



defensics™

TRAFFIC CAPTURE FUZZER

New technologies are infested with reliability issues. The systems and protocols used are increasingly complex, the release cycles are getting faster and new technologies are adopted before they have been thoroughly tested. The most thorough and systemic way to test software is Model-Based Stateful Fuzzing. However, even though Defensics provides smart Model-Based Fuzzers for over 150 protocols, there is not a ready model for every protocol. Developing a Model-Based test solution requires a protocol or file format specification, and, occasionally, products in the development phase are not specified in detail, or the specifications are proprietary and unavailable for testers.

DEFENSICS Traffic Capture Fuzzer complements our existing product range by providing new testing solutions to meet these testing challenges and to increase the test capability of Model-Based tests. It is also a valuable tool in testing highly complex systems with several interfaces. Such systems should not be Fuzzed with Traffic Capture based tests only. However, real network captures provide powerful insight into the system, which can be used to target and refine the tests, and save valuable resources.

[Learn more »](#)

CODENOMICON Ltd.
info@codenomicon.com
www.codenomicon.com

Tutkijantie 4E
FIN-90570 OULU
FINLAND
+358 424 7431

10670 North Tantau Avenue
Cupertino, CA 95014
UNITED STATES
+1 408 252 4000

25/F., Queen's Road Centre
152 Queen's Road Central
HONG KONG
+852 3426 22900

What is Traffic Capture Fuzzing?

» **MORE PROTOCOLS:** Traffic Capture Fuzzing differs from Model-Based Fuzzing in that it does not require protocol specifications to analyze protocols. Instead it utilizes network traffic captures to generate Fuzzers for security and robustness testing. The DEFENSICS testing platform utilizes packet analyzers to detect and capture network traffic. The use of packet analyzers the analysis of unspecified and even unknown protocols, e.g., WIRESHARK identifies over 750 protocols and also recognizes other protocol traffic.

» **REAL NETWORK TRAFFIC:** Network traffic consists of a packet or a stream of packets. Each packet contains a headers formed by known transport layer protocols, which ensure the delivery of the payload, coded in the protocol of interest. By analyzing the traffic of lower level protocols, we can make observations about the higher level protocol they are transporting, more specifically, about the protocol's message structures.

» **EASY TO CREATE AND EXECUTE:** The collected data is used by the DEFENSICS Testing Platform to create a test model and to mutate actual messages into anomalous feeds. DEFENSICS creates and executes the test cases; all the user needs to do is edit the messages if they contain System Under Test (SUT) specific information.

» **INTEGRATION:** The Traffic Capture Fuzzing model can be further developed by integrating expert knowledge, e.g., when developing Traffic Capture based tests for proprietary protocols, the protocol owners' knowledge of their own protocol provides valuable insight, which can be used to fine tune the models.

What do Traffic Fuzzers bring to Fuzz Testing?

» **NO SPECIFICATION NEEDED:** Traffic Captures can be used as a quick and easy solution to fuzz protocols for which there are no existing DEFENSICS test suites. No protocol specifications are needed, because the Fuzzers are created from captured messages. Traffic captures can also be used to expand models used to test proprietary protocols extensions with real network traffic data. The best testing results are achieved by combining the information gained from Traffic Captures with protocol specifications.

» **SAVE MONEY BY TESTING EVEN EARLIER:** You can gain time and save money through preemptive security and robustness testing. In general, the earlier you start testing, the cheaper it is to fix the flaws. DEFENSICS Traffic Capture Fuzzer enables you to test your applications, before any standards exist. A software based solution is the perfect add-on to a developer's toolkit.

» **COMPLEMENTS EXISTING FUZZING SOLUTIONS:** Traffic Capture Fuzzing alone is not a comprehensive testing method. However, it enables you to priorities your security testing efforts and to expand your existing Model-Based testing solutions with easy-to-deploy, general purpose Fuzzing solution. Traffic Capture Fuzzing can also be used as a low-priced starting point towards more comprehensive Fuzzing solutions.

» **REPRESENTS REAL THREATS:** Fuzzing is a very representative testing method; it enables testers to accurately simulate potential attacks, and to patch the found vulnerabilities, before somebody else finds them and exploits them. Essentially, Fuzzing is doing what the attackers do, but before them.

Why Model-Based Fuzz Testing still pays-off

» **TEST EXECUTION TIME:** Intelligent Model-Based tests target the known weaknesses of the tested protocol, thus reducing test run time considerably without compromising the comprehensiveness of the tests. Short test execution times also allow the integration of tests into regression tests, and automated nightly and weekly test suites.

» **COVERAGE:** PCAP does not represent the whole protocol implementation. The selection it makes is limited, because it only captures samples of network traffic. You might miss important rare messages, and thus fail to test the entire software implementation. A Model-Based approach covers the standard specifications and contains an optimized set of tests to cover the specifications, thus providing a wider test coverage of the actual implementation. Traffic captures also ignore rarely used features, which tend to cause havoc in systems, because they are not subjected to heavy day-to-day usage.

» **INTERACTION WITH SUT:** PCAP based testing does not enable easy stateful testing. The network traffic captures cannot provide the information needed to understand the messages, thus the state of the SUT cannot be deciphered. Understanding the state of the SUT is a prerequisite for testing higher level protocols systematically.

» **ZERO-DAY VULNERABILITIES:** Traffic Capture Fuzzing is based on visible network traffic and known threat scenarios, and therefore it does not fully address the problem of unknown vulnerabilities. Model-Based testing consistently reaches better Zero-Day discovery rates than other testing methods.

» **CONCLUSION:** Traffic Capture Fuzzers, like any testing solution based on pure mutation, is a valuable tool for testing simple protocols. However, the testing of more complex protocol implementation comprehensively requires an intelligent Model-Based approach.

Check out protocols supported by Codenomicon DEFENSICS at www.codenomicon.com or contact us to create testing solutions to match your company's specific needs.