

# CSI: Cyber

Truth or Fiction? Or somewhere in between?

# Fair Use Disclaimer

The views and opinions expressed in this presentation are those of the speaker.

There may be content in this presentation that contains copyrighted material and the speaker does not claim any right over them.

All the images and graphics used in the video belong to their respective copyright holder.

Copyright Disclaimer under section 107 of the Copyright Act of 1976, allowance is made for “fair use” for purposes such as criticism, comment, news reporting, teaching, scholarship, education and research. Fair use is a use permitted by copyright statute that might otherwise be infringing.

This presentation is for entertainment purposes only.

# Agenda

- Who am I?
- CSI Cyber: Background and Cast
- Storyline: OPM Hack
- Wrap it up

# Intro

Rebecca Ford

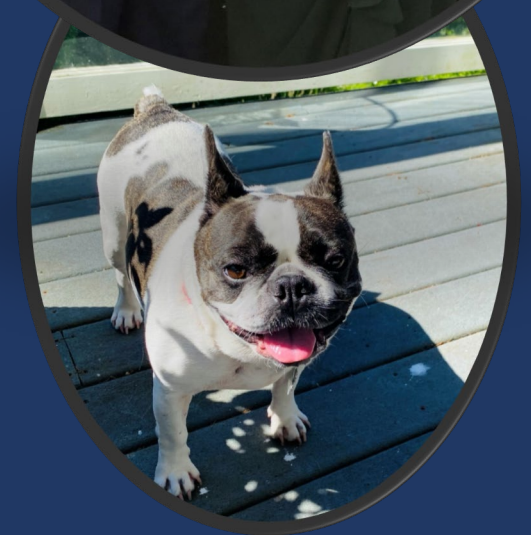
Cyber Threat Intelligence analyst

Former Department of Defense contractor

North Korea Cyber SME

Mentor transitioning veterans AND spouses

Twitter: @cybersquarepeg



QUESTIONS



# Cast of Characters



Brody  
"BowWow"  
Nelson

Daniel  
Krumitz

DB Russell

Dr. Avery Ryan  
Deputy Director, FBI

Elijah Mundo

Raven  
Ramirez



# Storyline: OPM Hack

- April 2015
- Affected 21.5 million Americans
- SF-86 records
- Attributed to Chinese nation-state actors

Standard Form 86 (EG)  
Revised September 1995  
U.S. Office of Personnel Management  
5 CFR Parts 731, 732, and 736

QUESTIONNAIRE FOR  
NATIONAL SECURITY POSITIONS

Form approved:  
OMB No. 3208-0007  
NSN 7540-00-834-4036  
86-111

Investigating Agency Use Only Codes Case Number

**Part 1** Agency Use Only (Complete items A through P using instructions provided by the investigating agency.)

**A** Type of Investigation  
**B** Extra Coverage  
**C** Sensitivity Level  
**D** Access  
**E** Nature of Action  
**F** Date of Action  
Month Day Year

**G** Geographic Location  
**H** Position Code  
**I** Position Title

**J** Location of Official Personnel Folder  
None  
NIPAC  
At SON  
Other Address  
ZIP Code

**L** Location of Security Folder  
None  
NIP  
Other Address  
ZIP Code

**N** OPAC-ALC Number  
**O** Accounting Data and/or Agency Case Number

**P** Requesting Official Name and Title Signature Telephone Number Date

Persons completing this form should begin with the questions below.

**1** FULL NAME \*If you have only initials in your name, use them and state (IO). \*If you are a "Jr.," "Sr.," "II," etc., enter this in the box after your middle name. \*If you have no middle name, enter "NMN".

**2** DATE OF BIRTH Month Day Year

**3** PLACE OF BIRTH - Use the two letter code for the State. City County State Country (if not in the United States)

**4** SOCIAL SECURITY

**5** OTHER NAMES USED Give other names you used and the period of time you used them (for example: your maiden name, name(s) by a former marriage, former name(s), alias(es), or nicknames(s)). If the other name is your maiden name, put "nee" in front of it.

**#1** Name Month/Year To Month/Year  
**#2** Name Month/Year To Month/Year  
**#3** Name Month/Year To Month/Year  
**#4** Name Month/Year To Month/Year

**6** OTHER IDENTIFYING INFORMATION Height (feet and inches) Weight (pounds) Hair Color Eye Color Sex (Mark one box)  
Male Female

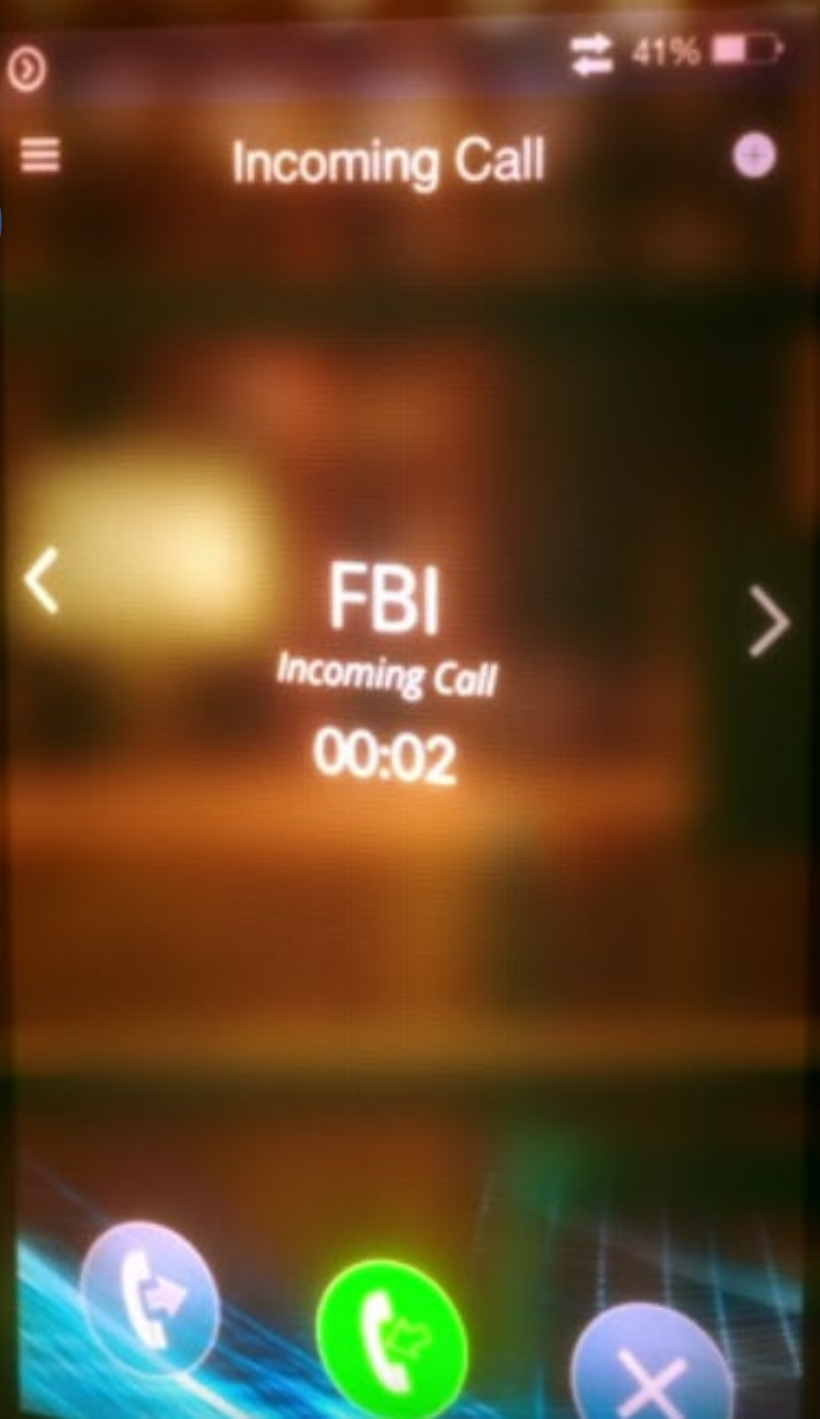
**7** TELEPHONE NUMBERS Work (include Area Code and extension) Home (include Area Code)  
Day Night Day Night

**8** CITIZENSHIP I am a U.S. citizen or national by birth in the U.S. or U.S. territory/possession. (Answer items b and d)  
I am a U.S. citizen, but I was NOT born in the U.S. (Answer items b, c and d)  
I am not a U.S. citizen. (Answer items b and e)

**9** UNITED STATES CITIZENSHIP If you are a U.S. citizen, but were not born in the U.S., provide information about one or more of the following proofs of your citizenship.  
Naturalization Certificate (Where were you naturalized?)  
Court City State Certificate Number Month/Day/Year Issued  
Citizenship Certificate (Where was the certificate issued?)  
City State Certificate Number Month/Day/Year Issued



Someone must have hacked the gov't servers









## Knowns

Someone has SF-86 forms

Communication via email

## Unknowns

Who?

Motivations?

What devices were used?

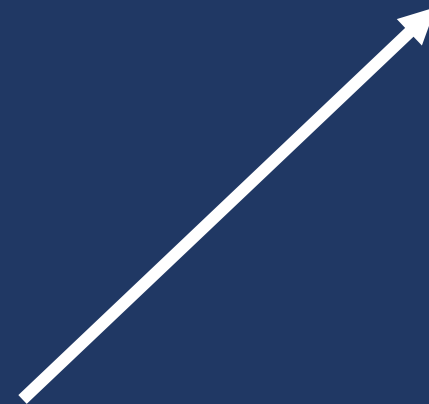
Point of intrusion?

### Action Items:

✓ Disconnect from the OPM network

✓ Hunt down the perp

✓ Start patching the vulnerability 





We are going back a few months monitoring "chatter" from the big 4 countries  
~\(\ツ)\\_/~



If we find out that a foreign adversary is involved, Congress will consider their actions an act of war. ~\(\ツ)\\_/~



A close-up shot of a man with a serious, questioning expression. He is wearing a dark suit jacket, a light-colored dress shirt, and a purple tie. A speech bubble is superimposed on the left side of the frame, containing text. The background is a blurred indoor setting with warm lighting.

“This is Snowden  
all over again.”

-uh, no.



“DHS is ready to help”

“Director, we got this”





**EXTRACTING CELLULAR HARD DRIVE**

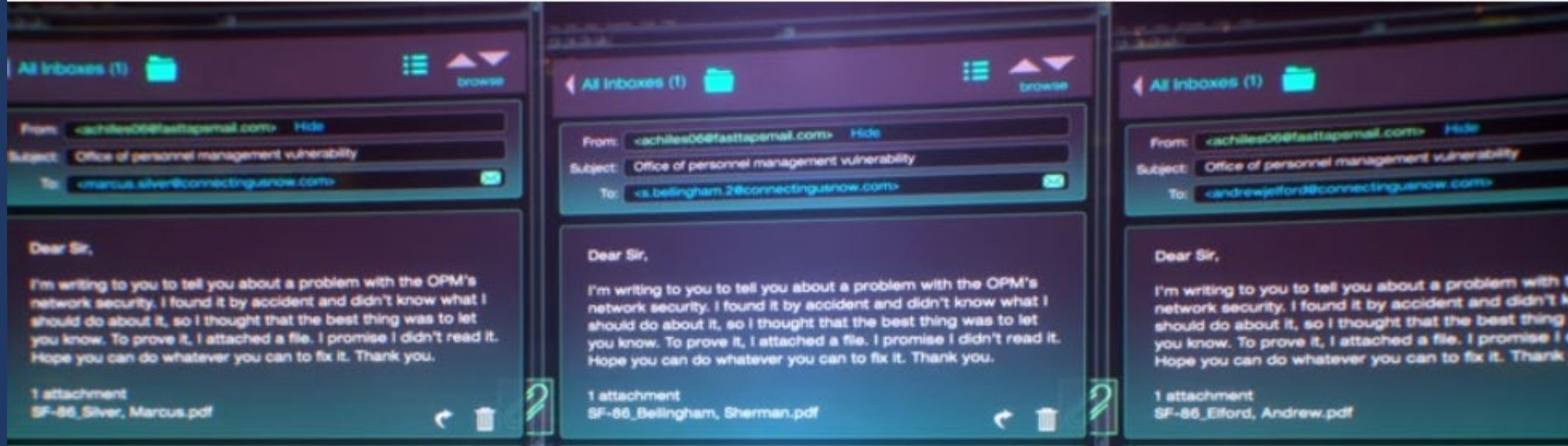
Size: 13.54 GB  
Contains: 9432 Files

Status: **CONNECTED**  
Extraction: All files extracted

**CONNECTED: TRANSFERRING ALL DATA**

**DOWNLOAD COMPLETE**

HARD DRIVE ID# 19838-302998	CPU ID# S298X8729-9398-000183
COM PORTS DISABLED	34D21 - 43F49 MEMORY RANGE BU



**Sender:** achilles06@fasttapemail.com  
**To:** each person domains: @connectingusnow.com, @colossalinks.net  
**Subject:** Office of Personnel Management  
**Attachment:** Each got a copy of their own SF-86

@connectingusnow.com -> redirects to -> paramount.com





Get the name and address from the ISP

The hack is NOT sophisticated, but good enough to evade IDS  
~\(\ツ)/~

```
COMCIS23.fasttapsmail.com
IP TRACE RESULTS:
IP Address: 139.51.267.181
Internet Service Provider: CABLEFIRE COMMUNICATIONS
Email Address: HAZELTON517@CONNECTINGUSNOW.COM
Name: ROBERT HAZELTON
Account Number: 8558300420379030
Services: INTERNET, PREMIUM TV
Billing Address: 3098 HARDY AVENUE, ARLINGTON, VA 22210
Contact Number: (703) 555-0194
m. [139.51.267.181]]
Received: from BAY1605-W21 ([139.51.267.181]) by BAY2285-
COMCIS23.fasttapsmail.com over TLS secured channel with Fast Taps Mail
SMTPSVC(7.5.7601.23008)
```



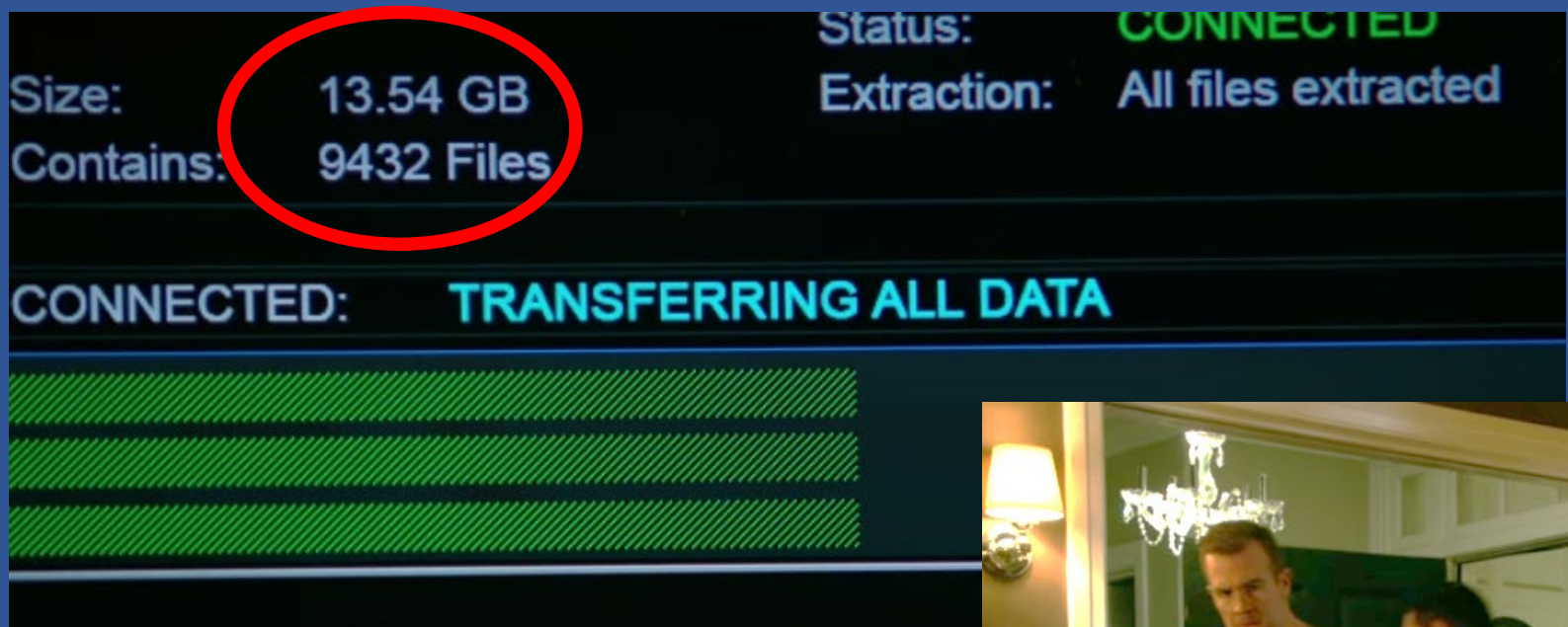
S  
W  
A  
T



#GotSearchWarrant?







How long would it really take?

13.54 GB data

Download speed: 1 Gbps

1 hr. 44 min.

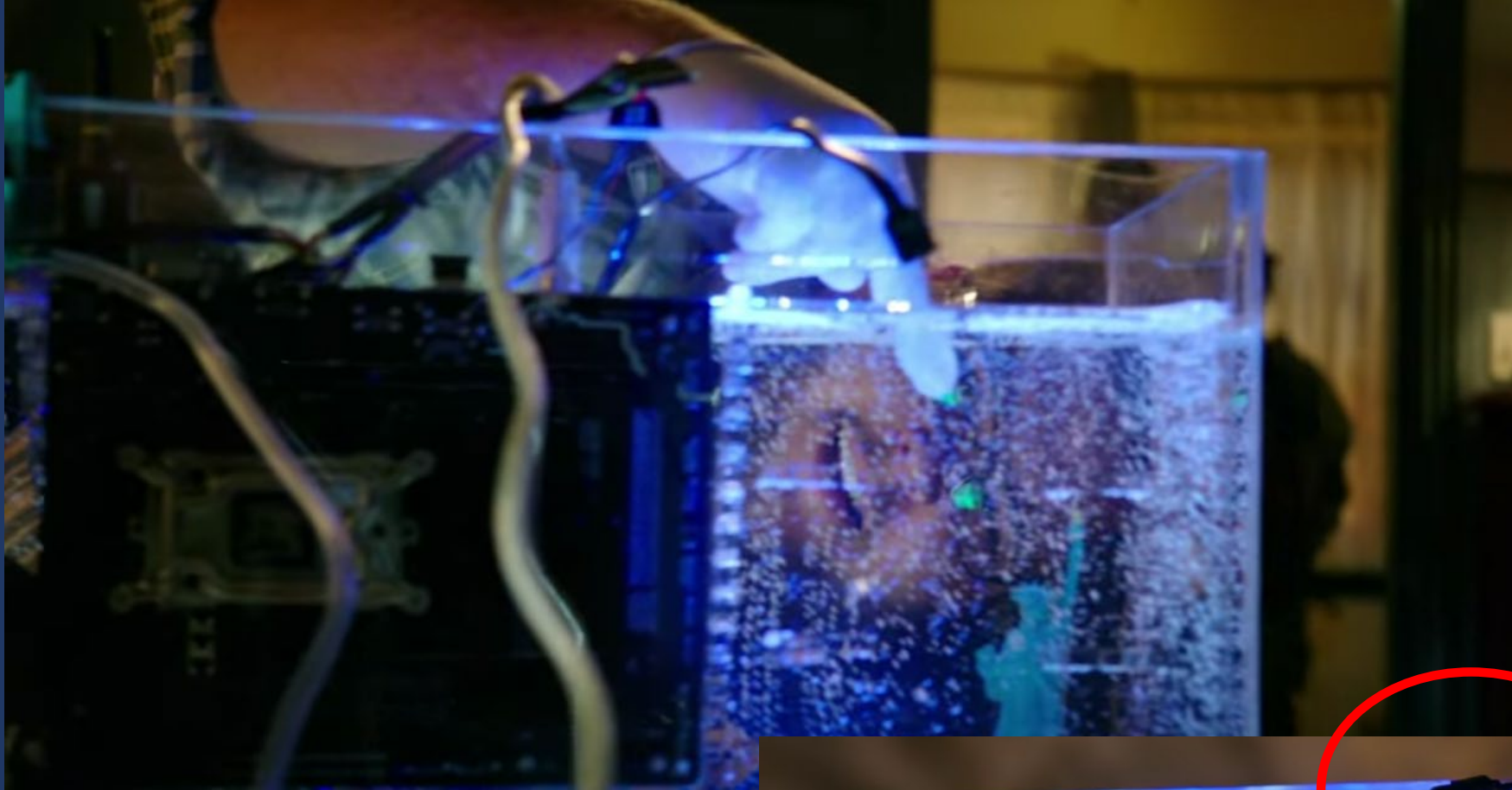


# Jake (aka Achilles) meets Wizard



Echo





JAKE IS THE HACKER!!!!!!!!!!





FEDERAL BUREAU OF INVESTIGATION  
CYBER CRIME DIVISION  
DEVICES CONNECTED TO ROUTER

SSID: **HAZELTON HOME**    EXTERNAL IP: **139.51.267.181**

DEVICE NAME	INTERFACE	MAC ADDRESS	IP ADDRESS
BLU-RAY PLAYER	WIRELESS	C1-40-EE-1A-4W-47	192.168.271.190
CENTRAL HEATING UNIT	WIRELESS	85-95-F3-B8-BJ-63	192.168.271.123
HOME SPEAKER SYSTEM	WIRELESS	E3-03-6F-E4-EP-34	192.168.271.110
EMMA'S MP3 PLAYER	WIRELESS	FE-A3-F8-86-7M-B5	192.168.271.189
JAKE'S DESKTOP	ETHERNET	74-88-24-B3-2B-6F	192.168.271.142
JBC	WIRELESS	3E-03-6F-E4-EP-34	192.168.271.173
MARGO'S CELL PHONE	WIRELESS	21-E9-27-A1-EW-19	192.168.271.159
MARGO'S TABLET	WIRELESS	D7-E1-AE-8F-0W-4C	192.168.271.118
P-TECH ALARM SYSTEM	ETHERNET	8C-57-AC-1F-9W-5C	192.168.271.134
ROBERT'S LAPTOP	WIRELESS	4E-43-3E-45-TV-04	192.168.271.166



SSID: HAZELTON HOME

EXTERNAL IP: 1

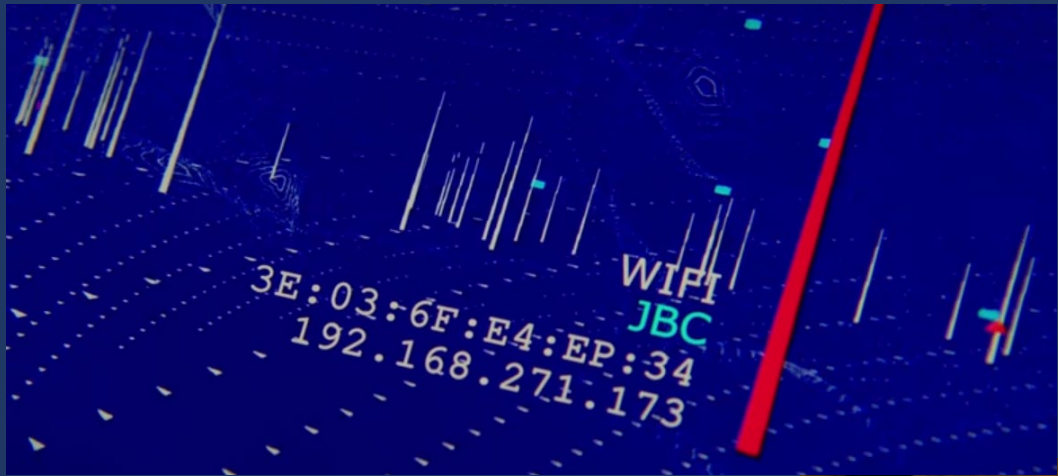
DEVICE NAME

INTERFACE

MAC ADDRESS

DEVICE NAME	INTERFACE	MAC ADDRESS
BLU-RAY PLAYER	WIRELESS	C1:40:EE:1A:4W:
CENTRAL HEATING UNIT	WIRELESS	85:95:F3:88:8.
HOME SPEAKER SYSTEM	WIRELESS	E3:03:6F:E4:EP:
EMMA'S MP3 PLAYER	WIRELESS	FE:A3:F6:86:7M:
JAKE'S DESKTOP	ETHERNET	74:8B:24:83:2B:8
JBC	WIRELESS	3E:03:6F:E4:EP:3
MARGO'S CELL PHONE	WIRELESS	21:E9:27:A1:EW:19
MARGO'S TABLET	WIRELESS	07:E1:AE:BI:DW:4C
P-TECH ALARM SYSTEM	WIRELESS	8C:57:1C:IF:9W:5C
ROBERT'S LAPTOP	ETHERNET	4E:43:3E:45:7V:D4
ROBERT'S CELL PHONE	WIRELESS	8B:31:43:55:55:00
SMART TV	WIRELESS	
WIRELESS PRINTER	WIRELESS	





We can use an app that makes wireless signals visible





Found it!







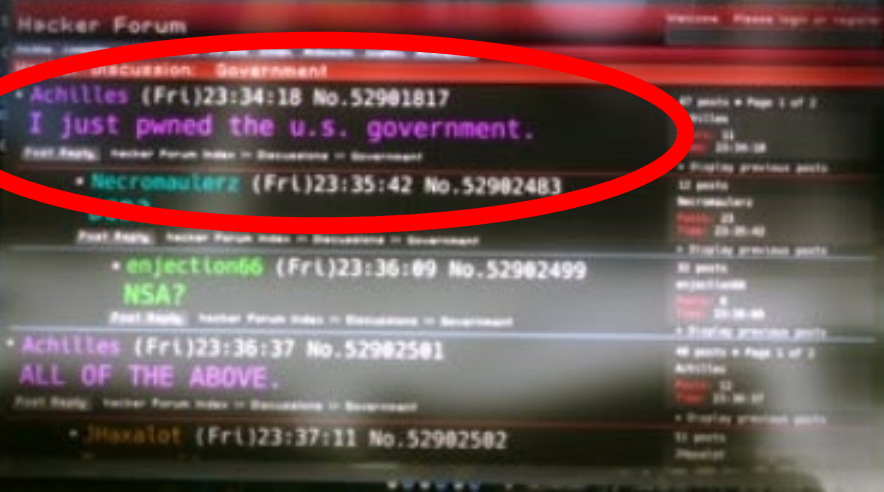
DHS Director

This happened on your watch, and you are responsible for this breach!!!



Protection measures were denied due to your budget restrictions

Check out  
this hacker forum.



I'm on the OPM website.  
The vulnerability has been  
patched.





Jake must have patched the vuln **AFTER** he sent the emails



I got a tip:  
Wizard



A man with short dark hair, wearing a grey hoodie, is looking down at a computer screen. The screen displays a forum post in a monospaced font. A white speech bubble with a black outline points to the screen, containing the text "Found him!". The background is dark and out of focus.

Found him!

r15k.  
Post Reply hacker Forum Index >> Discussions >> Government

- Wizard715 (Sat)23:45:17 No. 4290  
You're getting lots of  
attention.  
Let's take this  
conversation offline.

Post Reply hacker Forum Index >> Discussions >> Government



## legacy footprints -

A digital data trail you unintentionally  
leave online.

wizard715@fastappsmail.com

Phone#

Got a location on the cellphone



Meanwhile, back at the gym



Jake hands over the hard drive to Wizard -  
they are going to turn it in

Echo has other plans: sell the hard drive





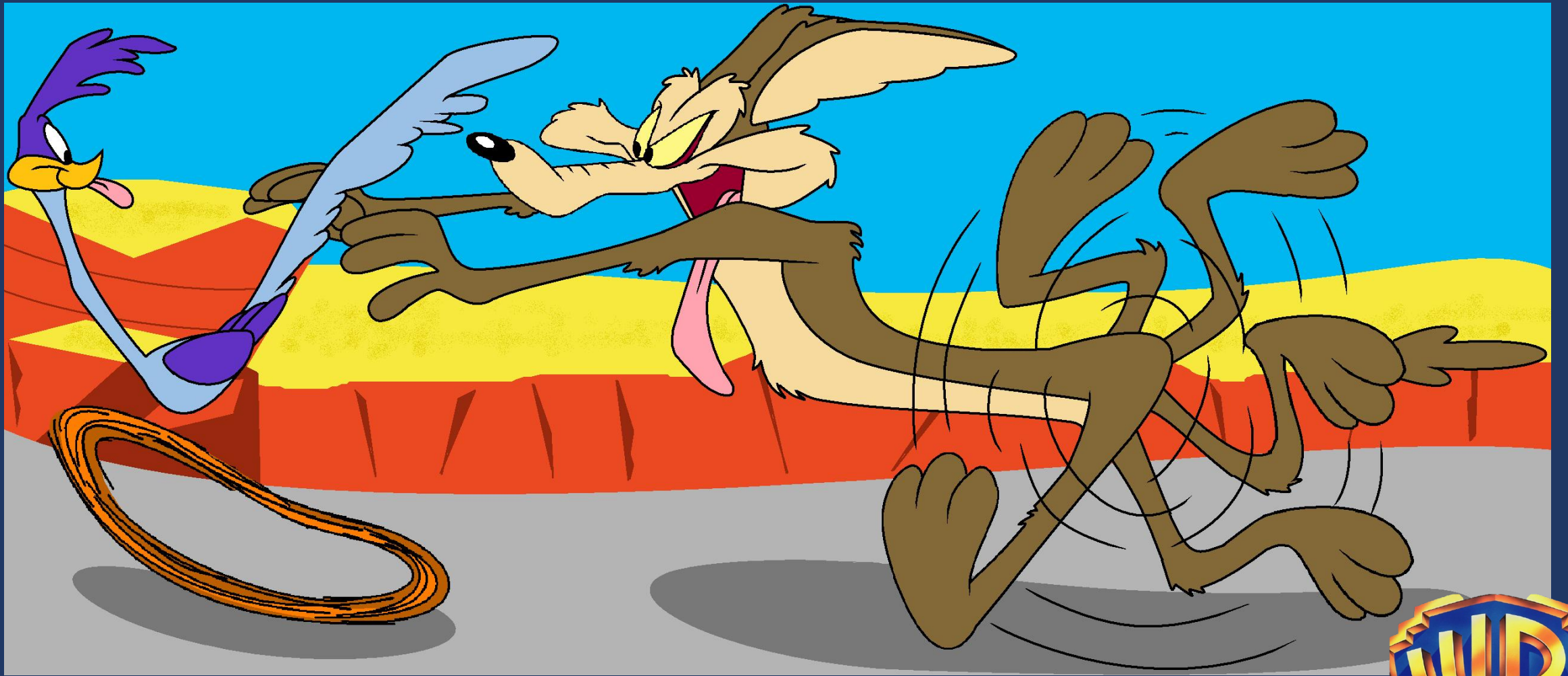


S  
W  
A  
T











Somebody brokered a deal to sell the OPM documents to Russia

Hullo... this is Vlad



On the Run



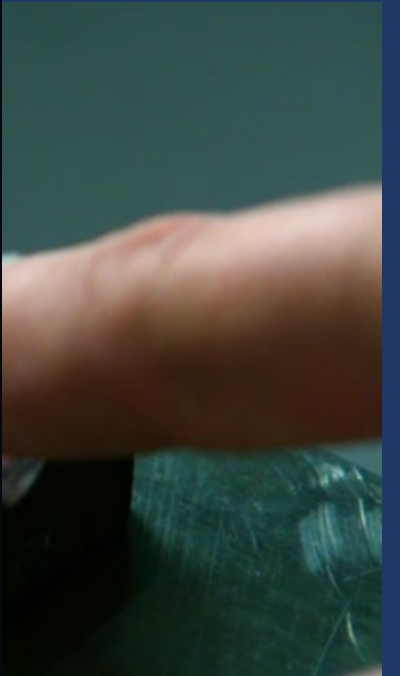
On the Run



R.I.P.







## Wizard's Laptop -

- Print must mat
- Human skin
- An active pulse



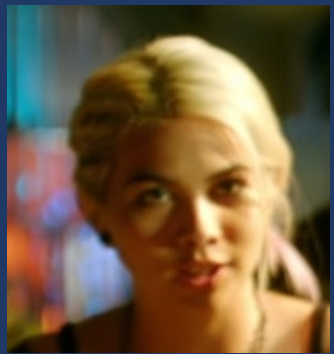




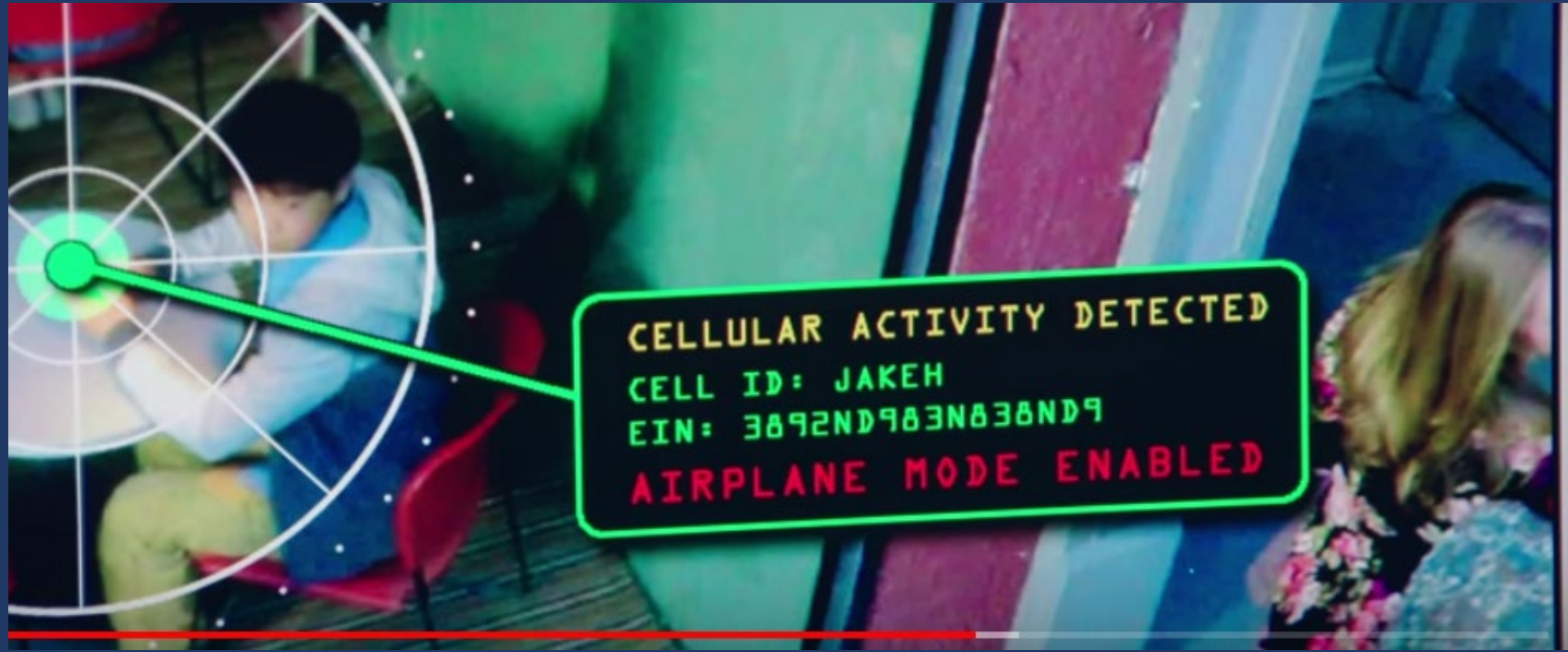
15:04:10

No!

...n in and  
...o he is  
...xting?

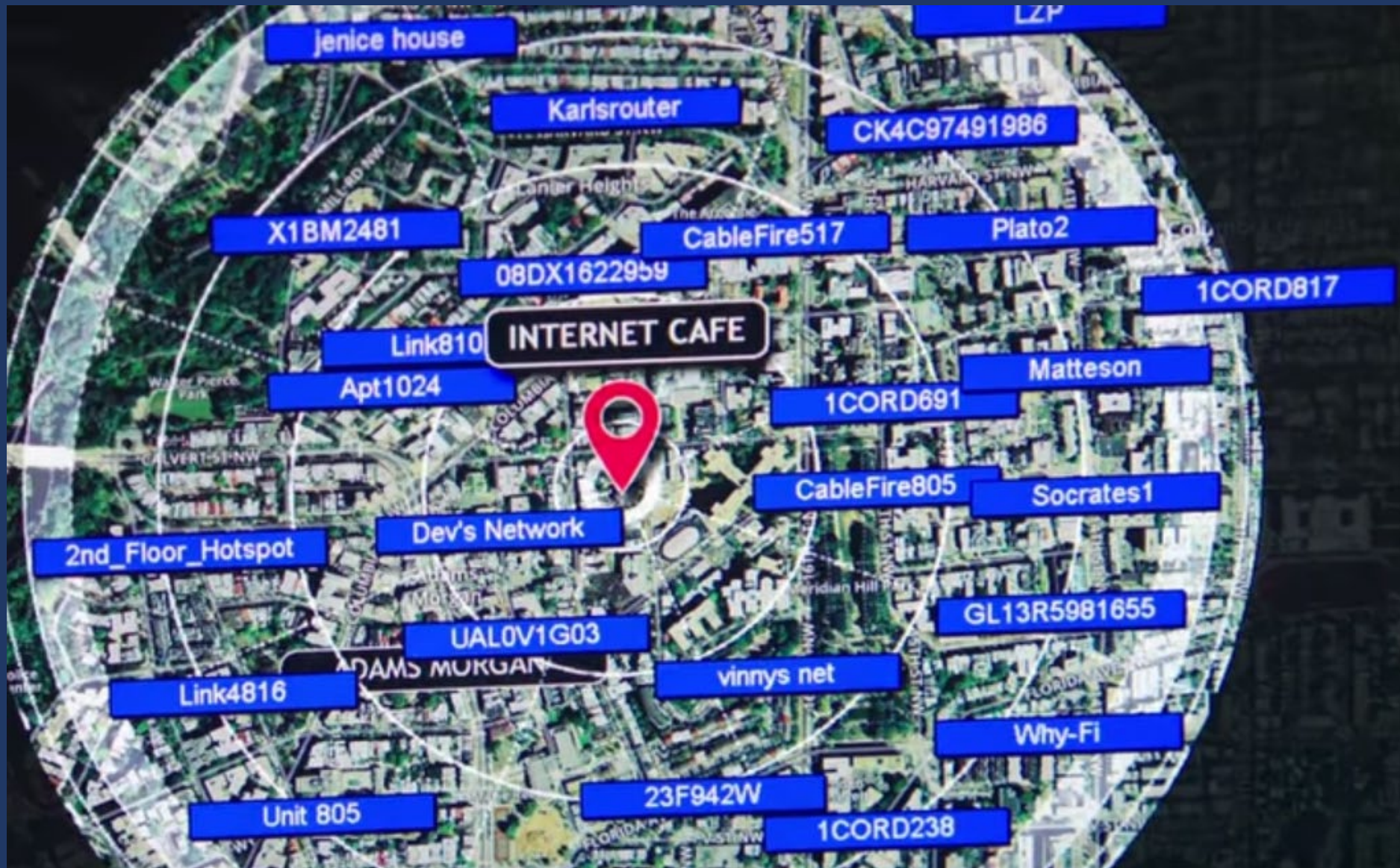






CELLULAR ACTIVITY DETECTED  
CELL ID: JAKEH  
EIN: 3892ND983N838ND9  
AIRPLANE MODE ENABLED









☰ Trusted Wifi Connections



Trusted Wifi



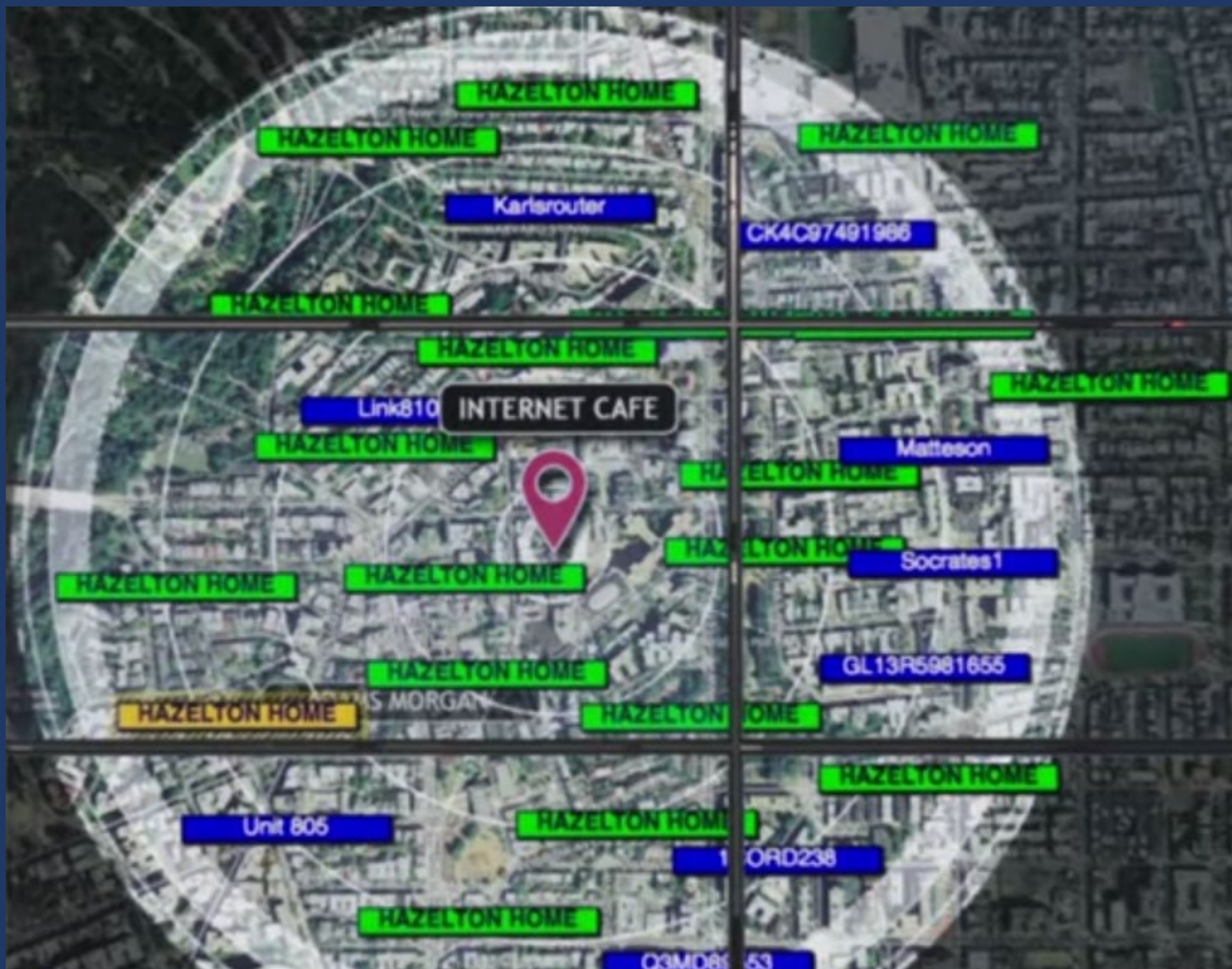
Hazleton Home





# Gone looking for Jake







MAP MAPPING SYSTEM



JAKE'S CELL

CONNECTION ESTABLISHED  
WIFI ROUTER: MEP SEC  
ID: "HAZELTON HOME"  
CELL ID: JAKEH  
EIN: 3892ND983N838ND9

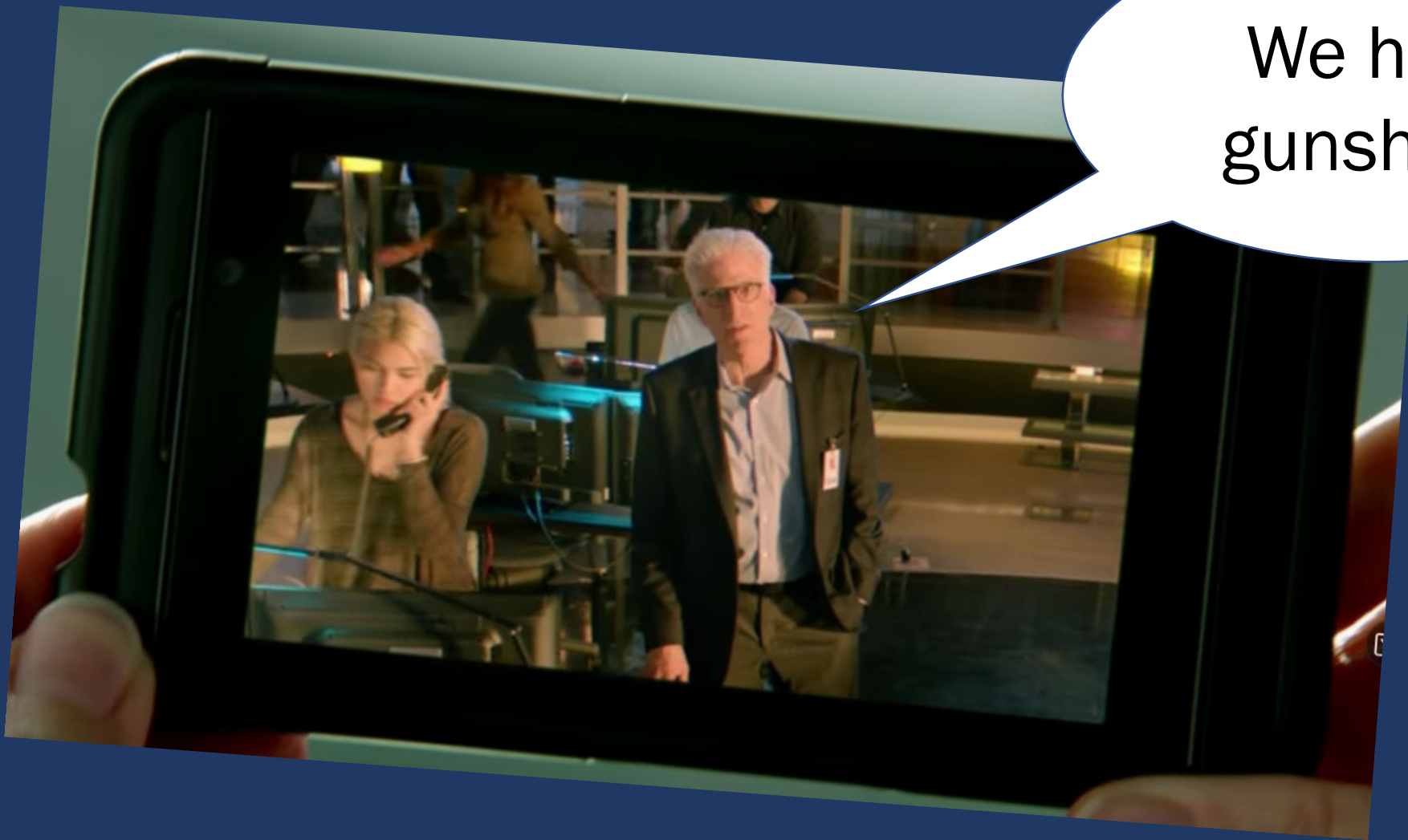




Jake this is the FBI –  
you aren't in any  
trouble – tell us where  
you are

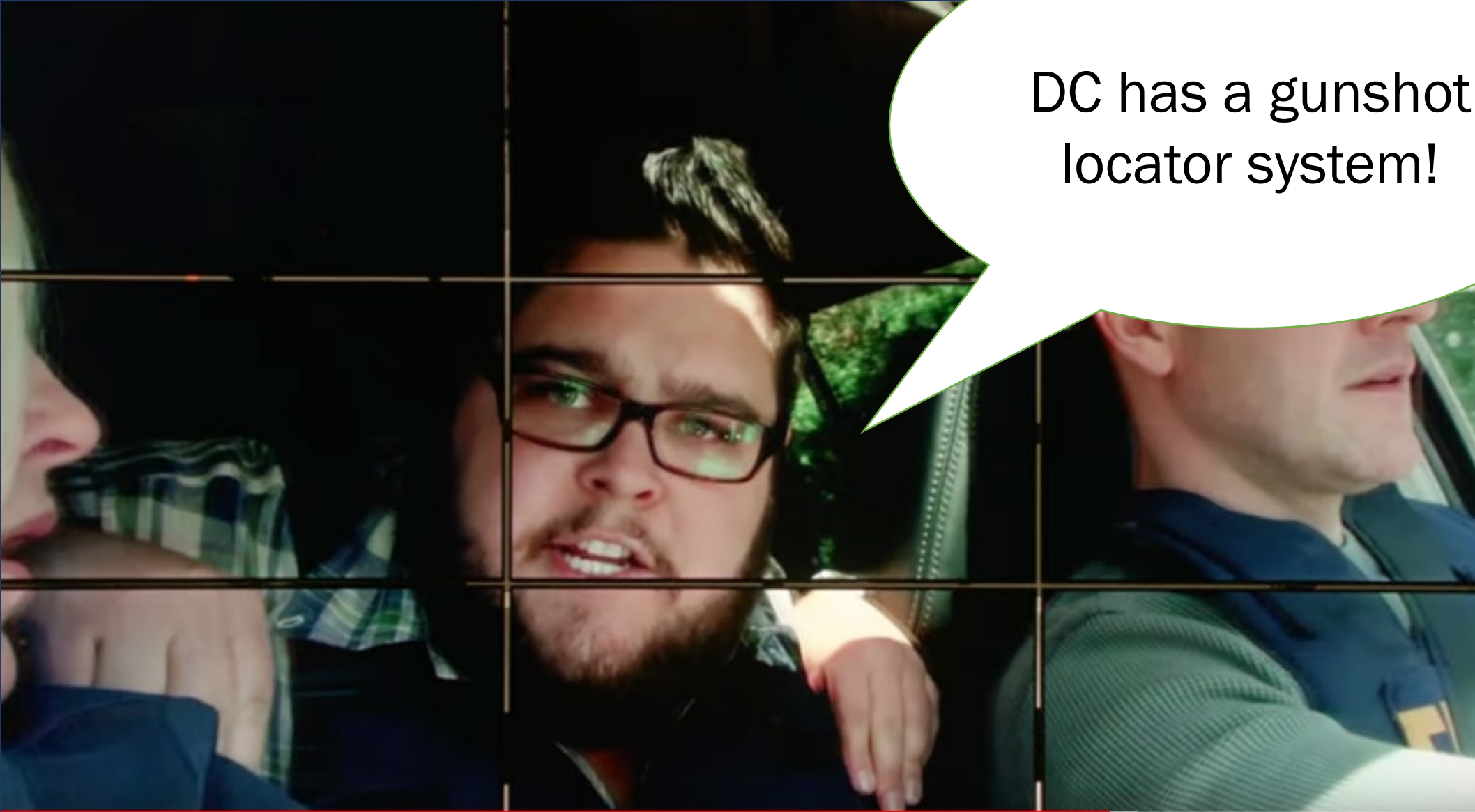






We hear  
gunshots!



A composite image featuring three men in a car. The man in the center is wearing glasses and has a beard. The man on the left is wearing a plaid shirt. The man on the right is wearing a blue shirt. A white speech bubble with a green border is overlaid on the right side of the image, containing the text "DC has a gunshot locator system!".

DC has a gunshot  
locator system!

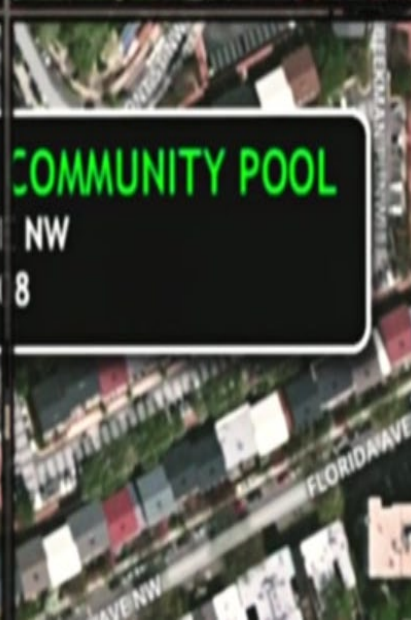
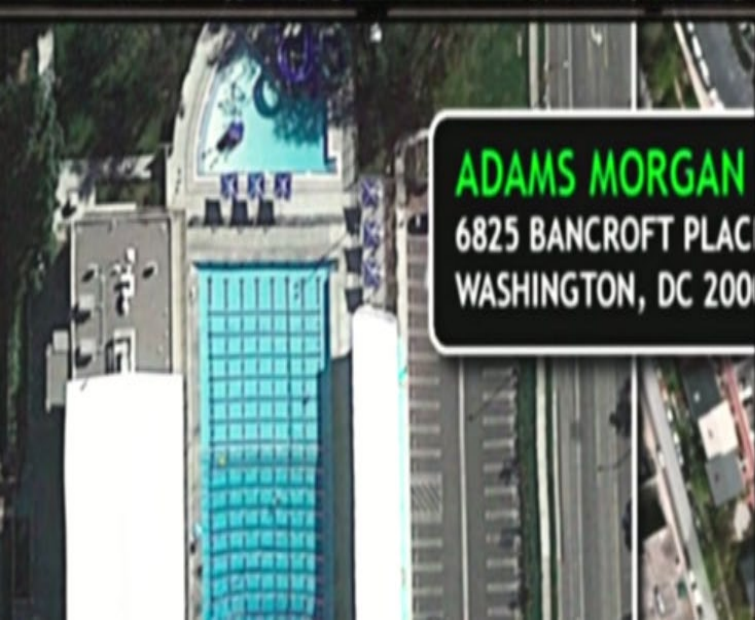


I need authorization  
to access the  
gunshot system



Hack it if you  
have to!





**ADAMS MORGAN COMMUNITY POOL**  
6825 BANCROFT PLACE NW  
WASHINGTON, DC 20008







S  
W  
A  
T



**BUSTED**

What happens  
to Jake?



He's covered under  
the Vulnerability  
Disclosure Program

-(ツ)-



# The Young Apprentice Program



## Requirements:

- Think outside the box
- Mad hacking skills
- Write code with your eyes closed

# Takeaways

- Humor
- This show is for everyone
- Realistic expectations
- Learned new technologies – (e.g. Wigle and ShotSpotter)
- Teamwork
- Redemption

Thank you.