










Microsoft Teams ve Skype’ın Uzaktan Eğitim Araçları Olarak Adli Bilişim Açısından İncelenmesi

Tugce KELES^{1*} , Yunus Emre COLAK² , Nurcan ILHAN³ , Kubra YILDIRIM⁴ ,
Arif Metehan YILDIZ⁵ , Turker Tuncer⁶ , Sengul Dogan⁷ 

^{1,2,3,4,5,6,7}Adli Bilişim Mühendisliği Bölümü, Teknoloji Fakültesi, Fırat Üniversitesi, Elazığ, Türkiye.
¹keles@firat.edu.tr, ²yunusemrecolak@outlook.com, ³ilhannc@gmail.com, ⁴kubra.yildirim@firat.edu.tr,
⁵a.metehanyildiz@gmail.com, ⁶turkertuncer@firat.edu.tr, ⁷sdogan@firat.edu.tr

Geliş Tarihi: 01.03.2023
Kabul Tarihi: 20.05.2024

Düzeltilme Tarihi: 04.09.2023

doi: <https://doi.org/10.62520/fujece.1462073>
Araştırma Makalesi

Alıntı: T. Keleş, Y. E. Çolak, N. İlhan, K. Yıldırım, A. M. Yıldız, T. Tuncer ve Ş. Doğan, “Microsoft teams ve skype’ın uzaktan eğitim araçları olarak adli bilişim açısından incelenmesi”, Fırat Üni. Deny. ve Hes. Müh. Derg., vol. 3, no 2, pp. 204-215, Haziran 2024.

Öz








Günümüz toplumunda internet, teknolojinin yaygın kullanımı nedeniyle her yerde bulunan bir ihtiyaç haline geldi. Bu gereklilik geleneksel normları alt üst etmiş ve hayatın her alanını etkilemiştir. Teknolojinin etkilediği en önemli alanlardan biri de kuşkusuz eğitim sektörüdür. Nüfus oranı arttıkça eğitimin önemi ve gerekliliği de artmaktadır. Bu eğitim ihtiyacına karşılık olarak çağın koşullarına göre yeni eğitim modelleri ortaya çıkmaktadır. Bu yeni modellerin ortaya çıkmasına neden olan kritik faktörlerden biri de Mart 2020’de tüm dünyayı etkisi altına alan COVID-19 salgınıdır. Bu salgın sonucunda ülkeler eğitim ve öğretim alanında çeşitli yöntemleri benimsemiştir. Bazı ülkeler eğitim faaliyetlerine ara vermiş, bazıları ise süreci uzaktan eğitim yoluyla sürdürmüştür. Uzaktan eğitim, ağırlıklı olarak bilgi ve bilgi araçlarının aktif kullanımına dayanan bir öğretim yöntemidir. Uzaktan eğitim araçlarının yaygın kullanımı, bu hizmetlere doğrudan veya dolaylı olarak erişmeye çalışan kötü niyetli kişilerin dikkatini çekebilir. Bu çalışma, Microsoft Teams ve Skype tarafından depolanan trafik bilgilerinin veya ağ üzerinden gelen ve giden trafik bilgilerinin izole bir ortamda analiz edilmesiyle elde edilen veri ve bilgilerin sunulmasını amaçlamaktadır. Çalışma, Windows 10 işletim sistemi ve web client uygulamaları kurulu bilgisayarlarda gerçekleştirilmiştir. Bu çalışmanın öncelikli amaçlarından biri gelecekte uzaktan eğitim araçlarını araştırarak olan araştırmacılara yardımcı olmaktır.

Anahtar kelimeler: Uzaktan eğitim, Microsoft teams, Skype, Wireshark

*Yazışılan Yazar



Investigation of Microsoft Teams and Skype as Distance Education Tools in Terms of Digital Forensics

Tugce KELES^{1*} , Yunus Emre COLAK² , Nurcan ILHAN³ , Kubra YILDIRIM⁴ ,
Arif Metehan YILDIZ⁵ , Turker TUNCER⁶ , Sengul DOGAN⁷ 

^{1,2,3,4,5,6,7}Department of Digital Forensics Engineering, College of Technology, Firat University, Elazig, Türkiye.

¹keles@firat.edu.tr, ²yunusemrecolak@outlook.com, ³ilhannrc@gmail.com, ⁴kubra.yildirim@firat.edu.tr,
⁵a.metehanyildiz@gmail.com, ⁶turkertuncer@firat.edu.tr, ⁷sdogan@firat.edu.tr

Received: 01.03.2023

Accepted: 20.05.2024

Revision: 04.09.2023

doi: <https://doi.org/10.62520/fujece.1462073>

Research Article

Citation: T. Keleş, Y. E. Çolak, N. İlhan, K. Yıldırım, A. M. Yıldız, T. Tuncer and Ş. Doğan,, “Investigation of microsoft teams and skype as distance education tools in terms of digital forensics”, Firat Univ. Jour.of Exper. and Comp. Eng., vol. 3, no 2, pp. 204-215, June 2024.

Abstract

In today's society, the internet has become a ubiquitous necessity due to the widespread use of technology. This necessity has disrupted traditional norms and has affected all aspects of life. Undoubtedly, the education sector is one of the most significant areas affected by technology. As the population rate increases, the importance and necessity of education also increase. In response to this need for education, new educational models emerge based on the contemporary conditions. One of the critical factors that lead to the emergence of these new models is the COVID-19 outbreak that affected the entire world in March 2020. As a result of this epidemic, countries have adopted various methods in the field of education and training. Some countries suspended their educational activities, while others have continued the process through distance education. Distance education is a teaching method that relies heavily on the active use of information and information tools. The extensive use of distance education tools can attract the attention of malicious individuals who may seek to access these services directly or indirectly. This study aims to present the data and information obtained from analyzing the traffic information stored by Microsoft Teams and Skype or incoming and outgoing traffic information over the network in an isolated environment. The study was conducted on computers with the Windows 10 operating system and web client applications installed. One of the primary goals of this study is to assist researchers who will study distance education tools in the future.

Keywords: Distance Eeducation, Microsoft teams, Skype, Wireshark

*Corresponding author

1. Introduction

The growth of societies is significantly influenced by education, making it a key element. The accessibility of education to individuals within a society and the value that education provides are directly correlated with the level of development of the educational system [1]. Throughout the history of humanity, education has served as an essential foundation for personal and societal development, with early education typically starting within the family unit [2].

Education is increasingly necessary and important, especially in the information society [3]. As the population grows, there is a greater demand for education. New educational models have arisen to meet the societal conditions and demands that make this process necessary. The COVID-19 epidemic prevalent in our era is one such demand that has significantly contributed to the birth of new models [4]. In March 2020, the first coronavirus case occurred in Turkiye, leading to several challenges, including disruptions and interruptions in schooling. In response to decisions made by the Ministry of National Education and The Council of Higher Education training was suspended for a period, and traditional face-to-face education was switched to distance education [5].

Distance education involves trainees and providers in various locations and at different times. This teaching strategy uses informatics and tools to facilitate learning [6]. Instruments used to implement these models include satellite TV channels, terrestrial TV channels, radio frequencies, computers, and the Internet. Online services such as shopping, job interviews, consultations, and educational services require internet use. However, frequent use of remote learning resources may attract malicious individuals who attempt to access user accounts. Hackers can use novel tactics and strategies to harm services used during distance education. In providing distance education services, procedures such as data preparation, analysis, and reporting may have evidentiary value in case of a crime [7]. Specialized forensic techniques, such as digital forensics, can access digital evidence by examining information systems and data storage devices [8].

Digital forensics provides different types of evidence depending on the crime committed. Data gathered by information system components are evidence in crimes involving computers [9]. Crime problems that once occurred in physical locations are now relocated to virtual environments as the use of distance education tools expands. Electronic evidence can be gathered from crimes committed with electronic tools such as computers, portable devices, network devices, and storage devices [10]. Distance learning systems and applications include Microsoft Teams, Microsoft Skype for Business, Zoom, Google Meet, Whatsapp, Slack, and Discord. Each of these systems and applications may require different procedures and techniques for analysis and processing in digital forensics. Bayındır et al. [11] used document analysis to present a descriptive analysis of crimes involving violations of the right to education and training during the 2019-2020 academic year. The issues of defamatory writing, insult, privacy, right to education, freedom and limits of communication were addressed and conclusions were drawn. The study is important to increase educational stakeholders' understanding of potential legal and administrative wrongdoings involving educational rights and freedoms in web-based applications. The findings reveal that teachers and students can misbehave by interfering with children's access to education, restricting their freedom of expression, violating their families' privacy, and using offensive language. Kamysbayeva et al. [12] conducted a study examining contemporary e-learning challenges, analysis of the learning process, problems related to online learning and opportunities offered by online learning. The study used a qualitative approach consisting of a two-stage procedure. The interview gave the participants a chance to talk about and compare their individual learning experiences, mostly those related to the COVID-19 problem. The findings of the study showed that developing soft skills requires more effort than developing hard skills, while at the same time identifying key elements of professional staff training that should be taken into account when creating a plan to integrate on-campus and online learning, as well as diversifying the curriculum using various pedagogical technologies and digital tools. Garcia and colleagues [13] endeavored to compare nine different aspects of nine video conferencing programs, to determine the most suitable option. In this paper, we conducted a comprehensive analysis utilizing questionnaires to gather data from two distinct samples at the national and international levels. The CDIO methodology was employed, which comprises four phases which are (1) conception, (2) design, (3) implementation, and (4) operation designed to tackle challenging issues. Our primary objective is to evaluate the best live-streaming alternative based on selected standards, with popular platforms such as

Jitsi, Zoom, Microsoft Teams, Google Meet, and Big Blue Button serving as examples. The evaluation of these platforms against predefined criteria is further enhanced by employing multi-criteria analysis. Our study provides an in-depth analysis of the various aspects of video conferencing programs, facilitating the identification of the best option based on the user's needs and preferences. Mahr and colleagues [14] investigate the Zoom video conferencing application through a primary disk, network, and memory forensic analyses. The researchers utilize network intercepts, forensic imaging of digital devices, and forensic memory to uncover users' critical information, including chat messages, names, e-mail addresses, passwords, and more, in plain text or encrypted/encoded formats. The findings reveal the app's vulnerability to digital forensic investigations, allowing for the retrieval of sensitive data. The authors also delve into the fascinating anti-forensic strategies the Zoom application employs when contacts are removed from the contact list, highlighting the app's efforts to conceal user information. Al-Saleh and colleagues [15] aimed to investigate the artifacts generated by Skype, one of the most popular VoIP applications, during calls and chats on Android devices. They conducted a thorough analysis of the RAM and NAND flash memories under various conditions and durations. Their findings demonstrate that while Skype offers secure internet communication, artifacts of calls and chats can be detected on the device. Remarkably, this study is the first to investigate Skype on Android devices, making it an important contribution to the field of digital forensics. Paligu et al. [16] conducted a meticulous investigation into the artifacts produced by Microsoft Teams and stored in the IndexedDB. The research team executed a single-case pretest-posttest quasi-experiment to establish artifacts in the Microsoft Teams repository and observed that these artifacts could be extracted without requiring user credentials, a phenomenon that gives rise to potential security issues. The researchers employed signature models to ascertain the relevance of the extracted artifacts and presented the findings in a conventional database format featuring related queries and grouping by relevance. They also utilized time frame analysis to scrutinize the material, rendering it appropriate for fellow researchers. The study's findings indicate that the artifacts contained in Microsoft Teams IndexedDB harbor the vast potential for digital investigations since they facilitate the extraction of private chat messages, voice messages, and team extensions, among other data. The cybersecurity company McAfee published a blog post titled "Top 10 Microsoft Teams Security Threats" where they identified some of the major security risks associated with Microsoft Teams [6]. The study used the McAfee MVISION Cloud and analyzed data from over 40 million users worldwide. The research found ten significant security issues with Microsoft Teams, including the possibility of malware uploads, data loss from file sharing, and guest users who may accidentally join calls with confidential information. Bowling [17] tested the app on both the Windows 10 operating system and mobile operating systems such as iOS and Android. Key features of Teams, including messaging, file sharing, video conferencing and other features, were tested in a closed environment. Both automated forensic techniques and manual analysis were used to examine these devices. Cellebrite UFED and Magnet AXIOM were used for mobile and Windows devices, respectively. The majority of the artifacts on all three devices were obtained, at least in part, through manual or non-automated interrogation. In their study, many of the objects discovered through manual examination could not be recovered by the forensic tools used. Iqbal et al. [18] undertook a digital forensic examination of Google Meet, a task that entailed the probing of the platform's efficacy on sundry browsers and operating systems, including but not limited to Windows 10 and Linux, Mozilla Firefox, Google Chrome, and Microsoft Edge. The research team, in the course of the study, collected artifacts or traces of possible evidence from the client's computer, including data sourced from the Random Access Memory (RAM) and the browser. These artifacts included many data points, ranging from meetings, conversations, e-mails, profile pictures, browsing history, downloads, bookmarks, cache, and cookies. The team also sought to scrutinize the effects of RAM size on the persistence and form of the extracted memory artifacts, a feat achieved by developing an extraction tool designed to automate the process. The study, in its full magnitude, seeks to underscore the precarious nature of user data protection, even with several privacy and security measures in place. Yang et al. [19] present the results of a forensic analysis of two well-known Windows Store instant messaging applications (IMs), Facebook and Skype. Installing, uninstalling, logging in, logging out, discussing, sharing data, and other private IM operations for the analyzed programs constituted the study. The findings showed that the use of instant messaging applications from the Windows Store can leave evidence on the hard disk, memory dumps and network captures that may be important or valuable for an investigation.

In April 2021, Microsoft Teams had 145 million daily active users, a platform that can be used as a tool for distance learning. In June 2022, the company's CEO announced increased daily active users to more than 250 million [20].

The Microsoft Teams app is widely used, as evidenced by the rising number of daily active users. Even though it hasn't been the focus of any lawsuits yet, it might soon require forensic analysis as a case. Additionally, it may be assumed that the rate of use of white-collar workers is similarly high due to its institutional framework [17].

In this study, the effectiveness of distant learning resources for digital forensics was investigated. This study includes facts and information gleaned through a solitary examination of the inbound and outbound traffic records kept by Skype and Microsoft Teams. The results highlight these technologies' significance in modern digital forensics.

1.1. Objective and motivation

Distance education, as described in the literature, refers to learning activities not restricted by time or place. The COVID-19 pandemic has forced many countries to adapt their teaching processes to distance education, resulting in its widespread acceptance among educational institutions. As we transition into the post-COVID era, distance education models are likely to remain prevalent, with many companies utilizing such systems to facilitate remote working environments. However, with the increasing digitization of education and work, electronic crimes are also becoming more common. Experts are required to handle electronic evidence obtained from devices such as computers, portable devices, network devices, and storage devices.

Popular distance education applications and platforms such as Microsoft Teams, Microsoft Skype for Business, Zoom, Google Meet, Whatsapp, Slack, and Discord are increasingly being used. However, examining and handling these platforms in terms of forensic informatics may require different methods and techniques. Microsoft Teams is an example of a platform that has seen significant growth in popularity. Despite only being released recently, in April 2021, it reached 145 million daily active users, nearly twice as many as the previous year. By June 2022, Satya Nadella, the CEO of Microsoft, announced that the number of daily active users had surpassed 250 million. Although it has not been the subject of any lawsuits to date, the increasing number of daily active users of the Microsoft Teams application suggests that it may require forensic examination in the future.

2. Analyzed Distance Education Tools

2.1. Microsoft Teams

Microsoft Teams is a comprehensive platform that combines chat, meetings, note-taking, and plugins, making it a crucial distance work and education tool. Its infrastructure can be integrated with fixed telephone (PSTN) services, and while Microsoft 365 services can be used, other PSTN services can also be preferred [21]. However, supporting services such as PSTN can broaden Microsoft Teams' attack surface, attracting malicious individuals. Furthermore, Microsoft Teams features can be enriched with numerous add-ons, some developed by Microsoft, while other companies or individuals create others. Microsoft Teams benefits from three primary categories of services available on computers and mobile devices: meeting needs, real-time communication needs, and other services customized with applications [22].

In meeting scenarios, Microsoft Sharepoint and Microsoft OneDrive enable users to collaborate on content and files, and store files with version numbers. Integration with Microsoft Exchange simplifies sending mail to calendar-enabled channels, assigning tasks, and availability notifications. Microsoft Teams also allows up to 10,000 people to attend live events simultaneously. Its text-to-text translation feature can translate speeches into different languages with the help of artificial intelligence integration. However, Turkish to text translation is currently not supported [21].

Regarding real-time communication, Microsoft Teams employs VOIP technology to enable simultaneous online voice, video, or data-sharing communication between internal and external users. With the help of applications, Microsoft Teams enables capacity building according to various needs. These applications can be produced by Microsoft or created by other companies, and there are hundreds of them available [23].

Microsoft Teams can be reviewed through the management center on corporate platforms. In accordance with the working logic of Microsoft Teams, the entire communication center rotates over the server. The examinations made on this corporate management center provide very productive information. As a result of a two-way dialogue within the organization, a lot of information is available, such as messages sent by users to each other, in-channel conversations, last activity time, operating system type of device used by users, etc. [23].

In some cases, in-house users can also communicate with external Skype users in line with the organizational settings. However, the data obtained from this management panel may be limited since the relevant user is outside, and communication is performed via Skype. In such cases, it may be necessary to analyze the traffic with network listening and different analysis methods of computer content with the installation of the SCB server. In this context, Windows applications usually store their own data in the AppData directory [24]. This AppData directory is usually located at C:\Users\\AppData\Roaming. The username in the path address differs depending on the current user. Although the AppData path may vary in Windows versions, it can be pointed to with the %AppData% variable. For example, the Teams AppData folder is located in the C:\Users\\AppData\Roaming\Microsoft\Teams folder path. The Cache folder in the Teams AppData folder contains the Chromium Cache format files belonging to Teams. The fact that the files are in chromium format shows that the Microsoft Teams desktop application was developed with the open source electron [16]. This is also similar to the format of the Google Chrome app. Therefore, the CromeCashView application is very easy to examine the cache folder of Microsoft Teams.

2.2. Skype

Skype is a widely used communication application that has been available since 2003. It enables users to make free one-to-one video or voice calls, group calls, send instant messages, and share files over the internet [25]. Previous studies have shown that useful data can be retrieved from Skype in iOS and Android operating systems [15]. Additionally, research has been conducted on Skype for Windows desktop environments and Microsoft's enterprise solution, Skype for Business [19].

Although Skype, Skype for Business, and Microsoft Teams are separate applications, the research results on where and how these applications stored data in the past can give an idea to our work.

3. Investigation of Microsoft Teams and Skype Distance Education Tools in Terms of Digital Forensics

This section explains the hardware and software materials used in the examination of Microsoft Teams and Skype Distance Education tools and the examination methods of these tools. Each application is presented within the framework of the method used uniquely. The hardware and software materials used in the applications are listed in Table 1.

Table 1. Hardware and software materials used in applications

Hardware Materials	Software Materials
1 Dell brand 7300 model laptop computer with Windows 10 20H2 version operating system, x64 bit architecture, 512 GB disk capacity and 32 GB RAM	1 Windows Operating System 1 VMware Workstation 16 Virtualization Solution 2 virtual computers with 2 GB RAM, 2 Virtual Processors, 50 GB Storage Space, Network Interface with NAT, Windows 10 21H2 x64 Operating System 2 Microsoft Teams Desktops with App Ver:1.5.00.11163 2 Microsoft Skype Web Applications 1 Chrome Cache Viewer Application 1 Skype Application 1 Fiddler Application 1 WireShark Application 1 Teams Admin Account 2 Independent User E-mail Accounts 1 Enterprise Office 365 and Office 365 E1 License

3.1. Extracting user data through network analysis of skype

In the first step, we defined the "Environment Variables" on the Windows 10 client to allow for the decryption of encrypted traffic before recording the network traffic of the Skype Web Client while it was running on the Chrome browser. This process involved running "sysdm.cpl" from regedit and creating a new environment variable named "SSLKEYLOGFILE" in the "Environment Variables" section. Once Wireshark was installed on the target computers, we initiated network recording on both user computers and performed user logins on the Skype Web application using the address <https://www.skype.com/tr/features/skype-web/>. We used usernames such as "test1forensic," "test2forensic," "test1," and "test2" to identify e-mail addresses and passwords that could be obtained by searching and analyzing network records.

After successfully logging in, we initiated a message chat between test1 and test2 users, utilizing various multimedia features such as sending pictures, emojis, and GIFs and adding reactions. A "Voice Call" was made between the same users that lasted for 25 seconds, and a "Video Search" was performed to examine all features while analyzing the network recording. During the "Video Call," the camera and microphone were turned on, and audio and visual data were streamed on the network.

Once we finished using the "Message Chat," "Voice Call," and "Video Call" features, we stopped network recording via Wireshark and saved the captured data for further analysis.

3.2. Extracting user data through network analysis of microsoft teams

In the initial phase, the "Environment Variables" were defined on the Windows 10 client to enable the decryption of encrypted traffic before network registration on the Microsoft Teams Web Client, which runs on the Chrome browser. This was accomplished by launching "sysdm.cpl" from regedit and setting up a new environment variable named "SSLKEYLOGFILE" within "Environment Variables". Subsequently, Wireshark was installed on the relevant machines, and network recording was commenced on both user computers. The Microsoft Teams Web application was accessed via the address <https://www.microsoft.com/tr-tr/microsoft-teams/log-in>, and user logins were performed using the usernames "test1forensic", "test2forensic", "test1", "test2", "forensic1", and "forensic2". The aim was to extract e-mail addresses and passwords through an analysis of the network records. Once a successful login was achieved, a message conversation was initiated between users "test1" and "test2", and an array of multimedia features, such as sending pictures, emojis, GIFs, and adding reactions, were employed. After the message exchange, a "Voice Call" was conducted, and data transmission continued over the network for a duration of one minute and 25 seconds.

4. Results and Findings

After the operations were completed, the network recording obtained via Wireshark was analyzed using specific filters and search queries. Firstly, the "HTTP" filter was applied in Wireshark to view the received HTTP packets. Then, the received HTTP objects were exported and subjected to further analysis.

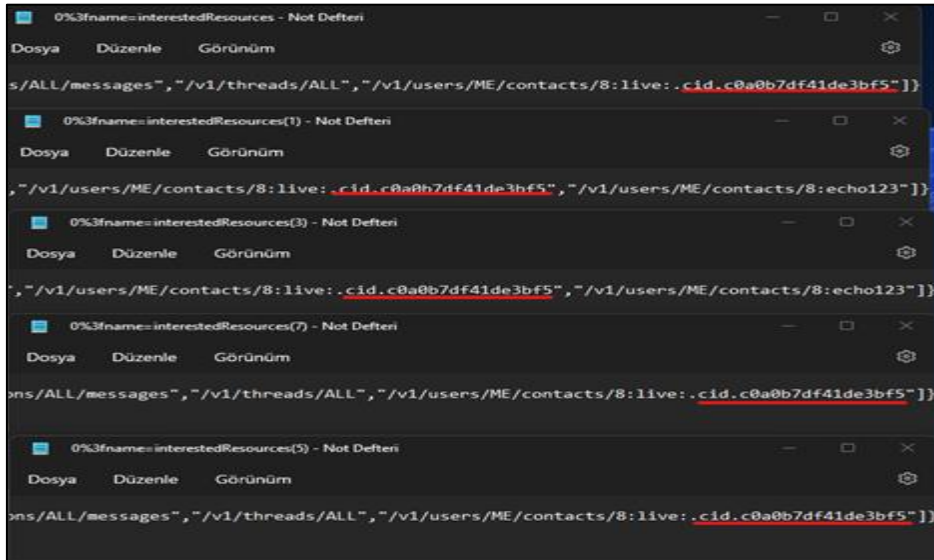


Figure 1. CID Values in Exported Files

Figure 1 clearly indicated that the exported file named "0%3fname=interestedResources" shared an identical caller identifier value (cid) with eight other files that had similar names.

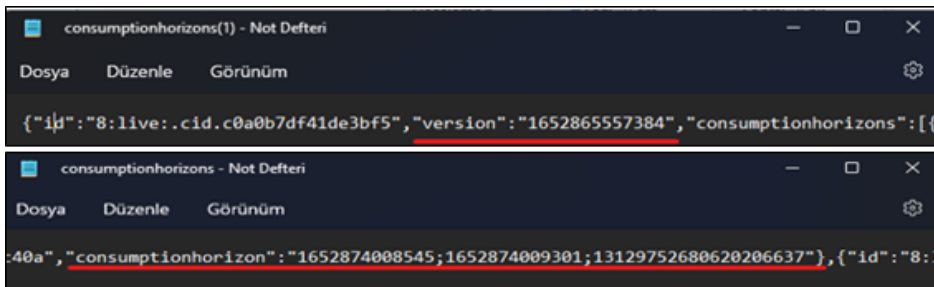


Figure 2. Timestamps of Received and Read Statuses

Figure 2 presented clear evidence that the file named "consumptionhorizons" contained timestamps of the received/read statuses. Moreover, the images/images that were exchanged during the messaging process were represented as thumbnails in files named "imgpsh_thumbnail_sx", "imgpsh_thumbnail_sx(1)", and "imgpsh_thumbnail_sx(2)".



Figure 3. Exif information of the Image Sent via Chat

Figure 3 showed the exif information of the image saved as "moon.png" sent by Test1 user via chat. Exif information was the area where information about any file was small but could contain evidence in terms of digital forensics. As a result of examining the Exif information, the following details were obtained:

- Name of the person who created the image
- Name of the program used to draw the image
- The version of the program
- It was also found that the name of the image was "Zodiac Constallements Circle" and what kind of drawing it was ("Vector hand illustration"). The name of the website from which the image was taken was also clearly visible.

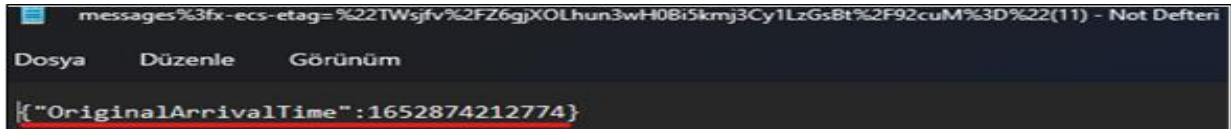
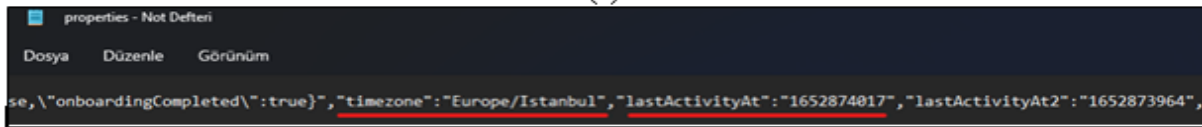


Figure 4. The arrival time of the message to the recipient

Messages sent were clear and concise in text form. The usernames of both the sender and receiver, "Test Forensic" and "Testt Forensic", were displayed along with the message ID and time. Upon examination, it was observed that all other messages were as clearly visible as the aforementioned ones. The file named "messages%3fx-ecs-etag=%22TWsjfv%2FZ6gjXOLhun3wH0Bi5kmj3Cy1LzGsBt%2F92cuM%3D%22(11)" displayed the arrival time of the message to the recipient in epoch format, as shown in the figure. Additionally, the caller identifier ID (cid) values of both users were stored and visible in video and voice calls.



(a)



(b)

Figure 5. CID and Timezone values (a) "cid" Values Retained in Voice and Video Calls, (b) Timezone and Last Active Time

In Figure 5, the "cid" values kept, the "timezones" of the users, and the last active times are marked. The method applied on Skype Web Client was also applied on Microsoft Teams Web Client, and as a result, the following findings were found;

While examining the exported objects, the first finding was "skypetoken". Since both applications belong to the same producer, it can be said that this is because they use the same infrastructure.

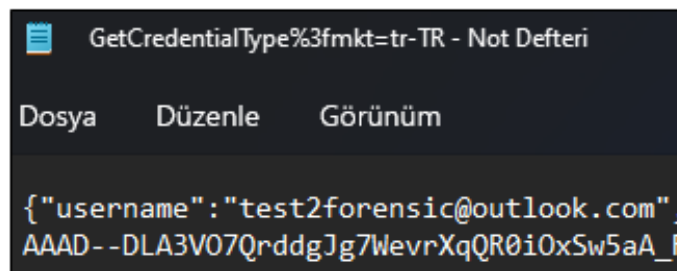


Figure 6. User Credential/ User Mail Information

It was seen in Figure 6 that the e-mail address used by the Test2 user when logging into Microsoft Teams was among the exported objects and could be read clearly.

```
102.0.5005.63@DeviceInfo.OsName Windows@DeviceInfo.OsVersion NT 10.0
DeviceInfo.Id$6a5dd49e-f0bd-4e78-833e-5e81f802804e
Session.Id$a763c0c0-a568-fddb-f20b-34fcb3f8da5b@AppInfo.ClientType@web@AppInfo.ProcessArchitecture@x64@AppInfo.WebVersion@1415/1.0.0.2022050105@
multi-window@DeviceInfo.OsFamily Windows@EventInfo.isNS@true
Panel.Context@iFrame
startReason
userInitiated@UserInfo.Language@tr-TR
UserInfo.Ring
UserInfo.Ring
life-general userAgentsMozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Window.Type@MW
Tenant.Mode@1@Session.TelemetryContext@web@AppInfo.BootType Unknown@UserInfo.UserLocale@tr-tr@UserInfo.OSorBrowserLocale@tr-TR@UserInfo.HostETag
```

Figure 7. Device ID, Session ID, Architecture and Language Information

In the exported file named "%3fqsp=true&content-type=application%2Fbond-compact-binary&client-id=NO_AUTH&sdk-version=ACT-Web-JS-2.5(2)", it is marked in Figure 7, and the architecture information of the device is x64., it could be inferred that the location of the user was "tr". There was an ID of the device used by the user in the format 8-4-4-4-12, and this ID is kept with the "Id" variable in the DeviceInfo class.

```
@EventInfo.Source@JS_default_source@EventInfo.InitId$190c261d-c1e4-3430- ea55-c0112008799f@EventInfo.Sequence@1@EventInfo.Name session@EventInfo.Time@2022-06-01T10:35:30.088Z
ession.Id$a763c0c0-a568-fddb-f20b-34fcb3f8da5b
ession.State Started@Session.FirstLaunchTime@2022-06-01T10:35:29.999Z@UserInfo.TimeZone@+03:00@DeviceInfo.BrowserName@Chrome@DeviceInfo.BrowserVersion
02.0.5005.63@DeviceInfo.OsName Windows@DeviceInfo.OsVersion@10
eviceInfo.Id$6a5dd49e-f0bd-4e78-833e-5e81f802804e
```

Figure 8. Session Start Time, Operating System Information, Timestamp

A timestamp of when the session was started, the session ID, the "Time.Zone" (UTC0+03:00) the user was in, the information that the user was using the "Chrome" browser and the browser version was "102.0.55005.63" Figure 8' was also clearly visible.

While examining the exported objects, the following information was obtained:

- The user's e-mail address,
- The user was running a Windows operating system, and the operating system version was "10",
- Session Id,
- The Id of the user's device, specified as "DeviceInfo",
- That the grammar of the user's location was "TR",
- Timestamps were kept in epoch and normal time format with different variables.

5. Discussions

We present a digital forensics analysis of Skype and Microsoft Teams distance education platforms. Our work includes a security analysis of both platforms, which makes us the first team to present such findings. In this paper, we discuss our analysis, findings, advantages, and limitations.

Our findings show that most distance education platforms do not use cryptographic protocols, relying solely on network security methods. This creates a significant security gap. Specifically, Skype's information security is relatively low. To acquire data from Skype and Microsoft Teams, we present two models.

Our research has several advantages. Firstly, we provide a digital forensics guide for these platforms. Secondly, we gather evidence from two distance education platforms using our model. Our primary objective is to present common digital investigation steps for distance platforms. However, since companies use different software development techniques and database structures, each platform requires different approaches. Our approach detects folder paths, which enables digital forensics analysis. Moreover, we provide the gathered information from Skype in Section 4.

The main limitation of this work is the use of only two platforms. Future work will involve investigating more distance education platforms such as Zoom and Google Meet. We plan to write a book on digital forensics analysis of distance education platforms.

6. Conclusions

The proliferation of distance education platforms has expanded the range of computer interactive crimes. Efficient case analysis requires the expertise of digital forensics professionals, who must possess knowledge of the platforms, including their APIs, background processes, and protocols.

The COVID-19 pandemic has led to a surge in the number of tools used in distance education systems, making them an essential part of people's lives. However, these platforms are vulnerable to computer interactive crimes. Digital forensics experts may encounter difficulties in investigating these crimes if they are not familiar with the components involved.

Our research offers a guide for digital forensics analysis of distance education platforms. The study employed Wireshark to record network traffic, filter it with predetermined keywords, and focus on objects that could serve as evidence. In this study, we conducted digital forensics analysis on Microsoft Teams and Skype Web Client. Information about users and devices can be obtained from network traffic and directories on these platforms.

In conclusion, digital forensics analysis of distance education tools is crucial in investigating potential computer interactive crimes. Digital forensics professionals can effectively collect evidence to assist in case analysis with the appropriate expertise and knowledge of the platforms involved.

7. Author Contribution Statement

Tugce KELES: Conceptualization, Methodology, Software, Investigation, Resources, Data Curation, Writing - Original Draft, Writing - Review & Editing. Yunus Emre COLAK: Conceptualization, Methodology, Investigation, Visualization, Writing - Original Draft, Writing - Review & Editing. Nurcan İLHAN: Methodology, Software, Resources, Data Curation. Kubra YILDIRIM: Software, Data Curation, Visualization. Sengul DOGAN: Validation, Formal Analysis, Investigation, Writing - Original Draft, Writing - Review & Editing, Supervision, Project Administration. Turker TUNCER: Validation, Formal Analysis, Investigation, Writing - Original Draft, Writing - Review & Editing, Supervision, Project Administration. Arif Metehan YILDIZ: Resources.

8. Ethics Committee Approval and Conflict of Interest

There is no need for an ethics committee approval in the prepared article. There is no conflict of interest with any person/institution in the prepared article.

9. References

- [1] Y. Akyüz, Türk eğitim tarihi. Ankara Üniv. Eğitim Bilimleri Fak., 1982.
- [2] L. Malaguzzi, C. Edwards, L. Gandini, and G. Forman, "History", Ideas and Basic Philosophy, 1993.
- [3] E. Alampay, "Beyond access to ICTs: Measuring capabilities in the information society", Inter.Jour. of Educ. and Devel. Using ICT, vol. 2, no. 3, pp. 4-22, 2006.
- [4] Y. Zhao and J. Watterston, "The changes we need: Education post COVID-19", Jour. of Educ. Chan., vol. 22, no. 1, pp. 3-12, 2021.
- [5] A. E. Al Lily, A. F. Ismail, F. M. Abunasser, and R. H. A. Alqahtani, "Distance education as a response to pandemics: Coronavirus and Arab culture", Techn. in Soci., vol. 63, p. 101317, 2020.
- [6] P. P. Wilson, D. Valentine, and A. Pereira, "Perceptions of new social work faculty about mentoring experiences", Jour. of Social Work Educ., vol. 38, no. 2, pp. 317-332, 2002.

- [7] K. Conlan, I. Baggili, and F. Breitingner, "Anti-forensics: furthering digital forensic science through a new extended, granular taxonomy", *Dig. Inves.*, vol. 18, pp. S66-S75, 2016.
- [8] A. Agarwal, M. Gupta, S. Gupta, and S. C. Gupta, "Systematic digital forensic investigation model", *Inter. Jour. of Comp. Sci. and Secur.(IJCSS)*, vol. 5, no. 1, pp. 118-131, 2011.
- [9] E. AkbaL, Ş. Doğan, T. Tuncer, and N. S. Atalay, "Adli bilişim alanında ağ analizi", *Bitlis Eren Üni. Fen Bil. Derg.*, vol. 8, no. 2, pp. 582-594, 2019.
- [10] Y. Korkmaz and A. Boyacı, "Adli bilişim açısından ses incelemeleri," *Fırat Üni. Müh. Bil. Derg.*, vol. 30, no. 1, pp. 329-343, 2018.
- [11] N. Bayindir and S. Levent, "An Awareness Study on Judicial/Administrative Crimes That May Occur During Web-Based Education Process," *Osmangazi Jour.of Educ. Res.*, vol. 8, no. 2, pp. 149-164.
- [12] A. Kamysbayeva, A. Koryakov, N. Garnova, S. Glushkov, and S. Klimenkova, "E-learning challenge studying the COVID-19 pandemic," *Inter. Jour. of Educ.Manag.*, vol. 35, no. 7, pp. 1492-1503, 2021.
- [13] N. O. García, M. D. Velásquez, C. T. Romero, J. O. Monedero, and O. Khalaf, "Remote academic platforms in times of a pandemic", *Inter. Jour. of Emer. Tech. in Learning (iJET)*, vol. 16, no. 21, pp. 121-131, 2021.
- [14] A. Mahr, M. Cichon, S. Mateo, C. Grajeda, and I. Baggili, "Zooming into the pandemic! A forensic analysis of the Zoom Application", *Fore. Sci. Intern.: Digital Inves.n*, vol. 36, p. 301107, 2021.
- [15] M. I. Al-Saleh and Y. A. Forihat, "Skype forensics in android devices," *Inter. Jour. of Comp. Appl.*, vol. 78, no. 7, 2013.
- [16] F. Paligu and C. Varol, "Microsoft Teams desktop application forensic investigations utilizing IndexedDB storage", *Jour. of Foren. Scie.*, vol. 67, no. 4, pp. 1513-1533, 2022.
- [17] H. R. Bowling, "A Forensic Analysis of Microsoft Teams", *Purdue University Graduate School*, 2021.
- [18] F. Iqbal, Z. Khalid, A. Marrington, B. Shah, and P. C. Hung, "Forensic investigation of Google Meet for memory and browser artifacts", *Foren. Scie. Inter.: Digital Inves.*, vol. 43, p. 301448, 2022.
- [19] T. Y. Yang, A. Dehghantanha, K.-K. R. Choo, and Z. Muda, "Windows instant messaging app forensics: Facebook and Skype as Case Studies", *PloS one*, vol. 11, no. 3, p. e0150300, 2016.
- [20] E. M. Osiakwan, "The KINGS of Africa's digital economy", *Digital Kenya*, pp. 55-92, 2017.
- [21] Z. Kristóf, "International trends of remote teaching ordered in light of the Coronavirus (COVID-19) and its most popular video conferencing applications that implement communication," *Central Europ. Jour. of Educ. Res.*, vol. 2, no. 2, pp. 84-92, 2020.
- [22] D. Pal and V. Vanijja, "Perceived usability evaluation of Microsoft Teams as an online learning platform during COVID-19 using system usability scale and technology acceptance model in India", *Child. and Youth Serv. Revi.*, vol. 119, p. 105535, 2020.
- [23] M. Nicoletti and M. Bernaschi, "Forensics for Microsoft teams", *arXiv preprint arXiv:2109.06097*, 2021.
- [24] R. Brewer, "Ransomware attacks: detection, prevention and cure", *Net. Secu.*, vol. 2016, no. 9, pp. 5-9, 2016.
- [25] V. Lo Iacono, P. Symonds, and D. H. Brown, "Skype as a tool for qualitative research interviews", *Sociol. Resea. Online*, vol. 21, no. 2, pp. 103-117, 2016.