

Reverse Engineering Business Guide

LEARN HOW CAN YOU LEGALLY BENEFIT FROM THE REVERSE ENGINEERING – THE MOST WANTED AND THE MOST FRIGHTENING SOFTWARE DEVELOPMENT TECHNIQUE

Mysterious Practice or Strong Business Approach You Can't Miss?

Every manager in software business is afraid to be a victim of the Reverse Engineering, but, like a forbidden fruit, everybody still wants to get benefit from it.

Reverse Engineering (RE) is the process of discovering the technological principles of a device, object or system through analysis of its structure, function and operation. It often involves taking something (e.g. a mechanical device, electronic component, or software program) apart and analyzing its workings in detail, used in maintenance or to try to make a new device or program that does the same thing without copying anything from the original. © Wikipedia.

Here we review different aspects of the Software Reverse Engineering to see how it can fit your needs, and what the proper way to use this powerful technique is.

Is It All About Your Software Project or Product? Yes, It Is.

If you are in the software business you are familiar with a lot of special *aspects of software project management*.

- You know how long, expensive and painful could be the integration of your software with some popular or especially not so popular systems. Different, often undocumented, file formats. Different and heterogeneous network protocols. Hidden and undocumented API calls. All this can delay your project up to 10 times, making your profits equal to zero or even negative.

- When you are starting to develop your own product, and there are several alternatives already on the market, you know that a wise solution would be to learn how your competitors work to avoid their errors and make your product even better.

- If you are stuck with huge legacy application with unreadable source code, and you need to integrate it into your new system, you know that everything may fall under the pressure of the really ugly code.

- If you are a development manager of a software company, you know how many undocumented things your target OS and libraries have, things that can become key points of your system. This report will show how you can benefit from them.

Just explore the following *situations*. Seem familiar, aren't they?

- Your product hit the audience and is selling well for 3 months, but then something happened which slowed down sales. You found out that competing product has appeared, which looks suspiciously similar to yours. And your task is to find out whether it is Reverse Engineered, and – if yes – is it possible to take this new product off by suing the competing company.

- Your brand new killing iPhone application is crashing on some devices, and working on others. And you suspect it is because new firmware is out, which has some changes, but Apple did not document this. And you should know what to do, because you are losing market each day you delay the release.

If you are a product manager, you know that to be the first on the market most of the times means to take huge market share. And you want to be the #1 with your product. We will provide you guidelines for the properly usage of the Reverse Engineering in your case.

Reverse Engineering can become indispensable tool in all of described situations as well as many others.

If you are a manager of any kind in the software development company you should know that Reverse Engineering can be used in a lot of ways for a lot of *purposes*:

- 1) Understanding how a product works more comprehensively than by merely observing it;
- 2) Investigating and correcting errors and limitations in existing programs;
- 3) Studying the design principles of a product as part of an education in engineering;
- 4) Making products and systems compatible so they can work together or share data;
- 5) Evaluating a product to understand its limitations;
- 6) Determining whether someone else has literally copied elements of one's own technology;
- 7) Creating documentation for the operation of a product whose manufacturer is unresponsive to customer service requests;
- 8) Transforming obsolete products into useful ones by adapting them to the new systems and platforms.

Main Threats About Not Using or Improper Using Of Reverse Engineering

You fail complex projects in crisis time, which results to big problems to you, your team and your company.

You can be made to pay 3rd party extremely huge amount of money to help you integrate with their software – those companies are making money this way.

You release products slower than competitors, and your market share is weak.

Your product contains security issues caused by interoperability with 3rd party tools and even Operating Systems.

You do not know hidden possibilities of your competing products, so you unexpectedly can lose market.

If you unwisely start using Reverse Engineering, you can be sued. This technique is very powerful and should only be used by highly experienced people.

2 Generic Ways to Solve Tasks without Reverse Engineering

1. You can download trial of your competing product, run it and see how it works. Also you can read documentation, for sure. Main disadvantage here is that it is extremely time consuming while your manager time costs a lot.
2. You can refuse on relying to undocumented stuff while your competitors are. You can think: “Oh, they are stupid, they will fail”. But what if they are not?

2 Generic Ways to Start Solving Tasks with the Reverse Engineering

1. You can hire extremely good and experienced developers, which has experience in everything. Choosing this way you should remember that it is just very hard to find them and often they are very expensive.
2. You can learn and start using Reverse Engineering yourself. The main threat here is to get issues with law - <http://www.jenkins.eu/articles/reverse-engineering.asp>

5th Approach to the Reverse Engineering – Safe and Profitable

So, what should you do if you want your Reverse Engineering work done safely and effectively? Below we provide you guidelines for this complex process.

At first you should not be afraid of using Reverse Engineering. It is a common practice in goods manufacturing, semiconductors and computer hardware. It is legal in these areas. There are several simple rules, which you should follow to get benefits from Reverse Engineering in *software business without problems*:

- You should legally own the software you are reverse engineering (buy or trial). It is easy.
- You should study license if it forbids Reverse Engineering. Some countries with emerging economies are still allowing this practice regardless any licensing statements.
- In the United States and many other countries, even if an artifact or process is protected by trade secrets, reverse engineering the artifact or process is often lawful as long as it is obtained legitimately. Patents, on the other hand, need a public disclosure of an invention, and therefore patented items do not necessarily have to be reverse engineered to be studied. One common motivation of reverse engineers is to determine whether a

competitor's product contains patent infringements or copyright infringements. See extract below:

"...[W]here disassembly is the only way to gain access to the ideas and functional elements embodied in a copyrighted computer program and where there is a legitimate reason for seeking such access, disassembly is a fair use of the copyrighted work, as a matter of law." Sega v. Accolade, 203 F.3d 596 (9th Cir. 1993)

So, now you see that Reverse Engineering is legal if used properly. Now you can see how you can **benefit from it**. It is easy.

The 5th approach we consider as the most safe, suitable and profitable is to **outsource Reverse Engineering tasks** to the professional team of Reversers. Several reasons can be mentioned to motivate this point:

- Professional team has knowledge of all legibility questions – they've worked for some time already and know what one may do and what may not.
- Professional team has experience in solving many tasks already. These specialists will spend much less time to get the answer as soon as they are familiar to a number of techniques, special tools and methods. They know what to do first, what to use, where to look in this stuff.
- Professional team can effectively grasp in a hard task as soon as Reverse Engineering is its main activity and it has already dealt with a lot of different unusual tasks.
- Professional team as a provider of the service is fully responsible for its quality. They can not just say after spending all of the assigned time: "We have not succeeded."

Just find proper Reverse Engineering experts who know law well and have deep experience. Examine their portfolio to see if they have experience in different areas of Reverse Engineering, including but not limited to your task or subject.

Several Tips You Should Remember Choosing The Right Reverse Engineering Experts

Bad Reverse Engineer can cause a lot of problems. Good Reverse Engineering Expert can bring your business to the next level. How to examine a pretender and choose the right variant?

First ensure that the pretending experts know the answers to these questions:

- Is the Reverse Engineering legal?
- What elements of a computer program are copyrightable?
- How does a court determine the difference between the ideas and expressions in a computer program?
- Are the functional elements of a software program protected by copyright?
- Is the Reverse Engineering affected by patent law?

- What kind of proof is necessary to show the copying of a computer program?
- Is the Reverse Engineering of a technological protection measure illegal under the DMCA?
- What are the limitations of the interoperability criteria for the DMCA's reverse engineering exemption?

Get the answers and ensure they are suitable for you.

Ask the experts if they are treating Reverse Engineering work as usual Software Development work – so, are they able to provide detailed project plan with time and money estimations for this work.

After that ensure pretenders have the experience in Reverse Engineering in general: find out how many years they are going for RE, what OS, software products and network systems they have worked with, what special tools they use.

Here Are Some Public Examples of Successful Reverse Engineering Usage

Google

http://news.cnet.com/8301-1001_3-10046395-92.html

Quote: *“Google stuck up for the practice, though. “Disassembling is a common and accepted practice in software development, frequently used to make sure software features are compatible with other software programs or operating systems,” the company said.”*

OpenOffice.org

OpenOffice.Org free office software package with its 15 millions of downloads is another good example of the Reverse Engineering applied well and properly. It is based on the results of the reverse engineering Microsoft Office file formats (way before they were made available to public by Microsoft themselves).

See the Real Success Story We Can Share With You

In this section we introduce you our Reverse Engineering team. Specialists from it helped a lot to create this guide and shared the real story from their work – to show you what is Reverse Engineering task and solution in real life.

All work usually done in Reverse Engineering is done under strict NDA (Non-Disclosure Agreement). We are able to disclose only a part of the information from our work experience. But we prefer to share successful stories, even if some details cannot be shared. We want to show you that Reverse Engineering can really save you time and money.

One of our customers was developing enterprise security system for Windows OSes. The biggest task was endpoint security which meant limiting user access to different periphery devices connected to PC.

It was pretty easy task until we met the necessity to manage access to the scanners for specified users.

The main complexity was the fact that - unlike other devices - access to scanning and imaging capability is provided not directly through the kernel level to user level processes (for which it is possible to detect User ID and apply security rules), but through the WIA (Windows Image Acquisition) Service which is run under LOCAL SYSTEM user account. So it was impossible to find easy way to manage access of different applications run by different users to the particular USB or LPT scanner from the kernel level perspective.

This task was given to our Reverse Engineering team.

It took them several weeks to reverse engineer WIA Service (which is in fact Windows COM service) and elaborate quick and easy set of hooks which made it possible to achieve target. After that proposed variants were researched properly and the most suitable one was implemented in the product.

Our preliminary estimations showed that plain approach without Reverse Engineering would take 4 months of the development with 80% probability to succeed, which was not satisfactory neither for us nor for our customer. So, this task was the critical task for the whole project where several man-years of the development were spent.

Results are applied and tested and became a part of the one popular product.

Continue the acquaintance with our Reverse Engineering Team

4 Things That Make Us Special Reverse Engineering Choice

1. We do Reverse Engineering for 6 years, with more than 60 tasks finished. Overall business value of our customers' saving could hardly be overestimated – it surely exceeds **\$1'000'000**. Our very brief portfolio includes:
 - a. Development of Fax Service Routing Engine for Windows 2003 Server Fax Service that provides fully customizable fax routing based on different criteria (CallerID, MS Office OCR). Full Active Directory Integration. During the development the built-in Windows 2003 Server Fax Service was extended by using undocumented information, system-wide API hooking and DLL injection.
 - b. RPC Proxy application for Microsoft Exchange with full logging of activity between client (Outlook) and Server (MS Exchange), full Exchange emulation. This project required reverse-engineering of several MS Exchange DLLs, and also Microsoft Outlook client, in order to get information about undocumented protocols as Microsoft RPC (MS RPC) and so on.
 - c. Implementing the routines for creating Outlook PST files. For this project we reverse-engineered MS PST system service, and developed our wrapper for it, which allows using all PST features.
 - d. Brute-force password breaker for well-known steganography tool "Steganos", and application for storing encrypted passwords "Stealth Password Kit". Heavy reverse engineering techniques was used, as password-breaking process should be performed as quickly as possible. Several flaws found in mentioned applications'

RSA algorithm implementation, so brute-forcing passwords was much quicker than exhaustive search.

2. We produce and sell our own software products and we know how to use Reverse Engineering in a legal way.
3. We have not only Reverse Engineering services - we also conduct 3 months Reverse Engineering courses for software developers.
4. We are treating Reverse Engineering work as usual software development – so, we are able to **provide detailed project plan with time and money estimations** for this work (and to follow them, of course). You are able to plan your budget for Reverse Engineering, which is very important for the large projects. And we believe that Reverse Engineering can be normal business practice with controlled and predictive results.

Use Our Reverse Engineering Experience – FOR FREE

It is clear for us that benefits of this powerful technique are hard to see when you do not use it.

So we decided to offer you the possibility to make a free check if Reverse Engineering is suitable and applicable for your project or product, within your organization and your business.

We would like to offer you **\$1000 Reverse Engineering Feasibility Audit for Free**.

During this Audit we will study your problem, task, project, product or anything you want us to study and provide at **no charge** the **Audit Report** which is to include the following items:

- Task Analysis (detailed task breakdown)
- Environment Analysis (OS, 3rd party products etc)
- Description of the approaches tried (with detailed information about the results of each approach, with links/code pieces etc)
- Recommended approach (with detailed steps description, description of the validation techniques used, if applicable – project plan with tasks breakdown could be provided)
- Additional information (usually it is plenty of information which our experts are getting during the work with task, we document all this for further usage)
- Prototypes, proof of concept, test code pieces and other deliverables

You do not have any obligation for the further work or any further relationships with us.

Our aim is your work experience with professional Reverse Engineering team.

Also please understand that due to high volume of work in Reverse Engineering area for our team this FREE offer is **limited in time by 30 days** after you download and read this report. We are doing our best to serve our current customers, and we still want you to get benefit from our experience, so this 30 days is reasonable trade-off between these 2 important goals.

Just email us at sales@apriorit.com and mention your interest in checking out Reverse Engineering abilities with no obligation to pay!

Or fill out the following form and fax it back to us to receive immediate response.

Please sign me up for a FREE Reverse Engineering Audit so I can make sure I get all possible benefits from it in my work. I understand that I am under **no obligation** to do or to buy anything by requesting this audit. I further understand that these audits are being made available on a **first-come, first-served basis**.

Please Complete And Fax Back:

Name:

Title:

Company:

Phone:

Fax

E-mail:

Fax To: +380-56-3715532

Call Me Direct At: +380-50-3401747