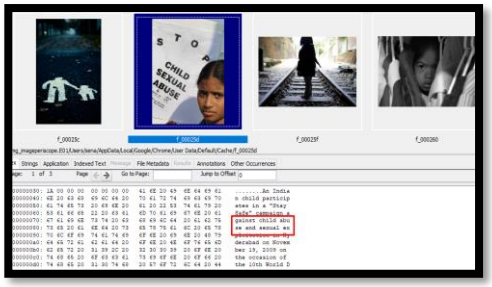
Şekil 5'de Facebook canlı yayın platformuna Google Chrome internet tarayıcısı üzerinden erişim ile ilgili bulgular gösterilmektedir. İmaj dosyası üzerinde

gerçekleştirilen adli analiz sonucunda canlı yayına ait erişim linki, ilk ve son erişim zaman damgaları, dosya türü gibi bulgulara ulaşılabildiği görülmüştür.



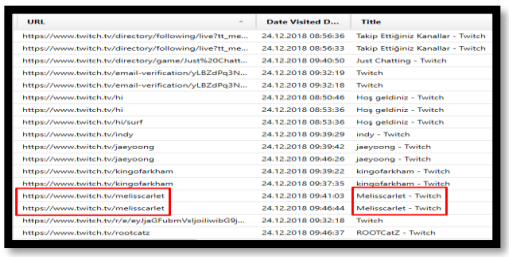
Şekil 5. Facebook canlı yayın içeriğine dair bulgular.

Şekil 6'da Periscope canlı yayın platformunun Google Chrome internet tarayıcısı üzerinde bıraktığı bulgular gösterilmektedir. Gerçekleştirilen Google Chrome ön bellek dosyalarının hex editör üzerinden yapılan incelemesinde yapılan yayınlar ile ilgili başlık ve resim türündeki medya verilerine erişilmiştir. Ayrıca hex editör üzerinde yayın ile ilgili kategori verileri ve yorumlara yönelik kanıt niteliği taşıyabilecek bulgulara erişilebildiği görülmüştür.



Şekil 6. Hex editörde Periscope canlı yayın uygulaması başlık ve resim türündeki ön bellek bulguları.

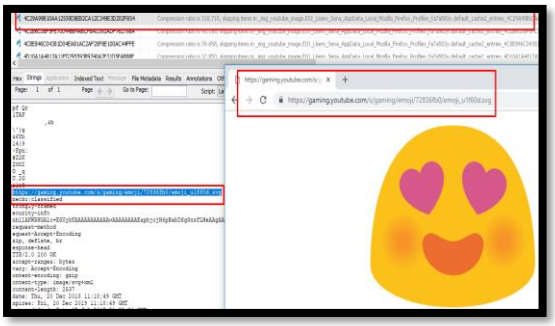
Şekil 7'de Twitch canlı yayın platformunun Google Chrome internet tarayıcısı ön belleğinde bıraktığı izler görülmektedir. İnceleme sonuçlarından canlı yayın başlık ve erişim linki, erişim zaman damgası, kategori verilerine ait kanıt niteliği taşıyabilecek bulguların elde edilebildiği görülmüştür.



Şekil 7. Twitch canlı yayın uygulaması erişilen başlık ve link adresi bulguları.

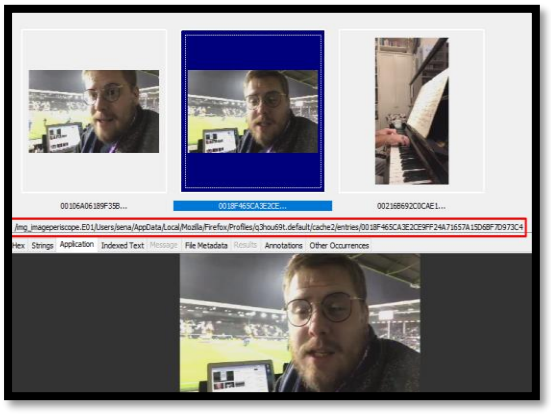
3.2 Mozilla Firefox İnternet Tarayıcısına Ön Bellek Analizinden Elde Edilen Bulgular

Canlı yayın platformlarına ait adli analizin yapılabilmesi için Google Chrome analizinde olduğu gibi üç farklı senaryo ışığında eylemler gerçekleştirilerek her senaryoya ait imaj dosyaları alınmıştır. Bu kapsamda öncelikli olarak kullanıcı oturumu açmadan canlı yayınlar izlenmiş, ikinci olarak kullanıcı oturum açıldıktan sonra canlı yayınlar izlenmiş ve etkileşim sağlanmış, son olarak ise kullanıcı oturumu açıldıktan sonra canlı yayın yapılmış ve diğer kullanıcılar ile etkileşim sağlanmıştır. Alınan imaj dosyaları üzerinden Mozilla Firefox internet tarayıcısı ön bellek analizi yapılarak elde edilen bulgular ortaya konmuştur. Mozilla Firefox internet tarayışının ön bellek analizinde izlenilmiş ya da açılmış olan canlı yayınların, içeriğine yönelik olarak içerik bilgisi, erişim tarih ve saat bilgilisi, canlı yayın başlık bilgisi, yayın sırasında gerçekleşen yorum ve simge bilgileri, canlı yayın izlenme sayısı, canlı yayına erişim sağlayan kullanıcı bilgisi, link adres bilgisi gibi canlı yayın uygulamasında gerçekleşen etkinlikler ile ilgili bulgulara erişilebildiği görülmüştür. Tarayıcılar üzerinde yapılan adli incelemeler sonucunda, delil niteliği taşıyacak verilerin sayısının en çok Mozilla Firefox tarayıcısından elde edildiği görülmüştür. Tarayıcı ön bellek analizinden elde edilen delil niteliği taşıyabilecek Şekil 8, Şekil 9, Şekil 10 ve Şekil 11'de gösterilmiştir. Şekil 8'de Youtube canlı yayın platformunun Mozilla Firefox internet tarayıcısı ön bellek dosyalarının analizinden elde edilen bulgular gösterilmektedir. Tarayıcı ön bellek analizi ile erişim sağlanan canlı yayın linkleri, http paket içeriği, resim, video içerikleri, kullanıcı bilgilerine ait bulgulara erişilebildiği görülmektedir.



Şekil 8. Hex editörde Youtube canlı yayın uygulaması simge ve yorum türündeki ön bellek bulguları.

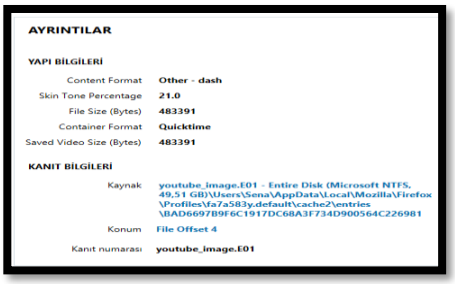
Şekil 9'de Periscope canlı yayın platformuna Mozilla Firefox internet tarayıcısı ile sağlanan erişimlere ait bulgular görülmektedir. Tarayıcı ön bellek analizi ile canlı yayın ID bilgisi, erişim linki, canlı yayına ait küçük resimlere (thumbnail) erişilebildiği görülmektedir.



Şekil 9. Periscope canlı yayın içeriğine dair bulgular.

Şekil 10 ve Şekil 11'de Youtube canlı yayın platformuna Mozilla Firefox internet tarayıcısı ile erişim sonucu ön bellek dosyalarından elde edilen bulgular gösterilmektedir. Tarayıcı ön bellek analizinde canlı yayın videoları ve video kareleri, dosya bilgileri, erişim link bilgisi, dosya format ve boyut bilgisi gibi kanıt niteliği olabilecek bulgulara erişilebildiği görülmüştür.

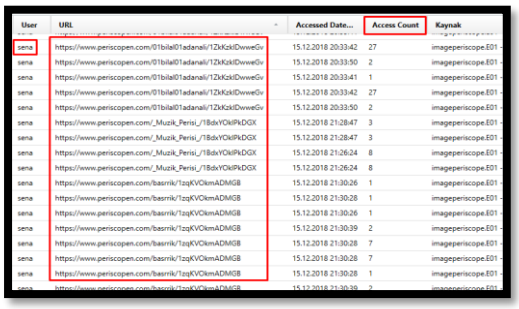
Şekil 10. Youtube canlı yayın içeriğine dair bulgular.



Şekil 11. Youtube canlı yayın içeriğine dair bulguların dosya konumu.

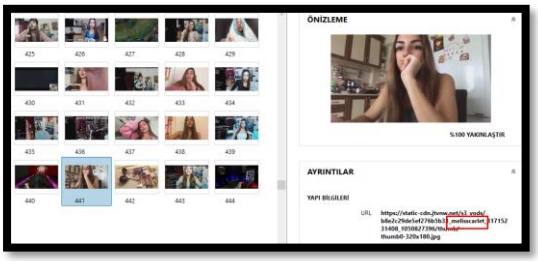
3.3 Microsoft Edge İnternet Tarayıcısına Ön Bellek Analizinden Elde Edilen Bulgular

Periscope, YouTube, Facebook ve Twitch canlı yayın platformlarına yönelik olarak Microsoft Edge internet tarayıcısında da benzer şekilde üç senaryo ışığında eylemler gerçekleştirilerek sanal makinelerin imajları alınmıştır. Bu kapsamda öncelikle internet tarayıcılarından kullanıcı oturumu açmadan canlı yayınlara katılım sağlanmıştır. İkinci aşamada kullanıcı oturumu açarak canlı yayınlara katılım ve etkileşim sağlanmıştır. Üçüncü aşamada ise kullanıcı olarak canlı yayın açılmış ve canlı yayına diğer kullanıcıların katılımı sağlanmıştır. Gerçekleştirilen işlemler sonucunda makinelerin imajları alınarak adli analiz için Autopsy ve Magnet Forensic yazılımları ile veri kazıma yapılmış elde edilen bulgular ortaya konmuştur. Yapılan inceleme sonucunda Microsoft Edge internet tarayıcısından Youtube ve Facebook canlı yayın platformlarından kanıt niteliği taşıyabilecek bulguların elde edilemediği görülmüştür. Periscope ve Twitch ile yapılan işlemlerin Microsoft Edge internet tarayıcısı ön belleğinde bıraktığı izler incelendiğinde ise canlı yayınlara ait tarih ve saat bilgileri, kısmen canlı yayın başlık bilgisi, erişim sağlayan kullanıcı bilgileri, katılım sağlanan link ve tarayıcı geçmiş bilgilerine erişim sağlanabildiği görülmüştür. Şekil 12'de Periscope canlı yayın platformunun Microsoft Edge tarayıcısının ön bellek dosyalarının inceleme sonuçlarından elde edilen kullanıcı hesap bilgisi, erişim link bilgisi, erişim zaman bilgisi, site erişim sayısı bilgisi gibi kanıt niteliği sayılabilecek bulguların geldiği gösterilmektedir.



Şekil 12. Periscope canlı yayın platform bulguları.

Şekil 13'de Twitch canlı yayın platformunun Microsoft Edge internet tarayıcısı ön bellek dosyalarının inceleme sonuçlarından elde edilen canlı yayın içeriğine dair bulgular gösterilmektedir. Microsoft Edge internet tarayıcısının ön bellek incelemesi ile Twitct üzerinden gerçekleştirilen canlı yayına ait küçük resimlere (thumbnail), canlı yayın erişim linkine, erişim linki üzerindeki kullanıcı bilgisine, yayın ID değerine ulaşılabildiği görülmüştür.



Şekil 13. Twitch canlı yayın bulguları.

Çalışma kapsamında Periscope, Twitch, Facebook ve Youtube platformlarından gerçekleştirilen canlı yayınların Google Chrome, Mozilla Firefox ve Microsoft Edge internet tarayıcıları üzerinden kullanımının ardından adli analizi gerçekleştirilerek delil niteliği taşıyabilecek bulgulara ulaşılmıştır. Adli analiz sonucu elde edilen bulgular Tablo 1, Tablo 2 ve Tablo 3'de verilmektedir.

Tablo 1. Google Chrome internet tarayıcısından elde edilen bulgular.

	Periscope	Facebook	Youtube	Twitch
Canlı Yayın İçerik / Video Erişimi	Yok	Yok	Var	Yok
Canlı Yayın Erişim Tarih-Saat Bilgisi	Var	Var	Var	Var
Canlı Yayın Başlık Bilgisi	Var	Var	Var	Var
Canlı Yayın Yorum Bilgisi	Yok	Yok	Var	Yok
Canlı Yayın Like -Unlike Bilgisi	Yok	Yok	Var	Yok
Canlı Yayın Emoji Bilgisi	Yok	Yok	Var	Yok
Canlı Yayın Takipçi – İzleme Sayısı	Yok	Yok	Yok	Yok
Canlı Yayın Erişim Kullanıcı Bilgisi	Var	Var	Var	Var
Tekrar Oynatma Bilgisi	Yok	Yok	Var	Yok
Canlı Yayın Link Adresi Bilgisi	Var	Var	Var	Var
Canlı Yayın / Video Kazıma	Yok	Yok	Var	Yok

Tablo 2. Mozilla Firefox internet tarayıcısından elde edilen bulgular.

	Periscope	Facebook	Youtube	Twitch
Canlı Yayın İçerik / Video Erişimi	Yok	Yok	Var	Var
Canlı Yayın Erişim Tarih-Saat Bilgisi	Var	Var	Var	Var
Canlı Yayın Başlık Bilgisi	Var	Var	Var	Var
Canlı Yayın Yorum Bilgisi	Yok	Var	Var	Yok
Canlı Yayın Like -Unlike Bilgisi	Yok	Yok	Yok	Yok
Canlı Yayın Emoji Bilgisi	Yok	Var	Var	Yok
Canlı Yayın Takipçi – İzleme Sayısı	Yok	Yok	Yok	Yok
Canlı Yayın Erişim Kullanıcı Bilgisi	Var	Var	Var	Yok
Tekrar Oynat	Yok	Yok	Var	Yok
Canlı Yayın Link Adresi Bilgisi	Var	Var	Var	Var
Canlı Yayın / Video Kazıma	Yok	Var	Var	Yok

Tablo 3. Microsoft Edge internet tarayıcısından elde edilen bulgular.

	Periscope	Facebook	Youtube	Twitch
Canlı Yayın İçerik / Video Erişimi	Yok	Yok	Var	Var
Canlı Yayın Erişim Tarih-Saat Bilgisi	Yok	Yok	Yok	Var
Canlı Yayın Başlık Bilgisi	Var	Var	Var	Var
Canlı Yayın Yorum Bilgisi	Yok	Yok	Yok	Yok
Canlı Yayın Like -Unlike Bilgisi	Yok	Yok	Yok	Yok
Canlı Yayın Emoji Bilgisi	Yok	Yok	Yok	Yok
Canlı Yayın Takipçi – İzleme Sayısı	Yok	Yok	Yok	Yok
Canlı Yayın Erişim Kullanıcı Bilgisi	Var	Yok	Yok	Var
Tekrar Oynat	Yok	Yok	Yok	Yok
Canlı Yayın Link Adresi Bilgisi	Var	Yok	Yok	Var
Canlı Yayın / Video Kazıma	Yok	Yok	Yok	Yok

4 Sonuç ve Değerlendirme

Adli bilişim incelemeleri kapsamında yapılan araştırmalar sonucunda delil niteliği taşıyan resim, video vb. medya verileri, kullanıcı bilgileri, erişim tarih ve saat bilgileri gibi bulgulara erişilebilmesi ve incelenmesi ile suça konu olabilecek durumun açıklığa kavuşturulması mümkün olabilmektedir. Teknolojinin gelişimine bağlı olarak sosyal medya platformları her geçen daha da yaygın olarak kullanılmaktadır. Yaygın kullanımının olumlu etkileri yansıdığı gibi çeşitli suçların oluşumu ve yaygınlaşması gibi olumsuz etkileri de yansımaktadır. Çalışmada sık kullanılan canlı yayın platformları üzerinden suça konu olabilecek bir yayın yapıldığında ya da o yayına katılım gösterildiğinde internet tarayıcıları ön bellek alanlarında bıraktığı izler analiz edilmiştir. Çalışma kapsamında Periscope, YouTube, Facebook ve Twitch canlı yayın platformlarında gerçekleştirilen aktivitelerin Google Chrome, Mozilla Firefox, Microsoft Edge internet tarayıcılarında bıraktığı izler analiz edilmiştir. İnternet tarayıcısı ön bellek bulgularında canlı yayın içeriğine erişim bilgileri, canlı yayına erişim zaman damgası bilgileri, canlı yayına ait verilen başlık bilgisi, canlı yayın için yapılan yorumlar, beğeni bilgileri, emoji bilgileri, canlı yayına ait izlenme bilgileri, canlı yayın yapan ya da katılımcılara ait kullanıcı bilgileri, yayının tekrar oynatılma bilgileri ve veri kazıma sonucu gelen veriler analiz edilmiştir. Yapılan çalışma ile canlı yayın platformlarından yapılan yayınlarda suça konu olabilecek durumlara karşın delil niteliği taşıyabilecek bulguların elde edilebildiği görülmüştür.

Bilgilendirme

Gerçekleştirilen çalışmada etik kurul onay belgesine gerek yoktur.

Kaynaklar

[1] Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital investigation*, 7, S64-S73.

[2] Al Fahdi, M., Clarke, N. L., & Furnell, S. M. (2013, August). Challenges to digital forensics: A survey of researchers & practitioners attitudes and opinions. In 2013 Information Security for South Africa (pp. 1-8). *IEEE*.

[3] Ayers, R., Brothers, S., & Jansen, W. (2013). Guidelines on mobile device forensics (draft). *NIST Special Publication*, 800, 101.

[4] Hoog, A. (2011). Android forensics: investigation, analysis and mobile security for Google Android. *Elsevier*.

[5] Horsman, G. (2018). A forensic examination of the technical and legal challenges surrounding the investigation of child abuse on live streaming platforms: A case study on Periscope. *Journal of information security and applications*, 42, 107-117.

[6] Horsman, G. (2018). Reconstructing streamed video content: A case study on YouTube and Facebook Live stream content in the Chrome web browser cache. *Digital Investigation*, 26, S30-S37.

[7] Oh, J., Lee, S., & Lee, S. (2011). Advanced evidence collection and analysis of web browser activity. *Digital Investigation*, 8, S62-S70.

[8] Horsman, G. (2018). A forensic examination of the technical and legal challenges surrounding the investigation of child abuse on live streaming platforms: A case study on Periscope. *Journal of Information Security and Applications* 42, 107–117.

[9] Verleg, P. (2014). *Cache Cookies: searching for hidden browser storage*. (Bachelor Dissertation, Radboud University).

[10] Ndubueze, P. (2017). High-Tech Crimes, Boundaryless policing and cyber security policy in digital Nigeria: A Periscope, *Federal University Dutse*, Nigeria.

[11] Sripanidkulchai, K., Maggs, B., & Zhang, H. (2004, October). An analysis of live streaming workloads on the internet. *In Proceedings of the 4th ACM SIGCOMM conference on Internet measurement (pp. 41-54).*

[12] Lu, Z., Xia, H., Heo, S., & Wigdor, D. (2018). You watch, you give, and you engage: a study of live streaming practices in China. In *Proceedings of the 2018 CHI conference on human factors in computing systems (pp. 1-13)*.

[13] El-Tayeb, M., Taha, A., & Fayed, Z. T. (2022). Live-Streamed Video Reconstruction for Web Browser Forensics. Retrieved June 22, 2021 from *http://iieta.org/journals/isi*, *27*(1), 61-66.

[14] Kandias, M., Stavrou, V., Bozovic, N., & Gritzalis, D. (2013, November). Proactive insider threat detection through social media: The YouTube case. *In Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society* (261-266).

[15] Chu, H. C., Deng, D. J., & Park, J. H. (2011). Live data mining concerning social networking forensics based on a facebook session through aggregation of social data. *IEEE Journal on Selected Areas in Communications*, *29*(7), 1368-1376.

[16] Umar, R., Yudhana, A., & Faiz, M. N. (2018). Experimental analysis of web browser sessions using live forensics method. *Int. J. Electr. Comput. Eng*, *8*(5), 2951-2958.

[17] El-Tayeb, M., Taha, A., & Fayed, Z. T. (2022). Live-Streamed Video Reconstruction for Web Browser Forensics. *Journal 27*(1), 61-66.

[18] Liao, Y. C. (2018). Investigating the Use of Online Open Source Information as Evidence in European Courts. In *Proceedings of the 13th International Conference on Availability, Reliability and Security* (pp. 1-6).

[19] Rathod, D. (2017). Web browser forensics: google chrome. *International Journal of Advanced Research in Computer Science*, *8*(7), 896-899.

[20] Umar, R., Yudhana, A., & Faiz, M. N. (2018). Experimental analysis of web browser sessions using live forensics method. *Int. J. Electr. Comput. Eng*, *8*(5), 2951-2958.

[21] Faiz, M. N., Umar, R., & Yudhana, A. (2016). Analisis Live Forensics Untuk Perbandingan Kemananan Email Pada Sistem Operasi Proprietary. *ILKOM Jurnal Ilmiah*, *8*(3), 242-247.

[22] Rasool, A., & Jalil, Z. (2020). A review of web browser forensic analysis tools and techniques. *Researchpedia Journal of Computing*, *1*(1), 15-21.