Subject: Strange memory problem in QTF RichView
Posted by mdelfede on Tue, 02 Mar 2010 23:21:33 GMT
View Forum Message <> Reply to Message

```
#include <CtrlLib/CtrlLib.h>

using namespace Upp;

class TestQTF : public TopWindow
{
 private:
  RichTextView tv;

 public:
  typedef TestQTF CLASSNAME;
  TestQTF();
};

TestQTF::TestQTF()
{
 Add(tv.SizePos());
 tv.SetQTF((String)"[, pipopo xxx ]kkkk {{");
}

GUI_APP_MAIN
{
 TestQTF().Run();
}
```

It shows the error in following image :

I don't know if it's related to QTF, RichView or String conversion. Without the (String) conversion, the 'freefreefree' is not shown (correctly).
The example is taken from an more complex one using EditString content to fill RichView :

```
EditString es;
es.SetText("[, pipopo xxx ]kkkk {{");
tv.SetQTF((String)es);
```

The result is exactly the same.
I noted this because on a bigger app I get weird memory problems that happens once on 30-40 runs, on which sometimes the app hangs on qtf output or renders QTF in weird way with many

freefreefree inside.

Ciao

Max

p.s.: an even clearer testcase :

```
TestQTF::TestQTF()
{
 Add(tv.SizePos());
 String s = "[, pipopo xxx ]kkkk {{";
 tv.SetQTF(s);
}
```

I tested it even with string as static (global), but the result is the same. I think the bug is related to SetQTF() or qtf processing, not String.

File Attachments

1) TestQTF.jpg, downloaded 563 times

Subject: Re: Strange memory problem in QTF RichView
Posted by mirek on Wed, 03 Mar 2010 06:40:17 GMT
View Forum Message <> Reply to Message

Thanks, fixed.

Your QTF is ill formed - ends with '{{', which is start of table and should be followed at least by space, but the problem was that parsing code fetched terminating zero, correctly decided there should not be any terminating zero at that point, but then while reporting the error attemted to read text past this terminating zero (which lead to "Free" usually and to crash sometimes).

So it was basically bug in bug reporting.

Mirek

Subject: Re: Strange memory problem in QTF RichView
Posted by mdelfede on Wed, 03 Mar 2010 10:25:04 GMT
View Forum Message <> Reply to Message

luzr wrote on Wed, 03 March 2010 07:40Thanks, fixed.

Your QTF is ill formed - ends with '{{', which is start of table and should be followed at least by space, but the problem was that parsing code fetched terminating zero, correctly decided there should not be any terminating zero at that point, but then while reporting the error attemted to read text past this terminating zero (which lead to "Free" usually and to crash sometimes).

So it was basically bug in bug reporting.

Mirek

Yep, I know that the QTF was malformed, but it was on purpose to demonstrate the bug. I don't know it the bug could happen also on corrected code.
BTW, in my app I have random of such problems, as I said before, but I can't reproduce them, because they happens seldom with the same test file.... they may be caused by other hidden bug.
Anyways, this bug could arise when constructing the qtf output directly with SetQTF, adding small pieces of qtf in steps, like my app does.

Ciao

Max
