FORENSIC ANALYSIS FOR MS TEAMS

COURSE NAME: FORENSICS AND EDISCOVERY
STUDENT NAME: KUCHUPUDI SAI ABHIGNA
STUDENT ID: 24191329

EXECUTIVE SUMMARY

There has been a significant increase in the video conferencing applications during the COVID-19 pandemic. With millions of VoIP users' data, ensuring the security of these platforms becomes crucial. This report provides an extensive forensic examination of a MS Teams application on a smartphone that employs an Android developer toolkit through a virtual phone testing environment. By utilizing Android Studio for emulation, ALEAPP tool has been utilized for parsing the artifacts and generating the HTML-based report from the mobile device. root AVD to root the device and Python for required dependencies. The investigation extracted artifacts include user data such as email, user account information, installed apps, timestamps, Session reports, and SQLite Journaling.

METHODOLOGY

LITERATURE REVIEW

A systematic method was employed to guarantee the use of pertinent and credible sources in this inquiry. This section covers a selection of recent papers, journals, and blogs.

Savannah Thompson (2025) offered a detailed ALEAPP walkthrough about the artifacts discovered and the usefulness of open-source tools for mobile forensics.

Ayers *et al.*(2014) explained guidelines for the forensics handling of mobile devices.

Josh Brunty (2021) emphasizes the significance of clear and concise reporting in digital forensic and incident response.

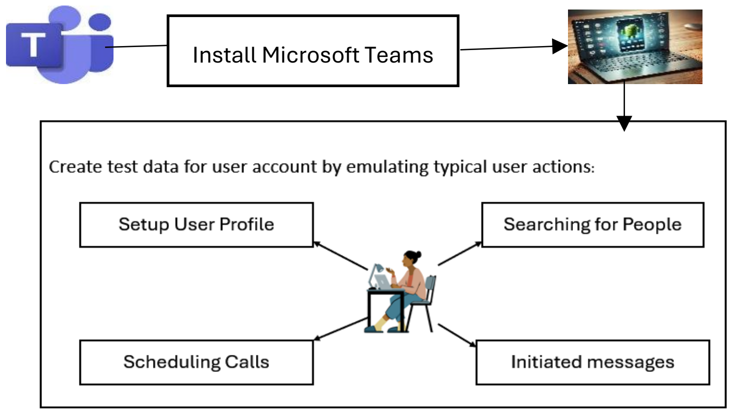
Web browsing using keywords like Android mobile forensics, MS Teams artifacts, and artifacts of ALEAPP Report. The Mobile Forensics module practical session has given insights on setting up a testing environment.

TEST ENVIRONMENT SETUP

For an assessment, used a Windows 11 machine with the configuration of 16GB RAM and 100GB free disk space. For Android emulation, Android Studio has been downloaded and created a virtual smartphone by selecting the hardware and configuration.

To create input data for forensic examination, the Microsoft Teams application has been downloaded, installed, and performed activities in the application such as setting up the user profile, searching for people, initiating messages, and scheduling a call.

Environmental Setup



RootAVD with Magisk software has been used to obtain root access to files of an Android virtual device. After obtaining root access to the data of the device, subsequently downloaded and installed ALEAPP from the GitHub repository and further installed Python to fulfil the required dependencies.

Extracted data from the device as an input folder and selected the desired output folder for exporting the report, then to initiate the process for artifacts, select all available modules for parsing and click process to begin generating the report.

Best practice to run the Android emulator is having good configuration of the machine for smooth performance, recommended minimum 16GB RAM, minimum 16 GB free storage space, a multi-core processor, and verify whether the components for the emulator are installed or not.

Tool	**Version**	**Usage**
Windows VM	11	Experimental OS
Android Studio	2024.2.2.14	To create and manage AVD
Android Device (Pixel _9_pro_Fold)	15-API 35	To install the MS Teams application and test
Microsoft Teams Application	1416/1.0.0.2025032402	Videoconferencing application under test for artifacts
ALEAPP	v3.3.0	To parse and validate the mobile forensic artifacts
Python	3.13.2	Used for ALEAPP dependencies
rootAVD using Magisk		Script designed to root AVD using Magisk to get root access

Table 1 lists the features of tools, OS, and device versions used for forensic analysis.

FORENSIC ANALYSIS WITH ALEAPP

MS TEAMS BACKGROUND

Microsoft released a new communication platform in 2017 and started gaining popularity in 2019. “Business Insider reported that as of March 18, 2020, teams had hit 44 million daily active users” (Zaveri,2020). Potential data such as user accounts, chats, call logs, shared files, channels can be considered as sensitive information required for forensic examination.

Microsoft Teams provides robust security and continuous improvements, these factors can present challenges for forensic investigators in terms of data scalability, analysis, and the need for up-to-date forensic tools and techniques.

SOURCES OF FORENSIC ARTIFACTS

Forensic artifacts were discovered in the emulated storage. The identified data types consist of account data, storage metadata, FCM data, database, cache files, teams user’ data, and messages report. The artifacts offer evidence of app utilization and user engagement.

ULR USER PREFERENCES

The ULR_User_PrefS.xml document contains configurations for the Google account kuchupudi6@gmail.com. Essential entries consist of account type, the history and reporting features are set to false here. This file shows basic settings but doesn’t provide details of user activity.

CALENDAR

The calendar.db file stores calendar-related data for the kuchupudi6@gmail.com. It verifies that the calendar was established on February 22, 2025, configured to the UTC time zone.

GMAIL

The active Gmail account found in the file is kuchupudi6@gmail.com. The database file bigTopDataDB retrieved from Gmail holds label information pertinent to email organization and message classification. Key Findings include the Main Inbox comprises eight emails with seven being unread. Social and promotional labels hold zero emails.

MICROSOFT TEAMS

Teams user report is a retrieved user information from the SkypeTeams.db database, found in the Microsoft Teams folder, which includes information about users, such as time stamps, names, email addresses and account types.

The dataset comprises four user records: Anushka Sharma (primary user holding a Gmail account), Sai Abhigna Kuchupudi (external user with a student email with restricted access), Abhigna Kuchupudi (internal user but no email documented, prompting worries about data incompleteness) and one entry lacking identifiable information but recorded as an active Teams user with private chat enabled.

And the messages from Microsoft Teams display an informal conversation between Anushka Sharma and Abhigna Kuchupudi, as well as automated system notifications. Anushka also sets up a Teams meeting called "Testing," providing a Meeting ID and Passcode, signifying a scheduled event.

CHROMIUM EDGE-COOKIES & GOOGLE PLAY SEARCHES

Forensic examination of Edge browser cookies from Microsoft Teams WebView uncovers authentication (MSPAuth) disabled, and user information (JSH), associated with kuchipudi6@gmail.com. These cookies reflect login activity, maintain session continuity, and enable tracking, supporting forensic inquiries into security threats. The search history on Google Play indicates that the user looked for Teams by Microsoft on February 22, 2025, at 20:02:36.

NATIVE DOWNLOADS

The details pertain to a collection of downloads from the Google Play Store or other services related to Android, including timestamp of the download, file name, URL source, and location. This information helps in tracking the download history, origins of files, and storage sites on a device for investigation.

EMULATED STORAGE METADATA

This metadata indicates recent file activity on February 22, 2025, including downloads of system files, and application-related information. Some downloads failed, suggesting potential disruptions.

IMAGE CACHE

The Image Manager cache report displays Microsoft Teams images in .cnt format, with timestamps ranging from 2025-02-22 20:15:27 to 2025-02-22 20:23:59. Certain entries include direct links while others are typical cache files.

GBOARD-SESSIONS & FCM

This keyboard usage dataset includes start and finish information of users’ majority usage on the Microsoft Teams application with respective Session ID.

Firebase Cloud Messaging (FCM) dataset containing a segregated dump of queued messages for the respective application, along with timestamp, source file, record ID, and key-value pairs.

INSTALLED APPS, STRINGS-SQLITE JOURNAL&WAL

The app updates database (Frosting.db) contains timestamps, package names, APK path, Bundle ID, Version Code, and SHA-256 Hash for validation. It additionally examines SQLite

rollback journals and WAL files, supporting forensic investigations by retrieving deleted or altered data.

ARCHITECTURE

The User Interface (UI) engages with the MS Teams Client on the device (mobile, desktop), the local storage (cache) keeps temporary information such as chat logs, files, and the cloud API Servers manage real-time interaction, messaging, file storage, and various cloud-based services.

[User Interface] <--> [MS Teams Client (App)]
↓
[Local Storage (cache)] <--> [Cloud API Servers (Messaging, File Storage, etc.)]

Microsoft Teams can be used for forensic analysis to investigate cyber threats, recover lost data, and monitor user activity sessions. Individuals can retrieve their lost/deleted messages, prevent unauthorized login and report phishing attempts. Organizations can prevent data leaks, insider threats, and track meeting records.

CONCLUSION

The forensic analysis shows that significant user data such as login activities, downloads, and messaging information can be obtained through tools like Android Studio, rootavd, and aleapp. For mobile devices, these artifacts can primarily be found in SQLite databases, or in file caches. However, forensic investigations might be difficult because of end-to-end encryption, regular app update, and substantial data quantities. Updating tool architecture and adherence to legal privacy regulation can enhance the efficiency of analysis. Furthermore, would welcome the opportunity to run an analysis report on various operating systems using other available tools/methods and analyze network traffic.

REFERENCES

Thompson, S. (2025) *Guide to Mobile Forensics with ALEAPP*, *CYBER 5W*. Available at: https://blog.cyber5w.com/a-guide-to-mobile-forensics-with-aleapp

Ayers, R., Brothers, S., and Wayne, J. (2014) *Guidelines on mobile device forensics*, *nist.gov*. Available at: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-101r1.pdf

Brunty, J. (2021) *Writing DFIR reports: A Primer*, *Forensic Focus*. Available at: https://www.forensicfocus.com/articles/writing-dfir-reports-a-primer/

Zaveri, P. (2020) *Microsoft teams now has 75 million daily active users, adding 31 million in just over a month*, *Business Insider*. Available at: https://www.businessinsider.com/microsoft-teams-hits-75-million-daily-active-users-2020-4

Sambita. (2023) *Microsoft Teams Forensics to Uncover Clues Hiding within Teams,* Available at: https://www.forensicsware.com/blog/microsoft-teams-forensics

Mohit. (2024) *Microsoft Teams Forensics for Artifact & Content Investigation*. Available at: https://www.mailxaminer.com/blog/microsoft-teams-forensics

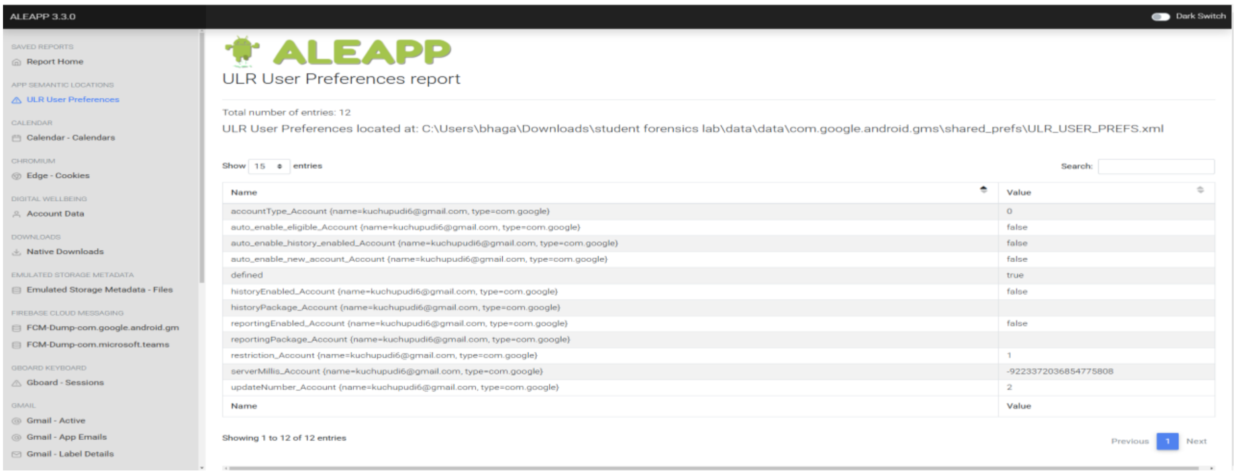
Andrade, R. (2022) *Exporting Microsoft Teams data from the Office 365 Security & Compliance Center for use in Axiom Cyber*, *Magnet Forensics*. Available at: https://www.magnetforensics.com/blog/exporting-microsoft-teams-data-from-the-office-365-security-compliance-center-for-use-in-axiom-cyber/

Matt, Z. (2024) *Mobile & Digital Forensics: How do experts extract data from phones*, Available at: https://www.forensicscolleges.com/blog/guide-to-mobile-forensics

Mobile device forensics: Challenges, threats, & solutions (2024) *SecurityScorecard*. Available at: https://securityscorecard.com/blog/mobile-device-forensics

APPENDIX

Fig 1: url user preferences



ULR User Preferences report

Total number of entries: 12

ULR User Preferences located at: C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.gms\shared_prefs\ULR_USER_PREFS.xml

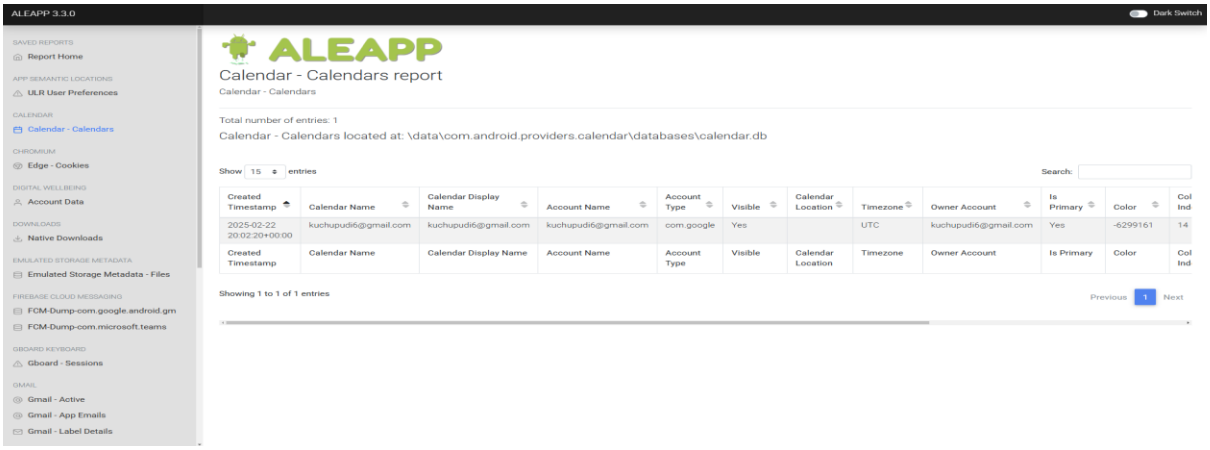
Show 15 entries Search:

Name	Value
accountType_Account {name=kuchupudi6@gmail.com, type=com.google}	0
auto_enable_eligible_Account {name=kuchupudi6@gmail.com, type=com.google}	false
auto_enable_history_enabled_Account {name=kuchupudi6@gmail.com, type=com.google}	false
auto_enable_new_account_Account {name=kuchupudi6@gmail.com, type=com.google}	false
defined	true
historyEnabled_Account {name=kuchupudi6@gmail.com, type=com.google}	false
historyPackage_Account {name=kuchupudi6@gmail.com, type=com.google}	
reportingEnabled_Account {name=kuchupudi6@gmail.com, type=com.google}	false
reportingPackage_Account {name=kuchupudi6@gmail.com, type=com.google}	
restriction_Account {name=kuchupudi6@gmail.com, type=com.google}	1
serverMillis_Account {name=kuchupudi6@gmail.com, type=com.google}	-9223372036854775808
updateNumber_Account {name=kuchupudi6@gmail.com, type=com.google}	2
Name	Value

Showing 1 to 12 of 12 entries

Previous 1 Next

Fig 2: calendar



Calendar - Calendars report

Calendar - Calendars

Total number of entries: 1

Calendar - Calendars located at: \data\com.android.providers.calendar\databases\calendar.db

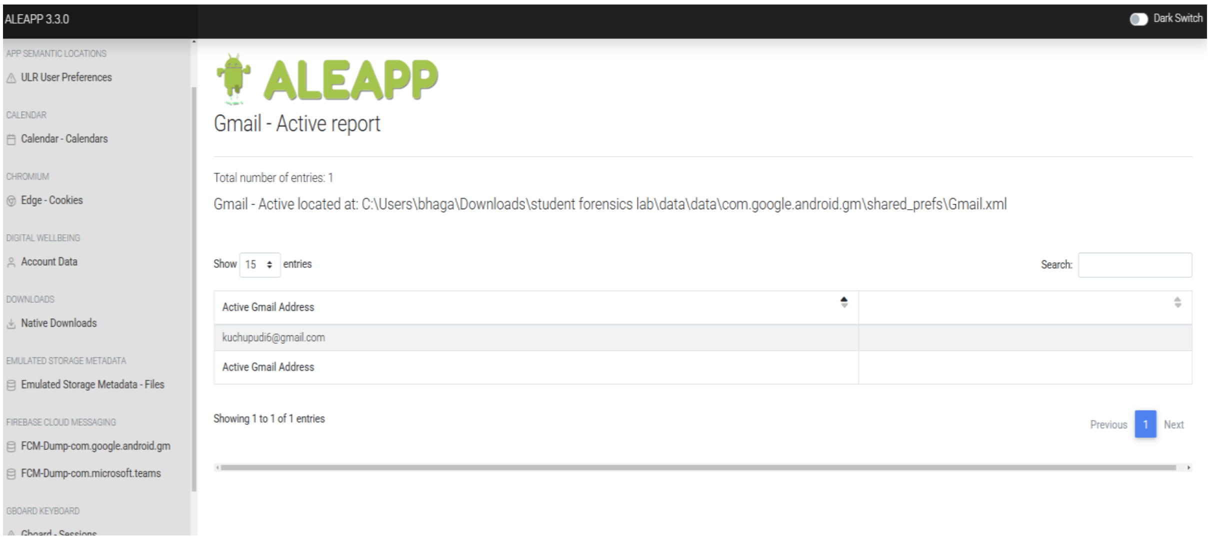
Show 15 entries Search:

Created Timestamp	Calendar Name	Calendar Display Name	Account Name	Account Type	Visible	Calendar Location	Timezone	Owner Account	Is Primary	Color	Col Ind
2025-02-22 20:02:20+00:00	kuchupudi6@gmail.com	kuchupudi6@gmail.com	kuchupudi6@gmail.com	com.google	Yes		UTC	kuchupudi6@gmail.com	Yes	-6299161	14
Created Timestamp	Calendar Name	Calendar Display Name	Account Name	Account Type	Visible	Calendar Location	Timezone	Owner Account	Is Primary	Color	Col Ind

Showing 1 to 1 of 1 entries

Previous 1 Next

Fig 3: Gmail



Gmail - Active report

Total number of entries: 1

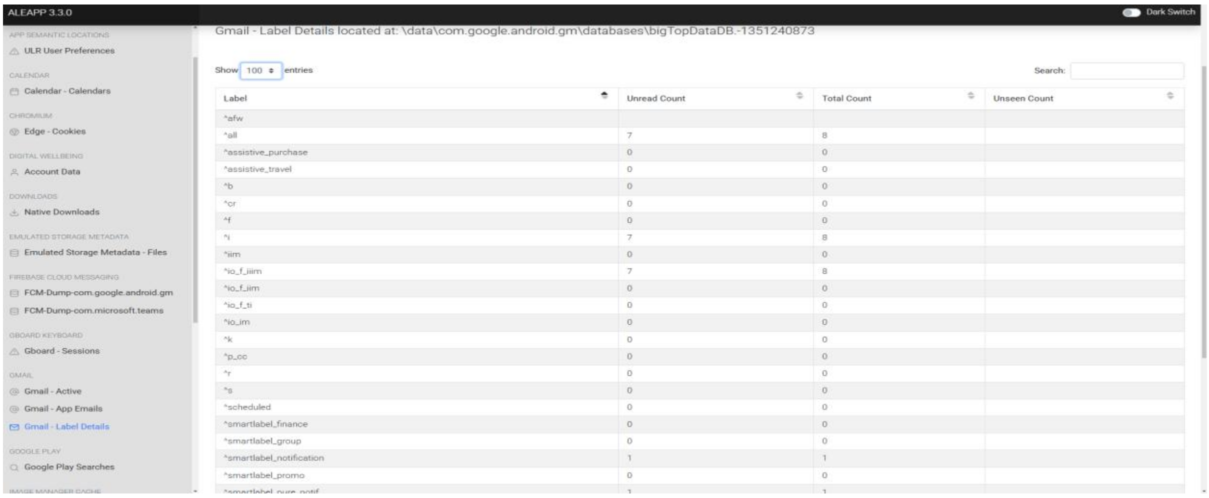
Gmail - Active located at: C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.gm\shared_prefs\Gmail.xml

Show 15 entries Search:

Active Gmail Address	
kuchupudi6@gmail.com	
Active Gmail Address	

Showing 1 to 1 of 1 entries

Previous 1 Next



ALEAPP 3.3.0

Dark Switch

APP SEMANTIC LOCATIONS
- ULR User Preferences

CALENDAR
- Calendar - Calendars

CHROMIUM
- Edge - Cookies

DIGITAL WELLBEING
- Account Data

DOWNLOADS
- Native Downloads

EMULATED STORAGE METADATA
- Emulated Storage Metadata - Files

FIREBASE CLOUD MESSAGING
- FCM-Dump-com.google.android.gm
- FCM-Dump-com.microsoft.teams

GBOARD KEYBOARD
- Gboard - Sessions

GMAIL
- Gmail - Active
- Gmail - App Emails
- Gmail - Label Details

GOOGLE PLAY
- Google Play Searches

IMAGE MANAGER CACHE

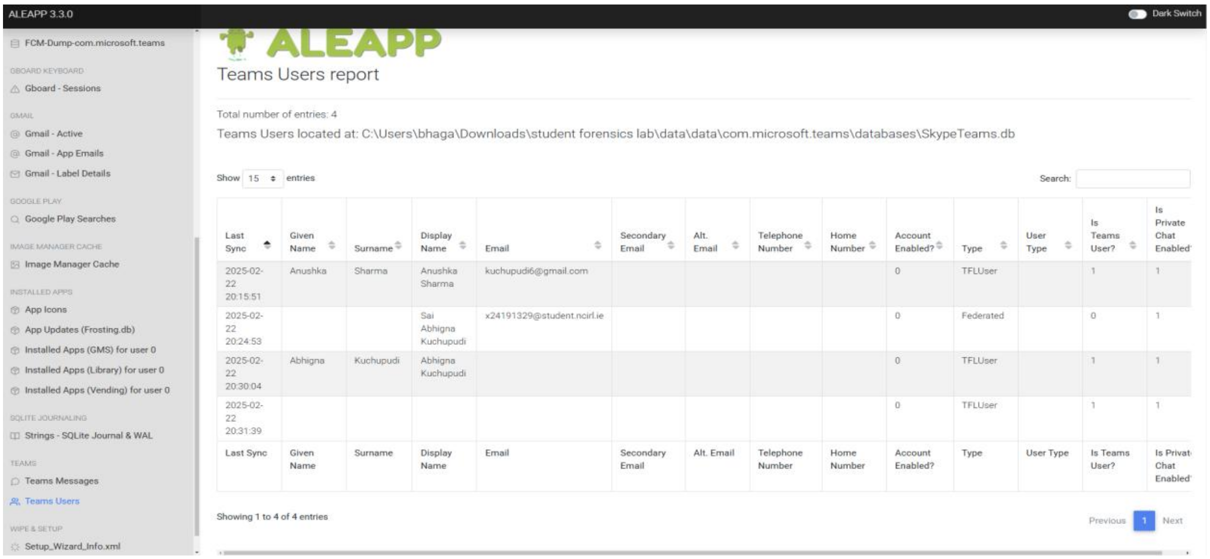
Gmail - Label Details located at: \data\com.google.android.gm\databases\bigTopDataDB.-1351240873

Show 100 entries

Search:

Label	Unread Count	Total Count	Unseen Count
^afw			
^all	7	8	
^assistive_purchase	0	0	
^assistive_travel	0	0	
^b	0	0	
^cr	0	0	
^f	0	0	
^i	7	8	
^iim	0	0	
^io_f_iiim	7	8	
^io_f_iim	0	0	
^io_f_ti	0	0	
^io_im	0	0	
^k	0	0	
^p_cc	0	0	
^r	0	0	
^s	0	0	
^scheduled	0	0	
^smartlabel_finance	0	0	
^smartlabel_group	0	0	
^smartlabel_notification	1	1	
^smartlabel_promo	0	0	
^smartlabel_pure_notif	1	1	

Fig 4: Teams



ALEAPP 3.3.0

Dark Switch

- FCM-Dump-com.microsoft.teams

GBOARD KEYBOARD
- Gboard - Sessions

GMAIL
- Gmail - Active
- Gmail - App Emails
- Gmail - Label Details

GOOGLE PLAY
- Google Play Searches

IMAGE MANAGER CACHE
- Image Manager Cache

INSTALLED APPS
- App Icons
- App Updates (Frosting.db)
- Installed Apps (GMS) for user 0
- Installed Apps (Library) for user 0
- Installed Apps (Vending) for user 0

SQLITE JOURNALING
- Strings - SQLite Journal & WAL

TEAMS
- Teams Messages
- Teams Users

WIPE & SETUP
- Setup_Wizard_Info.xml

ALEAPP

Teams Users report

Total number of entries: 4

Teams Users located at: C:\Users\bhaga\Downloads\student forensics lab\data\data\com.microsoft.teams\databases\SkypeTeams.db

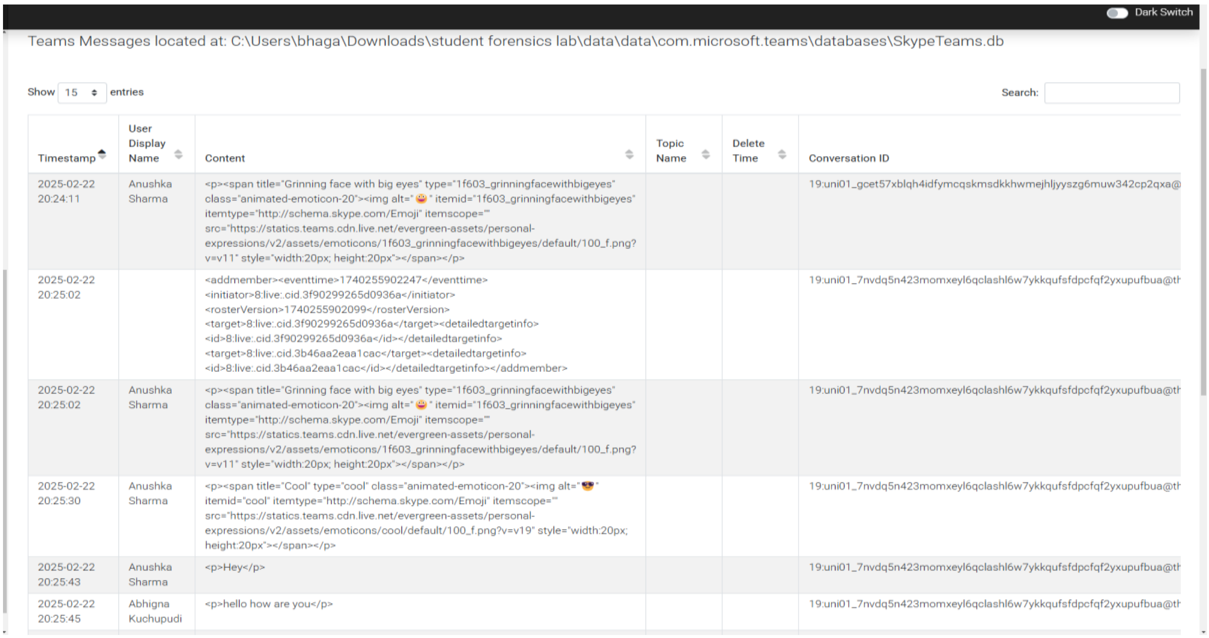
Show 15 entries

Search:

Last Sync	Given Name	Surname	Display Name	Email	Secondary Email	Alt. Email	Telephone Number	Home Number	Account Enabled?	Type	User Type	Is Teams User?	Is Private Chat Enabled'
2025-02-22 20:15:51	Anushka	Sharma	Anushka Sharma	kuchupudi6@gmail.com					0	TFLUser		1	1
2025-02-22 20:24:53			Sai Abhigna Kuchupudi	x24191329@student.ncirl.ie					0	Federated		0	1
2025-02-22 20:30:04	Abhigna	Kuchupudi	Abhigna Kuchupudi						0	TFLUser		1	1
2025-02-22 20:31:39									0	TFLUser		1	1
Last Sync	Given Name	Surname	Display Name	Email	Secondary Email	Alt. Email	Telephone Number	Home Number	Account Enabled?	Type	User Type	Is Teams User?	Is Privat Chat Enabled'

Showing 1 to 4 of 4 entries

Previous 1 Next



Dark Switch

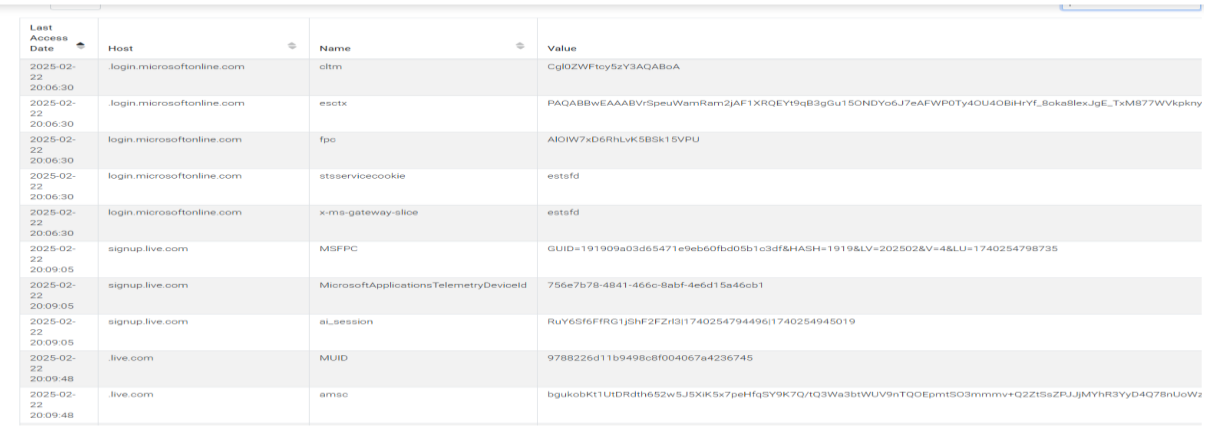
Teams Messages located at: C:\Users\bhaga\Downloads\student forensics lab\data\data\com.microsoft.teams\databases\SkypeTeams.db

Show 15 entries

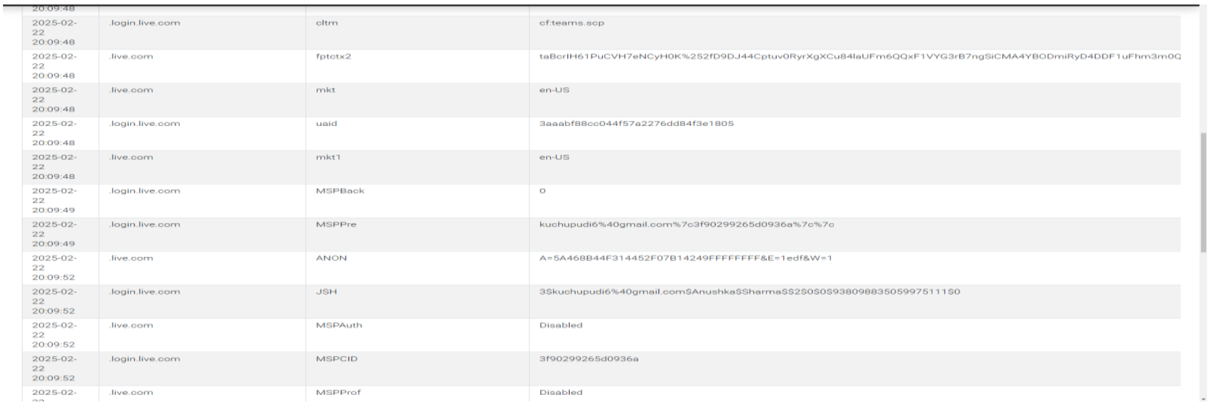
Search:

Timestamp	User Display Name	Content	Topic Name	Delete Time	Conversation ID
2025-02-22 20:24:11	Anushka Sharma	<p><span title="Grinning face with big eyes" type="1f603_grinningfacewithbigeyes" class="animated-emoticon-20"><img alt="😃" itemid="1f603_grinningfacewithbigeyes" itemtype="http://schema.skype.com/Emoji" itemscope="" src="https://statics.teams.cdn.live.net/evergreen-assets/personal-expressions/v2/assets/emoticons/1f603_grinningfacewithbigeyes/default/100_f.png?v=v11" style="width:20px; height:20px"></span></p>			19:uni01_gcet57xblqh4idfymcqskmsdkkhwmejhljyyszg6muw342cp2qxa@
2025-02-22 20:25:02		<addmember><eventtime>1740255902247</eventtime><initiator>8:live:.cid.3f90299265d0936a</initiator><rosterVersion>1740255902099</rosterVersion><target>8:live:.cid.3f90299265d0936a</target><detailedtargetinfo><id>8:live:.cid.3f90299265d0936a</id></detailedtargetinfo><target>8:live:.cid.3b46aa2eaa1cac</target><detailedtargetinfo><id>8:live:.cid.3b46aa2eaa1cac</id></detailedtargetinfo></addmember>			19:uni01_7nvdq5n423momxeyl6qclashl6w7ykkqufsfdpcfqf2yxupufbua@th
2025-02-22 20:25:02	Anushka Sharma	<p><span title="Grinning face with big eyes" type="1f603_grinningfacewithbigeyes" class="animated-emoticon-20"><img alt="😃" itemid="1f603_grinningfacewithbigeyes" itemtype="http://schema.skype.com/Emoji" itemscope="" src="https://statics.teams.cdn.live.net/evergreen-assets/personal-expressions/v2/assets/emoticons/1f603_grinningfacewithbigeyes/default/100_f.png?v=v11" style="width:20px; height:20px"></span></p>			19:uni01_7nvdq5n423momxeyl6qclashl6w7ykkqufsfdpcfqf2yxupufbua@th
2025-02-22 20:25:30	Anushka Sharma	<p><span title="Cool" type="cool" class="animated-emoticon-20"><img alt="😎" itemid="cool" itemtype="http://schema.skype.com/Emoji" itemscope="" src="https://statics.teams.cdn.live.net/evergreen-assets/personal-expressions/v2/assets/emoticons/cool/default/100_f.png?v=v19" style="width:20px; height:20px"></span></p>			19:uni01_7nvdq5n423momxeyl6qclashl6w7ykkqufsfdpcfqf2yxupufbua@th
2025-02-22 20:25:43	Anushka Sharma	<p>Hey</p>			19:uni01_7nvdq5n423momxeyl6qclashl6w7ykkqufsfdpcfqf2yxupufbua@th
2025-02-22 20:25:45	Abhigna Kuchupudi	<p>hello how are you</p>			19:uni01_7nvdq5n423momxeyl6qclashl6w7ykkqufsfdpcfqf2yxupufbua@th

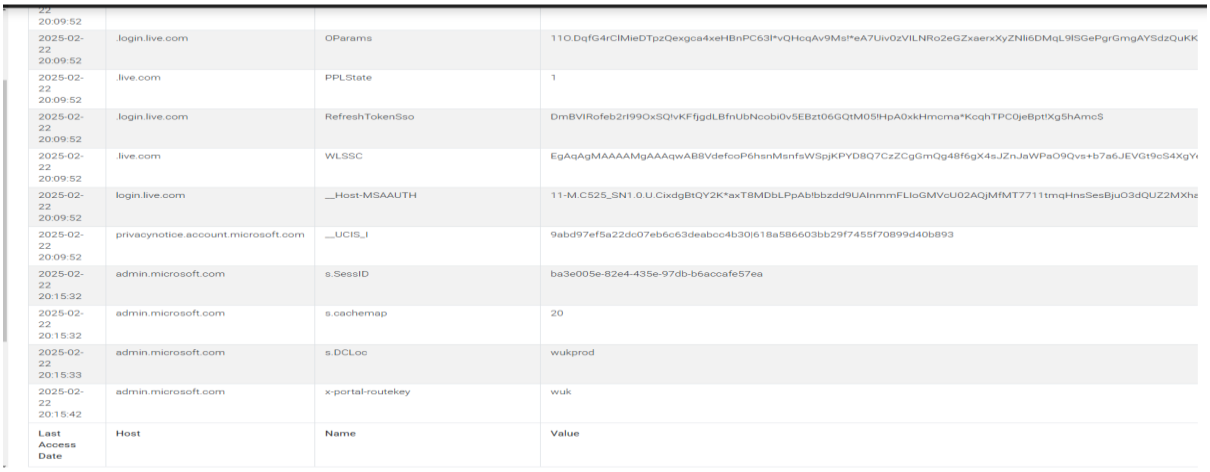
Fig 5: Edgecookies



Last Access Date	Host	Name	Value
2025-02-22 20:06:30	.login.microsoftonline.com	cltm	Cgl0ZWFtcy5zY3AQABoA
2025-02-22 20:06:30	.login.microsoftonline.com	esctx	PAQABBwEAAABVrSpeuWamRam2jAF1XRQEYt9qB3gGu15ONDYo6J7eAFWP0Ty4OU4OBiHrYf_8oka8lexJgE_TxM877WVkpkny
2025-02-22 20:06:30	login.microsoftonline.com	fpc	AlOIW7xD6RhLvK5BSk15VPU
2025-02-22 20:06:30	login.microsoftonline.com	stsservicecookie	estsfd
2025-02-22 20:06:30	login.microsoftonline.com	x-ms-gateway-slice	estsfd
2025-02-22 20:09:05	signup.live.com	MSFPC	GUID=191909a03d65471e9eb60fbd05b1c3df&HASH=1919&LV=202502&V=4&LU=1740254798735
2025-02-22 20:09:05	signup.live.com	MicrosoftApplicationsTelemetryDeviceId	756e7b78-4841-466c-8abf-4e6d15a46cb1
2025-02-22 20:09:05	signup.live.com	ai_session	RuY6Sf6FfRG1jShF2FZrl3|1740254794496|1740254945019
2025-02-22 20:09:48	.live.com	MUID	9788226d11b9498c8f004067a4236745
2025-02-22 20:09:48	.live.com	amsc	bgukobKt1UtDRdth652w5J5XiK5x7peHfqSY9K7Q/tQ3Wa3btWUV9nTQOEpmtSO3mmmv+Q2ZtSsZPJJjMYhR3YyD4Q78nUoWz

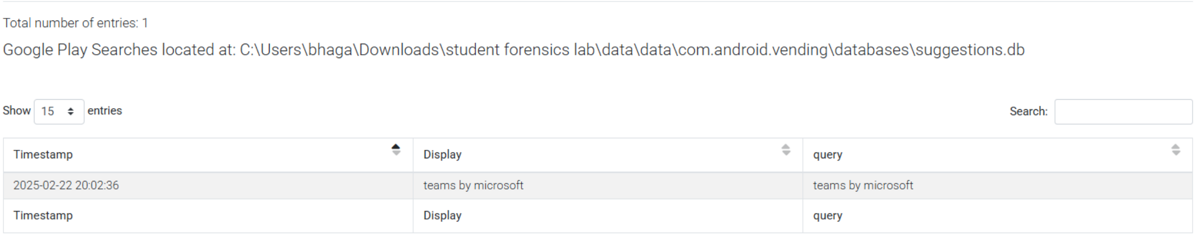


20:09:48			
2025-02-22 20:09:48	.login.live.com	cltm	cf:teams.scp
2025-02-22 20:09:48	.live.com	fptctx2	taBcrIH61PuCVH7eNCyH0K%252fD9DJ44Cptuv0RyrXgXCu84laUFm6QQxF1VYG3rB7ngSiCMA4YBODmiRyD4DDF1uFhm3m0Q
2025-02-22 20:09:48	.live.com	mkt	en-US
2025-02-22 20:09:48	.login.live.com	uaid	3aaabf88cc044f57a2276dd84f3e1805
2025-02-22 20:09:48	.live.com	mkt1	en-US
2025-02-22 20:09:49	.login.live.com	MSPBack	0
2025-02-22 20:09:49	.login.live.com	MSPPre	kuchupudi6%40gmail.com%7c3f90299265d0936a%7c%7c
2025-02-22 20:09:52	.live.com	ANON	A=5A468B44F314452F07B14249FFFFFFFF&E=1edf&W=1
2025-02-22 20:09:52	.login.live.com	JSH	3Skuchupudi6%40gmail.comSAnushkaSSharmaS$2S0S0S938098835059975111S0
2025-02-22 20:09:52	.live.com	MSPAuth	Disabled
2025-02-22 20:09:52	.login.live.com	MSPCID	3f90299265d0936a
2025-02-	.live.com	MSPProf	Disabled



22 20:09:52			
2025-02-22 20:09:52	.login.live.com	OParams	11O.DqfG4rClMieDTpzQexgca4xeHBnPC63l*vQHcqAv9Ms!*eA7Uiv0zVILNRo2eGZxaerxXyZNli6DMqL9lSGePgrGmgAYSdzQuKK
2025-02-22 20:09:52	.live.com	PPLState	1
2025-02-22 20:09:52	.login.live.com	RefreshTokenSso	DmBVIRofeb2rI99OxSQ!vKFfjgdLBfnUbNcobi0v5EBzt06GQtM05!HpA0xkHmcma*KcqhTPC0jeBpt!Xg5hAmc$
2025-02-22 20:09:52	.live.com	WLSSC	EgAqAgMAAAAMgAAAqwAB8VdefcoP6hsnMsnfsWSpjKPYD8Q7CzZCgGmQg48f6gX4sJZnJaWPaO9Qvs+b7a6JEVGt9cS4XgY
2025-02-22 20:09:52	login.live.com	__Host-MSAAUTH	11-M.C525_SN1.0.U.CixdgBtQY2K*axT8MDbLPpAb!bbzdd9UAInmmFLIoGMVcU02AQjMfMT7711tmqHnsSesBjuO3dQUZ2MXha
2025-02-22 20:09:52	privacynotice.account.microsoft.com	__UCIS_I	9abd97ef5a22dc07eb6c63deabcc4b30|618a586603bb29f7455f70899d40b893
2025-02-22 20:15:32	admin.microsoft.com	s.SessID	ba3e005e-82e4-435e-97db-b6accafe57ea
2025-02-22 20:15:32	admin.microsoft.com	s.cachemap	20
2025-02-22 20:15:33	admin.microsoft.com	s.DCLoc	wukprod
2025-02-22 20:15:42	admin.microsoft.com	x-portal-routekey	wuk
Last Access Date	Host	Name	Value

Fig6: google play



Total number of entries: 1

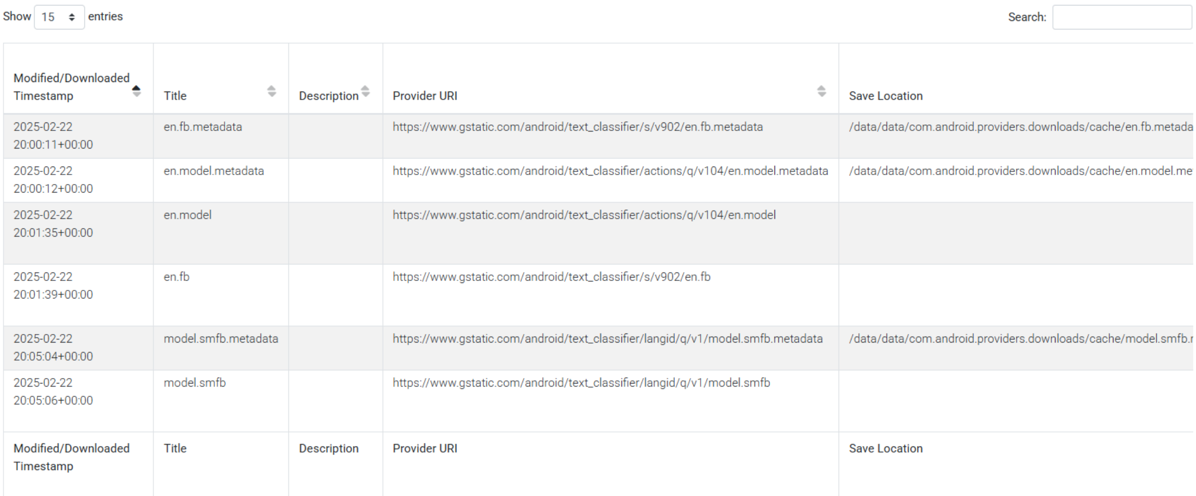
Google Play Searches located at: C:\Users\bhaga\Downloads\student forensics lab\data\data\com.android.vending\databases\suggestions.db

Show 15 entries

Search:

Timestamp	Display	query
2025-02-22 20:02:36	teams by microsoft	teams by microsoft
Timestamp	Display	query

Fig 7: native downloads

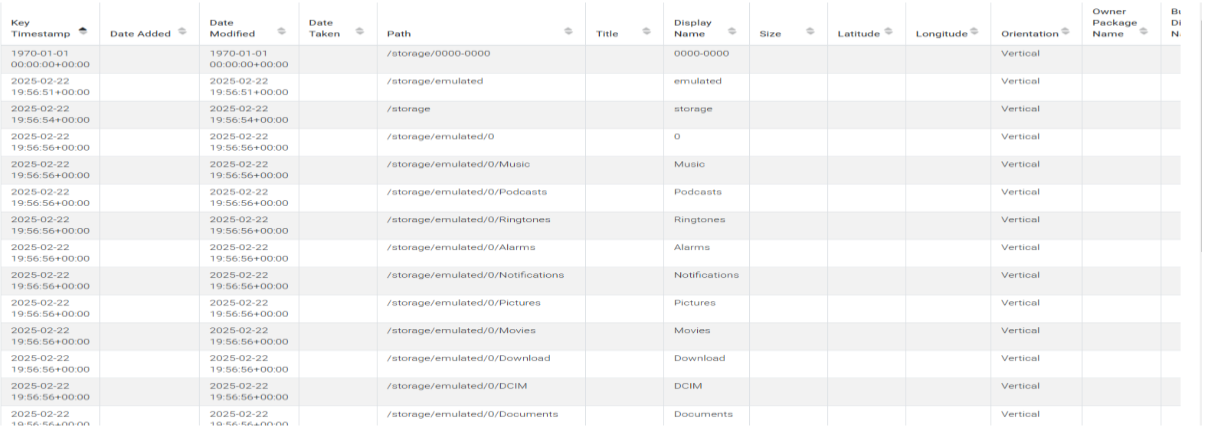


Show 15 entries

Search:

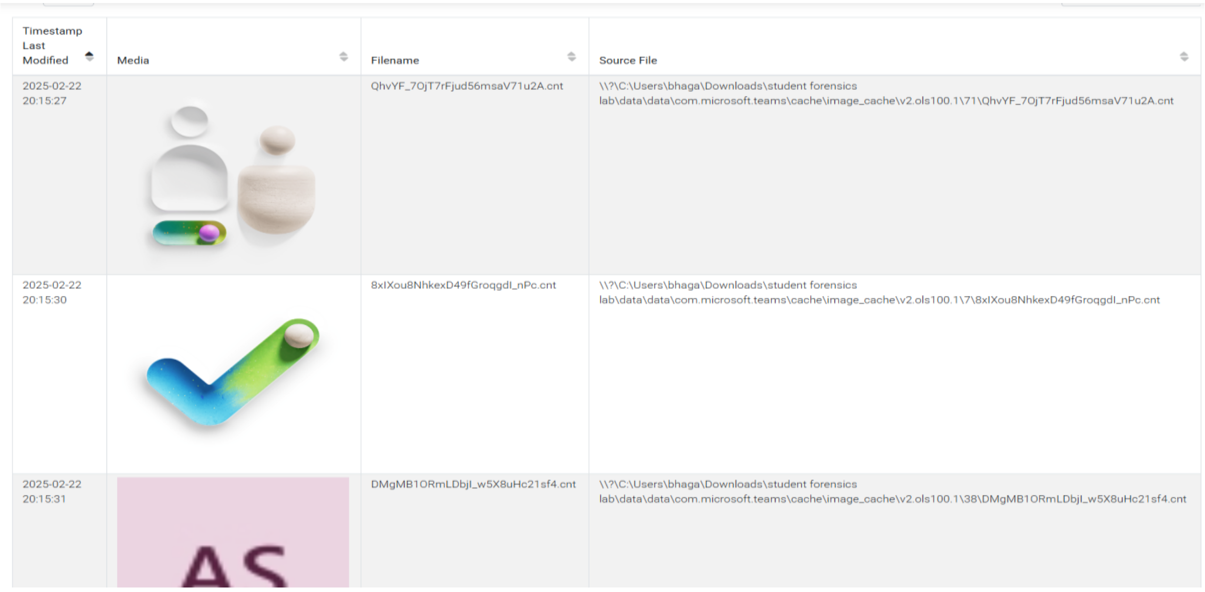
Modified/Downloaded Timestamp	Title	Description	Provider URI	Save Location
2025-02-22 20:00:11+00:00	en.fb.metadata		https://www.gstatic.com/android/text_classifier/s/v902/en.fb.metadata	/data/data/com.android.providers.downloads/cache/en.fb.metada
2025-02-22 20:00:12+00:00	en.model.metadata		https://www.gstatic.com/android/text_classifier/actions/q/v104/en.model.metadata	/data/data/com.android.providers.downloads/cache/en.model.me
2025-02-22 20:01:35+00:00	en.model		https://www.gstatic.com/android/text_classifier/actions/q/v104/en.model	
2025-02-22 20:01:39+00:00	en.fb		https://www.gstatic.com/android/text_classifier/s/v902/en.fb	
2025-02-22 20:05:04+00:00	model.smfb.metadata		https://www.gstatic.com/android/text_classifier/langid/q/v1/model.smfb.metadata	/data/data/com.android.providers.downloads/cache/model.smfb.r
2025-02-22 20:05:06+00:00	model.smfb		https://www.gstatic.com/android/text_classifier/langid/q/v1/model.smfb	
Modified/Downloaded Timestamp	Title	Description	Provider URI	Save Location

Fig 8 metadata



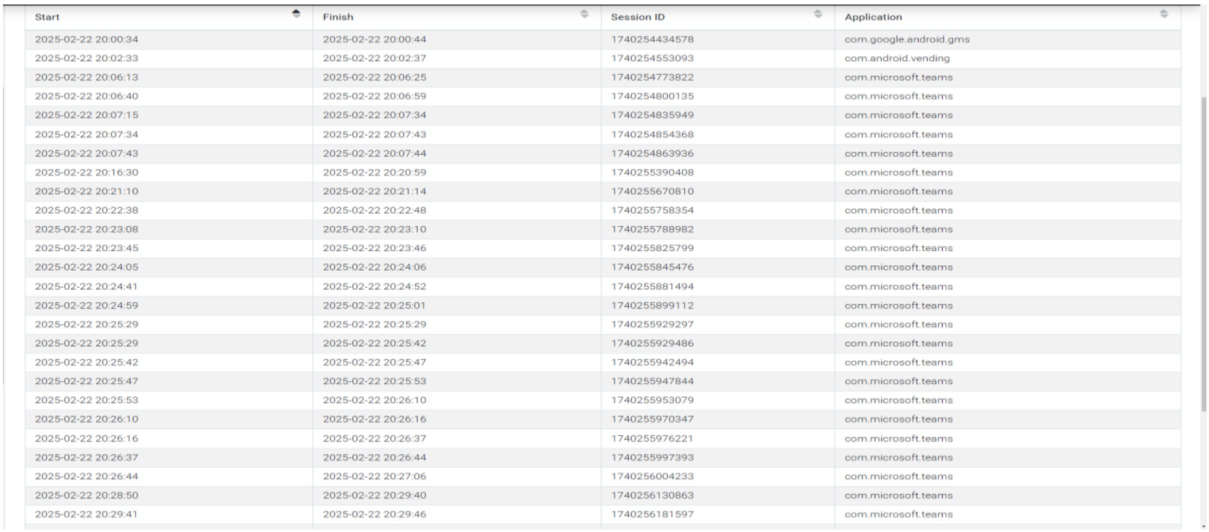
Key Timestamp	Date Added	Date Modified	Date Taken	Path	Title	Display Name	Size	Latitude	Longitude	Orientation	Owner Package Name	Bu Di N
1970-01-01 00:00:00+00:00		1970-01-01 00:00:00+00:00		/storage/0000-0000		0000-0000				Vertical		
2025-02-22 19:56:51+00:00		2025-02-22 19:56:51+00:00		/storage/emulated		emulated				Vertical		
2025-02-22 19:56:54+00:00		2025-02-22 19:56:54+00:00		/storage		storage				Vertical		
2025-02-22 19:56:56+00:00		2025-02-22 19:56:56+00:00		/storage/emulated/0		0				Vertical		
2025-02-22 19:56:56+00:00		2025-02-22 19:56:56+00:00		/storage/emulated/0/Music		Music				Vertical		
2025-02-22 19:56:56+00:00		2025-02-22 19:56:56+00:00		/storage/emulated/0/Podcasts		Podcasts				Vertical		
2025-02-22 19:56:56+00:00		2025-02-22 19:56:56+00:00		/storage/emulated/0/Ringtones		Ringtones				Vertical		
2025-02-22 19:56:56+00:00		2025-02-22 19:56:56+00:00		/storage/emulated/0/Alarms		Alarms				Vertical		
2025-02-22 19:56:56+00:00		2025-02-22 19:56:56+00:00		/storage/emulated/0/Notifications		Notifications				Vertical		
2025-02-22 19:56:56+00:00		2025-02-22 19:56:56+00:00		/storage/emulated/0/Pictures		Pictures				Vertical		
2025-02-22 19:56:56+00:00		2025-02-22 19:56:56+00:00		/storage/emulated/0/Movies		Movies				Vertical		
2025-02-22 19:56:56+00:00		2025-02-22 19:56:56+00:00		/storage/emulated/0/Download		Download				Vertical		
2025-02-22 19:56:56+00:00		2025-02-22 19:56:56+00:00		/storage/emulated/0/DCIM		DCIM				Vertical		
2025-02-22 19:56:56+00:00		2025-02-22 19:56:56+00:00		/storage/emulated/0/Documents		Documents				Vertical		

Fig 9: image cache



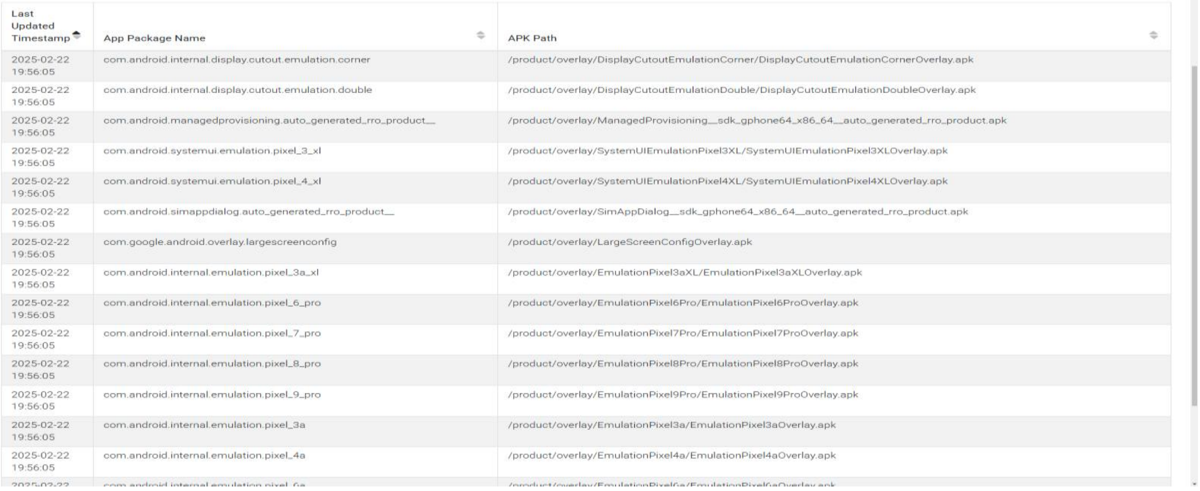
Timestamp Last Modified	Media	Filename	Source File
2025-02-22 20:15:27		QhvYF_7OjT7rFjud56msaV71u2A.cnt	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.microsoft.teams\cache\image_cache\v2.ols100.1\71\QhvYF_7OjT7rFjud56msaV71u2A.cnt
2025-02-22 20:15:30		8xIXou8NhkexD49fGroqgdI_nPc.cnt	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.microsoft.teams\cache\image_cache\v2.ols100.1\7\8xIXou8NhkexD49fGroqgdI_nPc.cnt
2025-02-22 20:15:31	AS	DMgMB1ORmLDbjI_w5X8uHc21sf4.cnt	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.microsoft.teams\cache\image_cache\v2.ols100.1\38\DMgMB1ORmLDbjI_w5X8uHc21sf4.cnt

Fig 10: gboard sessions

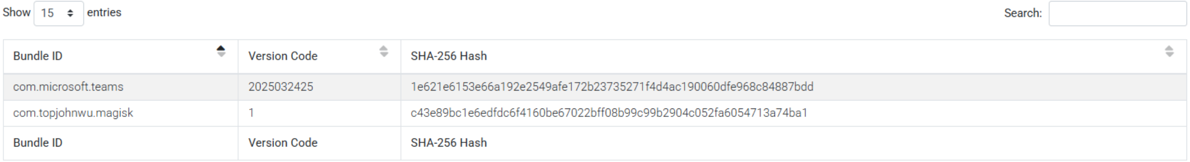


Start	Finish	Session ID	Application
2025-02-22 20:00:34	2025-02-22 20:00:44	1740254434578	com.google.android.gms
2025-02-22 20:02:33	2025-02-22 20:02:37	1740254553093	com.android.vending
2025-02-22 20:06:13	2025-02-22 20:06:25	1740254773822	com.microsoft.teams
2025-02-22 20:06:40	2025-02-22 20:06:59	1740254800135	com.microsoft.teams
2025-02-22 20:07:15	2025-02-22 20:07:34	1740254835949	com.microsoft.teams
2025-02-22 20:07:34	2025-02-22 20:07:43	1740254854368	com.microsoft.teams
2025-02-22 20:07:43	2025-02-22 20:07:44	1740254863936	com.microsoft.teams
2025-02-22 20:16:30	2025-02-22 20:20:59	1740255390408	com.microsoft.teams
2025-02-22 20:21:10	2025-02-22 20:21:14	1740255670810	com.microsoft.teams
2025-02-22 20:22:38	2025-02-22 20:22:48	1740255758354	com.microsoft.teams
2025-02-22 20:23:08	2025-02-22 20:23:10	1740255788982	com.microsoft.teams
2025-02-22 20:23:45	2025-02-22 20:23:46	1740255825799	com.microsoft.teams
2025-02-22 20:24:05	2025-02-22 20:24:06	1740255845476	com.microsoft.teams
2025-02-22 20:24:41	2025-02-22 20:24:52	1740255881494	com.microsoft.teams
2025-02-22 20:24:59	2025-02-22 20:25:01	1740255899112	com.microsoft.teams
2025-02-22 20:25:29	2025-02-22 20:25:29	1740255929297	com.microsoft.teams
2025-02-22 20:25:29	2025-02-22 20:25:42	1740255929486	com.microsoft.teams
2025-02-22 20:25:42	2025-02-22 20:25:47	1740255942494	com.microsoft.teams
2025-02-22 20:25:47	2025-02-22 20:25:53	1740255947844	com.microsoft.teams
2025-02-22 20:25:53	2025-02-22 20:26:10	1740255953079	com.microsoft.teams
2025-02-22 20:26:10	2025-02-22 20:26:16	1740255970347	com.microsoft.teams
2025-02-22 20:26:16	2025-02-22 20:26:37	1740255976221	com.microsoft.teams
2025-02-22 20:26:37	2025-02-22 20:26:44	1740255997393	com.microsoft.teams
2025-02-22 20:26:44	2025-02-22 20:27:06	1740256004233	com.microsoft.teams
2025-02-22 20:28:50	2025-02-22 20:29:40	1740256130863	com.microsoft.teams
2025-02-22 20:29:41	2025-02-22 20:29:46	1740256181597	com.microsoft.teams

Fig 11: installed apps



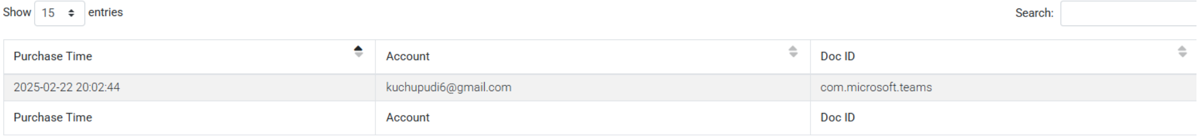
Last Updated Timestamp	App Package Name	APK Path
2025-02-22 19:56:05	com.android.internal.display.cutout.emulation.corner	/product/overlay/DisplayCutoutEmulationCorner/DisplayCutoutEmulationCornerOverlay.apk
2025-02-22 19:56:05	com.android.internal.display.cutout.emulation.double	/product/overlay/DisplayCutoutEmulationDouble/DisplayCutoutEmulationDoubleOverlay.apk
2025-02-22 19:56:05	com.android.managedprovisioning.auto_generated_rro_product__	/product/overlay/ManagedProvisioning__sdk_gphone64_x86_64__auto_generated_rro_product.apk
2025-02-22 19:56:05	com.android.systemui.emulation.pixel_3_xl	/product/overlay/SystemUIEmulationPixel3XL/SystemUIEmulationPixel3XLOverlay.apk
2025-02-22 19:56:05	com.android.systemui.emulation.pixel_4_xl	/product/overlay/SystemUIEmulationPixel4XL/SystemUIEmulationPixel4XLOverlay.apk
2025-02-22 19:56:05	com.android.simappdialog.auto_generated_rro_product__	/product/overlay/SimAppDialog__sdk_gphone64_x86_64__auto_generated_rro_product.apk
2025-02-22 19:56:05	com.google.android.overlay.largescreenconfig	/product/overlay/LargeScreenConfigOverlay.apk
2025-02-22 19:56:05	com.android.internal.emulation.pixel_3a_xl	/product/overlay/EmulationPixel3aXL/EmulationPixel3aXLOverlay.apk
2025-02-22 19:56:05	com.android.internal.emulation.pixel_6_pro	/product/overlay/EmulationPixel6Pro/EmulationPixel6ProOverlay.apk
2025-02-22 19:56:05	com.android.internal.emulation.pixel_7_pro	/product/overlay/EmulationPixel7Pro/EmulationPixel7ProOverlay.apk
2025-02-22 19:56:05	com.android.internal.emulation.pixel_8_pro	/product/overlay/EmulationPixel8Pro/EmulationPixel8ProOverlay.apk
2025-02-22 19:56:05	com.android.internal.emulation.pixel_9_pro	/product/overlay/EmulationPixel9Pro/EmulationPixel9ProOverlay.apk
2025-02-22 19:56:05	com.android.internal.emulation.pixel_3a	/product/overlay/EmulationPixel3a/EmulationPixel3aOverlay.apk
2025-02-22 19:56:05	com.android.internal.emulation.pixel_4a	/product/overlay/EmulationPixel4a/EmulationPixel4aOverlay.apk
2025-02-22	com.android.internal.emulation.pixel_6a	/product/overlay/EmulationPixel6a/EmulationPixel6aOverlay.apk



Show 15 entries

Search:

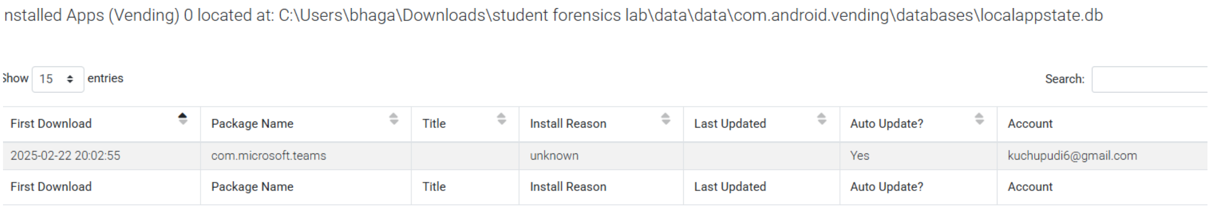
Bundle ID	Version Code	SHA-256 Hash
com.microsoft.teams	2025032425	1e621e6153e66a192e2549afe172b23735271f4d4ac190060dfe968c84887bdd
com.topjohnwu.magisk	1	c43e89bc1e6edfdc6f4160be67022bff08b99c99b2904c052fa6054713a74ba1
Bundle ID	Version Code	SHA-256 Hash



Show 15 entries

Search:

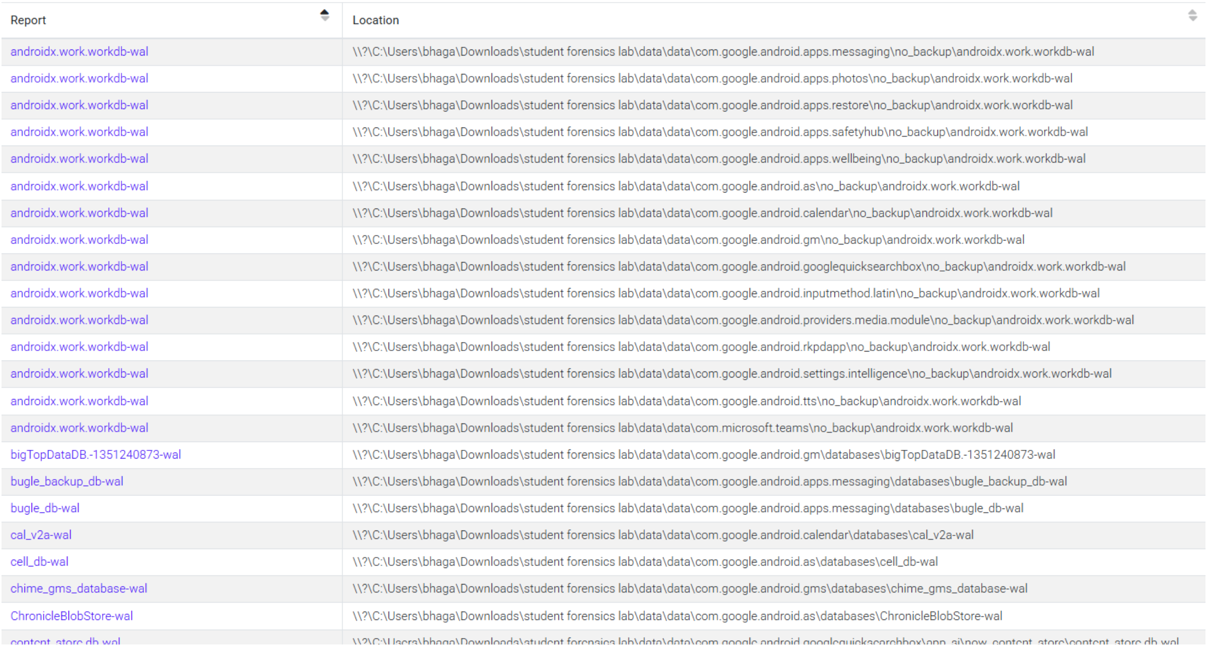
Purchase Time	Account	Doc ID
2025-02-22 20:02:44	kuchupudi6@gmail.com	com.microsoft.teams
Purchase Time	Account	Doc ID

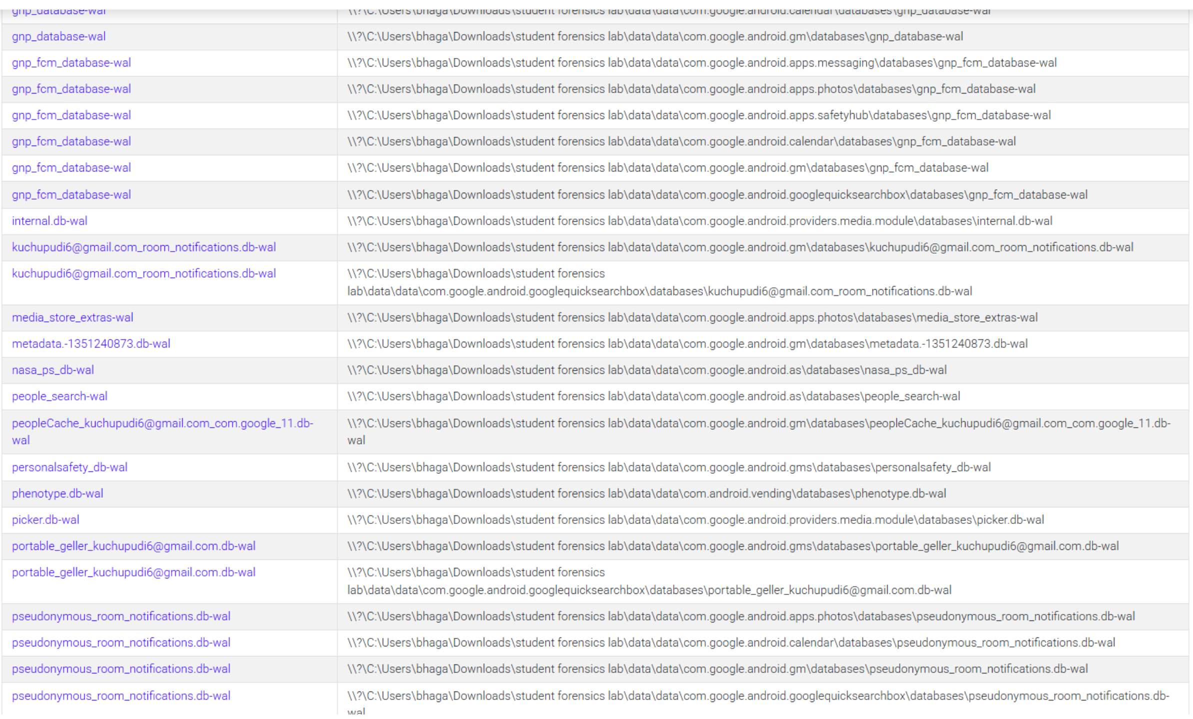


nstalled Apps (Vending) 0 located at: C:\Users\bhaga\Downloads\student forensics lab\data\data\com.android.vending\databases\localappstate.db

First Download	Package Name	Title	Install Reason	Last Updated	Auto Update?	Account
2025-02-22 20:02:55	com.microsoft.teams		unknown		Yes	kuchupudi6@gmail.com
First Download	Package Name	Title	Install Reason	Last Updated	Auto Update?	Account

Fig 12: SQLite journaling





Report	Location
androidx.work.workdb-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.apps.messaging\no_backup\androidx.work.workdb-wal
androidx.work.workdb-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.apps.photos\no_backup\androidx.work.workdb-wal
androidx.work.workdb-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.apps.restore\no_backup\androidx.work.workdb-wal
androidx.work.workdb-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.apps.safetyhub\no_backup\androidx.work.workdb-wal
androidx.work.workdb-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.apps.wellbeing\no_backup\androidx.work.workdb-wal
androidx.work.workdb-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.as\no_backup\androidx.work.workdb-wal
androidx.work.workdb-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.calendar\no_backup\androidx.work.workdb-wal
androidx.work.workdb-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.gm\no_backup\androidx.work.workdb-wal
androidx.work.workdb-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.googlequicksearchbox\no_backup\androidx.work.workdb-wal
androidx.work.workdb-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.inputmethod.latin\no_backup\androidx.work.workdb-wal
androidx.work.workdb-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.providers.media.module\no_backup\androidx.work.workdb-wal
androidx.work.workdb-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.rkpdapp\no_backup\androidx.work.workdb-wal
androidx.work.workdb-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.settings.intelligence\no_backup\androidx.work.workdb-wal
androidx.work.workdb-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.tts\no_backup\androidx.work.workdb-wal
androidx.work.workdb-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.microsoft.teams\no_backup\androidx.work.workdb-wal
bigTopDataDB.-1351240873-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.gm\databases\bigTopDataDB.-1351240873-wal
bugle_backup_db-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.apps.messaging\databases\bugle_backup_db-wal
bugle_db-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.apps.messaging\databases\bugle_db-wal
cal_v2a-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.calendar\databases\cal_v2a-wal
cell_db-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.as\databases\cell_db-wal
chime_gms_database-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.gms\databases\chime_gms_database-wal
ChronicleBlobStore-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.as\databases\ChronicleBlobStore-wal
content_store.db-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.googlequicksearchbox\app_si\now_content_store\content_store.db-wal
gnp_database-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.calendar\databases\gnp_database-wal
gnp_database-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.gm\databases\gnp_database-wal
gnp_fcm_database-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.apps.messaging\databases\gnp_fcm_database-wal
gnp_fcm_database-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.apps.photos\databases\gnp_fcm_database-wal
gnp_fcm_database-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.apps.safetyhub\databases\gnp_fcm_database-wal
gnp_fcm_database-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.calendar\databases\gnp_fcm_database-wal
gnp_fcm_database-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.gm\databases\gnp_fcm_database-wal
gnp_fcm_database-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.googlequicksearchbox\databases\gnp_fcm_database-wal
internal.db-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.providers.media.module\databases\internal.db-wal
kuchupudi6@gmail.com_room_notifications.db-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.gm\databases\kuchupudi6@gmail.com_room_notifications.db-wal
kuchupudi6@gmail.com_room_notifications.db-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.googlequicksearchbox\databases\kuchupudi6@gmail.com_room_notifications.db-wal
media_store_extras-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.apps.photos\databases\media_store_extras-wal
metadata.-1351240873.db-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.gm\databases\metadata.-1351240873.db-wal
nasa_ps_db-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.as\databases\nasa_ps_db-wal
people_search-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.as\databases\people_search-wal
peopleCache_kuchupudi6@gmail.com_com.google_11.db-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.gm\databases\peopleCache_kuchupudi6@gmail.com_com.google_11.db-wal
personalsafety_db-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.gms\databases\personalsafety_db-wal
phenotype.db-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.android.vending\databases\phenotype.db-wal
picker.db-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.providers.media.module\databases\picker.db-wal
portable_geller_kuchupudi6@gmail.com.db-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.gms\databases\portable_geller_kuchupudi6@gmail.com.db-wal
portable_geller_kuchupudi6@gmail.com.db-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.googlequicksearchbox\databases\portable_geller_kuchupudi6@gmail.com.db-wal
pseudonymous_room_notifications.db-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.apps.photos\databases\pseudonymous_room_notifications.db-wal
pseudonymous_room_notifications.db-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.calendar\databases\pseudonymous_room_notifications.db-wal
pseudonymous_room_notifications.db-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.gm\databases\pseudonymous_room_notifications.db-wal
pseudonymous_room_notifications.db-wal	\\?\C:\Users\bhaga\Downloads\student forensics lab\data\data\com.google.android.googlequicksearchbox\databases\pseudonymous_room_notifications.db-wal