Computer networks, course 7020511-5: final project

In this project, you will study attacks on secure messaging apps, such as WhatsApp and Telegram.
Please carefully read the instructions.

Submission instructions

1. Submit a .pdf file, named XXXX_YYYY.pdf, where XXXX and YYYY are your IDs. The file should include:
   - Answers to all the questions in the "dry part" below.
   - Links to your Github project and LinkedIn accounts, as detailed below.

2. Generate a Github (if you don't have one yet) and upload all your code there. Generate a Github repo. The repo should include:
   - *src* directory, which includes all your code.
   - *resources* directory, that includes some sample raw data for your work (e.g., traces / .pcap files).
   - *res* directory, that includes the results (saved as text files / Python pickle files).
   - *Readme.md* (in English) explaining and documenting your work and main results.
   - You **must verify** that one can run your code by cloning the repo and following basic instructions you give in the Readme file.
3. Generate a LinkedIn account (if you don't have one yet) for each student, and publish there a project/post with a link to your Github account.

Submission integrity
You can use the authors' Python code in GitHub. You can also use other code from the Internet, and AI tools (e.g., ChatGpt).
However, you should
- Add at the end of your work a list of references / tools you used.
- If you use AI tools, it's your responsibility to verify their products.

Dry part

Read the paper Practical Traffic Analysis Attacks on Secure Messaging Applications.
You can skip the very details of the algorithm and the mathematical analysis.
Answer the following questions **in Hebrew**:
Explain in your own words the paper's main idea. In particular, refer to the following points:
1. How does the attacker obtain ground truth about the traffic of the channel?
2. How does the attacker wiretap the network traffic?
3. Describe shortly the conclusions from Table II in the paper.
4. Fig. 8 in the paper.

Add to the dry part links to your Github project and LinkedIn accounts.

Wet part

Record communication in at least instant messaging (IM) groups. The easiest way to do that is to use WhatsApp Web on a PC, and Wireshark.

Generate for each such group plots of the inter-message delays and the message sizes, similarly to those presented in the paper.
Are there unique characteristics for each group?
Can one deduce the groups you take part in using the techniques detailed in the paper?
Consider 2 cases:

- The attacked user is always active in (at most) a single IM group.
- The attacked user may be active in several IM groups simultaneously.

It's recommended to use Python, but other languages are accepted as well.