Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

Forensic Perception of Artifacts Retrieval From Smart Wearable Glassess

Ramakrishnan P.N.*
Assistant Director & Scientist-C (Physics)
Central Forensic Science Laboratory
Directorate Of Forensic Science Services
Ministry Of Home Affairs, Govt. Of India
Hyderabad, Telangana State

***Abstract:-* With the dawn of increasing latest trends in Smart Augmented Reality Technology Wearable Devices (SARTWD) becoming the part and parcel of the day to day activity and integral part of the general public, the probability of these AR technology wearable devices to be encountered in electronic crimes also certain. Such devices as electronic evidence can be a challenge to forensic connoisseurs. The popularity of its usage is found alarmingly increasing every day as per the data released by International Data Corporation, during the year 2017-18. Wearable technologies are found mostly coupled with the mobile devices through their respective Apps. With increasing trends in mobile consumerization and advent of 5G telecommunication technology, the wearable technology devices are also improvising built-in applications knowhow. Today, the most common wearable technology devices that prevails are Smart Watches, Wrist Bands, Digital Smart Glasses, Implantable like Pacemakers or Defibrillators or Biosensors, Smart Jewels, Smart Clothing, Head Mounted Devices like Oculus or Rift etc. Of these, the most common and popular Wearable Devices are (i) Smart Watches, (ii) Wrist Bands or Fitness Bands and (iii) Smart Wearable Glasses. With contemporary advent and popular usage of these smart wearables, a new challenge would be encountered by the electronic forensic experts to retrieve the legalized artifacts from such ART Wearable Devices. In the present paper, the author present a brief theoretical methods available for the retrieval of artifacts from the Smart Augmented Reality Technology (SART) Wearable Glasses.**

Key Words : Smart Glasses, Artifacts, Electronic forensics

INTRODUCTION

2016-0034 - Data Protection and *smart glasses* - preliminary analysis

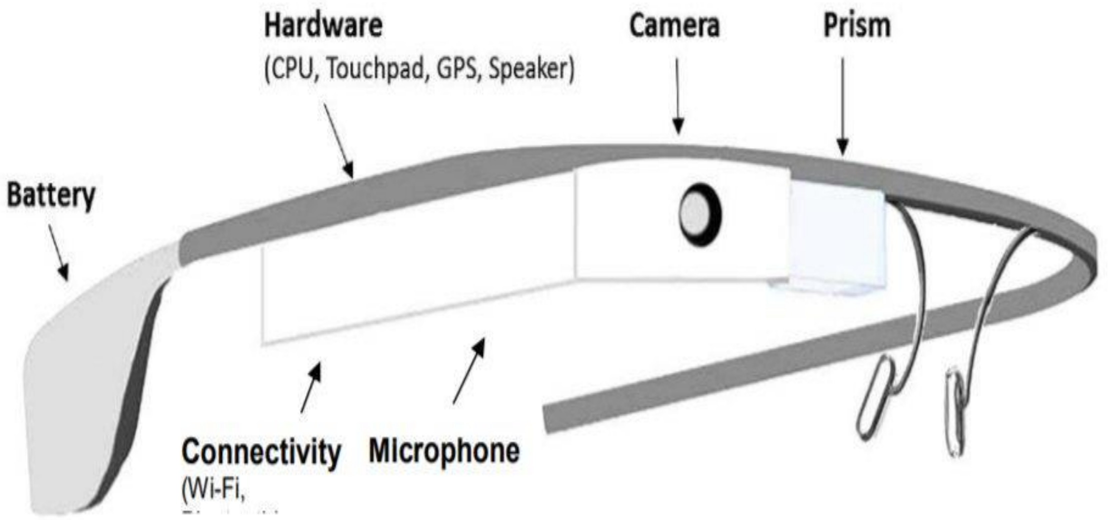

Figure 1. Smart Glass Hardware Components (Source: See endnote 2, license Creative Commons CC-BY)

Smart Wearable Glasses are similar to the conventional eye spectacles but with smart technology incorporated to display information within the eye field range. The Augmented Reality (AR) integrated in the smart glasses lets one to see text/graphic and other types of information in one's field of view. The Smart Glasses utilizes cellular technology , Wi-Fi, Internet as a mini-computer by running all the built-in Apps through the Smart Glasses Operating System.

The general components of the smart glasses comprises of CPU which maintain all the processing units, built-in capacitive sensors, Inertial Measurement Unit (IMU), GPS, built-in Wi-Fi and Bluetooth, Camera, microphone, speaker, the Display Unit and battery which is rechargeable. Mostly these devices were found to have third party developer software with voice activation enabled. The display unit is either mounted with an Optically Head Mounted Display or Augmented Reality or Heads Up Display Glasses. Most of these glasses are hands free and can communicate by human voice interface commands or both through touch pad.

These devices have the capability to control or retrieve or communicate data from other devices such as mobile equipment's or computers or other smart devices when synchronized through the applications either through Wi-Fi or Bluetooth or Internet. It is observed that most of the smart glasses run using Mobile Operating System such as Android based and also can function like a portable media players. These smart glasses wearable's has ability to capture pictures, video recording, search engines, GPS, to make or receive phone calls, fitness related data and other valuable information.

With the advent of the 5G cellular technology, the complexity of these Smart Glasses also increased with security based application also being introduced. In commercial context, the popular Smart Glasses available in market are belonging to GOOGLE, BOSE, NORTH, VUZIX, TENCENT, SAMSUNG etc.

METHODOLOGY

Based on the available literature and works carried out by the researchers all over the world it is observed that only few trial and error methodologies are being evolved and there is a very requirement of the standardized methodology to be developed. As on date, the methods followed are in principle in line of conformity with the NIST Guidelines for Mobile Device Forensics. The methods developed is mostly on the experimental works carried out on the "GOOGLE Glasses".

The extraction of the artifacts of forensic relevance from the smart wearable glasses could be obtained using the appropriate Software based techniques and few hardware based methodologies. It was observed that Android Developer Tools or ADT Suit Tools are required to be initialized on a Linux based operating machines. By installing the Python Script software and using the Linux commands, the rooting of the smart glasses for acquiring the image either logical or physical is possible. It is observed that tools like Scattered Script is most popular for acquisition through rooting methods as image of the smart glass wearable's. Using these tools the raw image of the smart glasses wearable can be successful. The hardware methods which were found to be utilized in the extraction of the raw image of the smart glasses were found to be NFI Memory Toolkit and JTAG method.

Once, the physical or logical image of the smart glasses is obtained, the raw data can be analyzed using SQLite Browser tools, Sleuth Kit and ADT Extractor. The data that could be extracted of forensic interest are mostly related to timeline, timestamps, voice commands, battery drain levels, pictures, images, videos, history browser files, thumbnails, meta-database files, MAC address of paired devices, contacts, call logs and other artifacts of audio files.

CONCLUSION

Based on literature survey studies, it is felt that much of the research can be carried out in the field of the smart glasses wearable's. This may be due to the complexity of the rooting methods and other chip-off techniques. As on date commercial hardware or software tools are yet to be developed. Hence, all the research so far were carried out on experimental basis only. The main vulnerability to apply these methods on real crime exhibits can be fatal at time since, these methods were not yet validated for minimizing the chance of the data getting data wiped off. However, initial works presented that abundant of forensic valuable artifacts information like activities in social media, browser history details, audio-video files, interaction with other messaging platforms, synchronization information, navigational information etc. can be obtained using these techniques mentioned.

REFERENCES

[1] NIST Special Publication; 800-101-revision, Guidelines on Mobile Devices Forensics, National Institute of Standards and Technology (2014).
[2] Google Glass Timeline Forensics; Blogspot (2014).
[3] Dumpsys, Android Developers; http://source.android.com/devices/tech/input/dump.html.
[4] Android Developer Tools, http://developer.android.com/too;s/help/adt.html
[5] Google Glass Specification Revealed, 16th April, 2013,http://cryptlife.com/gadgets/google-glass-specification.html