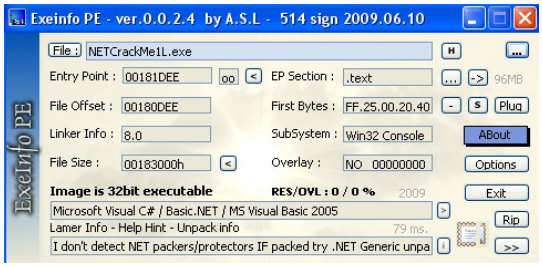
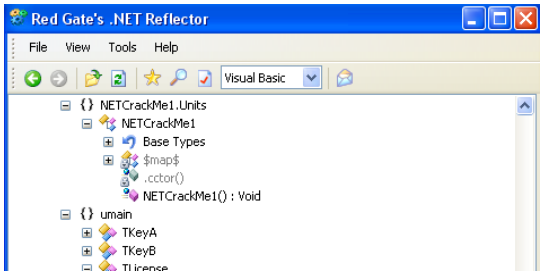
WinFan's NETCrackMe#1
.::KeyGen::.

Tools: Exeinfo PE, .NET generic unpacker and .NET Reflector





1. Take a look around

Run the crackme and look that the execution is not normal, a launcher encapsulate the program, ok go to the hell = internet for search something.
30 minutes searching all that you imagine and nothing…

2. Take a look around II

Suddenly, I realize that the solution is in the Exeinfo PE, I look that there is a reference to .NET Generic unpacker, ok download it and we have pass the first difficulty.

3. The NET's GOD.....Reflector

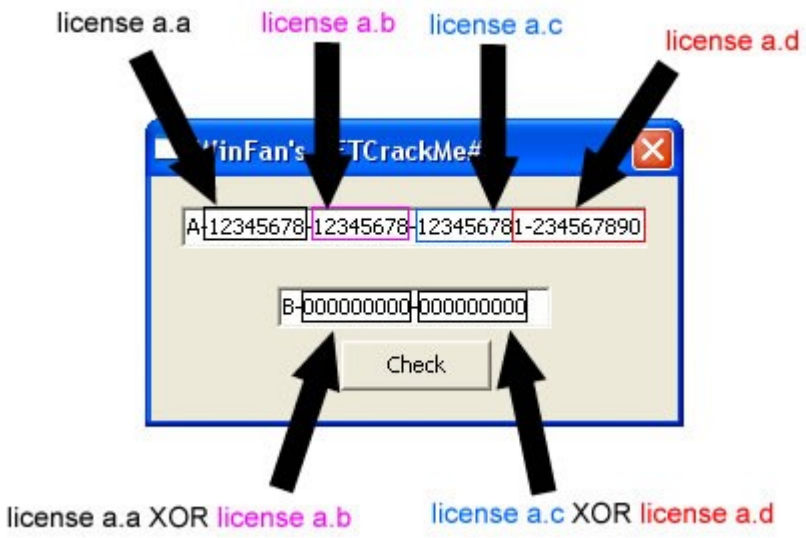
Now we can view the crackme in Reflector and we have this:

```
procedure TMainForm.btnCheckClick(Sender: TObject);
begin
    license := self.Parse;
    if (((license.a.a xor license.a.b) = license.b.a) and ((license.a.c xor license.a.d) = license.b.b))
then
        Windows.MessageBox(inherited Handle, 'Serial correct!', '', $40)
    else
        Windows.MessageBox(inherited Handle, 'Wrong serial!', '', $10)
end;
```

```
function TMainForm.Parse: TLicense;
var
    license: TLicense;
begin
    text := self.keyA.Text;
    System.@WStrDelete(@(text), 1, 2);
    text := SysUtils.StringReplace(text, ' ', '', TReplaceFlags.rfReplaceAll);
    license.a.a := SysUtils.StrToInt(System.@WStrCopy(text, 1, 8));
    System.@WStrDelete(@(text), 1, 9);
    license.a.b := SysUtils.StrToInt(System.@WStrCopy(text, 1, 8));
    System.@WStrDelete(@(text), 1, 9);
    license.a.c := SysUtils.StrToInt(System.@WStrCopy(text, 1, 8));
    System.@WStrDelete(@(text), 1, 10);
    license.a.d := SysUtils.StrToInt(text);
    dest := self.keyB.Text;
    System.@WStrDelete(@(dest), 1, 2);
    dest := SysUtils.StringReplace(dest, ' ', '', TReplaceFlags.rfReplaceAll);
    license.b.a := SysUtils.StrToInt(System.@WStrCopy(dest, 1, 9));
    System.@WStrDelete(@(dest), 1, 10);
    license.b.b := SysUtils.StrToInt(dest);
    Result := license
end;
```

By deurus

4. The algorithm



Be carefully with license a.c and license a.d for don't fall into the trap

OK!! With this to create a keygen is so easy.