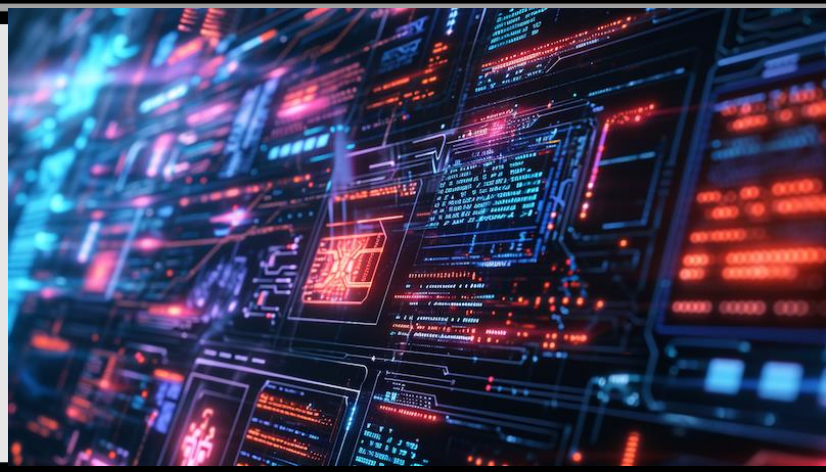
Class 1

CSC 600 Advanced Seminar
Introduction

Si Chen (schen@wcupa.edu)



What is computer security?

- Most developers and operators are concerned with **correctness**: achieving desired behavior
  - A working banking web site, word processor, blog, …
- Security is concerned with ***preventing*** **undesired behavior**
  - Considers an enemy/opponent/hacker/adversary who is *actively and maliciously* trying to *circumvent* any protective measures you put in place

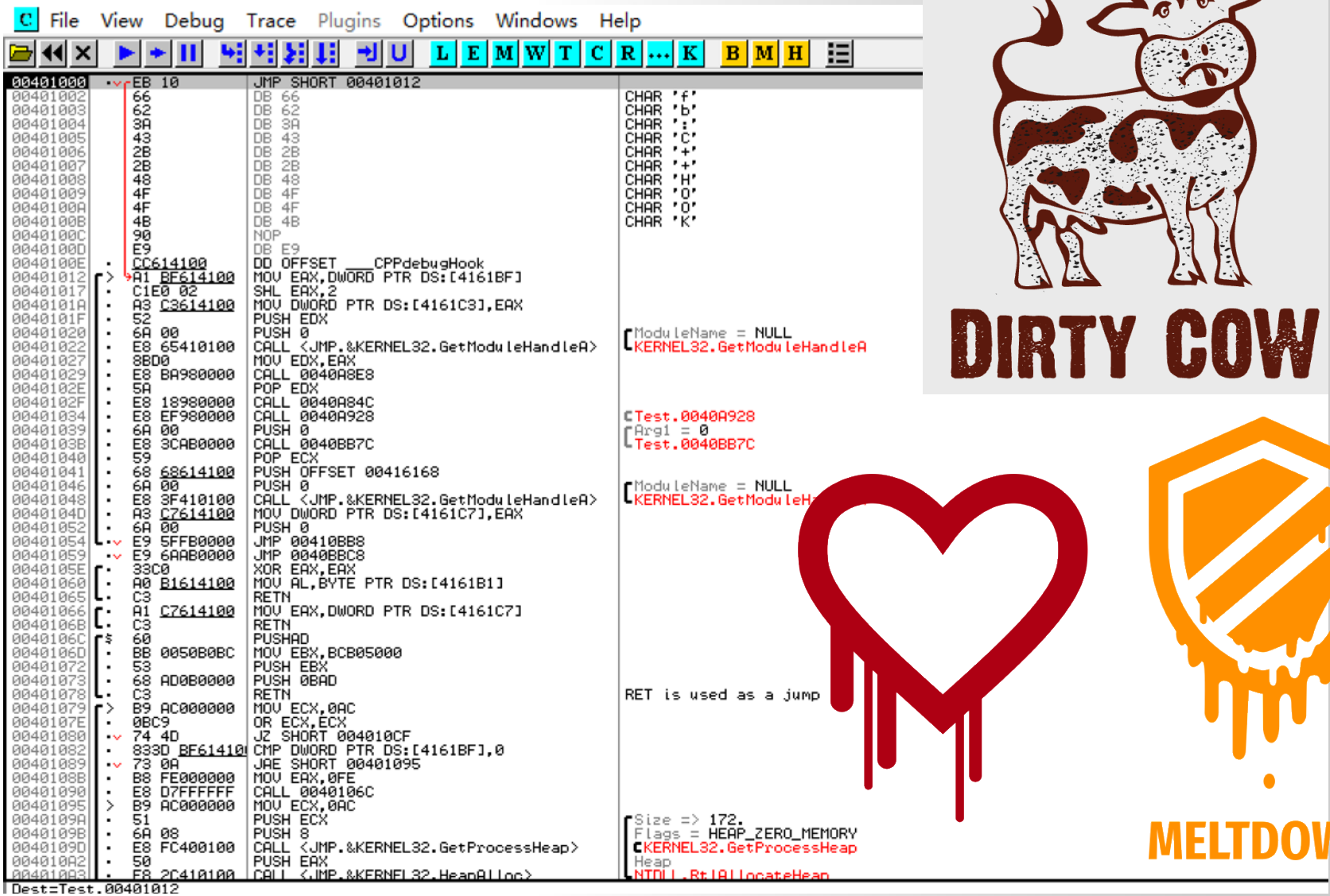
Security Expectations

- **Confidentiality**: requires that information be kept private
- **Integrity**: the trustworthiness and correctness of data.
- **Availability**: the capability to use information and resources.

Kinds of undesired behavior

- Stealing information: ~~**confidentiality**~~
  - Corporate secrets (product plans, source code, …)
  - Personal information (credit card numbers, SSNs, …)
- Modifying information or functionality: ~~**integrity**~~
  - Installing unwanted software (spyware, botnet client, …)
  - Destroying records (accounts, logs, plans, …)
- Denying access: ~~**availability**~~
  - Unable to purchase products
  - Unable to access banking information

General perspectives and attack research



General perspectives and attack research

Were you affected by the Xfinity data breach? Here's what you should do

Data breach underscores the importance of password protection, cybersecurity experts say

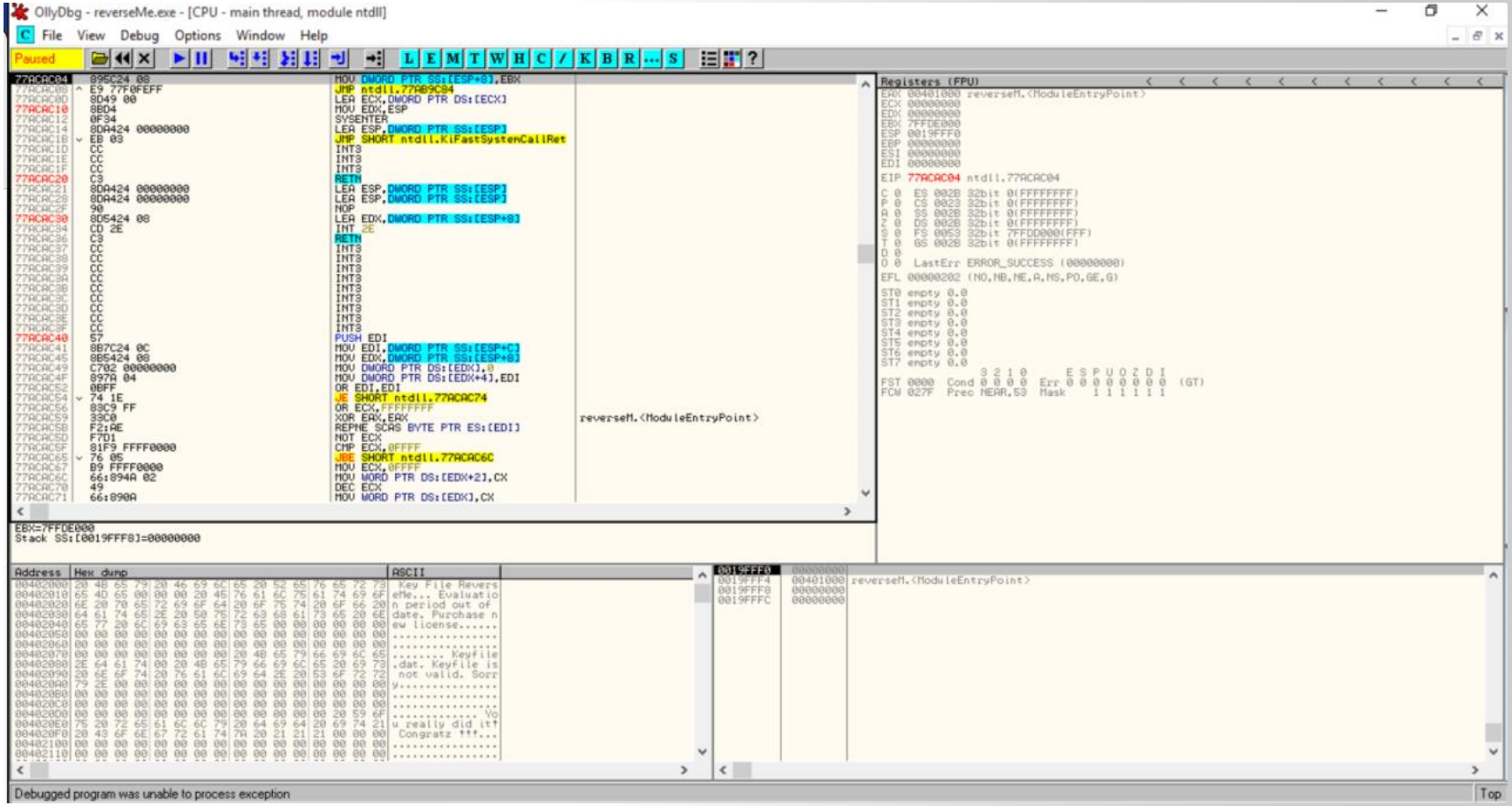
CVE-2023-4966 "Citrix Bleed"

Dr. Si Chen, associate computer science professor at West Chester University, thinks Comcast should be more transparent with customers and publish exactly what happened.

"They don't have to be a technical guru to understand the details, but as a company, you need to publish that information so the people will have a clear message of what's actually going on," he said.

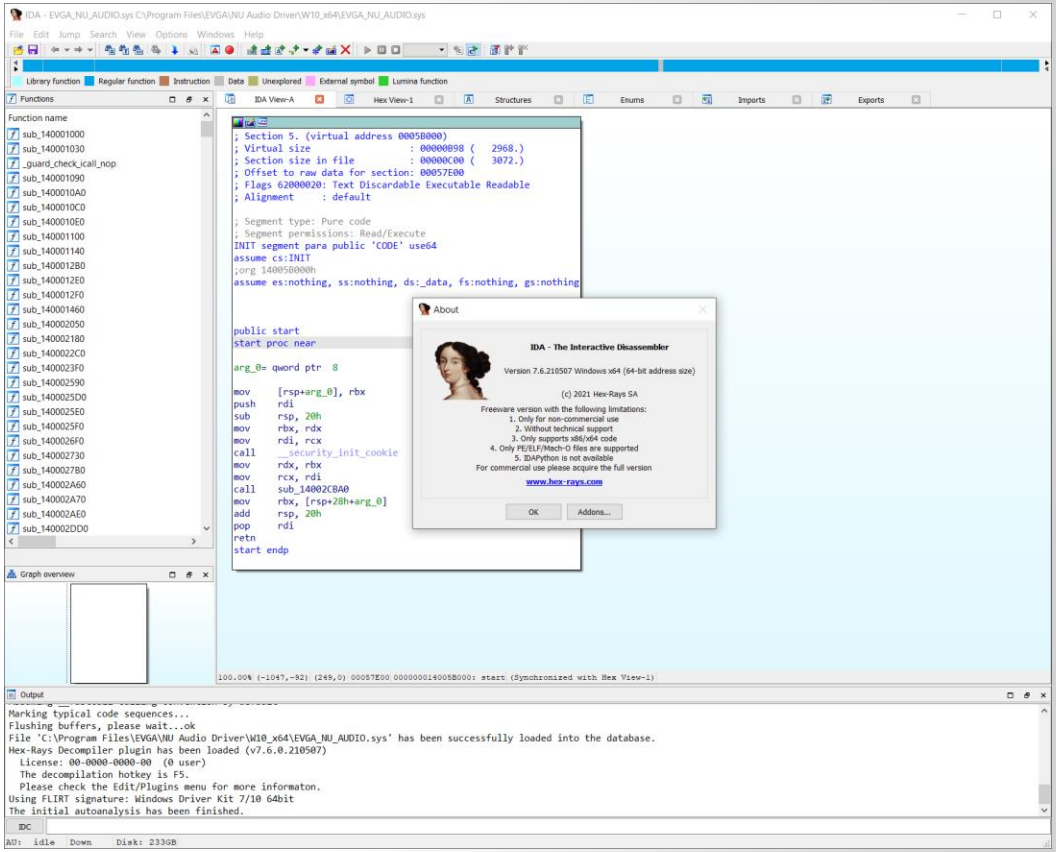
https://www.audacy.com/kywnewsradio/news/local/what-to-do-xfinity-data-breach-password-security-reset

Debugging Software



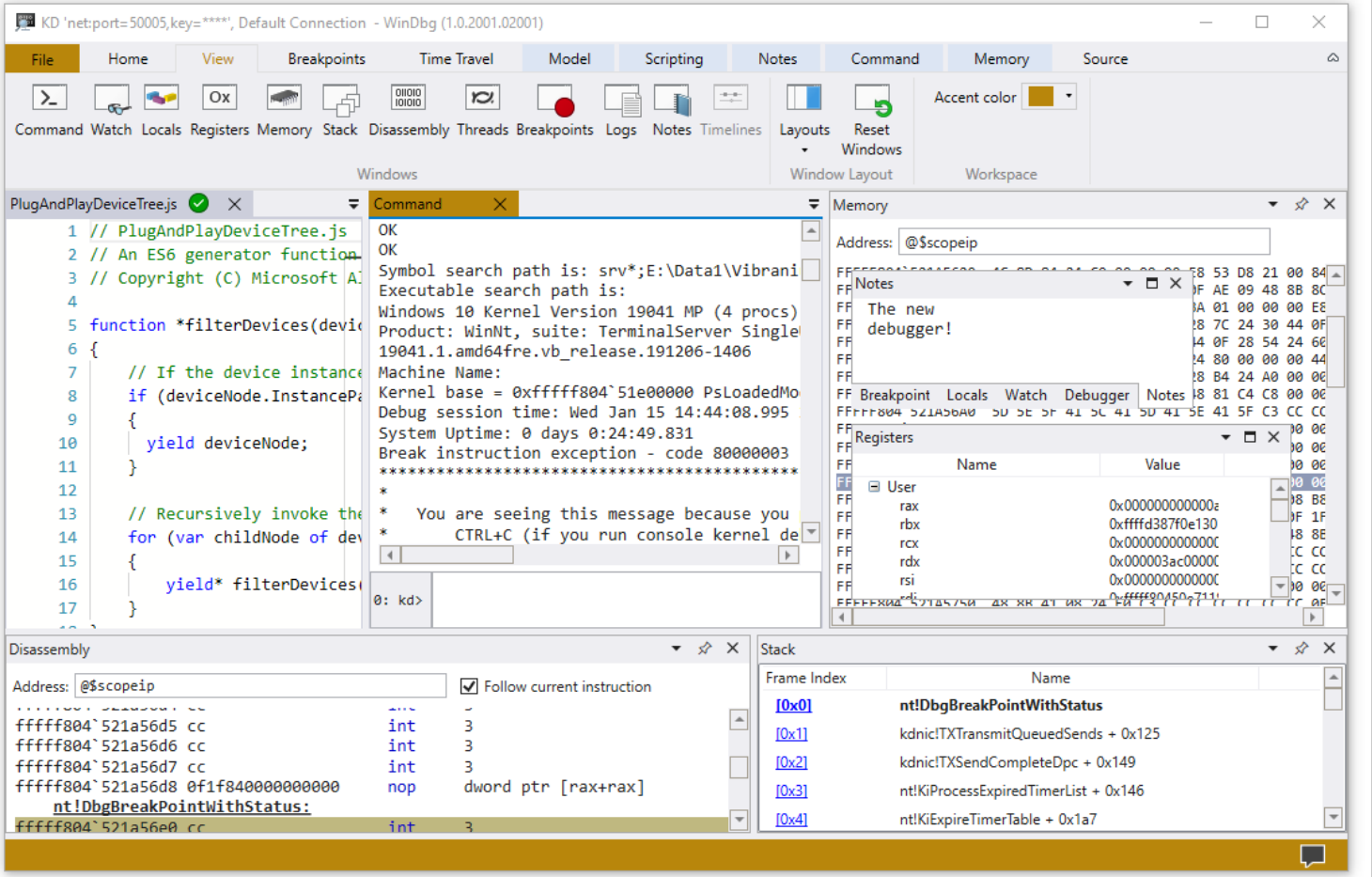
Ollydbg: OllyDbg was an x86 debugger that emphasizes binary code analysis, which is useful when source code is not available. It traces registers, recognizes procedures, API calls, switches, tables, constants and strings, as well as locates routines from object files and libraries. Wikipedia

Debugging Software



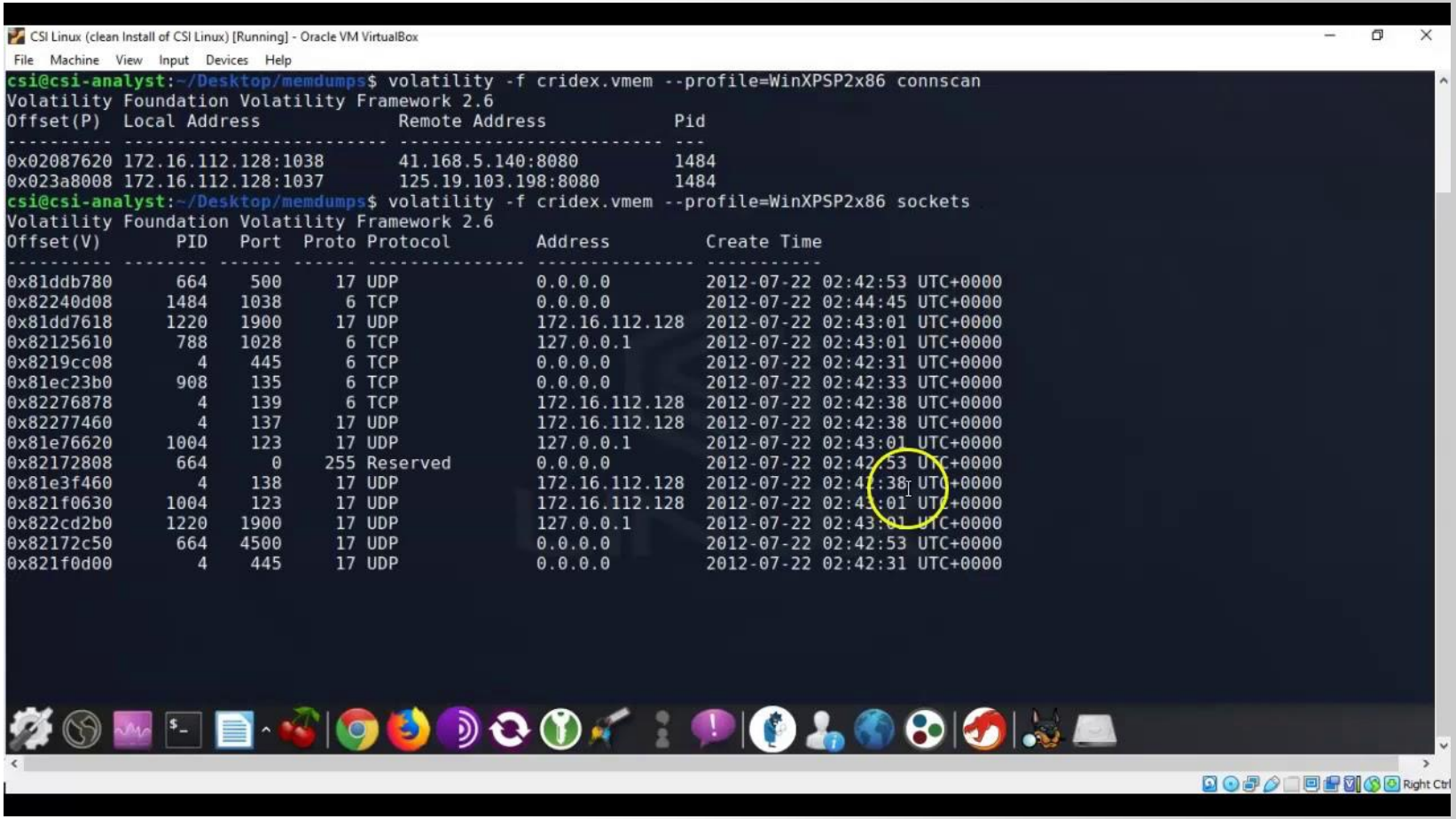
IDA free: This free version of IDA offers a privilege opportunity to see IDA in action. This light but powerful tool can quickly analyze the binary code samples and users can save and look closer at the analysis results.

Debugging Software



WinDbg: WinDbg is a multipurpose debugger for the Microsoft Windows computer operating system, distributed by Microsoft. Debugging is the process of finding and resolving errors in a system; in computing it also includes exploring the internal operation of software as a help to development. Wikipedia

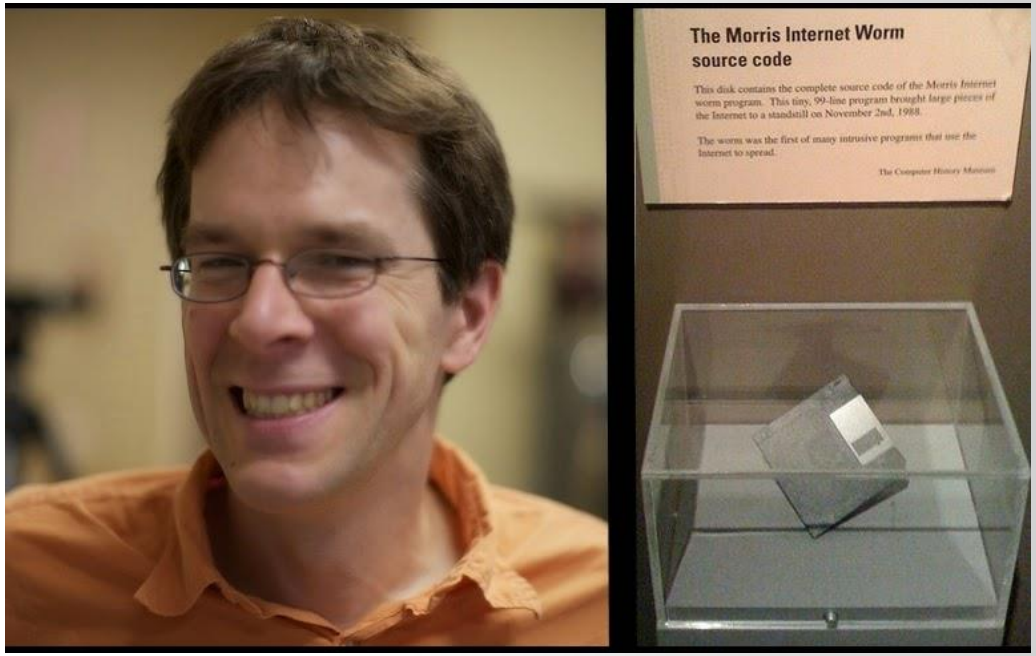
Volatility



Volatility: Volatility is an open-source memory forensics framework for incident response and malware analysis. It is written in Python and supports Microsoft Windows, Mac OS X, and Linux. Volatility was created by Aaron Walters, drawing on academic research he did in memory forensics. Wikipedia

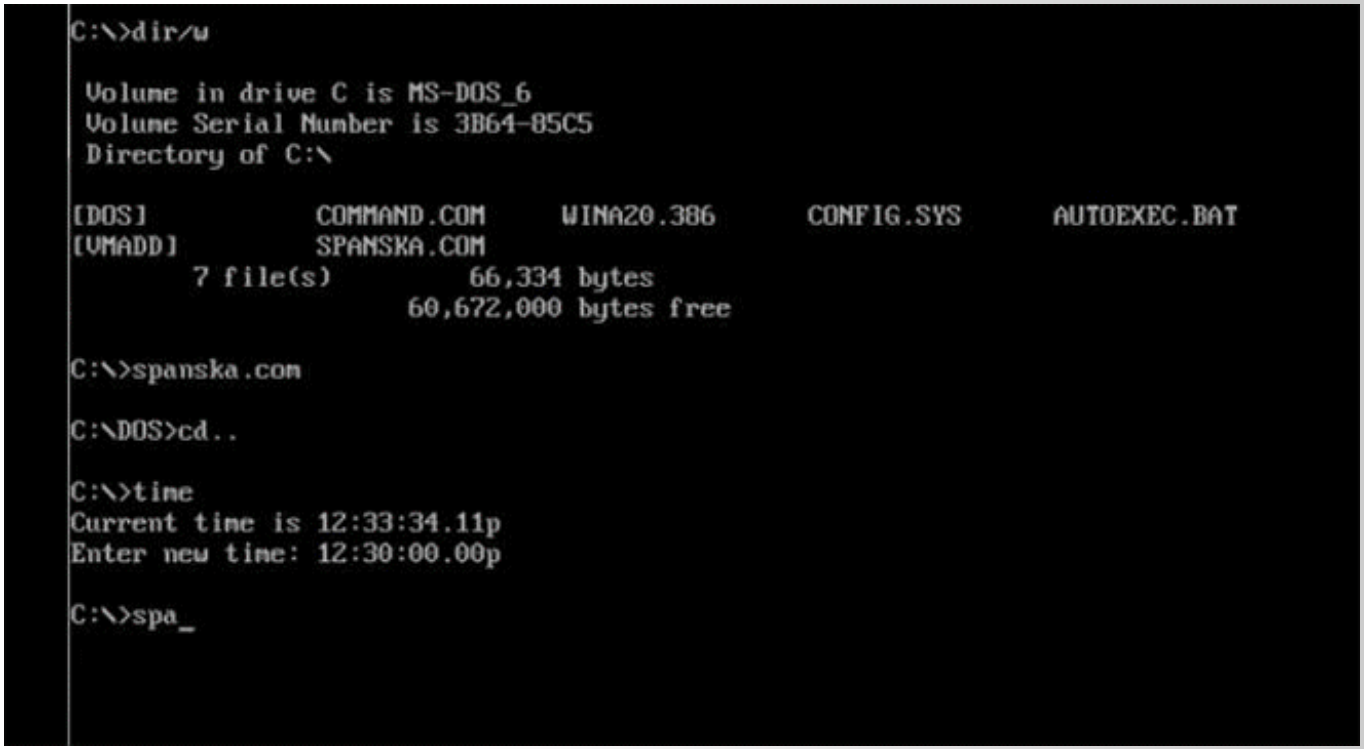
First-gen Hacker

- Morris Worm
  - On accident
  - Purpose: “gauge the size of the internet”
  - What happened: Fork bomb

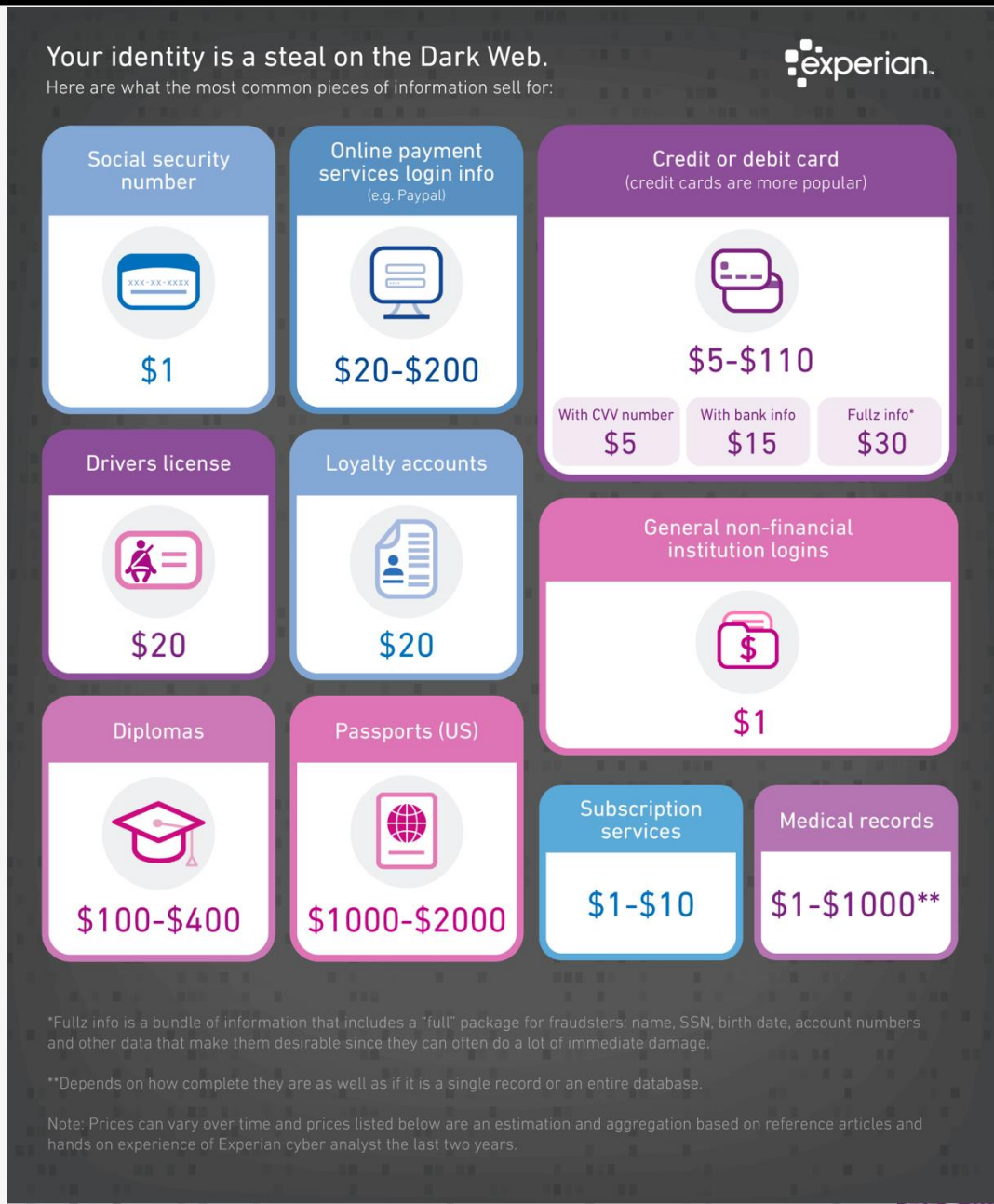


First-gen Hacker

- Once upon a time… (30 Years Ago)
  - Just for fun
  - Spread to other machines & display a message



- Today
  - — $$$
- Organizations buy malware
  - Steal passwords, credit cards, bank info, ransoms, intellectual property, trade secrets
  - They can use this info or sell it



Why do people write malware?

- ~~Future~~… Today
  - Gathering more information about a person.

Why do people write malware?

- ~~Future~~…Today
  - Spread False Information

Cougar Football | Cougars | Pac-12 | Sports

WSU coach Mike Leach tweets fake Barack Obama video, stirs up a Twitter storm

Originally published June 18, 2018 at 10:41 am | *Updated June 18, 2018 at 11:08 am*

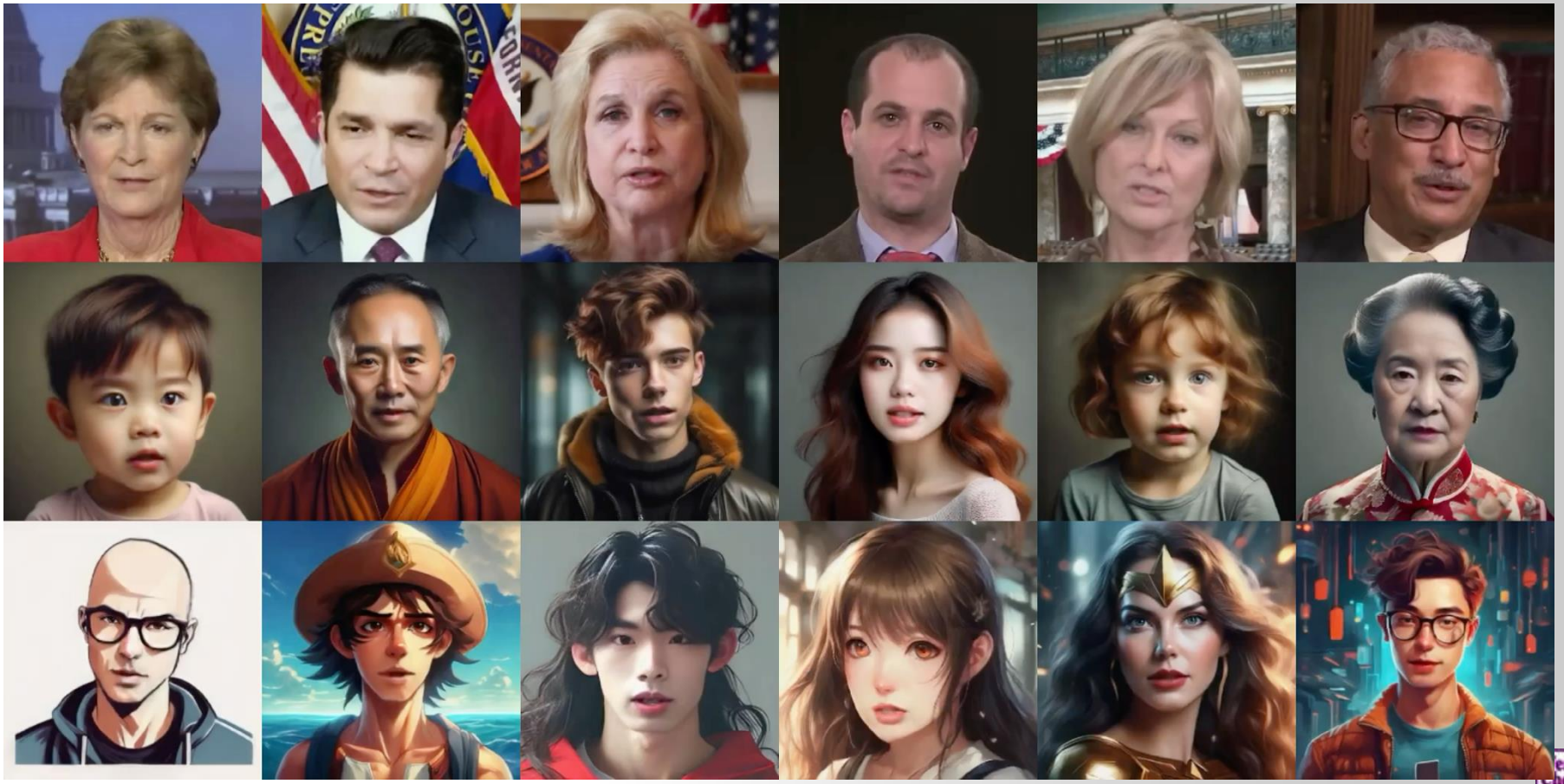
https://www.youtube.com/watch?v=cQ54GDm1eL0

Deepfakes are just the beginning for cybersecurity's Faceswap nightmare

Fergus Halliday (PC World) on 04 April, 2018 14:44

Why do people write malware?

VividTalk: One-Shot Audio-Driven Talking Head Generation Based on 3D Hybrid Prior



Why do people write malware?

Animate Anyone: Consistent and Controllable Image-to-Video Synthesis for Character Animation

- Future…
  - Spread False Information

Cougar Football | Cougars | Pac-12 | Sports

WSU coach Mike Leach tweets fake Barack Obama video, stirs up a Twitter storm

Originally published June 18, 2018 at 10:41 am | *Updated June 18, 2018 at 11:08 am*

https://www.youtube.com/watch?v=cQ54GDm1eL0

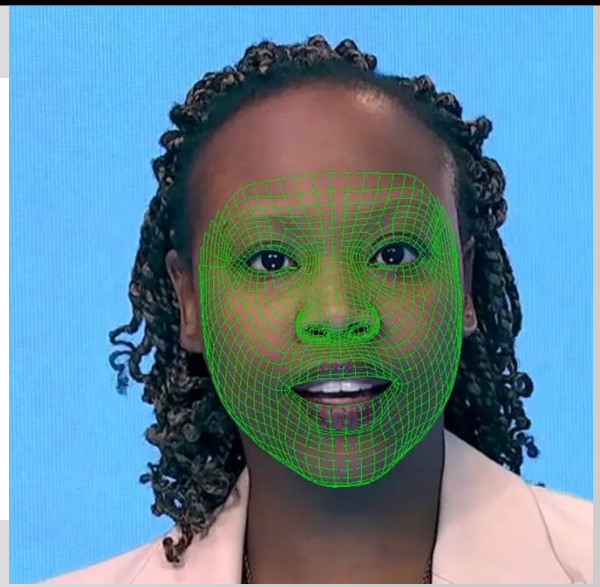
Deepfakes are just the beginning for cybersecurity's Faceswap nightmare

Fergus Halliday (PC World) on 04 April, 2018 14:44

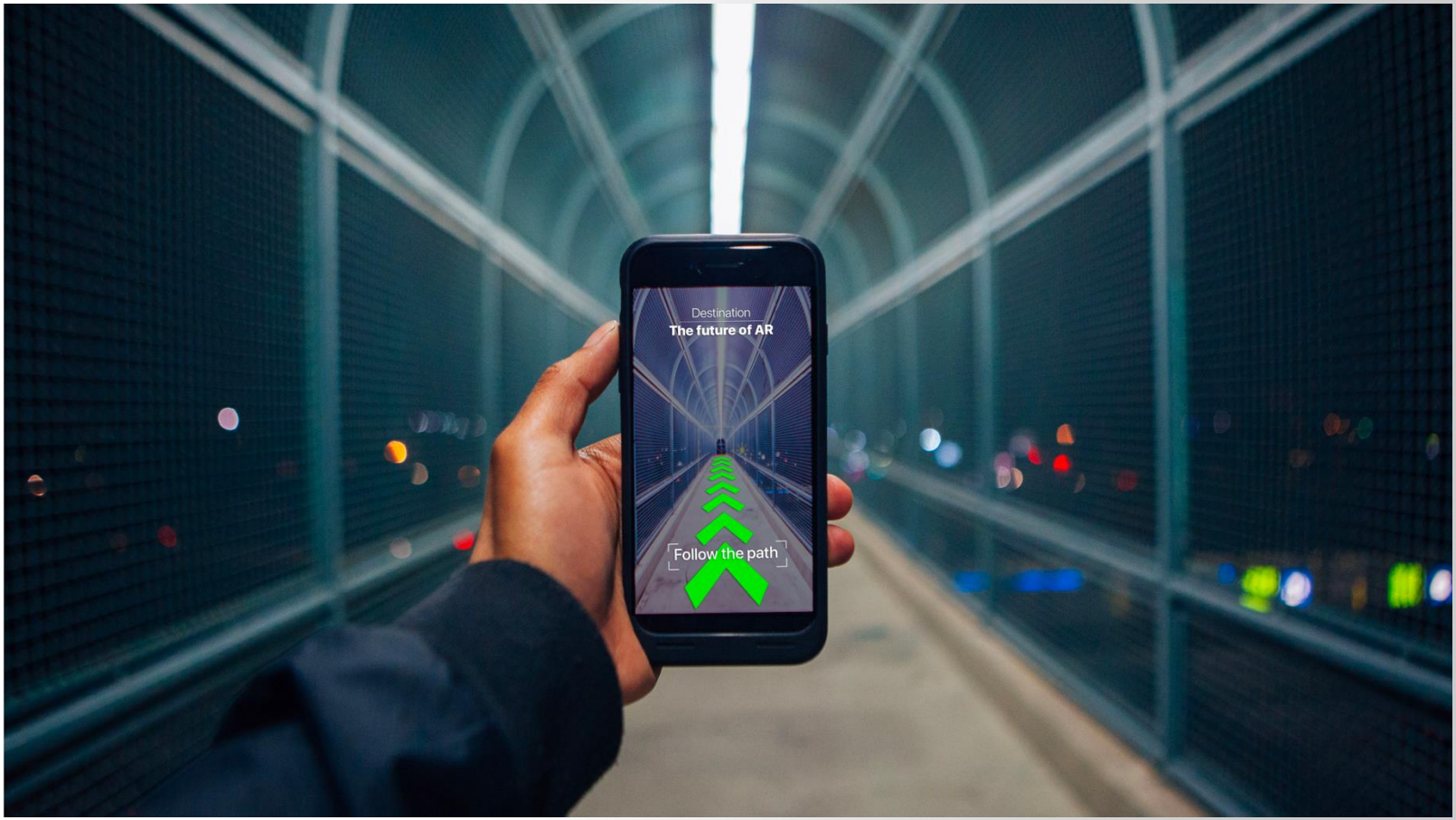
Why do people write malware?

As Deepfakes Flourish, Countries Struggle With Response

Few governments have approved regulations, often because of free-speech concerns. New mandates from China could change the tone of the debate on digital forgeries.

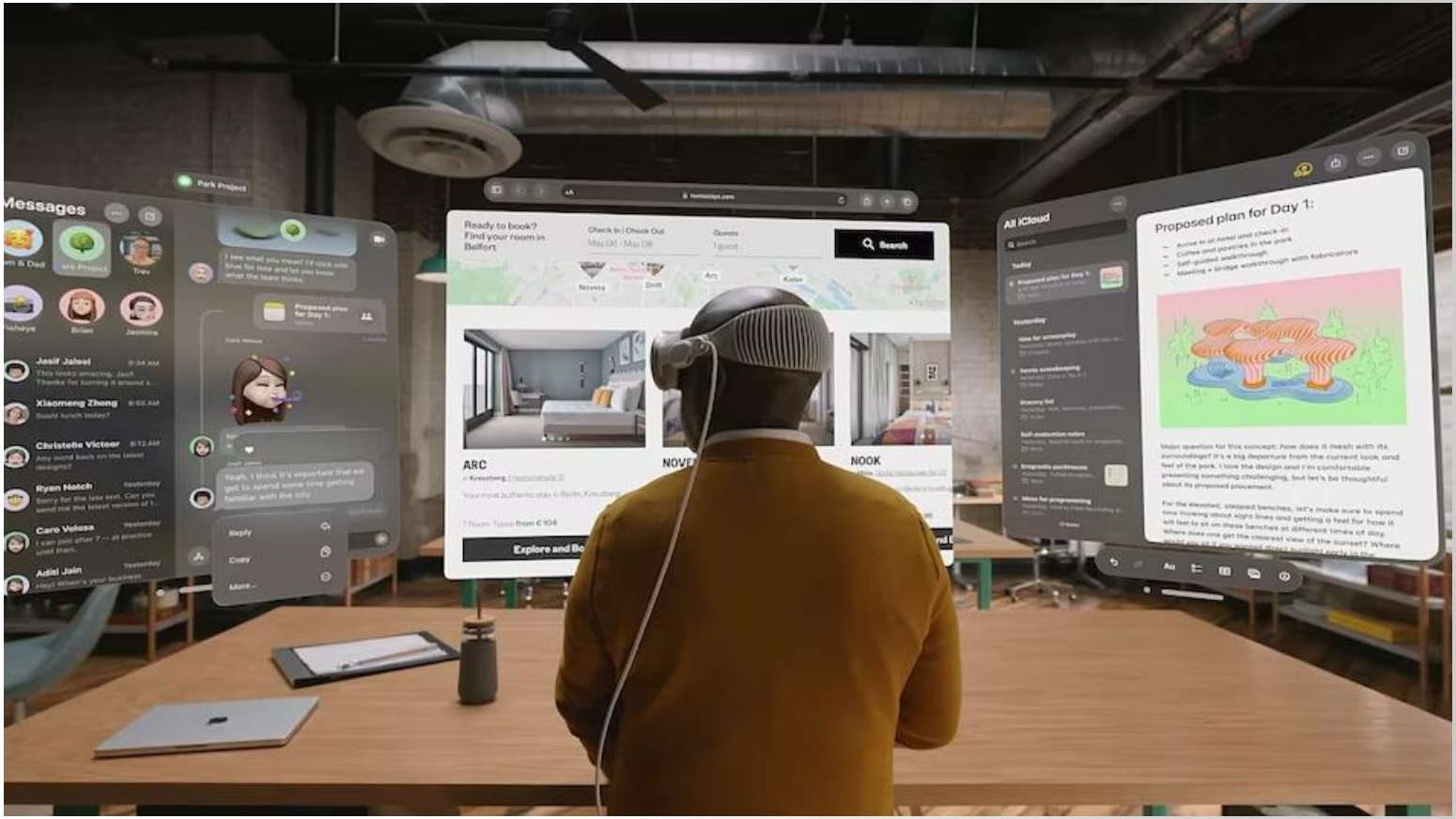


- Future…
  - Control your Life

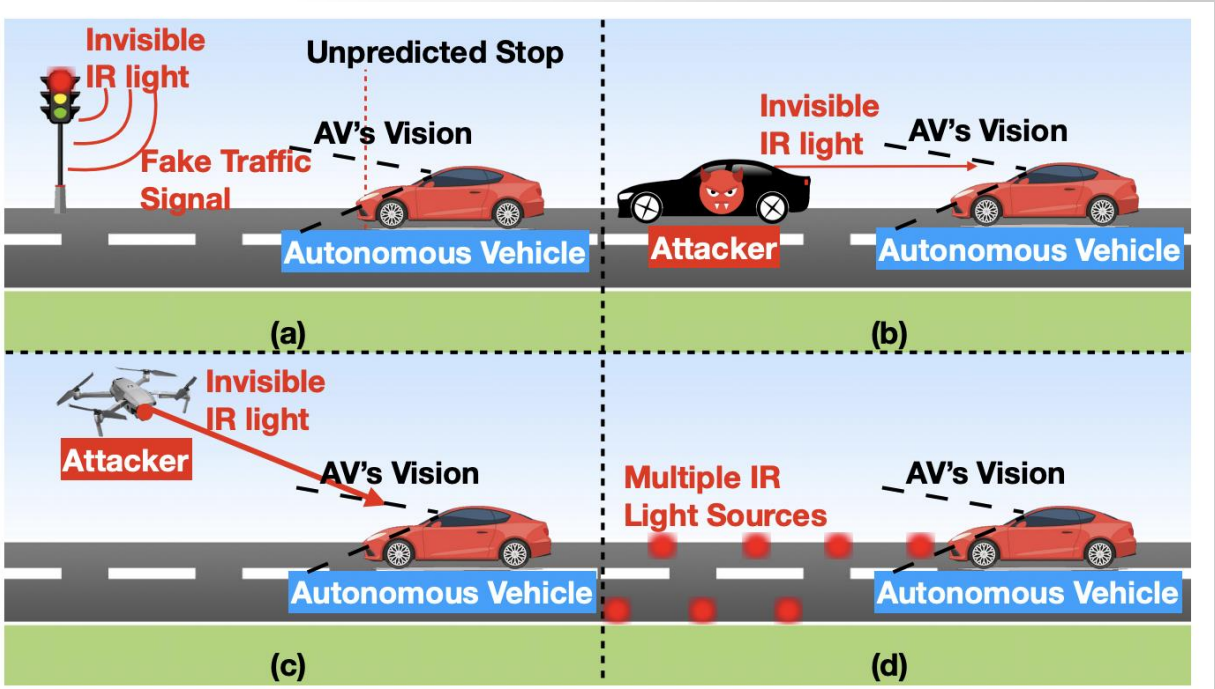


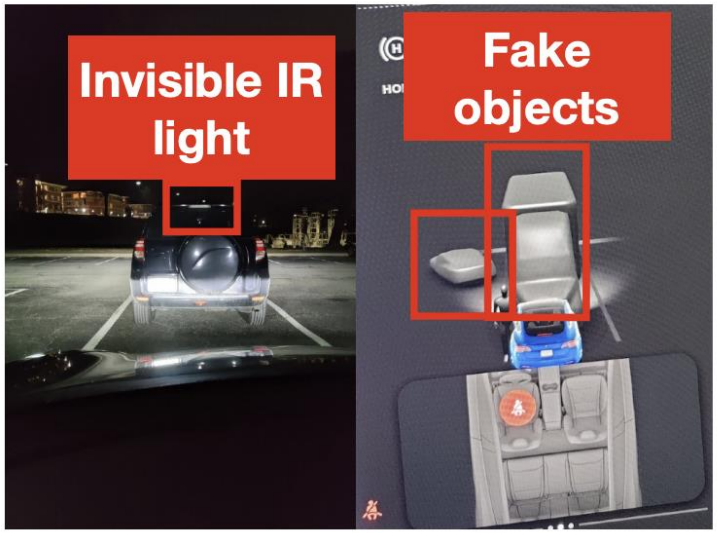
Why do people write malware?

- Future…
  - Control your Life

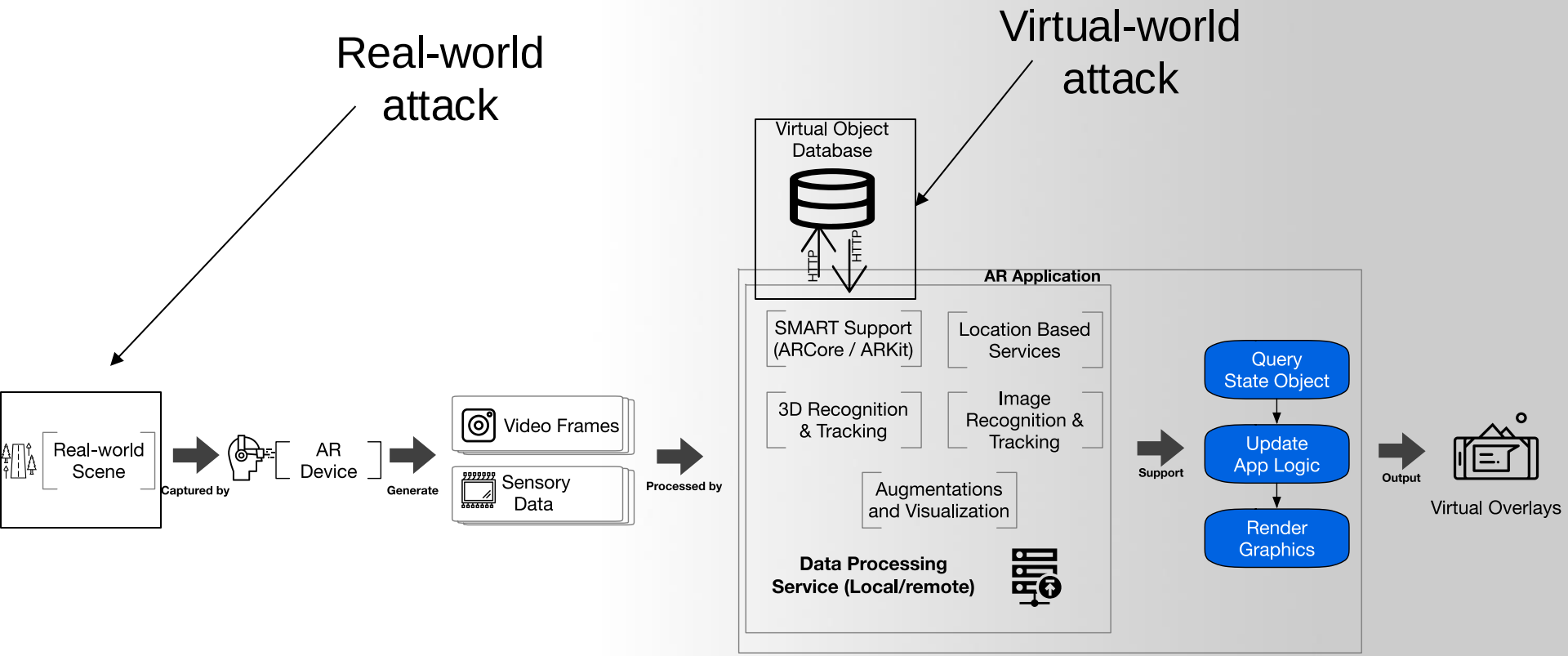


I Can See the Light: Attacks on Autonomous Vehicles Using Invisible Lights





Our project – AR Security



Our approach

- **The content of the course is broken down into two sections:**
  - **Section 1: Foundations and Perspectives**
    - Lecture on the topic
    - Reading paper and answer some questions (Lab Homework)
  - **Section 2: In-depth Examination of Research Topics**
    - Group presentation and discussion on the research topics

Top computer security conference

Top computer security conference

ACM Conference on Computer and Communications Security (CCS)

About CCS

The ACM Conference on Computer and Communications Security (CCS) is the flagship annual conference of the Special Interest Group on Security, Audit and Control (SIGSAC) of the Association for Computing Machinery (ACM). The conference brings together information security researchers, practitioners, developers, and users from all over the world to explore cutting-edge ideas and results. It provides an environment to conduct intellectual discussions. From its inception, CCS has established itself as a high-standard research conference in its area.

Top computer security conference

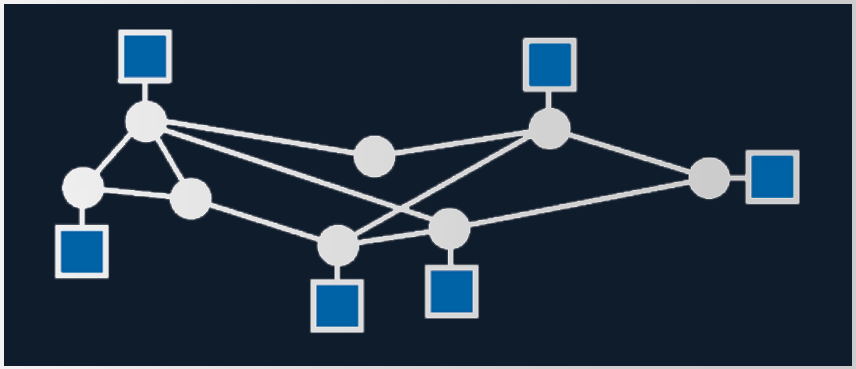
IEEE Symposium on Security and Privacy (S&P)

Since 1980, the IEEE Symposium on Security and Privacy (S&P)has been the premier forum for the presentation of developments in computer security and electronic privacy, and for bringing together researchers and practitioners in the field.

Top computer security conference

ISOC Network and Distributed System Security Symposium (NDSS)

The Network and Distributed System Security Symposium (NDSS) fosters information exchange among researchers and practitioners of network and distributed system security. The target audience includes those interested in practical aspects of network and distributed system security, with a focus on actual system design and implementation. A major goal is to encourage and enable the Internet community to apply, deploy, and advance the state of available security technologies.



Top computer security conference

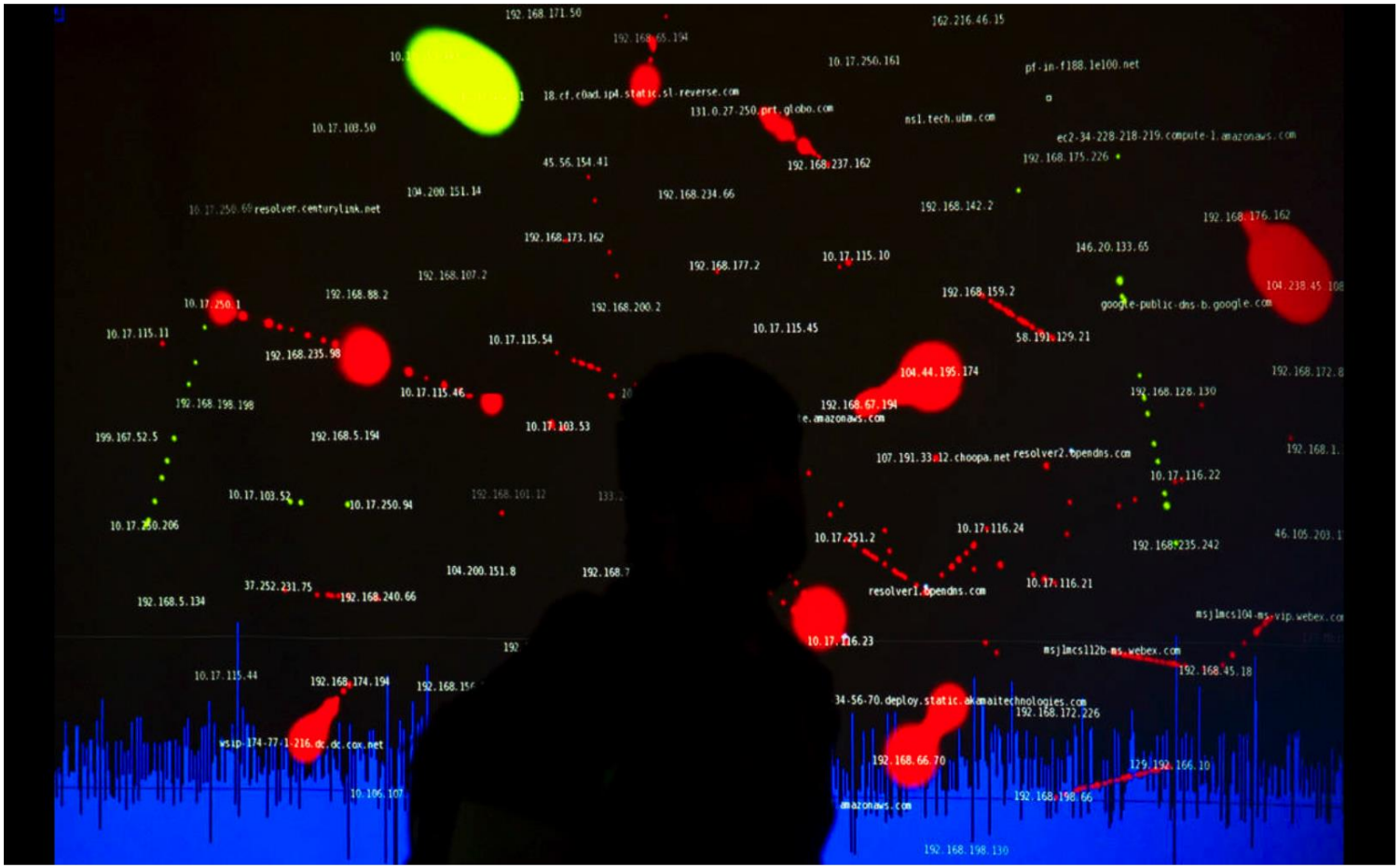
Usenix Security Symposium (USENIX)

The USENIX Security Symposium brings together researchers, practitioners, system administrators, system programmers, and others interested in the latest advances in the security and privacy of computer systems and networks.

- **Top Security Conference for Hacking**
  - **Black hat USA**
  - **DEFCON**

West Chester University

DefCon, Black Hat bring extra cybersecurity concerns to Las Vegas



A Black Hat tech associate works in the network operating center (NOC) during the Black Hat information security conference at Mandalay Bay, Wednesday, July 26, 2017, In Las Vegas. Richard Brian Las Vegas Review-Journal


PARADISE FISHING

Q & A