Journal of Information Systems Engineering and Management
2025, 10(20s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Forensics Analysis of Browser-Based GoToMeeting Clients: Uncovering Memory and Browser Artefacts

Subodh Kant Tiwari[1], Dr. Neeti Kashyap[2], Dr. Prachi[3]
[1,2,3]*Dept. of Computer Science & Engineering, The NorthCap University* Gurugram, Haryana, India
**Correspondence author E*-mail: *Subodh22csd005@ncuindia.edu*

ARTICLE INFO

Received: 19 Dec 2024

Revised: 29 Jan 2025

Accepted: 10 Feb 2025

ABSTRACT

In this paper, we address the method through memory forensics and browser forensics of recovering and searching hidden forensic evidence in a GoToMeeting session under a web browser-based (SaaS) platform. The goal of our research is to identify potential occurrences, such as meeting records (including meeting type, time zone, and duration), user details (such as username, display name, and email), participant details (such as display name and email id, join time, etc.), chat messages, notes shared during meetings, scheduled meeting details, and the AES key used for encrypting the contents. This will be done by exploring the techniques for acquiring and analysing the memory dumps and browser forensics. Particularly, we are considering the specific challenges and issues that one has to face when carrying out the forensic inspection of SaaS applications, such as GoToMeeting. Also, the findings of this study offer valuable insights into the efficacy of memory forensics and browser forensics in retrieving evidence from web-based video conferencing programs. This information may be useful for law enforcement and cyber security professionals engaged in a digital investigation, as well as for those who are implementing efficient security measures.

Keywords: GoToMeeting; Digital Forensics; Memory Forensics; Application Security; SaaS Forensics; Videoconferencing; Application security: Browser Forensics: Forensics Investigation: Application Security: Data Privacy

INTRODUCTION

As the world goes remote and hybrid with the rise of new work setups, the use of video conference applications has skyrocketed. As a result, user-focused apps including GoToMeeting, Zoom, Teams, Skype, and WebEx are fundamentally redefining the communication landscape. They foster a smoother flow of inter-staff teamwork, broaden productivity in various industries, and create a more integrated work environment. Specifically, the applications have demonstrated that they reshape the 21st-century communication environment by overcoming geographical barriers and promoting real-time interactions. Further, their influence extends into the nonprofessional environment, especially in education, where they create a more inclusive, collaborative, and fun learning environment.

Video conferencing is regularly used for group and solo activities. It's a critical tool in the everyday operation of 45% of teams, ensuring that 99% of users interact more effectively. Although 65% of conferences are limited to audio, 90% of users express themselves in video more freely. Videoconferencing is related to 51% of businesses being considered innovative and 47% of users saving money on travel. The market value is $6.03 billion in 2021(M, 2024; Team, 2023; Belyh, 2023).

Recent years have been marked by a tremendous rise in digital communication platforms that create new challenges in terms of cybersecurity. A recent issue of 'Zoom bombing', where unauthorized users intrude Zoom meetings and disrupt them by sharing inappropriate content, has been actively discussed in society. This issue was noted when one of the public Zoom webinars co-hosted by Chipotle Mexican Grill, Inc. was shut down by a user who displayed pornographic material to hundreds of viewers (T. Lorenz, 2020.). Additionally, social media have also had a bunch of significant breaches. In 2012, one of the most famous breaches was when hackers stole the account credentials of

6.5 million LinkedIn users and published them on a Russian forum.(2012 LinkedIn Breach, 2022).

GoToMeeting's significance in the global video conferencing software market can be found in the most recent market share analysis. As current data indicates as illustrated in Figure 1, GoToMeeting boasts the third-largest market share, accounting for 9.31% of the global market. The only two applications with a larger share include the market leader Zoom, with 57.24%, and Microsoft Teams, with a 24.57% share (Statista, 2024).

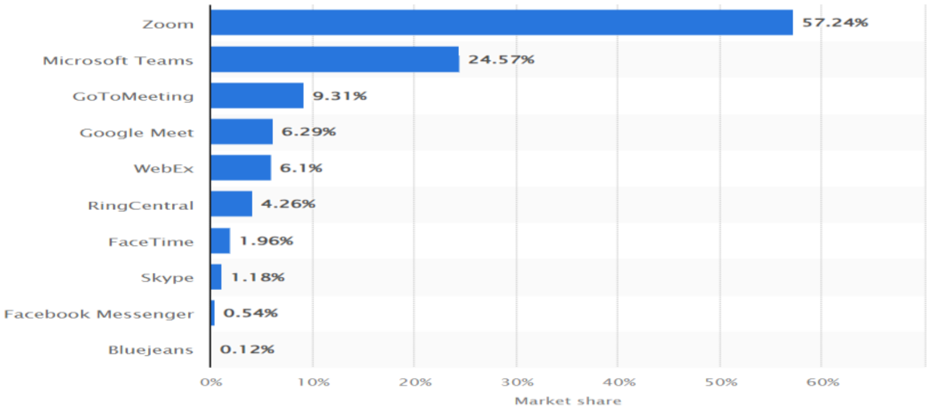


Fig. 1. Global market share of video conferencing software in 2023, categorized by program. (Statista, 2024)

Based on this information, the need for a strong security posture appears to be justified, considering the vast number of people and companies using GoToMeeting. Indeed, any of the aforementioned illicit activities are theoretically possible, given the global prevalence of GoToMeeting.

From the existing literature, several forensic researches have been conducted on different browser-based meeting applications such as Zoom, Google Meet, Cisco Webex, Microsoft Teams, etc.,. However, to my knowledge, no forensic research has been conducted on GoToMeeting's browser-based client. This is because every application is heterogeneous with the other; therefore, separate research must be carried out on each one of the applications individually.

Forensic research is paramount in countering the threat. It is feasible to determine potential forensic artefacts in the memory space of GoToMeeting, which enables the investigator to Gain valuable insights into past events which includes meeting records (including meeting type, timezone, and duration), user details (such as username, display name, and email), participant details (such as display name and email creation date), AES key used for content encryption, chat messages, shared notes during meetings, application usage traces, browser used for running application, scheduled meeting details and other browser based evidences in bookmarks, cookies, cache, sessions etc.

This paper is intended for two primary audiences:

1. Law enforcement professionals involved in digital investigations and cybersecurity, who can employ it to execute the memory and browser forensics strategies for analyzing Software as a Service (SaaS) Web-based video conferencing apps.

2. Web-based application (SaaS) developers and security specialists who are ensuring that adequate security features are incorporated in the development of the applications.

The structure of the paper is as follows. Section 2 discusses the previous related works and contributions. Section 3 explains the research methodology and the experimental setup and settings. Section 4 presents the results and findings of memory and Browser forensics analysis. Section 5 present the conclusion and future works.

RELATED WORKS

Web-based applications have become integral to modern digital interactions, driven by the agile nature of Service Oriented Architecture (SOA). However, the dynamic nature of web applications poses challenges in implementing robust security controls, thereby expanding the attack surface and raising concerns about privacy and security (Akremi et al., 2019).

In a study performed by (Iqbal et al., 2022), memory forensics techniques were used to identify meeting details, user information, communication records, and other relevant data from Google Meet. It emphasizes the significance of extracting digital evidence from memory artefacts for forensic investigations. He performed forensics analysis of Google Meet across multiple browser platforms i.e. Firefox, Chrome, and Edge. In a study by (Azhar et al., 2022) describes how to inspect and potentially taint artefacts from two popular video conferencing apps, Google Meet, and Microsoft Teams, using forensic techniques. Regarding the receptacle, a large body of research has documented the use of conventional cyberspace forensic tools to retrieve data from the memory, network, browser, and registry, among other sources. These results aim to verify the increased security and dependability of the program as an online video conference tool.

Barradas et al. (2019) conducted memory analysis to extract communication records from various mobile applications and web clients using string analysis. Forensic analysis of video conferencing applications has gained attention in recent research. Mahr et al. (2021) conducted an in-depth forensic analysis of Zoom, extracting artefacts such as chats, passwords, contacts, email addresses, and cache from client databases.

Khalid et al. (2021) focused on the forensic analysis of the Cisco WebEx application, further expanding the scope of research in this domain. Yang et al. (2016) conducted a thorough forensic examination of the Windows-based Skype app, revealing critical artefacts related to installation information, login details, conversations, and exchanged files. Their study highlighted the importance of examining application folders even after uninstallation to reconstruct forensic artefacts. Similarly, Nicoletti and Bernaschi. (2019)used a case study methodology to examine Skype for Business, emphasizing communication architecture, protocols, and VoIP artefacts as potential sources of forensic evidence.

Motyliński et al. (2020) delved into the digital forensic analysis of Discord applications, emphasizing artefact acquisition and analysis to understand user activities and interactions within the platform. (Walnycky et al.,2015) conducted device and forensic network analysis of social messaging applications on Android, revealing the extraction of artefacts from application data folders and highlighting the transmission of user data over networks in plaintext format. McFadden et al. (2020) conducted a forensic investigation of microblogging sites, using Tumblr and Pinterest as case studies to extract forensic artefacts that could be utilized in legal cases. Fernández-Álvarez and Rodríguez. (2022) utilized the Telegram desktop client's open-source code to retrieve frequently occurring artefacts from memory, such as contacts, communication logs, and user account data. Using the source code, they were able to reconstruct Telegram's Unified Modeling Language (UML) diagram, which let them determine how the objects of applications reside in memory. This provided a precise signature to look for, greatly reducing the possibility of mistakes and false findings in the extracted artefacts. The methodology that has been developed is a useful strategy for inquiries concerning open-source software. It doesn't apply to proprietary software, though.

(Cloyd et al.,2018) Their study found that a Facebook web browsing session leaves residual data on a browser. For Chrome, only 46% of the actions performed during those sessions made it back to their corresponding browser, while Firefox and Internet Explorer retained 61% and 52%, respectively. Marrington et al. (2012) examined the validity of privacy assertions by analysing Chrome in portable browser mode (in normal and private modes). According to the study, evidence of web browsing activity may still be recoverable from the disk of the host, warning that portable browsers may not actually be the best tool for users who wish to hide their past Internet usage. Oh et al. (2011) In a forensic study of web browsers, noted that the analysis typically involves log parsing only. Because artefacts' are often spread out across locations, they claimed a multi-method approach—integrating timeline analysis, search history analysis, user activity analysis, and recover of deleted data—was needed for complete investigation.

One of the most essential tools to access online services is a web browser. Rasool and Zunera (2020) stated in their report that, there were 4.39 Billion active internet users in 2019. However, due to its frequent usage by cybercriminals in illegal activities, it is vital for a digital forensic investigator to collect, extract and analyse any relevant data from each of the browsers encountered during an investigation (Beebe 2009; Paligu & Varol 2020). A forensic analysis of Brave, Google Chrome, Microsoft Edge and Mozilla Firefox while in private mode Evidence extraction from the hard disk and RAM were performed using tools like Bulk Extractor, String and Volatility in order to obtain a copy of search history, cookies, temporary files and Browser activities (Hughes et al.,2021).In study by Tsalis et al.(2017) forensic investigation Google Chrome, Mozilla Firefox, Internet Explorer and Opera were taken into consideration , and in order to forensic evidence collection related to browsing session activity to keep from being recoverable as a safeguard RAMDisk software was used.

RESEARCH METHODOLOGY AND EXPERIMENT SETUP

The server hosting the SaaS application is the best source of forensic evidence. However, because of international legal boundaries, such an acquisition is typically not feasible. The next best source of forensic evidence is to take a memory dump of the device and perform browser forensics on which the GoToMeeting web client was running. In our instance, a client's device was used in a controlled test environment for the forensic analysis of the GoToMeeting web client.

The research methodology for forensic analysis of the GoToMeeting web client consists of three stages, as follows:

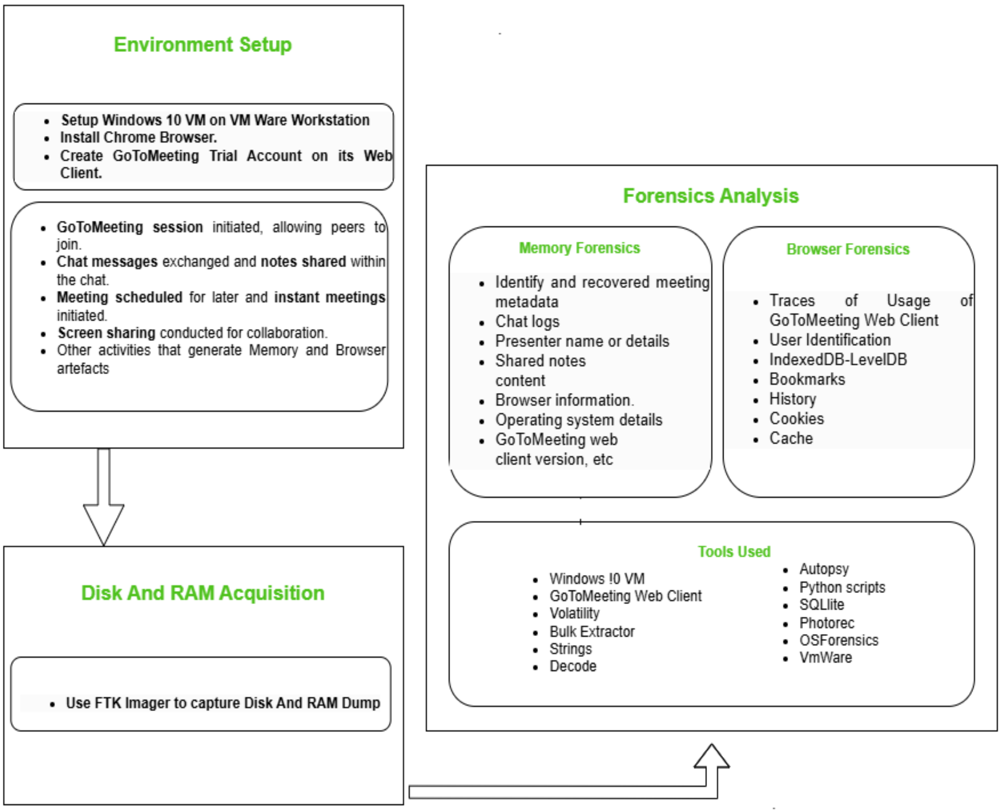

Environment Setup
Setup Windows 10 VM on VM Ware Workstation
Install Chrome Browser.
Create GoToMeeting Trial Account on its Web Client.
GoToMeeting session initiated, allowing peers to join.
Chat messages exchanged and notes shared within the chat.
Meeting scheduled for later and instant meetings initiated.
Screen sharing conducted for collaboration.
Other activities that generate Memory and Browser artefacts
Disk And RAM Acquisition
Use FTK Imager to capture Disk And RAM Dump
Forensics Analysis
Memory Forensics
Identify and recovered meeting metadata
Chat logs
Presenter name or details
Shared notes content
Browser information.
Operating system details
GoToMeeting web client version, etc
Browser Forensics
Traces of Usage of GoToMeeting Web Client
User Identification
IndexedDB-LevelDB
Bookmarks
History
Cookies
Cache
Tools Used
Windows !0 VM
GoToMeeting Web Client
Volatility
Bulk Extractor
Strings
Decode
Autopsy
Python scripts
SQLlite
Photorec
OSForensics
VmWare

Fig 2 Research Methodology and Environment Setup

a) Setting Up Controlled Environment for Research

The initial step of the research development is setting up a controlled environment that will allow for repeatable experiments. This step would involve creating a virtual machine using Windows 10 iso on a VMware workstation (VMware, 2024) with 3GB of RAM and 30G B of disk space. The virtual machine creates isolation, ensuring the replication of the experiment regardless of the surrounding environment. Afterward, a temporary GoToMeeting account would be created on the virtual machine to simulate the user experience. Next, since Chrome is the most common platform of access to GoToMeeting, it is installed on the virtual machine to simulate user experience. This aspect would culminate principles of realism. From the VM, a GoToMeeting web client session was initiated and allow the peers to join the meeting. Several user activities were performed which included chat messages, in-chat note sharing, scheduling a meeting for later, performing instant meetings, screen sharing, etc. that generated memory and browser artefact that will be relevant for our research.

b) Disk and Memory Acquisition

After the simulated meeting session ended, memory acquisition was the next focus area. Memory Acquisition was done using FTK Imager(FTK Imager, 2024), a validated forensic memory acquisition tool to obtain a full physical memory dump and disk image for browser forensics of the VM. Hashes of the memory dumps and disk image were calculated to ensure the integrity of the evidence. The acquisition process and any relevant technical details should be documented for future reference.

c) Forensics Analysis for Memory and Browser artefacts

The core of the said research is the analysis of the memory and disk image acquired. The goal is to find the possible forensic artefacts associated with the activity in GoToMeeting in the subsequent user's actions. Such artefacts could be the following: the meeting metadata; chat logs; presenter name or details; shared notes content; and browser information. Moreover, the relevant research artefacts could, probably, include details about the operating system, GoToMeeting web client version, etc., or any other artefacts that could be directly relevant i.e. and other browser-based evidences in bookmarks, cookies, cache, sessions etc. The memory analysis is performed with a multi-faceted tactic to ensure its highest effect on the data and its final analysis. For this task, the Strings (Strings,2024) tools are used. Some keywords and phrases related to GoToMeeting are used to search the memory image to help identify more apparent artefacts. It allows finding some of the artefacts with less intensive search techniques. Also, a more intensive search approach may be conducted using the OS Forensics too(OSForensic,2024) and Autopsy (Autopsy, 2024) to identify other potential artefacts. Volatility (Volatility, 2024) tool is used to identify which browser is used for accessing GoToMeeting web client. Bulk-Extractor (Bulk Extractor, 2024) tool is used to extract the 128-bit AES key. Browser forensics is performed to find the browser artefacts using Autopsy, FTK, And OSForensics

EXPERIMENT AND RESULTS

a) Memory Forensics

We examined the memory dumps produced by FTK Imager to look for artefacts using Photorec, Volatility, Strings, OS Forensics, and Bulk-Extracter etc. and Browser forensics using Autopsy, FTK, OSForensics etc. All of the tools we used for our forensic analysis are listed in Table II, along with the relevant versions and usage. Five basic forensic artefacts were our main focus, namely communication content, communication history, contacts, encryption keys, and passwords. Memory forensics is a more difficult process than static media (Simon and Slay, 2010). A device's memory holds a multitude of information about the programs and processes that are currently operating. Researchers are very interested in this topic since it may include unencrypted material in memory that is typically encrypted and kept on a hard drive.

i Traces of GoToMeeting Usage

While performing the forensic analysis, Volatility's Pstree plugin was used to identify that a Google Chrome browser was used in the system. Subsequently, the associated process's memory related to the Chrome process was dumped via Volatility's memmap plugin. We conducted a keyword search in the dumped process using terms related to GoToMeeting and found a positive hit. Therefore, we finally confirmed that the user was indeed actively interacting with GoToMeeting via Chrome

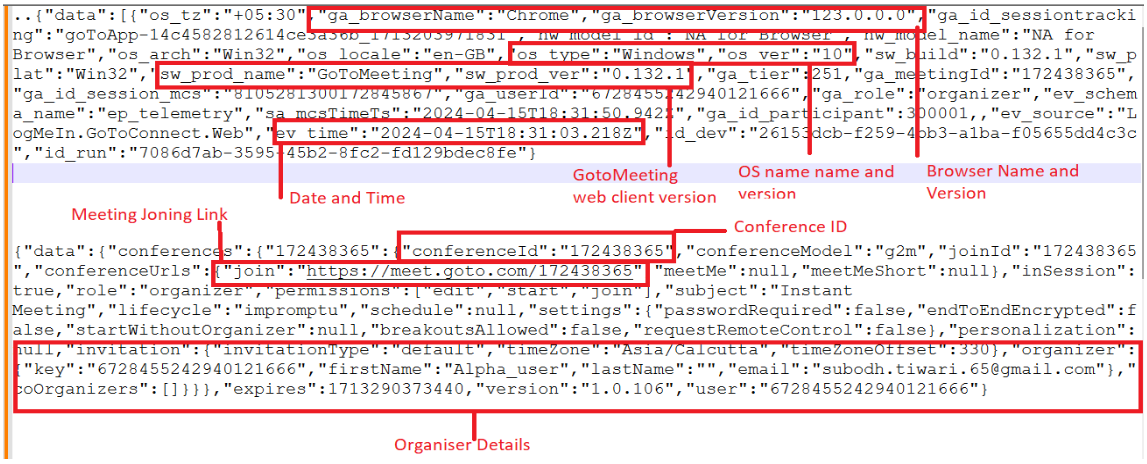
Table 1. Tools used for forensic analysis of GoToMeeting.

Tool	Software Version	Usage
Windows 10 VM	10	Test Environment
GoToMeeting Web Client	0.132.1	Web client for video conferencing to check for forensic artefacts
Volatility	3.0	Analysis of memory dumps
Bulk Extractor	2.1	Analysis of memory dumps
FTK Imager	4.7.1	Create a forensics image of the memory dump
OSForensics	10.0.1016	Analysis of memory dumps
Decode	5.6	timestamp decoding

Strings	2.54	String extraction and searching
Photorec	7.1	Carve profile picture from memory dump

ii Identify Meeting Records

We conducted the manual analysis on the acquired Ram dump using string and keyword searches. With this rigorous analysis, we successfully identify the information related to the meeting record as illustrated in Figure 3, which includes the name of the meeting, the type of meeting, the meeting ID, the number of participants in the meeting, the GoToMeeting web client version, details about the browser name and version used by the suspected user, and details of the host operating system, as well as the user ID of the meeting organizer.



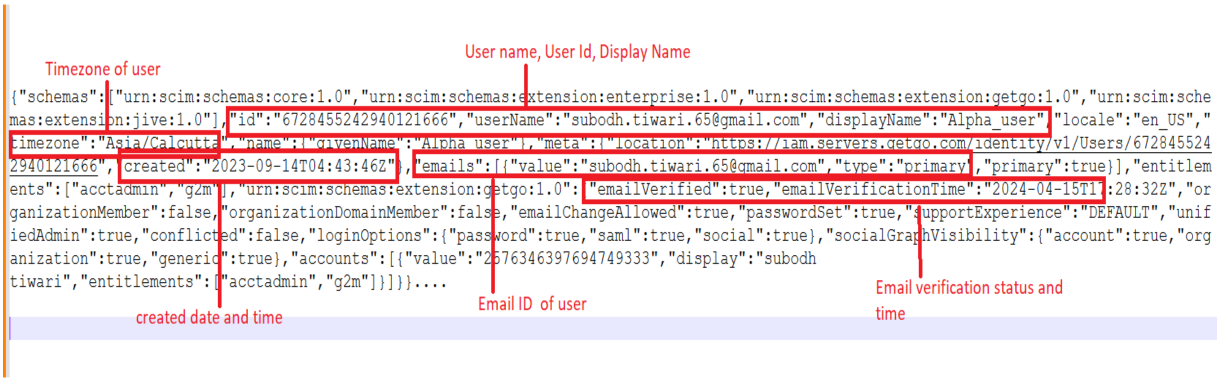
```
..{"data":[{"os_tz":"+05:30","ga_browserName":"Chrome","ga_browserVersion":"123.0.0.0","ga_id_sessiontracki
ng":"goToApp-14c4582812614ce3a36b_1713203971831","hw_model_id":"NA for Browser","hw_model_name":"NA for
Browser","os_arch":"Win32","os_locale":"en-GB","os_type":"Windows","os_ver":"10","sw_build":"0.132.1","sw_p
lat":"Win32","sw_prod_name":"GoToMeeting","sw_prod_ver":"0.132.1","ga_tier":251,"ga_meetingId":"172438365",
"ga_id_session_mcs":"8105281300172845867","ga_userId":"6728455242940121666","ga_role":"organizer","ev_schem
a_name":"ep_telemetry","sa_mcsTimeTs":"2024-04-15T18:31:50.942Z","ga_id_participant":300001,,"ev_source":"L
ogMeIn.GoToConnect.Web","ev_time":"2024-04-15T18:31:03.218Z","id_dev":"26153dcb-f259-4bb3-a1ba-f05655dd4c3c
","id_run":"7086d7ab-3595-45b2-8fc2-fd129bdec8fe"}
```

```
{"data":{"conferences":{"172438365":{"conferenceId":"172438365","conferenceModel":"g2m","joinId":"172438365
","conferenceUrls":{"join":"https://meet.goto.com/172438365","meetMe":null,"meetMeShort":null},"inSession":
true,"role":"organizer","permissions":["edit","start","join"],"subject":"Instant
Meeting","lifecycle":"impromptu","schedule":null,"settings":{"passwordRequired":false,"endToEndEncrypted":f
alse,"startWithoutOrganizer":null,"breakoutsAllowed":false,"requestRemoteControl":false},"personalization":
null,"invitation":{"invitationType":"default","timeZone":"Asia/Calcutta","timeZoneOffset":330},"organizer":
{"key":"6728455242940121666","firstName":"Alpha_user","lastName":"","email":"subodh.tiwari.65@gmail.com"},"
coOrganizers":[]}}},"expires":1713290373440,"version":"1.0.106","user":"6728455242940121666"}
```

Fig 3. Meeting Record

iii User details

We use the PhotoRec (CGSecurity,2024) tool to carve the profile picture of a GoToMeeting user from the acquired Ram Dump we find out that the profile pictures are not stored in encrypted format in memory. Besides, there was a kind of exhaustive search that was conducted during the memory analysis, which gave a lot of information involving users. It includes the username, the email ID along with a field indicating whether the provided email ID has been verified or not, the date on which the user account was created, the user's display name, and the user's timezone as illustrated in Figure 4.

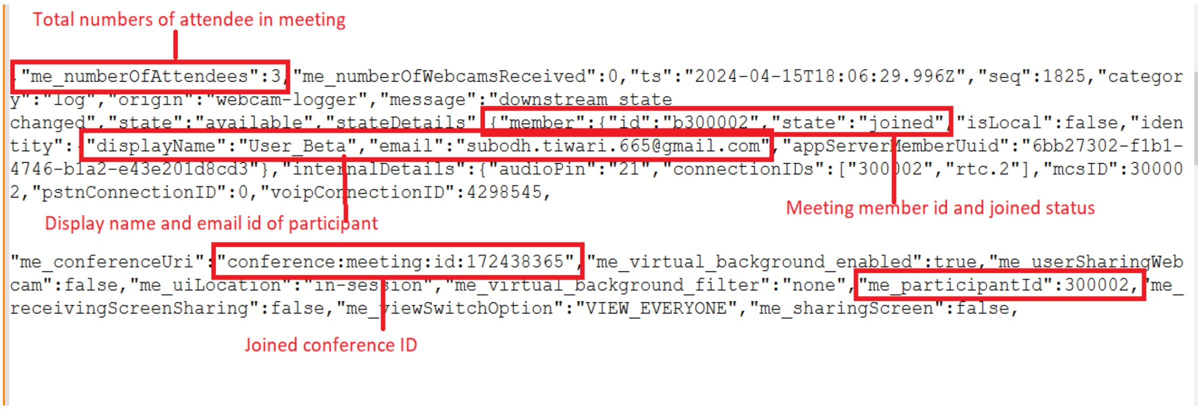


```
{"schemas":["urn:scim:schemas:core:1.0","urn:scim:schemas:extension:enterprise:1.0","urn:scim:schemas:extension:getgo:1.0","urn:scim:sche
mas:extension:jive:1.0"],"id":"6728455242940121666","userName":"subodh.tiwari.65@gmail.com","displayName":"Alpha_user","locale":"en_US","
timezone":"Asia/Calcutta","name":{"givenName":"Alpha_user"},"meta":{"location":"https://iam.servers.getgo.com/identity/v1/Users/672845524
2940121666","created":"2023-09-14T04:43:46Z"},"emails":[{"value":"subodh.tiwari.65@gmail.com","type":"primary","primary":true}],"entitlem
ents":["acctadmin","g2m"],"urn:scim:schemas:extension:getgo:1.0":{"emailVerified":true,"emailVerificationTime":"2024-04-15T17:28:32Z","or
ganizationMember":false,"organizationDomainMember":false,"emailChangeAllowed":true,"passwordSet":true,"supportExperience":"DEFAULT","unif
iedAdmin":true,"conflicted":false,"loginOptions":{"password":true,"saml":true,"social":true},"socialGraphVisibility":{"account":true,"org
anization":true,"generic":true},"accounts":[{"value":"2576346397694749333","display":"subodh
tiwari","entitlements":["acctadmin","g2m"]}]}}....
```

Fig 4 User Details

iv Participant details

All the email IDs were extracted from the memory dump. After that, each of these email IDs was searched individually within the memory dump, making it possible to ascertain exhaustive information regarding every participant. These details as illustrated in Figure 5, included the display name, the email ID of the participant, the meeting ID they joined, whether they used a virtual background, and the number of participants in the joined meeting.



Total numbers of attendee in meeting
Display name and email id of participant
Meeting member id and joined status
Joined conference ID

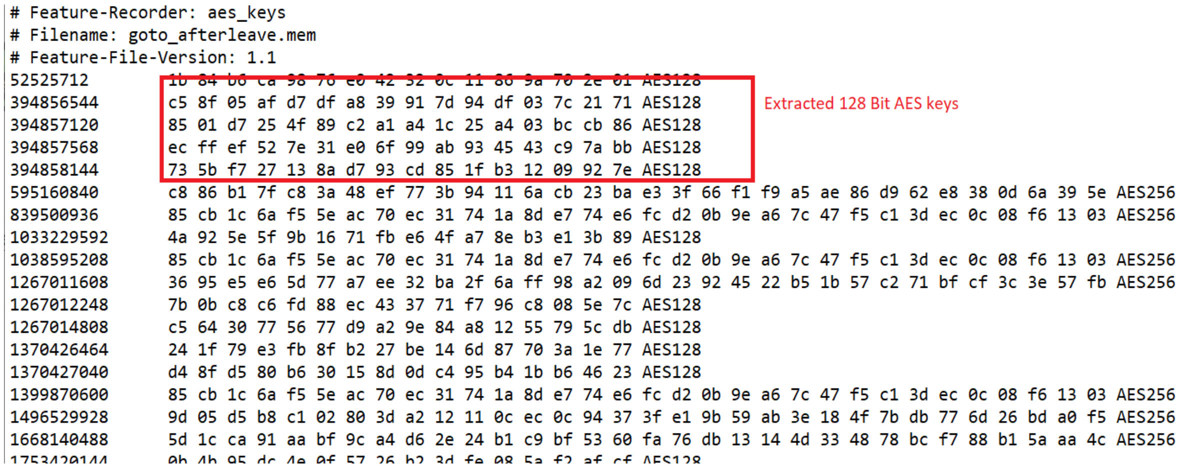
```
"me_numberOfAttendees":3,"me_numberOfWebcamsReceived":0,"ts":"2024-04-15T18:06:29.996Z","seq":1825,"categor
y":"log","origin":"webcam-logger","message":"downstream state
changed","state":"available","stateDetails":{"member":{"id":"b300002","state":"joined","isLocal":false,"iden
tity":{"displayName":"User_Beta","email":"subodh.tiwari.665@gmail.com","appServerMemberUuid":"6bb27302-f1b1-
4746-b1a2-e43e201d8cd3"},"internalDetails":{"audioPin":"21","connectionIDs":["300002","rtc.2"],"mcsID":30000
2,"pstnConnectionID":0,"voipConnectionID":4298545,

"me_conferenceUri":"conference:meeting:id:172438365","me_virtual_background_enabled":true,"me_userSharingWeb
cam":false,"me_uiLocation":"in-session","me_virtual_background_filter":"none","me_participantId":300002,"me_
receivingScreenSharing":false,"me_viewSwitchOption":"VIEW_EVERYONE","me_sharingScreen":false,
```

Fig 5 Participant Details

v *AES keys used by the platform to encrypt the data*

According to GoToMeeting's official website, the AES with a 128-bit key is used by the platform to encrypt the data sent. We could extract the corresponding AES keys on analysis as illustrated in Figure 6.

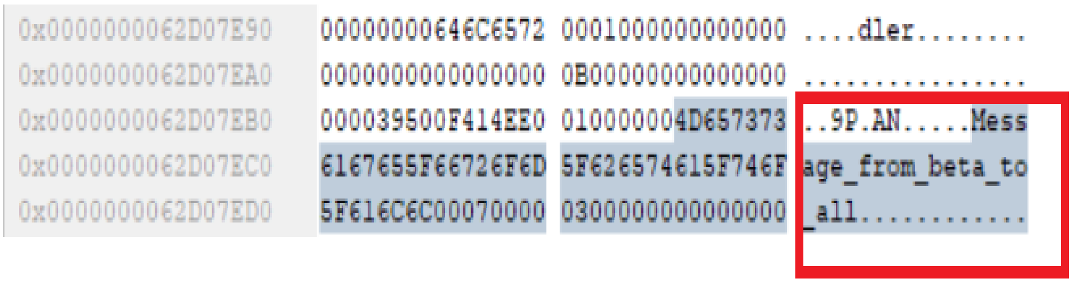


```
# Feature-Recorder: aes_keys
# Filename: goto_afterleave.mem
# Feature-File-Version: 1.1
52525712        1b 84 b6 ca 98 76 e0 42 32 0c 11 86 9a 70 2e 01 AES128
394856544       c5 8f 05 af d7 df a8 39 91 7d 94 df 03 7c 21 71 AES128
394857120       85 01 d7 25 4f 89 c2 a1 a4 1c 25 a4 03 bc cb 86 AES128
394857568       ec ff ef 52 7e 31 e0 6f 99 ab 93 45 43 c9 7a bb AES128
394858144       73 5b f7 27 13 8a d7 93 cd 85 1f b3 12 09 92 7e AES128
595160840       c8 86 b1 7f c8 3a 48 ef 77 3b 94 11 6a cb 23 ba e3 3f 66 f1 f9 a5 ae 86 d9 62 e8 38 0d 6a 39 5e AES256
839500936       85 cb 1c 6a f5 5e ac 70 ec 31 74 1a 8d e7 74 e6 fc d2 0b 9e a6 7c 47 f5 c1 3d ec 0c 08 f6 13 03 AES256
1033229592      4a 92 5e 5f 9b 16 71 fb e6 4f a7 8e b3 e1 3b 89 AES128
1038595208      85 cb 1c 6a f5 5e ac 70 ec 31 74 1a 8d e7 74 e6 fc d2 0b 9e a6 7c 47 f5 c1 3d ec 0c 08 f6 13 03 AES256
1267011608      36 95 e5 e6 5d 77 a7 ee 32 ba 2f 6a ff 98 a2 09 6d 23 92 45 22 b5 1b 57 c2 71 bf cf 3c 3e 57 fb AES256
1267012248      7b 0b c8 c6 fd 88 ec 43 37 71 f7 96 c8 08 5e 7c AES128
1267014808      c5 64 30 77 56 77 d9 a2 9e 84 a8 12 55 79 5c db AES128
1370426464      24 1f 79 e3 fb 8f b2 27 be 14 6d 87 70 3a 1e 77 AES128
1370427040      d4 8f d5 80 b6 30 15 8d 0d c4 95 b4 1b b6 46 23 AES128
1399870600      85 cb 1c 6a f5 5e ac 70 ec 31 74 1a 8d e7 74 e6 fc d2 0b 9e a6 7c 47 f5 c1 3d ec 0c 08 f6 13 03 AES256
1496529928      9d 05 d5 b8 c1 02 80 3d a2 12 11 0c ec 0c 94 37 3f e1 9b 59 ab 3e 18 4f 7b db 77 6d 26 bd a0 f5 AES256
1668140488      5d 1c ca 91 aa bf 9c a4 d6 2e 24 b1 c9 bf 53 60 fa 76 db 13 14 4d 33 48 78 bc f7 88 b1 5a aa 4c AES256
1753420144      0b 4b 95 dc 4e 0f 57 26 b2 3d fe 08 5a f2 af cf AES128
```

Fig 6 Extracted AES Keys

vi *Sent & Received messages*

A string search was done in the memory dump to identify text in a sent or received message. The manual search enabled the identification of the message text as illustrated in Figure 7, however, associated metadata such as timestamps, sender and receiver details, etc, could not be found. This implies that while the actual text of the in-meeting may be seen as plain text, metadata such as concerns these messages may be encrypted during the transmission, which can pose difficulties to the forensic investigator.

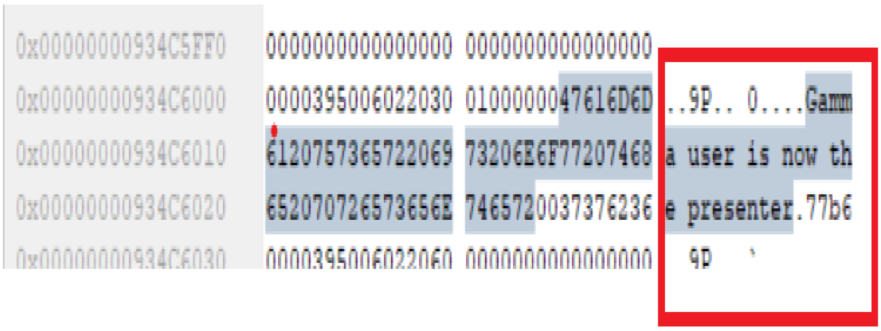


```
0x0000000062D07E90   00000000646C6572 0001000000000000 ....dler........
0x0000000062D07EA0   0000000000000000 0B00000000000000 ................
0x0000000062D07EB0   000039500F414EE0 010000004D657373 ..9P.AN.....Mess
0x0000000062D07EC0   6167655F66726F6D 5F626574615F746F age_from_beta_to
0x0000000062D07ED0   5F616C6C00070000 0300000000000000 _all............
```

Fig 7 Received Message Text

vii *Presenter details*

A more focused manual search was carried out to identify the traces of who presented or shared their screen during the meeting. After the analysis, it was found that the only information which was extractable was the display name as illustrated in Figure 8, of the person presenting/sharing the screen. Other relevant metadata like the user's email, the time when the presentation was presented, its duration, etc. were not found. This makes us conclude that while the display name is saved in clear text, other metadata is most probably encrypted and stored in the memory, which shows a higher level of protection implemented and more challenges to forensic investigators.

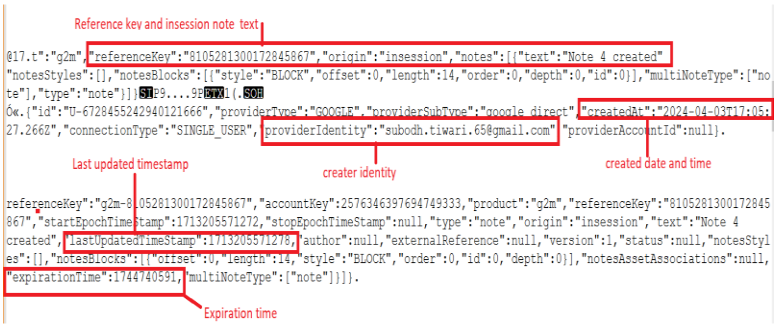


```
0x0000000000934C5FF0  0000000000000000 0000000000000000
0x0000000000934C6000  0000395006022030 0100000047616D6D  ..9P.. 0....Gamm
0x0000000000934C6010  6120757365722069 73206E6F77207468  a user is now th
0x0000000000934C6020  652070726573656E 7465720037376236  e presenter.77b6
0x0000000000934C6030  0000395006022060 0000000000000000    9P   `
```

Fig 8 Presenter Display Name

viii In-meeting note

GoToMeeting provides a feature of in-meeting notes that enables the organizer to create or update notes during the meeting. An exhaustive keyword search was made to identify the traces of these in-meeting. After a comprehensive analysis, as illustrated in Figure 9, we were able to find the content of the notes and all the associated metadata like the creator ID, email of the creator, the time last updated, and the time the note was created. These results could be used potentially for artefacts from the forensic point of view.



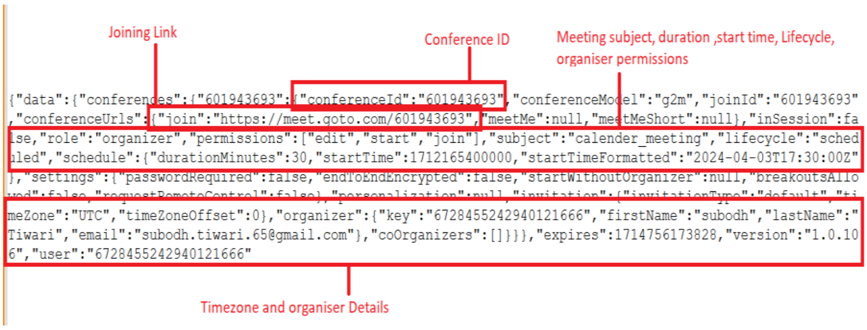
```
@17.t":"g2m","referenceKey":"8105281300172845867","origin":"insession","notes":[{"text":"Note 4 created"
"notesStyles":[],"notesBlocks":[{"style":"BLOCK","offset":0,"length":14,"order":0,"depth":0,"id":0}],"multiNoteType":["no
te"],"type":"note"}]}SIP9....9PETX1(.SOH
Ó«.{"id":"U-6728455242940121666","providerType":"GOOGLE","providerSubType":"google_direct","createdAt":"2024-04-03T17:05:
27.266Z","connectionType":"SINGLE_USER","providerIdentity":"subodh.tiwari.65@gmail.com","providerAccountId":null}.
```

```
referenceKey":"g2m-8105281300172845867","accountKey":2576346397694749333,"product":"g2m","referenceKey":"8105281300172845
867","startEpochTimeStamp":1713205571272,"stopEpochTimeStamp":null,"type":"note","origin":"insession","text":"Note 4
created","lastUpdatedTimeStamp":1713205571278,"author":null,"externalReference":null,"version":1,"status":null,"notesStyl
es":[],"notesBlocks":[{"offset":0,"length":14,"style":"BLOCK","order":0,"id":0,"depth":0}],"notesAssetAssociations":null,
"expirationTime":1744740591,"multiNoteType":["note"]}]}.
```

Fig 9 In-Meeting Notes

ix Schedule Meeting Details

GoToMeeting also has feature scheduling meetings, which allow the arrangements of meetings scheduled at future times. To obtain information about these scheduled meetings, we conducted an exhaustive string analysis to identify traces of information related to these scheduled meetings. This thorough research was successfully identified and revealed all relevant information as illustrated in Figure 10, regarding the scheduled meetings. including the meeting name, duration, start time and date, and timezone. Also, we successfully identified the first and last name of the user who scheduled the meeting along with their email ID and the invitation link. From the perspective of digital forensics, these results may be important artefacts.



Joining Link
Conference ID
Meeting subject, duration ,start time, Lifecycle, organiser permissions

```
{"data":{"conferences":{"601943693":{"conferenceId":"601943693","conferenceModel":"g2m","joinId":"601943693"
,"conferenceUrls":{"join":"https://meet.goto.com/601943693","meetMe":null,"meetMeShort":null},"inSession":fa
lse,"role":"organizer","permissions":["edit","start","join"],"subject":"calender_meeting","lifecycle":"sched
uled","schedule":{"durationMinutes":30,"startTime":1712165400000,"startTimeFormatted":"2024-04-03T17:30:00Z"
},"settings":{"passwordRequired":false,"endToEndEncrypted":false,"startWithoutOrganizer":null,"breakoutsAllo
wed":false,"requestRemoteControl":false},"personalization":null,"invitation":{"invitationType":"default","ti
meZone":"UTC","timeZoneOffset":0},"organizer":{"key":"6728455242940121666","firstName":"subodh","lastName":"
Tiwari","email":"subodh.tiwari.65@gmail.com"},"coOrganizers":[]}}},"expires":1714756173828,"version":"1.0.10
6","user":"6728455242940121666"
```

Fig 10 Scheduled Meeting Details

The Table 2 outlines artefacts found through memory forensics analysis of GoToMeeting web client as well as the tools used to discover and recover the artefacts.

Table 2. Memory artefacts of GoToMeeting web Client

Artefacts	Details	Tool Used
Traces of GoToMeeting Usage	Evidence of user interaction with GoToMeeting, including browser usage and active processes.	Volatility, Strings
Meeting Metadata	Meeting Name, Meeting Type, Meeting ID, Number of Participants, GoToMeeting Web Client Version, Browser Name and Version, Host Operating System, User ID of the Meeting Organizer	Strings, OSForensics, Autopsy
User details	Username, Display Name, Email ID, Email Verification Status, Account Creation Date, User's Timezone. Display picture of user	Photorec, Strings, OSForensics, Autopsy
Participant Details	Display Name, Email ID, Meeting ID Joined, Virtual Background Usage, Number of Participants in the Meeting.	Strings, OSForensics, Autopsy
Sent and Received Messages	Message Text (actual content), Metadata (timestamps, sender and receiver details not found)	Strings, OSForensics, Autopsy
AES Key Used by Platform	The 128-bit AES key used for encrypting data sent during the meeting	Bulk Extractor
Presenter Details	Display Name of the Presenter, (other metadata like email, presentation time, and duration not found).	Strings, OSForensics, Autopsy
In-Meeting Notes	Content of Notes, Creator ID, Creator's Email, Time Last Updated, Time Note Created.	Strings, OSForensics, Autopsy
Scheduled Meeting Details:	Meeting Name, Duration, Start Time and Date, Timezone, User's First and Last Name, User's Email ID, Invitation Link.	Strings, OSForensics, Autopsy

a) *Browser Artefacts*

i *Traces of GoToMeeting Usage*

While performing the forensic analysis, Volatility's Pstree plugin was used to identify that a Google Chrome browser was used in the system. Subsequently, the associated process's memory related to the Chrome process was dumped via Volatility's memmap plugin. We conducted a keyword search in the dumped process using terms related to GoToMeeting and found a positive hit. Therefore, we finally confirmed that the user was indeed actively interacting with GoToMeeting via Chrome.

ii *Traces Of Usage*

During a forensic investigation of GoToMeeting Web Client, there are several artefacts stand out important to establish that they have been used and to identify the user. Key indicators include the JumpListIconsRecentClosed directories which contains icons for frequently visited and recently closed web applications. Others include Top Sites database which contain thumbnails of most visited sites. the Favicons database stores favicons of web pages and applications. GoToMeeting Web Client was identified under these directories which points toward their regular usage.

Further evidence of usage includes the presence of URLs for GoToMeeting Web Client in the Network Action Predictor SQLite database. Last accessed timestamps can be extracted from the Shortcuts SQLite database. Additionally, session data found in the Sessions folder provides applications uses confirmation. All the above-mentioned artefacts found at location "`C:\Users\[username]\AppData\Local\Google\Chrome\User`

`Data\Default”.` Also `“BrowsingTopicsSiteData”` also consist the traces of GoToMeeting.

iii User Identification

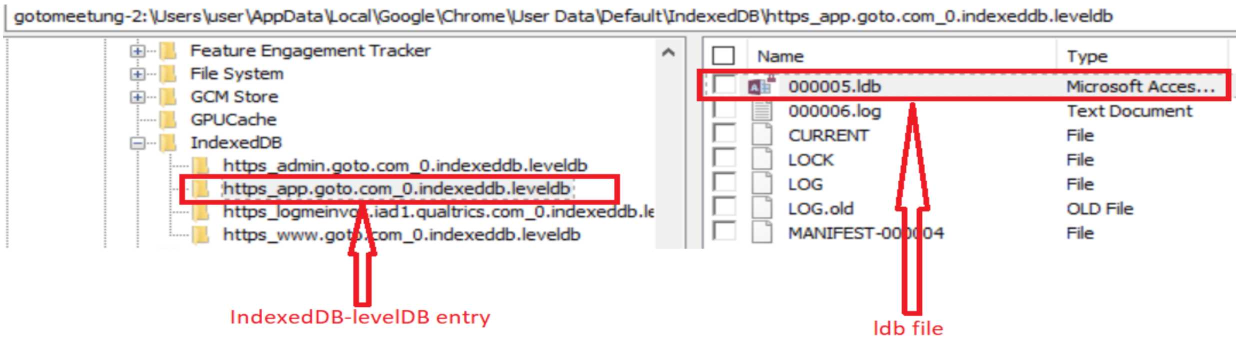
The email address related to the particular user profile may be derived from the Sessions folder Some of these session logs may also contain links to meeting that may have been conducted. Also, the display picture of Gmail account used to create the user GoToMeeting account can be found in `“C:\Users\[username]\AppData\Local\Google\Chrome\User Data\Default\Accounts\Avatar Images”.`

iv IndexedDB-levelDB

When a web application GoToMeeting is accessed via Google Chrome, an IndexedDB-levelDB database is created in the browser's data directory `“C:\Users\[username]\AppData\Local\Google\Chrome\User Data\Default\IndexedDB”,` for GoToMeeting created file is `“https_app.goto.com_0.indexeddb.leveldb”` as shown in Fig 11.These databases contain the records of the meeting logs and containing event logs, time stamp and serial number and any other information. Other databases can be processed as readable using, for instance, Autopsy, and Python scripts convert such databases to a json files which need to contain specific details regarding the case to be solved in forensic.

v Bookmarks

Bookmarks for GoToMeeting Web Client is stored at `“C:\Users\[username]\AppData\Local\Google\Chrome\User Data\Default\bookmarks”,` it contains GUID and the timestamp for adding each bookmark and, therefore, is a valuable source of the user’s interaction with the browser and bookmarking processes.



gotomeetung-2:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_app.goto.com_0.indexeddb.leveldb

- Feature Engagement Tracker
- File System
- GCM Store
- GPUCache
- IndexedDB
  - https_admin.goto.com_0.indexeddb.leveldb
  - https_app.goto.com_0.indexeddb.leveldb
  - https_logmeinvo.iad1.qualtrics.com_0.indexeddb.le
  - https_www.goto.com_0.indexeddb.leveldb

Name	Type
000005.ldb	Microsoft Acces...
000006.log	Text Document
CURRENT	File
LOCK	File
LOG	File
LOG.old	OLD File
MANIFEST-000004	File

IndexedDB-levelDB entry

ldb file

Fig. 11 IndexedDB-levelDb file created corresponding to GoToMeeting

vi Browser History

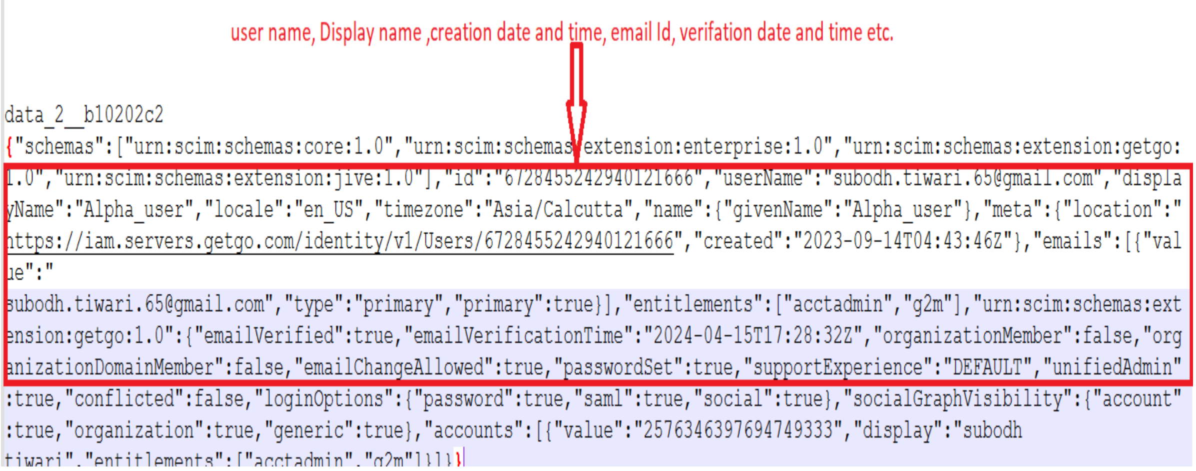
The browsing history for GoToMeeting Web Client can be found in the History SQLite database at `“C:\Users\[username]\AppData\Local\Google\Chrome\User Data\Default\History”` that contains records of visit date and time, visit frequency(count), a duration of visits, search terms, and details about the names, sizes, dates, and URLs that related to downloads; further specifics on the downloads can be found in the Download Metadata file located at `(“C:\Users\[username]\AppData\Local\Google\Chrome\User Data\Default\Download Metadata”),` If browsing history is deleted all tables in the History database are erased but there might be some tables concerning downloads which could contain valuable information.

vii Cookies

Cookies related to GoToMeeting Web Client were extracted from two folder located at `“C:\Users\[username]\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies”` and `“C:\Users\[username]\AppData\Local\Google\Chrome\User Data\Default\Safe Browsing Network\Safe Browsing Cookies”.` These cookies include the name, the host key & value, created time, expiry time and the last modified time of the cookies. It is critical to mention that the above databases help in identifying the pattern through which the web applications are being utilized.

viii Cache

The cache folder located at “`C:\Users\[username]\AppData\Local\Google\Chrome\User Data\Default\Cache`”. Contained considerable number of forensic data for GoToMeeting which includes profile photos, logo of GoToMeeting etc. The cache also contained the meeting link also details of meeting i.e. Meeting Type, Meeting ID, Number of Participants, GoToMeeting Web Client Version etc. also user details including username, display name, email-addresses, created date etc. as illustrated in fig. 12


user name, Display name ,creation date and time, email Id, verifation date and time etc.

```
data_2__b10202c2
{"schemas":["urn:scim:schemas:core:1.0","urn:scim:schemas:extension:enterprise:1.0","urn:scim:schemas:extension:getgo:
1.0","urn:scim:schemas:extension:jive:1.0"],"id":"6728455242940121666","userName":"subodh.tiwari.65@gmail.com","displa
yName":"Alpha_user","locale":"en_US","timezone":"Asia/Calcutta","name":{"givenName":"Alpha_user"},"meta":{"location":"
https://iam.servers.getgo.com/identity/v1/Users/6728455242940121666","created":"2023-09-14T04:43:46Z"},"emails":[{"val
ue":"
subodh.tiwari.65@gmail.com","type":"primary","primary":true}],"entitlements":["acctadmin","g2m"],"urn:scim:schemas:ext
ension:getgo:1.0":{"emailVerified":true,"emailVerificationTime":"2024-04-15T17:28:32Z","organizationMember":false,"org
anizationDomainMember":false,"emailChangeAllowed":true,"passwordSet":true,"supportExperience":"DEFAULT","unifiedAdmin"
:true,"conflicted":false,"loginOptions":{"password":true,"saml":true,"social":true},"socialGraphVisibility":{"account"
:true,"organization":true,"generic":true},"accounts":[{"value":"2576346397694749333","display":"subodh
tiwari","entitlements":["acctadmin","g2m"]}]}}
```

Fig 12 User and Meeting information found in browser cache.

Table 3 outlines the name of file or folder and database contains the artefacts related to GoToMeeting Web Client data along with the tools used for their analysis.

Table 3. Browser Artefacts of GoToMeeting web client

Artefacts	Path	Tool Used
Traces of Usage	\Default\JumpListIconsRecentClosed \Default\Top Sites \Default\Favicons \Default\Network Action Predictor \Default\Shortcuts, \Default\Sessions \Default\BrowsingTopicsSiteData	Autopsy,OSForensic, Python scripts
User Identification	\Default\Accounts\Avatar Images \Default\Sessions	Autopsy, OSForensic,
IndexedDB-LevelDB	\IdexedDB\ https_app.goto.com_0.in dexeddb.	Autopsy, Python scripts
Bookmarks	\Default\Bookmarks	Autopsy, OSForensic,
Browsing History	\Default\History	Autopsy, OSForensic, SQLite database tools
Cookies	\Default\Network\Cookies \Default\Safe Browsing Network\Safe Browsing Cookies	Autopsy, OSForensic, SQLite database tools
Cache	\Default\Cache	Autopsy, OSForensic,

CONCLUSION AND FUTURE WORK

Web applications respond to the complex needs of modern software consumers, but web applications also pose many security risks due to its dynamic nature, raising the attack surface. Our investigations cantered around a detailed forensics analysis of the GoToMeeting Web Client platforms to extracts the memory and browser artefacts for potential artefacts evidence in legal cases. Also Assist web-based application (SaaS) developers and security specialists in understanding how to maintain and mitigate user data privacy while enhancing the security of the application.

Memory analysis was carried about on GoToMeeting Web Client, utilizing manual string analysis along with data carving, simple text searches to retrieved critical artefacts including meeting metadata, content of send and receive messages but not the metadata (sender & receiver details, timestamps etc), participant details including email addresses etc., and in-meeting notes from the GoToMeeting application. This analysis provided insights into user interactions, communication history, and scheduled meetings, aiding forensic investigations.

Further, we examined the browser forensic with much focus GoToMeeting Web Client for Google Chrome. This involved; extraction of; traces of usage history, browsing history, downloads, favourites, cookies, profile pictures, cache, e-mail addresses, meeting details etc. It will be useful in future work to analyse GoToMeeting Web Client in other platforms like macOS, Android and iOS also on different browsers like edge, Firefox, opera etc. Further research could also examine other web clients and video conferencing applications to investigate their forensic potential and the information they may reveal, which is crucial for criminal investigations.

REFERENCES

[1] M, G. (2024). 'Video Conferencing Statistics: Usage and Trends 2022', QuickBlox. QuickBloxhttps://quickblox.com/blog/video-conferencing-statistics-usage-and-trends/ (accessed 15 January 2024).

[2] Team, S. (2023). '100 Video Conferencing Statistics and Facts for the 2022 Market' , 100 Video Conferencing Statistics and Facts for the 2022 Market | Sonary , https://sonary.com/content/100-video-conferencing-statistics-and-facts-for-the-2022-market/ (accessed 16 January 2024).

[3] Belyh, A. (2023). 'The Ultimate List of Video Conferencing Statistics for 2024', FounderJar,https://www.founderjar.com/video-conferencing-statistics/ (accessed 16 January 2024).

[4] Statista. (2024) 'Global market share of videoconferencing software 2023, by program.Statista.https://www.statista.com/statistics/1331323/videoconferencing-market-share/ (accessed 15 Febuary 2024).

[5] T. Lorenz, "'Zoombombing': When Video Conferences Go Wrong," The New York Times, Mar. 20, 2020.

[6] 2012 LinkedIn Breach had 117 Million Emails and Passwords Stolen, Not 6.5M - Security News -Trend Micro IN, https://www.trendmicro.com/vinfo/in/security/news/cyber-attacks/2012-linkedin-breach-117-million-emails-and-passwords-stolen-not-6-5m (accessed 13 March 2024).

[7] Akremi, A., Sallay, H., Rouached, M., & Bouaziz, R. (2020). 'Applying Digital Forensics to Service Oriented Architecture', International Journal of Web Services Research, Vol 17 No 1, pp17–42. https://doi.org/10.4018/ijwsr.2020010102

[8] Iqbal, F., Khalid, Z., Marrington, A., Shah, B., & Hung, P. C. (2022). 'Forensic investigation of Google Meet for memory and browser artefacts', Forensic Science International. Digital Investigation, Vol. 43, p.301448. https://doi.org/10.1016/j.fsidi.2022.301448

[9] Azhar, M. a. H. B., Timms, J., & Tilley, B. (2022). 'Forensic Investigations of Google Meet and Microsoft Teams–Two Popular Conferencing Tools in the Pandemic', Springer eBooks pp. 20–34. https://doi.org/10.1007/978-3-031-06365-7_2(accessed 01 june 2024).

[10] Barradas, D., Brito, T., Duarte, D., Santos, N., & Rodrigues, L. (2019). 'Forensic analysis of Communication records of messaging applications from physical memory', Computers & Security, Vol.86, pp.484–497. https://doi.org/10.1016/j.cose.2018.08.013

[11] Mahr, A., Cichon, M., Mateo, S., Grajeda, C., & Baggili, I. (2021). 'Zooming into the pandemic! A forensic analysis of the Zoom Application', Forensic Science International. Digital Investigation, Vol.36, p.301107. https://doi.org/10.1016/j.fsidi.2021.301107

[12] Khalid, Z., Iqbal, F., Kamoun, F., Hussain, M., & Khan, L. A. (2021). 'Forensic Analysis of the Cisco WebEx Application' https://doi.org/10.1109/csnet52717.2021.9614647

[13] Yang, T. Y., Dehghantanha, A., Choo, K. K. R., & Muda, Z. (2016). 'Windows Instant Messaging App Forensics: Facebook and Skype as Case Studies', PloS One, Vol.11, No.3, p.0150300. https://doi.org/10.1371/journal.pone.0150300

[14] Nicoletti, M., & Bernaschi, M. (2019). 'Forensic analysis of Microsoft Skype for Business', Digital Investigation, Vol. 29, pp.159–179. https://doi.org/10.1016/j.diin.2019.03.012

[15] Motylinski, M., MacDermott, A., Iqbal, F., Hussain, M., & Aleem, S. (2020). 'Digital Forensic Acquisition and Analysis of Discord Applications', https://doi.org/10.1109/ccci49893.2020.9256668

[16] Walnycky, D., Baggili, I., Marrington, A., Moore, J., & Breitinger, F. (2015). 'Network and device forensic analysis of Android social-messaging applications', Digital Investigation, Vol. 14, pp.577–584. https://doi.org/10.1016/j.diin.2015.05.009

[17] McFadden, B., Balasubramani, E., & Miebaka, W. E. (2019). 'Forensic Analysis of Microblogging Sites Using Pinterest and Tumblr as Case Study', Studies in big data, pp. 243–279. https://doi.org/10.1007/978-3-030-23547-5_13

[18] Fernández-Álvarez, P., & Rodríguez, R. J. (2022). 'Extraction and analysis of retrievable memory artefacts from Windows Telegram Desktop application', Forensic Science International. Digital Investigation, Vol. 40, p.301342. https://doi.org/10.1016/j.fsidi.2022.301342

[19] Cloyd, T., Osborn, T., Ellingboe, B., Glisson, W.B., Choo, K.K.R.(2018) 'Browser analysis of residual facebook data', 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering. TrustCom/BigDataSE), pp.1440-1445. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00200.

[20] Marrington, A., Baggili, I.M., Ismail, T.A., Kaf, A.A. (2012). 'Portable web browser forensics: A forensic examination of the privacy benefits of portable web browsers', International Conference on Computer Systems and Industrial Informatics, pp. 1-6. https://doi.org/10.1109/ICCSII.2012.6454516.

[21] Oh, J., Lee, S., Lee, S., (2011). 'Advanced evidence collection and analysis of web browser activity', Digit. Invest, Vol. 8, 562-570. https://doi.org/10.1016/ j.diin.2011.05.008.

[22] Rasool, A. and Zunera, J. (2020) 'A review of web browser forensic analysis tools and techniques', Research Pedia Journal of Computing, Vol. 11, No. 2020, pp.15–21.

[23] Beebe, N. (2009) 'Digital forensic research: the good, the bad and the unaddressed', in IFIP International Conference on Digital Forensics, January, pp.17–36, Springer, Berlin, Heidelberg.

[24] Paligu, F. and Varol, C. (2020) 'Browser forensic investigations of whatsapp web utilizing indexeddb persistent storage', Future Internet, Vol. 12, No. 11, p.184.

[25] Hughes, K., Papadopoulos, P., Pitropakis, N., Smales, A., Ahmad, J. and Buchanan, W.J. (2021) 'Browsers' private mode: is it what we were promised?', Computers, 2 December, Vol. 10, No. 12, p.165.

[26] Tsalis, N., Mylonas, A., Nisioti, A., Gritzalis, D. and Katos, V. (2017) 'Exploring the protection of private browsing in desktop browsers', Comput. Secur., Vol. 2017, No. 67, pp.181–197.

[27] Download VMware Workstation Pro. (2024). VMware.https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation_html.html.html(accessed 15 March 2024).

[28] Exterro. (2024). FTK Imager Version 4.7.1, Exterro https://www.exterro.com/ftk-product-downloads/ftk-imager-version-4-7-1 (accessed 15 january 2024).

[29] Markruss. (2024). Strings - Sysinternals. Microsoft Learn. https://learn.microsoft.com/en-us/sysinternals/downloads/strings(accessed 23 May january 2024).

[30] OSForensics - Download. (2024). https://www.osforensics.com/download.html. (accessed 23 may 2024).

[31] Autopsy (2024). Autopsy – Download, Autopsy. https://www.autopsy.com/download/ (accessed 23 may 2024).

[32] GitHub - volatilityfoundation/volatility3: Volatility 3.0 development. (2024). GitHub. https://github.com/volatilityfoundation/volatility3 (accessed 24 may 2024).

[33] Simsong. (2024). GitHub - simsong/bulk_extractor: This is the development tree. Production downloads are on: GitHub. https://github.com/simsong/bulk_extractor (accessed 23 may 2024).

[34] Simon, M., & Slay, J. (2010). Recovery of Skype Application Activity Data from Physical Memory.https://doi.org/10.1109/ares.2010.73