QGIS Application - Bug report #777

crashes with python reference to destroyed objects (e.g exportToWkt() crashes when geom has been deleted)

2007-10-07 08:37 PM - crschmidt -

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>High</td>
</tr>
<tr>
<td>Assignee:</td>
<td></td>
</tr>
<tr>
<td>Category:</td>
<td>Python plugins</td>
</tr>
<tr>
<td>Affected QGIS version:</td>
<td>master</td>
</tr>
<tr>
<td>Operating System:</td>
<td>All</td>
</tr>
<tr>
<td>Pull Request or Patch supplied:</td>
<td></td>
</tr>
<tr>
<td>Crashes QGIS or corrupts data:</td>
<td></td>
</tr>
<tr>
<td>Regression?:</td>
<td>No</td>
</tr>
<tr>
<td>Easy fix?:</td>
<td>No</td>
</tr>
<tr>
<td>Resolution:</td>
<td></td>
</tr>
<tr>
<td>Copied to github as #:</td>
<td>10836</td>
</tr>
</tbody>
</table>

Description

When a feature is destroyed, if it has ownership over a geometry, it deletes that geometry. After that point, if one tries to call functions on the geometry, it will return nulls (Linux) or cause a KERN_PROTECTION_FAILURE (OS X).

This can be reproduced by selecting a feature, then typing the following into the Python console:

```python
iface.activeLayer().selectedFeatures()[0].geometry().exportToWkt()
```

(Sometimes it requires calling it twice to reproduce the crash -- however, it will never return the correct answer.)

The reason for this appears to be that the feature created when it is pulled out of the list is then destroyed before exportToWkt() is called, taking the geometry with it.

A workaround is to instead call geometryAndOwnership(), which tells the feature to not destroy the geometry.

It seems like this problem may actually be exportGeosToWkb -- functions like wkbType() fail in the same way. It's possible that the mGeometry check at the beginning of these functions needs to move before teh exportGeosToWkb(), or that the exportGeosToWkb() needs to more resilient against being deleted.

Related issues:

- Related to QGIS Application - Bug report # 10755: Python Console crashes when...
  - Closed 2014-06-30
- Duplicated by QGIS Application - Bug report # 7228: Incorrect return on bound...
  - Closed 2013-02-24
- Duplicated by QGIS Application - Bug report # 9185: Crash when perform some c...
  - Closed 2013-12-09
- Duplicated by QGIS Application - Bug report # 13084: Segfault when accessing ...
  - Closed 2015-07-06
- Duplicated by QGIS Application - Bug report # 14320: Qgis crashes when trying...
  - Closed 2016-02-17

Associated revisions

Revision bd7d9133 - 2016-08-01 08:25 AM - Nyall Dawson

Refine QgsFeature geometry getters/setters

All pointer based methods have been removed.

Now we have only:

```cpp
void setGeometry( const QgsGeometry& geom )
```

and

```cpp
QgsGeometry geometry() const
```
Benefits include avoiding a whole lot of tricky pointer lifetime issues, potential memory leaks, and finally closing #777, which has survived for over 9 years!

Impacts on PyQGIS code:
- no more need for the messy
  
g = QgsGeometry( feature.geometry() )
  workaround, just use g = feature.geometry() instead
- IMPORTANT: you can no longer test whether a feature has geometry using 'if f.geometry()'; since QgsFeature::geometry() will
  always return an object. Instead, use
  'if not f.geometry().isEmpty()'; or preferably the new method
  'if not f.hasGeometry()':

Fix #777

---

**History**

**#1 - 2007-10-11 06:03 PM - Martin Dobias**

The problem here is in python bindings because the scenario seems to be like this:

1. get feature
2. store geometry's reference in Python
3. feature is deleted (together with geometry)
4. reference in Python still exists, but the object it's pointing to doesn't

I'm trying to find out how to cope with this correctly...

Martin

---

**#2 - 2008-08-29 02:27 AM - Jürgen Fischer**

see also #1248

---

**#3 - 2009-07-30 05:40 AM - Giovanni Manghi**

Hi,

what is the status of this issue?

cheers

---

**#4 - 2009-12-01 11:52 PM - Jürgen Fischer**

see also #2173

---

**#5 - 2010-06-12 12:24 AM - Paolo Cavallini**

Still true?
This haven't been fixed yet

No crashes in my Ubuntu 9.04, but I never get the correct results.

I tried wkbType() on the same selected geometry a lot of times and I get different (and also strange) results:
0, 16777216, 7, 187101, 92, 143587, ...

- **Target version changed from Version 1.7.4 to Version 1.7.0**
- Pull Request or Patch supplied set to No
- Crashes QGIS or corrupts data set to Yes
- Affected QGIS version set to master

- **Target version changed from Version 1.7.0 to Version 1.7.4**

- **Target version changed from Version 1.7.4 to Version 1.8.0**

- **Target version changed from Version 1.8.0 to Version 2.0.0**

- Priority changed from Low to High

Fix in pull request !#436

Not sure if it's the best way to do it.

Maybe a reference counter or the like could also help to overcome this problem. But I'm not sure how easy it is to do mixed ref-counting between python and C++?

- **Target version changed from Version 2.0.0 to Future Release - High Priority**

- Assignee deleted (Martin Dobias)

- Status changed from Open to Closed

Fixed in changeset commit:"bd7d913379b68a8104608b1afab4d380e4edc26b".