

If you are participating in the SecureWorld CyberHunt app game, please be sure to scan the QR code for this session.



Don't forget to take the survey on the SecureWorld app. It will also be emailed to you at the conclusion of the conference.



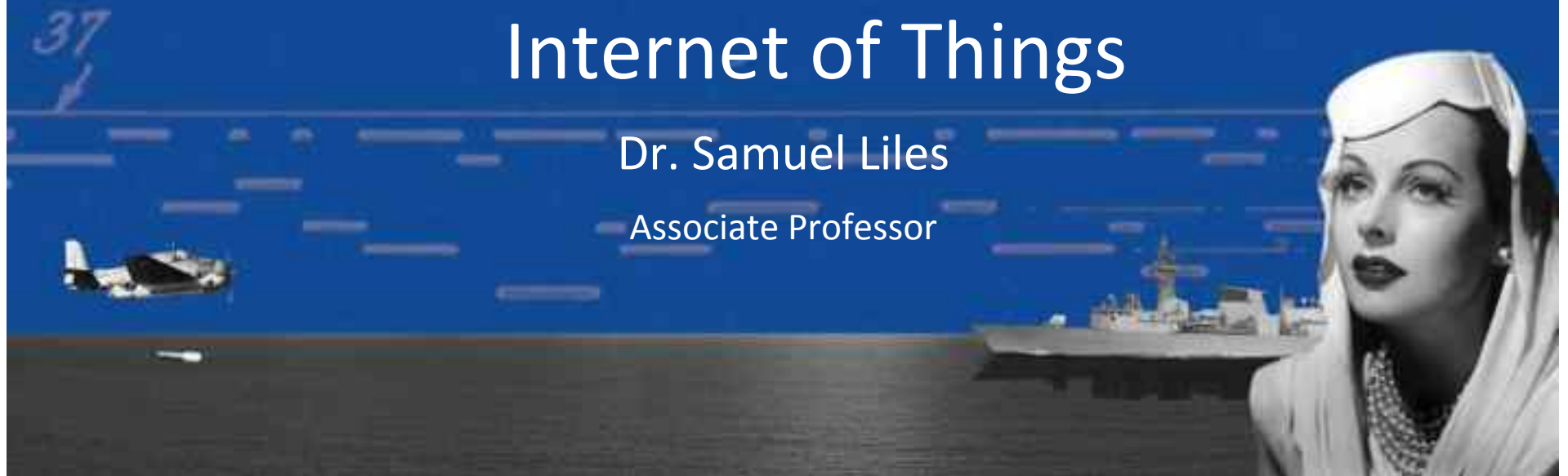
After this presentation, view the slides on the SecureWorld app.



# Digital forensics and the Internet of Things

Dr. Samuel Liles

Associate Professor



# Who am I?

- Nobody special, Nobody important
  - Purdue Professor and Dr. of DFIR
  - Non-traditional career track (Marine, Cop, IT/IR, Higher Ed, next?)
- Blog: <http://selil.com>
- Twitter: @selil
- Goal I just want to have a conversation



Slides located at <http://selil.com>



# Forensics

- Relating to or denoting the application of scientific methods and techniques to the legal process.
- The application of science to the finding of fact for use in a court of law or by the state to compel.
- My students and I do forensic analysis of stuff classified as the Internet of Things



Slides located at <http://selil.com>



# Technology

- **Technology**, the study of the art and craft of doing work with tools
- **Technologist**, a person who enhances the quality, efficiency, or capability of work through tools
- **Mission!** Study the art and craft of doing forensic analysis on the Internet of Things with better quality, efficiency, and enhance the capability of the forensic community

# Internet of Things

- The next big thing?
- Baloney?
- What was all that TCP/IP connected stuff called before IoT?
- The peeping Tom in your thermostat?

Dear Abby, my thermostat is asking a Chinese ZeusBot for relationship advice with my refrigerator. Should I intervene?



Slides located at <http://selil.com>



# Internet of Things

- RFID systems
- Sensors
- Actuators
- Devices
- Mobile phones
- Tablets
- Medical devices
- GPS devices
- Auto entertainment
- Auto driving assist or control systems
- Industrial Control Systems
- Autopilot collision avoidance systems
- Need not be a physical instantiation

```
=====UPDATE=====
> You have 15 pairs of underwear left.
  [Ok] [buy more underwear] [find help online]
> Your cat checked in at the litterbox.
> Your microwave just heated a lasagna.
> Record: You stared out the window for 23 minutes.
  [Ok] [post your score]
> Your couch likes your microwave's status update.
> It's raining again.
  [Ok]
> 15 of your things are broken.
> You haven't left the house in 5 days.
  [Ok]
=====
```

Source the Internet

# Controlling the edge


- Generally open architectures and connection types
- Sensors and actuators represent the real world connectivity via the digital domain
- Localized behaviors are globally connected
- Protocols are often “esoteric”



# ICS/DCS/BCS

- “You guys over in IT really don’t get industrial control systems.”
- MODBUS, DNP3, other ICS protocols are found in Wireshark, Metasploit and other “hacker” tools.
- Nessus and NMAP have detection rules
- “We found your SCADA system on the Internet” – xoxo Shodan

[Shodan](#)
[Exploits](#)
[Scanhub](#)
[Maps](#)
[Blog](#)
[Membership](#)



**SHODAN**

Services

Telnet	425
None	247
SNMP	177
BACnet	14
HTTP	12

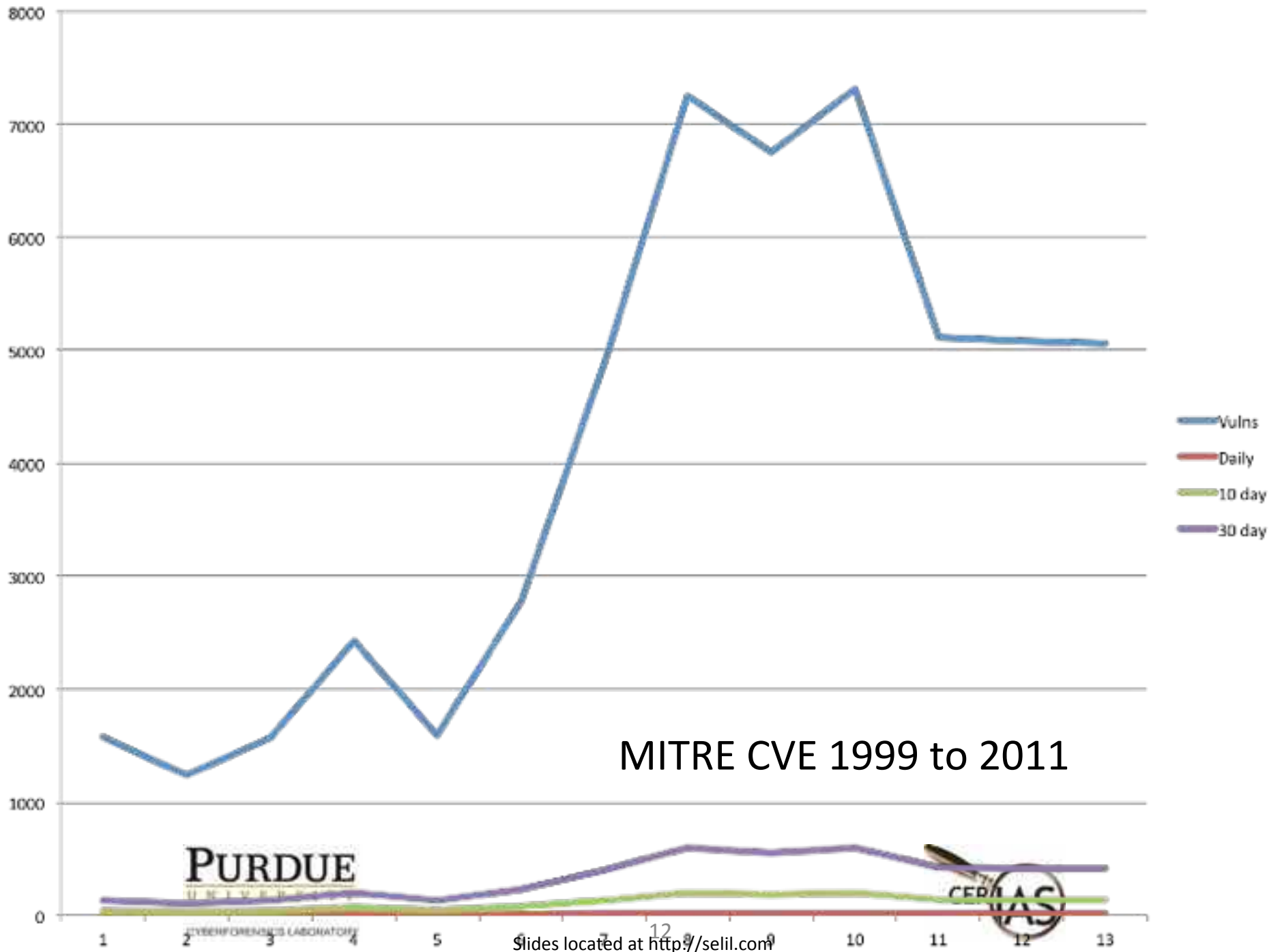
Top Countries

Italy	363
United States	292
France	53
Spain	28
China	12

46.233.143.32  
AES SpA  
Added on: 28-08-2011  


MODEM AES 32.0  
Press Command Number  
1) MBUS TEST STRING  
2) Lancia il Polling su MBUS  
3) Lancia il Polling su **MODBUS**  
4) Valore lettura regolatore Siemens  
5) Download applicazione  
6) Download applicazione di test  
7) TRACE ON/OFF  
8) AUTODISCOVERY START/STOP  
9) Synchronize time via NTP  
a) Device INFO  
b) Impostazioni porta seriale  
c) Memory info  
d) Stringhe memorizzate  
\*) Show Modem Version  
q) Informazioni sul segnale di rete  
r) R...

IoT risk is not necessarily predicted by the previous pattern of information technology risk. That being said what did that look like as the technology was adopted?

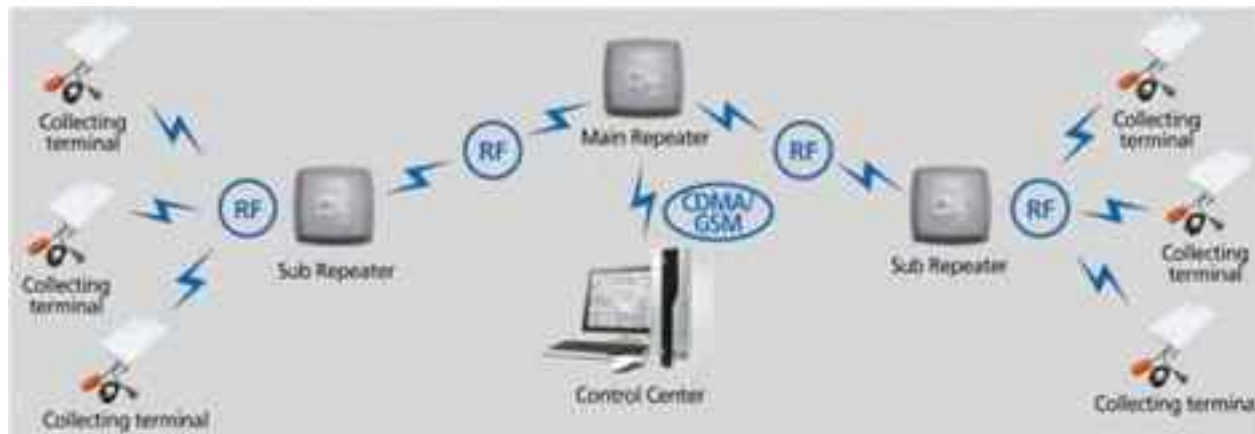


Just because somebody always  
wants to blow stuff up

# April 22, 1992 Guadalajara explosions

- Gasoline explosions in the sewer systems over 4 hour period destroys 8 km of streets
- 252 people killed, 500 injured
- Zinc coated iron pipes built next to steel pipes resulted in corrosion
- Sewer designed to evacuate fluids, but not gasses (fumes)

# That can't happen!



Do I hear an IoT fudastic story about to happen?



Slides located at <http://selil.com>









# Discussion

- Wireless
- Physically accessible
- Minimal security
- Replicable
- Requirements for operation contrary to security



Slides located at <http://selil.com>







# Reality?

- You need motive, means AND opportunity to do something bad.
- Just because it is possible does not mean it is probable.
- **Can** does not mean **will** happen.
- At the individual, personal, family level...
  - Risk is money, privacy, and safety not incidents of national significance

# Money..

- Not all Internet connected devices are for your benefit.
- Currently ATM card skimmers are a great way to steal both the card data and PIN you utilize
- Watch for the sideways attack....

<http://krebsonsecurity.com/2010/02/atm-skimmers-part-ii/>

<http://consumerist.com/2009/04/19/heres-what-a-card-skimmer-looks-like-on-an-atm/>

<http://www.geek.com/chips/criminals-start-using-3d-printing-to-make-better-atm-skimmers-1567392/>



Slides located at <http://selil.com>



# Money...

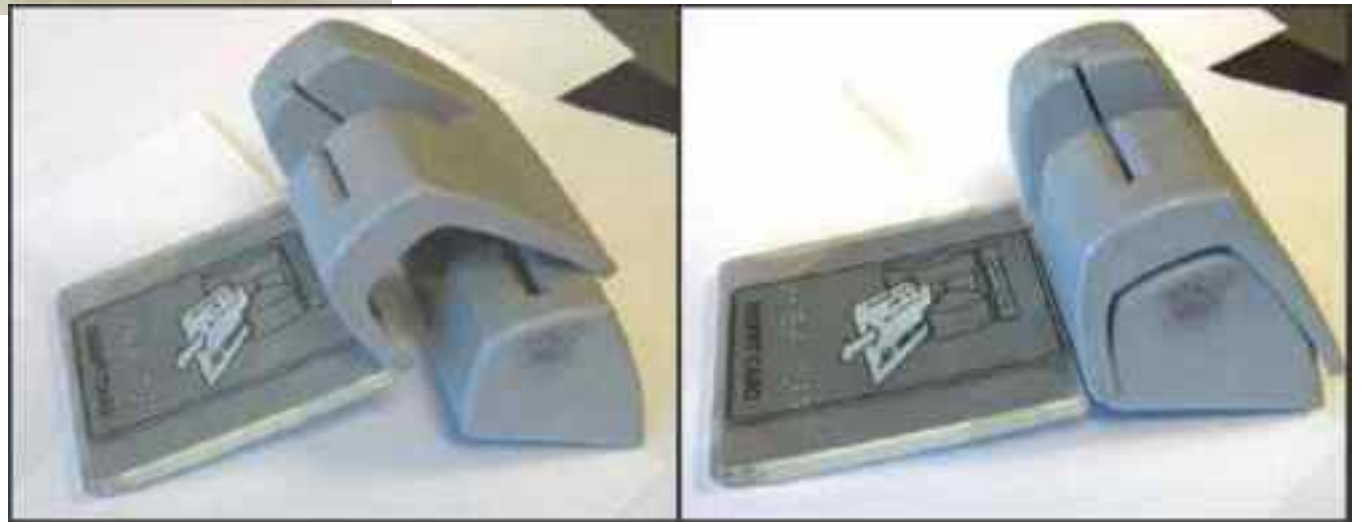


Image Source: <http://www.bootsnall.com/articles/10-04/atm-skimmers-how-to-protect-yourself.html>

# Money...

- Everybody likes money
- Credit card related breaches are in the news
- Credit cards work exactly as they were designed
- As they get smarter they join the IoT world
- The issue is not with the credit card so much as it is with the system of using credit cards
- Any significantly complex system can be used exactly as designed for nefarious purposes



Slides located at <http://selil.com>



# Privacy...

December 21, 2011 “Chinese hack into US Chamber of Commerce, “.... **At one point the penetration of the Chamber of Commerce was so complete that a Chamber thermostat was communicating with a computer in China.**” ABC News

<http://abcnews.go.com/International/chinese-hack-us-chamber-commerce-authorities/story?id=15207642>



Slides located at <http://selil.com>



# Safety...

- Your cell phone is a walking bundle of sensors.
- It contains radios (Cellular, Wifi, Bluetooth, Near Field Communication, GPS, FM)
- It contains sensors for light, microphone, camera, magnetism, heat, touch, shock, gyroscope.
- It knows when you are awake, eating, walking, running, sleeping, being lazy, and your most intimate secrets.
- And, you take it into your car



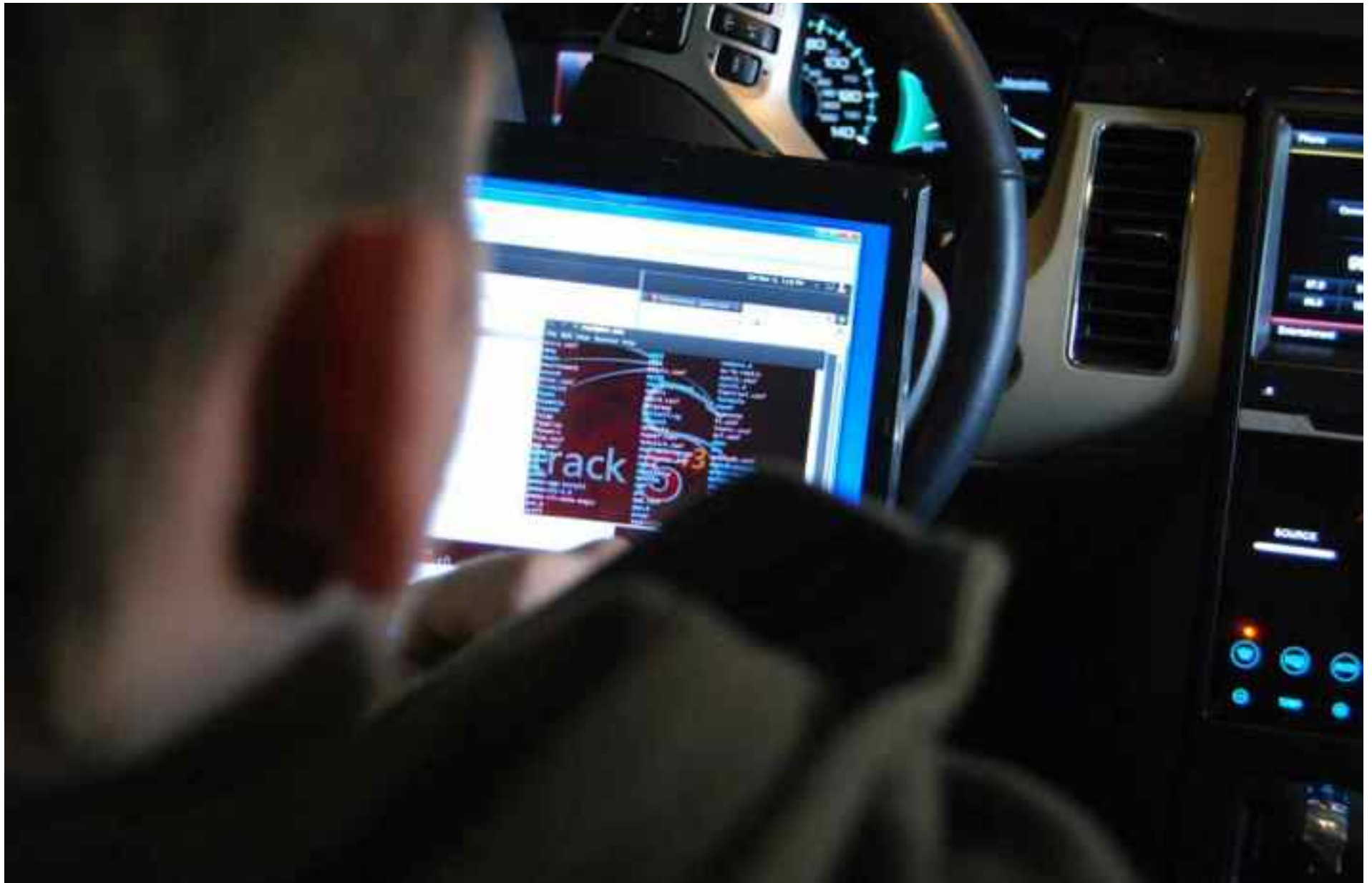
# So my students and I rented a car...

- The car was a newish Ford Flex with infotainment system
- We forensically processed the car for evidence
- We looked at both digital and physical evidence
- What we found was interesting
- It was a learning experience...



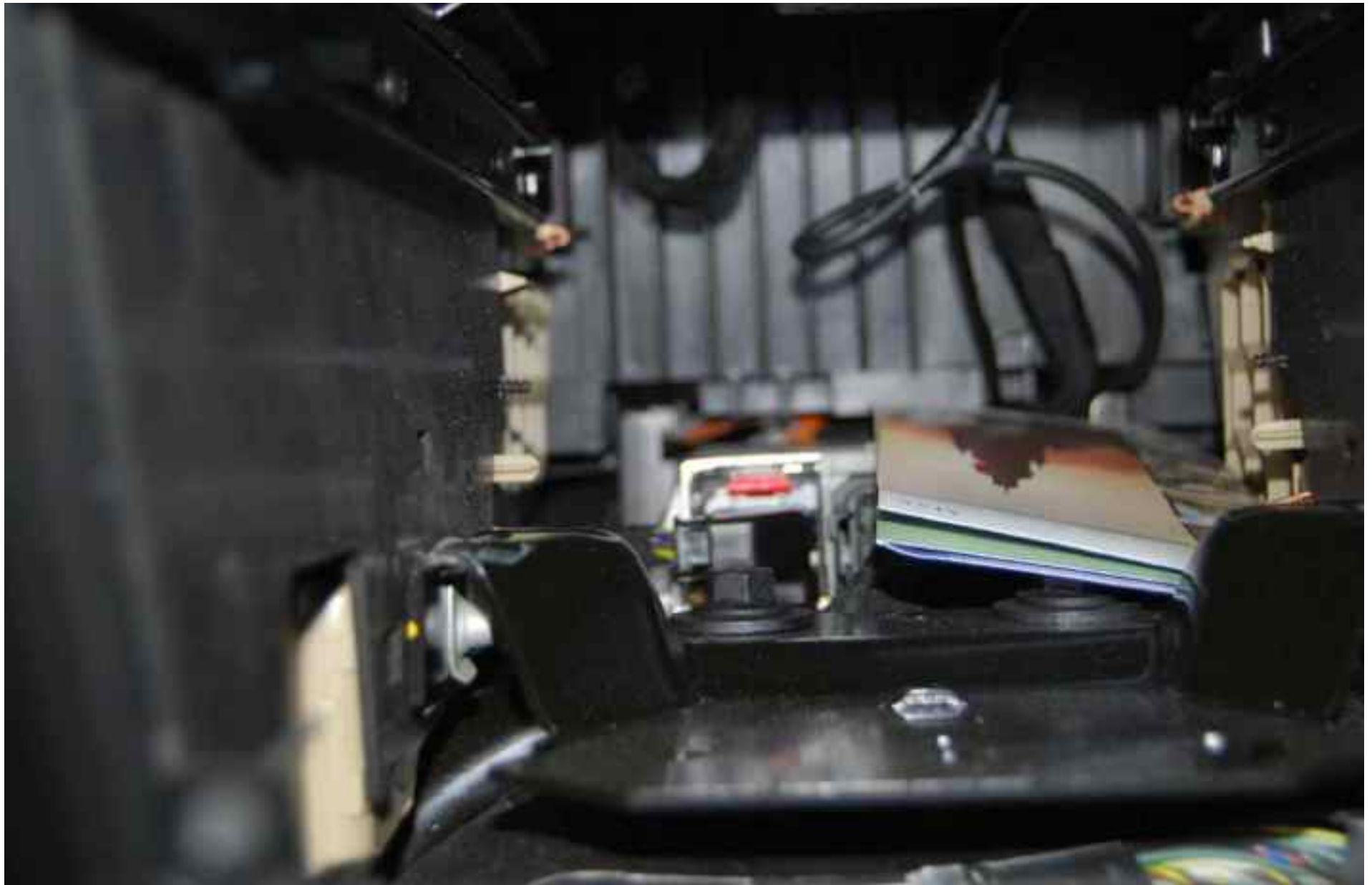












# REDACTED FOR PUBLICATION

Your stuff is watching you

Don't worry we are here to help



Slides located at <http://selil.com>

