

#ToyFail

A security review of IoT toys

Agenda



Our Customer



(The Norwegian Consumer Consul)

Why?



Regulations





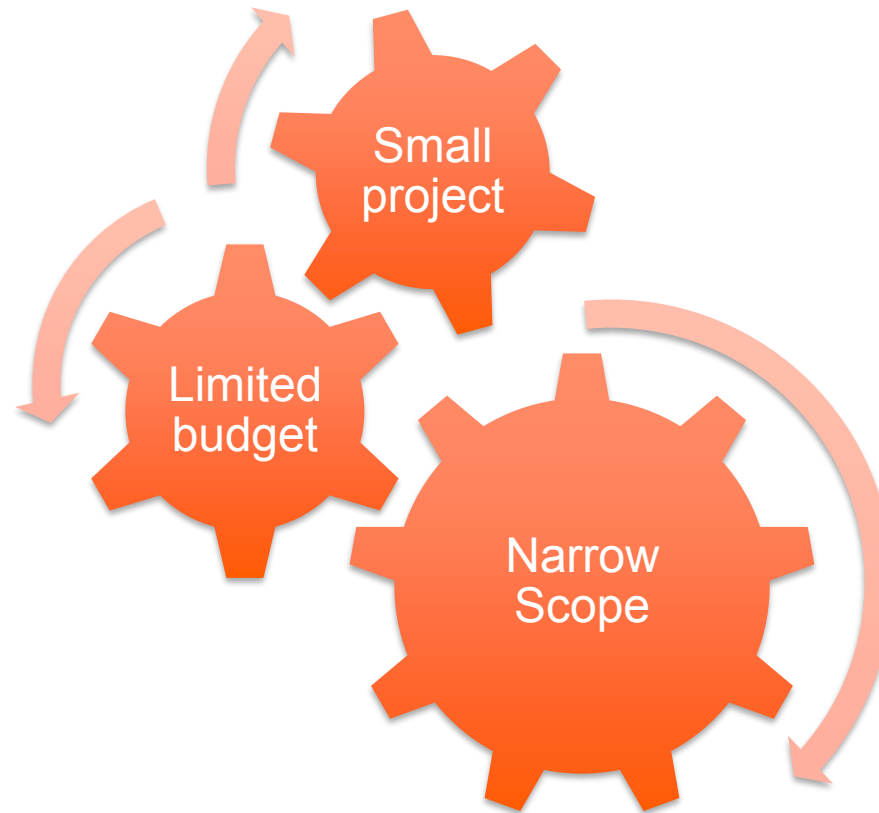
Security updates



Security updates



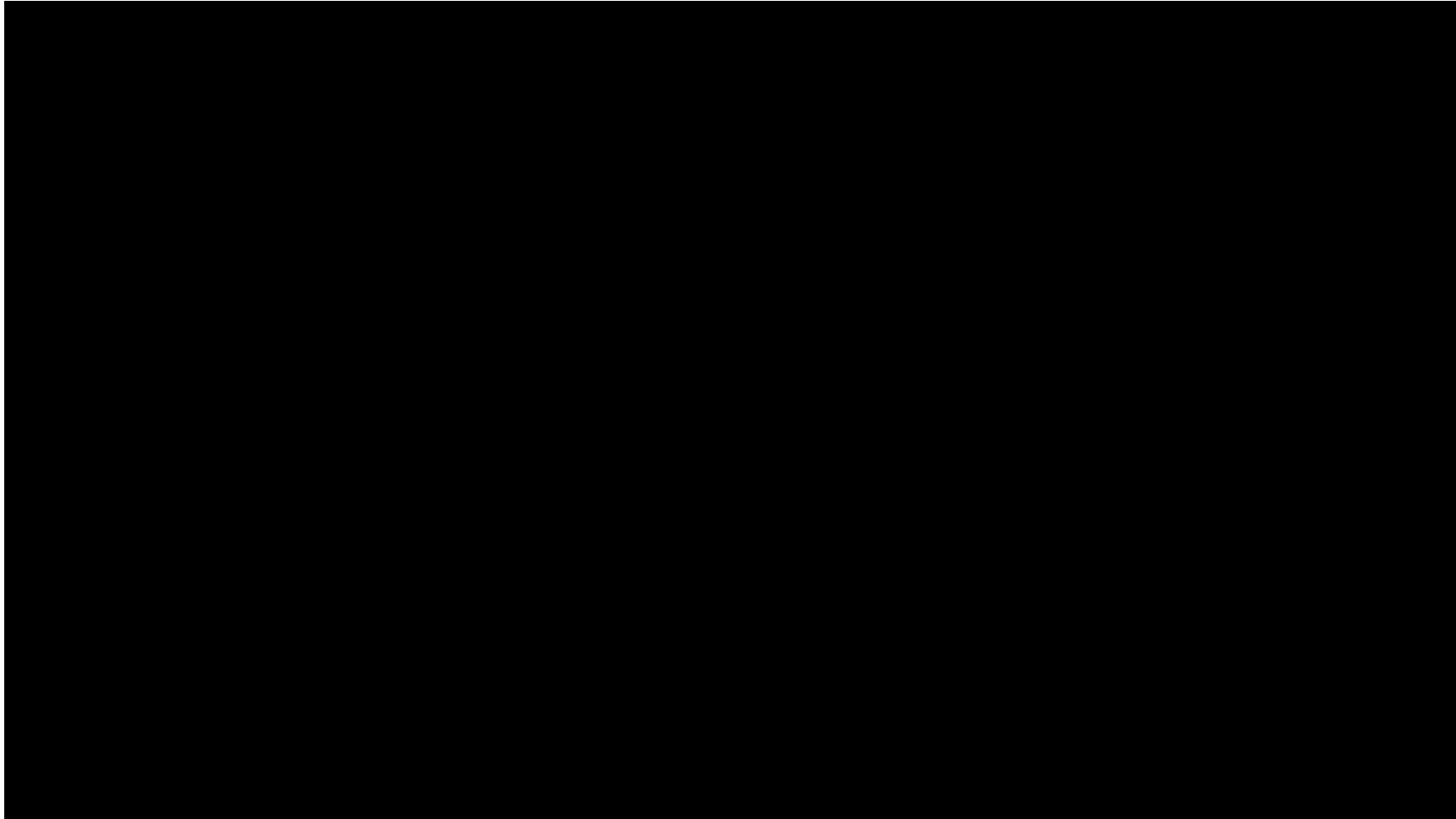
The project



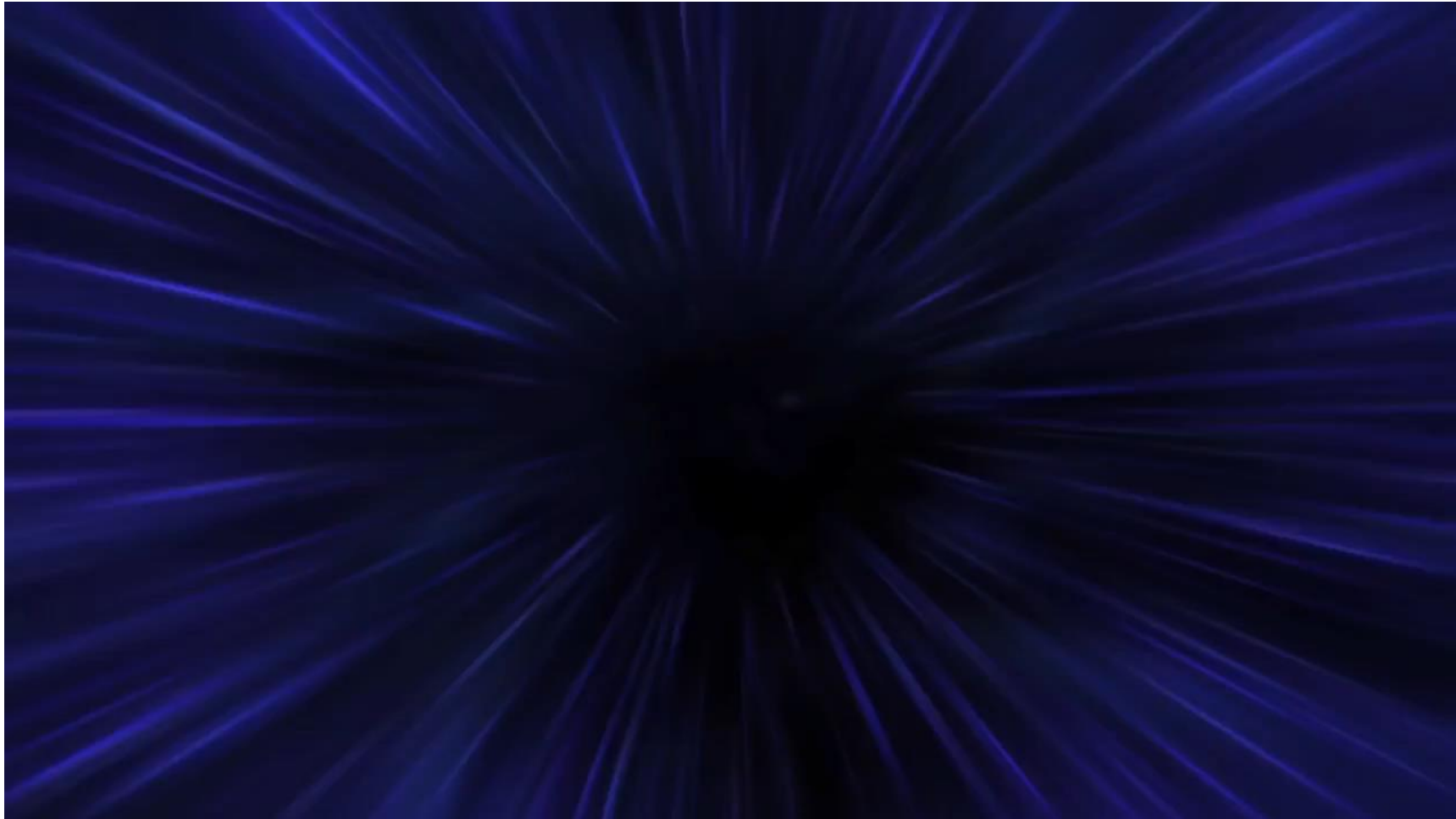
Meet the dolls



Cayla



i-que





Smart toys



Google WIKIPEDIA

 WEATHER
UNDERGROUND



 **Bluetooth®**

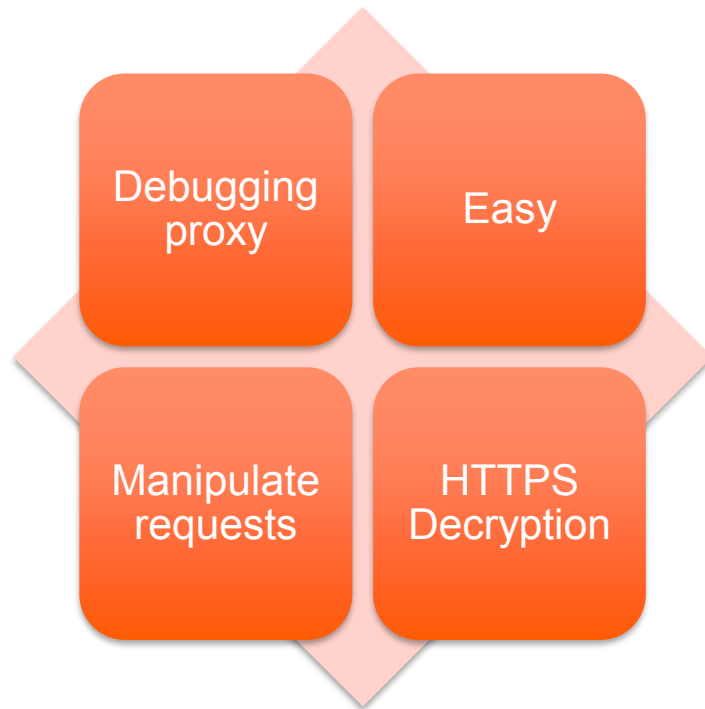


**Wi-Fi
4G**

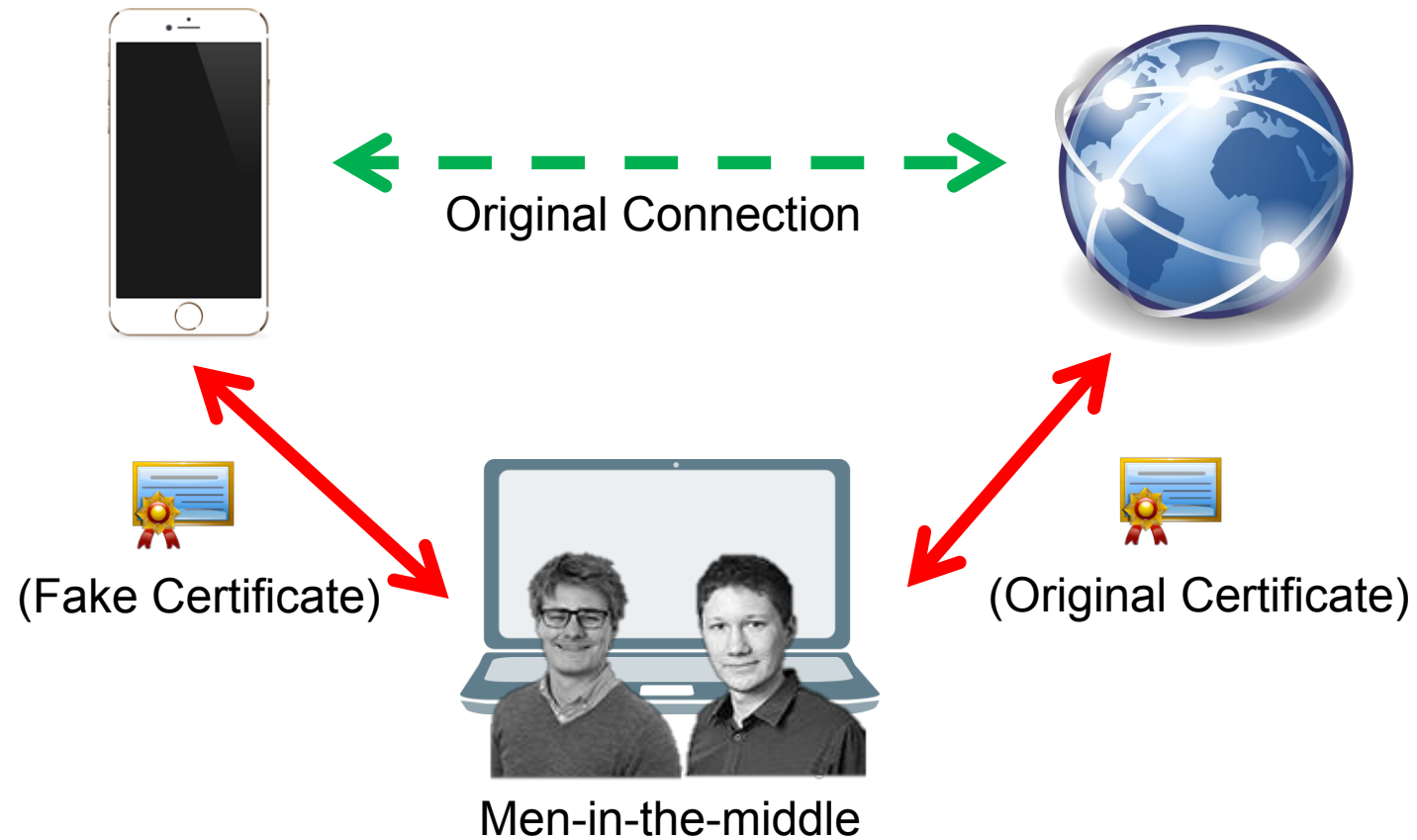


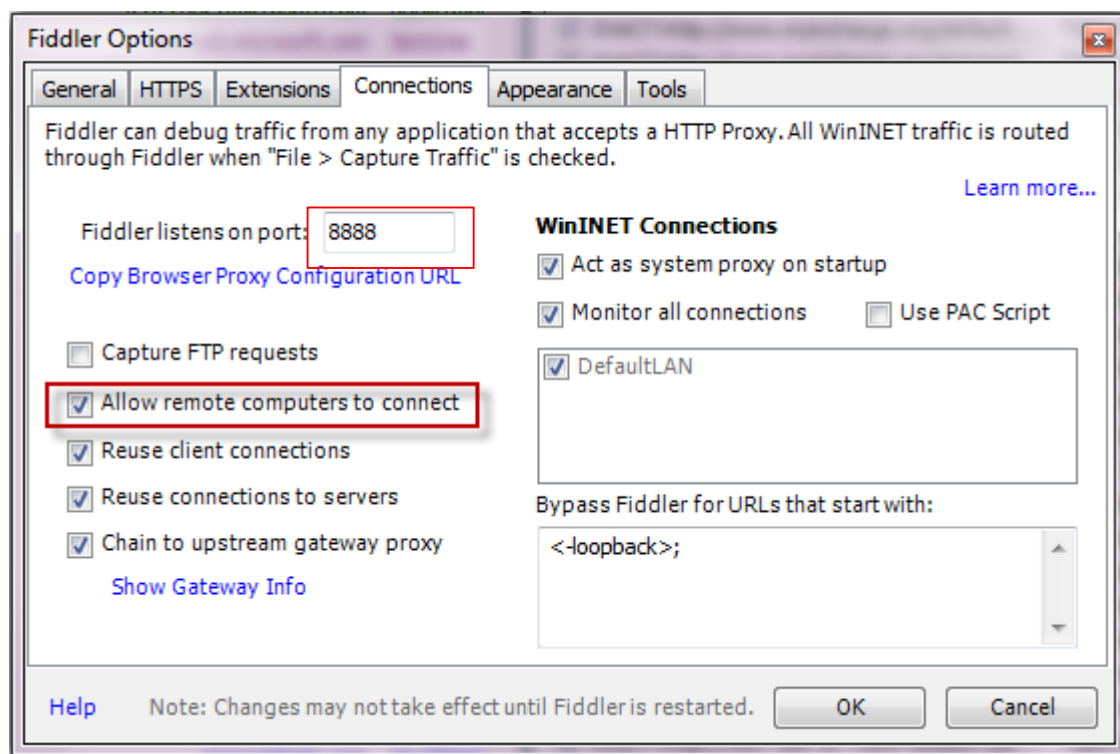
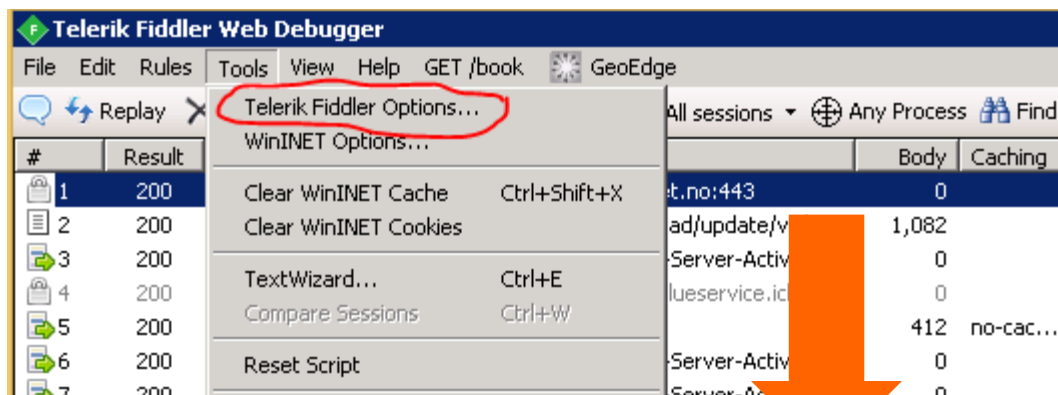
App <-> Internet



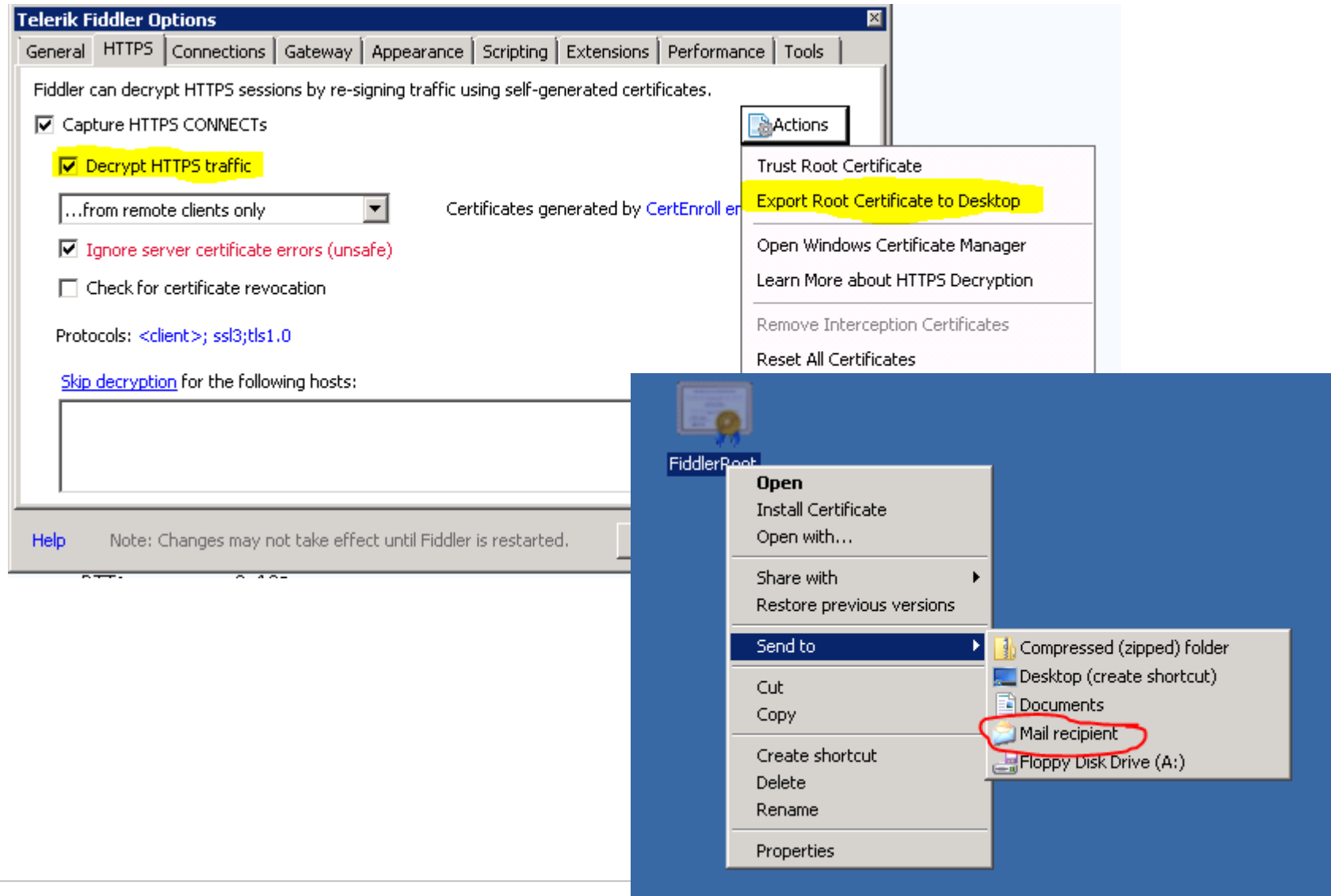


SSL Decryption

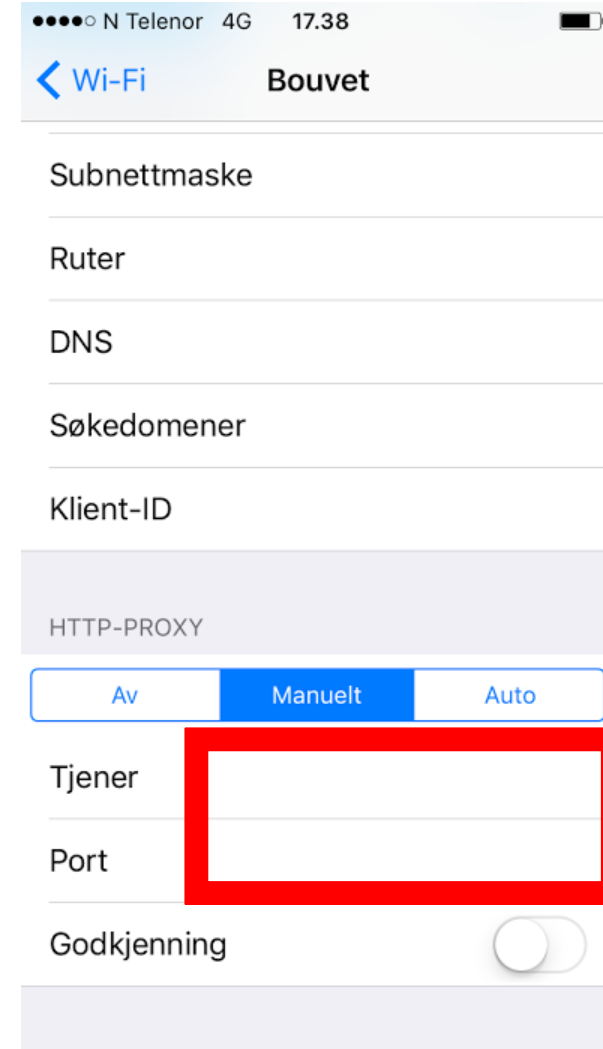
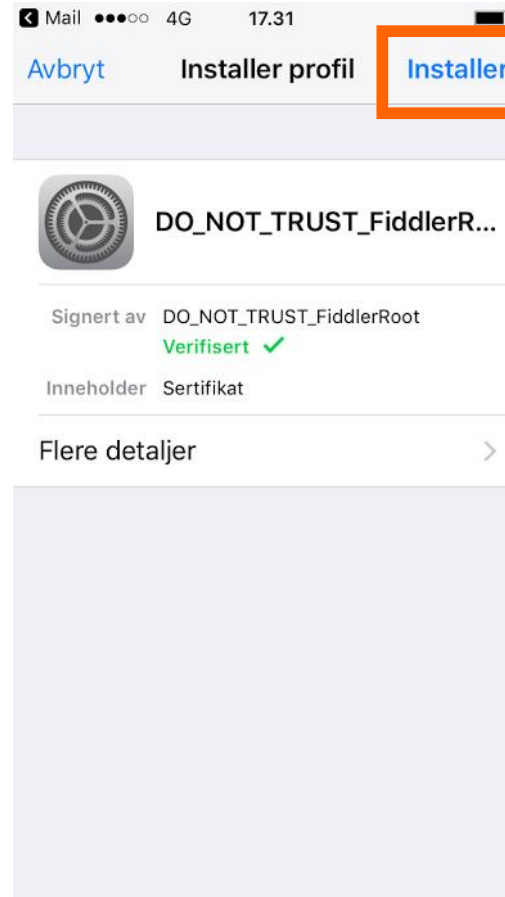
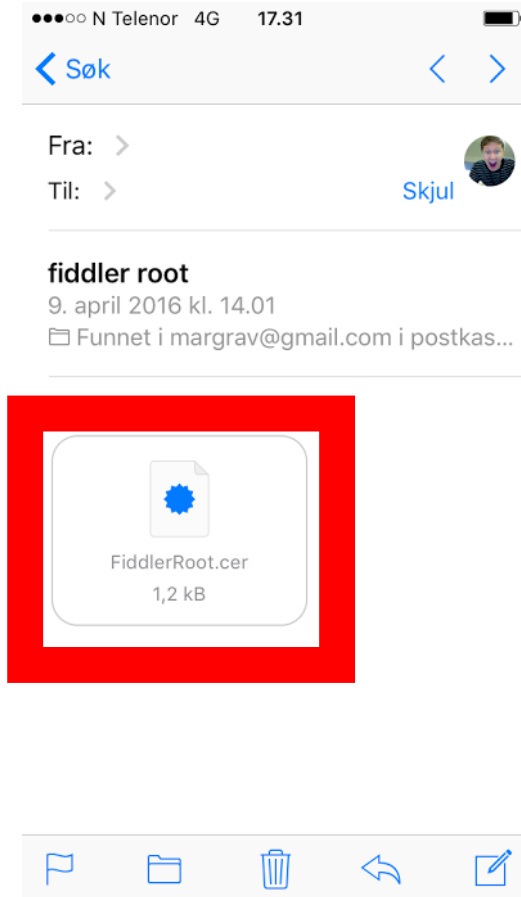




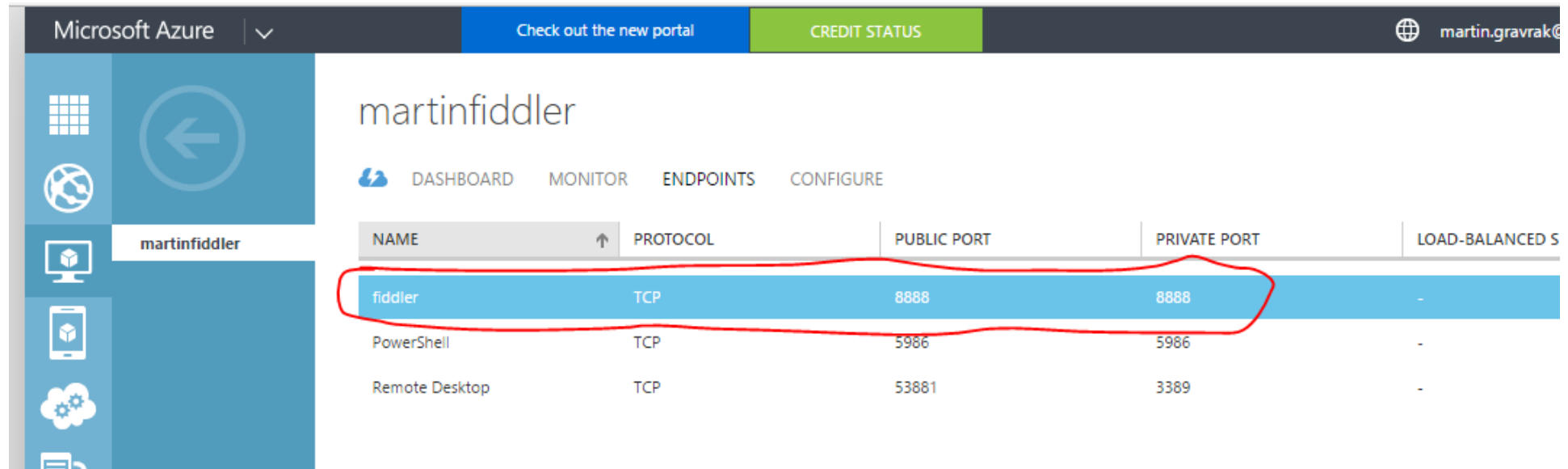
Decrypt HTTPS Traffic



Installing on iPhone..



Running Fiddler in Azure



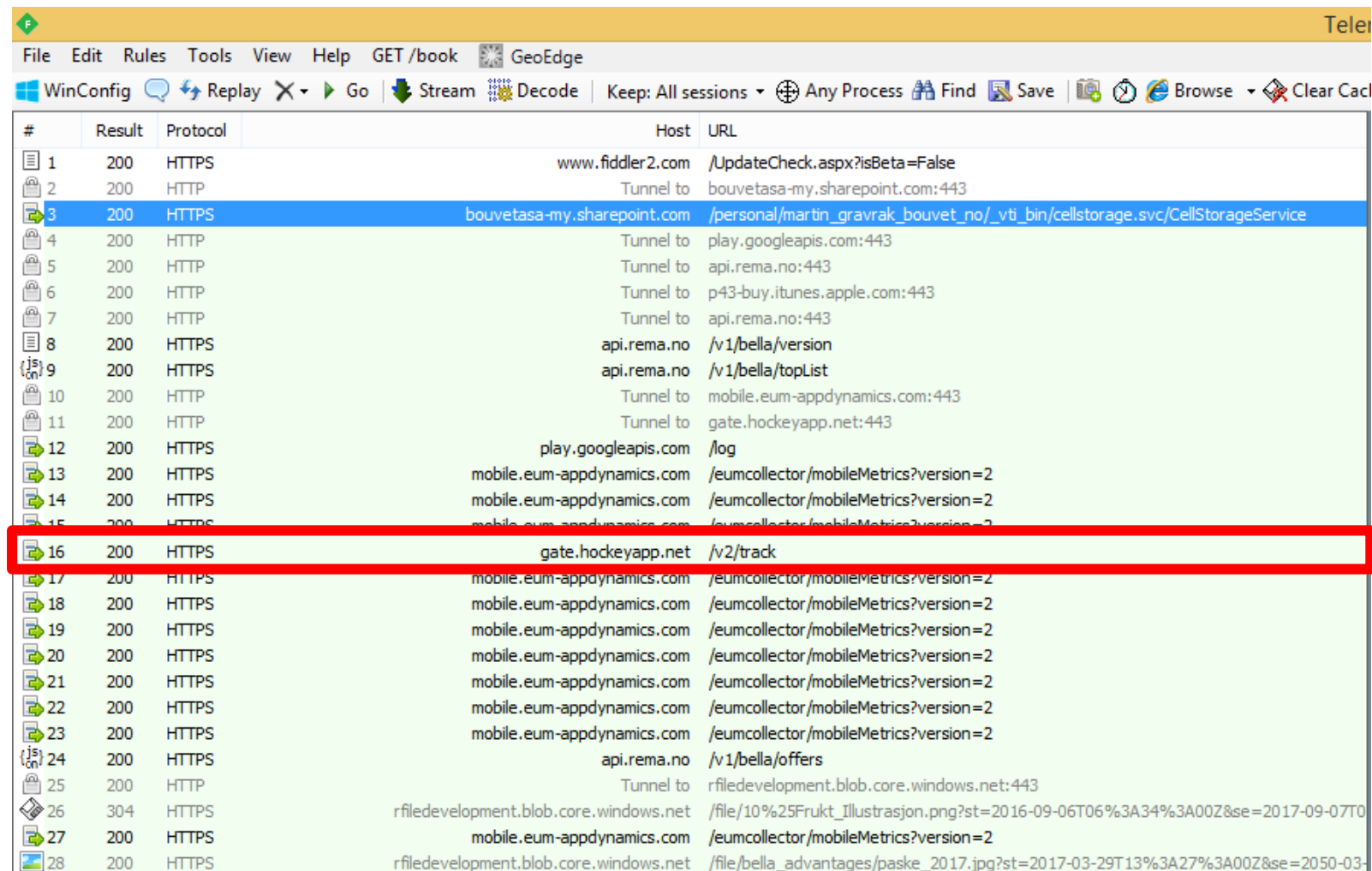
Microsoft Azure | Check out the new portal | CREDIT STATUS | martin.gravrak@

martinfiddler

DASHBOARD MONITOR **ENDPOINTS** CONFIGURE

NAME	PROTOCOL	PUBLIC PORT	PRIVATE PORT	LOAD-BALANCED S
fiddler	TCP	8888	8888	-
PowerShell	TCP	5986	5986	-
Remote Desktop	TCP	53881	3389	-

Running Fiddler



#	Result	Protocol	Host	URL
1	200	HTTPS	www.fiddler2.com	/UpdateCheck.aspx?isBeta=False
2	200	HTTP	Tunnel to	bouvetasa-my.sharepoint.com:443
3	200	HTTPS	bouvetasa-my.sharepoint.com	/personal/martin_gravrak_bouvet_no/_vti_bin/cellstorage.svc/CellStorageService
4	200	HTTP	Tunnel to	play.googleapis.com:443
5	200	HTTP	Tunnel to	api.rema.no:443
6	200	HTTP	Tunnel to	p43-buy.itunes.apple.com:443
7	200	HTTP	Tunnel to	api.rema.no:443
8	200	HTTPS	api.rema.no	/v1/bella/version
9	200	HTTPS	api.rema.no	/v1/bella/topList
10	200	HTTP	Tunnel to	mobile.eum-appdynamics.com:443
11	200	HTTP	Tunnel to	gate.hockeyapp.net:443
12	200	HTTPS	play.googleapis.com	/log
13	200	HTTPS	mobile.eum-appdynamics.com	/eumcollector/mobileMetrics?version=2
14	200	HTTPS	mobile.eum-appdynamics.com	/eumcollector/mobileMetrics?version=2
15	200	HTTPS	mobile.eum-appdynamics.com	/eumcollector/mobileMetrics?version=2
16	200	HTTPS	gate.hockeyapp.net	/v2/track
17	200	HTTPS	mobile.eum-appdynamics.com	/eumcollector/mobileMetrics?version=2
18	200	HTTPS	mobile.eum-appdynamics.com	/eumcollector/mobileMetrics?version=2
19	200	HTTPS	mobile.eum-appdynamics.com	/eumcollector/mobileMetrics?version=2
20	200	HTTPS	mobile.eum-appdynamics.com	/eumcollector/mobileMetrics?version=2
21	200	HTTPS	mobile.eum-appdynamics.com	/eumcollector/mobileMetrics?version=2
22	200	HTTPS	mobile.eum-appdynamics.com	/eumcollector/mobileMetrics?version=2
23	200	HTTPS	mobile.eum-appdynamics.com	/eumcollector/mobileMetrics?version=2
24	200	HTTPS	api.rema.no	/v1/bella/offers
25	200	HTTP	Tunnel to	rfiledevelopment.blob.core.windows.net:443
26	304	HTTPS	rfiledevelopment.blob.core.windows.net	/file/10%25Frukt_Illustrasjon.png?st=2016-09-06T06%3A34%3A00Z&se=2017-09-07T0
27	200	HTTPS	mobile.eum-appdynamics.com	/eumcollector/mobileMetrics?version=2
28	200	HTTPS	rfiledevelopment.blob.core.windows.net	/file/bella_advantages/paske_2017.jpg?st=2017-03-29T13%3A27%3A00Z&se=2050-03-

Inspecting the data

The screenshot shows a web debugging tool interface with two main panes. The top pane displays a POST request to `https://gate.hockeyapp.net/v2/track HTTP/1.1`. The request headers include `Host: gate.hockeyapp.net`, `ADRUM_1: isMobile:true`, `Accept: */*`, `Accept-Language: nb-no`, `Accept-Encoding: gzip`, `Content-Type: application/x-json-stream`, `Charset: UTF-8`, `Content-Length: 761`, `User-Agent: %C3%86/66 CFNetwork/808.3 Darwin/16.3.0`, `Connection: keep-alive`, and `ADRUM: isAjax:true`. The request body is a JSON object containing application insights data, including session state, device information (iPhone6,2), and session details.

The bottom pane displays the response, which is an `HTTP/1.1 200 OK` with headers: `Content-Length: 49`, `Content-Type: application/json; charset=utf-8`, `Server: Microsoft-IIS/8.5`, `X-ms-session-id: 8E8BA5FF-C9F3-4BD6-8CCB-AA2B5193CA36`, `Strict-Transport-Security: max-age=31536000`, `Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Name, Content-Type, Accept`, `Access-Control-Allow-Origin: *`, `Access-Control-Max-Age: 3600`, `X-Content-Type-Options: nosniff`, `X-Powered-By: ASP.NET`, and `Date: Wed, 05 Apr 2017 13:35:10 GMT`. The response body is a JSON object: `{"itemsReceived":1,"itemsAccepted":1,"errors":[]}`.

JSON

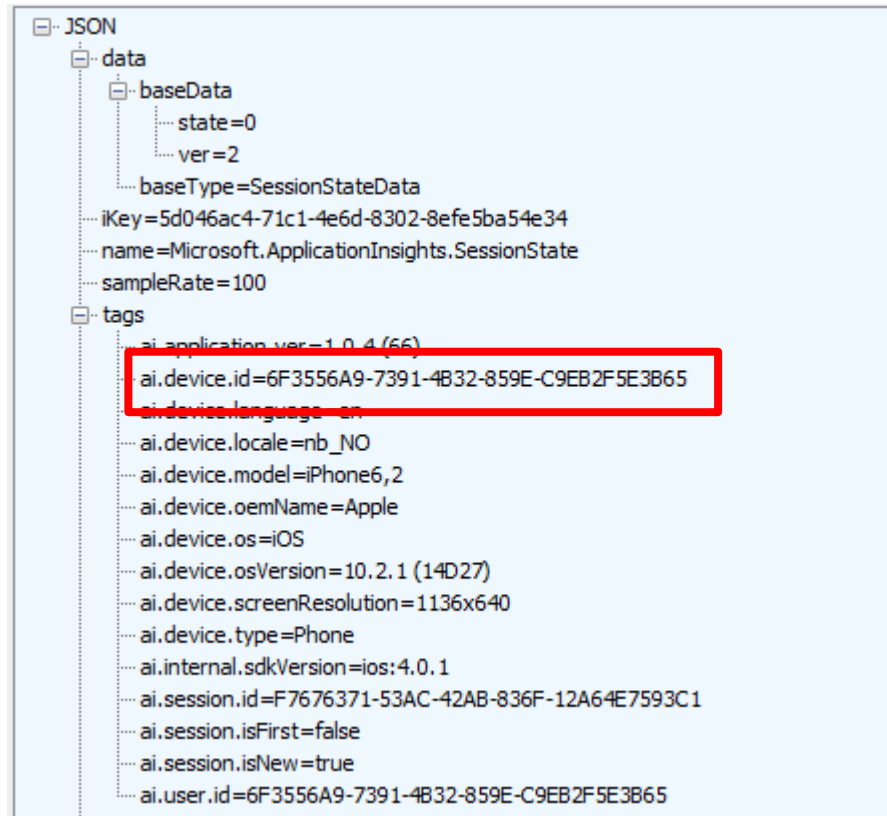
The screenshot displays a web debugging tool interface with a top toolbar containing icons for Statistics, Inspectors, AutoResponder, Composer, FiddlerScript, Log, Filters, Timeline, and APITest. Below the toolbar is a row of tabs: Headers, TextView, SyntaxView, WebForms, HexView, Auth, Cookies, Raw, JSON (selected), and XML. The main content area shows a JSON object with a tree view on the left and its raw text on the right. The JSON structure is as follows:

```
{
  "data": {
    "baseData": {
      "state": 0,
      "ver": 2,
      "baseType": "SessionStateData"
    },
    "iKey": "5d046ac4-71c1-4e6d-8302-8efe5ba54e34",
    "name": "Microsoft.ApplicationInsights.SessionState",
    "sampleRate": 100
  },
  "tags": {
    "ai.application.ver": "1.0.4 (66)",
    "ai.device.id": "6F3556A9-7391-4B32-859E-C9EB2F5E3B65",
    "ai.device.language": "en",
    "ai.device.locale": "nb_NO",
    "ai.device.model": "iPhone6,2",
    "ai.device.oemName": "Apple",
    "ai.device.os": "iOS",
    "ai.device.osVersion": "10.2.1 (14D27)",
    "ai.device.screenResolution": "1136x640",
    "ai.device.type": "Phone",
    "ai.internal.sdkVersion": "ios:4.0.1",
    "ai.session.id": "F7676371-53AC-42AB-836F-12A64E7593C1",
    "ai.session.isFirst": false,
    "ai.session.isNew": true,
    "ai.user.id": "6F3556A9-7391-4B32-859E-C9EB2F5E3B65",
    "time": "2017-04-05T13:35:07.611Z",
    "ver": 1
  }
}
```

Below the JSON text, there are buttons for "Expand All" and "Collapse", followed by the status message "JSON parsing completed." At the bottom, there is another row of tabs: Transformer, Headers, TextView, SyntaxView, ImageView, HexView, WebView, Auth, Caching, Cookies, Raw, JSON (selected), and XML. The bottom-most section shows a partial JSON object:

```
{
  "errors": ...,
  "itemsAccepted": 1,
  "itemsReceived": 1
}
```

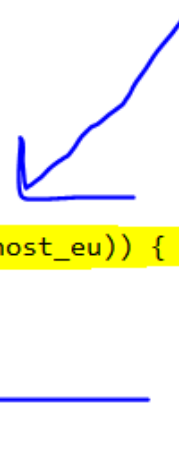
A closer look



SSL Pinning

```
class C15251 implements HostnameVerifier {
    C15251() {
    }

    public boolean verify(String str, SSLSession sSSLSession) {
        try {
            X509Certificate[] peerCertificateChain = sSSLSession.getPeerCertificateChain();
            peerCertificateChain[0].checkValidity();
            String name = peerCertificateChain[0].getSubjectDN().getName();
            if (AppsDeviceParameters.isLog) {
                LogUtils.m6489i(EuropeHttpsPost.TAG, name + " :: " + str);
            }
            if (name.contains(EuropeHttpsPost.host_com_cn) || name.contains(EuropeHttpsPost.host_eu)) {
                LogUtils.m6489i("server", "certificate verify successfully");
                return true;
            }
            LogUtils.m6493w("server", "certificate verify failed :: 1");
            return false;
        } catch (SSLPeerUnverifiedException e) {
            LogUtils.m6493w("server", "certificate verify failed :: 3");
            e.printStackTrace();
            return false;
        } catch (CertificateExpiredException e) {
```





Wireshark

Application	(HTTP)
Transport	(TCP)
Network	(IP)
Link	(Ethernet)

Wireshark



Wireshark

- Filter data

Wireshark

- Filter data
- Multiple recordings
- Strict testing protocol

Wireshark

- t=5s: start app
- t=15s: press play button
- t=20s: ask the doll a question
- t=60s: ask about the weather

Wireshark

- Demo...

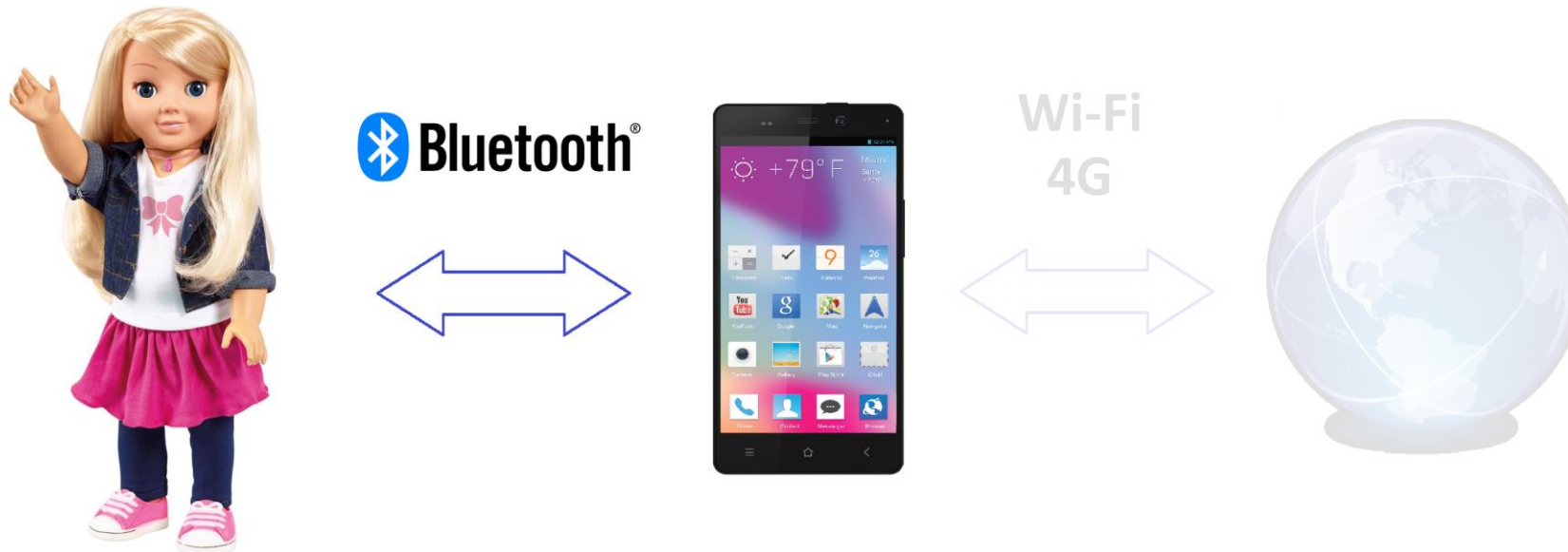
Wireshark

- 23kB of data sent to Nuance
- Toll quality voice at 12kbps

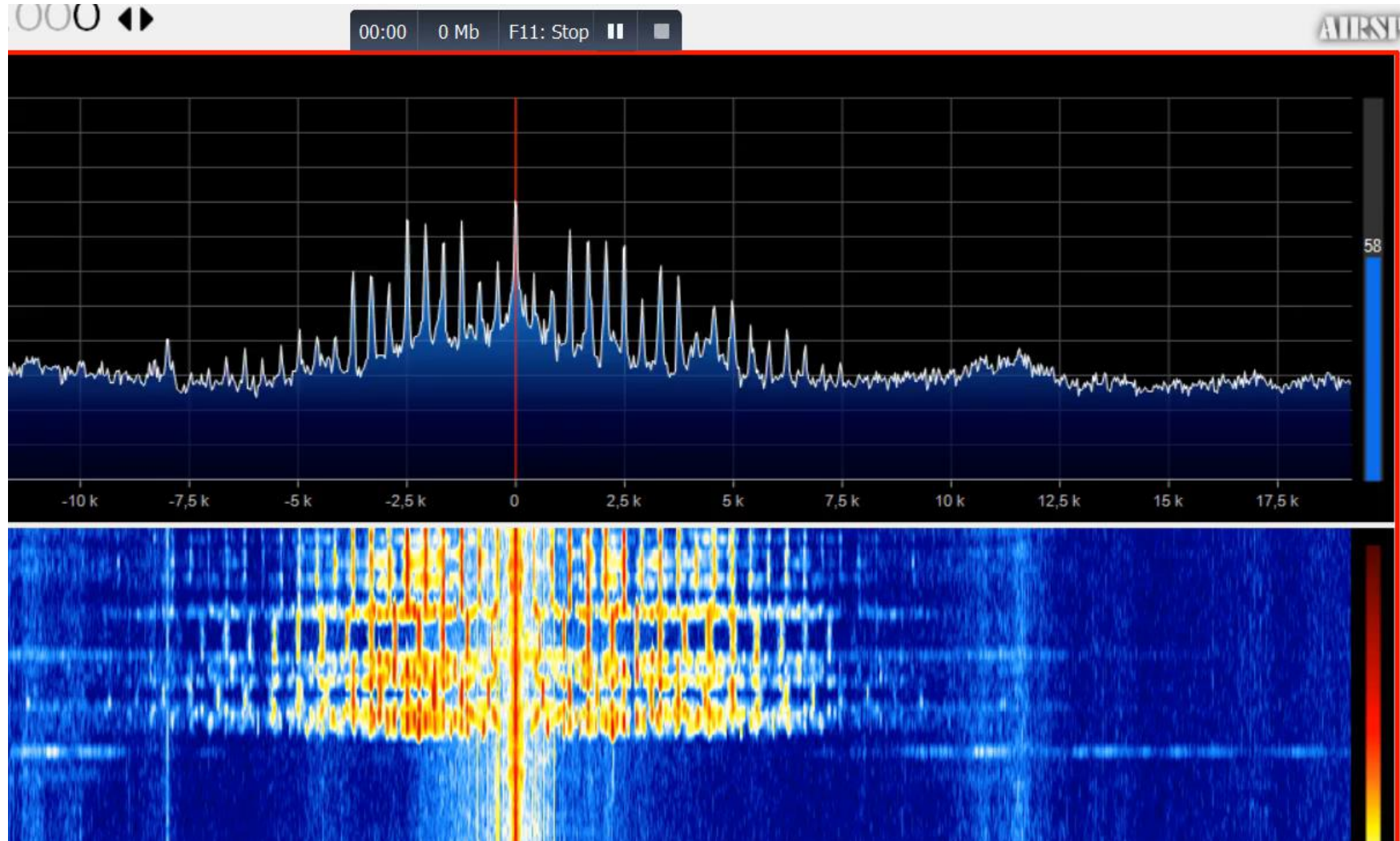
Wireshark

- 23kB of data sent to Nuance
- Toll quality voice at 12kbps
- 15 seconds of voice recording

Toy <-> App



Frequency Jumping



Bluetooth communication



HackRF



Übertooth



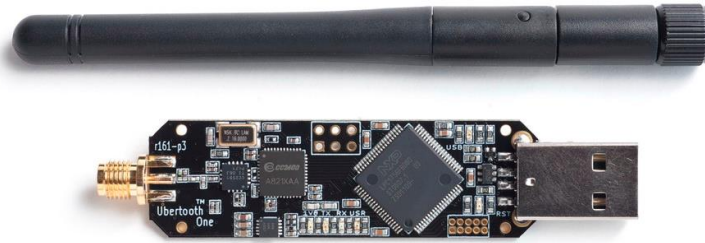
Bluetooth LE Sniffer

Bluetooth Low Energy



Bluetooth LE Sniffer

Bluetooth Classic



Ubertooth

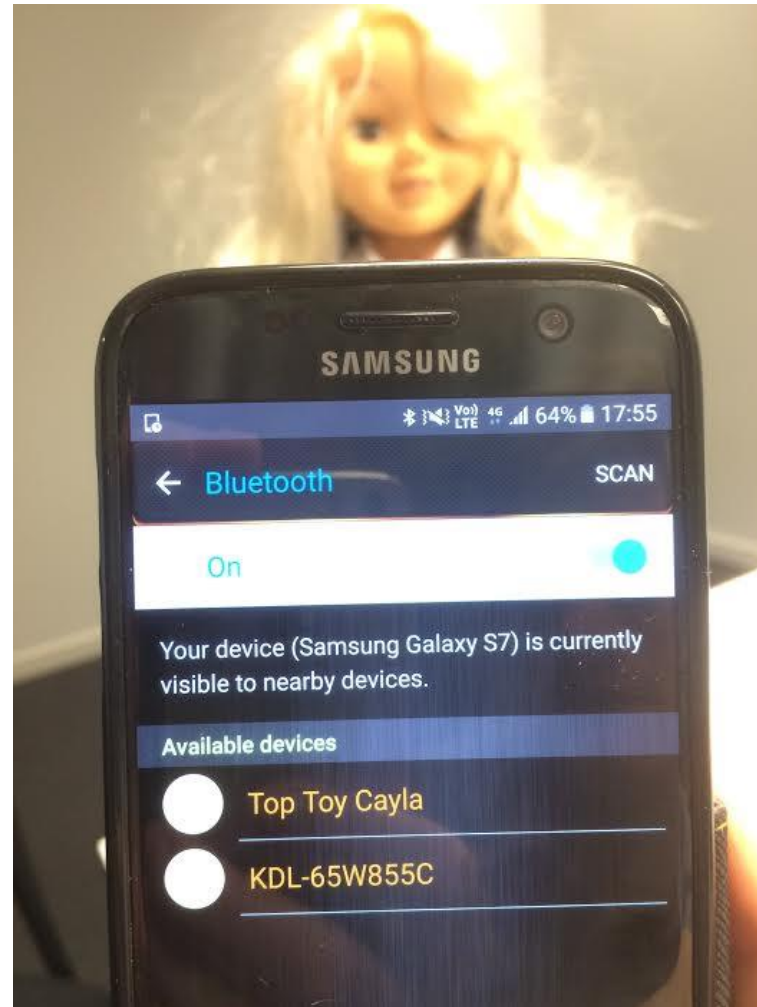
<http://ubertooth.sourceforge.net/>

Software Defined Radio



HackRF

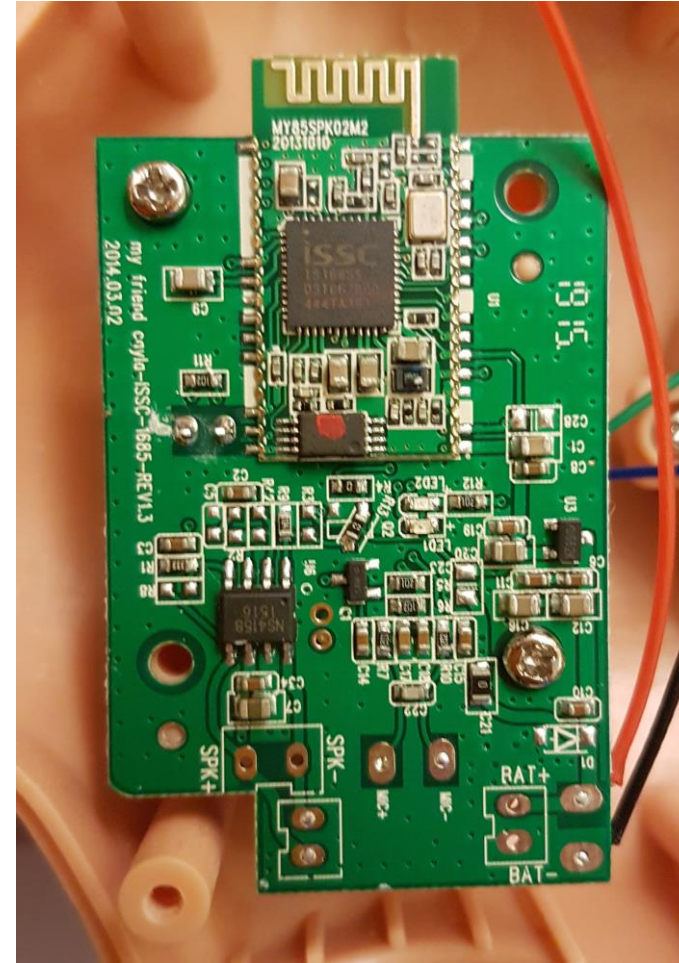
No need for fancy tools..



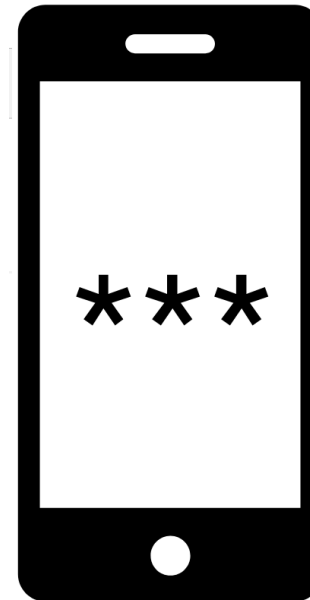
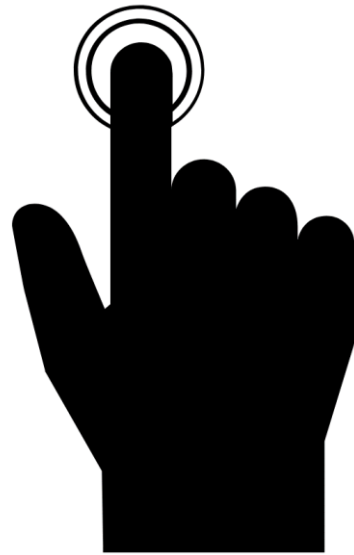
Hardware



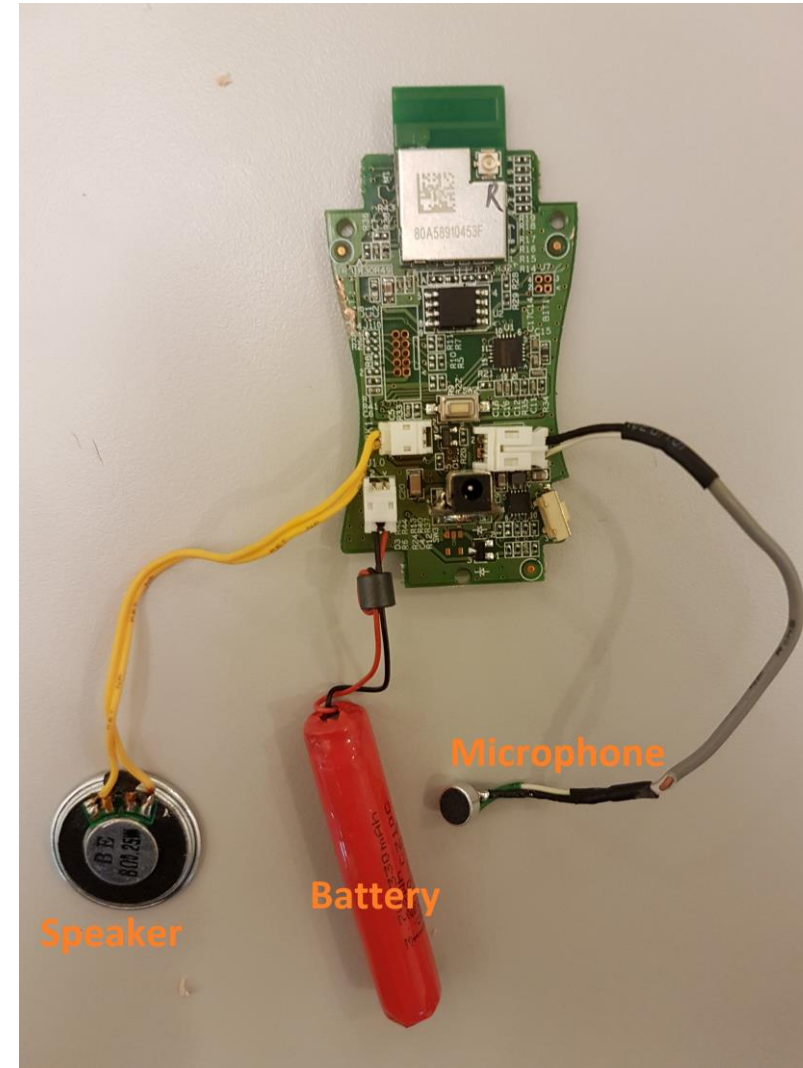
Hardware



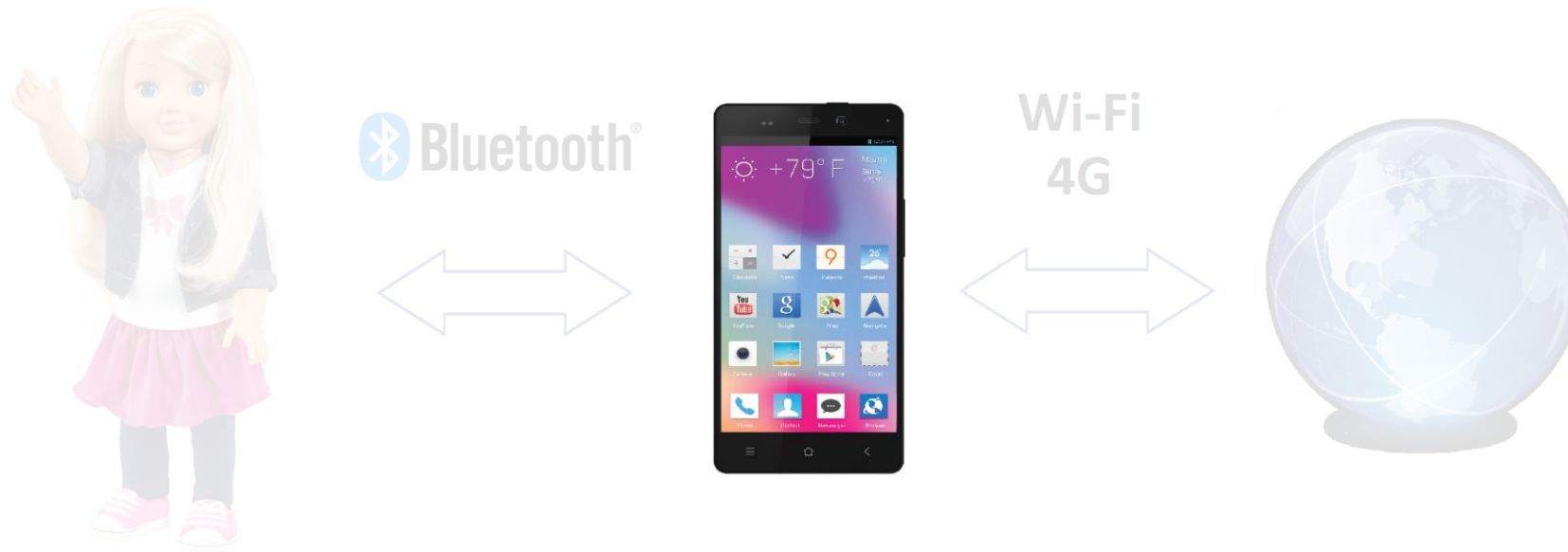
“...useful whenever product implementers want to make the user experience easier and have accepted the increased risk of security attacks.”



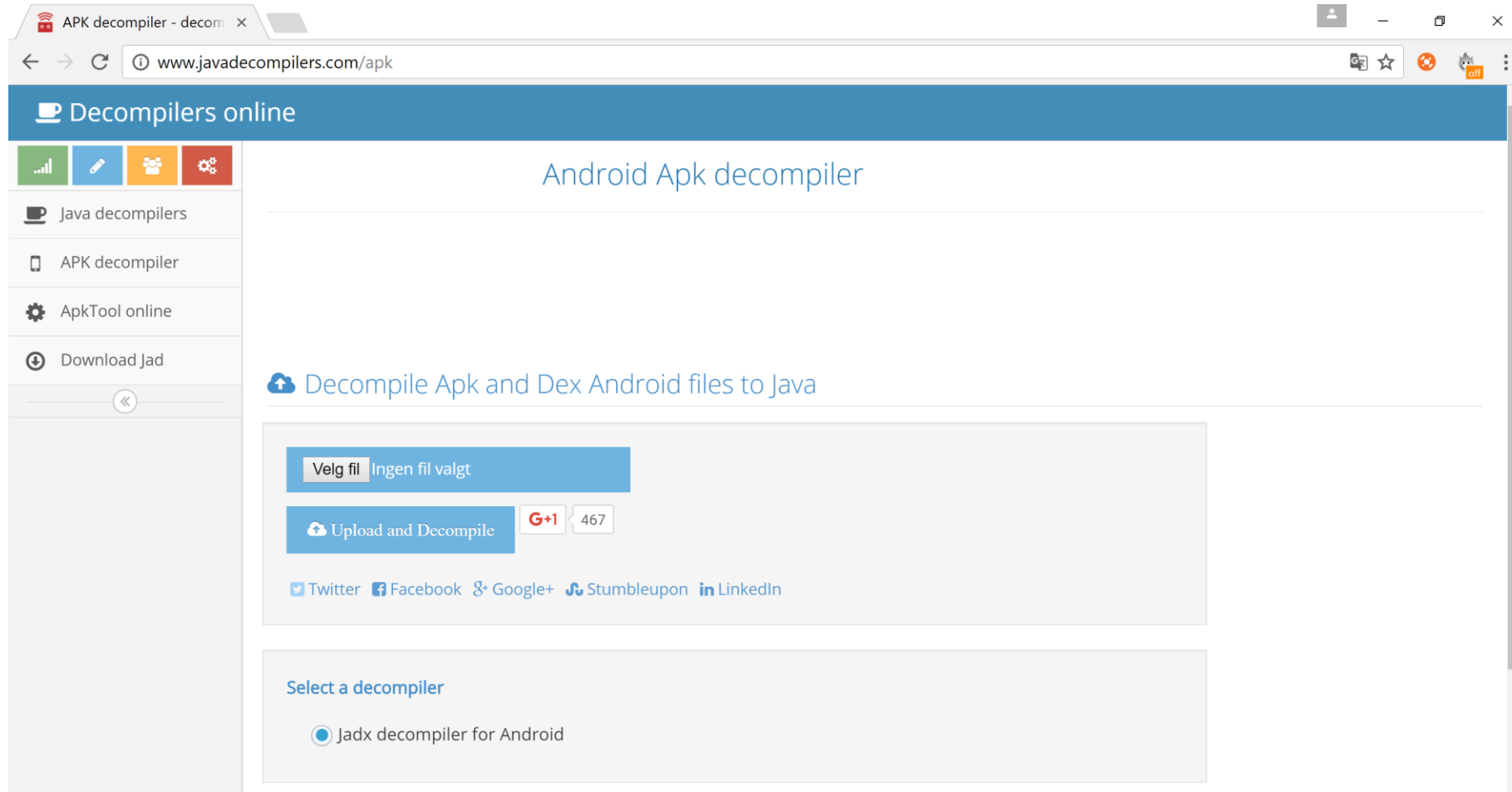




Application



Decompile



Decompile

```
package test;

import java.util.regex.Matcher;
import java.util.regex.Pattern;

public class TestMath {
    public void test1() {
        String[] patterns = new String[]{"add (d{+}) by (d{+})", "multiply (d{+} by (d{+}))"};
        for (String q : new String[]{"add 200 by 30", "add 200 by do", "multiply 5 by 10"}) {
            for (String p : patterns) {
                Matcher matcher = Pattern.compile(p).matcher(q);
                System.out.println(q + ", found:" + matcher.find());
                String g = matcher.group();
                int gc = matcher.groupCount();
                for (int i = 0; i < gc; i++) {
                    if (matcher.find()) {
                        System.out.println(matcher.group(i));
                    }
                }
            }
        }
    }

    public static void main(String[] args) {
        new TestMath().test1();
    }
}
```

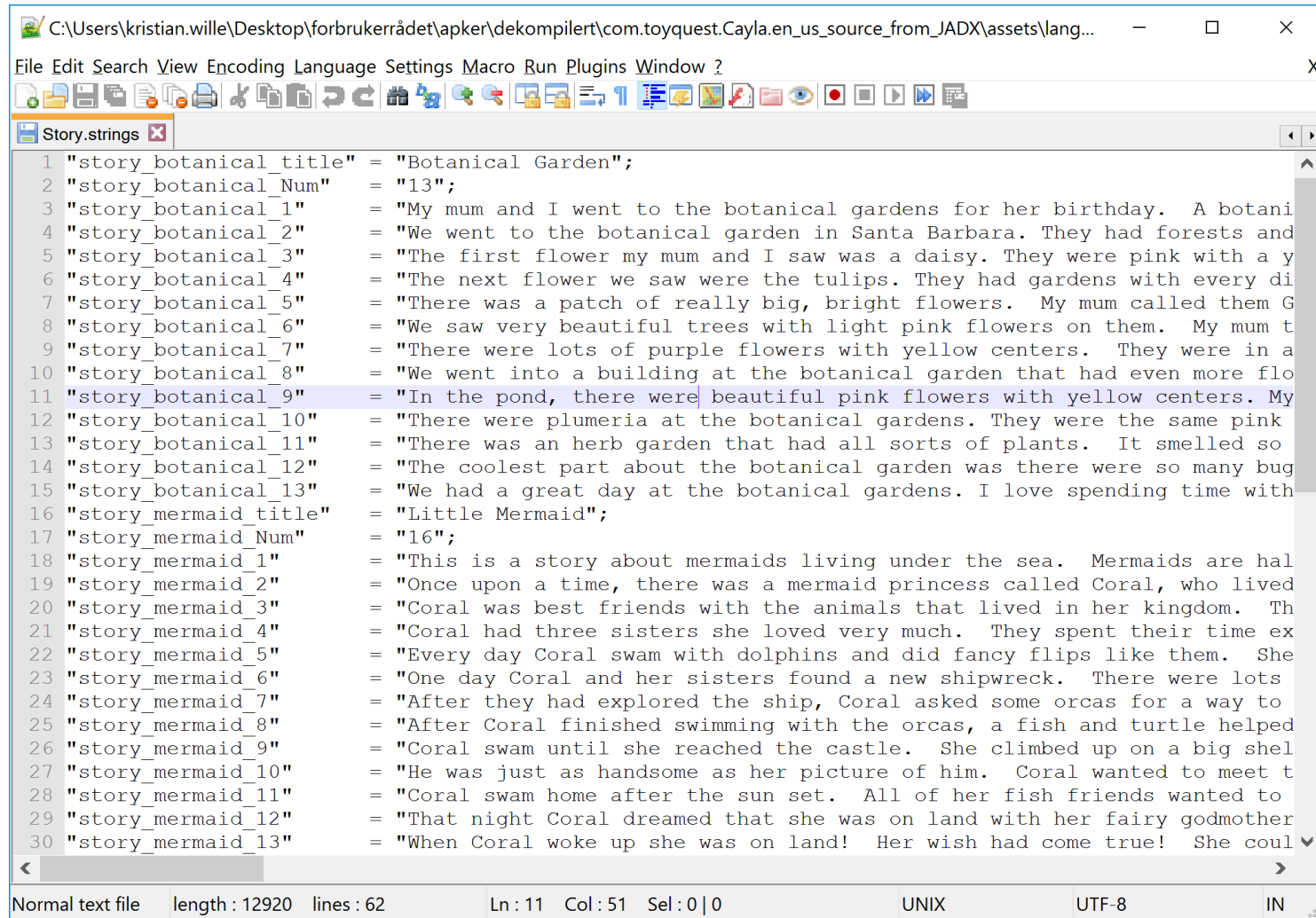
Decompile

android	23.11.2016 12.29	File folder	
assets	23.11.2016 12.29	File folder	
cn	23.11.2016 12.30	File folder	
com	23.11.2016 12.30	File folder	
cz	23.11.2016 12.30	File folder	
javacommon	23.11.2016 12.30	File folder	
lib	23.11.2016 12.29	File folder	
net	23.11.2016 12.30	File folder	
org	23.11.2016 12.30	File folder	
original	23.11.2016 12.29	File folder	
res	23.11.2016 12.29	File folder	
test	23.11.2016 12.30	File folder	
unknown	23.11.2016 12.29	File folder	
AndroidManifest	23.11.2016 12.30	XML Document	4 KB
apktool.yml	23.11.2016 12.29	YML File	1 KB
JDOMAbout\$Author.java	23.11.2016 12.29	JAVA File	1 KB
JDOMAbout\$Info.java	23.11.2016 12.29	JAVA File	2 KB
JDOMAbout.java	23.11.2016 12.29	JAVA File	2 KB
Ognl.java	23.11.2016 12.29	JAVA File	4 KB

Decompile

 audio	23.11.2016 12.29	File folder	
 ccbi	23.11.2016 12.29	File folder	
 ccbResources	23.11.2016 12.29	File folder	
 fonts	23.11.2016 12.29	File folder	
 i18n-resources-iphonehd	23.11.2016 12.29	File folder	
 language	23.11.2016 12.29	File folder	
 location	23.11.2016 12.29	File folder	
 resources-iphonehd	23.11.2016 12.29	File folder	
 song	23.11.2016 12.29	File folder	
 vox	23.11.2016 12.29	File folder	
 agreement	23.11.2016 12.29	HTML File	49 KB
 agreement_ios	23.11.2016 12.29	Microsoft Word 9...	82 KB
 cayla.cd	23.11.2016 12.29	Class Diagram file	938 KB
 fileLookup.plist	23.11.2016 12.29	PLIST File	1 KB
 icudt46l	23.11.2016 12.29	Compressed (zipp...	2 252 KB

Decompile

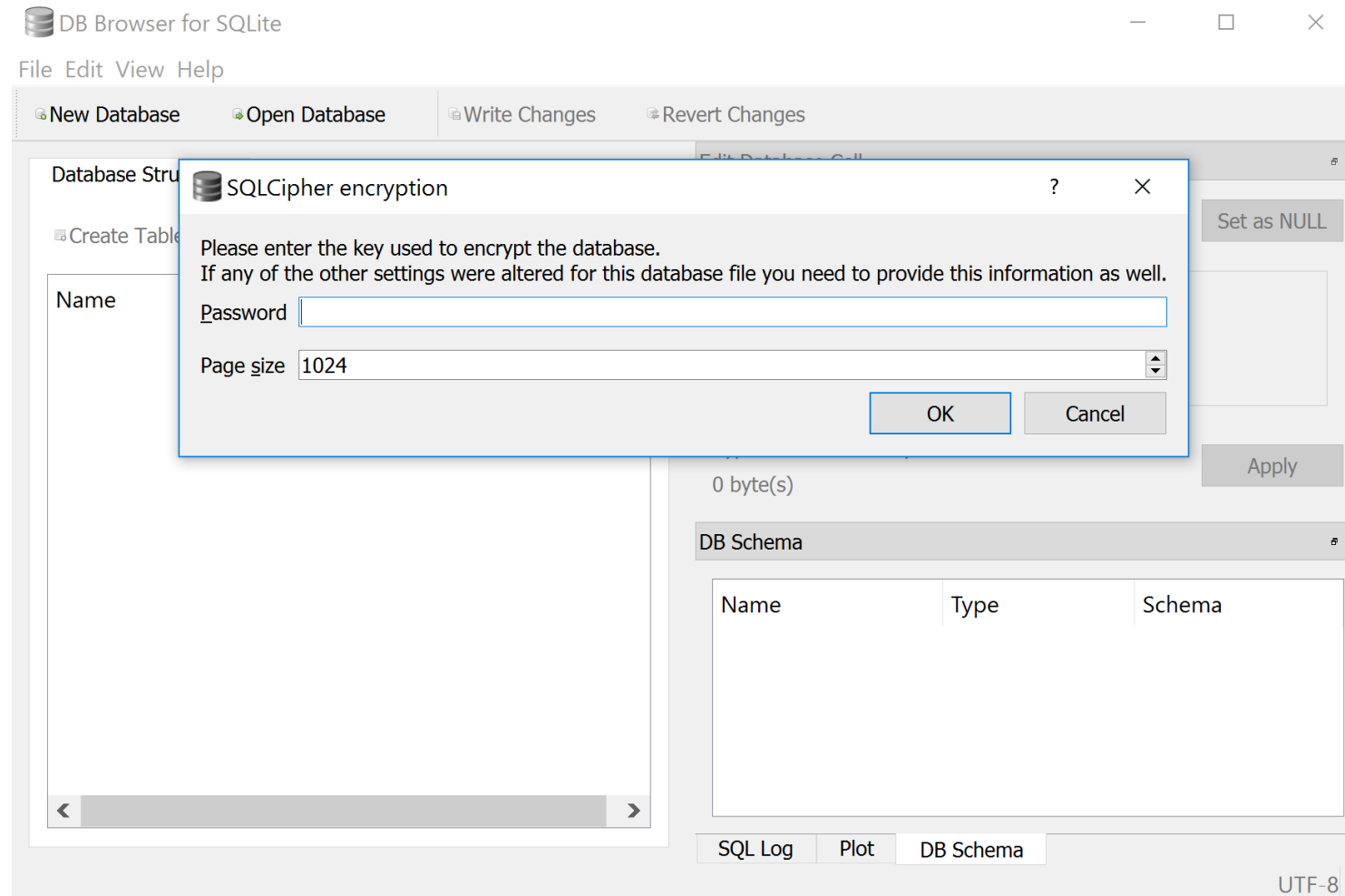


```
C:\Users\kristian.wille\Desktop\forbrukerrådet\apker\dekompile\com.toyquest.Cayla.en_us_source_from_JADX\assets\lang...
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
Story.strings
1 "story_botanical_title" = "Botanical Garden";
2 "story_botanical_Num" = "13";
3 "story_botanical_1" = "My mum and I went to the botanical gardens for her birthday. A botani
4 "story_botanical_2" = "We went to the botanical garden in Santa Barbara. They had forests and
5 "story_botanical_3" = "The first flower my mum and I saw was a daisy. They were pink with a y
6 "story_botanical_4" = "The next flower we saw were the tulips. They had gardens with every di
7 "story_botanical_5" = "There was a patch of really big, bright flowers. My mum called them G
8 "story_botanical_6" = "We saw very beautiful trees with light pink flowers on them. My mum t
9 "story_botanical_7" = "There were lots of purple flowers with yellow centers. They were in a
10 "story_botanical_8" = "We went into a building at the botanical garden that had even more flo
11 "story_botanical_9" = "In the pond, there were beautiful pink flowers with yellow centers. My
12 "story_botanical_10" = "There were plumeria at the botanical gardens. They were the same pink
13 "story_botanical_11" = "There was an herb garden that had all sorts of plants. It smelled so
14 "story_botanical_12" = "The coolest part about the botanical garden was there were so many bug
15 "story_botanical_13" = "We had a great day at the botanical gardens. I love spending time with
16 "story_mermaid_title" = "Little Mermaid";
17 "story_mermaid_Num" = "16";
18 "story_mermaid_1" = "This is a story about mermaids living under the sea. Mermaids are hal
19 "story_mermaid_2" = "Once upon a time, there was a mermaid princess called Coral, who lived
20 "story_mermaid_3" = "Coral was best friends with the animals that lived in her kingdom. Th
21 "story_mermaid_4" = "Coral had three sisters she loved very much. They spent their time ex
22 "story_mermaid_5" = "Every day Coral swam with dolphins and did fancy flips like them. She
23 "story_mermaid_6" = "One day Coral and her sisters found a new shipwreck. There were lots
24 "story_mermaid_7" = "After they had explored the ship, Coral asked some orcas for a way to
25 "story_mermaid_8" = "After Coral finished swimming with the orcas, a fish and turtle helped
26 "story_mermaid_9" = "Coral swam until she reached the castle. She climbed up on a big shel
27 "story_mermaid_10" = "He was just as handsome as her picture of him. Coral wanted to meet t
28 "story_mermaid_11" = "Coral swam home after the sun set. All of her fish friends wanted to
29 "story_mermaid_12" = "That night Coral dreamed that she was on land with her fairy godmother
30 "story_mermaid_13" = "When Coral woke up she was on land! Her wish had come true! She coul
Normal text file length : 12920 lines : 62 Ln : 11 Col : 51 Sel : 0 | 0 UNIX UTF-8 IN
```

Decompile

 audio	23.11.2016 12.29	File folder	
 ccbi	23.11.2016 12.29	File folder	
 ccbResources	23.11.2016 12.29	File folder	
 fonts	23.11.2016 12.29	File folder	
 i18n-resources-iphonehd	23.11.2016 12.29	File folder	
 language	23.11.2016 12.29	File folder	
 location	23.11.2016 12.29	File folder	
 resources-iphonehd	23.11.2016 12.29	File folder	
 song	23.11.2016 12.29	File folder	
 vox	23.11.2016 12.29	File folder	
 agreement	23.11.2016 12.29	HTML File	49 KB
 agreement_ios	23.11.2016 12.29	Microsoft Word 9...	82 KB
 cayla.cd	23.11.2016 12.29	Class Diagram file	938 KB
 fileLookup.plist	23.11.2016 12.29	PLIST File	1 KB
 icudt46l	23.11.2016 12.29	Compressed (zipp...	2 252 KB

Decompile



Decompile

	database	Date modified: 23.11.2016 12.30
	database	Date modified: 23.11.2016 12.29
	DatabaseHelper.java	Date modified: 23.11.2016 12.30 Size: 6,51 KB
C:\Users\kristian.wille\Desktop\forbrukerrådet\apker...	Type: JAVA File	
	DatabaseConnectionProxy.java	Date modified: 23.11.2016 12.30 Size: 4,18 KB
C:\Users\kristian.wille\Desktop\forbrukerrådet\apker...	Type: JAVA File	
	DatabaseErrorHandler.java	Date modified: 23.11.2016 12.30 Size: 167 bytes
C:\Users\kristian.wille\Desktop\forbrukerrådet\apker...	Type: JAVA File	
	DatabaseInitializer.java	Date modified: 23.11.2016 12.30 Size: 3,39 KB
C:\Users\kristian.wille\Desktop\forbrukerrådet\apker...	Type: JAVA File	
	DatabaseObjectNotClosedException.java	Date modified: 23.11.2016 12.30 Size: 297 bytes
C:\Users\kristian.wille\Desktop\forbrukerrådet\apker...	Type: JAVA File	
	DatabaseUtils.java	Date modified: 23.11.2016 12.30 Size: 29,1 KB
C:\Users\kristian.wille\Desktop\forbrukerrådet\apker...	Type: JAVA File	
	DatabaseConnection.java	Date modified: 23.11.2016 12.30 Size: 1,79 KB
C:\Users\kristian.wille\Desktop\forbrukerrådet\apker...	Type: JAVA File	

Decompile

```
DatabaseHelper.java
4 import com.innomindsolution.Cayla.model.Appscript;
5 import com.innomindsolution.Cayla.model.Badword;
6 import com.innomindsolution.Cayla.model.Joke;
7 import com.innomindsolution.Cayla.model.Kcategory;
8 import com.innomindsolution.Cayla.model.Kkeyword;
9 import com.innomindsolution.Cayla.model.Oid;
10 import com.innomindsolution.Cayla.model.Pquestion;
11 import com.innomindsolution.Cayla.model.Qcategory;
12 import com.innomindsolution.Cayla.model.Qquestion;
13 import com.innomindsolution.Cayla.model.Rcategory;
14 import com.innomindsolution.Cayla.model.Rresponse;
15 import com.innomindsolution.Cayla.model.Trivia;
16 import com.innomindsolution.Cayla.model.Type2category;
17 import com.innomindsolution.Cayla.model.Type2question;
18 import com.innomindsolution.Cayla.model.Type3question;
19 import com.j256.ormlite.dao.Dao;
20 import com.j256.ormlite.dao.RuntimeExceptionDao;
21 import com.j256.ormlite.sqlcipher.android.apptools.OrmLiteSqliteOpenHelper;
22 import com.j256.ormlite.support.ConnectionSource;
23 import java.io.File;
24 import java.io.IOException;
25 import java.sql.SQLException;
26 import net.sqlcipher.database.SQLiteDatabase;
27
28 public class DatabaseHelper extends OrmLiteSqliteOpenHelper {
29     private static final String DATABASE_NAME = "cayla.cd";
30     private static final String DATABASE_PASSWORD = "DJKNTIVtVAf7ge";
31     private static final int DATABASE_VERSION = 4;
32     private Dao<Appscript, Integer> AppscriptDao;
33     private Dao<Joke, Integer> JokeDao;
34     private Dao<Kcategory, Integer> KcategoryDao;
35     private Dao<Kkeyword, Integer> KkeywordDao;
36     private final String LOG_NAME;
37     private Dao<Oid, Integer> OidDao;
38     private Dao<Pquestion, Integer> PquestionDao;
```

Java source file length : 6669 lines : 185 Ln : 41 Col : 38 Sel : 0 | 0 UNIX UTF-8 IN

Decompile

```
DatabaseHelper.java
4 import com.innomindsolution.Cayla.model.Appscript;
5 import com.innomindsolution.Cayla.model.Badword;
6 import com.innomindsolution.Cayla.model.Joke;
7 import com.innomindsolution.Cayla.model.Kcategory;
8 import com.innomindsolution.Cayla.model.Kkeyword;
9 import com.innomindsolution.Cayla.model.Oid;
10 import com.innomindsolution.Cayla.model.Pquestion;
11 import com.innomindsolution.Cayla.model.Qcategory;
12 import com.innomindsolution.Cayla.model.Qquestion;
13 import com.innomindsolution.Cayla.model.Rcategory;
14 import com.innomindsolution.Cayla.model.Rresponse;
15 import com.innomindsolution.Cayla.model.Trivia;
16 import com.innomindsolution.Cayla.model.Type2category;
17 import com.innomindsolution.Cayla.model.Type2question;
18 import com.innomindsolution.Cayla.model.Type3question;
19 import com.j256.ormlite.dao.Dao;
20 import com.j256.ormlite.dao.RuntimeExceptionDao;
21 import com.j256.ormlite.sqlcipher.android.apptools.OrmLiteSqliteOpenHelper;
22 import com.j256.ormlite.support.ConnectionSource;
23 import java.io.File;
24 import java.io.IOException;
25 import java.sql.SQLException;
26 import net.sqlcipher.database.SQLiteDatabase;
27
28 public class DatabaseHelper extends OrmLiteSqliteOpenHelper {
29     private static final String DATABASE_NAME = "cayla_cd";
30     private static final String DATABASE_PASSWORD = "DJKNtIVtVaf7ge[REDACTED]";
31     private static final int DATABASE_VERSION = 4;
32     private Dao<Appscript, Integer> AppscriptDao;
33     private Dao<Joke, Integer> JokeDao;
34     private Dao<Kcategory, Integer> KcategoryDao;
35     private Dao<Kkeyword, Integer> KkeywordDao;
36     private final String LOG_NAME;
37     private Dao<Oid, Integer> OidDao;
38     private Dao<Pquestion, Integer> PquestionDao;

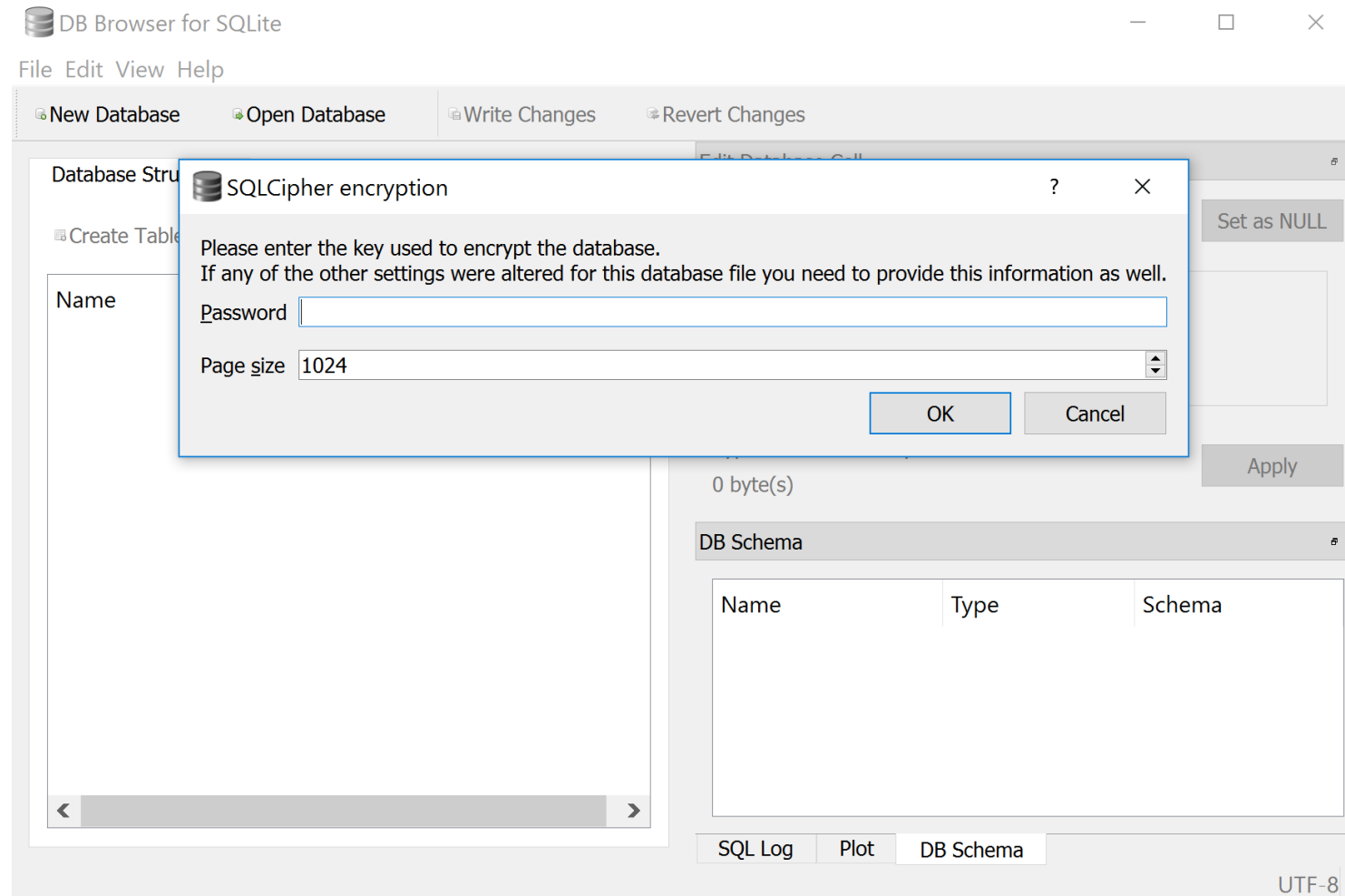
```

Java source file length : 6669 lines : 185 Ln : 41 Col : 38 Sel : 0 | 0 UNIX UTF-8 IN

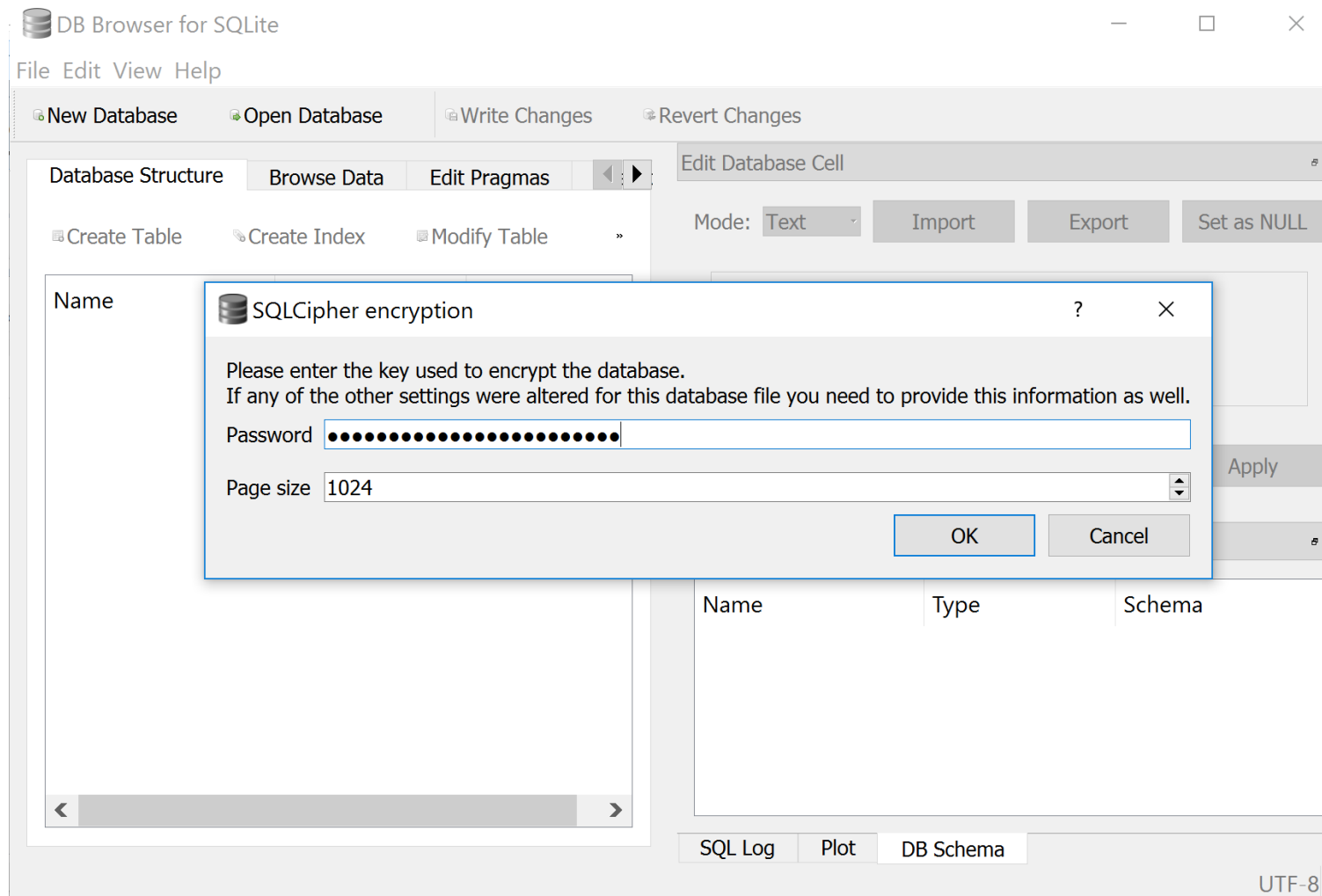
Decompile

 audio	23.11.2016 12.29	File folder	
 ccbi	23.11.2016 12.29	File folder	
 ccbResources	23.11.2016 12.29	File folder	
 fonts	23.11.2016 12.29	File folder	
 i18n-resources-iphonehd	23.11.2016 12.29	File folder	
 language	23.11.2016 12.29	File folder	
 location	23.11.2016 12.29	File folder	
 resources-iphonehd	23.11.2016 12.29	File folder	
 song	23.11.2016 12.29	File folder	
 vox	23.11.2016 12.29	File folder	
 agreement	23.11.2016 12.29	HTML File	49 KB
 agreement_ios	23.11.2016 12.29	Microsoft Word 9...	82 KB
 cayla.cd	23.11.2016 12.29	Class Diagram file	938 KB
 fileLookup.plist	23.11.2016 12.29	PLIST File	1 KB
 icudt46l	23.11.2016 12.29	Compressed (zipp...	2 252 KB

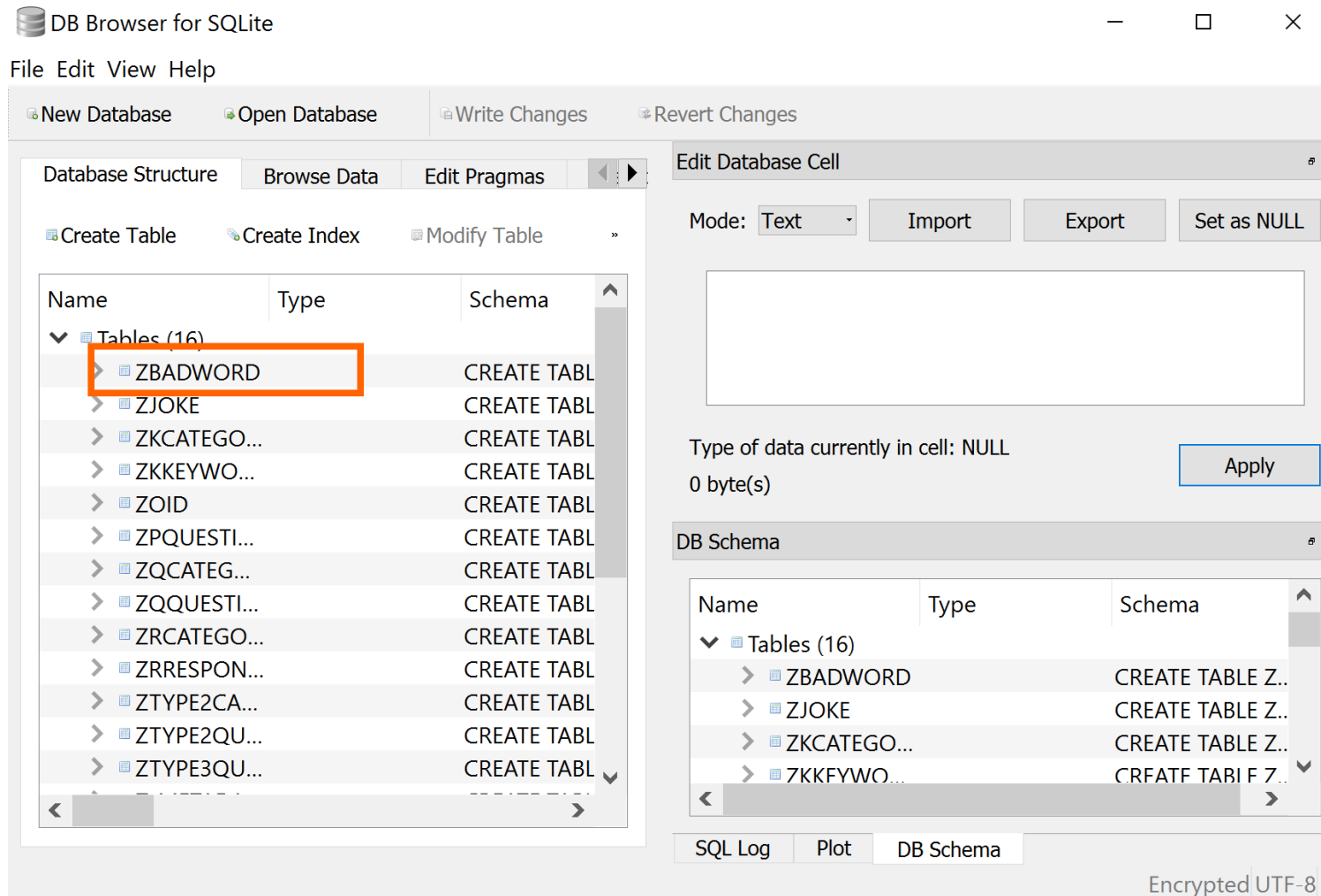
Decompile



Decompile



Decompile



Decompile

Database StructureBrowse DataEdit PragmasExecute SQL

Table: ZBADWNew RecordDelete Record

	ZTYPE	ZNAME
	er	Filter
335		Honky
336		Hooker
337		H
338		
339		
340		
341		
342		HOT DAMN
343		HOT TO TROT
344		HOTPUSSY
345		HUGE DICK

< < 335 - 346 of 1372 > >| Go to: 1

Edit Database Cell

Mode: TextImportExportSet as NULL

HONKEY

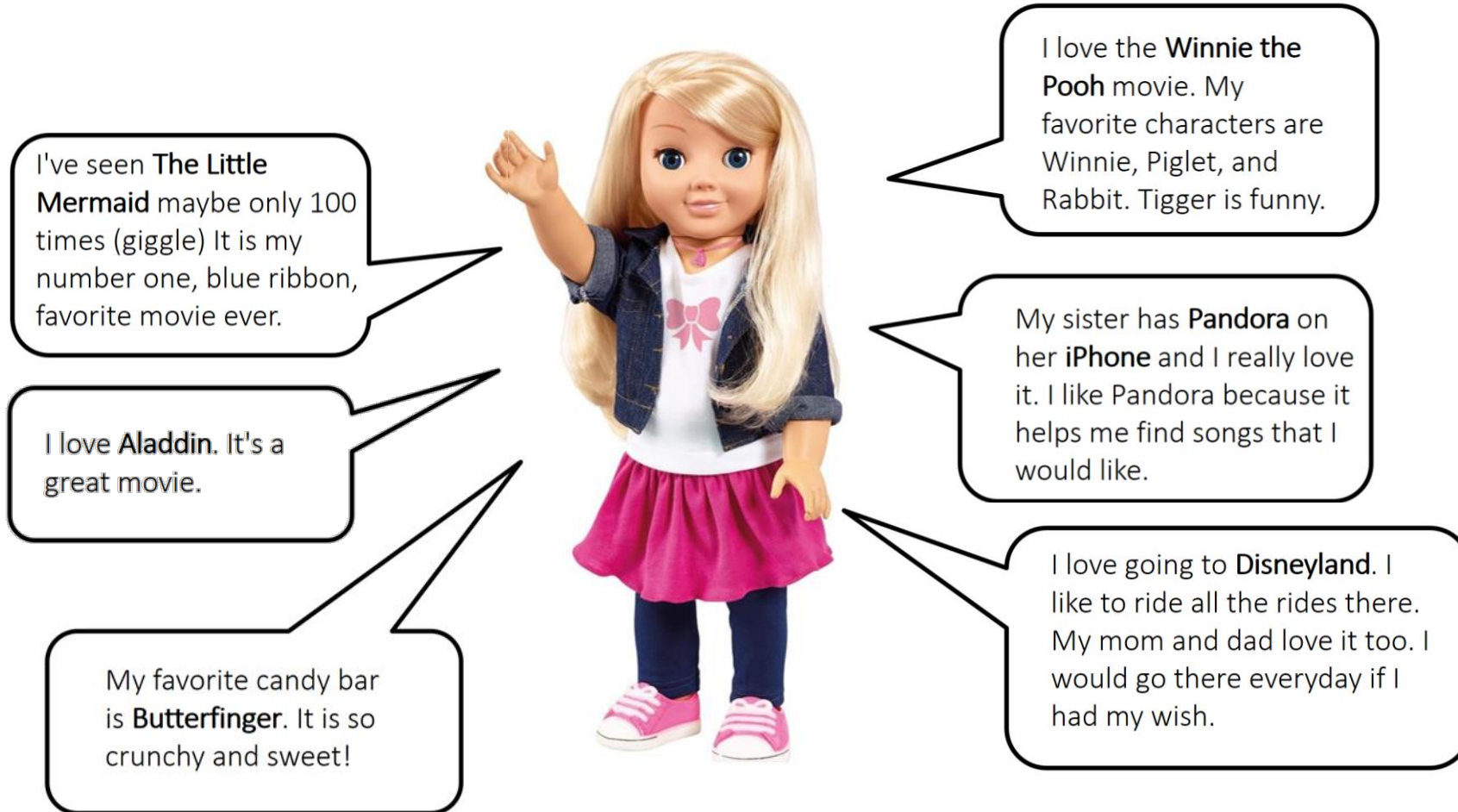
Type of data currently in cell: Text / Numeric
6 char(s)

Apply

DB Schema

Name	Type	Schema
▼ Tables (16)		
> ZBADWORD		CREATE TABLE Z..
> ZJOKE		CREATE TABLE Z..
> ZKCATEGO...		CREATE TABLE Z..
> ZKKEYWO...		CREATE TABLE Z..
> ZOID		CREATE TABLE Z..
> ZPQUESTI...		CREATE TABLE Z..
> ZQCATEG...		CREATE TABLE Z..

Hidden marketing



Results

5.2 Bluetooth Communication

4.1 Man-in-the-middle

To monitor the communication between the app and its web-services a man-in-the-middle approach was taken. This was achieved by routing all of the Internet traffic between the phone/tablets through our computer, making it what is known as a proxy-server. This made it possible to see what information was transmitted between the app and the various Internet servers and how often the communication occurred. Fiddler¹ was used to monitor the Internet Traffic and to create the proxy server.

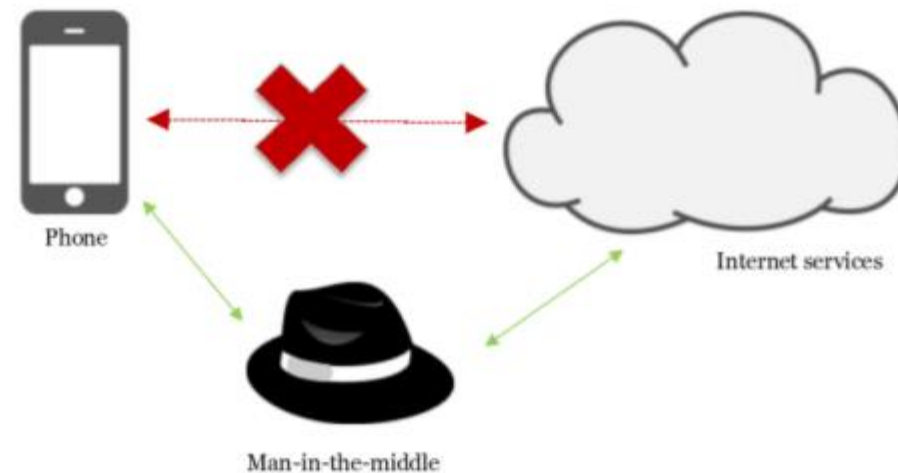


Figure 4: Overview of a man-in-the-middle attack

security, see section 5.2.3. Currently it is possible to stand outside a building and connect to the device given that it is within range, turned on and not connected to another device.

Figure 6, Screenshot on Android during pairing process

While this test were meant to

Results



THE WALL STREET JOURNAL.

SubscribeSPECIAL OFFER

HomeWorldU.S. PoliticsEconomyBusinessTechMarketsOpinionArtsLifeReal Estate

Talking Dolls May Spread Children's Secrets, Privacy Groups Allege

AT&T CEO: Time Warner Deal World 'Disrupt' Cable TV Model

In Southeast Asia, Facebook and Instagram Are Where People Shop

Belarus Aims to Be the Silicon Valley of Eastern Europe



TECH

Talking Dolls May Spread Children's Secrets, Privacy Groups Allege

Complaint alleges My Friend Cayla and I-Que Intelligent Robot collect and use personal information from children

By **GEORGIA WELLS**

Updated Dec. 6, 2016 7:26 p.m. ET

Internet-connected toys pose privacy risks to children, and their parents often aren't aware, according to advocacy groups for children and consumers.

A complaint filed Tuesday with the Federal Trade Commission says the toys—My Friend Cayla and I-Que Intelligent Robot—collect and use personal information from children without their parents' knowledge.

Most Popular Videos

The Boston Globe

TUESDAY, DECEMBER 6, 2016

Two children's toys raise privacy alarms

Voice technology from Nuance comes under fire

By **Hawatha Bray**

An international coalition of consumer watchdogs says Nuance Communications is violating the privacy of children who play with two toys that use the Burlington company's speech-recognition software.

The toys, My Friend Cayla and I-Que Intelligent Robot, use Nuance software to answer questions posed by children. But in complaints they expect to file with federal regulators on Tuesday, the consumer groups allege that Nuance is saving recordings of those interactions with children for future use without providing adequate warning to parents, in violation of a 1998 federal law to protect the online privacy of minors.

Both toys are made by Genesis Toys of Los Angeles, which will also be named in a complaint to the Federal Trade Commission.



Onsdag 7 dec

Sök

Kundservice

Dagens tidning

Pressemeny

SvD NÄRINGSLIV

Start > Näringsliv • Börs Börsplus Motor Näringsliv Debatt Sök företag Kultur L

SSAB B: 31,43 +2,55 % Ericsson B: 50,00 +0,66 % EnQuest PLC: 4,58 +4,90 % Nordic Mines: 0,46 +2,15 % Volvo B: 105,90 +1,15 % Nordex Bank: 99,00 +

Näringsliv

Av TT

61 år 06:19

cb Spara artikel

Viaplay

SvD digital - Viaplay ingår!

Beställ SvD digital och få två månader Viaplay utan extra kostnad

Till enguldsänd

Uppkopplade leksaker är obegripliga användarvillkor – och en teknik som gör avlyssna barnkammaren och kontakta barnet. Nu anklagar konsumenter två leksaker på den svenska marknaden



Sveriges Konsumenter anmäler dockan My Friend Cayla och roboten I-Que till Konsumentverket och Datainspektionen. Foto: Fotokollern.se

Det är dockan My Friend Cayla och roboten I-Que som anmäls till Konsumentverket och Datainspektionen. Detta sedan Sveriges Konsumenters norska motsvarighet testat leksakerna och funnit ett problem.

LE FIGARO.fr

ÉCONOMIE > CONSOMMATION

Les poupées connectées, des espionnes au pied du sapin

Par **Le Figaro.fr** | Mis à jour le 06/12/2016 à 18:02 / Publié le 06/12/2016 à 07:06



Si vous avez prévu d'offrir une poupée connectée pour Noël, vous devriez vous méfier. Selon plusieurs associations de consommateurs, qui ont porté plainte contre deux poupées fabriquées par le hongkongais Genesis Toys, elles peuvent être contrôlées à distance.

Aftenposten

A-magasinet Osloby Sport Meninger

Bli abonnent Meny

Hevder disse lekene sladrer på barnet ditt

GEIR AMUNDSEN

OPPDATERT: 06. DES. 2016 14:13 | PUBLISERT: 06. DES. 2016 12:34

f

t

@



BBC

Sign in

News Sport Weather Shop Earth Travel

NEWS

Home Video World UK Business Tech Science Magazine Entertainment & Arts

Technology

Call for privacy probes over Cayla doll Que toys

trunk porter

2016 Technology

Share



id Cayla doll has been shown in the past to be hackable

of the I-Que and Cayla smart toys have been accused of children to "ongoing surveillance" and posing an "imminent and threat" to their safety and security.

#Toyfail

bouvet

Results



Media Impact



The toys were withdrawn from several markets

- Big toy chains in the United States, Belgium and the Netherlands has stopped the sale of the toys.
- In Norway, Sweden and Denmark BR-Toys and Toys R Us offered money back without a receipt.



In Germany the doll got banned



At the Berlin Spy Museum...



Lesson to be learned





Rate Session

