T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

UZAKTAN EĞİTİM ARAÇLARININ ADLİ BİLİŞİM AÇISINDAN İNCELENMESİ

Yunus Emre ÇOLAK

Yüksek Lisans Tezi

ADLİ BİLİŞİM MÜHENDİSLİĞİ ANABİLİM DALI

TEMMUZ 2022

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Adli Bilişim Mühendisliği Anabilim Dalı

Yüksek Lisans Tezi

UZAKTAN EĞİTİM ARAÇLARININ ADLİ BİLİŞİM AÇISINDAN İNCELENMESİ

Tez Yazarı
Yunus Emre ÇOLAK

Danışman
Doç. Dr. Şengül DOĞAN

TEMMUZ 2022
ELAZIĞ

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Adli Bilişim Mühendisliği Anabilim Dalı

Yüksek Lisans Tezi

Başlığı:	Uzaktan Eğitim Araçlarının Adli Bilişim Açısından İncelenmesi
Yazarı:	Yunus Emre ÇOLAK
İlk Teslim Tarihi:	01.05.2022
Savunma Tarihi:	04.07.2022

TEZ ONAYI

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına göre hazırlanan bu tez aşağıda imzaları bulunan jüri üyeleri tarafından değerlendirilmiş ve akademik dinleyicilere açık yapılan savunma sonucunda OYBİRLİĞİ ile kabul edilmiştir.

	İmza	
Danışman:	Doç. Dr. Şengül DOĞAN Fırat Üniversitesi, Teknoloji Fakültesi	Onayladım
Başkan:	Doç. Dr. Türker TUNCER Fırat Üniversitesi, Teknoloji Fakültesi	Onayladım
Üye:	Dr. Öğr. Üyesi Mehmet BAYĞIN Ardahan Üniversitesi, Mühendislik Fakültesi	Onayladım

Bu tez, Enstitü Yönetim Kurulunun ...../...../20..... tarihli toplantısında tescillenmiştir.

İmza

Prof. Dr. Kürşat Esat ALYAMAÇ
Enstitü Müdürü

BEYAN

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırladığım "Uzaktan Eğitim Araçlarının Adli Bilişim Açısından İncelenmesi" Başlıklı Yüksek Lisans Tezimin içindeki bütün bilgilerin doğru olduğunu, bilgilerin üretilmesi ve sunulmasında bilimsel etik kurallarına uygun davrandığımı, kullandığım bütün kaynakları atıf yaparak belirttiğimi, maddi ve manevi desteği olan tüm kurum/kuruluş ve kişileri belirttiğimi, burada sunduğum veri ve bilgileri unvan almak amacıyla daha önce hiçbir şekilde kullanmadığımı beyan ederim.

04.07.2022

Yunus Emre ÇOLAK

ÖNSÖZ

Günümüzde uzaktan eğitim araçlarının adli bilişim açısından incelenmesi çevrim içi ortamlarda meydana gelen olaylar neticesinde ihtiyaç ve zorunluluk hâline gelmiştir. İçinde bulunduğumuz zamanın gereklilikleri ve zorunlulukları doğrultusunda birçok eğitim ortamı fiziksel den çevrim içi alanlara taşınmıştır. Bu da inceleme gerektiren birçok olayın fiziksel ortamlardan çevrim içi alanlara taşındığını göstermektedir.

Fiziksel ortamlarda gerçekleşen eğitim sürecinde meydana gelen bir adli olayda, delillerin incelenmesi çoğu zaman maddi, fiziksel ve somut verilere dayanmaktadır. Bu da her ne kadar uzmanlık gerektiren bir inceleme aşaması olsa da elle tutulan, gözle görülen deliller adli inceleme çalışmasında kolaylık sağlamaktadır.

Çevrim içi olarak uzaktan eğitim modellerinin benimsendiği platformlarda meydana gelecek adli olaylar sonucunda, adli inceleme çalışmalarına ihtiyaç duyulması hâlinde bu adli inceleme çalışmalarının yukarıda bahsettiğimiz fiziksel ortamlardan daha zorlu bir inceleme süreci doğuracağı olasıdır. Bu zorluğun farkında olarak uzaktan eğitim araçlarının adli incelemeye konu olması durumunda gereksinim duyulan bilgilere nereden ve nasıl ulaşılabileceğine dair bir çalışmanın gereksinimden ziyade bir zorunlu ihtiyaç hâline geldiği değerlendirilmiş, araştırmamızda eğitim araçlarından bazılarının adli bilişim açısından incelenmesine çalışılmıştır.

Bu tez çalışmasının tamamlanmasında yardımlarını esirgemeyen danışmanım Sayın Doç. Dr. Şengül DOĞAN' a, Fırat Üniversitesi Adli Bilişim Mühendisliği Bölümü'nün kıymetli hocalarına, tez yazım sürecinde desteği olan tüm arkadaşlarıma, Nurcan İLHAN' a ve hayat yolunu beraber yürüdüğüm sevgili eşim Gül'e teşekkür ederim.

Yunus Emre ÇOLAK
ELAZIĞ, 2022

İÇİNDEKİLER

Sayfa

ÖZET

Uzaktan Eğitim Araçlarının Adli Bilişim Açısından İncelenmesi

Yunus Emre ÇOLAK

Yüksek Lisans Tezi

FIRAT ÜNİVERSİTESİ
Fen Bilimleri Enstitüsü

Adli Bilişim Mühendisliği Anabilim Dalı

Temmuz 2022, Sayfa: x + 31

Dijital alanda adli bilişim araştırması yapan kişilerin işleri bu alanın bakir olmasından dolayı bu alanda çalışma yapmak zor olabilmektedir. Gün geçtikçe teknolojinin sürekli gelişmesi, yeni platform ve programların yayınlanması her uygulamanın, programın kendine özgü inceleme metotlarının olması gerekliliği sonucunu doğurmaktadır. Bu durum dijital inceleme yapacak olan kişilerin kendini sürekli geliştirmesini ve bu alanda kendilerine yol gösterecek kaynaklara ihtiyaç duymasını gerekli kılar.

Uzaktan eğitim araçlarının adli bilişim açısından incelenmesi önemli bir konudur. Dijitalleşmenin giderek arttığı çağımızda, salgın hastalıklarında etkisiyle yüz yüze eğitimden ziyade uzaktan eğitim araçları kullanılarak dersler, sunumlar, etkinlikler ve hatta sanatsal faaliyetler yapılmaktadır.

Uzaktan eğitim araçlarının adli bilişim açısından incelenmesinin amacı, bu materyallerin kullanımı esnasında meydana gelebilecek adli olayların ve inceleme gerektiren durumların ortaya çıkmasıdır. Bu çalışmayla uzaktan eğitim araçları kullanılarak gerçekleştirilen etkinlikler sonrası önemli veriler elde edilmiştir. Bu veriler, kimin, kiminle, nerede, ne zaman, nasıl, ne amaçla bir etkinlik düzenlediği şeklindeki sorulara cevap olarak araştırmayı yapacak kişilere de fayda sağlayacaktır. Birden çok uzaktan eğitim aracı bulunmasına karşın bu çalışmanın kapsamı daha yaygın kullanıldığı için uzaktan eğitim araçlarından olan Microsoft Teams ve Skype uygulamaları üzerinedir.

2017 yılında Microsoft yeni bir iletişim platformu olan Microsoft Teams'i yayınlamıştır. Uygulamanın diğer benzer uygulamalara göre daha yeni bir yayınlanma tarihi olduğu için bu alanda yapılmış çalışmalar oldukça azdır. Ancak alanda edinilen gözlem sonucunda kullanım oranının hızla arttığını görülmektedir. Bu durumda dijital alanda inceleme yapacak kişilerin söz konusu uygulama ile ilgili olarak çalışma gereksinimlerinin olacağını göstermektedir.

Windows 10 işletim sistemine sahip web client uygulamaların yüklü olduğu bilgisayarlar üzerinde gerçekleştirilen bu çalışmada Microsoft Teams ve Skype tarafından depolanan veya ağ üzerinden gelen giden trafik bilgilerinin izole bir ortamda incelenmesi sonucu elde edilen veri ve bilgiler sunulmuştur. Bu çalışmanın gelecekte uzaktan eğitim araçlarına dair araştırma yapacak kişilere yardımcı olması temel amaçlardan biridir.

Anahtar Kelimeler: Uzaktan Eğitim, Adli Bilişim Analizi, Skype Adli Bilişim Analizi, Microsoft Teams Adli Bilişim Analizi

ABSTRACT

Investigation of Distance Education Tools in Terms of Forensic Informatics

Yunus Emre ÇOLAK

Master's Thesis

FIRAT UNIVERSITY
Graduate School of Natural and Applied Sciences

Department of Digital Forensic Engineering

July 2022, Pages: x + 31

People who do forensic research in the digital field have a very difficult job. The continuous development of technology, the publication of new platforms and programs day by day result in the necessity for each application and program to have its own examination methods. This leads to the natural result that the people who will do digital analysis should constantly improve themselves and need resources to guide them in this field.

Examining distance education tools in terms of forensic informatics is an important issue. In our era of increasing digitalization, lectures, presentations and activities are carried out by using distance education tools rather than face-to-face education with the effect of epidemic diseases.

The purpose of examining distance education tools in terms of forensic informatics is to reveal the forensic events that may occur during the use of these education tools and the situations that require investigation. Thanks to this study, important data will be obtained after the activities carried out using distance education tools. Questions such as Who, With Who Where, When, What kind of an event were answered. Although there are multiple distance education tools, the scope of this study is on Microsoft Teams and Skype applications, which are distance education tools.

In 2017, Microsoft released a new communication platform, Microsoft Teams. Since the application has a more recent publication date compared to other similar applications, studies in this area are very few. In this case, it shows that people who will examine in the digital field will need to work on this application.

In this study, which was carried out on computers with client applications with the Windows 10 operating system, the data and information obtained as a result of examining the traffic information stored by Microsoft Teams and Skype or incoming / outgoing over the network in an isolated environment are presented. One of the main purposes of this study is to help people who will do research in this field in the future.

Keywords: Distance Education, Forensic Analysis of Distance Education Tools, Microsoft Teams and Skype Forensic Investigation,

ŞEKİLLER LİSTESİ

Sayfa

TABLOLAR LİSTESİ

Sayfa

KISALTMALAR

Kısaltmalar

TEAMS	:Microsoft Teams Uygulaması
FIREWALL	:Siber Güvenlik Duvarı
IDS	:Intrusion Detection Systems – Saldırı Tespit Sistemleri
SBC	:Session Border Controllers
CID	:Arayan Tanımlayıcı Kimliği
ID	:Identification number- Tanımlayıcı Numara
GIF	:Hareketli Resim
HTTP	:Hiper Metin Transfer Protokolü
WEB	:World Wide Web
EPOCH TIME	:1 Ocak 1970'den (01/01/1970) beri geçen saniye sayısına denilen sayısal veri tipi
PSTN	:Public Switched Telephone Network-Genel Aktarmalı Telefon Şebekesi
VOIP	:Voice Over Internet – Internet Üzerinden Ses,Video veya Mesaj Gönderme
PBX	:Private Branch Exchange – Özel Telefon Şebekesi
ESI	:Elektronic Stored Information
CSV	:Comma Separated Values – Virgülle Ayrılmış Değerler dosyası
API	: Application Programming Interface - Uygulama Programlama Arayüzü

1. GİRİŞ

Tez çalışmamızın giriş kısmında; tezin bilimsel konusu, önemi, problemi, tezin başlıca amacı, problemin çözümüne yönelik geliştirilen hipotezler ve/veya varsayımlar anlatılmıştır.

Toplumların gelişimlerini etkileyen önemli unsurlardan biri eğitimdir. Eğitim sisteminin gelişmişlik düzeyi o toplumdaki bireylerin de eğitime ulaşma ve ulaştığı eğitimin bireye katacağı değer ile doğru orantılıdır.

Eğitim; kişinin zihin, beden, duygusal, toplumsal kabiliyetlerinin, davranışlarının en iyi bir biçimde ya da istek doğrultusunda geliştirilmesi, bireye belirli amaçlara yönelik yetenekler, edinimler, bilgiler kazandırılması süreçlerinin bir bütünüdür [1].

Eğitim faaliyetlerinin insanlık tarihi ile başladığı söylenebilmektedir. Bu anlamda her birey ilk eğitimini ailesinde almaya başlar. Eğitimin önemi ve gerekliliği zamanla daha çok artmaktadır. Bilgi toplumu olabilmek için ön koşullardan biri eğitimli bireylerin sayısının artmasıdır. Ortaya çıkan problemlerin çözümü için metotlar arayan, yaratıcı, kendine koyduğu hedef konularını gerçekleştirmede paylaşımcı olan, adil, bireyler arasındaki ilişkilerde demokratik ve özgün, sosyal ve kültürel konularda hoşgörülü, bütünleyici özellikleri ağır basan, meslek kültürü oturmuş, ahlaki ve etik değerleri bilen bireyleri yetiştirmek ancak eğitimin önemine inanmış toplumlarda mümkün olabilmektedir.

Gün geçtikçe artan nüfus oranı ile beraber eğitime olan ihtiyaçta şüphesiz artmaktadır. Bu eğitim ihtiyacı ortamında bazı gereklilikler ve süreci zorunlu kılan durumlar sonucu yeni eğitim modelleri ortaya çıkmıştır. Yeni modellerin ortaya çıkmasında büyük rol oynayan zorunluluk ve gerekliliklerden biri de çağımızda görülen ve insanoğlu olarak maruz kaldığımız Covid-19 salgınıdır.

Çok kısa bir süre zarfında tüm ülkeleri etkisi altına alan koronavirüsün olumsuz yönde etkilediği süreçlerden biri de eğitimdir. Ülkemizde ilk koronavirüs vakasının ortaya çıktığı tarih Mart 2020'dir. Bu tarihten itibaren doğrudan veya dolaylı olarak bazı zorluklar gün yüzüne çıkmıştır. Bu zorluklardan biri de eğitim alanında yaşanan bazı aksama ve kesintilerdir. Milli Eğitim Bakanlığı ve YÖK tarafından alınan kararlar doğrultusunda öncelikle bir süre eğitimlere ara verilmiş ardından geleneksel yüz yüze eğitim yerine uzaktan eğitime geçiş yapılmıştır [2]. Pek çok uzaktan eğitim uygulama modelleri bu dönemde ortaya çıkmıştır. Uydu TV kanalları, karasal TV kanalları, radyo telsiz frekansları, bilgisayar ve internet bu modellerin uygulanmasında kullanılan araçlardan bazılarıdır.

Bu çalışmada üzerinde duracağımız husus, söz konusu eğitim modellerinin internet ve bilgisayar kullanılarak uzaktan eğitim modeli şeklinde gerçekleştirilenleridir. Çeşitli bilişim teknolojileri araçlarının kullanıldığı bu eğitim modeli çağımızın artık olmazsa olmazları arasında yerini almıştır.

Uzaktan eğitim modellerinde hem eğitimi alanlar hem de verenler farklı zaman ve mekanlarda bulunabilmektedir. Bu durum, eğitimlerin gerçekleştirilmesi ve öğrenmenin kolaylıkla sağlanması amacıyla bilişim ve bilişim araçlarının aktif bir şekilde kullanılmasına dayalı olarak gerçekleştirilen ve "Uzaktan Eğitim" adı verilen bir öğretim yöntemi olarak tanımlanmaktadır [3].

Bilgi çağının bilim insanları, bilgi gelişim sürecinde, maddeyi atomlarına ayırarak bir yerden başka bir yere transfer etmekle ilgili (Teleportasyon), sanal üniversitelerden (Virtual University) , gelişmiş öğrenme ağlarından (Learning Networks) pek çok kişinin şu an hayal bile etmekte zorlanacağı gelişmelerden bahsetmektedirler [4]. Bu durumlar gösteriyor ki hayalini içinde bulunduğumuz yüzyılda kuramadığımız daha nice yeniliklerle karşılaşacağımız olasıdır.

Günümüzde teknoloji kullanımı oldukça yaygınlaşmaktadır. Akla gelebilecek her alanda internet kullanımı neredeyse zorunluluk hâline gelmiştir. İnternet üzerinden yapılan alışverişler, aday mülakat görüşmeleri, danışan-doktor-hasta seansları, eğitim hizmetleri gibi alanlar bu duruma örnek gösterilebilir. Bu gibi alanlarda uzaktan hizmet veren ve/veya hizmet alanların sayısı gün geçtikçe doğal olarak artmaktadır. Uzaktan eğitim araçlarının yoğun kullanılması doğrudan veya dolaylı olarak bu hizmetlere erişimde kötü niyetli kişilerin de ilgisini çekebilmektedir. Gelişen teknolojiye paralel olarak bilgisayar korsanları çeşitli yeni yöntemler ve tekniklerle kişilerin uzaktan eğitim süresince aldığı veya verdiği hizmete çeşitli zararlar verebilmekte ve tehditler oluşturabilmektedirler. Bu bağlamda adli bilişim, dijital platformlarda yer tutan ve çeşitli platformlarca iletilen ses, görüntü, veri veya buna benzer diğer unsurların mahkemelerce sayısal delil olarak nitelendirilebilmesi için saklanıp, incelenip ve mahkemeye sunulabilmesi çabalarının bir bütünü şeklinde tanımlanabilir [5].

1.1. Problem Tespiti

Dijital alanda inceleme yapan adli bilişim uzmanlarının çalıştıkları konuları iyi bir şekilde anlama sorumlulukları vardır. Bununla birlikte bir adli bilişim araştırmacısının teknolojinin sürekli gelişmesi ve yeni platformların ve programların ortaya çıkmasıyla karşılaştığı her yeni uygulamaya aşina güçlük teşkil edebilir. Adli bilişim araştırıcılarının, ihtisas alanları çerçevesinde yer alan bazı uygulamaların nasıl ele alınması ve incelenmesi gerektiğini tüm çerçeveleriyle bilmesi mümkün olmayabilir.

Uzun süredir uzaktan eğitim aracı olarak kullanımda olan platform ve uygulamaların adli bilişim açısından nasıl ele alınacağı, geçmişte konu oldukları adli davalar sonucu bir ihtiyaç hâline gelerek bazı çalışmalar ortaya çıkmıştır. Ancak diğerlerine kıyasla daha yeni bir platform olan Microsoft Teams, ilk defa 2017'de iletişim platformu olarak Microsoft tarafından dünya genelinde yayınlanmıştır [6]. Diğerlerine kıyasla daha yeni yayınlanmış olan Microsoft Teams gibi uzaktan

eğitim uygulama ve platformlarının bu tür adli bilişim inceleme çalışmaları yeterince bulunmamaktadır.

1.2. Amaç

Uzaktan eğitim literatürde zaman ve mekân bağımsız öğrenme aktiviteleri olarak tanımlanmıştır [7]. COVID-19 salgını birçok ülkeyi eğitim öğretim alanında farklı uygulamalara yöneltmiştir. Bazı ülkeler eğitim faaliyetlerine ara vermeyi seçerken bazı ülkeler ise eğitim faaliyetlerine ara vermeden öğretim süreçlerini uzaktan eğitime çevirmiştir. Örneğin; Çin, öğrencilerin eğitim süreçlerinin etkilenmemesi için öğrenmeyi durdurmadan yüz yüze derslere ara verme politikası başlatmıştır [8]. Ancak bu değişiklik için çevrim içi öğrenme ortamının kullanılması ve benimsenmesi sadece teknik bir gereksinimin yerine getirilmesi ile ilgili değildir. Bu olgu aynı zamanda pedagojik ve eğitimsel bir geçişi de ifade etmektedir. Bu nedenle öğretim materyalleri ve müfredat açısından değerlendirildiğinde, süreç önemini artırır. Teknolojinin öğrenci, öğretmen ve kurumlar bazında çapraz iş birliği metodu ile eş zamanlı uygulanması ve uygulanırken bilişim güvenliği bileşenlerinin de göz ardı edilmemesi gerekir [9]. COVID-19 salgının ortaya çıkması birçok eğitim kuruluşu arasında uzaktan eğitim sisteminin daha çok kabul görüp yaygınlaşmasına yardımcı olmuştur [10].

Adli bilişim alanında mevcut olan kanıtlar, meydana gelen suçun çeşitliliğine bağlı olarak değişiklik gösterebilmektedir. Bilgisayar ile etkileşimli suçlarda, bilişim sisteminin farklı bileşen unsurları tarafından toplanan veriler kanıt niteliği taşımaktadır [5]. Uzaktan eğitim araçlarının kullanımının yaygınlaşması ile beraber daha önceden fiziksel olarak sınıflar, toplantı odaları ve konferans salonları gibi eğitim öğretim faaliyetinin gerçekleştiği alanlarda meydana gelen suç konularının bir kısmı artık sanal ortamlara taşınmıştır. Birçok farklı uygulama ve platformlar uzaktan eğitim aracı olarak kullanılmaya başlanmıştır. Geçmişte daha çok fiziksel aletler ve yöntemlerle işlenebilen suçlar dijitalleşmenin giderek artmasıyla birlikte yerini bir takım dijital araçlarla işlenen suçlara bırakmaktadırlar. Elektronik araçlarla işlenen bu suç aralarının arasında; bilgisayarlar, taşınabilir cihazlar, ağ cihazları ve depolama aygıtları gibi elektronik delillerin elde edilebileceği argümanlar bulunur [11]. Microsoft Teams, Microsoft Skype for Business, Zoom, Google Meet, Whatsapp, Slack, Discord bu uzaktan eğitim uygulama ve platformlarından bazılarıdır. Her birinin adli bilişim açısından incelenmesi ve ele alınması farklı metot ve teknikler gerektirebilmektedir.

Uzaktan eğitim aracı olarak kullanılan platform ve uygulamalara bir örnek olan Microsoft Teams, yayınlanmasının üzerinden çok kısa bir süre geçmesine rağmen 2021 yılı nisan ayında 145 milyon günlük aktif kullanıcı sayısına ulaşmıştır [12]. Bu rakam bir önceki yıl olan 2020'nin neredeyse iki katı büyüklüğündedir [13]. Hızlı büyümesinin sonucu olarak da 2022 yılının haziran

ayında şirketin CEO'su Satya Nadella, son 3 aylık kazançlarını açıklarken günlük aktif kullanıcı sayısının da 250 milyonun üzerinde olduğunu belirtmiştir. [14].

Microsoft Teams uygulamasının gün geçtikçe artan günlük aktif kullanıcı sayısı insanlar arasında benimsendiğini göstermektedir ancak şu ana kadar herhangi bir davaya konu olmamış olsa da çok yakın zamanda bir dava konusu olarak adli incelemeye ihtiyaç duyulabilir. Kurumsal yapısı dolayısıyla özellikle beyaz yaka çalışanlarının kullanım oranının da yüksek olduğu düşünülebilir [15].

Amaç; bu çalışma ile bazı uzaktan eğitim araçlarının adli bilişim açısından bir incelenmesinin yapılarak daha sonra bu alanda yapılması muhtemel inceleme ve araştırma çalışmalarına bir ışık tutmaktır.

1.3. Hipotez

Koronavirüs ile iyice yaygınlaşan ve oturmaya başlayan uzaktan eğitim sistemlerinde kullanılan araçların sayısı günden güne artmaktadır. Sadece okula giden öğrenciler değil kurs, seminer ve eğitim kapsamında olan her türlü etkinlik uzaktan yapılmaya başlanıldığı için birçok insanın hayatında aktif yer almıştır. Söz konusu uzaktan eğitim platformlarından bazıları bu çalışmada incelenecek olan Microsoft Teams Web Client ve Skype Web Client uygulamalarıdır.

Bu süreçte, söz konusu platformlarda olası bilgisayar etkileşimli suçların yaşanabileceği göz ardı edilmemelidir. Olası bilgisayar etkileşimli suçların adli incelemelerinde deliller birçok farklı bileşenden elde edilebilir. Bu bileşenler bilinmediği ya da öngörülemediği takdirde bir adli bilişim görevlisi vaka inceleme /analiz aşamalarında yetersiz kalabilir. Bahsedilen durumda daha önce yapılmış benzer bir çalışma adli bilişim incelemesi yapan kişiler için yol gösterici olma niteliği taşıyacaktır.

Olası bir vakada adli bilişim araştırmacıları tarafından alınan bir ağ trafiği kaydı, bu çalışmada izlenecektir. Ağ kaydı alınması, birçok kritere göre paket filtreleme özelliği olan Wireshark uygulaması üzerinden belirtilen anahtar kelimelere göre yapılacaktır, dışa aktarılan nesneler üzerinde çalışılması gibi maddeler içeren bir metot izlenecek inceleme ve analiz adımında vakaya ilişkin delil niteliği taşıyabilecek unsurlara rastlanılmaya çalışılacaktır.

1.4. Tezin Yapısına Genel Bakış

Özet bölümünde tez hakkında genel bir bilgilendirme yapılmıştır. Giriş bölümde tezin önemi, amacı ve hipotezlerinden bahsedilerek kısaca tez özetlenmiştir. Adli bilişim ve bilgi güvenliği kavramları uzaktan eğitim araçlarının adli bilişim açısından incelenmesi bölümü öncesi açıklanarak çalışma zemini hazırlanmıştır.

Ana bölüm olarak uzaktan eğitim araçlarından birkaçının adli bilişim açısından bazı metotlar ile incelenmesi ele alınıp bu alandaki mevcut araçlardan ve çalışma yapılarından bahsedilmiştir. Yapılan çalışma ile ağ dinleme metodu ve dosya yapısı incelemeleri ile ne tür yararlı verilerin elde edilebileceği gözlemlenmiştir. Öneriler bölümünde ise tezin daha nasıl bir ek çalışmalar ile ileri seviyeye taşınabileceği değerlendirilmiş ve tavsiyelerde bulunulmuştur.

2. ADLİ BİLİŞİM VE BİLGİ GÜVENLİĞİ

Bu bölümde adli bilişim ve bilgi güvenliği kavramları ele alınacak ve söz konusu kavramların birbirleri ile ilişkisi üzerinde durulacaktır.

2.1. Adli Bilişim

Adli bilişim, bilişim sistemleri ve üzerinde bulunan veri depo ünitelerinin kullanım alanı olarak incelenerek, bu kullanım alanının dava konusu olayı veya suçu gerçekleştirmede kullanılıp kullanılmadığına dair tüm kanıtları ilgili otoritelerce anlamlı hâlde okunabilecek bir düzende sunma faaliyetlerinin bütünü şeklinde tanımlanabilir [16].
Adli bilişimin birçok tanımı olmasına karşın bütün açıklamalara bu çalışmada yer verilmeyecektir. Araştırma içinde, daha çok dijital araçlar aracılığıyla bir suça karışılmış olması durumunda bu araçların yazılımsal ve donanımsal kısımların teknik olarak incelenmesi konusuyla ilgilenilmiştir.

2.1.1. Adli Bilişimin Önemi

Kısaca özetlemek gerekirse teknolojinin hızla devinimine bağlı olarak, dumanla haberleşme terk edilmiş, el yazısı ve daktilo kullanımları da en az düzeye düşmüştür. Eğitim, zamana ve mekâna bağlı olsun veya olmasın tek yönlü ya da karşılıklı iletişim ön gereksinimine ihtiyaç duyar. İletişim faaliyetlerinin dijital araçlar üzerinden yapılmasıyla birlikte dökümanların ve verilerin de bilgisayar, tablet ve cep telefonu gibi dijital araç ortamlarında oluşturulup saklanması olası hâle gelmiştir. Bazı suçlar fiziksel ortamların yanı sıra artık bu dijital sahalara da işlenebilmektedir [17]. Çeşitli dijital ortamlarda meydana gelen suç sonrası delil niteliği taşıyabilecek verilerin hazırlık, toplama, analiz ve raporlama gibi süreçleri bulunur [18]. Dijital delillere ulaşabilmek için adli bilişim yöntemleri kullanılır [16]. Süreçte adli bilişime konu olmuş delillerin kopyalanması önem arz eder. Adli bilişim disiplininin işaret ettiği şekilde usulüne uygun kopyalanmayan dijital materyaller delil niteliği taşımayacaktır. Ayrıca adli bilişimin işaret ettiği yönde dijital materyallerin kopyalanması araştırma sürecinde de kolaylık sağlayacaktır [19].

2.1.2. Dijital Delil Kullanım Alanları

Dijital deliller, mahkemede kanıt olarak değerlendirilebilen yol gösterici temelinde ikili sayı formatında saklanan veya iletilen bilgilerdir [20]. Bu deliller diğer fiziksel olay yerlerine kıyasla daha çok bilgisayar, tablet, telefon gibi depolama ünitesi olan dijital araçların hafızalarında bulunurlar. Suçların çözülmesinde ve davaların hazırlanmasında kritik bir rol oynarlar. Ancak çoğu zaman bilgisayarlarda, cep telefonlarında ve diğer cihazlarda bulunan kanıtların karmaşıklığı ve çokluğu, kolluk kuvvetlerinin müfettişlerini zorlayabilir [21].

Dijital deliller, sadece elektronik suç için değil her türlü suçun soruşturma ve kovuşturma evresinde kullanılabilir. Örneğin, şüpheliden elde edilen e-posta veya cep telefonu dosyaları şüphelilerin niyetlerini, suç anında nerede olduklarını ve diğer kişilerle fiziksel ilişkilerini ortaya çıkarabilir [20].

2.2. Bilgi Güvenliği

Her kişi veya organizasyonun ister kamu ister özel sektör içinde olsun büyük veya küçük boyutta olması fark etmeksizin korumak istediği bilgileri vardır. Bunlar; müşteri bilgileri, ürün veya hizmet bilgileri veya çalışan bilgileri olabilir. Organizasyon ve kişiler paydaşlarına karşı bilginin güvenliğini en iyi şekilde sağlamakla yükümlüdürler. Maalesef güvenlik alanında yeterince uzmanlaşmış profesyonel personeller her zaman bulunamayabilir. Bunun bir sonucu olarak kurumlar veya kişiler; kendi bilgi ve birikimleri doğrultusunda kısmen doğru veya yanlış bir tutum sergileyerek bilgiyi yetkisiz erişim, bozulma/zarar görme veya yok olma gibi durumlardan korumaya çalışmak için çözüm üretmeye çalışırlar. Bu durumların hepsi birlikte değerlendirildiğinde bir çözümün parçası değilseniz bir problemin parçasınızdır sonucu ortaya çıkabilmektedir [22].

2.2.1. Bilgi

Bilgi, yorumlanmış ya da kişisel anlamda düzenlenmiş enformasyonu ifade eder. Ayrıca bilgi, toparlanıp derlendikten sonra yorumlayarak belirli bazı yöntemlerle kararlara varabilmek için ilgili birimlere gönderilen, bir işlem aşamasından geçerek anlamlı ve belirli bir değer arz eden, kararlara ve davranışlara yön verebilen veri olarak da ifade edilebilir [23]. Varlıkların güvende tutulabilmesi, kuruluşların risklere karşı maruz kalacakları olumsuzlukları en aza indirgemesi ve hizmet kesintisi olmaksızın işin devamı yönünde sürekliliğin sağlanması Bilgi Güvenliği Yönetim Sistemleri'nin üst yönetimin de desteği ile kurulup işletilmesi ile mümkün olabilmektedir [24] . Bu yönetim sistemlerinin koruduğu odak konu ise şüphesiz bilgi olmaktadır.

2.2.2. Enformasyon

Enformasyona kısaca; düzenlenmiş ve elden geçirilerek organize edilmiş veri denilebilir. Enformasyon veriden daha gelişmiş yazılı, sözlü veya görsel ifadeler olarak tanımlanabilir. Enformasyon mesajı alan kişinin algı ve yargısında değişiklik yapmayı hedefler [23]. En sade ifadeyle verilerin bir kademe daha işlenmiş şeklidirler. Veriler anlam kazanarak enformasyona temel oluştururlar. Bu bağlamda enformasyona kısaca anlam kazandırılmış veya yüklenmiş veri de denebilmektedir [25].

2.2.3. Veri

Veriler, üzerinde herhangi bir işlem veya yorumlama yapılmamış ham edinimlerdir [23]. Veriler genellikle araştırma sürecinin ilk girdilerini oluştururlar. Bu girdiler çeşitli işlemlerden geçtikten sonra farklı anlamlar ifade eden birikimlere dönüşürler. Verinin yanı sıra büyük veri kavramı ise veri kümelerini ifade edebilmek için kullanılan bir terimdir. Bu kavram, dünya üzerinde ilk kez 2000 yılının Ağustos ayında düzenlenen 8. Dünya Ekonometri Kongresi'nde ortaya atılmıştır [26]. Büyük veri (Big Data); geleneksel veri saklama alanları ve veriyi işleme teknolojilerinin yeterli olamadığı durumları betimlemek için kullanılan bir terim olmuştur. Büyük veri kavramı yalnızca veri ve verinin barındırıldığı ortamı değil eş zamanlı olarak veriden edinim elde etmeye odaklanmış ileri seviye analiz tekniklerini de kapsar. Büyük veri analizi; iş zekası uygulamaları, tıbbi alandaki analizler, askeri alandaki suçlar olmak üzere benzer birçok alanda kullanılabilmektedir [27].

2.3. Adli Bilişim ve Bilgi Güvenliği İlişkisi

Adli bilişim kavramı mahkemelere mahsus kullanılan ve adli anlamına gelen "forensic" kelimesi ile "computer" kelimesinin birleşiminden ortaya gelmiştir. Yani "computer forensic" terimi dilimize çevrildiğinde "adli bilgisayar" söz öbeği karşımıza çıkar fakat bu söz öbeği yerine adli bilişim kavramı yaygın olarak kullanılmaktadır. Yine adli bilişim terimi bilgisayar kriminalistiği şeklinde de kullanılır [28]. Adli bilişim kapsam olarak dijital verilerin tanımlanıp korunmasını, belgelendirilip yorumlanmasını ifade eder. Ayrıca adli bilişim, dijital verilerden örnek alınması işlemlerini, bazı metodolojileri ve prosedürleri uygulayarak gerçekleştirir [29]. Bilişim teknolojileri bu alanda yapılan çalışmalarla birlikte hayatımıza değişiklik ve yenilik katabilmektedir. Bilişim teknolojilerinin kattığı yenilikler kamu kurumları başta olmak üzere tüm kurum ve kuruluşları kısa sürede etkisi altına almayı başarabilmiştir. Ekonomiden ticarete bilgi sistemlerinden sağlık sektörüne kadar pek çok alanda bilişim teknolojileri aktif olarak kullanılır. Elbette bu durum; bilgi hırsızlığını, bilgiye yetkisiz erişimi ve sistemlere fiziksel olarak zarar verme gibi siber suçları da karşımıza çıkarabilir [30].

Dijital iletişim araçlarının yaygın bir şekilde kullanılması neticesinde elektronik ortamdaki veriler her geçen gün artış göstermektedir. Bu artış hem kurumsal hem de bireysel alanda bilgi güvenliğinin sağlanmasını bir ihtiyaç hâline getirmiştir. Bilgi güvenliğine olan ihtiyacın ortaya çıkmasının sebepleri; elektronik uygulama araçlarının artması, veri paylaşımlarının ağ sistemleri üzerinden gerçekleştirilmesi, bilgiye birçok ortamdan erişilebilir olması, bu ortamlarda güvenlik açıklarının tehdit oluşturması, kişisel ve kurumsal veri kaybında artış meydana gelmesi şeklinde sıralanabilir. Tüm bu faktörlerin yanı sıra saldırganların siber saldırı gerçekleştirirken ihtiyaç duydukları yazılımlara internet üzerinden rahat bir şekilde erişebilmeleri de bilgi güvenliğine olan

gereksinimi artırabilmektedir. Bu gereksinim, bireysel veya kurumsal düzlemde yeni tedbirleri ve dava konusu olaylar sonrası incelemeleri ortaya çıkarır [24]. Dolayısıyla, adli bilişim ve bilgi güvenliğinin ayrılmaz bir bütün oluşturduğu daha net anlaşılabilir. Ayrıca bilgi güvenliği, adli bilişim süreçlerinde elde edilen veriler bağlamında da önem arz eder.

2.3.1. Adli Bilişim Süreçlerinde Bilgi Güvenliği

Adli bilişim süreçleri; bulma, analiz etme ve raporlama olarak sıralanabilir [31]. Her bir işlemin bir başlangıç noktası vardır. Bu başlangıç noktaları; IDS bildirimleri, firewall üzerindeki şüpheli trafik kayıtları, ağ güvenlik sistemlerinin uyarıları, uç nokta koruma uygulamaları gibi suç teşkil etmesi muhtemel konuların birer yansıması şeklinde oluşabilir [32]. Adli bilişim süreçlerinde bilgi güvenliği gerekliliklerinin takip edilmesi uygulanacak olan adli bilişim süreçlerinin geçerliliğini ve verimini de artıracaktır. Adli bilişim süreçleri işletilirken; el konulması planlanan bilgisayardan veri alınması, bilgisayarın dondurulması, verilerin kopyalanması, klonlanması, bilgisayarların kapatılması ve inceleme yapılacak olunan laboratuvara götürülmesi gibi tüm aşamalarda hassas davranılmalıdır. Böylece eldeki delillerin hiçbirinin kaybolmaması veya zarar görmemesi sağlanmalıdır [33]. Adli bilişimde olay yerinin incelenmesinden, elde edilen delillerin adli makamlara sunulmasına kadar birçok aşama bulunmaktadır. Süreçlerin sınıflandırılması bir başka açıdan ise olay yeri tespiti ön incelemesi, delil toplama, analiz ve raporlama olmak üzere dört farklı ana başlık altında değerlendirilebilmektedir [34]. Bu aşamada bahsedilen inceleme süreçlerine değinilmeyecek olup ancak delil toplama aşamasında stenografi yöntemi ile bazı gizlenmiş dosyalar imaj dosyalarında bulunabilmektedir. İsnat edilen suçun niteliği ve kullanıcının bilgisayar yeteneği de dikkate alınarak bu tür gizlenmiş veri kontrolü yapan araçların kullanılması önem arz etmekte olup bu hususun göz önünde bulundurulması inceleme açısından faydalı olabilir [35].

3. UZAKTAN EĞİTİM ARAÇLARININ ADLİ BİLİŞİM AÇISINDAN İNCELENMESİ

Bu bölümde bazı uzaktan eğitim araçlarının adli bilişim açısından incelenmesinin öneminden bahsedilmektedir. Uzaktan eğitim araçlarının çalışma mantığı anlatılarak ilgili literatür incelenecektir.

Uzaktan Eğitim araçlarından Microsoft Teams ve Skype incelemesi yapılan uygulamalar olacaklardır.

3.1. Uzaktan Eğitim Araçlarının Bazılarına Genel Bir Bakış

Bu çalışmada, uzaktan eğitim aracı olarak kullanılabilen uygulamalardan Microsoft Teams ve Skype uygulamaları hakkında adli bilişim açsından genel bir bakış gerçekleştirilecektir.

3.1.1. Skype

Skype ilk yayınlanma tarihi olan 2003 yılından günümüze kadar kullanım oranı oldukça yüksek bir iletişim uygulaması olarak karşımıza çıkmaktadır. Bu uygulama, internet üzerinden telefon ve video görüşmesine imkân tanımaktadır.

Geçmişte yapılan araştırmalar, Skype ile ilgili olarak iOS işletim sisteminden işe yarayabilecek bazı verilerin kurtarılabileceğini gösterir [36]. iOS işletim sisteminin yanı sıra Android ortamlarda da verilerin elde edilebileceğini gösteren çalışmalar bulunmaktadır [37]. Mobil işletim sistemlerindeki bu çalışmaları destekleyici olarak Skype için Windows ortamlarındaki araştırmalar da bulunur [38]. Ayrıca Microsoft'un kurumsal çözümü olan Skype for Business için de Windows masaüstü ortamlarında yapılmış mevcut araştırma çalışmalarına rastlanabilir [38].
Skype, Skype for Business ve Microsoft Teams birbirlerinden bağımsız yapılar olmasına karşın, geçmişte bu uygulamaların verileri nerede ve nasıl depoladıklarına dair yapılan araştırma sonuçları çalışmalarımıza fikir verebilir.

Tablo 3.1. Skype Veri Yolları

SIRA No	Veri Adres Yolu
1	%AppData%\Local\Packages\Microsoft.SkypeApp_kzf8qxf38zg5c\LocalState\
2	%LOCALAPPDATA%\Microsoft\Office\16.0\Lync\7
3	HKEY_USERS\<SID>\Software\Classes\LocalSettings\Software\Microsoft\Windows\CurrentVersion\AppModel\Repository\Families\Microsoft.SkypeApp_kzf8qxf38zg5c
4	HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Lync

Yinelenen anahtar dosya yolu Tablo 3.1. de 1 numaralı sırada bulunmaktadır [38]. Bu dosya yolundaki %AppData% geçerli Windows kullanıcısının dolaşımdaki uygulama verilerinin bulunduğu yere işaret eder [18].

3.1.2. Microsoft Teams

Microsoft Teams altyapısı, PSTN telefon servisleri ile entegre olabilmektedir. Varsayılan olarak Microsoft 365 servisleri kullanılabilirken diğer PSTN servisleri de tercih edilebilir. PSTN gibi servisleri desteklemiş olması Microst Teams'in çeşitli kötü niyetli kişilerin ilgisiyle beraber saldırı gelebilecek atak alanlarını da genişletebilir.

Microsoft Teams özellikleri birçok eklentiler ile zenginleştirilebilmektedir. Bu eklentilerin bazıları Microsoft tarafından geliştirilmişken bazıları diğer firmalar/kişiler tarafından geliştiririlebilir.

Microsoft Teams, bilgisayarlar ve mobil cihazlar tarafından kullanılabilen 3 ana hizmet kategorisinde fayda sağlayan güçlü bir iletişim aracıdır. Bu 3 hizmet kategorisi; toplantı ihtiyaçları, gerçek zamanlı iletişim ihtiyaçları ve uygulamalar yardımıyla özelleştirilmiş diğer hizmetler olarak sınıflandırılabilir.

Toplantı ihtiyaçları doğrultusunda kullanım gerçekleştirilen senaryolarda Microsoft Sharepoint ve Microsoft OneDrive diyalog içeriklerini ve dosyalarını kullanıcıların birlikte çalışabilmelerine ve dosyaları versiyon numaraları ile saklamaya imkân tanır. Aynı zamanda Microsoft Exchange ile entegre olması takvim özelliği etkinleştirilmiş kanallara mail gönderme, görev atama ve uygunluk durum bildirimleri gibi konularda kolaylık sağlar. Canlı etkinlikler ile eş zamanlı 10.000 kişiye kadar katılım imkânı sunar. Metne çeviri özelliği ile beraber canlı

etkinliklerde, sahip olduğu yapay zekâ entegrasyonu marifetiyle değişik dillerdeki konuşmaları farklı lisanlara çevirebilmektedir. Ancak bu çalışmanın yapıldığı zaman diliminde Türkçe konuşmadan metne çeviri henüz desteklenmemektedir.

Gerçek zamanlı iletişim hizmeti kapsamında VOIP teknolojisi ile kuruluş içi veya kuruluş dışı kullanıcıların eş zamanlı olarak çevrim içi sesli, görüntülü veya veri paylaşımlı iletişimine olanak sağlar. Ayrıca dijital resepsiyon, çağrı kuyruk yönetimi otomatik çağrı atamaları veya yönlendirme politikalarının kullanımına yardımcı olarak bir sanal santral gibi kullanıma olanak verir.

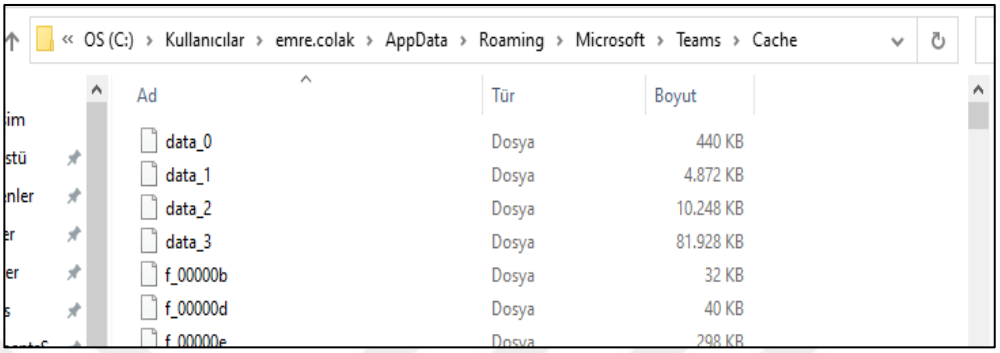
Uygulamalar yardımıyla Microsoft Teams çeşitli ihtiyaçlar doğrultusunda kapasite geliştirmeye imkân tanır. Bu yüzlerce uygulama Microsoft tarafından üretilmiş olabileceği gibi diğer firmalarca da oluşturulmuş olabilir.

Microsoft Teams'in incelemeleri kurumsal platformlarda yönetim merkezi üzerinden yapılabilmektedir. Microsoft Teams'in çalışma mantığı gereğince tüm iletişim merkezi server üzerinden dönmektedir. Bu kurumsal yönetim merkezi üzerinden yapılan incelemeler oldukça verimli bilgiler sunmaktadırlar. Kuruluş içerisinde gerçekleştirilen iki yönlü bir diyalog sonucunda kullanıcıların birbirlerine göndermiş oldukları mesajlar, kanal içi görüşmeler, son aktivite saati, kullanıcıların kullandıkları cihazın işletim sistemi türü vb. gibi birçok bilgiye ulaşılabilmektedir.

Bazı durumlarda kuruluş ayarları doğrultusunda kurum içi kullanıcılar dışarıdaki Skype kullanıcıları ile de görüşme sağlayabilmektedirler. Ancak ilgili kullanıcı dışarıda olduğu ve Skype üzerinden bir iletişim gerçekleştirildiği için bu yönetim panelinden elde edilecek veriler maalesef kısıtlı olabilmektedir. Bu gibi durumlarda ise SCB server kurulumu ile trafiğin ağ dinleme ve bilgisayar içeriğinin farklı inceleme yöntemleri ile bazı aksiyonlar alınarak analiz edilmesi gerekebilmektedir.

Bu bağlamda Windows uygulamaları genellikle kendi datalarını AppData dizininde saklarlar [39]. Bu AppData dizini genellikle C:\Kullanıcılar\<kullanıcı_adi>\AppData\Roaming yolunda bulunur. Yol adresindeki kullanıcı adı geçerli kullanıcının kim olduğuna göre değişiklik gösterir. AppData yolu Windows sürümlerinde değişiklik gösterebilse de %AppData% değişkeni ile işaret edilebilir. Teams AppData klasörü, C:\Kullanıcılar\<kullanıcı_adi>\AppData\Roaming\Microsoft\Teams klasör yolunda bulunur. Teams AppData klasör içinde bulunan Cache isimli klasör Teams'e ait Chromium Cache formatındaki dosyaları barındırır. Dosyaların chromium formatında olması Microsoft Teams masaüstü uygulamasının açık kaynak kodlu electron ile geliştirildiğini göstermektedir [40]. Bu aynı zamanda Google Chrome uygulamasının formatı ile benzerlik gösterir. Bu nedenle CromeCashView uygulaması Microsoft Teams'in cache klasörünü incelemede oldukça kolaylaştırıcıdır.

Ayrıca Teams in AppData klasörü içerisinde indexDB isimli klasör bulunur. Bu klasör içerisinde levelDB isimli veri tabanı yapısını barındırır. LevelDB, veriye ait anahtar ve değerleri içerir. Şekil 3.1. Microsoft Teams Cache Klasörü Dosya Yapısı ile cache klasörü dosya yapısı gösterilmiştir.

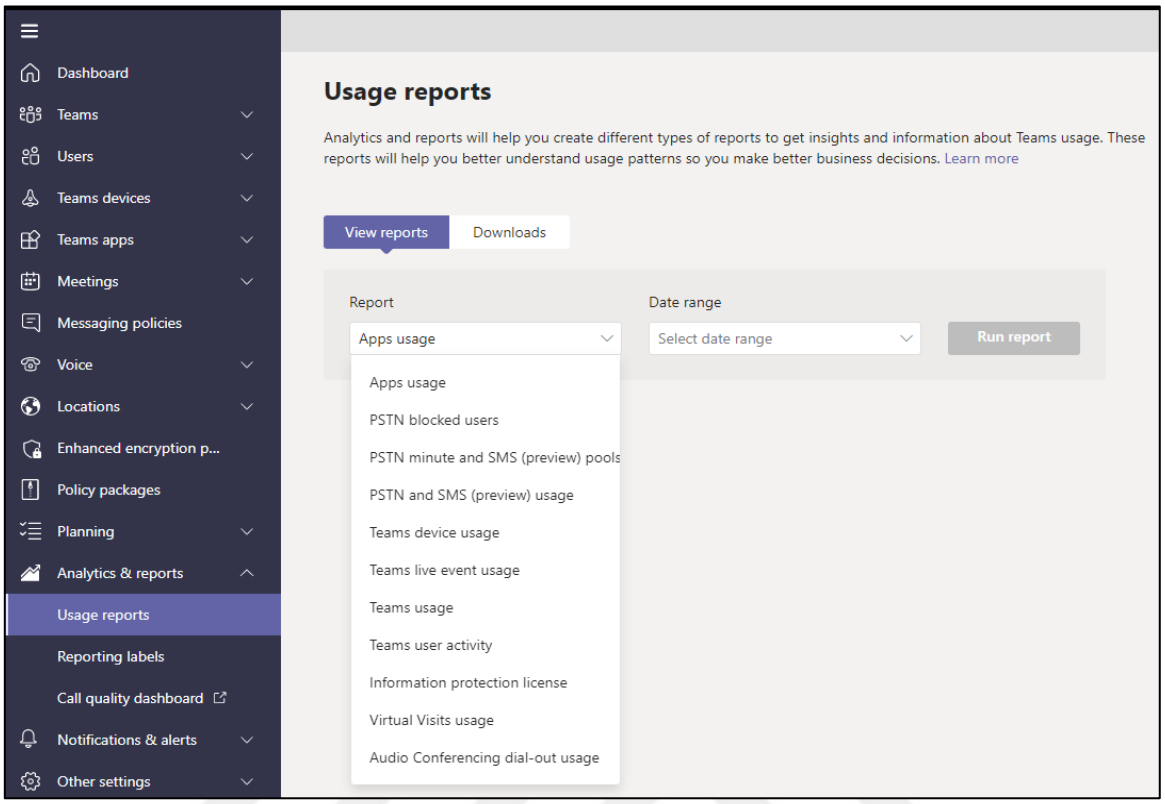


Şekil 3.1. Microsoft Teams Cache Klasörü Dosya Yapısı

3.2. Microsoft Teams'in Proaktif ve Reaktif Bağlamda Adli Bilişim Açısından İncelenmesi

Dava konusu olan olayın durumuna göre kurumsal çatı altında bazı kullanıcıların yapmış oldukları her dijital hareketin kayıt altına alınmasına ve daha sonrasında bu kayıtların dışarı aktarılmasına ihtiyaç duyulabilmektedir. Bir olayın meydana gelmesinden önce bu tür bir önlemin alınarak ilgili kullanıcı veya kullanıcılar ile ilgili kayıt tutma işlemine başlanması "proaktif" bir yaklaşım tarzını ortaya koyarken; ani gelişen bir durum sonucunda mevcuttaki durumun bir ön hazırlık olmaksızın aniden incelenmesi ve delil elde edilebilmesi çalışma çabaları "reaktif" bir durumu ortaya çıkarmaktadır.

Kurumsal yapılarda Microsoft Teams kurulumu varsayılan ayarlar ile yapılmış ise Teams üzerinden kullanıcılar ancak 30 günlük geçmişe dönük arama kayıtları aktivitesi görüntüleyebilmektedir. Daha eski kayıtlara ulaşılmak isteniyor ise yönetici yetkisine sahip bir personel, Teams Yönetici Merkezine giderek Analiz ve Raporlar bölümündeki Kullanım Raporları bölümünden 90 günlük geçmiş kayıtları görüntüleyebilir ve dışarı aktarabilir. Bu rapor türü aşağıda bulunan Şekil 3.2. Teams Kullanıcı Kullanım Raporları Bölümü görülebileceği üzere özelleştirilebilmektedir. Özelleştirilerek oluşturulan rapor daha sonra "İndirmeler" bölümünden dışarıya aktarılabilmektedir. Ayrıca zaman tarih aralığı seçilerek istenen bir zaman dilimine özgü raporlar da oluşturulabilmektedir.



Şekil 3.2. Teams Kullanıcı Kullanım Raporları Bölümü

Şekil 3.3. Teams Kullanıcı ve Yönetici Etkinlik Kaydını Etkinleştirme görselinde de görüleceği üzere, geçmişte bulunan detaylı kayıtlarına ulaşılmak istenmesi durumunda; Microsoft'un uyumluluk merkezi olan https://compliance.microsoft.com/ adresine gidilerek sol menüdeki denetim sekmesinden "Kullanıcı ve Yönetici Etkinliğini Kaydet" butonuna tıklanmalıdır. Böylece etkinlik kaydı kurumsal bağlamda etkin hâle getirilmelidir.

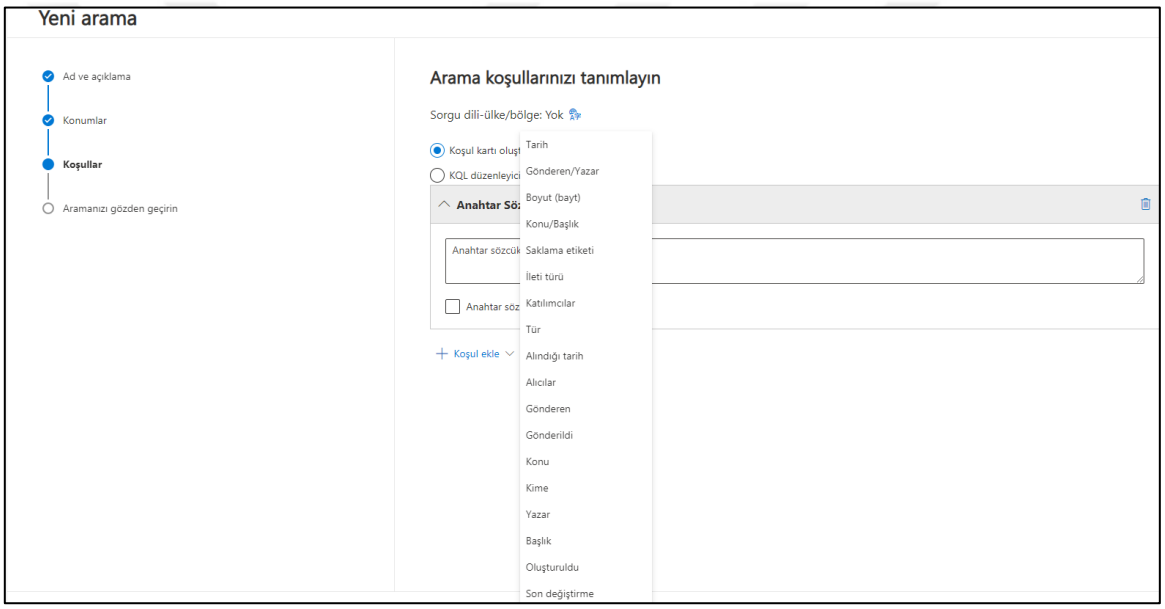
Şekil 3.3. Teams Kullanıcı ve Yönetici Etkinlik Kaydını Etkinleştirme

Etkinleştirme yapıldıktan sonra kurumsal bağlamda etkinlik kayıtlarının tutulması faaliyeti en geç 60 dakika içerisinde aktifleşmiş olmaktadır [41].

3.2.1. Microsoft Teams İçerik Arama

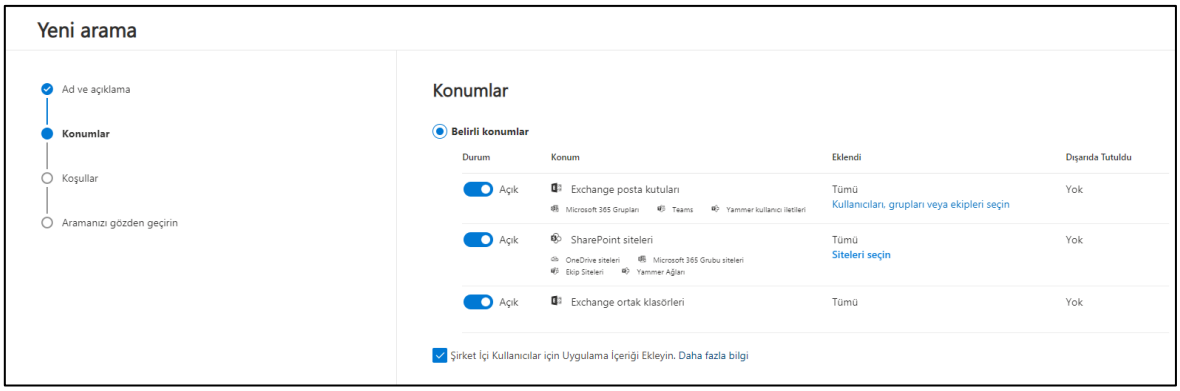
Teams yönetici yetkilerine sahip olan personel, uyumluluk merkezine giderek sol menüde bulunan İçerik Arama sekmesinden kuruluşla ilgili olarak birçok arama gerçekleştirebilir. Bu işlemi yaparken arama kriteri olarak birçok koşul belirlenebilmektedir.

Yeni bir arama yapılırken Kim, Kime, Ne zaman, Konumlar gibi birçok hazır koşul sistem tarafından sunulmaktadır. Şekil 3.4. Teams İçerik Arama Bölümü Koşul Özelleştirmeleri görselinde seçilebilecek bazı koşullar gözlenmektedir.



Şekil 3.4. Teams İçerik Arama Bölümü Koşul Özelleştirmeleri

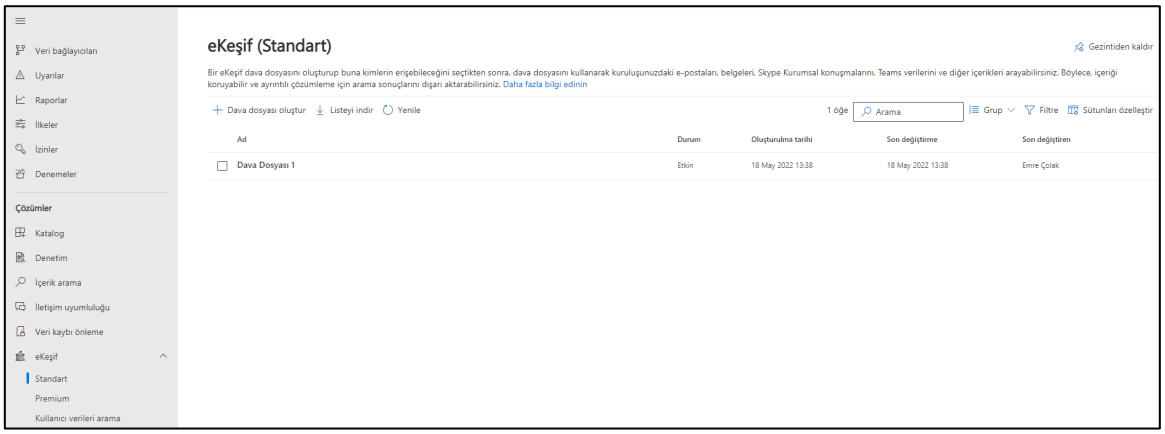
Şekil 3.5. Teams İçerik Arama Bölümü Konum Özelleştirmeleri görselinde ise konumların seçiminin yapılabileceği alan görülmektedir. Bu bölümde istenen tüm bilgilere erişilebilmektedir. Ancak bu geniş yetki yelpazesi bir yönden de gizlilik konusunda sorun teşkil etmektedir. İlgili dava konusu sadece belirli kişi veya kişiler olmasına karşın bu bölümden istenen tüm kullanıcıların verilerine erişilebilmektedir. Bu sorunun önüne geçmek için Microsoft e-keşif adı verilen bir bölümü de kullanıma sunmaktadır.



Şekil 3.5. Teams İçerik Arama Bölümü Konum Özelleştirmeleri

3.2.2. Microsoft Teams E-Keşif

Microsoft dava konusu olan olaylarla ilgili olarak soruşturma safhasında gizlilik ihlalinin önüne geçebilmek adına bazı tedbirleri almıştır. Sadece ilgili davaya konu olmuş veya olması muhtemel kişi ya da kişilerin ilgili araştırma dosyasına eklenebilmesine olanak tanır. Aynı zamanda farklı farklı dava dosyaları oluşturulmasına da imkân verir. Bu bölüm ise yine Şekil 3.6. E-Keşif Bölümünde Oluşturulan Örnek Bir Dava Dosyası görselinde de sol menüde gözüken e-keşif bölümünden yapılabilmektedir. E-keşif bölümde oluşturulan dava dosyası ile o davaya özgü araştırmalar ve dışa aktarımlar belirli kişilere yetki verilerek atanabilmektedir.



Şekil 3.6. Teams E-Keşif Bölümünde Oluşturulan Örnek Bir Dava Dosyası

Dava dosyası üzerinde yönetici tarafından yetkilendirilen kişiler yine yönetici tarafından kendilerine verilen yetki çerçevesinde ilgili dava dosyası içerisinde araştırma ve sorgulama işlemlerini yürütebilmektedirler.

4. MATERYAL VE METOT

Bu bölüm bu çalışmada kullanılan materyal ve metotları açıklamaktadır.

4.1. Materyal

Kullanılan materyaller Yazılım ve Donanımsal materyal olarak iki başlık altında değerlendirilmiştir.

4.1.1. Donanımsal Materyaller

1 Adet Windows 10 20H2 versiyonlu işletim sistemine sahip x64 bit mimaride 512 GB disk kapasiteli 32 GB RAM'e sahip Dell marka 7300 model dizüstü bilgisayar.

4.1.2. Yazılımsal Materyaller

1 Adet Windows İşletim Sistemi
1 Adet WMware Workstation 16 Sanallaştırma Çözümü
2 Adet Sanal Bilgisayar
- 2 GB RAM
- 2 Sanal İşlemci
- 50 GB Depolama Alanı
- NAT'lı Ağ Arayüzü
- Windows 10 21H2 x64 İşletim Sistemi
- Etki Alanı Harici Temiz Yerel Hesaplı Kurulum

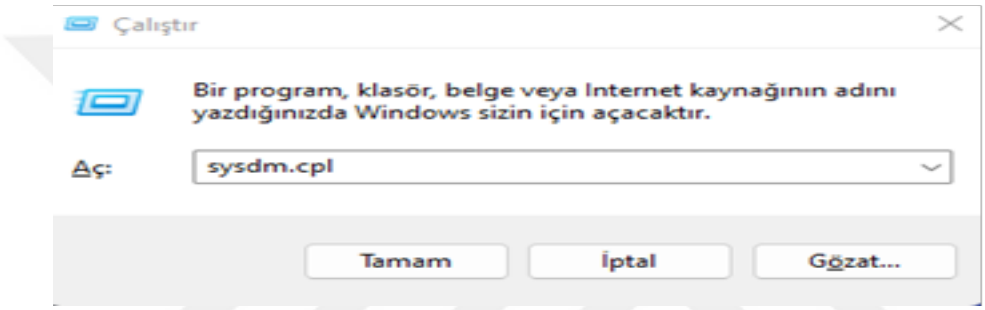
2 Adet Microsoft Teams Masaüstü Uygulaması Ver:1.5.00.11163
2 Adet Microsoft Skype Web Uygulaması
1 Adet Chrome Cache Viewer Uygulaması
1 Adet Skype Uygulaması
1 Adet Fiddler Uygulaması
1 Adet WireShark Uygulaması
1 Adet Teams Yönetici Hesabı
2 Adet Bağımsız Kullanıcı E-mail Hesabı
1 Adet Kurumsal Office 365 Kiracı Hesabı ve Office 365 E1 Lisansı

4.2. Metot

Çalışma yapılırken kullanılan inceleme metotları bu başlık altında toplanmıştır. Her bir uygulama kendisine özgü olarak kullanılan metot çerçevesinde incelenmiştir.

4.2.1. Skype Web Client İnceleme Metodu

İlk adımda tarayıcı üzerinde çalışan Skype Web Client üzerinde ağ kaydı alınmadan önce şifreli trafiğin decrypt edilmesini sağlayan SSL Anahtarları için Windows 10 Client üzerinde "Environment Variables (Ortam Değişkenleri)" tanımlaması yapılmıştır. Bunun için regedit'ten "sysdm.cpl" çalıştırılıp "Ortam Değişkenlerinden "SSLKEYLOGFILE" adında yeni bir ortam değişkeni tanımlanmıştır.



Şekil 4.1. Ortam Değişkeni İçin Sistem Özelliklerine Giriş

Bu Şekil 4.1. Ortam Değişkeni İçin Sistem Özelliklerine Giriş görselinde de görüldüğü üzere sunucu ile client arasında geçen şifreli trafiğin decrypt edilebilmesi için gerekli anahtarları sağlamıştır.

Wireshark inceleme yapılacak olan bilgisayarlara kurulmuş sonrasında ise her iki kullanıcı bilgisayarında da Wireshark ağ kaydı başlatılıp Chrome Tarayıcı üzerinden Skype Web uygulamasına https://www.skype.com/tr/features/skype-web/ adresi üzerinden kullanıcı girişleri yapılmıştır.

Ağ kayıtlarında arama ve analiz yaparken rastlanılabilecek mail adresleri ve şifrelerin belli olması için "test1forensic", "test2forensic", "test1", "test2" kullanıcı adları kullanılmıştır. Giriş yapıldıktan sonra test1 ve test2 kullanıcıları arasında bir mesaj sohbeti başlatılmış ve bu kısımda gönderilebilecek text mesaj, chat üzerinden resim gönderimi, emoji ve GIF (hareketli resim), tepki ekleme işlemleri sırasıyla yapılmıştır.

Mesaj sohbeti sonrasında test1 ve test2 kullanıcıları arasında 25 saniye süren bir "Sesli Arama" yapılmıştır. Sonrasında ise yine ağ kaydı analizi yaparken tüm özelliklerin incelenebilmesi

için “Videolu Arama” gerçekleştirilmiş ve hem kamera hem mikrofon açılarak ses ve görsel verilerinin ağda akışı sağlanmıştır. “Mesaj Sohbeti”, “Sesli Arama” ve “Videolu Arama” özellikleri kullanıldıktan sonra Wireshark üzerinden alınan ağ kaydı durdurulup kaydedilmiştir.

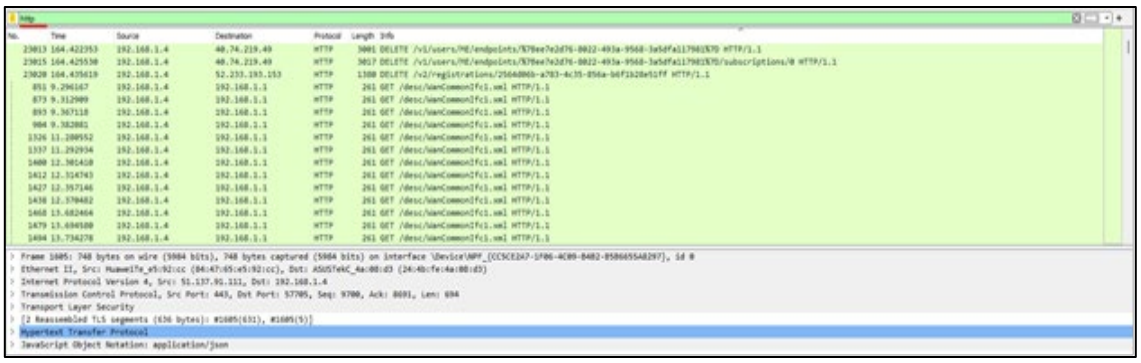
4.2.2. Microsoft Teams İnceleme Metodu

İlk adımda tarayıcı üzerinde çalışan Microsoft Teams Web Client üzerinde ağ kaydı alınmadan önce şifreli trafiğin decrypt edilmesini sağlayan SSL Anahtarları için Windows 10 Client üzerinde “Environment Variables (Ortam Değişkenleri)” tanımlaması yapılmıştır. Bunun için regedit’ten “sysdm.cpl” çalıştırılıp “Ortam Değişkenlerinden “SSLKEYLOGFILE” adında yeni bir ortam değişkeni tanımlanmıştır. Sunucu ile client arasında geçen şifreli trafiğin decrypt edilebilmesi için gerekli anahtarları sağlamıştır.

Wireshark inceleme yapılacak olan bilgisayarlara kurulmuş sonrasında ise her iki kullanıcı bilgisayarında da Wireshark ağ kaydı başlatılıp Chrome Tarayıcı üzerinden Microsoft Teams Web uygulamasına https://www.microsoft.com/tr-tr/microsoft-teams/log-in adresi üzerinden kullanıcı girişleri yapılmıştır.

Ağ kayıtlarında arama ve analiz yaparken rastlanacak mail adreslerinin ve şifrelerin belli olması için “test1forensic”, “test2forensic”, “test1”, “test2”, “forensic1”, “forensic2” kullanıcı adları kullanılmıştır. Giriş yapıldıktan sonra test1 ve test2 kullanıcıları aralarında bir mesaj sohbeti başlatılmış ve bu kısımda gönderilebilecek text mesaj, chat üzerinden resim gönderimi, emoji ve GIF (hareketli resim), tepki ekleme işlemleri sırasıyla yapılmıştır. Mesaj sohbeti sonrasında “Sesli Arama” başlatılmış ve 1 dakika 25 sn süresince ağda verilerin akışı sağlanmıştır. Sonrasında ise yine ağ kaydı analizi yaparken tüm özellikleri incelenebilmesi için “Videolu Arama” ve “Toplantı Araması” gerçekleştirilmiş ve hem kamera hem mikrofon açılarak ses ve görsel verilerinin ağda akışı sağlanmış Wireshark üzerinden alınan ağ kaydı durdurulup kaydedilmiştir.

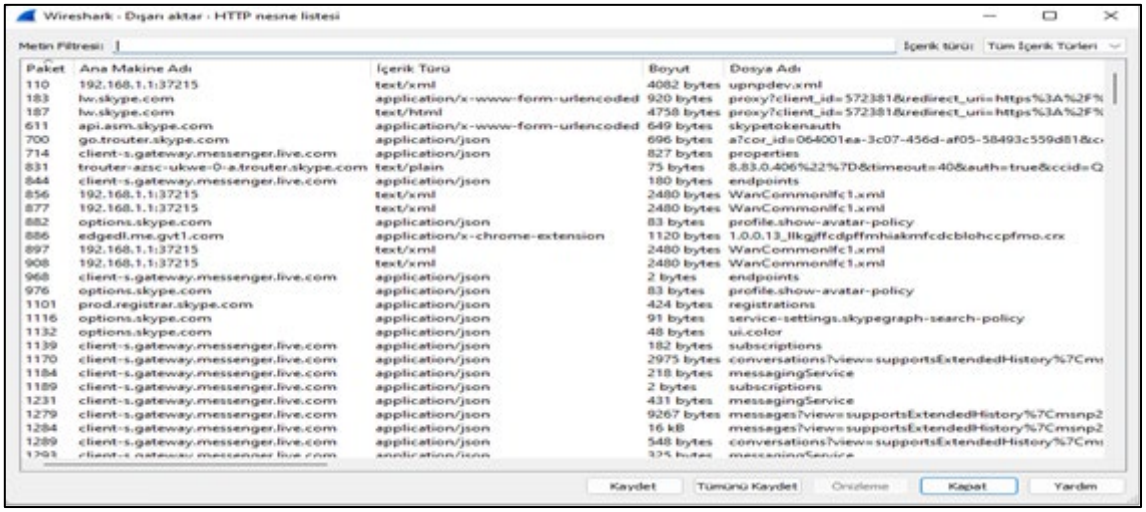
5. BULGULAR VE TARTIŞMA



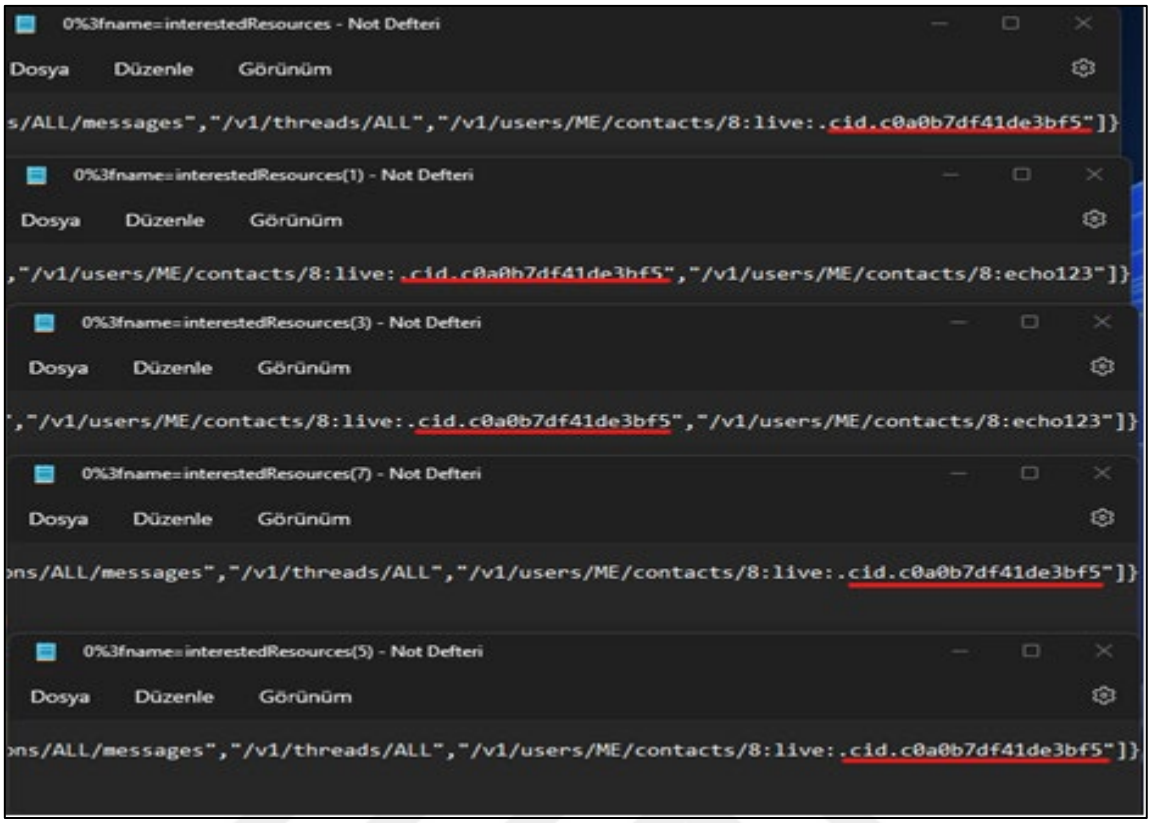
Şekil 5.1. Wireshark http trafik filtresi

İşlemler tamamlandıktan sonra Wireshark ağ kaydı üzerinde belirli filtreler ve aramalar ile yapılan incelemeler aşağıdaki gibidir. Şekil 5.1. Wireshark http trafik filtresi görselinde önce alınan HTTP paketlerinin görüntülenmesi için "http" filtresi uygulanmıştır. Sonrasında alınan HTTP objeleri dışa aktarılarak, dışa aktarılmış nesneler üzerinde analize başlanmıştır.

Şekil 5.2. Dışa Aktarılan http Nesneleri ve Şekil 5.3 Export Edilen Dosyalardaki CID Değerleri görsellerinde de görüldüğü üzere dışarı aktarılan "0%3fname=interestedResources" adlı dosyada ve benzer ada sahip 8 farklı dosyada aynı olan bir "cid" değerine rastlanmıştır.

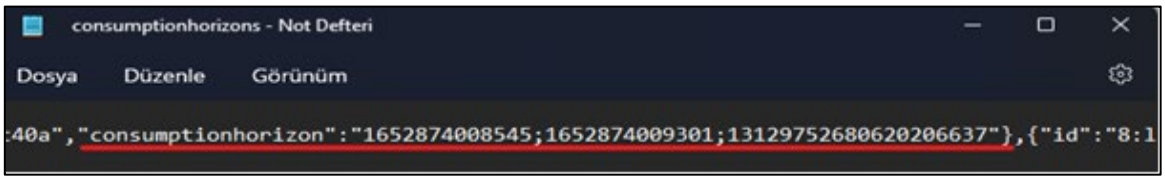


Şekil 5.2. Dışa Aktarılan http Nesneleri



Şekil 5.3. Export Edilen Dosyalardaki CID Değerleri

Şekil 5.4. Alındı ve Okundu Durumlarının Zaman Damgaları görselinde görüldüğü üzere "consumptionhorizons" adlı dosyada alındı/okundu durumlarının zaman damgalarına rastlanmıştır.



Şekil 5.4. Alındı ve Okundu Durumlarının Zaman Damgaları

İlgili zaman damgalarının insan zamanı ile değil bilgisayar zamanı olarak adlandırılan "Epoch Timestamp" formatında olduğu Şekil 5.5. Epoch Timestamp Formatındaki Zaman Damgaları görselinde görülmüştür.

Şekil 5.5. Epoch Timestamp Formatındaki Zaman Damgaları

Rastlanılan zaman damgalarının tutulduğu değişkenler ""consumptionhorizons" ve "version" olmak üzere 2 tanedir.

Şekil 5.6. Zaman Damgası Formatı Dönüşümü

Şekil 5.6. Zaman Damgası Formatı Dönüşümü görselinde gözlemlenebileceği üzere zaman damgalarının karşılık geldiği zaman dilimleri görülebilmektedir.

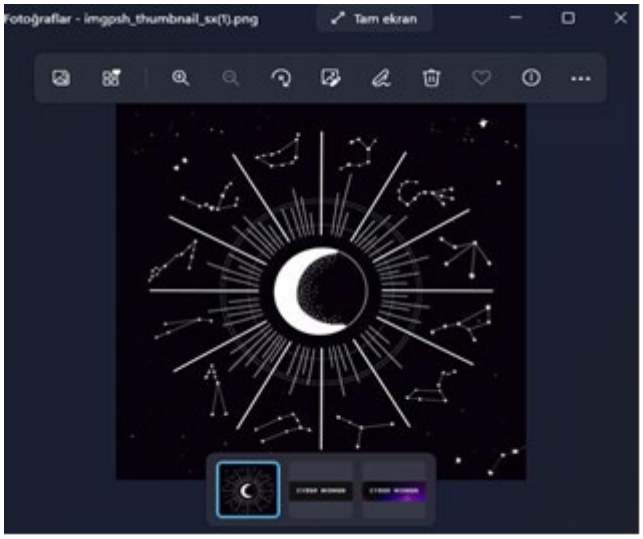
Export edilen "destinations%3flanguage=tr&deviceId=064001ea-3c07-456d-af05-58493c559d81&sessionId=0c75dccd-a807-4f58-a64f-942c1cdb9d03" adlı dosyanın adında Şekil 5.7. Dil, Cihaz Id'si ve Oturum Id'si görselinde işaretlendiği üzere dil, cihaz Id'si ve oturum Id'si görülmektedir.

Şekil 5.7. Dil, Cihaz Id'si ve Oturum Id'si

Ayrıca Şekil 5.8. Skype Tanıtım Metni görselinde de görülebileceği üzere dosyanın içinde Skype'a ait Türkçe dilinde yazılmış bir reklam-tanıtım metnine rastlanmıştır.

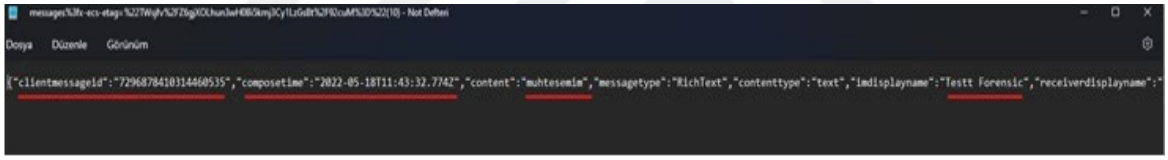
Şekil 5.8. Skype Tanıtım Metni

Şekil 5.9. Chat Üzerinden Gönderilen Görsel ile de görüldüğü üzere mesajlaşma sırasında chat üzerinden karşıdaki kullanıcının gönderdiği görsel/resimler "imgpsh_thumbnail_sx", "imgpsh_thumbnail_sx(1)" ve "imgpsh_thumbnail_sx(2)" adlı dosyalarda thumbnail olarak görülmüştür.



Şekil 5.9. Chat Üzerinden Gönderilen Görsel

Gönderilen mesajların text şeklinde açık ve net olduğu aşağıdaki Şekil 5.10. Gönderilen Mesajlar görselinde de gözükmektedir. Aynı zamanda gönderici ve alıcının kullanıcı adları, "Test Forensic" ve "Testt Forensic" olarak, kullanıcının mesaj Id'si ve zamanı da görülmektedir.

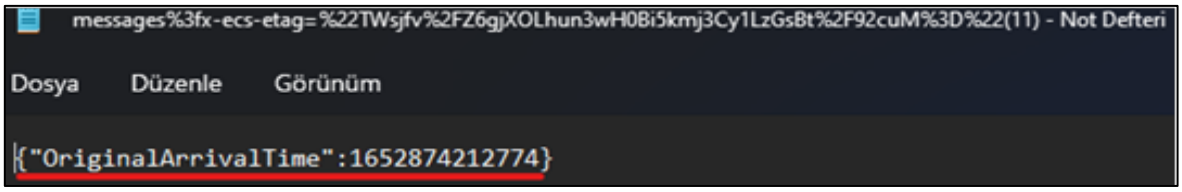


Şekil 5.10. Gönderilen Mesajlar

Kullanıcının karşıya "merhaba test1" mesajını gönderdiği Şekil 5.11. Gönderilen "merhaba test1" Mesajı görselinde gösterilmiştir.

Şekil 5.11. Gönderilen "merhaba test1" Mesajı

Yapılan incelemeler sonucunda diğer tüm mesajların da yukarıdaki mesajlar gibi açık ve net görüldüğü gözlemlenmiştir. Mesajın karşıdaki alıcıya varış zamanı "messages%3fx-ecs-etag=%22TWsjfv%2FZ6gjXOLhun3wH0Bi5kmj3Cy1LzGsBt%2F92cuM%3D%22(11)" adlı dosyada aşağıdaki Şekil 5.12. Mesajın Karşıdaki Alıcıya Ulaşma Zamanı görselinde epoch formatında gösterilmektedir.



Şekil 5.12. Mesajın Karşıdaki Alıcıya Ulaşma Zamanı

Kullanıcının o anki ulaşılabilirlik durumunun, çevrim içi/çevrim dışı olduğu bilgisinin de tutulduğu Şekil 5.13. Kullanıcının O Anki Ulaşılabilirlik Durumu görselinde gözlemlenmiştir.

Şekil 5.13. Kullanıcının O Anki Ulaşılabilirlik Durumu

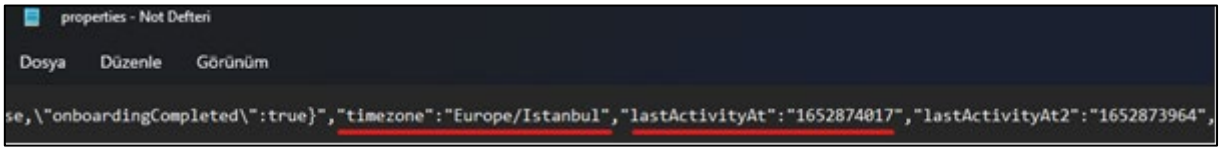
Şekil 5.14. Kullanıcıların Profil Resimlerinin cid Değerleri ve Dosya Adları isimli görselde kullanıcıların profil fotoğraflarının "cid" değerleri ile birlikte "filename" de belirtilerek tutulduğu gözlemlenmiştir.

Şekil 5.14. Kullanıcıların Profil Resimlerinin cid Değerleri ve Dosya Adları

Videolu ve sesli aramalarda her iki kullanıcının da cid'lerinin tutulduğu ve görüldüğü gözlemlenmiştir. Cid'ler Şekil 5.15. Sesli ve Görüntülü Aramalarda Tutulan "cid" Değerleri görselinde de işaretlenmiştir.

Şekil 5.15. Sesli ve Görüntülü Aramalarda Tutulan "cid" Değerleri

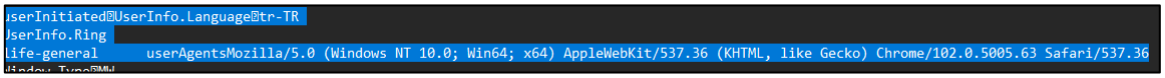
Kullanıcılarının "timezone"ları ve son aktif oldukları zamanların aşağıdaki Şekil 5.16. Timezone ve Son Aktif Olunan Zaman görselinde ki gibi olduğu gözlemlenmiştir.



Şekil 5.16. Timezone ve Son Aktif Olunan Zaman

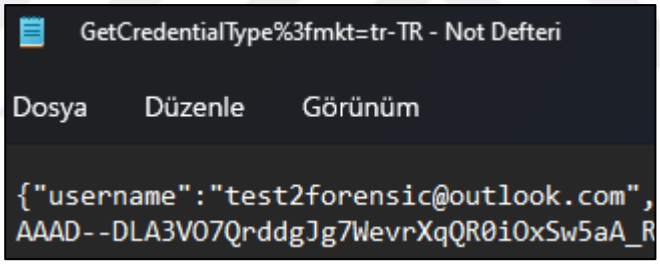
Skype Web Client üzerinde uygulanan metot Microsoft Teams Web Client üzerinde de uygulanmış ve sonucunda aşağıdaki bulgulara rastlanmıştır;
Dışa aktarılan nesneler üzerinde inceleme yapılırken ilk rastlanan bulgu “skypetoken” olmuştur. Her iki uygulama da aynı yapımcıya ait olduğundan bunun sebebinin aynı altyapıyı kullanmaları olduğu söylenilebilir.

Şekil 5.17. Kullanılan Dilin Türkçe Olduğu Bilgisi görselinde görüldüğü üzere kullanılan dilin” Türkçe” olduğu bilgisine rastlanmıştır.

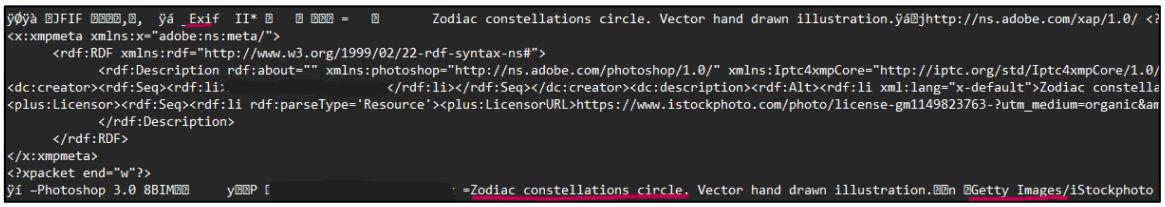


Şekil 5.17. Kullanılan Dilin Türkçe Olduğu Bilgisi

Test2 kullanıcısının Microsoft Teams’ e giriş yaparken kullandığı mail adresinin de dışarı aktarılan nesneler arasında olduğu ve net bir şekilde okunabildiği Şekil 5.18. User Credential/ Kullanıcı Maili Bilgisi görselinde görülmektedir.



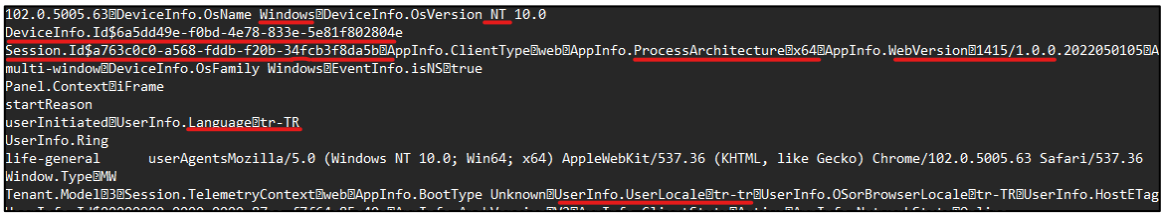
Şekil 5.18. User Credential/ Kullanıcı Maili Bilgisi



Şekil 5.19. Chat Üzerinden Gönderilen Görsele Ait Exif Bilgisi

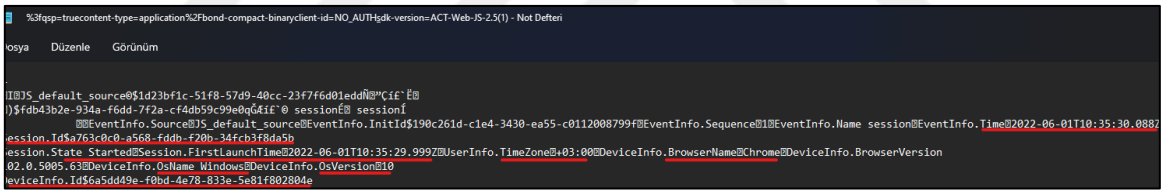
Şekil 5.19. Chat Üzerinden Gönderilen Görsele Ait Exif Bilgisi ekran alıntısında da chat üzerinden Test1 kullanıcısının gönderdiği bilgisayara “moon.png” olarak kaydedilen görselin exif bilgilerine rastlanmıştır. Exif bilgileri herhangi bir dosyaya ait küçük ama adli bilişim açısından delil niteliği barındırabilen bilgilerin yer aldığı alandır. Yine EXIF bilgileri arasında görselin çizerinin adına, görselin yapıldığı programın adına “Photoshop” ve programın versiyonunun “3.0” olduğuna rastlanmıştır. Ayrıca görselin isminin “Zodiac Constalletions Circle” olduğuna ve ne tür bir çizim

olduğuna dair "Vector hand illustration" bilgisine de rastlanmıştır. Görselin alındığı web sitenin ismi de açık bir şekilde görülmektedir.



Şekil 5.20. Cihaz ID, Oturum Id, Mimari ve Dil Bilgileri

Dışa aktarılan "%3fqsp=true&content-type=application%2Fbond-compact-binary&client-id=NO_AUTH&sdk-version=ACT-Web-JS-2.5(2)" adlı dosyada Şekil 5.20. Cihaz ID, Oturum Id, Mimari ve Dil Bilgileri görselinde işaretlenerek gösterilen kısımda cihaza ait mimari bilgisinin x64 olduğu, kullanıcının lokasyonunun "tr" olduğu, kullanıcının kullandığı cihaza ait 8-4-4-4-12 formatında bir ID olduğu ve bu ID'nin DeviceInfo sınıfındaki "Id" değişkeni ile tutulduğu düşünülebilir.



Şekil 5.21. Oturum Başlatılma Zamanı, İşletim Sistemi Bilgileri, Zaman Damgası

Oturumun ne zaman başlatıldığı bilgisine ilişkin bir vakit damgası, oturum Id'si, kullanıcının içinde bulunduğu "Time.Zone" (UTC0+03:00), kullanıcının "Chrome" tarayıcını kullandığı ve tarayıcı versiyonunun "102.0.5005.63" olduğu bilgileri Şekil 5.21. Oturum Başlatılma Zamanı, İşletim Sistemi Bilgileri, Zaman Damgası görselinde de açıkça görülmektedir.

Dışa aktarılan nesneler incelenirken birçok kez kullanıcının mail adresine, kullandığı işletim sisteminin Windows ve işletim sistemi versiyonunun "10" olduğuna, oturum Id'sine, "DeviceInfo" olarak belirtilen, kullanıcının cihazına ait Id değerine, kullanıcının bulunduğu konuma ilişkin dil bilgisinin "tr" olduğu bilgisine, epoch ve normal zaman formatında farklı değişkenler ile tutulan zaman damgalarına rastlanılmıştır.

6. SONUÇLAR

Günümüz dünyasında her türlü suçun bilişim sistem ve araçları ile işlenebilmesi mümkün hâle gelmiştir. Bu durum göz önüne alındığında kâğıt delillerin yerini artık dijital deliller alabilmektedir. Dijital deliller ise yazıcı gibi cihazlardan gelişmiş, belleğe sahip makinelere kadar genişleyebilen bir yelpazede en küçük log tutabilen ve belleğe sahip her türlü cihazdan elde edilebilir.

Dijital delillerin elde edilebileceği alanların yazılımsal ve donanımsal anlamda ne kadar geniş ve çeşitli olduğu göz önünde bulundurulduğunda günümüzde uzaktan eğitim platformlarının sayısında her geçen gün yaşanan artış, kullanıcıya sunulan çeşitli yelpazeyle birlikte farklı platformlarda olası bilgisayar etkileşimli suçların sayısında yaşanabilecek artışı da beraberinde getirmektedir.

Bir vaka analizinin optimum verimle yapılması adli bilişim görevlisinin yeteneklerinin yanı sıra inceleme yapılacak platformlar hakkında, API'lerin nasıl çalıştığı, arka planda neler olduğu, hangi protokolleri kullandığı gibi bilgilere sahip olmasına da bağlıdır. Bu çalışmada Microsoft Teams ve Skype Web Client üzerinde yapılan çalışmalar sonucunda bu platformların ağ üzerinde kullanıcılara ve kullanıcıların cihazlarına ait birçok bilginin ağ trafiğinden ve uygulamaların cihaz üzerinde kullanıcıya ve cihaza ait verileri tuttuğu dizinlerden ulaşılabildiği anlaşılmıştır.

ÖNERİLER

Gerçekleştirilen bu çalışmanın kapsamı genişletilerek farklı üreticilere ait olan diğer uzaktan eğitim araçlarından Zoom, Discord, Cisco Webex ve Zoom gibi uygulamaların da incelenmesi yapılabilir.

Ayrıca Microsoft Teams ve Skype için incelemenin gerçekleştirildiği Web Client uygulamalarının yanı sıra gün geçtikçe mobil cihaz kullanımlarının artması dikkate alındığında Android ve iOS ortamlar için geliştirilen bazı uygulamaların kapsama dâhil edilmesi düşüncesi ortaya çıkabilir. Bu kapsamda yapılan inceleme sonucunda hangi veri yollarında hangi verilerin bulunabildiği ve bu verilerin adli bilişim incelemesi bağlamında yararlı olup olmadığı değerlendirilebilir. Microsoft Teams ve Skype açısından Windows masaüstü uygulamasının da incelemesi gerçekleştirilerek Windows işletim sistemi içerisinde ne tür kalıntıların ve izlerin olduğu detaylı şekilde araştırılabilir.

Masaüstü veya mobil cihazlara kurulu olan uzaktan eğitim aracı uygulamalarının araştırmasının yapıldığı durumlar da olabilir. Bu durumlarda masaüstü veya mobil cihazlarda kurulu olan Microsoft Teams ve Skype uygulamalarının yüklü olduğu cihazların internet erişimlerinin kontrollü bir şekilde sağlandığı öngörülür. Bu ortamlarda internet erişiminin sağlandığı switch portu üzerinde Port Mirroring yöntemi ile trafiğin kopyalanarak WireShark vb. uygulamalar ile incelenerek izlenmesi durumunda adli bilişim açısından yararlı olabilecek ne tür verilere erişimin mümkün olup olmadığı analiz edilebilir.

Gerekli yasal izinler alınarak yüksek sayılı kullanıcıya sahip olan gerçek canlı kurumsal yapılar üzerinde Teams Yönetim Merkezi ve Microsoft Uyumluluk Merkezi üzerinden elde edilen veriler araştırılarak hangi yararlı bilgilere kolaylıkla erişimin sağlanabildiği detaylandırılabilir.

Bir Teams istemcisi tarafından başka bir Teams istemcisine veya başka bir uygulama tarafından yapılan PSTN cihazına giden/bu cihazdan gelen tüm VoIP konuşmaları, Microsoft 365'te izlenerek Microsoft tarafından sağlanan hizmetlerden yararlanılarak adli analiz yapılabilir. Microsoft' un sunmuş olduğu SBC çözümü ile gerekli yönlendirmeler sonrasında VOIP görüşmelerinin ses kayıtlarına ulaşılıp ulaşılamayacağı incelenebilir. Ulaşılabilmesi durumunda ses dosyalarının türü ve ses kalitesi değerlendirilerek kişilerin ses özellikleri tanımlamaları ışığında bir adli inceleme süreci gerçekleştirilebilir. Sesli mesajların codec çözümlemeleri yapılarak daha verimli donelere ulaşılıp ulaşılamayacağı değerlendirilebilir.

KAYNAKLAR

[1] Y. Akyüz, *Türk eğitim tarihi*. Ankara: Ankara Üniversitesi, 1982.

[2] R. H. A. Al Lily, A. E., Ismail, A. F., Abunasser, F. M., & Alqahtani, "Distance education as a response to pandemics", *Technol. Soc.*, s. 63, 2020.

[3] and A. P. Wilson, Pamela P., Deborah Valentine, "Perceptions of new social work faculty about mentoring experiences.", *J. Soc. Work Educ.*, c. 38.2, ss. 317–332, 2002.

[4] N. Negroponte, "The digital revolution: Reasons for optimism", *Futurist*, sayı 29, s. 68, 1995.

[5] N. S. Akbal, E., Doğan, Ş., Tuncer, T., & Atalay, "Adli Bilişim Alanında Ağ Analizi", *dergipark.org.tr*, c. 8, sayı 2, ss. 582–594, 2019.

[6] K. Koenigsbauer, "Microsoft teams rolls out to office 365 customers worldwide", *Microsoft*, 2017. https://www.microsoft.com/en-us/microsoft-365/blog/2017/03/14/microsoft-teams-rolls-out-to-office-365-customers-worldwide/.

[7] G. Moore, M. G., & Kearsley, *Distance education: A systems view of online learning.* Cengage Learning, 2011.

[8] C. Zhang, W., Wang, Y., Yang, L., & Wang, "Suspending ClassesWithout Stopping Learning: China‟s Education Emergency Management Policy in the COVID-19 Outbreak", *J. Risk Financ. Manag.*, c. 13, sayı 55, ss. 1–6, 2020.

[9] D. W. Al, "Online and Remote Learning in Higher Education Institutes: A Necessity in light of COVID-19 Pandemic", *Can. Cent. Sci. Educ.*, c. 10, sayı 3, ss. 1–3, 2020.

[10] S.Dhawan, "Online learning: A panacea in the time of COVID-19 crisis", *J. Educ. Technol. Syst.*, c. 49, ss. 5–22, 2020.

[11] A. Korkmaz, Y., & Boyacı, "Adli bilişim açısından ses incelemeleri", *Fırat Üniversitesi Mühendislik Bilim. Derg.*, c. 30, sayı 1, ss. 329–343, 2018.

[12] T. Wright, "Teams hits 145 million daily active users", *Microsoft*, 2021. https://www.uctoday.com/collaboration/teams-hits-145-million-daily-active-users/.

[13] P. Zaveri, "Microsoft teams now has 75 million daily active users, adding 31 millionin just over a month", *Microsoft*, 2020. https://www.businessinsider.com/microsoft-teams-hits-75-million-daily-active-users-2020-4.

[14] M. Foley, "Microsoft Teams hits 250 million monthly active user milestone", *Microsoft*, 2022. https://www.zdnet.com/article/microsoft-teams-hits-250-million-monthly-active-user-milestone/.

[15] H. . Bowling, "A forensic analysis of microsoft teams", Purdue University, 2021.

[16] T. Henkoğlu, *Adli bilişim:Dijital delillerin elde edilmesi ve analizi*. Pusula, 2020.

[17] S. Mohammed, “An Introduction to digital crimes.”, *Int. J. Found. Comput. Sci. Technol.*, c. 5, ss. 13–24, 2015.

[18] F. B. K. Conlan, L. Baggili, “‘Anti-forensics: Furthering digital forensic science through a new extended, granular taxonom’”, *Digit. Investig.*, c. 18, ss. 66–75, 2016.

[19] S. Akbal, E. Dogan, “Forensics Image Acquisition Process of Digital Evidence”, *I. J. Comput. Netw. Inf. Secur.*, c. 5, ss. 1–8, 2018.

[20] M. Novak, “Improving the Collection of Digital EVİDENCE”, *Natl. Inst. Justice*, sayı 284, 2021.

[21] C. M. Whitcomb, “An Historical Perspective of Digital Evidence: A Forensic Scientist’s View”, *Int. J. Digit. Evid.*, c. 1, sayı 1, 2002.

[22] H. J. Whitman, M. E., & Mattord, *Principles of information security.* Cengage Learning, 2021.

[23] K. Sebetci, Ö., & Yayın, *Bilgi Teknolojileri ve Yönetim Bilişim Sistemleri*. Kodlab Yayın Dağıtım Yazılım Ltd. Şti., 2018.

[24] Ş. Vural, Y., & Sagiroglu, “Kurumsal bilgi güvenliği ve standartlari üzerine bir inceleme”, *Gazi Üniversitesi Mühendislik Mimar. Fakültesi Derg.*, sayı 23–2, 2008.

[25] M. Yılmaz, “Enformasyon ve Bilgi Kavramları bağlamında enformasyon yönetimi”, *Ankara Üniversitesi Dil ve Tar. Coğrafya Fakültesi Derg.*, sayı 49(1), 2017.

[26] K. C. V.M. Schönberg, *Büyük Veri - Yaşama, Çalışma ve Düşünme Şeklimizi Dönüştürecek Bir Devrim*. İstanbul: Paloma Yayınları, 2013.

[27] N. Takcı, H. , Baktıt, “Büyük Veri Yaklaşımıyla Birden Çok Bilgi Erişim Merkezinin Kolektif Kullanımı”, *Bilişim Teknol. Derg.*, c. 2, sayı 11, 2018.

[28] J. Volonino, L., Anzaldua, R., & Godwin, *Principles and Practices (Prentice Hall Security Series)*. 2006.

[29] J. G. Kruse II, W. G., & Heiser, *Computerforensics: incidentresponseessentials*. Pearson Education, 2001.

[30] A. Öğün, M. N. , Kaya, “Siber güvenliğin milli güvenlik açısından önemi ve alınacak tedbirler”, *J. Secur. Strateg.*, sayı 18, s. 18,145,181, 2013.

[31] M. Orta, “Bilişim suçlarında adli analiz”, Selçuk Üniversitesi, 2015.

[32] E. Casey, *Digital evidence and computer crime*. ABD/AP, 2004.

[33] S. L. Garfinkel, ““Digital forensics research: The next 10 years”, *Digit. Investig. 7*, s. 64, 2010.

[34] G. Muharrem, Ö. Z. E. N., & Özocak, “Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi”, *Ankara Barosu Derg.*, c. 1, 2015.

[35] J. Altschaffel, R., Kiltz, S., Dittmann, “From the Computer Incident Taxonomy to a Computer Forensic Examination Taxonomy”, 2009.

[36] N. A. Sgaras, C., Kechadi, M., & Le-Khac, “Forensics acquisition and analysis of instant messaging and VoIP applications”, *arXiv Prepr.*, sayı 1612.00204, ss. 188–199, 2016.

[37] Y. A. Al-Saleh, M. I., & Forihat, “Skype forensics in android devices.”, *nternational J. Comput. Appl.*, c. 78.7, 2013.

[38] Z. Yang, T. Y., Dehghantanha, A., Choo, K. K. R., & Muda, “Windows instant messaging app forensics: Facebook and Skype as case studies”, *PLoS One*, c. 11(3), sayı e0150300, 2016.

[39] R. Brewer, “Ransomware attacks: detection, prevention and cure”, *Netw. Secur.*, sayı 9, ss. 5–9.

[40] A. Maguire, D., Martinez, J., Payne, H., & Borys, “How microsoft teams uses memory - microsoft teams.”, *Microsoft*, 2020. https://docs.microsoft.com/%0Aen-us/microsoftteams/teams-memory-usage-perf.

[41] Microsoft, “Tur On Admin and User Audit”, *Microsoft*, 2022. https://docs.microsoft.com/en-us/microsoft-365/compliance/turn-audit-log-search-on-or-off?view=o365-worldwide.

ÖZGEÇMİŞ

Yunus Emre ÇOLAK

[redacted]