6 Location based forensics

See **labinstruktion.pdf** for general instructions regarding laborations. Read thru the lab before you begin.

Table of Contents

6.1 GPS spårning

Scenario
Du har i ditt arbete som it-forensiker ombetts att försöka kartlägga var en misstänkt terrorist befunnit sig någonstans en viss dag. Det finns en misstanke om att ett terrordåd planeras mot en större anläggning som är någorlunda kritisk för regionens funktion utmed den misstänktes färdväg.
Lyckligtvis har du lyckats extrahera en slags formaterad positionslogg ifrån den misstänktes GPS navigator (navlog.txt) för just denna dag.
Vad du är intresserad av är är att tyda positionsloggens olika värden. På vilka platser har personen varit eller färdats en viss tidpunkt, samt göra en bedömning om var målet för attacken är beläget.

Se: ”6.5 Bilaga till uppgift 6.1 och GIS referenser” för lösningstips.

Redovisning av uppgiften
Lämna in ett dokument med svar på frågorna.

a) Vilka slags värden är det i positionsloggen?

b) Var har personen varit? En kartbild med den misstänktes rörelser utritade på är ett krav ur rapportsynpunkt.

c) Vad är din bedömning om var målet för attacken är?

Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE

Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/

6.2 Track and trace using cell-id

Report

Hand in the source code with your program solution and answers to questions below.
a) Where have the suspect been for this particular log?
b) Try to determine what kind of transport the suspect have been using?

Scenario
You have requested the Call Detail Record (CDR) and position log for a suspected customer from a certain mobile operator during one whole day 08:00 – 17:00. This because you only found the last used LAC (Location Area Code) on the suspected customers SIM card, a geographical area which can be rather large.

What you got from the mobile operator in return is a log with Cell-Id, LAC, MCC (Mobile Country Code) and Date Time in the included file: **cellid_suspect.txt**. Examine this log and pinpoint the locations where the suspect have been the specific day. The suspects movements for this day and possibly other days are very important for the investigation.

Unfortunately you have no idea how to handle this task. You also know it is probably going to be much more of this type of work in the case, so you decide to do some research in writing a little application that gives the investigators an easy way to check this themselves. You do a quick scan on Internet and found the information/solutions/options below:

Task
Write or modify an existing program that shows the latitude and longitude (location) of the Cell-Id and display it on a map. Look into the attached example program (image below) which is **crippled** and therefore only displaying the same location and the article: "Location-Based Services Using CellID in Windows Mobile" at: http://www.devx.com/wireless/Article/39709, which is attached as well in the folder: devx.com.
If you choose to use this example as basis for your program most of the work is done and you just have to create a Visual C# Windows Forms Application and paste in the devx code listings and the GMM.cs class.

The devx article uses the Google Geolocation API (maps Cell-Id etc. to lat/long values): https://developers.google.com/maps/documentation/business/geolocation/ in an undocumented way. You can use the Google Maps Geolocation API in a documented way if you want, but then you need to write your own requests and obtain an API key. It can then also be used with Wi-Fi access point parameters for even better location precision. You can for testing and development only use it for 100 requests per day.

To get rid of the Script Error dialogues set the property **ScriptErrorsSupressed** to **True** for the webBrowser component.

You may also need to turn off the compatibility view if possible: http://stackoverflow.com/questions/18333459/c-sharp-webbrowser-ajax-call/20848398#20848398

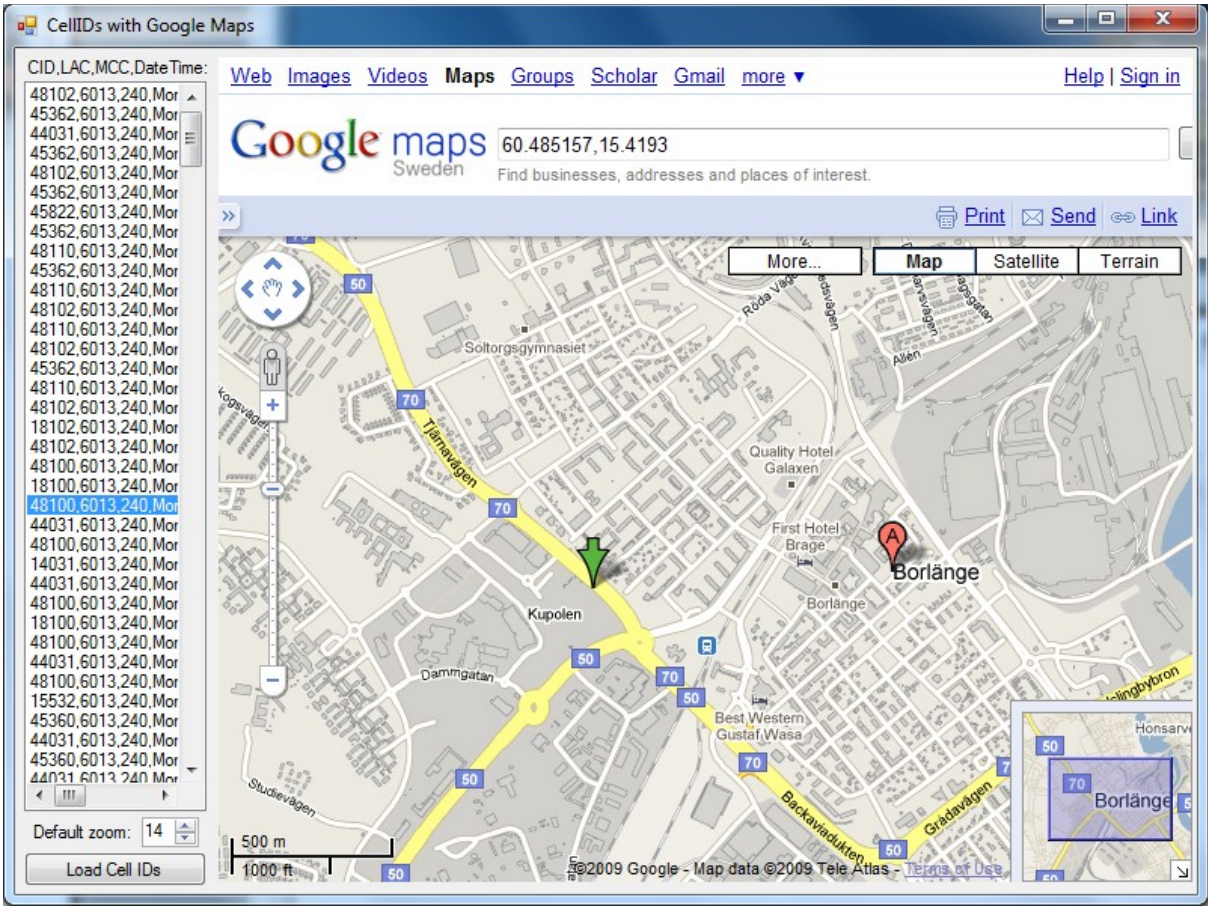
Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE

Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/

You should be able to use other CellId APIs/services/databases as:

- OpenCellId API at: http://www.opencellid.org
- Combain: https://combain.com/
- Unwired labs: http://unwiredlabs.com/
- And possibly others - http://stackoverflow.com/questions/82184/public-cell-id-databases

The problem with the other Cell-Id databases is that they probably not are as good and accurate as the Google Geolocation database.



Cell ID program using Google Maps API.

6.2.1 Voluntary extension task for 6.2

Write a new script/program or extend your above solution so that it processes your collected Cell-Id list/file and produces a new CSV file with <User-Id>,<Latitude>,<Longitude>,<Date Time>, KML file or other file format with the same content. With this file you should be able to display the suspected users movement on a map with common GIS software.

Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE

Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/

6.3 Location History tracking via data from Google Takeout

Report
Show a working solution of some of yours or the attached location history data. Answer with a web link to your solution (your web folder at school for example). If you find a better more forensically controllable visualization solution than the suggested one, hand in this solution instead.

Method
If you got a Google account, download your Google Location History in JSON format here: https://www.google.com/settings/takeout/custom/location_history. The Google Takeout site can also be reached from: https://myaccount.google.com > Personal Info & Privacy > Control your content.

Otherwise (if you don not have a Coogle account, which I doubt) use the attached location history in the file: LocationHistory_small.json.

Using the two Python scripts:

- latitude-trail: https://github.com/Scarygami/latitude-trail
- location-history-json-converter: https://github.com/Scarygami/location-history-json-converter

Make the solution work as my example here: http://users.du.se/~hjo/lbs/location-trail/

Note that there may be some small changes required in the script usage and also file name changes for the JSON data in the .js file. By viewing the browsers console output, if it does not work, you should be able to fix problems that may arise.

Other visualization resources

- http://beneathdata.com/how-to/visualizing-my-location-history/
- https://github.com/theopolisme/location-history-visualizer

6.4 Lab Feedback

a) Was this a relevant and appropriate lab and what about length etc?
b) What corrections and/or improvements do you suggest for this lab?

Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE

Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/

6.5 Bilaga till uppgift 6.1 och GIS referenser

GIS bakgrund och lösningstips
Elementära kunskaper om GIS (Geografiska Informations System), olika GIS programvaror och vad man kan göra med GIS är viktig kunskap för alla it-forensiker enligt denna artikeln: http://www.officer.com/article/10248785/the-other-side-of-mobile-forensics.

För att få mer information om GIS ta t.ex. en titt på: http://sv.wikipedia.org/wiki/GIS, http://en.wikipedia.org/wiki/Geographic_information_system, http://en.wikipedia.org/wiki/List_of_GIS_software och http://en.wikipedia.org/wiki/Category:Free_GIS_software

Tyvärr är de flesta GIS verktyg enormt dyra som t.ex. de två mest använda företagens produkter - ESRIs programsvit http://www.esri.com/ och MapInfo http://www.mapinfo.com/. De är dessutom inte så enkla att använda utan kräver en utbildning, mer eller mindre.

Turligt nog finns det fria alternativ som t.ex. programvarorna listade i ovanstående wiki länkar och på webbsiten: http://www.freegis.org/ som har många olika program för avancerad GIS. Ett annat alternativ är förstås online tjänster baserade på Google Maps etc. men dessa brukar endast kunna användas för enklare problem med liten datamängd.

En programvara jag själv rätt ofta använder för diverse GIS problem är ShapeUp: http://nilione.com/ vilket en god vän till mig utvecklar **(se stycket om ShapeUp för användning)**. Det har en hel del av de funktioner som de dyra programmen har plus att du kan göra egna plugins och då i princip lösa vadsomhelst. Alternativ till detta program är dels Quantum GIS: http://www.qgis.org/ och MapWindow GIS: http://www.mapwindow.org/.

Du kan i arbetet med denna uppgift använda dig av de ovan nämnda programvarorna och shape filerna på: http://users.du.se/~hjo/cs/dt2016/GIS/. Andra exempel på program som du kan ha hjälp av är GPSBabel http://www.gpsbabel.org/, Google Earth och kartorna/funktionerna på: http://www.hitta.se, http://eniro.se/ samt http://maps.google.se/.

SHP2KML
På bloggen: http://freegeographytools.com/2007/recap-of-exporting-shapefiles-to-google-earth-series kan man läsa lite om olika shape 2 KML lösningar samt hur det bifogade shp2kml http://www.zonums.com/shp2kml.html programmet används.

En annan mycket bra sida är: http://lsntap.org/Mapping_CM_Data_1_0709 där det mesta om Google Earth finns beskrivet med presentationer, videos och ett programarkiv.

En script lösning via Google Maps API eller en programvara som i uppgift 6.2 är också en möjlighet för dig att lösa uppgiften.

En mycket enkel lösning är att tillverka en KML fil och öppna den med Google Earth. Du kan prova med denna KML fil: http://users.du.se/~hjo/cs/dt2016/GIS/lecture-cellid.kml

Sedan Januari 2015 är Google Earth Pro gratis (licensen kostade $400 per år tidigare):
http://google-latlong.blogspot.se/2015/01/google-earth-pro-is-now-free.html

Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE

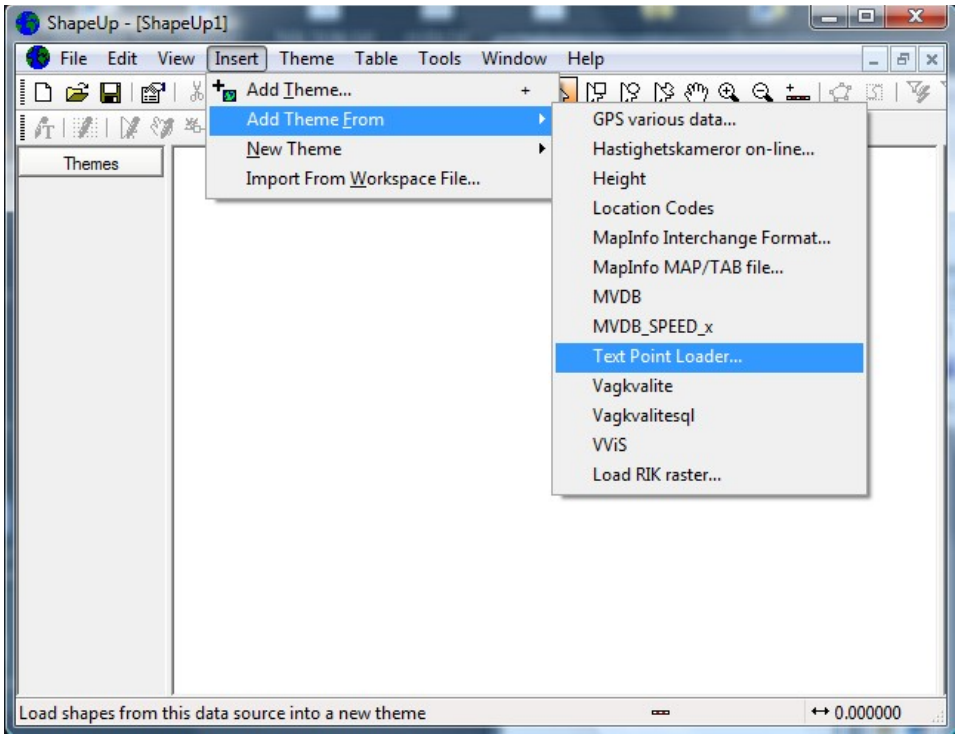
Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/

Vill man lära sig liter mer om GIS är MIT:s Geographic Information Systems Laboratory en excellent resurs: http://libguides.mit.edu/gis/.

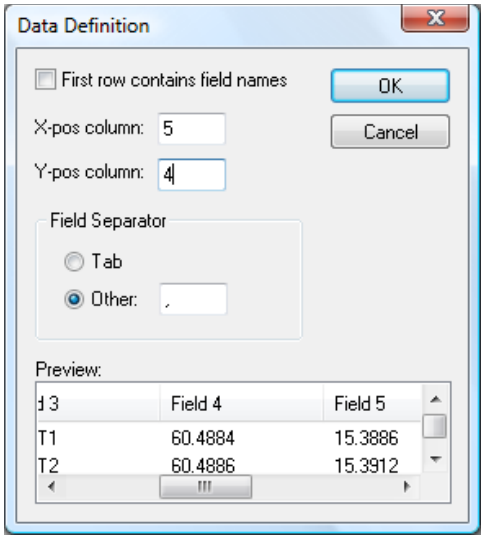
ShapeUp

How-to view a position log file in external GIS (Geographical Information System) program. You may use the log file your mobile phone have generated in the Simple Tracker program from embedded forensics.

With the ShapeUp GIS program you can easily import your position file and view it in this tool with other GIS files as for example shape files. View the following simple instructions.



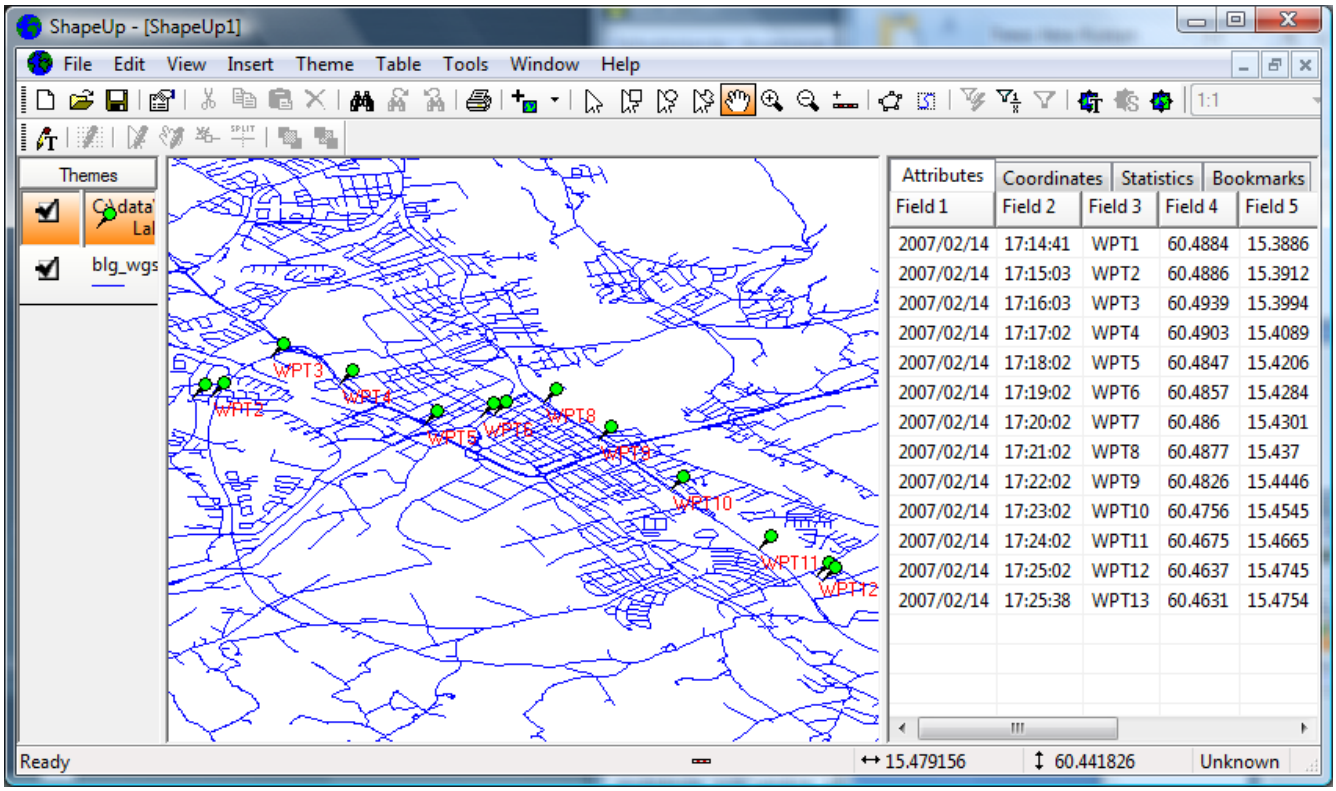
To add a CSV waypoint file with lat, long values etc. use the Text Point Loader...



Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE

Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/

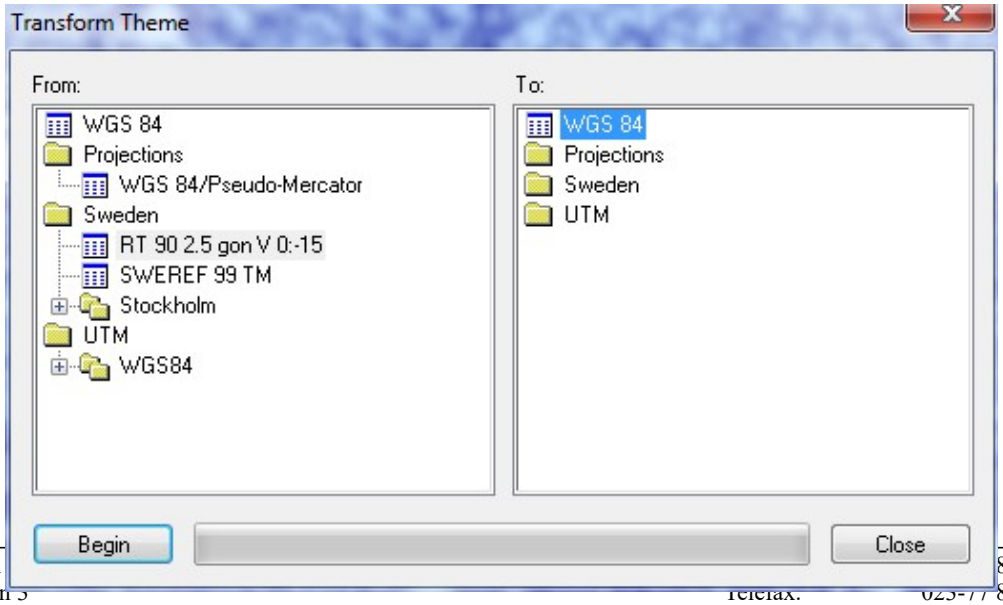
Select Long as X and Lat as Y and the correct field separator. When finished the waypoint file will be available as a theme in the left hand list of Themes.



Here I also have added a shape file (back ground map) with a road network and configured the loaded theme from previous step (right click the theme and press Properties) to show WPTx push pins.

There are some spatial background road network maps available at: http://users.du.se/~hjo/cs/dt2016/GIS/shape/. Shape files are added with Insert > Add theme.

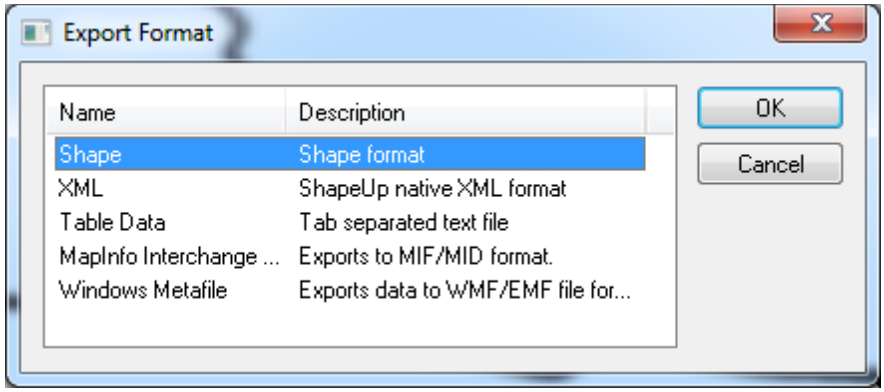
To make a theme editable right click and press Enable Editing. When you have done that you can transform the theme to some other format. For example can you transform a RT 90 road link network to WGS 84 by choosing Theme > Transform from the menu.



Högskolan
Röda vägen 3
781 88 BORLÄNGE
80 00
80 50
URL: http://www.du.se/

With Shapeup you can do a lot of other intelligent things with your GIS data…

If you have loaded data from text and want to export the data to shape format use Theme > Export on the menu.



6.6 Voluntary task 1 – WLAN geolocation

Report:

a) Find out the geographic location of the given BSSID/MAC addresses. It is said that the suspect begun his trip in USA and then traveled to Borlänge, Sweden where the crime took place. He then escaped to a secret hideout that we do not know where it is yet.

b) We need to know the color of the secret hideout house and how many bicycles that is parked outside the house.

Wi-Fi equipment connections can also be located much in the same manner as cell id but with much higher accuracy. Check out Harlan Carveys article "Where was Waldo?" at his blog: http://windowsir.blogspot.com/2009/09/where-was-waldo.html

Using one of the Perl scripts ssid.pl for XP or networklist.pl for Vista and above systems you have extracted some WAP (Wireless Access Points) MAC addresses from a registry hive of a suspects laptop according to below.

WAP1-MAC: 00:19:07:5B:36:92
WAP2-MAC: 00:24:b2:d8:52:45
WAP3-MAC: 00:24:b2:d8:52:42

We can locate the WLAN-router using Backtrack 5R3 or Kali Linux. You can use the VMware version of Backtrack.
Open Application > Backtrack > Exploitation Tools > Wireless Exploitation Tools > WLAN Exploitation > Fern-Wifi-Cracker.
Select the ToolBox Option and then select the Geolocatry Locator.
Now enter the BSSID/MAC-address that you want to geolocate and click on the Track button.

Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE

Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/

Note that this may not work (it did summer 2013). Most of the services/API:s including the Google Maps Geolocation API have made this a business paid solution for developers. Link: https://www.fern-pro.com/

6.7 Voluntary task 2 – Simple map web service for mobile phones

Report:

Attach a link to the website where the solution execute and hand in the source code.

We are going to do the server part of a solution that is very similar to this one: *"Share your geographical location with friends, family and colleagues. Position is sent by SMS, and receiver will see your exact location presented on a map on their phone. You as a sender need a GPS, either built in or a Bluetooth GPS. Receiver does not need anything else than a regular cell phone to view your location."*
More information is found at: http://www.posit.me

Required skills for constructing a web service of this type are actually surprisingly little. Knowledge about HTML and PHP basics, Google Maps static API with an API key and a web server with PHP is all you need.

We are going to construct a simple REST (http://en.wikipedia.org/wiki/REST) service that acts as a proxy between a mobile phone and Google maps. This is because the Google (developer) API keys (usually) only works on a defined DNS address as http://users.du.se/~hjo/.
REST is a simple way of implementing one of the buzzwords in computer land the last years, SOA (Service-oriented architecture, http://en.wikipedia.org/wiki/Service-Oriented_Architecture).

Task
You can take a look on my web service at: http://users.du.se/~hjo/lbs/gmap/ and the gmap1.php file. Read the instructions on the page for testing the different properties of the Google static API. The gmap1.php and staticgmap.php source code is downloadable from the above WWW-address as 7zip archives.

The purpose with the web service is to make it a part of our Android SMS position solution. The clients are simple mobile phones with only a web browser.

What you are going to implement in this part of the lab is the gmap2.php script which is suitable for the receiving (user B) mobile phones web browser. You can use the gmap1.php script as a base for your solution.

Further information
The content of the sent SMS with for example users A:s position can look like this:
Hi there I'm now positioned at: http://users.du.se/~hjo/lbs/gmap/gmap2.php?location=&lat=60.48860&lng=15.38820&zoom=8
or

Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE
Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/

Hi there I'm now positioned at the red marker but I'm going to be in Gagnef in a while:
http://users.du.se/~hjo/lbs/gmap/gmap2.php?location=&lat=60.48860&lng=15.38820&zoom=8&markers=gagnef
You can simulate the user A:s cell phone software by just typing in the SMS by hand and send it to user B:s mobile phone or just try the URL above in your favorite web browser.

When user B:s cell phone receives the SMS message and press the web link in the message, the cell phones built in web browser starts and display the map. Other possible applications are for example surveillance alarms for kids, wild animals and expensive items as boats, cars etc. (electronic fencing). This implies that the sending part (user A) is a rugged GPS tag with SMS function and long battery life.

Remember that there may be a limit for some mobile phones and operators regarding larger content (concatenated SMS, multipart or segmented SMS or "long SMS"). Ideally you keep the size below the GSM 7-bit default alphabet of 160 chars (web service parameter strings could for example be shorter in our case).

Tip! You are probably going to have a problem maintaining the web browsers state when zooming in and out in the map image. There are three ways to fix this, either use session variables, cookies or hidden form parameters.
Sometimes the mobile browser does not support cookies just as they don't support java script.

A simple PHP script to test if your web server support session variables is the following PHP source code (put the code in a file as sessiontest.php on your web server):

```
<?php
session_start();
if(!isset($_SESSION["kaka"])) {
      $_SESSION["kaka"] = "Det &Auml;r gott med kakor!";
}
else {
      $_SESSION["kaka"] .= "!";
}
echo $_SESSION["kaka"];
?>
```

Note! You may need to give your session variable a unique name on your web server (du.se) as for example "<user name>_kaka" to avoid collisions of active session variables.

Web resources:

Static Maps Developer Guide
https://developers.google.com/maps/documentation/staticmaps/

HTML
http://www.w3schools.com/html/

PHP
http://www.w3schools.com/php/
or search on: "php skola" in Google.

Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE

Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/

The base for this lab comes from some Google Static Maps PHP classes a kind blogger already have made. I however modified them a bit to suit my needs. He called the solution "wrapper for Google static map API" and it is found here:
http://hasin.me/2008/10/31/wrapper-for-google-static-map-api/

6.8 Voluntary task 3 – Become familiar with professional GIS systems

I denna uppgift skall vi bekanta oss med kraftfulla databas och GIS lösningar som är gratis. Det vi skall gå igenom är en FOSS4G http://foss4g.org/ workshop som genomfördes på FOSS4G 2007 http://wiki.osgeo.org/wiki/FOSS4G2007.
Tidsmässigt ska det gå åt max: 3h att genomföra momentet. Efter det skall du ha en ganska bra uppfattning om vad som kan åstadkommas med kartdata, spatsiellt enablade databaser och en GIS data viewer.

Området är intressant eftersom det mesta numera kan positioneras i realtid med hög precision. Det finns också många webbaserade lösningar som har just denna teknik i botten för att kunna hämta och visa efterfrågad positionssatt data och t.ex. rutter mm. mycket snabbt.

Workshopen har jag sparat här: http://users.du.se/~hjo/cs/dt2016/GIS/extra-task/ och heter "W-04: Introduction to PostGIS". Om du vill kan du även kika lite på "W-02: Shuffling Quantum GIS into the Open Source GIS Stack".

Jag har lagt äldre versioner av de program som behövs på samma ställe plus lite andra filer att testa med om intresse finns. Workshopen går att köra på andra OS (GNU/Linux och Mac OS X tror jag) men då får ni själva ladda ner dessa versioner av programmen.

Vill du veta lite mer allmänt om databaser, PostgreSQL och PostGIS så kolla in presentationen PostGIS.ppt innan du börjar.

Öppna dokumentet postgis_workshop\PostGIS Workshop.doc och följ anvisningarna i detta dokument. Du bör följa med i PostGIS Workshop.ppt presentationen samtidigt för att se skärmdumpar och få förklaringar på tekniska moment etc.

Den CDROM som nämns i workshopen behövs inte utan allt material finns på respektive programvaras webbplats eller under GIS foldern. Dvs:

- PostgreSQL – postgresql-8.3.6-1-windows.exe
- PostGIS – postgis-pg83-setup-1.3.5-1.exe
- Quantum GIS – installeras med osgeo4w-setup.exe
- PgAdmin – pgadmin3-1.8.4

För att visa GIS data rekommenderar jag Quantum GIS eftersom den är skriven i native språk.

Du behöver inte genomföra övningarna från och med rubrik 5 och senare (Mapserver) i workshopen.

Om det inte fungerar med de nyare versioner av programvarorna får du backa till de versioner som finns under GIS foldern.

Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE
Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/

Redovisning:

- Jag vill se en identifierbar (att det är du) skärmdump ifrån din GIS data viewer när du laddat in den GIS data ifrån PostgreSQL/PostGIS databasen som hör till workshopen.
- Vilket latitud har det sjukhus som ligger längst norrut i provinsen (bc_hospitals)?

Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE

Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/