# An Introduction to Reverse Engineering

Jake Vossen

Colorado School of Mines - oresec

2019-03-19

# What is Software Reverse Engineering?

- IEEE defines it as “he process of analyzing a subject system to identify the system’s components and their interrelationships and to create representations of the system in another form or at a higher level of abstraction”
- Generally is taking a piece of compiled software and analyzing it, revealing information about the source code
- Often used in security research, but also have implication in game emulation and other areas of proprietary software.

# Why Ghidra?

| | Target OS: Linux | |
|---|---|---|
| IDAPROCL | IDA Pro Computer License [Linux] | 1879 USD |
| IDAPROFL | IDA Pro Floating License [Linux] | 2819 USD |
| IDASTACL | IDA Starter Computer License [Linux] | 979 USD |
| IDASTAFL | IDA Starter Floating License [Linux] | 1469 USD |
| HEXARM64FL | ARM64 Decompiler Floating License [Linux] | 3944 USD |
| HEXARM64L | ARM64 Decompiler Fixed License [Linux] | 2629 USD |
| HEXARMFL | ARM32 Decompiler Floating License [Linux] | 3944 USD |
| HEXARML | ARM32 Decompiler Fixed License [Linux] | 2629 USD |
| HEXPPCFL | PPC Decompiler Floating License [Linux] | 3944 USD |
| HEXPPCL | PPC Decompiler Fixed License [Linux] | 2629 USD |
| HEXX64FL | x64 Decompiler Floating License [Linux] | 3944 USD |
| HEXX64L | x64 Decompiler Fixed License [Linux] | 2629 USD |
| HEXX86FL | x86 Decompiler Floating License [Linux] | 3944 USD |
| HEXX86L | x86 Decompiler Fixed License [Linux] | 2629 USD |
| UPDHEXARM64FL | ARM64 Decompiler Floating Support Renewal [Linux] | 1319 USD |
| UPDHEXARM64L | ARM64 Decompiler Fixed Support Renewal [Linux] | 879 USD |
| UPDHEXARMFL | ARM32 Decompiler Floating Support Renewal [Linux] | 1319 USD |
| UPDHEXARML | ARM32 Decompiler Fixed Support Renewal [Linux] | 879 USD |
| UPDHEXPPCFL | PPC Decompiler Floating Support Renewal [Linux] | 1319 USD |
| UPDHEXPPCL | PPC Decompiler Support Renewal [Linux] | 879 USD |
| UPDHEXX64FL | x64 Decompiler Floating Support Renewal [Linux] | 1319 USD |

# And if that wasn't enough...

| | Shipping | |
|---|---|---|
| COURIER | Courier Shipping | 75 USD |

# Readable Mathematics

Let $X_1, X_2, \ldots, X_n$ be a sequence of independent and identically distributed random variables with $\mathrm{E}[X_i] = \mu$ and $\mathrm{Var}[X_i] = \sigma^2 < \infty$, and let

$$S_n = \frac{X_1 + X_2 + \cdots + X_n}{n} = \frac{1}{n} \sum_{i}^{n} X_i$$

denote their mean. Then as $n$ approaches infinity, the random variables $\sqrt{n}(S_n - \mu)$ converge in distribution to a normal $\mathcal{N}(0, \sigma^2)$.