
THE ETHICAL
HACKER
NETWORK


EH-NET
Live!

Deepfakes:
A Technical Peek Behind the Curtain

March 31, 2020

PRESENTER:
Alyssa Miller

AGENDA

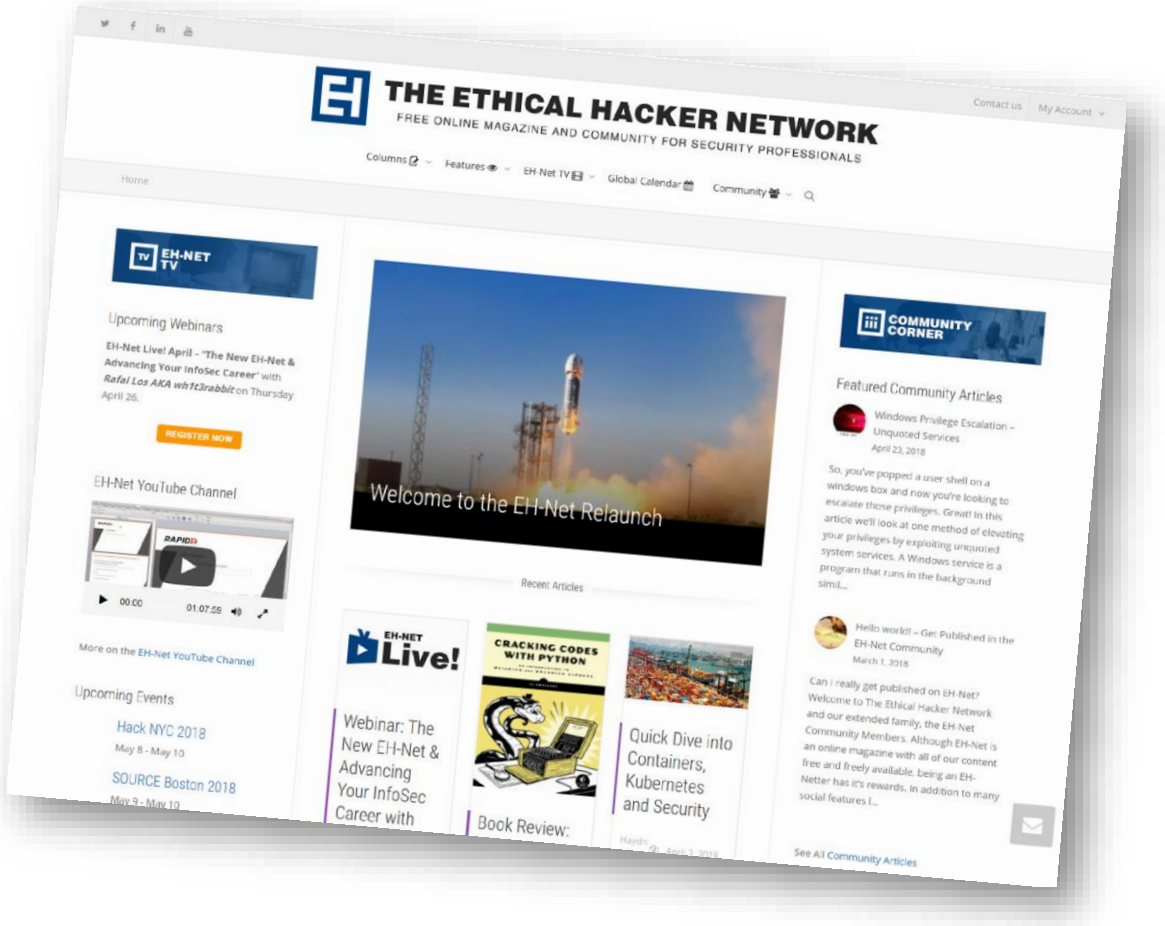
- Intro by Don Donzal, EH-Net Editor-in-Chief
- Bio – Alyssa Miller
- Presentation
  - A Brief History of Deepfakes
  - Beyond Fun and Cyber Security: Effects on Global Markets
  - Not All Doom & Gloom
  - Live Demos
  - Career Aspects
  - Your Turn! How to get there.
- Q&A

INTRO

- Video will be made available on EH-Net
- Style = Interview!
  - Q&A in question tab in GTW
  - Twitter using #EHNet
- Post Game in EH-Net "**Data Science**" Group: https://www.ethicalhacker.net/groups/data-science/
- Goal for today – Spark conversation. Advance your career!

OVERVIEW OF THE NEW EH-NET

- General Layout
  - Magazine side - Columnists, Features, Global Calendar
  - Community side – Members & Profiles, Activity, Forums, Groups, Community Articles
- Building your “Personal Ethical Hacker Network”
- Hello world! – Get Published in the EH-Net Community
- Limited Time – All new members get a free pen testing course from eLS!!



BIO – Alyssa Miller

Alyssa Miller is a hacker, security evangelist, cybersecurity professional and public speaker with almost 15 years of experience in the security industry. A former developer, her background is application security, not only conducting technical assessments, but also helping develop secure SDLC procedures. However, she specializes in designing and deploying effective security programs to strengthen enterprise security strategy. Miller speaks regularly at industry and vendor conferences, has been featured in industry media, is a Board Member for Women of Security (WoSEC) and a member of the Advisory board for Blue Team Con. Miller is currently an Application Security Advocate for Snyk, a London-based open source security firm. She holds a CISM certification from ISACA.

What are “Deepfakes”?

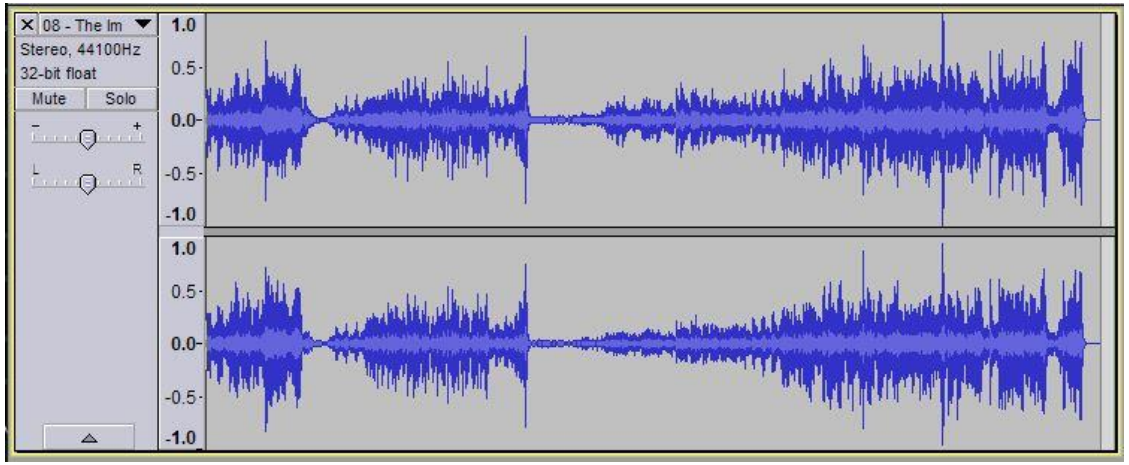
Deepfakes

[ˈdēp, fāks]
NOUN

Deepfakes (a portmanteau of "deep learning" and "fake"[1]) are synthetic media[2] in which a person in an existing image or video is replaced with someone else's likeness. While the act of faking content is a not new, deepfakes leverage powerful techniques from machine learning and artificial intelligence to manipulate or generate visual and audio content with a high potential to deceive.[3] The main machine learning methods used to create deepfakes are based on deep learning and involve training generative neural network architectures, such as autoencoders[3] or generative adversarial networks (GANs).[4][5]

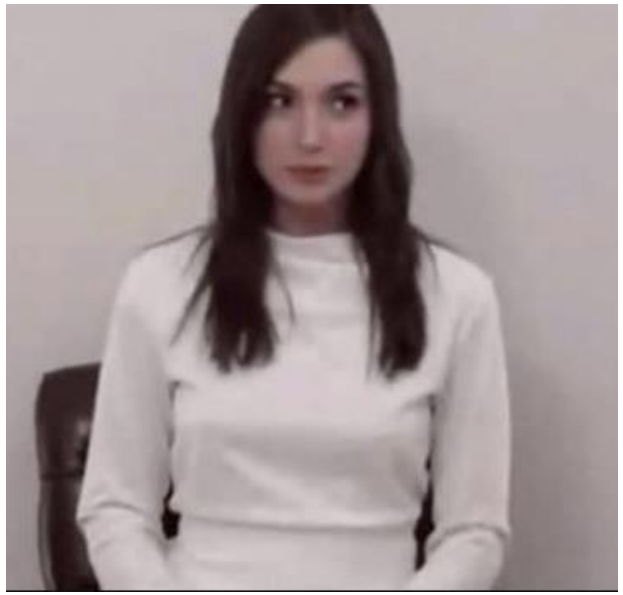
Source: https://en.wikipedia.org/wiki/Deepfake

Expanding that Definition a little…

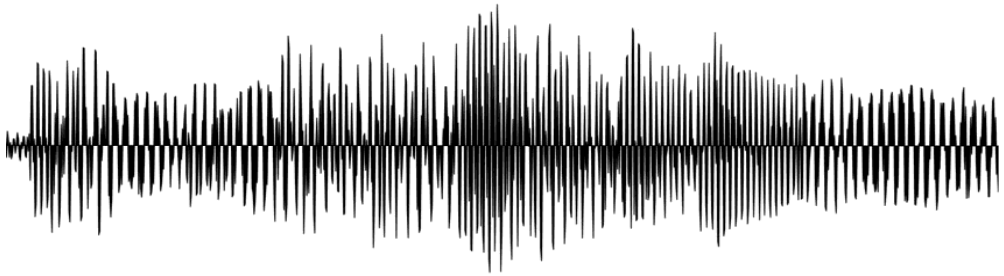


Where Deepfakes Began

Deepfakes Beginning…



The Threats…



Social Engineering

Extortion

“Outsider” Trading

Market Manipulation

Not All Doom and Gloom – Positive Apsects of ML

- Education
- Translation
- Pharma / Imaging
- Weather
- Global Relief Efforts
- Disaster Prevention
- Simulations w/o Human Harm
- Protect Us – Cybersecurity, privacy, etc.

Understanding GANs…

Target Media

Generator

Training Set

Fake

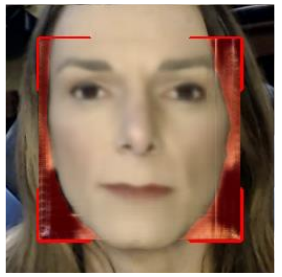
Discriminator

Real

Deeper into Deep Learning…

Encoder

Decoder



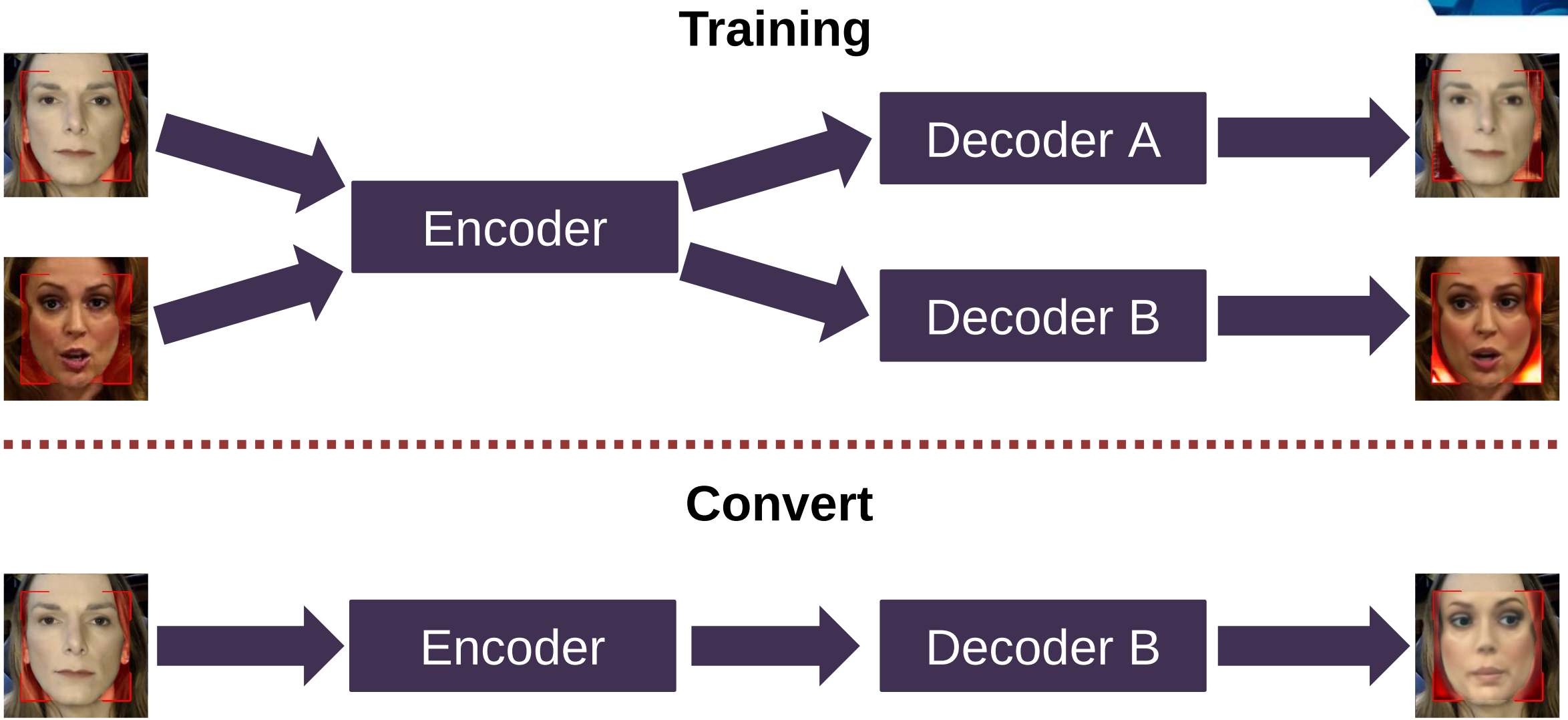
Loss

Discriminator

Weights

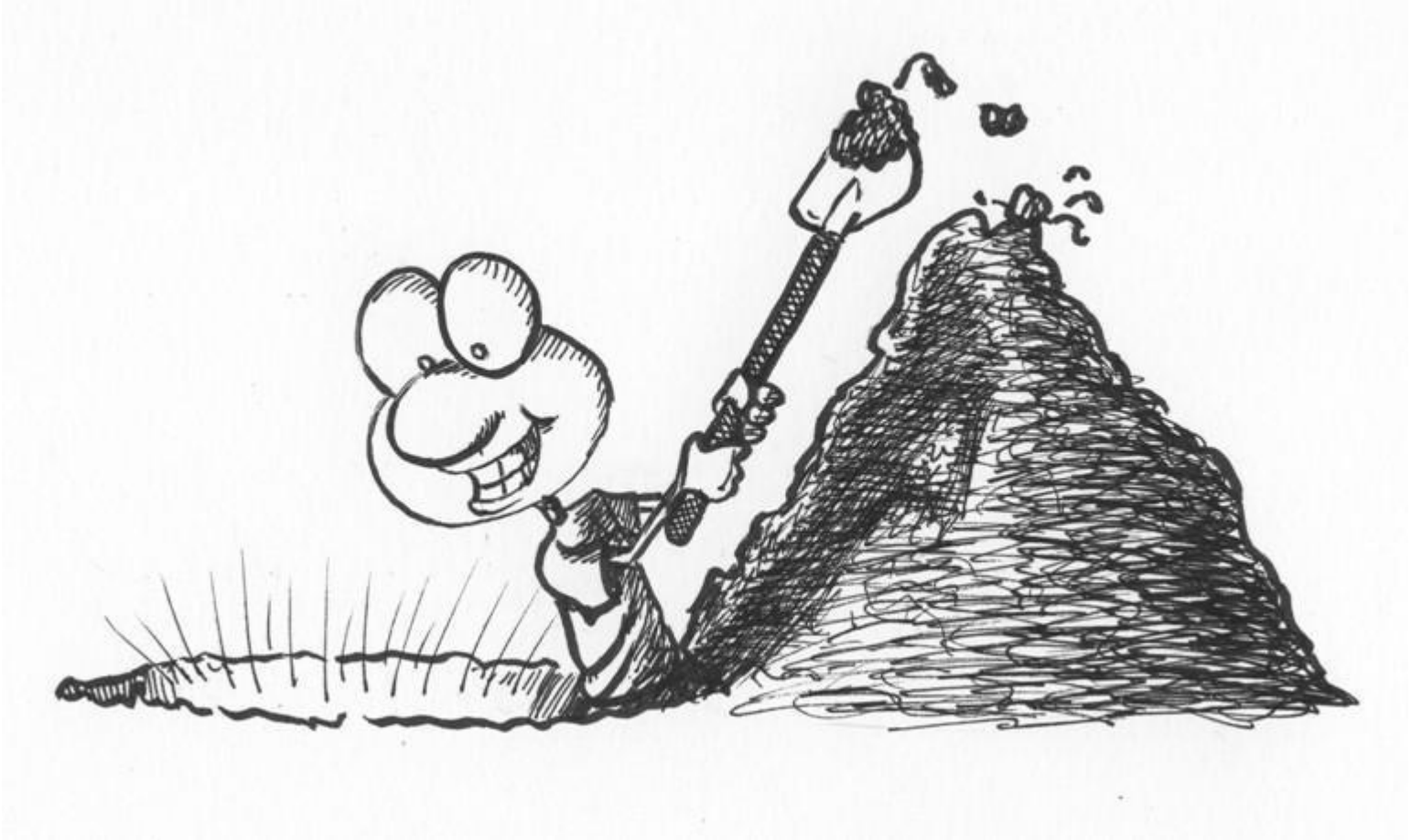
Model

Training and Conversion…



Let’s look at the process (FaceSwap Demo)

DEMO TIME!

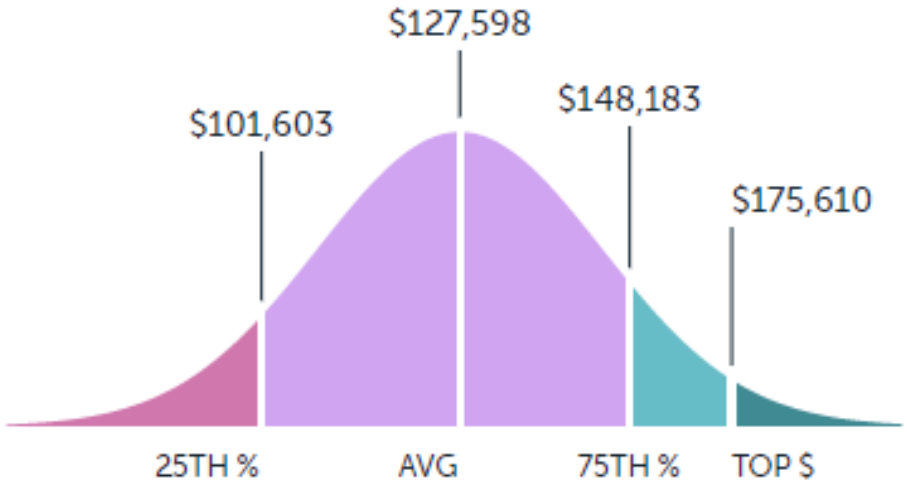


CAREER OPPORTUNITIES

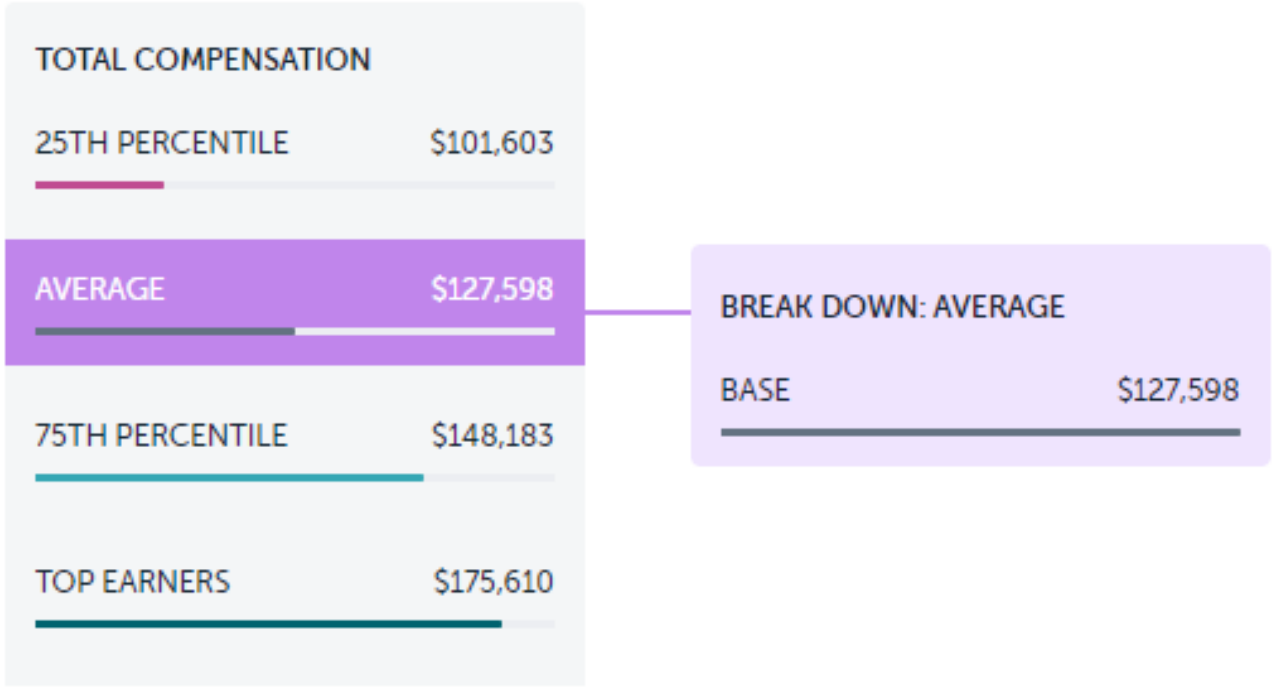
- Data Science Research
- Malware Analysis
- Threat Intelligence
- Deepfake Research
- IDS/IPS Design
- Email Security
- Network Traffic Analysis
- User Behavior Analytics

Salaries for Data Scientists

*This **is** a valuable skill.*



Salaries for Senior Data Scientists



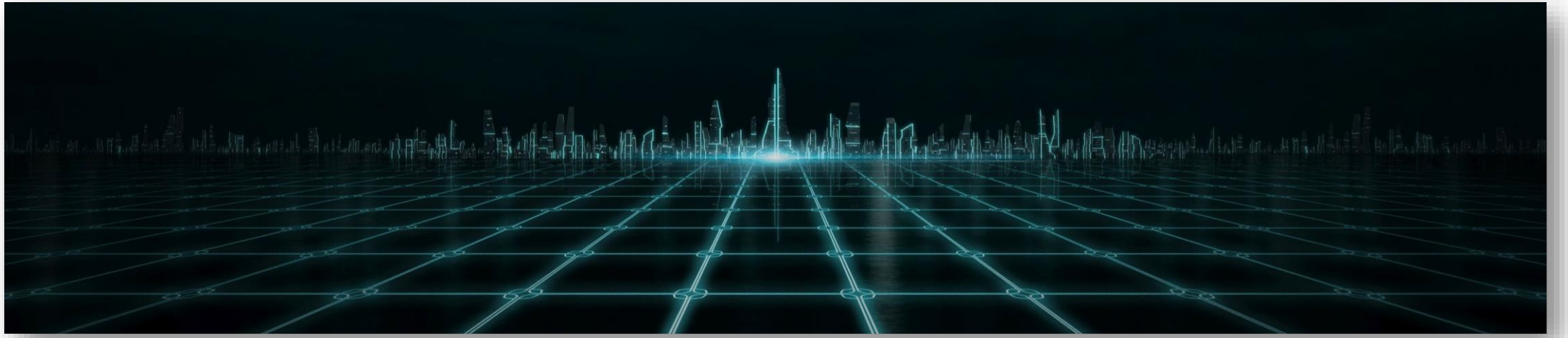
Source: https://www.paysa.com/salaries/senior-data-scientist--t

BUILDING YOUR SKILLSET - ALYSSA'S RESOURCE LIST

- **MIT 6.S191 Intro to Deep Learning** http://introtodeeplearning.com/
- **Hiding Faces in Plain Sight** https://arxiv.org/pdf/1906.09288.pdf
- **TensorFlow Learning** https://www.tensorflow.org/learn
- **Introduction to Adversarial Machine Learning** https://mascherari.press/introduction-to-adversarial-machine-learning/
- **Generate Fake Videos with GANs** https://www.peerlyst.com/posts/how-to-generate-fake-videos-with-generative-adversarial-networks-deepfake-chiheb-chebbi
- **Learn Data Science by Analyzing COVID-19** https://blog.rmotr.com/learn-data-science-by-analyzing-covid-19-27a063d7f442

HOW DO I GET THERE?

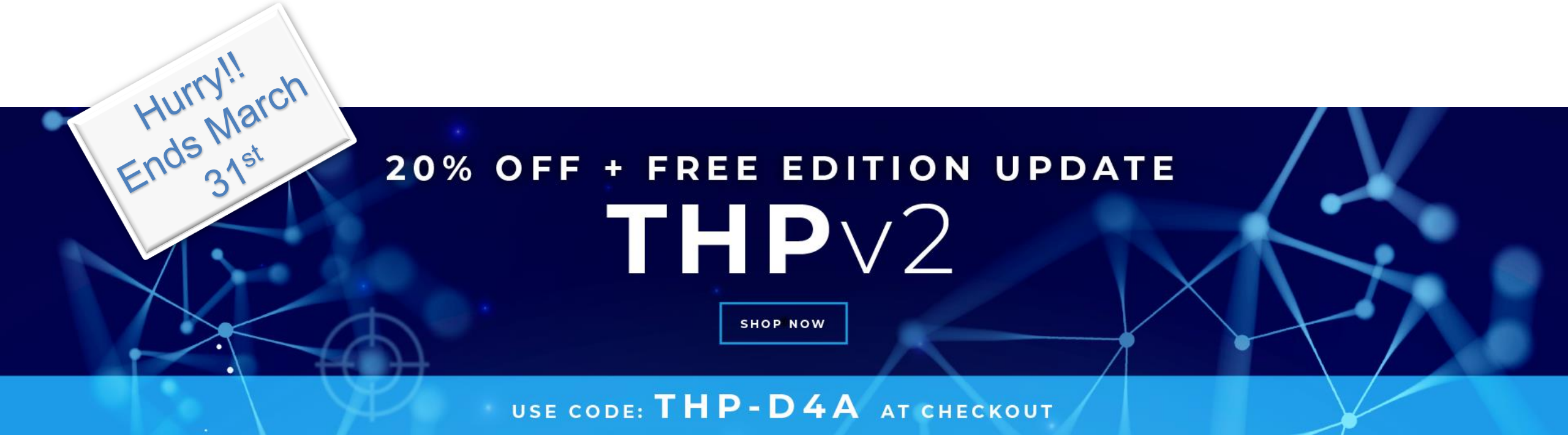
- Tech to Know – FaceSwap, Python, Google Colab/Jupyter, TensorFlow, etc.
- Practical Training – AWS Machine Learning, Azure AI, TensorFlow.org, RMOTR, edX
- Experience – Employment, Home lab, Non-profits, Open source projects, etc.
- Soft Skills – Conferences, Local meetups, social media, your own blog, mentors…



CONTACT ALYSSA

- https://alyssasec.com/
- Twitter (@AlyssaM_Infosec)
- LinkedIn (/in/alyssam-infosec)

eLS Special Discount!



https://www.elearnsecurity.com

Virtual IoT Village - IoT Hacking 101

Thursday April 23, 2020 @ 1:00 PM EST

Village ID/IOT Labs is a Canadian registered Non-Profit Organization (NPO) and was founded on these three simple pillars:

1. To promote awareness of security vulnerabilities and defenses against such vulnerabilities
2. To advance education by providing workshops, seminars and training programs on existing, new and emerging security topics
3. To conduct research and development in the pursuit of responsible disclosure through security vulnerability discovery

Guests, Dates & Topics Subject to Change

Q&A

POST GAME IN EH-NET GROUPS

THANK YOU

FOR JOINING

EH-NET Live!

THE ETHICAL HACKER NETWORK

Follow us:

www.ethicalhacker.net
team@ethicalhacker.net