

TLFeat

A Dedicated, Robust and Fast TLS
Feature Extraction Tool

FAQ

Version: 0.90
Date: 2023-07

FAQ

1. Why TLSfeat has only command line?

TLSfeat is designed for feature extraction, and command line is easier to use for this goal. A GUI version might be released, but it's not clear if GUI will be useful. If you need GUI, let us know.

2. Can TLSfeat run in Windows?

TLSfeat supports only Linux for now, and the Windows version is going to be released. Meanwhile, virtual machines is recommended to use if you don't have Linux at hand.

3. Does TLSfeat support live capture?

No, it analyzes only pcaps.

4. Environment and running issues

a) Is virtual machine okay to run TLSfeat?

Though physical machines are preferred, TLSfeat can definitely run in virtual machines (we have tested it). Pay attention to hardware resources of virtual machines, especially CPU, memory and disk.

b) libpcap.so not found

This is a common issue. First, use `locate libpcap.so` to check if libpcap.so has been installed. Second, for Ubuntu, libpcap.so must be named as libpcap.so.1, and correct path should be `/usr/lib/x86_64-linux-gnu/libpcap.so.1`.

c) TLSfeat process is killed during analysis

A very likely reason is thread number specified is beyond CPU capability. e.g., a virtual machine has one 1 CPU, but TLSFeat is using 4 threads. Adjust threads to a proper value.

5. Is TLSfeat free to use?

Yes, it's free and distribute the program and documents under CC BY-NC-ND 4.0, e.g., for research and security analysis. However, you should not use the program and documents for commercial purposes or modify them.

6. Is it okay to publish a derived 'dataset' using TLSfeat?

'Dataset' in this context means structured features rather than pcaps. It's okay to publish a derived 'dataset' using TLSfeat, as long as the 'dataset' does not conflict interests with parties who collected or published the pcaps.

7. How to analyze huge pcaps?

TLSfeat has been tested to analyze single 10GB pcaps. It provides 'large mode' to analyze large pcaps (currently up to 1GB), but as the program may consume substantial memory, the thread number is limited. We are actively working on reducing memory usage.

For pcaps over 1GB, you can use Wireshark or other tools to filter non-TLS traffic.

8. Does TLSfeat have logs?

No, TLSfeat is 'log free', and all information is displayed in terminal.

9. Why messages printed in terminal is problematic?

If the terminal is using light theme, use `--no-color` option in common line. But it's suggested to use dark theme to show multicolors properly.

10. How to cite TLSfeat in research papers?

You may include the name, author and URL of the tool in research papers as citation.

11. How to report bugs, feedbacks and other questions?

TLSfeat is young, and there might be lots of bugs. Give us feedbacks through email <zliucd66@gmail.com> or post an issue. We will be glad to hear from you!

For bugs, please describe how to reproduce the bug, e.g., pcap, environment and screenshot. For feature requests, please describe use case.