Mobile Analytics
mit Elasticsearch und Kibana

Dominik Helleberg
Dominik Helleberg

Mobile Development
Android / Embedded
Tools

http://dominik-helleberg.de/+
Warum?
Warum?

Server
- Software
  - Runtime
  - OS
  - Hardware

Server
- Software
  - Runtime
  - OS
  - Hardware

![Diagram](image.png)
Warum?

- Backend
- Client
  - Software
  - Runtime
  - OS
  - Hardware
- Backend
  - Client
  - Software
  - Runtime
  - OS
  - Hardware
  - Hardware
Was?

Crash Reporting

Logging

Analytics
Crash Reporting

E/AndroidRuntime (1188): Caused by: java.lang.RuntimeException: CRASH
E/AndroidRuntime (1188): at org.cirrus.mobi.pegel.c.b (Unknown Source)
E/AndroidRuntime (1188): at org.cirrus.mobi.pegel.SelectRiver.onStart (Unknown Source)
E/AndroidRuntime (1188): at android.app.Instrumentation.callActivityOnStart (Instrumentation.java:1163)
E/AndroidRuntime (1188): at android.app.Activity.performStart (Activity.java:5018)
E/AndroidRuntime (1188): at android.app.ActivityThread.performLaunchActivity (ActivityThread.java:2032)
E/AndroidRuntime (1188): ... 11 more
• Pro-aktive Benachrichtigung bei Crashes
• Nachvollziehbare Stacktraces
• Device / App und Umgebungs-Infos
• Optional: Nachricht vom Benutzer
• Statistische Analysen
Crash Reporting

Nachvollziehbare Stacktraces

E/AndroidRuntime(1188): Caused by: java.lang.RuntimeException: CRASH
E/AndroidRuntime(1188): at org.cirrus.mobi.pegel.c.b(Unknown Source)
E/AndroidRuntime(1188): at org.cirrus.mobi.pegel.SelectRiver.onStart(Unknown Source)
E/AndroidRuntime(1188): at android.app.Instrumentation.callActivityOnStart(Instrumentation.java:1163)
E/AndroidRuntime(1188): at android.app.Activity.performStart(Activity.java:5018)
E/AndroidRuntime(1188): at android.app.ActivityThread.performLaunchActivity(ActivityThread.java:2032)
E/AndroidRuntime(1188): ...

Exception Type: SIGSEGV
Exception Codes: SEGV_ACCERR at 0x13babeb8
Crashed Thread: 8

Thread 8 Crashed:
0 libobjc.A.dylib 0x00000000196f5bbd0 0x196f40000 113616
1 CoreFoundation 0x0000000185369458 0x185364000 21592
2 QuartzCore 0x000000018983cad8 0x189830000 51928
3 QuartzCore 0x0000000189842aec 0x189830000 76524
4 libobjc.A.dylib 0x00000000196f61724 0x196f40000 136996
5 CoreFoundation 0x000000018536d074 0x185364000 36980
6 Foundation 0x00000001862acfffc 0x186298000 86012
7 CFNetwork 0x00000000184ec9aac 0x184dac000 1170092....
Crash Reporting

- Crash reporter
- DISTRIBUTION PLATFORM
- Mobile
  - App
  - Crash reporter
- dSYM mapping
- Crash reporter
- Analytics reporter
- Logging reporter

Graphical representation of the processes involved in crash reporting.
Crash Reporting

• App-Stores

• 3rd Party

• Custom inhouse
### Adventure ... 1.0.0 Crash Reports (Feb 23, 2013)

#### iOS 5.0

<table>
<thead>
<tr>
<th>Most Frequent Crashes</th>
<th>% of Submitted Crashes</th>
<th>Download Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medal_iPhone_NA: PopupHandle_DisplayQuestsPageList + 630</td>
<td>55%</td>
<td>[Download Report]</td>
</tr>
<tr>
<td>Medal_iPhone_NA: 0x65a92</td>
<td>22%</td>
<td>[Download Report]</td>
</tr>
<tr>
<td>Medal_iPhone_NA: LoadCb + 178</td>
<td>7%</td>
<td>[Download Report]</td>
</tr>
<tr>
<td>Medal_iPhone_OriginResult + 69</td>
<td>2%</td>
<td>[Download Report]</td>
</tr>
<tr>
<td>Medal_iPhone_IsActionInActiveQuest + 66</td>
<td>2%</td>
<td>[Download Report]</td>
</tr>
<tr>
<td>CoreFoundation: -[KeyDictionary objectTicker:]</td>
<td>2%</td>
<td>[Download Report]</td>
</tr>
</tbody>
</table>
## CRASHES & ANRS

<table>
<thead>
<tr>
<th>Type</th>
<th>Show hidden</th>
<th>Last reported</th>
<th>Android version</th>
<th>Application version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crashes</td>
<td>YES</td>
<td>Last 7 days</td>
<td>All versions</td>
<td>Current production</td>
</tr>
<tr>
<td>ANRs</td>
<td>NO</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Device

Add filter

---

0 new crashes | 4 total crashes

<table>
<thead>
<tr>
<th>NAME</th>
<th>NEW</th>
<th>REPORTS THIS WEEK</th>
<th>REPORTS TOTAL</th>
<th>LAST REPORTED</th>
<th>HIDE</th>
</tr>
</thead>
<tbody>
<tr>
<td>java.lang.IllegalArgumentException</td>
<td></td>
<td></td>
<td>213</td>
<td>Today, 3:19 PM</td>
<td>Hide</td>
</tr>
</tbody>
</table>
in org.apache.http.HttpHost.<init>              |     |                   |               |        |      |
| java.lang.NullPointerException               |     |                   | 6             | Apr 29, 1:50 AM     | Hide |
in com.inovex.zabbixmobile.model.Trigger.getSharableSt… |     |                   |               |        |      |
| java.lang.NullPointerException               |     |                   | 22            | Apr 28, 8:34 AM     | Hide |
in com.inovex.zabbixmobile.data.HomescreenWidgetServ… |     |                   |               |        |      |
| java.lang.IllegalStateException            |     |                   | 3             | Apr 24, 11:22 PM    | Hide |
in org.apache.http.impl.client.DefaultRequestDirect… |     |                   |               |        |      |
Unfortunately, [app] has stopped.

Report  OK
• No unified interface
• Internal betas
• Internal apps
• Limited to App-Store functionality
• Internal apps (if there’s internet access)
• Pricing
• Privacy
Crash Reporting

inhouse

Crash Analytics

Analytics + Alarming

Storage

Receiver

dSYM mapping

Crash reporter
### Recent Reports

<table>
<thead>
<tr>
<th>REPORT</th>
<th>PACKAGE NAME</th>
<th>USER CRASH DATE</th>
<th>CREATED AT</th>
</tr>
</thead>
<tbody>
<tr>
<td>B395A17B-977C-4B21-8462-74C08F1CE241</td>
<td></td>
<td>April 24, 2015 14:28</td>
<td>April 26, 2015 10:10</td>
</tr>
<tr>
<td>2F1CACBE-7ED7-4237-B008-EF7220C83BF</td>
<td></td>
<td>April 22, 2015 05:36</td>
<td>April 25, 2015 17:01</td>
</tr>
<tr>
<td>6800E4BE-7E7F-45F4-8CFD-379871357A74</td>
<td></td>
<td>April 22, 2015 13:03</td>
<td>April 22, 2015 15:03</td>
</tr>
</tbody>
</table>

### Recently Updated Apps

<table>
<thead>
<tr>
<th>PACKAGE NAME</th>
<th>VERSION</th>
<th>UPDATED AT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5</td>
<td>June 11, 2013 11:36</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>February 17, 2012 10:58</td>
</tr>
</tbody>
</table>

### Statistics

- # REPORTS TODAY: 0
- # REPORTS LAST 7 DAYS: 1
- # REPORTS TOTAL: 406

**Help**

Configure your client to send crash reports to (using POST):

http://.../reports

Send queries for new application versions to:

http://.../app_version/check?package_name=your_android_package&code_version=your_app_version
Crash Reporting

inhouse

## Reports

<table>
<thead>
<tr>
<th>Report</th>
<th>Product</th>
<th>Phone Model</th>
<th>Android Version</th>
<th>App Version Name</th>
<th>App Version Code</th>
<th>Package Name</th>
<th>User Crash Date</th>
<th>Created At</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>iPad2.7</td>
<td>8.3</td>
<td>1.6</td>
<td></td>
<td></td>
<td>April 27, 2015 22:57</td>
<td></td>
<td>View Delete</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iPad2.7</td>
<td>8.3</td>
<td>1.6</td>
<td></td>
<td></td>
<td>April 26, 2015 10:10</td>
<td></td>
<td>View Delete</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iPad3.4</td>
<td>8.3</td>
<td>1.6</td>
<td></td>
<td></td>
<td>April 25, 2015 17:01</td>
<td></td>
<td>View Delete</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iPad2.7</td>
<td>8.3</td>
<td>1.6</td>
<td></td>
<td></td>
<td>April 24, 2015 13:18</td>
<td></td>
<td>View Delete</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iPad4.2</td>
<td>8.3</td>
<td>1.5</td>
<td></td>
<td></td>
<td>April 22, 2015 13:03</td>
<td></td>
<td>View Delete</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iPad4.2</td>
<td>7.1.1</td>
<td>1.5</td>
<td></td>
<td></td>
<td>April 21, 2015 21:07</td>
<td></td>
<td>View Delete</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iPad4.1</td>
<td>8.1.1</td>
<td>1.5</td>
<td></td>
<td></td>
<td>April 21, 2015 15:59</td>
<td></td>
<td>View Delete</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iPad5.3</td>
<td>8.2</td>
<td>1.5</td>
<td></td>
<td></td>
<td>April 21, 2015 15:56</td>
<td></td>
<td>View Delete</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iPad5.3</td>
<td>8.2</td>
<td>1.5</td>
<td></td>
<td></td>
<td>April 21, 2015 15:56</td>
<td></td>
<td>View Delete</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iPad5.3</td>
<td>8.3</td>
<td>1.5</td>
<td></td>
<td></td>
<td>April 21, 2015 15:56</td>
<td></td>
<td>View Delete</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iPad5.3</td>
<td>8.2</td>
<td>1.5</td>
<td></td>
<td></td>
<td>April 21, 2015 15:56</td>
<td></td>
<td>View Delete</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iPad5.3</td>
<td>8.2</td>
<td>1.5</td>
<td></td>
<td></td>
<td>April 21, 2015 15:56</td>
<td></td>
<td>View Delete</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iPad5.3</td>
<td>8.2</td>
<td>1.5</td>
<td></td>
<td></td>
<td>April 21, 2015 15:56</td>
<td></td>
<td>View Delete</td>
</tr>
</tbody>
</table>
• Limited Analytics (Trends, queries, search etc.)
• User Interface
• Fixed data-structures
• Custom stack
ELK?

https://pixabay.com/p-145930/
Crash Reporting – with ELK

Elasticsearch  
Logstash  
Kibana
Crash Reporting – with ELK
inhouse 2.0

Logstash
“Logstash is a data pipeline that helps you process logs and other event data from a variety of systems. With 165 plugins and counting, Logstash can connect to a variety of sources and stream data at scale to a central analytics system.”

https://www.elastic.co/products/logstash
Crash Reporting – with ELK

Logstash

- Input Plugins
- Filter Plugins
- Output Plugins
Crash Reporting – with ELK

inhouse 2.0

Logstash

- Input Plugins (~40)
  - elasticsearch
  - eventlog
  - file
  - http
  - jdbc
  - kafka

- Filter Plugins
  - jmx
  - log4j
  - tcp
  - twitter
  - syslog
  - rabbitMQ

- Output Plugins
  - redis
  - udp
  - zeromq
Crash Reporting – with ELK

Logstash

Input Plugins

aggregate
anonymize
collate
csv
checksum
drop
dns
geoip
grok
extractnumbers
mutate
metrics

Filter Plugins (~40)
ruby
uuid
throttle
urldatecode
translate

Output Plugins
Crash Reporting – with ELK

Logstash

Input Plugins
- elasticsearch
- csv
- cloudwatch
- datadog
- email
- file
- g_c_s
- hipchat
- http
- irc
- jira
- kafka

Filter Plugins
- mongodb
- nagios
- pipe
- s3
- redmine
- redis

Output Plugins (~50)
- sqs
- tcp
- rabbitmq
- syslog
- stdout
- zabbix
Crash Reporting – with ELK

Logstash

- Input: HTTP (json)
- Filter: de-obfuscate (custom)
- Output: elastic search

dSYM mapping
Crash Reporting – with ELK

**Elasticsearch**

- Document / Data Store (JSON)
- RESTful API
- Uses Lucene for indexing
- Optimized for search queries
- Easy to distribute and scale
- Auto-Schema
- Easy to start with
Crash Reporting – with ELK

Terms:

- Index
- Type
- Document
- Field
- Mapping
Index:

logstash-%{platform}%{PACKAGE_NAME}%{+YYYY.MM.dd}

Type

“crash-report”

Document

{  "APP_VERSION_NAME": "1.3.2",
  "AVAILABLE_MEM_SIZE": 10004287488,
  "USER_APP_START_DATE": "2015-08-27T13:37:59.000+02:00",
  "CUSTOM_DATA": {},
  "BRAND": "samsung"
}
Kibana is an open source analytics and visualization platform designed to work with Elasticsearch. You use Kibana to search, view, and interact with data stored in Elasticsearch indices. You can easily perform advanced data analysis and visualize your data in a variety of charts, tables, and maps. Kibana makes it easy to understand large volumes of data. Its simple, browser-based interface enables you to quickly create and share dynamic dashboards that display changes to Elasticsearch queries in real time.

Crash Reporting – with ELK

inhouse 2.0
Crash Reporting – with ELK

Crash Analytics

Kibana

elastic search

Logstash

dSYM mapping

Crash Reporter
ACRA (Android)
QuincyKit (iOS)

Logstash elastic search dSYM mapping

Crash Reporting

inhouse 2.0
Crash Reporting – with ELK

inhouse 2.0
Crash Reporting – with ELK

Crash Analytics

- Kibana
- elastic search
- Logstash

- Kibana Plugins (soon!)
- dSYM mapping
- Watcher

Crash Reporter
ACRA (Android)
QuincyKit (iOS)
Logging with ELK

Remote Logging

Kibana  elastic search  Logstash

Logging Library
A bit more complicated then crash reporting and logging…
Analytics

Amazon Mobile Analytics

Google Analytics
Anywhere. Anytime.

mixpanel

FLURRY
from YAHOO!
Analytics with ELK

Kibana

elastic search

Logstash

Analytics Library

(userID, Session Tracking, PageViews)

Kibana-Plugins (not yet!)

Carrier GeoIP

Device Infos

UserProfiles
ELK -> Getting started

Hosting:
  elastic.co
  google-compute
  qbox

Define index strategy

Check your Schema
  Changes are hard
  .raw vs. analyzed fields
Summary

ELK Stack seems like a good fit for mobile analytics.

Kibana PlugIns will help with missing Features.

Logstash PlugIns and Client Side Library needed in order to improve Analytics capabilities.

It needs a bit of time and work but it looks promising.
Danke!