**Telegrip Forensic tool**

1. **Description**

The vast majority of our daily activities are carried out through mobile applications, that usually produce and store large data sets on the smartphone which makes the digital forensic analysis of this data play an important role during an investigation. Telegram is one of the social media applications that facilitate communication between individuals and groups, and it is widely used due to its various distinctive security features. Telegrip Forensic Tool was built as a reliable and easy-to-use tool to be used by the digital investigators to acquire, parse, and analyze needed information efficiently to be utilized in the cases related to Telegram messaging application.

1. **Features:**

Telegrip, a Python-based forensic tool aims to acquire and analyze sparse images, preserve evidence related to Telegram application while maintaining the integrity of the evidence gathered and reports produced. Telegrip helps digital investigators to extract and analyze artifacts generated on Android mobile phones by Telegram easily by using an interactive graphical user interface (GUI). Telegrip features include:

1. Telegrip acquires sparse image from Android mobile devices containing the device information and all Telegram-related data.
2. Parses and analyzes all types of messages, whether public such as channels and groups or private such as secret and normal messages, then it converts them into human readable format to aid the digital investigators during the investigation process.
3. The tool provides analysis of all types of media sent in different types of images, videos, documents, links, and GIF with the identity of the sender and the receiver.
4. Telegrip allows the digital investigator to create digital reports containing all the written comments and evidence selected by the investigator while ensuring the integrity of the report by calculating a hash value for each report.
5. Telegrip provides the feature of saving the digital case as a password-protected, where the passwords are securely stored using a salted hash.
6. **Installation and requirements**

Telegrip is applicable with Windows operating system and requires a database to store the cases’ information. The tool was developed using Python programing language, and the parsing techniques was tested with Telegram version (v7.4.1), and rooted Samsung Galaxy S6 edge with version 7.0 (Nougat) of Android operating system.

1. **License**

Telegrip License is GNU General Public License v2.0.

1. **Brief Tool Manual**

**1- Enter case information in the first interface to create a new case or open previously saved case.**

* When opening an existing saved case, enter the password if the case was password-protected.

**2- To acquire the device sparse image, click on create device image button.**



* Make sure the device is connected, then click on start imaging button.
* The image will be created, and you can start your investigation.

**Graphical user interface, application

Description automatically generated3- Click on and scroll through the evidence tree to analyze the image content.**

**4- To add an evidence to the report, click on the check box near the evidence in interest.**

Table

Description automatically generated with medium confidence

* Add comment if needed in the comment dialog box that appears after selecting the evidence.

**5- To generate the report, click on Generate report button.**



* The generated report will contain the selected evidence with their comments.
* Click on download button to export the report in PDF format.

**6- To save the case click on Save as button.**



* Enter the required information then click ok.
* To save the case as a password-protected, select the "protected " check box.