Guidelines for contributing

===========================

To report a security issue (segfault, buffer overflow, infinite loop, arbitrary

code execution etc) please send an e-mail to security@tcpdump.org, do not use

the bug tracker!

To report a non-security problem (failure to compile, failure to capture packets

properly, missing support for a network interface type or DLT) please check

first that it reproduces with the latest stable release of libpcap. If it does,

please check that the problem reproduces with the current git master branch of

libpcap. If it does (and it is not a security-related problem, otherwise see

above), please navigate to https://github.com/the-tcpdump-group/libpcap/issues

and check if the problem has already been reported. If it has not, please open

a new issue and provide the following details:

\* libpcap version (e.g. from tcpdump --version)

\* operating system name and version and any other details that may be relevant

(uname -a, compiler name and version, CPU type etc.)

\* configure flags if any were used

\* statement of the problem

\* steps to reproduce

Please note that if you know exactly how to solve the problem and the solution

would not be too intrusive, it would be best to contribute some development time

and open a pull request instead.

Still not sure how to do? Feel free to [subscribe](https://www.tcpdump.org/#mailing-lists)

to the mailing list tcpdump-workers@lists.tcpdump.org and ask!