Mobile and Forensics
Vol. 5, No. 1, March 2023, pp. 01-11
ISSN: 2714-6685 (online), 2656-6257 (print)
DOI: http://dx.doi.org/10.12928/mf.v5i1.8046

FORENSIC ARTIFACT DISCOVERY AND SUSPECT PROFILING THROUGH GOOGLE ASSISTANT

[1]Saiyeda Marzia, [2]Tafsir Haque Arnob, [3]Md. Zahidur Rahman, [4]Jesmin Akhter and [5]Abu Sayed Md. Mostafizur Rahaman
[1,2,3]Department of Computer Science and Engineering, Bangladesh University of Professionals, Dhaka, Bangladesh
[4]Institute of Information Technology, Jahangirnagar University, Savar, Dhaka, Bangladesh
[5]Department of Computer Science and Engineering, Jahangirnagar University, Savar, Dhaka, Bangladesh
[1,*]saiyedamarziam@gmail.com, [2]sshuvo6219@gmail.com, [3]tharnob@gmail.com, [4]jesmin@juniv.edu
[5]asmmr@juniv.edu
[*]correspondence email

Abstract

It has become impossible to imagine modern society without the internet and mobile devices dominating our daily lives. As a result, popular apps like Google Assistant, Gmail, Google Home, etc., are quietly entering our veins. People aren't even aware of how much of a digital footprint they leave behind, let alone the fact that it can be completely chronologized and used to put any criminal in jail. The data that we intentionally send to Google is fully retrievable from both the client side (a mobile device) and the cloud. Even if a suspect changes his mobile device, his previous digital footprint still follows him wherever he goes. In this project, we pinpointed the location of the primary database and the major repository for Google Assistant. Here, forensic artifacts of interest from our inquiry have been revealed, including the timeline and copies of previously traded audio chats, as well as a record of deleted data. In addition to that, we have applied the K-means clustering algorithm to isolate the suspect's voice records and their chronological order among various call records stored in the cloud, where the cluster size is determined using the Silhouette score and the CH index. The findings of the research are to identify forensic artifacts and suspect profiling so that forensic investigators make it easier to conduct criminal investigations.

Keywords: Google Assistant, Cloud Forensics, Mobile Forensics, Suspect Profiling, Clustering

INTRODUCTION

Today, Google has ingrained itself in every aspect of our lives. We are incredibly reliant on smartphones. No matter whether it's Android, an iPhone, or a Tesla, Google is above all of them. With Google's massive storage facility and wide range of applications, life is getting easier day by day [1]. These applications not only give futuristic benefits, but they also silently push our data into huge risk [2][3]. Investigation of Google Assistant is not easy for forensic analytics, as it combines mobile and cloud forensics [4]. For deep-level analysis, we need powerful forensic tools. Inadequate imaging may prevent the discovery of forensic artifacts and pieces of evidence. Cloud forensics is another major challenge.

In [5], the authors have worked with Android mobile devices, connecting Google Assistant and Google Home Mini. Both client-centric and cloud-centric forensic analysis has been done using the Celebrate UFED physical analyzer. Like our project, they have used Google Takeout to extract Google Assistant data, but they did not recover the chronological other of voice call. In [6], Germanos introduced the type of personal data and its location in the virtual assistant ecosystem. They used Forensic Toolkit (FTK) for their research on Amazon's Alexa, Google's Assistant, and Microsoft's Cortana and questioned the existence of privacy issues; that is, some data is accessible to security professionals or an investigator, which has the possibility of forecasting a cyber-attack. Google Takeout was used to extract cloud data. Another study in [7] was conducted on Amazon Alexa with its smart speaker Echo Plus 2nd Generation and Google Assistant with its smart speaker Google Home Mini for finding digital evidence. The first section of the study agrees with our

Article History: *Received May 8, 2023; Revised June 17, 2023; Accepted September 7, 2023*

findings. The project is determined to find Google data from Google Assistant and *Google Home Mini*. A similar type of experiment is done with the Amazon Echo and Amazon Alexa. In [8], the authors have concerns about the continuous process of Alexa listening to private conversions, which are valuable evidence of digital forensics. In [9], the findings of the artifacts of Google Assistant in both the cloud and mobile devices were highly appreciated. A case study on mobile suspicious activities forensics is introduced in [10], The investigation of deleted data from mobile devices to determine whether or not the owner was a criminal is described in [11][12].

Our primary contribution to this research is the collection of Google Assistant data through mobile and cloud forensics. We used *Google Home Mini* and Google Assistant itself for data entry. We utilized Google Takeout to collect cloud data. Two Android mobile devices were used in several important steps of the investigation. The imaging process was done using the Magnet Acquire tool. The results were analyzed using the *FinalMobile Forensic* tool and ADB Shell. We found forensic artifacts of Google Assistant audio clips of users in different locations on the Samsung mobile device. We also found proof of Google Assistant eavesdropping while investigating the *Infinix* mobile device.

Based on the findings from cloud forensics, we have three additional contributions. Google Assistant audio clips of users' voices were retrieved from Google Takeout. We sought to discover the following among the audio clips: a) *How many users are present in the audio clips?* b) *Which voice records belong to which user?* c) *And finally, between two specific periods, how can we highlight the activities of any user in chronological order?* We used MFCC, PCA, and the K-mean clustering algorithm to discover the answers to the first two questions. Each cluster represented one user. We computed the silhouette score, elbow method, and CH index scores to show that our clustering is well-established. Furthermore, we have also produced spectrogram images. To respond the last query, we created our own Python code using several libraries to fetch Google Assistant activities within two specific periods.

METHODS

We have split our project into two major parts: Google Assistant data on mobile devices and on the cloud. We begin by retaining the mobile devices of the possible suspect user. Since we do not anticipate that random people will use the devices, Google Assistant is only responsible for carrying out voice commands from the suspected user. The Google Home Mini is flexible and has a range of facilities. There are many other people who use Mini, including our suspect user. We expect the other people to be friends and family members of the suspect user. Figure 1 shows the conceptual design of our project and points out the fact that all the voice inputs from all the users reach their destination, the cloud.

Mobile Data Acquisition

One Infinix and one Samsung smartphone were used. The Infinix X657B was lacking the main package "*com.google.android.googlequicksearchbox*." We used Infinix to set up a sample Google account. The special command "Hay! Google" triggers Google Assistant to respond to the user. All the commands and their immediate results are saved in the sample Google account. The package name "*com.google.android.googlequicksearchbox*" is needed for Google Assistant data collection. The Samsung SM-G960F package was used for Google Assistant data acquisition.

Samsung phones are also used to set up the Google Home Mini, which listens to everything around it, with the special command "OK! Google." We have included almost 500+ voice recordings using Google Home Mini. We've logged 150+ live questions, 1500+ consecutive conversational discussions with Google Assistant via Google Home Mini and received hundreds of feedback links in Google Assistant. All entries typically link to YouTube, various websites, music podcasts, simple text, and Google Map location details.

One of the major contributions is acquiring Google Assistant data from mobile devices, which isa very crucial task, especially with powerful forensic software. Most of the best mobile data acquisition software is not free; some paid versions are also not available for public purchase. Mobile forensic software companies are very rigid in their access to their highly sophisticated software. We are fortunate to have access to *Magnet Acquire* and the *FinalMobile Forensic* Tool.

Before creating an image of the mobile device, we rooted Samsung to break down all the barriersto the internal files. An image file is a basic step in the forensic analysis of digital devices. Googlehas stated in its account policy documents that Google does save activity records of audio, web searches, etc. on the mobile device on which the Google account is activated. We turned on USB debugging by turning on Developer Options in the settings. Then we used Magnet Acquire to create the image.

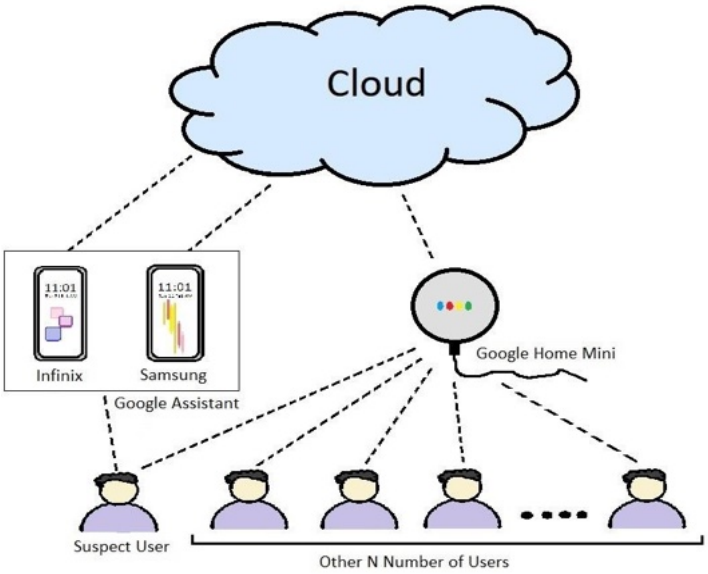


Figure 1 The conceptual project design

Cloud Data Acquisition

The second major contribution of this project is to collect Google Assistant data from the cloud. To extract Google Assistant data, we need to extract the entire activity log of user data from the sample Google account using Google Takeout. List of all the Google products linked to the account on the Google Takeout page. For export, we have the option to choose one or more products. The export process takes a reasonable amount of time to finish, depending on how much data is selected for download. Once it is complete, Google Takeout will send a notification email from which we can download the archived files in zip format. Figure 2 shows the results of taking out organizational files from a mobile device, the results of extracting data via Google Assistant and examples of the results.

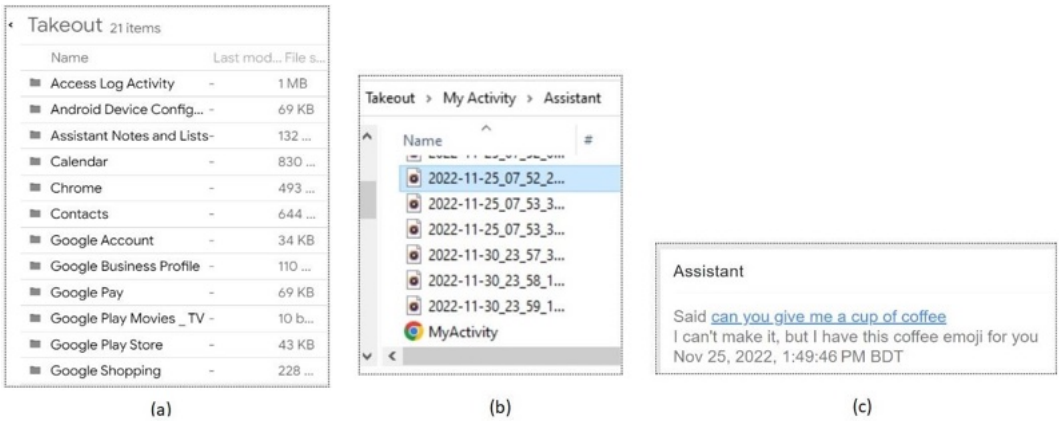


Figure 2. (a) Takeout file organization; (b) User-to-Google Assistant audio files; (c) Example of User-to-Google Assistant conversation

We were able to retrieve 21 items from the sample Google account (Figure 2.a). All audio files

of the user-to-Google Assistant are to be found in the *"Takeout/MyActivity/Assistant/"* folder. The inputs from the Google Assistant and Google Home Mini were found to be combined. We did not see any separation of the audio commands between "Ok! Google" and "Hay! Google." The audio files are in UTC-time-stamped MP3 format and do not require any extra software to play (Figure 2.b). It has all the voice commands, including background environmental sounds. Here is an example of the user's voice command: *"Can you give me a cup of coffee?"* was created on November 25, 2022, at 1:49:46 PM BDT. And Google replied, *"I can't make it, but I have this coffee emoji for you"* (Figure 2.c). This audio file was stored in the format *2022-11-25_07_49_47_730_UTC.mp3* inside the directory *"/Takeout/MyActivity/Assistant/."* The size of the audio files varies from 9 to 20 KB. The creation date is used to classify files. The conversation between "Google Assistant-to-User" is found in the following path of the Takeout folder: *"/Takeout/MyActivity/Assistant/MyActivity.html"* in the HTML file format.

RESULTS

We did all the prerequisite experimental setups on the Samsung mobile device. Magnet Acquire has produced three files during the process of mobile image creation: *Samsung SM-G960F Logical Image-Data.tar, activity_log.txt,* and *image_info.txt*. The *image_info.txt* file contains the MD5 and SHA1 hash values of the image file, etc. The *FinalMobile Forensics* tool calculates MD5 in its own way for the image file and matches the value from *image_info.txt*. If the two hash values match, only then is the image file opened for analysis. Figure 3 shows the audio file and evidence on the data using Google Assistant.

Samsung: Evidence of Google Assistant Data in the "Files" Folder

Google Assistant data usually resides in the *com.google.android.googlequicksearchbox* package (Figure 3.a). At the bottom of this directory, there is a folder named *"files."* Inside the *"files"* folder, we have found hundreds of audio files under the directory *"data\data\a\data\com.google.android.googlequicksearchbox\files\datadownload\shared\public\."* These audio files are forensic artifacts. These audio files are named followed by a long digit number, e.g., *"datadownloadfile_1678683472305"*. The number at the end may indicate the serial number. As shown in Figure 3(b), we see that the audio files are not aligned in numerical order. There are no extensions for these files. or, we can say the *FinalMobile Forensic* tool failed to identify the file type. Whenever software fails to determine the file type of a file, the file type is shown as *"File."* From the *ADB* shell, we find that the audio files are *"data"* files, MIME type Application/binary-octet.

The files are in complete binary format. These binary files need to be converted into human-understandable forms. We were able to open one of the files, *"datadownloadfile_1678683472305",* in *Audacity* and hear a human voice along with a lot of noise after setting the byte order to *"no endianness,"* using one channel (mono), starting offset at 0 bytes, encoding signed 16-bit PCM, and sampling at 19000 Hz (Figure 4.b). The human voice giving commands to Google is shown in Figure 4(c).

Samsung: Evidence of Google Assistant Data in the "app_sid" Folder

One audio file and one PB file were discovered in the *"app_sid"* folder found in the directory of *"data\data\com.google.android.googlequicksearchbox\app_sid\enrollment\storage\"* using the *FinalMobile Forensic* Tool, but we could not determine the exact file type (Figure 3.c).

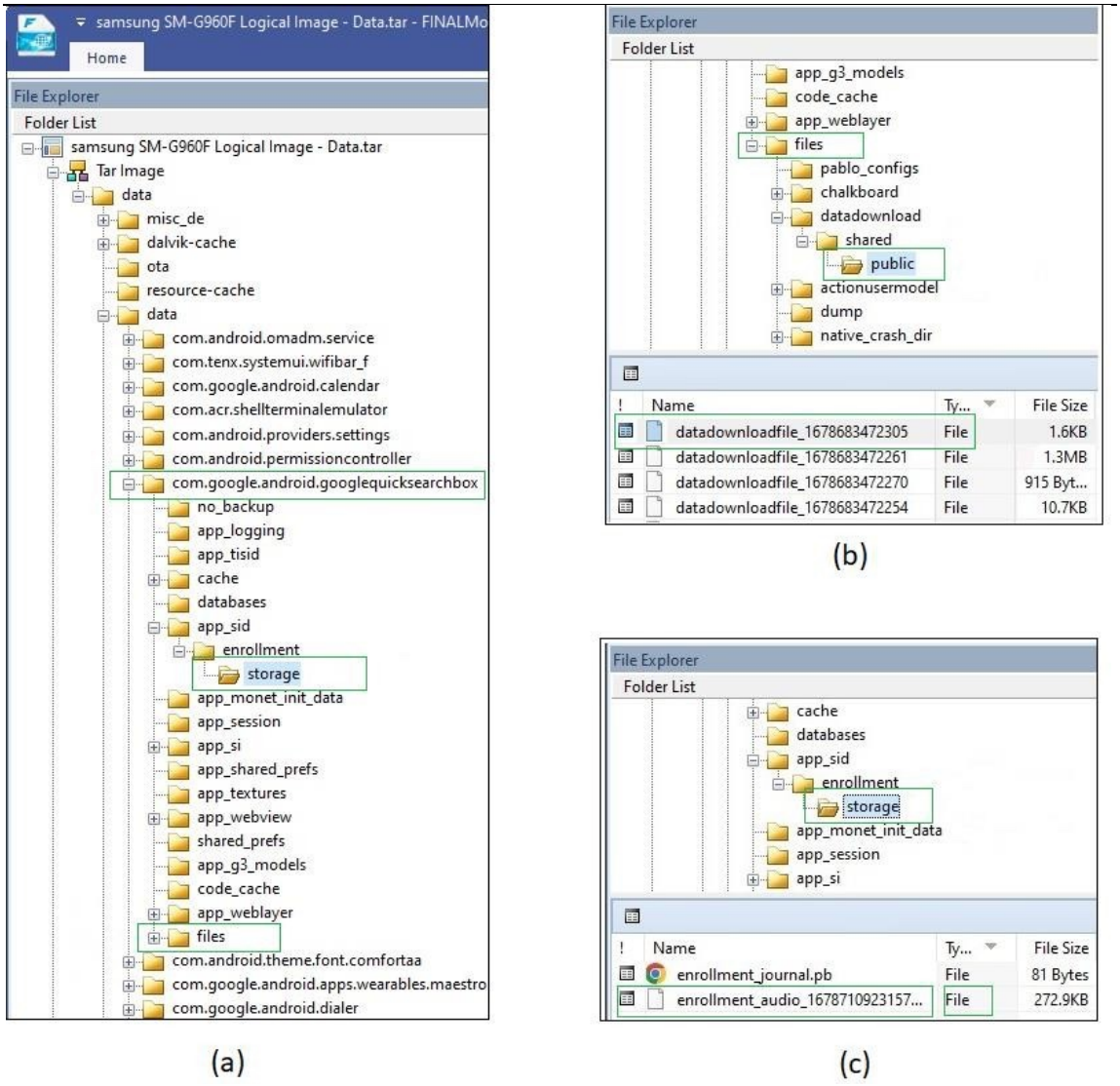
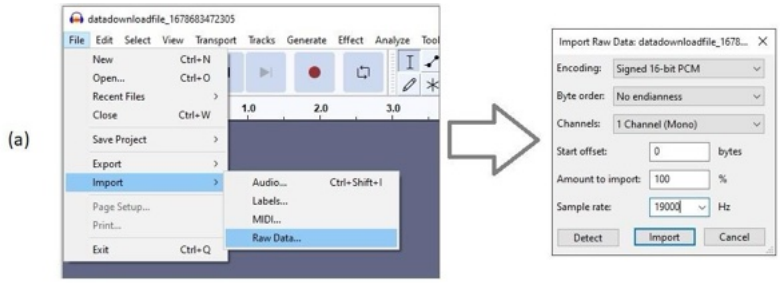


Figure 3. (a) Google Assistant audio files in the *com.google.android.googlequicksearchbox*; (b) evidence of Google Assistant data in the *files* folder; (c) evidence of Google Assistant data in the *app_sid* folder.



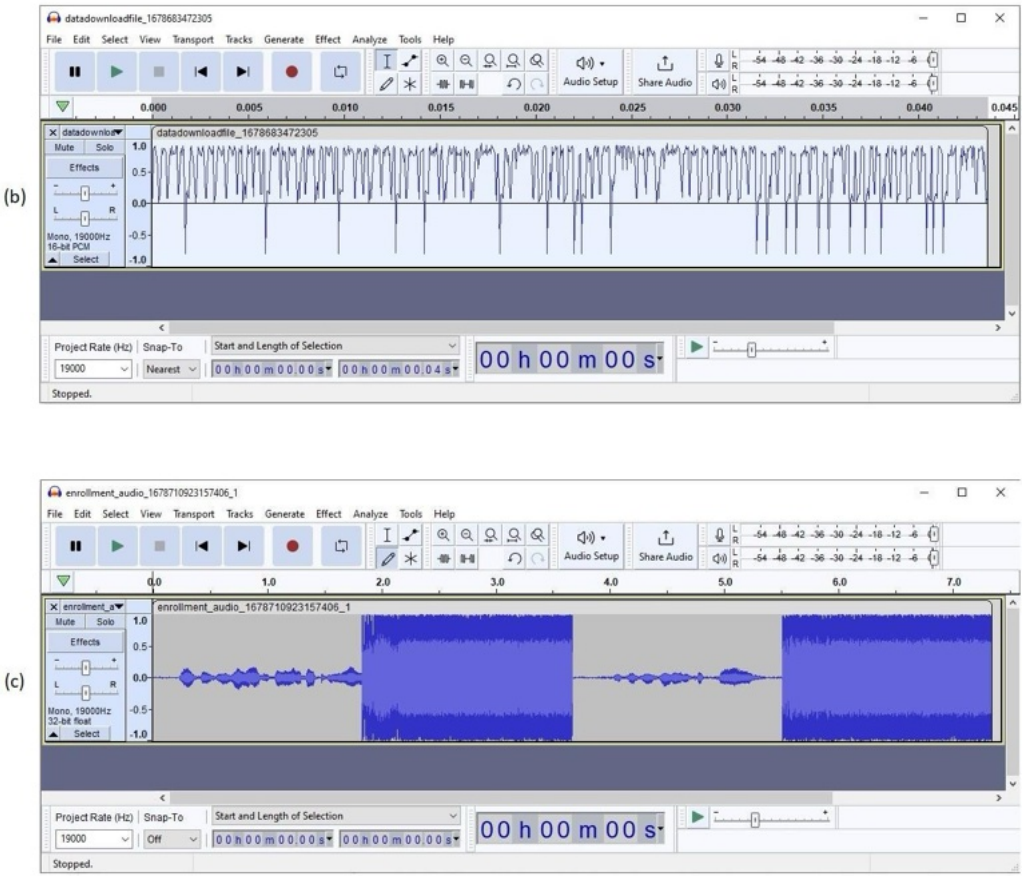


Figure 4. (a) Audacity setups (b) opening binary audio files using Audacity (c) opening "*enrollment_audio_1678710923157406_1*" using Audacity.

Using the ADB shell, we hit the *ls* command. Until this point, we had no idea that several interesting facts were just ahead of us. We were surprised by the ls command's discovery of a second file, *"enrollment_model_1678710923153780_1,"* which had no extension (Figure 5.a). This is a significant forensic finding. Either the *Magnet* Acquire tool failed to collect it or the Final Mobile Forensic tool failed to represent it. After that, we use the ls -s command to determine how many bytes it took up. Once we realize that the *ls -s* command has let us into Pandora's box, we are in a state of shock. We discovered another file called *"dd"* with no extension at the end (Figure 5.b). This *"dd"* file occupied 4 bytes, as we see in figure 5. Again, we have to say that either the MagnetAcquire tool failed to collect it or the FinalMobile Forensic tool failed to represent it.

Finally, we hit the *ls -n* command. The *"dd"* appeared to be very mysterious, as it was shown to have occupied 4 bytes in Figure 5, but now, it is showing 0 bytes. Our main audio file, *"enrollment_audio_1678710923153780_1"* consumed 279436 bytes in size; the file must be a combined form of all the audio clips that were added to the sample Google account till now. Using the same settings in Audacity, we were able to execute the file (Figure 4.a). We were able to decode two audio clips from the file. The two thinner lines in Figure 4(c) are human voices giving commands to Google. The fat parts make noise.

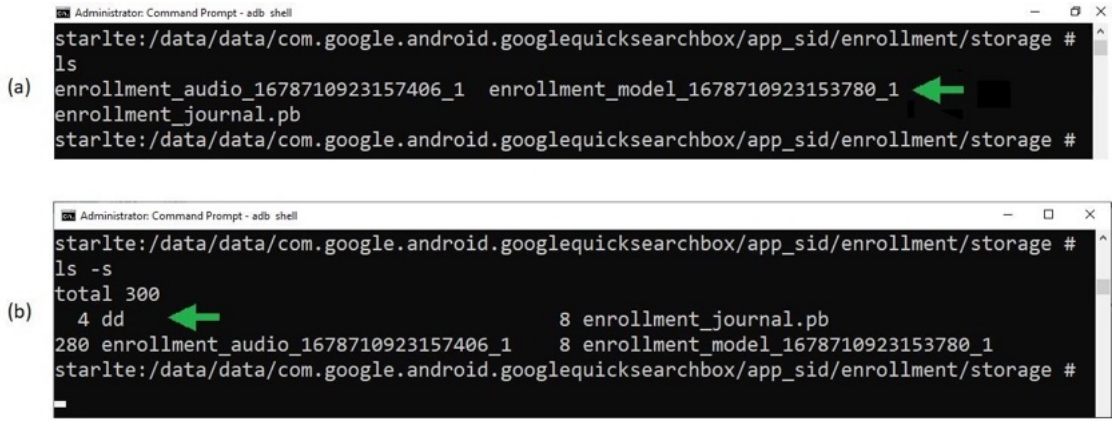


Figure 5. (a) finding the existence of the *enrollment_model_1678710923153780_1* file; (b) finding the existence of the *dd* file

Every digital action leaves digital traces that may be relevant as forensic artifacts. Even though the *Infinix* was not rooted, we still discovered evidence of Google Assistant eavesdropping and sending unrecorded voice inputs to an unidentified location. Following the same procedure as Samsung, we used Magnet Acquire to create an image file for the *Infinix* mobile device.

Infinix: Extracting Google Assistant's Feedback Links

On the Infinix mobile device, we found a folder named *"Okhttp3"* under the directory *"ExtractedFiles/Tar/adb-data /apps/com.google.android.apps.assistant/a/base.apk"*. This folder was very unusual and had so much to explore. We found the *"publicsuffixes.gz"* file under the directory *"/base.apk/okhttp3/internal/publicsuffix/publicsuffixes/}"*. We unzipped and opened the file in Notepad and found the partial web links of Google Assistant's feedback to user's requests , as shown in Figure 6.

Infinix: Proof of Google Assistant Eavesdropping

Final Mobile Forensic captured live data images of the *Infinix* mobile device. The tool captured all present activities from the memory. In the *"Live Data"* folder, all possible audio transmissions over the internet were documented. The highly important *"audio.txt"* file is located in the *"/Live Data/Dumpsys Data/"* directory that contains all input and output communication data via different apps to the internet. We need to carefully observe the highlighted parts, the date and time, and what functions are called in Figure 7. We have cross-checked the time of the green highlight parts can be found in Google Assistant's history, being the actual input of the user's voice. But as we can see, highlighted as *"blue marking boxes"* the same type of process has been generated and executed before. We found a huge number of similar processes to be generated and executed before and after real user voice input. Even at distinct times when no user voice input was nearby, these similar processes were found to have been executed.

We cross-checked with Google Assistant's history, and no recordings were found at these times. This means Google Assistant was silently listening but not recording. Or, we might say these inputs may have been recorded but not provided to the user's account.

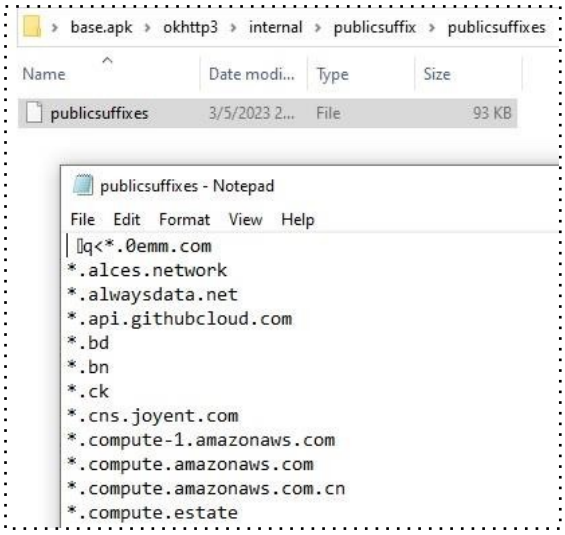


Figure 6. Output of the *publicsuffixes* file

Suspect Profiling

For our additional contributions, we have utilized a few Python features to conduct suspect profiling. We also want to highlight the activities of the suspect in chronological order. To achieve this, we have amassed 1,448 MP3 files containing all user voice recordings from Google Takeout. The 39 features of MFCC have been applied to these files. We attained Delta and Delta2. Using PCA's reduction technique, we have reduced the 39 features of the MFCC into only 10 major components. We used the *Python Librosa, NumPy, Sklearn, and Matplotlib* libraries to write the code. The K-mean clustering algorithm has applied to find the number of people used this device including our suspect. The value of K determines the number of users. For K = 3, we have calculated clusters 0, 1, and 2.

The elbow method is used to prove the value of K = 3 by calculating the WCSS value by applying (1) (Figure 8.a). The silhouette score is a standard measurement that can determine the perfection of a clustering technique. Using (2) for K = 3, we have calculated the highest silhouette score of 0.432430 (Figure 8.b). We obtained a Calinski-Harabasz index (CH) score of 2218.5143841018526 by using (3), which measures how well clustering algorithms have evolved. Now that we have confirmed the presence of three clusters representing three distinct users in the audio records collected from the cloud, we can easily compare the clusters with the recordings collected from the mobile device in order to identify the suspect.

The final and last contribution in this research consists of managing search requests for the suspect's activity between specified time frames in a precise chronological order. We are still in the development phase of this Python code. Based on the dates and times of every user, Figure 9 can show chronological activity. The cluster based chronological order is yet to come.

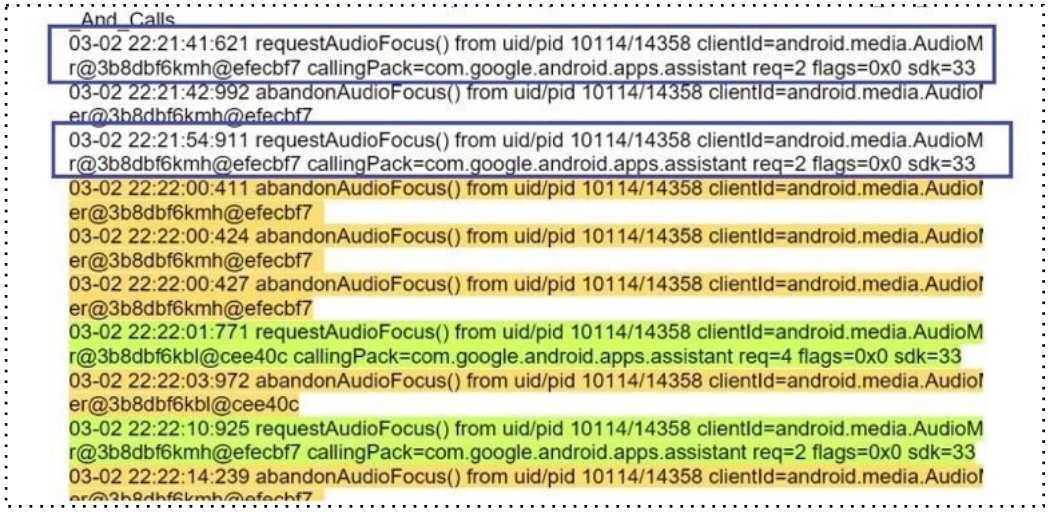


Figure 7. Google Assistant listens secretly.

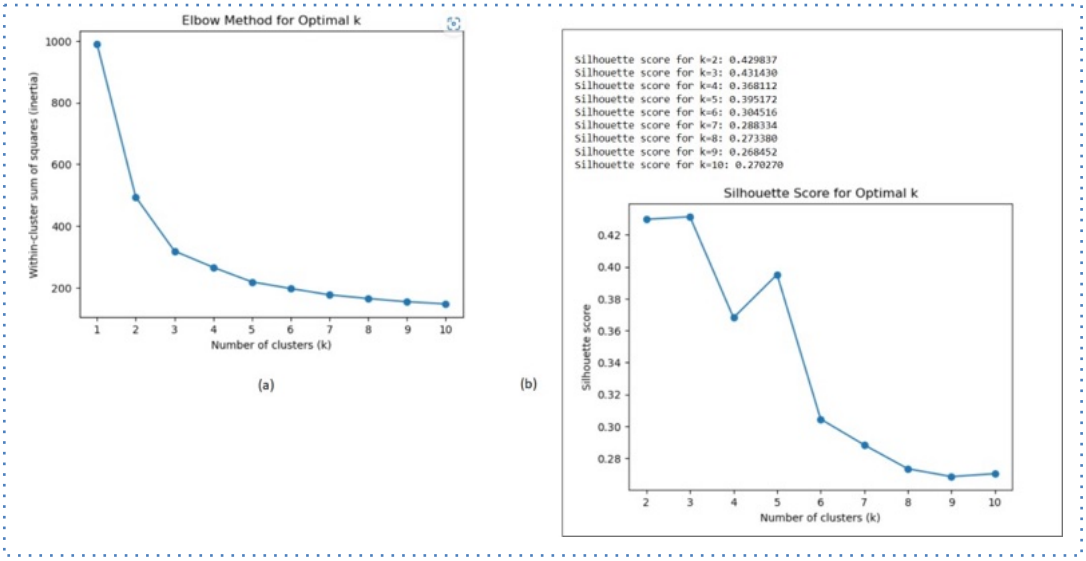


Figure 8. (a) Results of the Elbow Method; (b) Results of the Silhouette Score

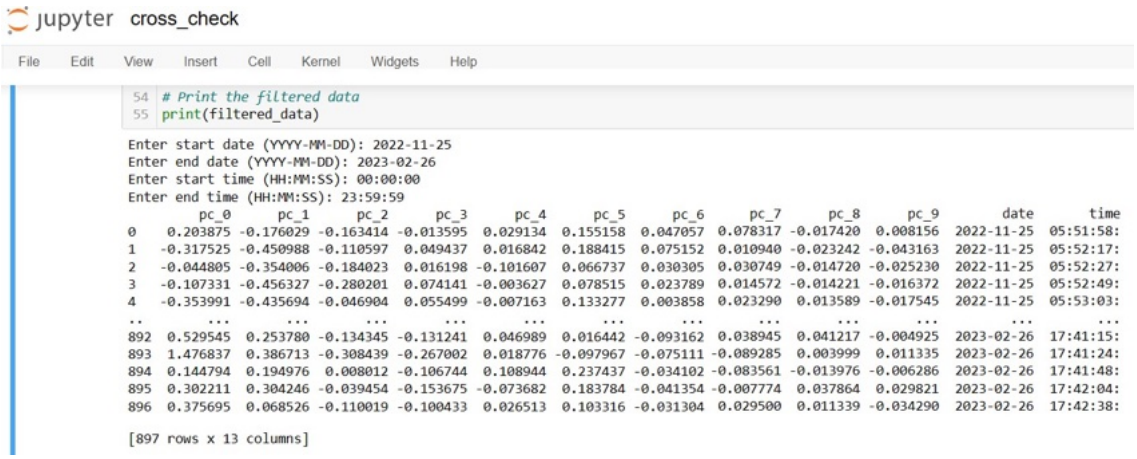


Figure 9. All users' activities in chronological order (including the suspect).

CONCLUSIONS

It's very challenging to locate anyone in this era who doesn't have some sort of relationship with technology. Smartphone ownership can be found among people of all social classes. The vast acceptance of the advantages should not lead us to the dark side of these technologies. It is not at all unusual to see Google Assistant at a crime scene. Our aim to conduct a forensic examination of Google Assistant was successful. On mobile devices, eavesdropping evidence and audio clip artifacts have been discovered. We have also been able to get data from the cloud. And finally, we were introduced to a suspect identification model based on the forensic artifacts we discovered. As part of our future work, we wish to unearth more mobile device artifacts. The audio files must be easily convertible into a form that people can comprehend and most importantly, we want to construct a client-centric and cloud-based chain of custody (CoC) for conducting digital forensic investigations on Google Assistant. In this research, we highlighted our major contributions and our future objectives. The findings of the research are to identify forensic artifacts and suspect profiling so that forensic investigators make it easier to conduct criminal investigations.

REFERENCES

[1] S. Levy, *In the plex: how Google thinks, works, and shapes our lives*, 1. ed. New York, NY: Simon & Schuster, 2011.

[2] N. Zhang, X. Mi, X. Feng, X. Wang, Y. Tian, and F. Qian, "Dangerous Skills: Understanding and Mitigating Security Risks of Voice-Controlled Third-Party Functions on Virtual Personal Assistant Systems," in *2019 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA: IEEE, May 2019, pp. 1381–1396. doi: 10.1109/SP.2019.00016.

[3] A. Klein, A. Hinderks, M. Rauschenberger, and J. Thomaschewski, "Exploring Voice Assistant Risks and Potential with Technology-based Users:," in *Proceedings of the 16th International Conference on Web Information Systems and Technologies*, Budapest, Hungary: SCITEPRESS - Science and Technology Publications, 2020, pp. 147–154. doi: 10.5220/0010150101470154.

[4] A. Castro and A. Perez-Pons, "Virtual Assistant for Forensics Recovery of IoT Devices," in *2021 7th IEEE Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, NY, USA: IEEE, May 2021, pp. 186–190. doi: 10.1109/BigDataSecurityHPSCIDS52275.2021.00043.

[5] A. Akinbi and T. Berry, "Forensic Investigation of Google Assistant," *SN COMPUT. SCI.*, vol. 1, no. 5, p. 272, Sep. 2020, doi: 10.1007/s42979-020-00285-x.

[6] G. Germanos, D. Kavallieros, N. Kolokotronis, and N. Georgiou, "Privacy Issues in Voice Assistant Ecosystems," in *2020 IEEE World Congress on Services (SERVICES)*, Beijing, China: IEEE, Oct. 2020, pp. 205–212. doi: 10.1109/SERVICES48979.2020.00050.

[7] I. Yildirim, E. Bostanci, and M. S. Guzel, "Forensic Analysis with Anti-Forensic Case Studies on Amazon Alexa and Google Assistant Build-In Smart Home Speakers," in *2019 4th International Conference on Computer Science and Engineering (UBMK)*, Samsun, Turkey: IEEE, Sep. 2019, pp. 1–3. doi: 10.1109/UBMK.2019.8907007.

[8] C. Krueger and S. McKeown, "Using Amazon Alexa APIs as a Source of Digital Evidence," in *2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, Dublin, Ireland: IEEE, Jun. 2020, pp. 1–8. doi: 10.1109/CyberSecurity49315.2020.9138849.

[9] K. P, K. G. Ganiga, C. L, A. Srivatsava, D. V. S. S. Kumar, and P. N. S, "Forensic Data Analysis using the Case Studies on Anti Forensic Devices," vol. 9, no. 9, pp. 49–52, Sep. 2022.

[10] D. D. Nath, N. I. Khan, J. Akhter, and A. S. Md. M. Rahaman, "Prediction of Android Malicious Software Using Boosting Algorithms," in *Emerging Technologies in Computing*, vol. 395, M. H. Miraz, G. Southall, M. Ali, A. Ware, and S. Soomro, Eds., in Lecture Notes of the

Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 395. , Cham: Springer International Publishing, 2021, pp. 21–36. doi: 10.1007/978-3-030-90016-8_2.
[11] D. Saha, S. Karmakar, F. N. Nur, A. Mariam, N. N. Moon, and A. Ahmed, "Mobile Device and Social Media Forensic Analysis: Impacts on Cyber-Crime," in *2021 1st International Conference on Emerging Smart Technologies and Applications (eSmarTA)*, Sana'a, Yemen: IEEE, Aug. 2021, pp. 1–8. doi: 10.1109/eSmarTA52612.2021.9515742.
[12] N. Zhang, X. Mi, X. Feng, X. Wang, Y. Tian, and F. Qian, "Understanding and Mitigating the Security Risks of Voice-Controlled Third-Party Skills on Amazon Alexa and Google Home," 2018, doi: 10.48550/ARXIV.1805.01525.

AUTHORS BIBLIOGRAPHY

SAIYEDA MARZIA
Saiyeda Marzia was the first Gold medalist from the IT department and the 7th place finisher at the third Convocation of UITS. In 2014, she graduated with a B.Sc. in Information Technology from the University of Information Technology & Sciences in Dhaka, Bangladesh. She won the scholar award at the CSE & IT Festival in 2012, which UITS organized. She did her undergraduate thesis on Cryptography, which was titled "A combination approach on Triple DES and AES: TDA-5." She is currently working on an ongoing research project on Digital Forensics as part of the MISS program at Bangladesh University of Professionals (BUP), where she is pursuing her Master's degree in Information Systems Security. Currently, she works at Contessa Solutions & Consultants Ltd. as a Cloud Engineer. Apart from studying, she spends the majority of her time volunteering with Haqqani Mission Bangladesh's youth programs. She also received professional classical music training and considers herself a student of Murshidi songs.

TAFSIR HAQUE ARNOB
Tafsir Haque Arnob has a BSc in CSE from BAIUST and is pursuing a Master's in Information Systems Security from the Bangladesh University of Professionals. He has participated in several programming contests, including the ICPC, and workshops on robotics and IoT. Tafsir secured the 68th position in the National Cyber Drill 2021 and continually updates his skills by completing training programs, such as Fundamental Web and Application Security Issues for NREN Professionals in 2021.

MD ZAHIDUR RAHAMAN
Md Zahidur Rahaman has been serving in Bangladesh Army since 2001. He has served in various capacities at different outfits of Bangladesh Army and Border Guard Bangladesh. He has done BSc in Electrical Electronic and Communication Engineering (EECE) from the Military Institute of Science and Technology. He is a graduate from Defence Services Command and Staff College, Mirpur, Bangladesh. Presently, he is pursuing aster's in information system security in Bangladesh University of Professional.

JESMIN AKHTER
Jesmin Akhter has received PhD degree in 2019 in the field of 4G wireless networks. from Department of Computer Science and Engineering of Jahangirnagar University, Savar, Dhaka, Bangladesh and obtained M.Sc Engineering degree in Computer Science and Engineering from Jahangirnagar University, Savar, Dhaka, Bangladesh in 2012. She also received her B.Sc. Engineering degree in Computer Science and Engineering from Jahangirnagar University, Savar, Dhaka, Bangladesh in 2004. Since 2008, she is a faculty member having current Designation "Professor" at the Institute of Information Technology in Jahangirnagar University, Savar, Dhaka, Bangladesh. Currently her research focuses are on IoT, network traffic, complexity and algorithms and software engineering. Being a dynamic and versatile person who is capable of merging innovative ideas, technology, knowledge, and experience for positive contribution towards the system development in the rapidly changing scenario of Information Technology and become a good teacher in the field of software and telecommunication systems.

ABU SAYED MD. MOSTAFIZUR RAHAMAN
Abu Sayed Md. Mostafizur Rahaman received his PhD degree in 2014 from the Department of Computer Science and Engineering of Jahangirnagar University, Savar, Dhaka, Bangladesh, and obtained his M.Sc. degree from Stuttgart University at Stuttgart, Germany, in Information Technology (INFOTECH) in the branch of *Embedded System Engineering* in 2009. He received his B.Sc. degree in Electronics and Computer Science, from Jahangirnagar University, Savar, Dhaka, Bangladesh, in 2003. Since 2004, he has been a faculty member with the current designation ″Professor″ in the Department of Computer Science and Engineering of Jahangirnagar University, Savar, Dhaka, Bangladesh. During his graduation, he worked at BOSCH (biggest automobile company in Germany) as a trainee engineer (Industrial internship) as part of his graduate degree in embedded systems. Currently, his research focuses on Digital Forensics, Cryptography, IoT, Web Security and S/W Systems.