



---

# ICE License Overview – Cracking TomahawkGold 3.0

anorganix of ARTeam

December 2005

1.	Brief Introduction .....	2
2.	Things needed to get started .....	3
3.	Target Analysis .....	3
4.	Conclusions.....	5
5.	Greetings.....	5

### Keywords

ICE License, Delphi, TomahawkGold, OllyDbg, PExplorer, PEiD

## 1. Brief Introduction

ICE License is the strongest and most complete protection available today for Borland Delphi and C++ Builder. It is a new and innovative licensing protection system for Borland developers wishing to integrate copy protection and maximum security into their applications. With ICE License you can create "Trial Editions" of your software. Key generation is prevented using sophisticated asymmetric encryption technology. It is regularly evaluated by professional developers around the world. Their findings repeatedly demonstrate that this tool has many advantages over other copy-protection systems.

ICE License Overview :

- Antidebugging & Antimonitors Protection (protect against Code Tracing)
- Sophisticated Asymmetric Encryption Technology (prevent against Key Generator)
- Advanced Digital Authentication to prevent against patching
- Advanced Code Encryption Protection to prevent against cracking or dumping
- Transfer License to another PC (Trial License or Full License)
- Create a Key Generator for your partner or distributor
- Detects backdating or demo reinstallation to gain additional usage
- AES Rijndael Encryption functions to protect your data
- Cryptographic hashing MD5 to lock licenses to your software
- Reliable Machine Locking Protection (based on manufacturer's information)
- Network LAN Control Protection by TCP/IP Protocol (in Trial or Full Mode)
- Encrypt & Hide Application Strings to provide a high level of security
- Prevent and Control your LicenseKey against illegal exportation - New !
- Using compact LicenseKeys to register with ActiveKey for increased security
- Add Extra Information inside License (in Trial or Full Mode)
- View LicenseKey to see details about any License
- Create custom URL links to directly access your ordering web page
- Invisible software based protection requiring no dongles
- Create evaluation copies of your software by days, number of uses, hours or a set date
- Compatible with Windows 95, 98, Me, NT, 2000, XP (with SP2)
- Support Windows XP SP2 (from ICE License v2.09)

Find out more at:

<http://www.ionworx.com/IceLicense.html>

## 2. Things needed to get started

### Required Tools

- » OllyDbg
- » PEiD 0.94
- » PE Explorer (or other resource editor)

### Target Application & Protection

- » Tomahawk Gold <http://nativewinds.montana.com/downloads/Tomahawk.zip>
- » TlceLicense for Delphi <http://www.ionworx.com>

## 3. Target Analysis

In this tutorial, our target is called Tomahawk Gold, packed with UPX and using the ICE License protection system. Soon after opening the program we notice that we are dealing with a trial version with some disabled functions. See below:

About-Box	
User Name:	<b>Trial License</b>
User Company:	<b>Evaluation</b>
Product Name:	<b>Tomahawk</b>
Vendor Info:	<b>NativeWinds / Jack D. Lewis</b>
Creation Date:	<b>2005/11/23 @ 1:24:47 AM</b>
License Expiration:	<b>30 days</b>
Software Status:	<b>Trial</b>
Hardware Locked:	<b>No</b>
Network Protection:	<b>No</b>
Network User Allowed:	<b>No</b>

Now we open the target with PEiD and see that it's compressed with "UPX 0.89.6 - 1.02 / 1.05 - 1.24 (Delphi) stub -> Markus & Laszlo". Notice that KANAL reports only "CRC32 [poly]". Easy enough, let's start unpacking. I will not go over unpacking UPX in detail. There are some very good tutorials about this topic. Shortly, fire up Olly and load our target. We are here:

### Unpacking UPX with Olly

```

00C75340 > 60          PUSHAD
00C75341 BE 00209A00      MOV ESI,Tomahawk.009A2000
00C75346 8DBE 00F0A5FF    LEA EDI,DWORD PTR DS:[ESI+FFA5F000]
00C7534C C787 10B75E00 5F8>MOV DWORD PTR DS:[EDI+5EB710],714A815F
00C75356 57              PUSH EDI
  
```

Press F8 to pass the PUSHAD (notice the ESP register is now highlighted). Select “Follow in Dump” and set a HW BP (Byte) on the first char. Hit F9 and the program breaks on a JMP. After that, push F7 to enter it and we land at the OEP. Let’s dump...

Reaching the Target’s OEP		
009B4F2C	55	PUSH EBP
009B4F2D	8BEC	MOV EBP,ESP
009B4F2F	83C4 F0	ADD ESP,-10
009B4F32	53	PUSH EBX
009B4F33	B8 FC3A9B00	MOV EAX,Tomahawk.009B3AFC

OK, so now we have unpacked the program. Load it in PEiD (again) and analyze it with KANAL. Wicked stuff we find...

PEiD’s KANAL Analysis	
1 x	BASE64 table
2 x	CRC32
1 x	FGInt ElGamalDecrypt
3 x	MD5

Seems damn hard, but in fact it’s easier than you imagined. Let’s open our target with PExplorer and go to “Resources Viewer/Editor”. Expand the “RC Data” section and start browsing thru the forms.

At some point we reach “TFORM3” and by double-clicking on it, we notice the components it holds... look closer – the last one is “TIceLicense”. This is a very big achievement for us, because now we are dealing with some easy stuff. If we take a closer look at the TIceLicense component we will see the following:

PExplorer’s Initial View	
OnAppKeyIncorrect	IceLicense1AppKeyIncorrect
OnTrialExpired	IceLicense1TrialExpired
OnLicenseInvalid	IceLicense1AppKeyIncorrect
OnLicenseFileError	IceLicense1AppKeyIncorrect
OnLicenseInfo	IceLicense1LicenseInfo
OnTrial	IceLicense1Trial
OnRegistered	IceLicense1Registered
OnTrialProgress	IceLicense1TrialProgress

Now it’s obvious... We just need to do some replacements (with PExplorer). Your events should now look like this:

PExplorer’s Modified View	
OnAppKeyIncorrect	IceLicense1Registered
OnTrialExpired	IceLicense1Registered
OnLicenseInvalid	IceLicense1Registered
OnLicenseFileError	IceLicense1Registered
OnLicenseInfo	IceLicense1Registered
OnTrial	IceLicense1Registered
OnRegistered	IceLicense1Registered
OnTrialProgress	IceLicense1Registered

After we save, let's test...

The program starts, and after a second or two it exits... hmm we did something that bothered him. Just open the file "Tomahawk.key" with Notepad (**do not delete it**), clear all text found inside and save it.

Why we do this?

Because we modified it earlier ("OnLicenseInvalid >> IceLicense1Registered" and "OnLicenseFileError >> IceLicense1Registered"). Now the program ignores the bad content of the Key file. **If you do not clear the Keyfile, the program will remain unregistered!**

Open the program and go to the about-box... yup, we did it!  
ICE License defeated!

## 4. Conclusions

Well, this is the end of this story, I hope all the things said here will be useful to understand future versions of ICE License. I suggest as usual to use this tutorial for learning purposes only, and not for cracking programs.

### Disclaimer

All the code provided with this tutorial is free for public use, just make a greetz to the authors and the ARTeam if you find it useful to use. Don't use these concepts for making illegal operation, all the info here reported are only meant for studying and to help having a better knowledge of application code security techniques.

## 5. Greetings

*I would like to thank Shub-Nigurrath for guiding me with my first tutorial as an ARTeam member*

[ ARTeam ] [ EXETools ] [ all the RO scene ] [ bLaCk-eye ] [ vybez\_mR ]