Ghidra vs IDA Pro. На что способен бесплатный тулзит для реверса, созданный в АНБ

Игорь Скулкин · Технический эксперт · Сообщество

В марте 2019 года Агентство национальной безопасности США (АНБ) опубликовало свой бесплатный тулзит для реверса и бинарного анализа Ghidra. Тулзит был представлен на конференции RSA и вызвал интерес сообщества. Мы обратили внимание на Ghidra еще на этапе RSA, а сейчас уже прошло достаточно времени, чтобы сделать выводы о том, насколько в АНБ для реверса. Пилотно ещё дорабатывать, чтобы в полной мере использовать в коммерческом проекте, но в исследовательских целях его стоит попробовать.

Проблема доверия

IDA в данном контексте Hex-Rays. Ghidra — бесплатный тулзит, который распространяется по лицензии Apache 2.0 и доступен на GitHub. Ghidra — это не просто замена IDA, это полноценная альтернатива. Мы сравнили Ghidra с IDA Pro по ключевым аспектам для реверса: декомпиляция, отладка, поддержка процессоров, скриптинг, производительность. Ниже — результаты сравнения, чтобы вы понимали, что можно ожидать от Ghidra.

Ghidra — бесплатный тулзит, созданный АНБ для реверса. Есть декомпилятор, отладчик, поддержка процессоров, скриптинг. Пилотно стоит доработать, чтобы в полной мере использовать в коммерческом проекте, но для исследований уже подходит.

Бесплатная IDA стоит в стиле Hacker. Ghidra стоит в стиле Ghidra. Ghidra — это не просто замена IDA, это полноценная альтернатива. Ghidra стоит использовать, если нужно: 1) бесплатный инструмент, 2) открытый исходный код, 3) поддержка нестандартных процессоров, 4) скриптинг на Ghidra Script API. Ghidra — это не просто замена IDA, это полноценная альтернатива. Ghidra стоит использовать, если нужно: 1) бесплатный инструмент, 2) открытый исходный код, 3) поддержка нестандартных процессоров, 4) скриптинг на Ghidra Script API. Ghidra — бесплатный тулзит, который распространяется по лицензии Apache 2.0 и доступен на GitHub. Ghidra — бесплатный тулзит, который распространяется по лицензии Apache 2.0 и доступен на GitHub. Ghidra — бесплатный тулзит, созданный АНБ для реверса. Есть декомпилятор, отладчик, поддержка процессоров, скриптинг. Пилотно стоит доработать, чтобы в полной мере использовать в коммерческом проекте, но для исследований уже подходит.

Ghidra — бесплатный тулзит, созданный АНБ для реверса. Есть декомпилятор, отладчик, поддержка процессоров, скриптинг. Пилотно стоит доработать, чтобы в полной мере использовать в коммерческом проекте, но для исследований уже подходит.