Forensic Analysis of Webex on the iOS Platform

Jiaxuan Zhou and Umit Karabiyik(✉)

Purdue University, West Lafayette, IN 47907, USA
{zhou757,umit}@purdue.edu

Abstract. An increasing number of companies have adopted online telecommunication software for their office software pack, and Webex was one of the popular choices. With the surging usage of online telecommunication software, online meeting exploitation and disruptions cases also increased. However, there is limited research performed on online telecommunication software from the forensics perspective, and most are focused on Skype. Also, even though the iPhone's market share outperforms Android in the United States, the iOS system is under-researched. This paper fills the gap by performing a forensic analysis of Webex on the iOS platform, elucidating the structure of Webex in the iOS system, and displaying pertinent artifacts. The findings show that retrieving critical information in plain text from the application is possible. We retrieved data such as the username, phone number, device type, meeting session start time, meeting session attendee ID, etc. Also, we compared the evidence left from two types of accounts, basic and enterprise. The result shows that an enterprise account leaves more user data on the phone, a basic account keeps more device data. We used three tools, Cellebrite, Axiom, and DB Browser for SQLite, to validate the results. The result of the three tools all align.

Keywords: Mobile Forensics · Webex · Digital Forensics · iOS Forensics

1 Introduction

With the continuation of the COVID-19 pandemic, many organizations use a hybrid work model, which allows the employee to work from home most of the time. When employees stay at home, they rely on online telecommunication tools to attend meetings and communicate with their colleagues. Thus, teleconferencing applications became essential software for work. With the increase in the use of teleconferencing applications, the number of malicious attacks against teleconferencing applications also increased in the United States. FBI received multiple reports on the use of online meeting rooms and disruptions [19].

The idea of identifying forensically valuable data from video conferencing applications is not new. Studies began more than a decade ago, but most of

S. Goel et al. (Eds.): ICDF2C 2022, LNICST 508, pp. 84–96, 2023.
https://doi.org/10.1007/978-3-031-36574-4_5

the work focused on the Skype application [15]. Some research has been done on other popular software, such as Microsoft Teams and Zoom [10], but most studies are limited to covering only the Android and Windows platforms. However, in real life, there are many mobile applications and software on the market. The combination of mobile and software would decide where and how the evidence is preserved. Therefore, to help forensic practitioners deal with this issue, researchers should expand the scope from both the platform and the software perspectives.

This research paper fills the gap in forensic analysis for video conferencing software by investigating the digital evidence produced by the Webex application on the iOS platform. This information would help forensic practitioners solve an investigation involving the Webex application. Specifically, this research determines data discovered on iOS smartphones, such as installation data, user data, location information, contact database, and attachment files. This research is broken down into three phases. The first phase is the configuration of the device and the population of data. The mobile device used in this research is an iPhone 7 with iOS 14.4.1. The data population followed the Mobile Device Data Population Setup Guide published by NIST [16]. The second phase is acquisition. Cellebrite UFED 4PC with version 7.30.1.165 was used to acquire data from the iOS device. The final phase examined the images created using Magnet AXIOM Examine and Cellebrite Physical Analyzer. Both forensic analysis software are widely adopted in the digital forensics community. SQLite databases were verified using DB Browser for SQLite with version 3.12.1.

The rest of this paper is structured as follows. Section 2 discusses related work conducted for the Voice over Internet Protocol (VoIP) application from the forensic perspective. Section 3 details the acquisition and analysis techniques of this study. Section 4 presents the analysis findings and compares the result with other VoIP applications. Finally, Sect. 5 concludes the comments and future work.

2 Literature Review

Research related to the analysis of VoIP applications on iOS is precious for case investigation due to the time restriction nature. Therefore, we present the current literature on forensic analysis of VoIP applications.

Levinson et al. in [12] mentioned that the analysis of third-party applications could be difficult for forensic investigators if no prior study has been conducted. There is no standard that all companies need to follow when developing applications; therefore, how data are stored varies from application to application. Every application stores general information, such as username or email, but developers have the flexibility to decide the format and location. Previous work can provide guidance to law enforcement when investigating cases involving VoIP applications.

Although vendors store a lot of information on the server, cooperation could be tricky [11]. For example, the Tango software saves user personally identifiable information and non-personal identifiable information. However, Tango's

Privacy Policy gives the company immense flexibility for investigation cooperation. Furthermore, Tango does not share the retention period of stored data; the needed data can be deleted from the company side [11].

A Voice Over IP application is software that is installed on a computer or mobile device that can make a voice or video call over the Internet [7]. Webex belongs to the category of VoIP applications. Early work mainly focused on Skype, because it was one of the few VoIP software at the time. Later, researchers expanded the scope to Webex [9], Zoom [15], Microsoft Teams [10], Viber [20], and Tango [11].

Simon and Slay in [21] conducted an early research on VoIP. In 2006 VoIP was a novel technology that was not prevalent. So long ago, they wrote that VoIP's rise would bring a challenge to law enforcement. Unlike traditional phone calls, VoIP applications have strong encryption to control message and voice payload. This characteristic could make VoIP applications abused by criminals to communicate illegal activities. They defined the categories of retrievable data, which influenced many future researches.

Le-Khac et al. [11] analyzed the Tango application on iOS and Android devices. They were enlightened by Simon and Slay's work and defined the category of potential artifacts. Their paper [11] compared the artifacts available after three different extraction methods applied to the iOS device: logical extraction, file system extraction, and manual file system extraction. The result shows that the logical extraction contains no related data, the file system extraction has some data left, and the manual file system extraction retains most of the data. The research finding aligns with the study of [20].

In [9], Khalid et al. performed network analysis, memory analysis, and disk space analysis of the Webex application on the Windows operating system. The authors found that memory forensics provides ample amount of information; especially some encrypted artifacts on the static disk are plain text in memory. The username, email address, personal room number, and video address of the user were found. Even chat messages communicated and media shared were found with timestamps. Disk space analysis found that most databases are encrypted, but they found some artifacts in plain text, including profile photos, meeting metadata, and location information. The network artifacts offer information regarding client-server communication.

Mahr et al. in [15] analyzed the primary disk, memory, and network of the Zoom application on various operating systems such as Android, iOS, Windows, and macOS. They found that critical information could be retrieved from the device, such as chat messages, contact lists, exchanged media, and user profiles. Different devices show minor differences in terms of artifacts left. The research found that Zoom creates separate folders for every logged-in user. If no user logs in, then the *Zoommetting* and *Zoomus* databases are used to store information. Furthermore, Mahr et al. [15] warned that the Zoom company continues to patch vulnerabilities; when they started the research, they stopped updating. However, it is interesting that the Windows system automatically starts the update every time Zoom is initiated.

In [17], Nisticò et al. analyzed and compared thirteen real-time communication applications from the perspective of the network, which includes Skype, Google Meet, Microsoft Teams, Webex, and other communication applications. Webex employs normal RTP to stream media for network protocol and employs STUN to establish sessions. This shows similarities with Skype and Microsoft Teams. Webex does not provide peer-to-peer communication. Although peer-to-peer communication keeps communication latency low, the security level is also low. As an enterprise solution, Webex weighs security over speed. Their solution offers customers the option to install dedicated appliances.

Carpene in [3] approached the iTunes backup method to extract data from the mobile device and detailed the attainable data from the device. Skype and Facebook were included as two examples of application analysis. The author explained that *info.plist* is forensically valuable. It contains metadata on installed applications and can be used to check the list of applications that have been installed on the device. They found that the Skype folder is located under the *Library/Application Support* path. The data left behind includes limited contacts, limited call history, and limited chat history.

Sgaras et al. examined and analyzed four VoIP applications (WhatsApp, Skype, Viber, and Tango) for both Android and iOS in [20]. They concluded that the logical extraction of iOS does not produce any explicit data related to the four applications. However, with the extraction of the file system, they successfully recovered the installation data, traffic data, content data, user profile data, and contact database. The authors argue that manual file system analysis is still necessary even after the file system extraction, and it is highly possible that more valuable artifacts remain. In their research, they found more information on the four applications after manual analysis. Another contribution of the paper is the definition of the taxonomy of target artifacts; the purpose is to guild future forensic researches. They created eight categories of artifacts: installation data, traffic data, content data, user profile data, user authentication data, contact database, attachments, and location data.

There is several research done on Android phones, however, there is limited research done on iOS devices [1]. The original iOS device lacked many security features at first, so it was relatively easier to obtain forensic data from the devices [2]. However, with newer versions, iOS added additional security features in the software to prevent such data extractions along with the hardware to enable extra encryption of data. Such updates are a feature that disables USB data traffic if the phone has been locked for an hour [6]. Another update is the feature that the data on iOS can completely delete the data on the device if the password was incorrectly entered 10 times [13]. These security features make digital forensics harder to do on iOS devices [2].

The study in [18] performed research on iOS devices. The authors did a wide scale analysis of applications on Android and iOS devices and cross-validated the result using commercial and open source forensic software. More than 30 applications were analyzed. Popular choices of telecommunication application covered are Skype, Zoom, Houseparty, and Viber. The authors found that iOS takes a

snapshot for all applications that were moved to the background before. Snapshots are saved under the path `<AppUUID>/Library/SplashBoard/Snapshots/sceneID:<AppPackage>`. Also, among all applications, most have relevant artifacts left behind in the `/private/var/mobile/Containers` folder.

3 Methodology

This study for the Webex Meet application is broken down into three stages: data population, data extraction, and data analysis. Data population and data extraction followed the National Institute of Standards and Technology (NIST) guidelines [16], a guidebook published on mobile device forensics. The mobile device that was used in this research is an iPhone 7 running iOS 14.4.1.

The data population phase aims to simulate real life scenario and mimic real user behaviors. This phase is crucial because it determines what could be found later in the analysis phase. The iPhone 7 was jailbroken in the data extraction phase. This will ensure that researchers can access the full file system and maximize the amount of data that can be found.

Image acquisition was performed with Cellebrite UFED 4PC version 7.30.1.165 because it is known for its efficiency in data extraction and is widely accepted in the mobile forensics community [8]. As for the workstation, an HP ENVY laptop running Microsoft Windows 10 Home 64-bit Build 19042 with 32 GB RAM and an Intel(R) Core(TM) i7-10750H processor was used for extraction and analysis.

3.1 Data Population

This stage focuses on simulating real user behaviors and populating data in the mobile phone device. First, we reset the mobile device to factory settings. Then, a proton email was signed up and the proton email account was used to register a new iCloud account. The Webex Meet application was then downloaded from the Apple Store. Two types of Webex accounts were used: basic and enterprise. The new proton email address was used to register for a new Webex basic account, and an email with our institution's domain was used for the enterprise account. Lastly, we started to mimic user interactions. The user behaviors stimulated are the following:

- Add contact
- Delete contact
- Host meeting
- Attend meeting
- Record meeting
- Schedule meeting and tag other attendee(s)
- Send text messages, images, website URLs, and videos via chat
- Add profile picture
- Post question in Q&A board during meeting session

- Answer question in Q&A board during meeting session
- Share picture during meeting session
- Add annotation during meeting session
- Log in to Google Drive during meeting session
- Draw in white board during meeting session

3.2 Data Extraction

In this stage, the main objective is to acquire the phone image. We conducted an advanced logical acquisition that combines logical and file system extractions [4]. Cellebrite also took the role of jailbreaking the iPhone device, jailbreaking allows full access to the file system and extract the maximum amount of data.

3.3 Data Analysis

In this phase, we examined the acquired image and searched for artifacts. We examined the image using two forensic tools: Cellebrite Physical Analyzer with version 7.42.0.50 and Magnet Axiom Examine with version 4.9.1. For the database files in the image, we used DB Browser SQLite with version 3.12.1.

We first used the Cellebrite Physical Analyzer for analysis, mainly through the file system feature. Cellebrite is a popular tool that supports data extraction on various devices. Cellebrite does not proprietary the image, which allows investigators and researchers to have the freedom to load the image created by Cellebrite into many different forensic analysis tools [14]. The UFED extension image file was successfully loaded into the AXIOM Process for case generation. After the case was generated, AXIOM Examine was launched to analyze the image. Most artifacts found by both software were identical. Some files with *db* extension files could not be properly loaded. These database files were later loaded into the DB Browser SQLite for cross-validation.

4 Results and Findings

This section presents the findings of the study and explains the findings in detail. A summary of the findings is organized in Table 1, and all screenshots are presented subsequently in the rest of this section. The artifacts tell a story about the interactions the device had with Webex before, and practitioners could use the pieces found to complete the story of the case.

To analyze Webex, we first need to understand how the iOS device stores Webex data locally. The application status database records the file path for application source and application data, the path to the database is `/private/var/mobile/Library/FrontBoard/applicationState.db`. In the directory of application source, it contains application bundle such as libraries and icons. These information has little forensic value. The path of application data is `/containers/Bundle/Application/<Webexfolder>`, which is the main directory that Webex used to store user generated data. Besides the two paths provided by the applicationState.db, the path `/mobile/Containers/Shared/<Webex>` also contains forensically valuable data of Webex.

Table 1. List of Behaviors and Recovered Artifacts

Behavior	Artifacts Recovered
Add contact	No
Delete contact	No
Host meeting	Yes
Attend meeting	Yes
Record meeting	No
Schedule meeting and tag other attendee(s)	Yes
Send text messages, images, website URLs, and videos via chat	No
Add profile picture	Yes
Post question in Q&A board during meeting session	No
Answer question in Q&A board during meeting session	No
Share picture during meeting session	No
Add annotation during meeting session	Partial
Log in to Google Drive during meeting session	No
Draw in white board during meeting session	Partial

4.1 Application Information

Identifying the target application in the device is essential in the initial stages, as these findings lead to the subsequent investigation. That is why the path `/private/var/mobile/Library/ApplicationSupport/com.apple.remotemanagementd/RMAdminStore-Local.sqlite` was searched. This database contains application usage information such as the installed application name, start time, and total active time. Investigators could use this database and its information to determine whether the target application is installed, how long the target application was used, what time the target application was used, etc.

4.2 User Data

User information was recovered from the path `/private/var/mobile/Containers/Data/Application/72DAA48E-576A-427B-9BB3-DEC25487AFEC/SystemData/com.apple.SafariViewService/Library/WebKit/WebsiteData/https\_cart.webex.com\_0.localstorage-wal`. The file recorded the user's timezone as shown in Fig. 1. The location of the user could be narrowed down using the timezone information. Additionally, this file also records the Internet provider and the ASN information. Both information can be used to estimate which region the user is in.

The path `/private/var/mobile/Containers/Data/Application/72DAA48E-576A-427B-9BB3-DEC25487AFEC/Library/Caches/Datas/Avatars` contains the avatars of the users that were uploaded. Each user has its own encrypted folder. Inside the folder, the avatar has 5 copies in different sizes.

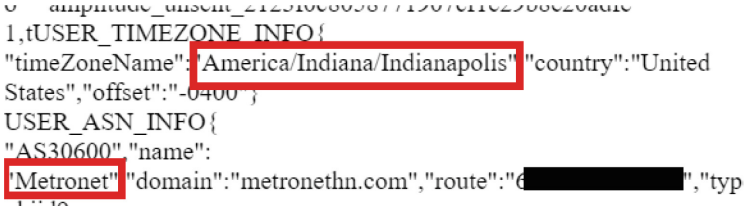

Fig. 1. Recovered timezone and ASN of an account

As Webex defines itself as a product for business meetings, security was an important factor when the application was developed [5]. The company can limit the sign-in request to Webex to accounts only from a predefined list of domains. The sign-in request from other domains can be blocked. Information about the predefined domain list could be found in `/private/var/mobile/Containers/Data/Application/72DAA48E-576A-427B-9BB3-DEC25487AFEC/Library/Caches/com.apple.WebKit.Networking/HSTS.plist`. The basic account has a domain name of "idbroker-b-us.webex.com" and the institution account had a domain of "purdue-student.webex.com" as shown in Fig. 2.

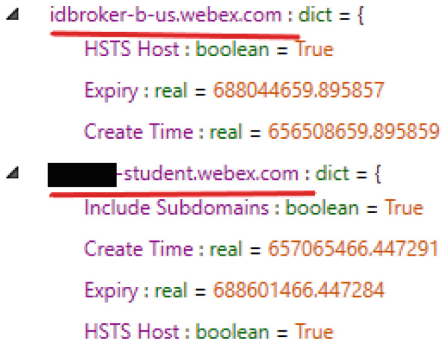

Fig. 2. List of account domains recovered

Many of the user information for the institution account is located in the path `/var/mobile/Containers/Data/Application/72DAA48E-576A-427B-9BB3-DEC25487AFEC/Library/Caches/com.webex.meeting/Cache.db`. Using the information saved in this database, a professional profile can be drawn, as it contains many user information. In the *cfurl_cache_receiver* table of the database, many valuable information about the account owner's were found. The details of the account user information, as well as the employer information, are saved inside. The data are of the form of a JSON object, as shown in Fig. 3.

It is worth noting that the employer's name is displayed here. This name is the name of the account owner registered in the company. An experiment

Fig. 3. Information recovered about enterprise account

was conducted to see if the real name can be deleted. The display name of the institution account in Webex was changed. However, the real name of the account still remained there. The basic account recorded more information about the device on which the Webex was installed compared to the institution account. The type of device, device name, device model and system version were recorded in the database as shown in Fig. 4.

4.3 Meeting Data

The list of all previous meetings was stored in the file path `/private/var/mobile/Containers/Data/Application/72DAA48E-576A-427B-9BB3-DEC25487AFEC/Library/Caches/com.webex.meeting/Cache.db-wal`. For each meeting, the start time, local IP address, user type, attendeeID, and browser type could be found on the device as shown in Fig. 5. An interesting finding was that using the institution account, hosted meetings were recorded on the phone as call events. The file In the file `/private/var/mobile/Containers/Shared/AppGroup/049A2701-EE6F-48E2-A24E-67B69C93FA93/Library/Caches/Logs/current\_log.txt` provides some details about the initial setup of the video call, such as if the video was enabled when the video initiated, and when the video was turned on. An example of metadata for video initialization is shown in Fig. 6.

As for scheduled meetings, the Webex application interacted with the Calendar application and wrote down the scheduled meeting as a calendar event. The calendar event contains the start time, end time, meeting URL, attendees, and timezone of the scheduled meeting as shown in Fig. 7.

4.4 Interactions During Meeting Session

Few data about the interactions inside the meeting room was left in the device. No plain text of the conversation was found on the QA board. However, we were able to find that a data-proven annotation and a whiteboard were used during the meeting session. In the file `/private/var/mobile/Containers/Shared/`

```
{"url":"https://wdm-r.wbx2.com/wdm/api/v1/devices/254da7e0-5344-
    "webSocketUrl":"wss://mercury-connection-partition0-r.wbx2.c
    "deviceType":"WEBEX_IPHONE",
    "name":"Jane's iPhone",
    "model":"iPhone 7",
    "localizedModel":"iPhone",
    "systemName":"Webex@iOS",
    "systemVersion":"iOS(13.7)/Webex(41.10.1)",
    "capabilities":{"groupCallSupported":false,
        "localNotificationSupported":false,
        "deleteNotificationSupported":false,
        "sdpSupported":true,
        "isBackgroundCapable":false,
        "isNseFilterEnabled":false,
        "isApnsMissedCallPushSupported":false},
        "creationTime":"2021-10-26T09:05:19.373Z",
        "modificationTime":"2021-10-26T09:05:19.373Z",
        "deviceSettings":{},"deviceSettingsString":"{}",
            "showSupportText":false,
            "reportingSiteUrl":"",
            "reportingSiteDesc":"",
            "customerCompanyName":"Self Signup 20210920-2424",
```


Fig. 4. Information recovered about basic account


```
pd":"WebEx","v":{"extVal":{"appversio
n":"41.10.1"},"label":"first time","e
vent":"Connected Meeting","category":
"App"}"ver":"2.1.8"},{"t":"Info","ts
":"2021-10-26T08:08:21.950-0400""tid
":"952D3137-E85A-4684-AD3C-D4A6D5DB50
04_0_656942900","pd":"WebEx","v":{"ex
tVal":{"meetNumber":"1725308711","mee
tType":"MC","CMRVersion":"0","CMRFlag
":true,"userType":"host""nodeID":"16
781313","confID":"209233521448853622"
,"appversion":"41.10.1","SignInFlag":
true,"joinType":"return user","GID":"
551774567","siteID":"868262","siteNam
e":"https:\/\/[redacted]-student.webex.co
m\/[redacted]-student","attendeeID":"7572
73""TrainVersion":"41.10.7.14","PMRF
lag":true},"userID":"584986127","cate
gory":"Conference","version":"Webex\/
```


Fig. 5. Various recovered metadata for video meeting

`AppGroup/049A2701-EE6F-48E2-A24E-67B69C93FA93/Library/Caches/Logs/current\_log.txt`, the Webex logs were recorded. The log message was written when the annotation function, shown in Fig. 8, or the whiteboard function was enabled (see Fig. 9).

```
true
2021-10-26T09:25:53.584Z <Detail> [0x10ccd9840]
VideoStreamContentViewController.swift:720
updateVideoLayerIfNecessary():stream [local]: canRender = true, hasVideo
= true isVideoAdded = nil
2021-10-26T09:25:53.584Z <Detail> [0x10ccd9840]
VideoStreamContentViewController.swift:726
```

Fig. 6. Various recovered metadata for video initialization

Summary	**Meeting**
Start Date/Time	**10/27/2021 11:30:00 PM**
End Date/Time	**10/28/2021 12:30:00 AM**
Notes	**Join Cisco Webex meeting** **https://meet154.webex.com/m/cad5093e-fd99-496d-9bb7-d0fd652a698f** **Join by Video system** **sip:25540765144@meet154.webex.com** **Join using Microsoft Skype for Business** **sip:25540765144.meet154@lync.webex.com**
Calendar	**Home**
Attendees	**Jane Doe (mailto:janedoecnit55700@protonmail.com), Jane Doe (mailto:janedoecnit55700@protonmail.com), [redacted] (mailto:[redacted])**
Timezone	**America/Indiana/Indianapolis**

Fig. 7. Recovered scheduled meeting invitation

```
userapps-data-migration-enabled:true
dev-portal-search:true
ios-board-annotation-shared-screen:true
web-pmr-contact-card:true
ios-cobranding-enabled-v2:true
mobile-cucm-callforward-enabled:true
```

Fig. 8. Recovered log data for annotation

```
mobile-cucm-callforward-enabled:true
desktop-whiteboard-snapshot-format-pdf:true
atlas-control-hub-refresh-notification--spark-
```

Fig. 9. Recovered log data for whiteboard

5 Conclusion and Future Work

With the continuity of the COVID pandemic, videoconferencing software became an integral part of people's lives and is used as a basic tool by everyone from kids to seniors. Webex is one of the video conferencing software which is favored by educational institutions. However, to the best of our knowledge, no published paper has focused on the forensic analysis of Webex on mobile platforms. This research fills the gap by conducting a forensic analysis of the Webex software on the iOS platform. The identified artifacts could assist practitioners when performing investigation. The results indicate that much user-related information, meeting information, and software information could be retrieved. The institution account contains additional professional information, such as title, phone number, name, and employer. The basic account contains additional device-related information, such as the device type, device name, and device model. However, not all previous operations could be discovered. For events such as recorded meetings, QA board interaction, video call chats, and video call media sharing, no data were found locally.

Future extensions of this work could include other platforms of Webex, including Android, Windows, and MacOS. Another direction could be conducting an investigation of the memory and network. This may provide additional valuable artifacts. Furthermore, a comparison of different versions of Webex is worth looking into. With rapid patching and update, the structure and evidence presented in this paper may be different from other Webex versions.

References

1. Azfar, A., Choo, K.-K.R., Liu, L.: Android mobile VoIP apps: a survey and examination of their security and privacy. Electron. Commer. Res. **16**(1), 73–111 (2015). https://doi.org/10.1007/s10660-015-9208-1
2. Bullock, D., Aliyu, A., Maglaras, L., Ferrag, M.A.: Security and privacy challenges in the field of iOS device forensics (2020). https://doi.org/10.3934/ms.2019.x.xxx
3. Carpene, C.: Looking to iPhone backup files for evidence extraction (2011)
4. Cellebrite: Supporting new extraction methods and devices (2019)
5. Center, W.H.: Configure a list of allowed domains to access WebEx while on your corporate network (2021)
6. Edge, C., Trouton, R.: The Evolution of Apple Device Management, pp. 1–54 (2020). https://doi.org/10.1007/978-1-4842-5388-5_1
7. Goode, B.: Voice over internet protocol (VoIP). Proc. IEEE **90**(9), 1495–1517 (2002). https://doi.org/10.1109/JPROC.2002.802005
8. Hutchinson, S., Shantaram, N., Karabiyik, U.: Forensic analysis of dating applications on Android and iOS devices. In: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 836–847 (2020). https://doi.org/10.1109/TrustCom50675.2020.00113
9. Khalid, Z., Iqbal, F., Kamoun, F., Hussain, M., Khan, L.A.: Forensic analysis of the Cisco WebEx application. In: 2021 5th Cyber Security in Networking Conference (CSNet), pp. 90–97 (2021). https://doi.org/10.1109/CSNet52717.2021.9614647

10. Kim, Y., Kwon, T.: On artifact analysis for user behaviors in collaboration tools-using differential forensics for distinct operating environments. J. Korea Inst. Inf. Secur. Cryptol. **31**(3), 353–363 (2021)
11. Le-Khac, N.A., Sgaras, C., Kechadi, T.: Forensic acquisition and analysis of Tango VoIP (2014)
12. Levinson, A., Stackpole, B., Johnson, D.: Third party application forensics on apple mobile devices. In: 2011 44th Hawaii International Conference on System Sciences, pp. 1–9 (2011). https://doi.org/10.1109/HICSS.2011.440
13. Lutes, K.D.: Challenges in mobile phone forensics (2008)
14. Magnet: Loading cellebrite images into magnet axiom (2021). https://www.magnetforensics.com/blog/loading-cellebrite-images-into-magnet-axiom/
15. Mahr, A., Cichon, M., Mateo, S., Grajeda, C., Baggili, I.: Zooming into the pandemic! A forensic analysis of the zoom application. Forensic Sci. Int.: Digit. Investig. **36**, 301107 (2021). https://doi.org/10.1016/j.fsidi.2021.301107
16. NIST: Mobile device data population setup guide (2016). https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/cftt-technical/mobile
17. Nisticò, A., Markudova, D., Trevisan, M., Meo, M., Carofiglio, G.: A comparative study of RTC applications. In: 2020 IEEE International Symposium on Multimedia (ISM), pp. 1–8 (2020). https://doi.org/10.1109/ISM.2020.00007
18. Salamh, F.E., Mirza, M.M., Hutchinson, S., Yoon, Y.H., Karabiyik, U.: What's on the horizon? An in-depth forensic analysis of android and iOS applications. IEEE Access **9**, 99421–99454 (2021). https://doi.org/10.1109/ACCESS.2021.3095562
19. Secara, I.A.: Zoombombing - the end-to-end fallacy. Netw. Secur. **2020**(8), 13–17 (2020). https://doi.org/10.1016/S1353-4858(20)30094-5
20. Sgaras, C., Kechadi, T., Le-Khac, N.A.: Forensics acquisition and analysis of instant messaging and VoIP applications (2014). https://doi.org/10.1007/978-3-319-20125-2_16
21. Simon, M., Slay, J.: Recovery of skype application activity data from physical memory. In: 2010 International Conference on Availability, Reliability and Security, pp. 283–288 (2010). https://doi.org/10.1109/ARES.2010.73