Among ELFs and DWARFs

Volker Krause
volker.krause@kdab.com
@VolkerKrause

Qt WORLD SUMMIT 2015

Why look at the binary?

KDAB

- Linker errors
- Locating and loading DLLs/plugins
- Startup performance
- Memory usage
- Nasty runtime bugs
- ...

What is in the binary?

KDAB

- 3 or more mmap'ed segments (ro, rw, ro+executable)
- symbol table
- GOT/PLT
- debug information

Linker Errors

Symbols

KDAB

- Is the symbol present?
- Is the symbol exported?
- Tools:
  - `nm, readelf -s, objdump -t` (part of binutils)
  - `depends.exe` (Dependency Walker)

Loader Errors

Finding Libraries

KDAB

- LD_LIBRARY_PATH
- RPATH/RUNPATH
- Tools:
  - `ldd / otool -L / depends.exe`
  - `readelf -d, otool -l`
  - LD_DEBUG=libs
  - `strace -e file`

KDAB

Qt Plugins

Qt Plugin Metadata

KDAB

- Metadata in separate ELF section: .qtmetadata
- Tools:
  - `qtplugininfo` (Qt >= 5.5)
  - `readelf --sections`
  - check if qt_plugin_instance symbol is present and exported
  - check if plugin dependencies are found

Static Connects

Connecting to member functions

KDAB

```
class IBreakThings : public QBuffer {
    IBreakThings() { readyRead(); }
};

int main(int, char**) {
  QBuffer b(...);
  QObject::connect(&b, &QIODevice::readyRead, ...);
  ...
  IBreakThings badGuy;
}
```

Connecting to member functions

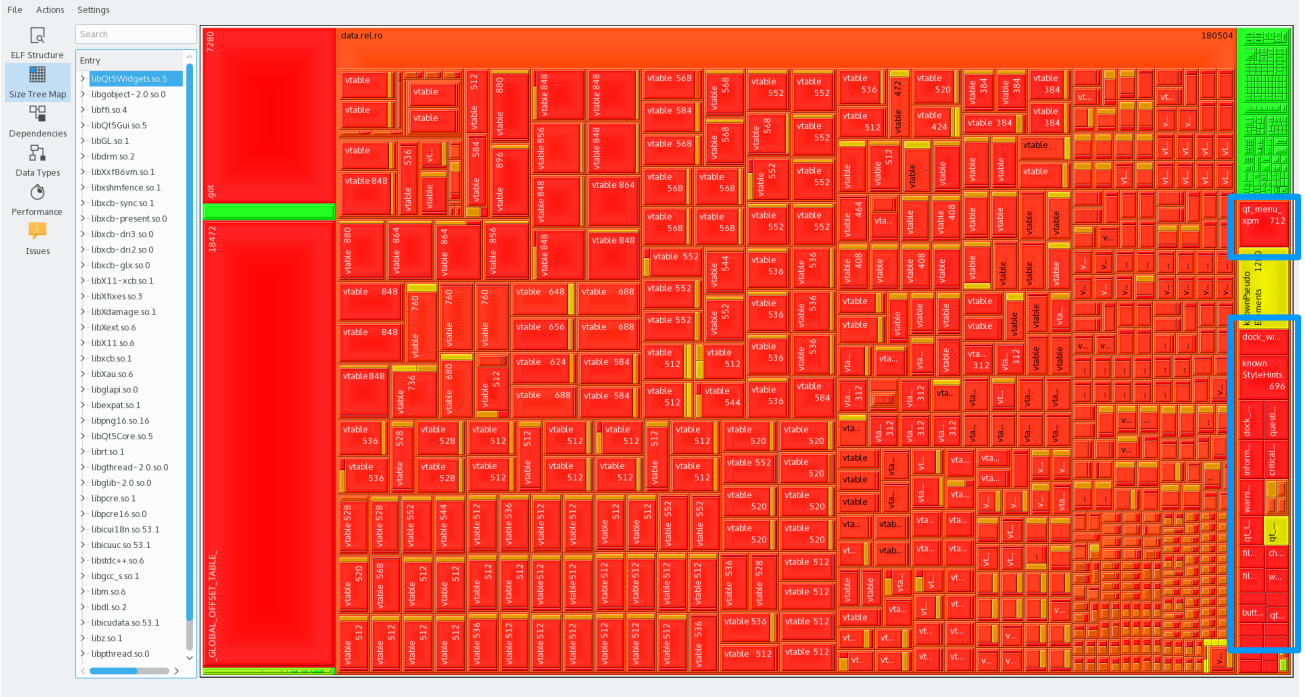
KDAB

- Uses function pointer comparison, possibly across DLL boundaries
- Avoid comparing two different DLL-local PLT entries!
- Tools:
  - `-fPIC`/`-fPIE`, `-Bsymbolic`
  - `readelf --relocs`
  - recent Qt 5

KDAB

Memory Consumption

Unshared data segments



- Tools:
  - `elf-dissector` (KDE)

Structure packing

KDAB

```
class MyClass : public QSharedData {
    QString s;
    int n;
};
```

- Tools:
  - `elf-dissector` / `elf-packcheck`
  - `dwarves` / `pahole`
  - `-Wpadded`

Debugging

GDB index

KDAB

- 5-8x speed-up for attaching GDB
- Tools:
  - `(gdb) save gdb-index <lib>`

```
objcopy \
  --add-section .gdb_index=<lib>.gdb-index \
  --set-section-flags .gdb_index=readonly \
  <lib> <lib>
```

  - `gold --gdb-index`

Questions?

KDAB

Thank you!

www.kdab.com

volker.krause@kdab.com

References

KDAB

- Dependency Walker: http://www.dependencywalker.com/
- ELF Dissector: git.kde.org:elf-dissector

- John R. Levine: “Linkers and Loaders”, Morgan-Kauffman, ISBN 1-55860-496-0. 2000 http://www.iecc.com/linker/
- Ulrich Drepper: “How To Write Shared Libraries”. 2011 http://www.akkadia.org/drepper/dsohowto.pdf

- Slides & code: http://www.kdab.com/~volker/devdays/2015