Forensic Analysis of Microsoft Teams: Investigating Memory, Disk and Network

Zainab Khalid[1](✉), Farkhund Iqbal[2], Khalil Al-Hussaeni[3], Aine MacDermott[4], and Mohammed Hussain[2]

[1] National University of Science and Technology (NUST), SEECS, Islamabad, Pakistan
zkhalid.msis18seecs@seecs.edu.pk
[2] College of Technological Innovation, Zayed University, Dubai, UAE
[3] Department of Computer Science, Rochester Institute of Technology, Dubai, UAE
[4] Liverpool John Moores University, Liverpool, UK

Abstract. Videoconferencing applications have seen a jump in their userbase owing to the COVID-19 pandemic. The security of these applications has certainly been a hot topic since millions of VoIP users' data is involved. However, research pertaining to VoIP forensics is still limited to Skype and Zoom. This paper presents a detailed forensic analysis of Microsoft Teams, one of the top 3 videoconferencing applications, in the areas of memory, disk-space and network forensics. Extracted artifacts include critical user data, such as emails, user account information, profile photos, exchanged (including deleted) messages, exchanged text/media files, timestamps and Advanced Encryption Standard encryption keys. The encrypted network traffic is investigated to reconstruct client-server connections involved in a Microsoft Teams meeting with IP addresses, timestamps and digital certificates. The conducted analysis demonstrates that, with strong security mechanisms in place, user data can still be extracted from a client's desktop. The artifacts also serve as digital evidence in the court of Law, in addition to providing forensic analysts a reference for cases involving Microsoft Teams.

Keywords: Artifacts · Digital forensics · Memory forensics · Microsoft Teams · Network forensics · Videoconferencing · VoIP

1 Introduction

Adaptation of videoconferencing applications in the wake of COVID-19 pandemic has proved to be an efficient alternative as businesses and schools continue to utilize them for meetings and online classes. This technology may be used well past the pandemic is over owing to the convenience, higher productivity levels reported by employees and reduced travel costs among other advantages [1]. The market value of Voice over Internet Protocol (VoIP) applications is estimated at $6.03 billion in 2021 [1]. Most prevalent of these applications include Zoom, Cisco WebEx, Microsoft Teams, Google Hangouts, BlueJeans and Adobe Connect according to a recent G2 report [2].

S. Paiva et al. (Eds.): SmartCity360° 2021, LNICST 442, pp. 583–601, 2022.
https://doi.org/10.1007/978-3-031-06371-8_37

Any application that connects to the internet is at risk. It is therefore important to consider the security and privacy risks posed by videoconferencing applications because they store and transmit data of millions of users. Malicious actors leverage the vulnerabilities present and exploit them to gain access to users' account/data to harass, abuse or bully them. *Zoom-bombing* is an example of intruders exploiting a vulnerability (Zoom's screen sharing feature) to hijack meetings to stream improper content or harass attendees [3]. Such vulnerabilities have since been patched; however, other persistent risks can be categorized into: software development risk, personal information loss, communication interception, unlawful access to confidential data and privacy violation [4]. Andrew Lewis, in his report, discusses how it is important to compare the security of a VoIP application compared to others but it is also important to analyze the risks of videoconferencing in terms of a broader digital platform [4].

WebEx, in 2019, was patched for critical vulnerabilities: CVE-2020-3419, CVE-2020-3441 and CVE-2020-3471, which would have allowed a hacker to obtain private user data without leaving a trace, therefore violating confidentiality and non-repudiation [5]. Houseparty was reported to have questionable privacy policies and collecting end-user information while Google Meet did not offer full encryption initially [6].

Evidently, there is a need to forensically analyze videoconferencing applications to extract artifacts that can *attribute malicious actions to guilty individuals*. These artifacts can therefore serve as digital evidence in criminal investigations. Microsoft Teams has experienced a surge in its userbase, with 145 million daily active users and 100+ million downloads on Google Play Store [7]. It is one of the top 3 videoconferencing applications in the market. This research work forensically analyzes the Microsoft Teams desktop application on a Windows virtual client machine to determine, carve and extract artifacts of potential evidential value from different locations on the client's desktop. These include memory, disk-space and network. To the best of our knowledge, this is the first forensic analysis of the Microsoft Teams desktop application.

1.1 Microsoft Teams Protocol Overview

VoIP applications, with their upward trends of demand and userbase, have been scrutinized for the security services they offer. Zoom initially faced backlash in this regard. However, with time, security practices such as: (1) media encryption, (2) session encryption, and (3) hashing for integrity and authentication etc. have been adopted and implemented in these applications. Microsoft Teams has particularly benefitted from Microsoft's mature security model [4]. Security services provided by Microsoft Teams' communication protocols are discussed below [8]:

- Transport Layer Security (TLS) is used for client-to-server signaling and Mutual Transport Layer Security (MTLS) is used to encrypt server-to-server messages.
- Media traffic is encrypted using Secure Real-time Transport Protocol (SRTP).
- Federal Information Processing Standard (FIPS) compliant algorithms are used for encryption key exchanges.
- Client-to-server authentication is achieved using Modern Authentication (MA) which is Microsoft's implementation of OAUTH 2.0. Multi-Factor Authentication (MFA) and conditional access are implemented using MA.

- User Datagram Protocol (UDP) 3478–3481 and Transmission Control Protocol (TCP) 443 over TLS are used by the client to request for audio visuals.
- Microsoft Teams stores files in *SharePoint* which is primarily a *cloud-based document management and storage system* developed by Microsoft. The files stored in SharePoint servers are protected by SharePoint encryption.

With strict encryption and authentication protocols being used for data in transit and at rest, our main goal in this research is to investigate what artifacts can be extracted from a client's desktop (memory, disk-space and network). The contributions of our research are as follows:

- We perform a detailed memory forensic analysis of Microsoft Teams to extract artifacts that are corroborated with artifacts from disk-space and network.
- We analyze the Windows Registry on disk-space to extract registry keys pertaining to Microsoft Teams.
- We present an in-depth network forensic analysis of Microsoft Teams' (encrypted) traffic.

The rest of this paper is structured as follows. Section 2 discusses research previously done in VoIP applications' forensic analysis and other similar Instant Messaging (IM)/social media applications. Section 3 presents the research methodology adopted and the experimental setup. Sections 4, 5 and 6 present the findings of memory forensics, disk-space forensics and network forensics for Microsoft Teams, respectively. Finally, Sect. 7 provides a summary of the contributions and discusses prospects of further research that can be performed in VoIP forensics.

2 Literature Review

Previous research in the domain of forensic analysis of videoconferencing applications is limited. Some of the most recent works in VoIP application forensics are discussed in this section.

Sgaras et al. [9] presented forensic analyses of some IM and VoIP applications namely WhatsApp, Viber, Skype and Tango on both Android and iOS platforms. They developed a taxonomy of the artifacts that can be extracted using logical and manual analyses.

Yang et al. [10] performed an in-depth forensic analysis of Facebook and Skype on a Windows 8.1 machine. Terrestrial artifacts such as installation information, log-in and log-off information, contact lists, conversations and transferred files were extracted from memory, disk-space and network traffic. The authors also observed that uninstalling the applications removed most artifacts from the file-system, but some installation data still remained on the disk; therefore, anti-forensics attempts by deleting data can be detected.

Tandel and Rughani [11] investigated the client artifacts that can be extracted from an Asterisk server during a (Zoiper) VoIP communication if the server is compromised. The authors used Encase to extract usernames, passwords, call records, access logs and error logs from the server.

Dargahi et al. [12] presented the analysis of forensically valuable remnants of mobile VoIP applications: Viber, Skype and WhatsApp messenger on an Android smartphone. They recovered artifacts such as messages, contact details, phone numbers, images and video files from logical images of a rooted Samsung Galaxy S3 GT-i9300 smartphone.

Mohemmed et al. [13] presented a packet level *forensic analyzer* for VoIP network traffic. The framework can identify and analyze the VoIP-SIP stream (which is the protocol used to initiate a VoIP communication session) and regenerate the VoIP-RTP stream (protocol used for data transfer) in order to trace malicious users involved in a conversation.

Recently, Nicoletti and Bernaschi [14] forensically analyzed Skype for Business with a focus on Skype's communication architecture, protocols and VoIP codec to extract artifacts. They presented case studies that elaborated the relevance of extracted artifacts in different investigative cases. They identified the Windows Registry, Event Viewer, client application folder and log files as sources of potential evidence in the presented case studies.

After the COVID-19 outbreak, the number of VoIP applications and their usage has surged but research regarding forensic analysis of the most recent and prevalent videoconferencing applications is still scarce. Zoom, however, has been analyzed in-depth by Mahr et al. [15]. The authors presented a detailed disk-space forensic analysis of Zoom on Windows and macOS desktops. Their research included an analysis of Android and iOS smartphones as well. Various databases in the Zoom data directory were investigated to extract artifacts that included chats, contacts, caches, video meetings and user/device configurations. Preliminary memory and network forensic analyses were also presented.

The Zoom databases analyzed by Mahr et al. [15] were stored on disk in un-encrypted form at the time of their research. However, from our own forensic analysis of the Zoom data directory, we have observed that the databases are now stored in encrypted form on the disk-space. This adds another layer of complexity for the forensic analyst since a passphrase or key is required for decryption.

Similar works include forensic analysis of Social Media applications such as Instagram [16], Facebook, Twitter, LinkedIn [17], WhatsApp, Hangouts and Line [18] on mobile operating systems such as Android and iOS for digital forensic artifacts.

3 Methodology and Experimental Setup

For the purpose of this research, a controlled test environment created using a Windows 10 Virtual Machine (VM) was used. 4 GB RAM and 60 GB disk-space was allotted to the VM. A Microsoft Teams user account was created and signed-in. A clean test environment facilitates a more precise analysis as unnecessary mixing or over-writing of artifacts of Microsoft Teams with other applications or system files is avoided.

To create test data for the forensic analysis, the Microsoft Teams user account was used emulating typical user actions such as: setting up the user profile ID, searching for people in correspondence using keyword search, adding/deleting contacts, audio/video calls and one-to-one/group meetings etc. Table 1 lists features of Microsoft Teams and some user actions that were performed accordingly in order to create the test data.

Table 1. Key features of Microsoft Teams.

Teams feature	User actions
Account setup	Set-up a username, password and profile photo
Search	Find people using keyword search
Contacts	Add/delete contacts
Teams	Create and join teams
Messaging	Send/delete chat messages, URLs, text files and media files
Meetings	Conduct one-to-one and group meetings (+in-meeting chat messages)
Recording	Record meetings
Screen share	Conduct meetings while using the screen sharing feature

Following test user activities, FTK imager was used to create memory and disk images of the VM. For memory analysis, each memory dump was taken after major user actions were performed such as user login, chat messages, meetings etc. to analyze them separately.

For automated analysis of the forensic images, tools such as Volatility, Bulk Extractor and Photorec were used. Manual forensic analysis was performed using string searching, employing relevant keywords/phrases. The artifacts in focus are categorized into different *profiles* [12]: (1) installation data, (2) traffic data, (3) content data, (4) user profile data, (5) user authentication data, (6) contact database, (7) attachment/files and (8) location data.

To capture and analyze the network traffic, we used Wireshark. Network miner was also used to analyze *.pcap* traffic captured using Wireshark. The research methodology is illustrated in Fig. 1 (Table 2).

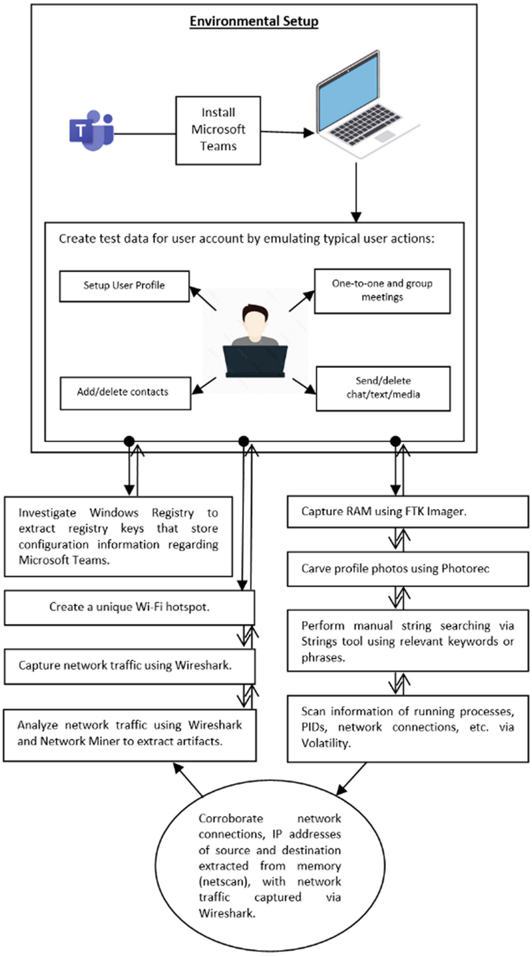


Fig. 1. Research methodology.

Table 2. Tools used for forensic analysis.

Tool	Version	Usage
Windows 10 VM	10	Test OS
Microsoft Teams desktop application	1.4.00.7174	Videoconferencing application under test for forensic artifacts
FTK imager	4.5.0.3	Create forensic image dumps
Volatility	2.6	Forensic analysis of image dumps
Strings	2.53	Manual string searching

(*continued*)

Table 2. (*continued*)

Tool	Version	Usage
Bulk Extractor	1.6.0	Forensic analysis of image dumps
Photorec	7.2	Carve.jpeg images from image dumps
Regedit	10	View the windows registry
Wireshark	3.4.6	Capture/analyze network traffic
Network miner	2.7.1.0	Analyze network traffic

4 Memory Forensics

Random Access Memory (RAM), or memory, stores information about the Operating System's (OS) running processes and applications. Data is often stored in un-encrypted form in the memory which makes it an interesting reserve of information that can serve as digital evidence. Microsoft Teams' artifacts carved from the memory of the VM are presented.

Determining whether Microsoft Teams was running on a device or not was fairly simple; the *pslist*, or *pstree* plug-ins of Volatility showed the *teams.exe* processes running in the memory. The processes were displayed against their Process IDs (PID). The PID's Parent Process Identifier (PPID) can also be traced to make sure that the *teams.exe* originated from the legitimate Teams process and not a foreign/malicious process. The timestamps of the *teams.exe* process also indicated when the application was running. The *pstree* output in Fig. 2(a), shows the Teams processes. Volatility can also be used to investigate the network connections that were listening/established close to when the

```
Name                                              Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0xfffffa8008ba5b00:Teams.exe                     2188   3232     38   1050 2021-07-14 08:24:13 UTC+0000
. 0xfffffa8003f1bb00:Teams.exe                     704   2188     11    220 2021-07-14 08:24:27 UTC+0000
. 0xfffffa80097ad060:Teams.exe                    2328   2188     10    278 2021-07-14 08:24:21 UTC+0000
. 0xfffffa8007223060:Teams.exe                    1144   2188     13    401 2021-07-14 08:24:22 UTC+0000
. 0xfffffa8004d21060:Teams.exe                    3184   2188     16    234 2021-07-14 08:39:12 UTC+0000
. 0xfffffa8004013060:Teams.exe                    3996   2188     18    383 2021-07-14 08:25:37 UTC+0000
. 0xfffffa8003f1ab00:Teams.exe                    2492   2188     15    271 2021-07-14 08:24:23 UTC+0000
. 0xfffffa8003f4eb00:Teams.exe                    2240   2188     13    256 2021-07-14 08:33:55 UTC+0000
```

(a)

```
Rule: r1
Owner: Process Teams.exe Pid 3744
0x05592e58  5a 61 69 6e 61 62 20 20 4b 68 61 6c 69 64 22 0a   Zainab..Khalid".
0x05592e68  70 72 6f 70 65 72 74 69 65 73 6f 22 0a 64 65 6c   propertieso".del
0x05592e78  65 74 65 74 69 6d 65 4e 00 80 89 94 42 aa 77 42   etetimeN....B.wB
0x05592e88  7b 01 22 02 69 64 22 0d 31 36 32 36 32 35 31 37   {.".id".16262517
0x05592e98  32 34 38 32 38 22 04 74 79 70 65 22 07 4d 65 73   24828".type".Mes
0x05592ea8  73 61 67 65 22 0a 73 65 71 75 65 6e 63 65 49 64   sage".sequenceId
0x05592eb8  49 2c 22 0b 6d 65 73 73 61 67 65 4b 69 6e 64 22   I,".messageKind"
0x05592ec8  11 73 6b 79 70 65 4d 65 73 73 61 67 65 4c 6f 63   .skypeMessageLoc
0x05592ed8  61 6c 22 0b 63 6f 6d 70 6f 73 65 74 69 6d 65 22   al".composetime"
0x05592ee8  1c 32 30 32 31 2d 30 37 2d 31 34 54 30 38 3a 33   .2021-07-14T08:3
0x05592ef8  35 3a 32 34 2e 38 32 38 30 30 30 30 5a 22 13 6f   5:24.8280000Z".o
0x05592f08  72 69 67 69 6e 61 6c 61 72 72 69 76 61 6c 74 69   riginalarrivalti
0x05592f18  6d 65 22 1c 32 30 32 31 2d 30 37 2d 31 34 54 30   me".2021-07-14T0
0x05592f28  38 3a 33 35 3a 32 34 2e 38 32 38 30 30 30 30 5a   8:35:24.8280000Z
0x05592f38  22 11 63 6c 69 65 6e 74 41 72 72 69 76 61 6c 54   ".clientArrivalT
0x05592f48  69 6d 65 22 18 32 30 32 31 2d 30 37 2d 31 34 54   ime".2021-07-14T
```

(b)

Fig. 2. (a) Pstree output for Microsoft Teams via Volatility. (b) Yarascan search for PID 3744 via Volatility.

memory image was captured. The output of *netscan* for Microsoft Teams is discussed in Sect. 6.

Yarascan is another Volatility plugin that was used to search artifacts particular to a PID. Figure 2(b) shows information regarding a message deletion related to a Teams process (searched using Teams PID 3744).

As shown, Yarascan searches can reveal useful information about user activity, but it displayed a limited window of information and further analysis required tracing the physical/virtual offsets of the displayed output. The same information was easily extracted using string searching as discussed further.

Another tool, Bulk Extractor was used to carve Advances Encryption Standard (AES) keys, as shown in Fig. 3(a). The email histogram (Fig. 3(b)) showed the user's correspondence in one-to-one and group meetings in an order. It is observed that the user communicated most with user accounts associated with the emails at the top of the histogram.

```
# Feature-Recorder: aes_keys
# Filename: calldump.mem
# Feature-File-Version: 1.1
68887940        1a 6c cd f3 c5 26 3d 06 46 95 30 c5 f8 90         AES128
176251128       48 18 9e 20 04 79 3c 22 c4 6f c3 b1 f3 2c 6c 04 7b 2e 70 2a 17 1f 62 cf 0d d5 ad 6a e7 cd        AES256
176251776       e1 1e 45 71 de f3 fa cc 42 b9 33 4a 3e 8d c1 63 e6 c6 22 32 1c a1 c7 52 52 fb 59 7a 4b 00        AES256
509692536       48 18 9e 20 04 79 3c 22 c4 6f c3 b1 f3 2c 6c 04 7b 2e 70 2a 17 1f 62 cf 0d d5 ad 6a e7 cd        AES256
509693184       e1 1e 45 71 de f3 fa cc 42 b9 33 4a 3e 8d c1 63 e6 c6 22 32 1c a1 c7 52 52 fb 59 7a 4b 00        AES256
1022826464      e1 1e 45 71 de f3 fa cc 42 b9 33 4a 3e 8d c1 63 e6 c6 22 32 1c a1 c7 52 52 fb 59 7a 4b 00        AES256
1145976800      e1 1e 45 71 de f3 fa cc 42 b9 33 4a 3e 8d c1 63 e6 c6 22 32 1c a1 c7 52 52 fb 59 7a 4b 00        AES256
1331799232      cf 33 df a0 8e 3e 74 5b 55 32 5e 5f b5 bd 03 d2 a2 77 20 e4 e6 45 f1 95 00 28 27 2e c1 01        AES256
1384461056      12 b2 79 15 15 00 92 e1 5b 52 19 2b e2 b2         AES128
1860916612      1a 6c cd f3 c5 26 3d 06 46 95 30 c5 f8 90         AES128
2046707016      27 17 6d b4 b8 92 ac 99 fc 75 ea ae cb 80 83 d3 32 1a 0c c4 c2 4e 58 f4 d0 15 15 15 e6 6f        AES256
2046707664      e3 b5 63 aa 3c 58 b8 3c e8 7d 8d da 72 e1 51 d3 a0 a4 f6 2e 17 4e c4 93 c5 1e 89 12 bf dd        AES256
2295347632      48 18 9e 20 04 79 3c 22 c4 6f c3 b1 f3 2c 6c 04 7b 2e 70 2a 17 1f 62 cf 0d d5 ad 6a e7 cd        AES256
2313253472      8b 18 63 cb 13 03 11 5f 8c 02 c4 2c 64 12         AES128
2438508792      48 18 9e 20 04 79 3c 22 c4 6f c3 b1 f3 2c 6c 04 7b 2e 70 2a 17 1f 62 cf 0d d5 ad 6a e7 cd        AES256
2438509440      e1 1e 45 71 de f3 fa cc 42 b9 33 4a 3e 8d c1 63 e6 c6 22 32 1c a1 c7 52 52 fb 59 7a 4b 00        AES256
2712266220      ca b0 c9 13 9d 42 4a 78 51 aa 2e 20 61 66         AES128
2930948584      48 18 9e 20 04 79 3c 22 c4 6f c3 b1 f3 2c 6c 04 7b 2e 70 2a 17 1f 62 cf 0d d5 ad 6a e7 cd        AES256
2930949232      e1 1e 45 71 de f3 fa cc 42 b9 33 4a 3e 8d c1 63 e6 c6 22 32 1c a1 c7 52 52 fb 59 7a 4b 00        AES256
4637786672      33 37 91 70 18 98 85 3e a0 27 86 c4 90 1b 77 34 72 5f d6 8f fe 89 97 f5 33 e7 93 20 26 85        AES256
5031073292      04 21 85 20 00 1b 8e db eb aa 93 28 93 7a         AES128
```

(a)

```
# Feature-Recorder: email
# Filename: calldump.mem
# Histogram-File-Version: 1.1
n=744    zkhalid.msis18seecs@student.nust.edu.pk  (utf16=123)
n=166    haftab.msis17seecs@student.nust.edu.pk   (utf16=19)
n=140    bnoor.msis19seecs@student.nust.edu.pk    (utf16=12)
n=124    bnoor.msis19seecs@nustedupk0.onmicrosoft.com
n=122    meet598@nustedupk0.onmicrosoft.com
n=92     meet598@nust.edu.pk
n=83     info@diginotar.nl
n=49     00@unq.gb        (utf16=49)
n=38     hp@login.microsoftonline.com     (utf16=38)
n=34     premium-server@thawte.com
n=34     sales@ouriginal.com      (utf16=34)
n=30     appro@openssl.org
```

(b)

Fig. 3. (a) AES keys extracted via Bulk Extractor. (b) Email histogram displaying most contacted emails extracted via Bulk Extractor.

Photorec was used to carve photographic images from the memory dumps. We were able to extract critical images, such as: (1) profile photo of the logged-in user account, (2) profile photos of accounts the user interacted with, (3) Microsoft Teams logos and (4) other favicon images related to the application, as shown in Fig. 4. This shows that Microsoft Teams's profile images are processed in un-encrypted form in the memory; a useful artifact in regard to investigations.

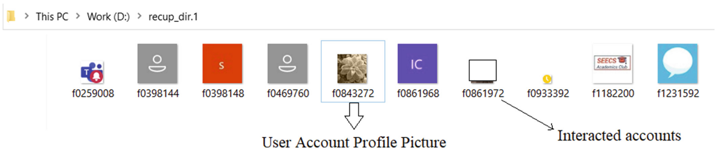


Fig. 4. Profile photos carved from memory via Photorec.

Manual forensic analysis was also conducted using string searches against the memory dumps which revealed a plethora of information such as the user's account details (user display name, email address associated with Microsoft Teams and the user ID etc.), as shown in Fig. 5(a). The user password was not found in the memory in plaintext as a result of string search against the memory dump. This was expected since sensitive authentication information is stored in encrypted form.

Figure 5(b) shows details about an audio call that was made. The start time, end time, user ID and display name of the account that made the call and the recipient's user ID were all present in the memory.

The keyword search option in Microsoft Teams enables the user to search for aquaintances and friends. In memory, information regarding searches made using the option were found under the *QueryString* tag as shown in Fig. 5(c).

auth_time":1585208534,"family_name":"Khalid","given_name":"Zainab",
"ipaddr":"119.160.64.145","name":"Zainab Khalid",
"oid":"b6718102-1033-4ce3-9fed-1834d982ed00",
"tid":"1511ab2e-502b-4e2d-bd68-f679f549b5a2",
"unique_name":"zkhalid.msis18seecs@student.nust.edu.pk","upn":"zkhalid.msis18seecs@student.nust.edu.pk",
"uti":"VnID4zHLokWt9ROTf-l1AA","ver":"1.0","wids":["b79fbf4d-3ef9-4689-8143-76b194e85509"]},
"userId":"1511ab2e-502b-4e2d-bd68-f679f549b5a2__b6718102-1033-4ce3-9fed-1834d982ed00",
"profileType":"AAD","userName":"zkhalid.msis18seecs@student.nust.edu.pk"}},
"homeUserUpn":"zkhalid.msis18seecs@student.nust.edu.pk"}

(a)

{"startTime":"2021-05-12T07:52:17.3695395Z","connectTime":"2021-05-12T07:52:30.5273908Z",
"endTime":"2021-05-12T08:01:22.5864977Z","callDirection":"outgoing","callType":"twoParty",
"callState":"accepted","originator":"8:orgid:b6718102-1033-4ce3-9fed-1834d982ed00","target":
"8:orgid:d94d4c0c-ba6b-4813-94ba-db68f7b55389","originatorParticipant":
{"id":"8:orgid:b6718102-1033-4ce3-9fed-1834d982ed00","type":"default",
"displayName":"Zainab Khalid"},"targetParticipant":
{"id":"8:orgid:d94d4c0c-ba6b-4813-94ba-db68f7b55389"

(b)

EntityRequests":[{"Query":{"QueryString":"Hira","DisplayQueryString":"Hira"}
,"EntityType":"People","Provenances":["Mailbox","Directory"],"From":0,"Size":5,
"Filter":{"And":[{"Or":[{"Term":{"PeopleType":"Person"}},{"Term":{"PeopleType":"Other"}}]},
{"Or":[{"Term":{"PeopleSubtype":"OrganizationUser"}},{"Term":{"PeopleSubtype":"Guest"}}]}]},
"Fields":["Id","DisplayName","EmailAddresses","CompanyName","JobTitle","ImAddress",
"UserPrincipalName","ExternalDirectoryObjectId","PeopleType","PeopleSubtype",
"ConcatenatedId","Phones","MRI","Alias"]},{"Query":{"QueryString":"Hira"},"EntityType":"File","Size":3}]
,"LogicalId":"318cbac7-11e2-42f1-90ef-2e1047b82aae","Cvid":"0f77adda-e8f6-4907-9c06-80dee0c542ff",
"AppName":"Microsoft Teams","Scenario":{"Name":"powerbar"}}

(c)

Fig. 5. (a) User account details extracted via manual string search. (b) Call information extracted via manual string search. (c) Keyword search extracted via manual string search.

The *Microsoft Teams Chat Files* tag stores information about the exchanged text files (including deleted text files) as shown in Fig. 6. The user name, email address of the sender, date and time of exchange, user IDs, name and size of the text file were extracted. Under the same (*Microsoft Teams Chat Files*) tag, information about the exchanged and deleted (photo) media files, their sizes and timestamps were also extracted. The SharePoint server addresses, where these files are stored, were extracted under the tag as well.

https://nustedupk0-my.sharepoint.com/personal/zkhalid_msis18seecs_student_nust_edu_pk/Documents/Microsoft Teams Chat Files/test.txt"
fileServerRelativeUrl"_/personal/zkhalid_msis18seecs_student_nust_edu_pk/Documents/Microsoft Teams Chat Files/test.txt"
{"from":{"displayName":"Zainab Khalid","email":"zkhalid.msis18seecs@student.nust.edu.pk"},"clientId":"10390474803042892000",
"draftObjectId":null,"replyChainId":null,"conversationId":
"19:853db850-c649-404f-ab10-4019f1175348_b6718102-1033-4ce3-9fed-1834d982ed00@unq.gbl.spaces",
"subject":"","dateTimeSent":"2021-07-14T08:36:32.501Z","state":null,"isDraft":true,"isNewMessage":true,
"conversationIndex":"10390474803042892000","isPendingSend":true,"body":"","attachments":
[{"objectId":"817b1222-d9af-47c3-94a0-762a8cee734c",
{"id":"973f5f79-7a40-4465-b243-ab92fa1c6518","name":"test.txt","size":19,"viewId":"10390474803042892000",
"progress":5,"state":3,"isNotificationHandled":true,"retentionPolicy":"none","uploadBeginTimestamp":"2021-07-14T08:37:27.336Z",

(a)

{"id":"20f4ef62-9f4d-4579-9f5e-5380a973abff","name":"del.txt",
"size":6238,"viewId":"626968173333597400","progress":100,"state":2,
"isNotificationHandled":true,"uploadBeginTimestamp":"2021-07-14T08:33:53.433Z",
"sourceProviderMetaData":"{\"code\":null,\"type\":0}","destinationProviderMetaData":"
{\"code\":null,\"type\":0}","sourceOfFile":3,
"siteUrl":"https://nustedupk0-my.sharepoint.com/personal/zkhalid_msis18seecs_student_nust_edu_pk"

(b)

https://nustedupk0-my.sharepoint.com/personal/zkhalid_msis18seecs_student_nust_edu_pk/Documents/Microsoft Teams Chat Files/books.jpg"
fileServerRelativeUrl"`/personal/zkhalid_msis18seecs_student_nust_edu_pk/Documents/Microsoft Teams Chat Files/books.jpg"
Teams%20Chat%20Files%27&@file=%27books.jpg%27
{"id":"2fa24289-006a-4865-98d0-268756f1a11e","name":"books.jpg","size":7537,
"viewId":"5461178093984267000","progress":100,"state":2,"isNotificationHandled":true,
"retentionPolicy":"none","uploadBeginTimestamp":"2021-07-14T08:38:26.208Z",

(c)

{"id":"bd5db3ba-3fc1-45d8-aa0d-8ee0a601bdf1",
"name":"asdf.jpg","size":10371,"viewId":"626968173333597400",
"progress":66,"state":3,"isNotificationHandled":true,
"retentionPolicy":"none","uploadBeginTimestamp":"2021-07-14T08:33:53.425Z",
"sourceProviderMetaData":"{\"code\":null,\"type\":0}",
"destinationProviderMetaData":"{\"code\":null,\"type\":0}"

(d)

Fig. 6. (a) Exchanged text file extracted via manual string search. (b) Deleted text file extracted via manual string search. (c) Exchanged media file extracted via manual string search. (d) Deleted media file extracted via manual string search.

Messages exchanged between the user and other parties were also extracted from the memory under the *skypexspaces-[user ID]* tag, which is the database name of the particular user. This database (stored in *SharePoint*) seemingly stores all the messages of the user including timestamps and other information as shown in Fig. 7. This included deleted messages as well. Microsoft Teams stores messages in the databases even after they are deleted. Using the timestamps, a messaging exchange can be reconstructed in chronological order including the deleted messages. Exchanged Uniform Resource Locators (URLs) were also found under the *skypexspaces-[user ID]* tag (Fig. 7).

Note that some text messages, URLs and media/text files exchanged between users during test activities were deleted. These artifacts were then extracted from the memory dumps using manual string searches as discussed, which shows that deleted information that is *seemingly* deleted and no longer visible on the application's user interface, still resides in the memory and can be recovered using *Microsoft Teams Chat Files* and *skypexspaces-[user ID]* tags. Therefore, anti-forensic attempts like such can be detected using an analysis of the memory.


```
%{"rendererId":"MainRenderer","requestId":"database-142","type":"database",
"payload":{"requestOperationtype":"Put","version":1,
"dbName":"skypexspaces-b6718102-1033-4ce3-9fed-1834d982ed00",
"context":{"storeName":"conversations","
itemOrItems":[{"id":"19:853db850-c649-404f-ab10-4019f1175348_b6718102-1033-4ce3-9fed-1834d982ed00@unq.gbl.spaces",
"type":"Chat","messages":"","properties":{"consumptionhorizon":"1626251363047;1626251372786;3617257132460533000",
"consumptionHorizonBookmark":"",
"interopconversationstatus":"None","conversationblockedat":0},"targetLink":"","version":1625478087273,"syncStateUpdatedBy":
"MessageSyncJob_saveSyncState","lastMessage":{"messagetype":"RichText/Html","contenttype":"text",
"content":"<div>Hi how are you doing?</div>","renderContent":"<div>Hi how are you doing?</div>",
"activitytype":"","clientmessageid":"9361982320257786000","amsreferences":[],
"imdisplayname":"Zainab  Khalid","properties":{"importance":0,"subject":null},
"id":"1626251376624","type":"Message","messageKind":"skypeMessageLocal","composetime":"2021-07-14T08:29:17.229Z",
"originalarrivaltime":"2021-07-14T08:29:36.624Z",
"conversationLink":"
blah/19:853db850-c649-404f-ab10-4019f1175348_b6718102-1033-4ce3-9fed-1834d982ed00@unq.gbl.spaces;messageid=1626251376624",
"from":"blah/8:orgid:b6718102-1033-4ce3-9fed-1834d982ed00","idUnion":"9361982320257786000",
```


(a)


```
{"rendererId":"MainRenderer","requestId":"database-162",
"type":"database","payload":{"requestOperationtype":"Put",
"version":1,"dbName":"skypexspaces-b6718102-1033-4ce3-9fed-1834d982ed00",
"context":{"storeName":"replychains",
"itemOrItems":[{"conversationId":
"19:853db850-c649-404f-ab10-4019f1175348_b6718102-1033-4ce3-9fed-1834d982ed00@unq.gbl.spaces",
"parentMessageId":"clientId_6275769237913159000","messages":{"6275769237913159000,8:
orgid:b6718102-1033-4ce3-9fed-1834d982ed00":{"messagetype":"RichText/Html","contenttype":"text",
"content":"<div>Can we schedule a meeting for tomorrow?</div>"
```


(b)


```
{"rendererId":"MainRenderer","requestId":"database-181","type":"database",
"payload":{"requestOperationtype":"Put","version":1,"dbName":
"skypexspaces-b6718102-1033-4ce3-9fed-1834d982ed00","context":{"storeName":"conversations",
"itemOrItems":[{"id":"19:853db850-c649-404f-ab10-4019f1175348_
b6718102-1033-4ce3-9fed-1834d982ed00@unq.gbl.spaces","type":"Chat","messages":""
"lastMessage":{"messagetype":"RichText/Html","contenttype":"text",
"content":"<div><div><a href=\"https://www.youtube.com/\"
rel=\"noreferrer noopener\" target=\"_blank\"
title=\"https://www.youtube.com/\">https://www.youtube.com/</a><br />\n
```


(c)


```
{"from":{"displayName":"Zainab  Khalid","email":"zkhalid.msis18seecs@student.nust.edu.pk"}
"clientId":"4009176384473812000","draftObjectId":null,"replyChainId":null,
"conversationId":"19:853db850-c649-404f-ab10-4019f1175348_
b6718102-1033-4ce3-9fed-1834d982ed00@unq.gbl.spaces",
"subject":"","dateTimeSent":"2021-07-14T08:31:12.678Z","state":null,"isDraft":
true,"isNewMessage":true,
"conversationIndex":"4009176384473812000","isPendingSend":true,"body":
"<div><a href=\"https://www.forensicfocus.com/forums/\"
```


(d)

Fig. 7. (a) Exchanged text message extracted via manual string search. (b) Deleted text message extracted via manual string search. (c) Exchanged URLs extracted via manual string search. (d) Deleted URLs extracted via manual string search.

Information regarding scheduled meetings was also extracted from the memory. Figure 8 shows that a meeting named "Test Meeting" was scheduled for 2 PM Wednesday on July 14, 2021. The organizer's user ID is also extracted along with other information. Chat messages sent (deleted messages included) were also found in the memory (Table 3).

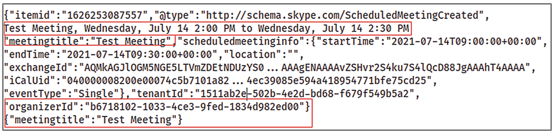


Fig. 8. Scheduled meeting information extracted via manual string search.

Table 3. Summary of memory artifacts of Microsoft Teams.

Artifact	Tool/manual string tag
Running teams processes	(*pslist*/*pstree*) volatility
Network connections	(*netscan*) volatility
AES keys	Bulk extractor
Profile photos	Image carving against memory dumps via Photorec
User account details (user display name, email address, user ID etc.)	<*unique_name*>/<*userId*>String tag
Keywords searched	<*QueryString*>String tag
Media/text files exchanged (+deleted)	<*Microsoft Teams Chat Files*>String tag
Chat/URLs exchanged (+deleted)	<*skypexspaces-[user ID]*>String tag
Scheduled meetings' details	<*scheduledmeetinginfo*>String tag

5 Disk-Space Forensics

Unlike the memory, disk-space stores information for a relatively longer time. While our analysis of Microsoft Team's client application folder did not reveal information/artifacts of critical value, the Windows Registry is nonetheless a potential source of forensic artifacts. Microsoft Operating System's Windows Registry is a central hierarchal database that stores configuration information about the OS. This includes information about the users, (Microsoft or foreign) applications that are (or were) installed on the device and hardware devices attached to the device. User information can also include credentials and relevant timestamps that can prove useful for an investigation.

We performed an in-depth analysis of the Windows Registry for keys related to Microsoft Teams and it was observed that while basic information about the user account is retrievable from the registry, no credentials/authentication information was found.

The *HKCU\SOFTWARE\RegisteredApplications key* lists Microsoft Teams in registered applications. The *HKCU\SOFTWARE\Microsoft\Office\Teams* key stores basic user account information, as shown in Fig. 9, such as the email address, private meeting settings, the installation source used to install Microsoft Teams, the web account ID and login information etc. The *HKCU\SOFTWARE\Microsoft\Office\Teams\Capabilities\URLAssociations* key stores the URL associations of Microsoft Teams: *sip*, *sips*, *im*, *callto* and *msteams*. The *HKCU\SOFTWARE\Microsoft\Office\Outlook\Addins\TeamsAddin.FastConnect* lists the Microsoft Teams add-in for Outlook. If Microsoft Teams is uninstalled, it is listed in *HKCU\SOFTWARE\Microsoft\UserData\UninstallTimes* key (Table 4).

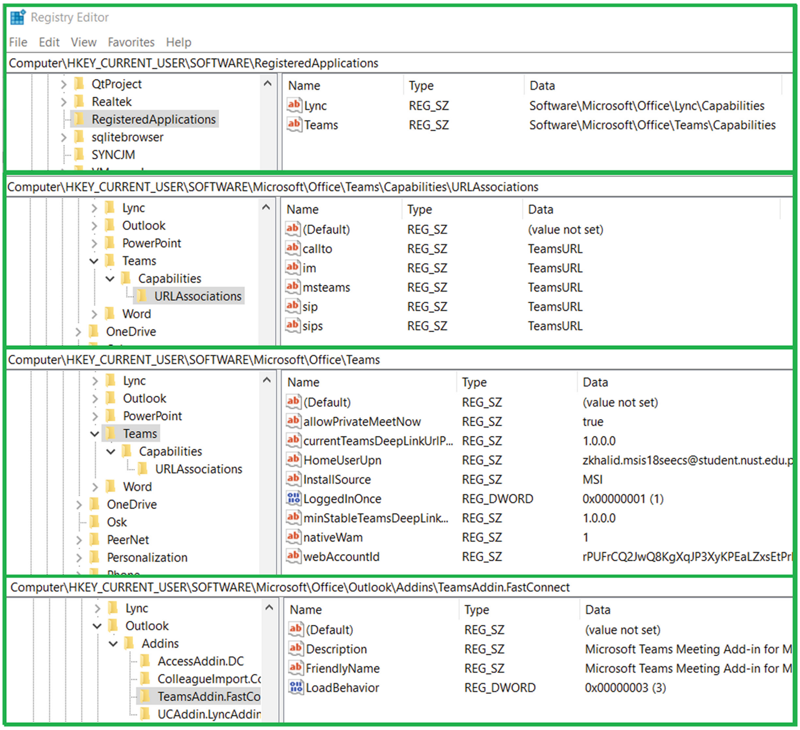


Fig. 9. Registry keys for Microsoft Teams.

Table 4. Registry keys for Microsoft Teams.

Registry key – Value explanation
HKCU\SOFTWARE\RegisteredApplications List of registered applications in the client desktop (Microsoft Teams inclusive).
HKCU\SOFTWARE\Microsoft\Office\Teams User account information including email address, private meeting settings, installation source, web account ID and login information etc.
HKCU\SOFTWARE\Microsoft\Office\Teams\Capabilities\URLAssociations URL associations of Microsoft Teams (e.g., sip, IM, callto etc.).
HKCU\SOFTWARE\Microsoft\Office\Outlook\Addins\TeamsAddin.FastConnect Microsoft Teams add-in for Outlook.
HKCU\SOFTWARE\Microsoft\UserData\UninstallTimes Microsoft Teams is listed if it is uninstalled.

6 Network Forensics

The *netscan* output of Microsoft Teams (Fig. 10) shows connections established with Microsoft servers over UDPv4, UDPv6 and TLSv4 while transferring meeting media during a Teams meeting. Volatility seemingly missed some PIDs and IP addresses, which is a recurring problem with the newer versions of Windows (i.e. Windows 10 and its various versions). Nonetheless, the *netscan* output still offers valuable information

Offset(P)	Proto	Local Address	Foreign Address	State	Pid	Owner	Created
0×13a9a8470	TCPv6	:::49152	:::0	LISTENING	528	wininit.exe	
0×13ab3d640	TCPv4	0.0.0.0:49153	0.0.0.0:0	LISTENING	964	svchost.exe	
0×13af83ee0	TCPv4	0.0.0.0:49156	0.0.0.0:0	LISTENING	588	services.exe	
0×13af83ee0	TCPv6	:::49156	:::0	LISTENING	588	services.exe	
0×13a683bd0	TCPv4	192.[redacted]:49564	40.77.18.167:443	CLOSED	-1		
0×13a6bdcd0	TCPv4	192.[redacted]:49508	20.190.175.23:443	CLOSED	-1		
0×13a9c08f0	TCPv4	192.[redacted]:49568	52.114.132.73:443	ESTABLISHED	-1		
0×13addf3d0	TCPv4	192.[redacted]:49569	52.114.132.73:443	ESTABLISHED	-1		
0×13b06fcc0	TCPv4	0.0.0.0:49156	0.0.0.0:0	LISTENING	588	services.exe	
0×13c2c3220	UDPv4	192.[redacted]:50024	*:*		4076	Teams.exe	2021-07-14 08:58:56 UTC+0000
0×13c2dbec0	UDPv6	fe80[redacted]	*:*		3648	svchost.exe	2021-07-14 08:23:40 UTC+0000
0×13c2dfcd0	TCPv4	192.[redacted]:49523	52.114.14.235:443	ESTABLISHED	-1		
0×13e77c3a0	UDPv4	192.[redacted]:2177	*:*		3648	svchost.exe	2021-07-14 08:46:33 UTC+0000
0×13e6d1450	TCPv4	192.[redacted]:49453	52.113.199.100:443	ESTABLISHED	-1		
0×13e6d1cd0	TCPv4	192.[redacted]:49546	52.114.36.125:443	ESTABLISHED	-1		
0×13e9ec580	TCPv4	192.[redacted]:49553	119.160.63.43:443	ESTABLISHED	-1		
0×13ee6c880	UDPv6	fe80[redacted]	*:*		3648	svchost.exe	2021-07-14 08:46:33 UTC+0000
0×13ef0ccb0	UDPv4	0.0.0.0:51209	*:*		4076	Teams.exe	2021-07-14 08:46:02 UTC+0000
0×13ef0ccb0	UDPv6	:::51209	*:*		4076	Teams.exe	2021-07-14 08:46:02 UTC+0000
0×13ef99ec0	UDPv4	0.0.0.0:55228	*:*		3572	Teams.exe	2021-07-14 09:03:23 UTC+0000
0×13ef99ec0	UDPv6	:::55228	*:*		3572	Teams.exe	2021-07-14 09:03:23 UTC+0000
0×13f215240	UDPv4	0.0.0.0:0	*:*		4076	Teams.exe	2021-07-14 08:45:56 UTC+0000
0×13f215240	UDPv6	:::0	*:*		4076	Teams.exe	2021-07-14 08:45:56 UTC+0000
0×13f327900	UDPv4	0.0.0.0:55941	*:*		1212	svchost.exe	2021-07-14 08:57:34 UTC+0000
0×13f55d160	UDPv4	0.0.0.0:60165	*:*		4076	Teams.exe	2021-07-14 08:46:05 UTC+0000
0×13f55d160	UDPv6	:::60165	*:*		4076	Teams.exe	2021-07-14 08:46:05 UTC+0000
0×13ec39790	TCPv4	192.[redacted]:49469	52.114.16.76:443	ESTABLISHED	-1		
0×13ee536d0	TCPv4	192.[redacted]:49562	52.114.75.149:443	CLOSED	-1		
0×13efe2010	TCPv4	192.[redacted]:49520	52.113.194.132:443	ESTABLISHED	-1		
0×13f036820	TCPv4	192.[redacted]:49563	20.190.175.23:443	CLOSED	-1		
0×13f1a6bb0	TCPv4	192.[redacted]:49547	52.114.36.125:443	CLOSED	-1		
0×13f1e3010	TCPv4	192.[redacted]:49567	40.77.18.167:443	CLOSED	-1		
0×13f222a50	TCPv4	192.[redacted]:49549	119.160.63.43:443	ESTABLISHED	-1		
0×13f26a700	TCPv4	192.[redacted]:49557	52.114.75.149:443	CLOSED	-1		
0×13f2dcac0	TCPv4	192.[redacted]:49566	40.77.18.167:443	FIN_WAIT1	-1		
0×13f321470	TCPv4	192.[redacted]:49565	40.77.18.167:443	CLOSED	-1		
0×13f329cd0	TCPv4	192.[redacted]:49551	119.160.63.43:443	ESTABLISHED	-1		
0×13f7a9330	UDPv4	0.0.0.0:5355	*:*		1212	svchost.exe	2021-07-14 08:23:08 UTC+0000
0×13f7a9330	UDPv6	:::5355	*:*		1212	svchost.exe	2021-07-14 08:23:08 UTC+0000
0×13f7f11c0	UDPv4	0.0.0.0:5355	*:*		1212	svchost.exe	2021-07-14 08:23:08 UTC+0000

Fig. 10. Netscan output via volatility.

including timestamps, and other IP addresses that can be corroborated with the *pslist* output or packets captured using a network protocol analyzer as discussed further. Owing to the volatile nature of memory, it is not always available during an investigation. The disk-space, on the other hand, can be manipulated one way or another. In such a case, the network proves to be a reliable alternative for extracting artifacts because network traffic cannot be tampered with.

To perform network forensic analysis of the Microsoft Teams application, we setup a unique Wi-Fi hotspot to isolate the traffic. This was done to aid the process of analysis. We used the Wireshark network protocol analyzer to both capture and analyze the traffic. Network miner was also used for the analysis of the *.pcap* traffic captured using Wireshark. The IP addresses of servers were investigated using https://ipdata.co/?ref=iplocation.

The traffic was captured intermittently, i.e., the login activity, exchange of messages/URLs/image media and (one-to-one and group) meetings were captured separately to be analyzed individually. From our observations, all the network traffic of Microsoft Teams was encrypted as no credentials, messages, or transferred image or text files were observed in the packet captures in plaintext. The encryption keys were exchanged using the Elliptic Curve Diffie Hellman (ECDH) key agreement protocol, while the application data was transferred using either HTTP over TLSv1.2 or HTTP2, as shown in Fig. 11.

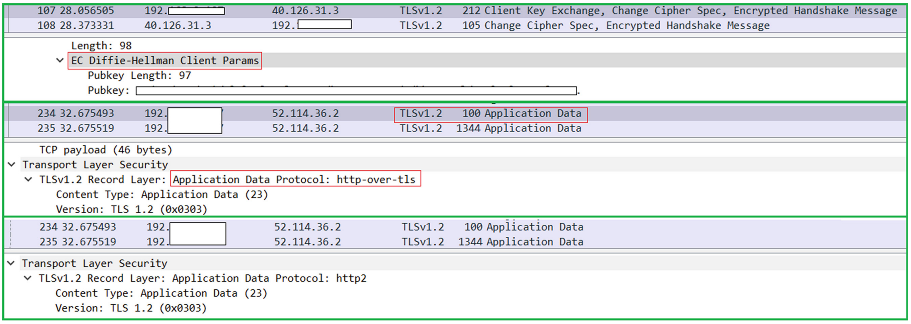


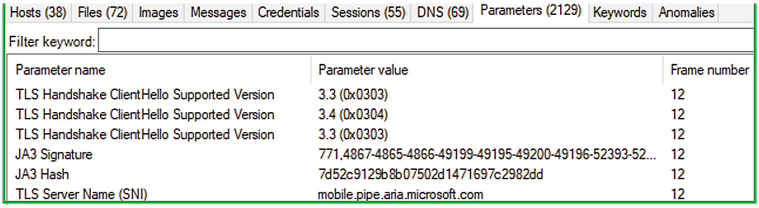
Fig. 11. Communication protocols used by Microsoft Teams as observed via Wireshark.

Sessions between client and Microsoft Teams' servers were encrypted using TLS (Fig. 12). As can be seen, JA3 and JA3S hashing was used to fingerprint the negotiation between client and server.

Analyzing network traffic of Microsoft Teams using Network Miner, we observed that the application makes connections to Microsoft servers mostly (unlike other applications which are likely to use services of other organizations as well). This is expected since Microsoft has an established infrastructure that is capable of all required services. However Akamai Technologies, as observed in the network traffic, is used by Teams as a content distribution system.

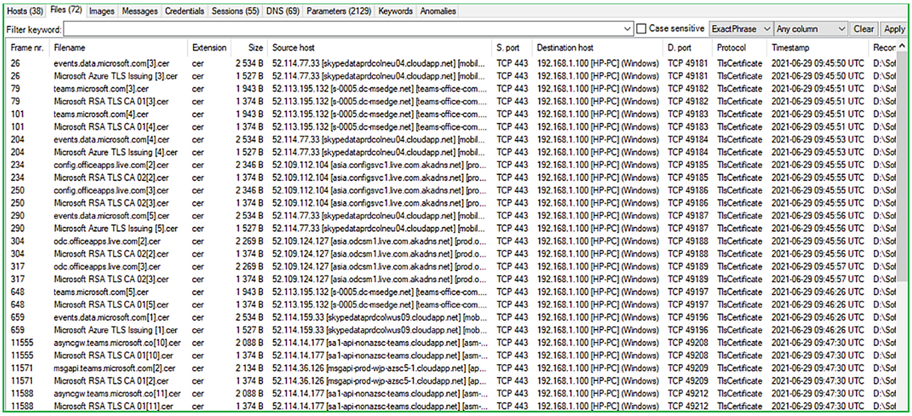
Logging into Microsoft Teams, client is first authenticated to the Teams cloud skypedataprdcolneu04.cloudapp.net, login.microsoftonline.com, stamp2.login.microsoftonline on port 443. Another point to note is that Microsoft Teams uses several of Skype's servers as well. Configuration data is fetched from settingsfd-geo.trafficmanager.net, settings-win.data.microsoft.com.

As previously discussed, since network traffic is encrypted, captured frames did not contain any plaintext data. However, digital certificates employed and transferred during the meetings and other activities were extracted. The digital certificates can be used to track whether the communicating hosts were authenticated or not.



Parameter name	Parameter value	Frame number
TLS Handshake ClientHello Supported Version	3.3 (0x0303)	12
TLS Handshake ClientHello Supported Version	3.4 (0x0304)	12
TLS Handshake ClientHello Supported Version	3.3 (0x0303)	12
JA3 Signature	771,4867-4865-4866-49199-49195-49200-49196-52393-52...	12
JA3 Hash	7d52c9129b8b07502d1471697c2982dd	12
TLS Server Name (SNI)	mobile.pipe.aria.microsoft.com	12

(a)



Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host	D. port	Protocol	Timestamp	Recon
26	events.data.microsoft.com[3].cer	cer	2 534 B	52.114.77.33 [skypedataprdcolneu04.cloudapp.net] [mobil...	TCP 443	192.168.1.100 [HP-PC] (Windows)	TCP 49181	TlsCertificate	2021-06-29 09:45:50 UTC	D:\Sof
26	Microsoft Azure TLS Issuing [3].cer	cer	1 527 B	52.114.77.33 [skypedataprdcolneu04.cloudapp.net] [mobil...	TCP 443	192.168.1.100 [HP-PC] (Windows)	TCP 49181	TlsCertificate	2021-06-29 09:45:50 UTC	D:\Sof
79	teams.microsoft.com[3].cer	cer	1 943 B	52.113.195.132 [s-0005.dc-msedge.net] [teams-office-com....	TCP 443	192.168.1.100 [HP-PC] (Windows)	TCP 49182	TlsCertificate	2021-06-29 09:45:51 UTC	D:\Sof
79	Microsoft RSA TLS CA 01[3].cer	cer	1 374 B	52.113.195.132 [s-0005.dc-msedge.net] [teams-office-com....	TCP 443	192.168.1.100 [HP-PC] (Windows)	TCP 49182	TlsCertificate	2021-06-29 09:45:51 UTC	D:\Sof
101	teams.microsoft.com[4].cer	cer	1 943 B	52.113.195.132 [s-0005.dc-msedge.net] [teams-office-com....	TCP 443	192.168.1.100 [HP-PC] (Windows)	TCP 49183	TlsCertificate	2021-06-29 09:45:51 UTC	D:\Sof
101	Microsoft RSA TLS CA 01[4].cer	cer	1 374 B	52.113.195.132 [s-0005.dc-msedge.net] [teams-office-com....	TCP 443	192.168.1.100 [HP-PC] (Windows)	TCP 49183	TlsCertificate	2021-06-29 09:45:51 UTC	D:\Sof
204	events.data.microsoft.com[4].cer	cer	2 534 B	52.114.77.33 [skypedataprdcolneu04.cloudapp.net] [mobil...	TCP 443	192.168.1.100 [HP-PC] (Windows)	TCP 49184	TlsCertificate	2021-06-29 09:45:53 UTC	D:\Sof
204	Microsoft Azure TLS Issuing [4].cer	cer	1 527 B	52.114.77.33 [skypedataprdcolneu04.cloudapp.net] [mobil...	TCP 443	192.168.1.100 [HP-PC] (Windows)	TCP 49184	TlsCertificate	2021-06-29 09:45:53 UTC	D:\Sof
234	config.officeapps.live.com[2].cer	cer	2 346 B	52.109.112.104 [asia.configsvc1.live.com.akadns.net] [pro...	TCP 443	192.168.1.100 [HP-PC] (Windows)	TCP 49185	TlsCertificate	2021-06-29 09:45:55 UTC	D:\Sof
234	Microsoft RSA TLS CA 02[2].cer	cer	1 374 B	52.109.112.104 [asia.configsvc1.live.com.akadns.net] [pro...	TCP 443	192.168.1.100 [HP-PC] (Windows)	TCP 49185	TlsCertificate	2021-06-29 09:45:55 UTC	D:\Sof
250	config.officeapps.live.com[3].cer	cer	2 346 B	52.109.112.104 [asia.configsvc1.live.com.akadns.net] [pro...	TCP 443	192.168.1.100 [HP-PC] (Windows)	TCP 49186	TlsCertificate	2021-06-29 09:45:55 UTC	D:\Sof
250	Microsoft RSA TLS CA 02[3].cer	cer	1 374 B	52.109.112.104 [asia.configsvc1.live.com.akadns.net] [pro...	TCP 443	192.168.1.100 [HP-PC] (Windows)	TCP 49186	TlsCertificate	2021-06-29 09:45:55 UTC	D:\Sof
290	events.data.microsoft.com[5].cer	cer	2 534 B	52.114.77.33 [skypedataprdcolneu04.cloudapp.net] [mobil...	TCP 443	192.168.1.100 [HP-PC] (Windows)	TCP 49187	TlsCertificate	2021-06-29 09:45:56 UTC	D:\Sof
290	Microsoft Azure TLS Issuing [5].cer	cer	1 527 B	52.114.77.33 [skypedataprdcolneu04.cloudapp.net] [mobil...	TCP 443	192.168.1.100 [HP-PC] (Windows)	TCP 49187	TlsCertificate	2021-06-29 09:45:56 UTC	D:\Sof
304	odc.officeapps.live.com[2].cer	cer	2 269 B	52.109.124.127 [asia.odcsm1.live.com.akadns.net] [prod.o...	TCP 443	192.168.1.100 [HP-PC] (Windows)	TCP 49188	TlsCertificate	2021-06-29 09:45:56 UTC	D:\Sof
304	Microsoft RSA TLS CA 02[2].cer	cer	1 374 B	52.109.124.127 [asia.odcsm1.live.com.akadns.net] [prod.o...	TCP 443	192.168.1.100 [HP-PC] (Windows)	TCP 49188	TlsCertificate	2021-06-29 09:45:56 UTC	D:\Sof
317	odc.officeapps.live.com[3].cer	cer	2 269 B	52.109.124.127 [asia.odcsm1.live.com.akadns.net] [prod.o...	TCP 443	192.168.1.100 [HP-PC] (Windows)	TCP 49189	TlsCertificate	2021-06-29 09:45:57 UTC	D:\Sof
317	Microsoft RSA TLS CA 02[3].cer	cer	1 374 B	52.109.124.127 [asia.odcsm1.live.com.akadns.net] [prod.o...	TCP 443	192.168.1.100 [HP-PC] (Windows)	TCP 49189	TlsCertificate	2021-06-29 09:45:57 UTC	D:\Sof
648	teams.microsoft.com[5].cer	cer	1 943 B	52.113.195.132 [s-0005.dc-msedge.net] [teams-office-com....	TCP 443	192.168.1.100 [HP-PC] (Windows)	TCP 49197	TlsCertificate	2021-06-29 09:46:26 UTC	D:\Sof
648	Microsoft RSA TLS CA 01[5].cer	cer	1 374 B	52.113.195.132 [s-0005.dc-msedge.net] [teams-office-com....	TCP 443	192.168.1.100 [HP-PC] (Windows)	TCP 49197	TlsCertificate	2021-06-29 09:46:26 UTC	D:\Sof
659	events.data.microsoft.com[1].cer	cer	2 534 B	52.114.159.33 [skypedataprdcolwus09.cloudapp.net] [mob...	TCP 443	192.168.1.100 [HP-PC] (Windows)	TCP 49196	TlsCertificate	2021-06-29 09:46:26 UTC	D:\Sof
659	Microsoft Azure TLS Issuing [1].cer	cer	1 527 B	52.114.159.33 [skypedataprdcolwus09.cloudapp.net] [mob...	TCP 443	192.168.1.100 [HP-PC] (Windows)	TCP 49196	TlsCertificate	2021-06-29 09:46:26 UTC	D:\Sof
11555	asyncgw.teams.microsoft.co[10].cer	cer	2 088 B	52.114.14.177 [sa1-api-nonazsc-teams.cloudapp.net] [asm-...	TCP 443	192.168.1.100 [HP-PC] (Windows)	TCP 49208	TlsCertificate	2021-06-29 09:47:30 UTC	D:\Sof
11555	Microsoft RSA TLS CA 01[10].cer	cer	1 374 B	52.114.14.177 [sa1-api-nonazsc-teams.cloudapp.net] [asm-...	TCP 443	192.168.1.100 [HP-PC] (Windows)	TCP 49208	TlsCertificate	2021-06-29 09:47:30 UTC	D:\Sof
11571	msgapi.teams.microsoft.com[2].cer	cer	2 134 B	52.114.36.126 [msgapi-prod-wjp-azsc5-1.cloudapp.net] [ap...	TCP 443	192.168.1.100 [HP-PC] (Windows)	TCP 49209	TlsCertificate	2021-06-29 09:47:30 UTC	D:\Sof
11571	Microsoft RSA TLS CA 01[2].cer	cer	1 374 B	52.114.36.126 [msgapi-prod-wjp-azsc5-1.cloudapp.net] [ap...	TCP 443	192.168.1.100 [HP-PC] (Windows)	TCP 49209	TlsCertificate	2021-06-29 09:47:30 UTC	D:\Sof
11588	asyncgw.teams.microsoft.co[11].cer	cer	2 088 B	52.114.14.177 [sa1-api-nonazsc-teams.cloudapp.net] [asm-...	TCP 443	192.168.1.100 [HP-PC] (Windows)	TCP 49212	TlsCertificate	2021-06-29 09:47:30 UTC	D:\Sof
11588	Microsoft RSA TLS CA 01[11].cer	cer	1 374 B	52.114.14.177 [sa1-api-nonazsc-teams.cloudapp.net] [asm-...	TCP 443	192.168.1.100 [HP-PC] (Windows)	TCP 49212	TlsCertificate	2021-06-29 09:47:30 UTC	D:\Sof

(b)

Fig. 12. (a) TLS handshake via Network Miner. (b) Digital certificates via Network Miner.

The IP addresses and timestamps from the network traffic were used to reconstruct the history of whom the client device communicated with and when. Table 5 provides details of the captured traffic, IP addresses and servers that the host communicated with. This information can also be used to flag Microsoft Teams' network traffic.

Table 5. Network information.

URLs	IP addresses
Microsoft Corporation.	
skypedataprdcolneu04.cloudapp.net, mobile.events.data.trafficmanager.net, mobile.pip.aria.microsoft.com, teams-office-com.s-0005.s-msedge.net, teams.microsoft.com, asia.configsvc1.live.com.akadns.net, officeclient.microsoft.com, config.officeapps.live.com, asia.odcsm1.live.com.akadns.net, odc.officeapps.live.com, settingsfd-geo.trafficmanager.net, settings-win.data.microsoft.com, sa1-api.nonazsc-teams.cloudapp.net, asm-api-golocal-geo-as-teams.trafficmanager.net, asm.skype.com, as-prod.asyncgw.teams.microsoft.com, apac.ng.msg.teams-msgapi.trafficmanager.net, msgapi.teams.microsoft.com, asm-api-prod-geo-as-skype.trafficmanager.net, as-api.asm.skype.com, teams.events.data.microsoft.com, mobile.pipe.aria.microsoft.com, login.microsoftonline.com, stamp2.login.microsoftonline.	52.114.77.33 52.113.195.132 52.109.112.104 52.109.124.127 52.114.159.33 40.174.108.123 52.114.14.177 52.114.36.126 52.114.15.135 52.114.77.164 138.91.140.216 20.190.175.23 52.114.128.9 52.113.194.132 52.114.16.138 52.114.14.237
Akamai Technologies, Inc.	
e12370.g.akamaiedge.net, cdn.odc.officeapps.live.com.edgekey.net, cdn.odc.officeapps.live.com.	104.120.112.79

7 Conclusion and Future Work

VoIP applications are here to stay. Their tremendous use in business and education raises some security and privacy concerns for users. This paper presented an elaborate forensic analysis of Microsoft Teams in terms of different data localities, namely memory, disk-space and network. Nowadays, companies ensure implementation of security best practices in their applications to build and maintain user trust. Our aim was to analyze Microsoft Teams with its security mechanisms in place and see what critical user information can still be extracted. We presented an in-depth memory forensic analysis of the application, extracting email addresses, profile photos, user account IDs, AES keys, exchanged (including deleted) messages, text/media files, URLs, meeting information and more, in plaintext. Moreover, analysis of Windows Registry keys related to Microsoft Teams revealed some configuration information related to the user account. Network traffic of Teams was encrypted; however, information regarding server domains, their associations, IP addresses and relevant timestamps were investigated. All extracted artifacts can be corroborated holistically to reconstruct events in a forensically sound manner.

Research in the area of forensic analysis of recent VoIP applications is limited; therefore, it would be interesting to extend our research to other videoconferencing applications such as Google Hangouts, BlueJeans and Adobe Connect. Additionally, a comprehensive comparative analysis of the top VoIP applications can be done to highlight the security posture of each application individually as well as VoIP security as a broader communication platform. Secondly, other Operating Systems (such as macOS, Linux, Android and iOS) can be considered for forensic artifact investigation.

Acknowledgment. This study is supported with research funds from Research Incentive Funds (R19044) and Provost Research Fellowship Award (R20093), Zayed University, United Arab Emirates.

References

1. 20 Astonishing Video Conferencing Statistics for 2021. Digital in the Round, 10 May 2021. digitalintheround.com/video-conferencing-statistics/
2. Best Video Conferencing Software in 2020 | G2. *G2*. https://www.g2.com/categories/video-conferencing
3. Lorenz, T.: 'Zoombombing': When Video Conferences Go Wrong. The New York Times, 20 March 2020
4. Andrew Lewis, J.: Video Conferencing Technology and Risk. www.csis.org, 03 December 2020. https://www.csis.org/analysis/video-conferencing-technology-and-risk
5. Zorz, Z.: Cisco WebEx vulnerabilities may enable attackers to covertly join meetings. Help Net Security, 19 November 2020. https://www.helpnetsecurity.com/2020/11/19/cisco-webex-vulnerabilities-attackers-covertly-join-meetings/
6. Gode, S.: Video Conferencing Security Issues and Opportunities. Unify Square. https://www.unifysquare.com/blog/video-conferencing-security-issues-and-opportunities/
7. Warren, T.: Microsoft Teams usage jumps to 145 million daily active users. The Verge, 27 April 2021. https://www.theverge.com/2021/4/27/22406472/microsoft-teams-145-million-daily-active-users-stats
8. Security guide for Microsoft Teams - Microsoft Teams. docs.microsoft.com. https://docs.microsoft.com/en-us/microsoftteams/teams-security-guide#encryption-for-teams
9. Sgaras, C., Kechadi, M.-T., Le-Khac, N.-A.: Forensics Acquisition and Analysis of instant messaging and VoIP applications. In: Computational Forensics, pp. 188–199 (2015)
10. Yang, T.Y., Dehghantanha, A., Choo, K.R., Muda, Z.: Windows instant messaging app forensics: Facebook and Skype as case studies. PLOS ONE **11**(3), e0150300 (2016). https://doi.org/10.1371/journal.pone.0150300
11. Tandel, H., Rughani, P.H.: Forensic analysis of asterisk-FreePBX based VoIP server. Int. J. Emerg. Res. Manage. Technol. **6**, 2278–9359 (2018). https://doi.org/10.23956/ijermt.v6i8.133
12. Dargahi, T., Dehghantanha, A., Conti, M.: Forensics analysis of android mobile VoIP Apps. In: Contemporary Digital Forensic Investigations of Cloud and Mobile Applications, pp. 7–20 (2017). https://doi.org/10.1016/b978-0-12-805303-4.00002-2
13. Sha, M.M., Manesh,T., Abd El-atty, S.M.: VoIP forensic analyzer. Int. J. Adv. Comput. Sci. Appl. **7**(1) (2016). https://doi.org/10.14569/ijacsa.2016.070116
14. Nicoletti, M., Bernaschi, M.: Forensic analysis of Microsoft Skype for Business. Digit. Investig. **29**, 159–179 (2019). https://doi.org/10.1016/j.diin.2019.03.012
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. Alisabeth, C., Restu Pramadi, Y.: Forensic analysis of instagram on android. IOP Conf. Ser. Mater. Sci. Eng. **1007**, 012116 (2020). https://doi.org/10.1088/1757-899x/1007/1/012116

17. Awan, F.A.: Forensic examination of social networking applications on smartphones. In: 2015 Conference on Information Assurance and Cyber Security (CIACS), pp. 36–43 (2015). https://doi.org/10.1109/CIACS.2015.7395564
18. Zhang, H., Chen, L., Liu, Q.: Digital forensic analysis of instant messaging applications on android smartphones. In: 2018 International Conference on Computing, Networking and Communications (ICNC), pp. 647–651 (2018). https://doi.org/10.1109/ICCNC.2018.8390330