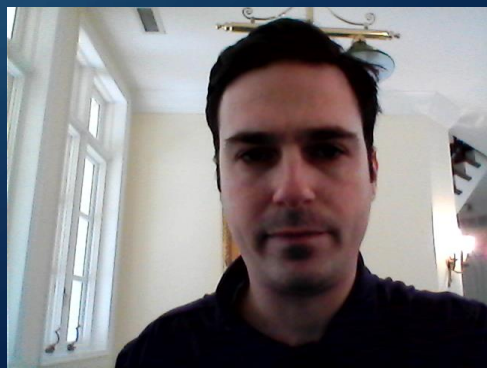
MALWARE DETECTION WITH MACHINE LEARNING

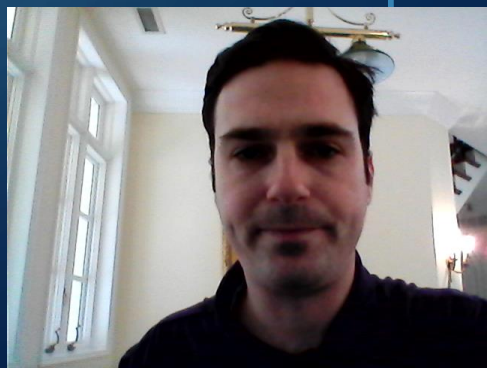
BRETT LUSKIN

DATA 606 – CAPSTONE SPRING 2020



PURPOSE

- Apply Machine Learning methods to cybersecurity
- Compare and interpret results
- Manage a data science project from beginning to end



UNSW-NB15 DATASET

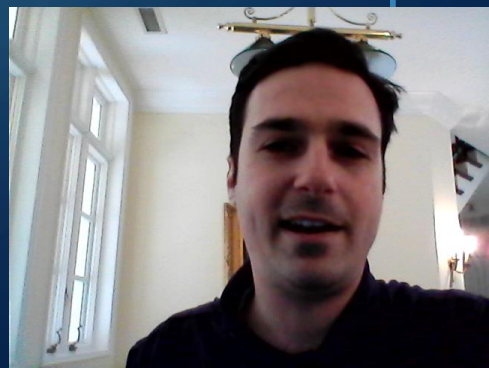
- Cyber Range Lab of the Australian Centre for Cyber Security (ACCS)
- Real network data mixed with synthetic attack data
- 49 unique features including label

DOMAIN KNOWLEDGE

What is this?

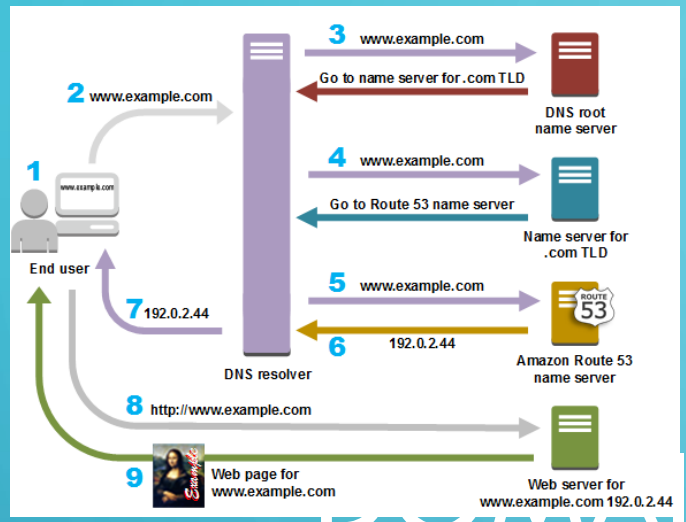
DOMAIN KNOWLEDGE

What is this?



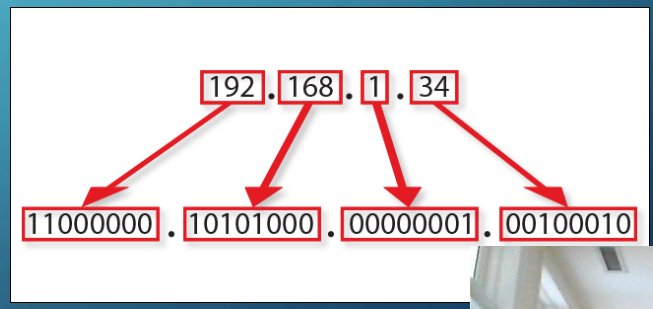
DOMAIN KNOWLEDGE

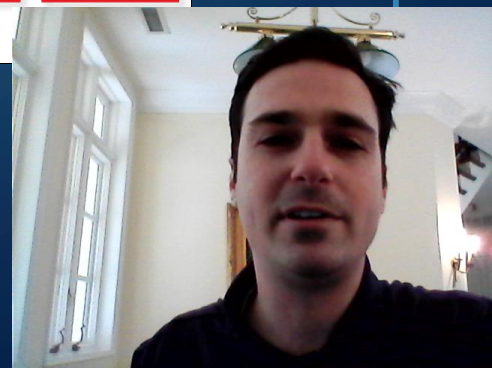
What is this?

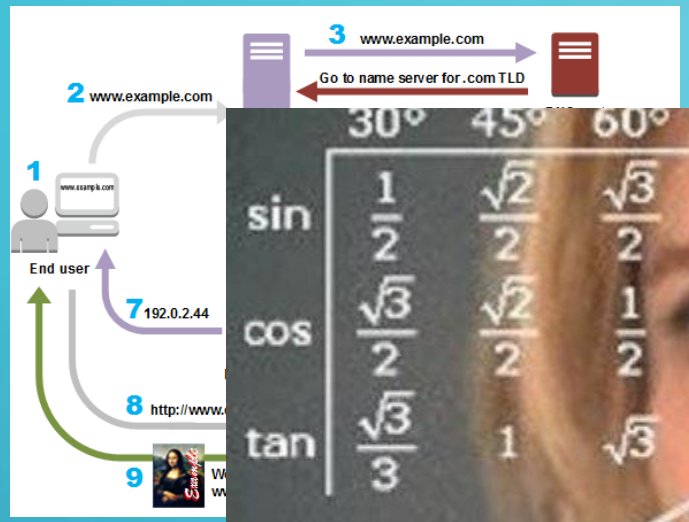


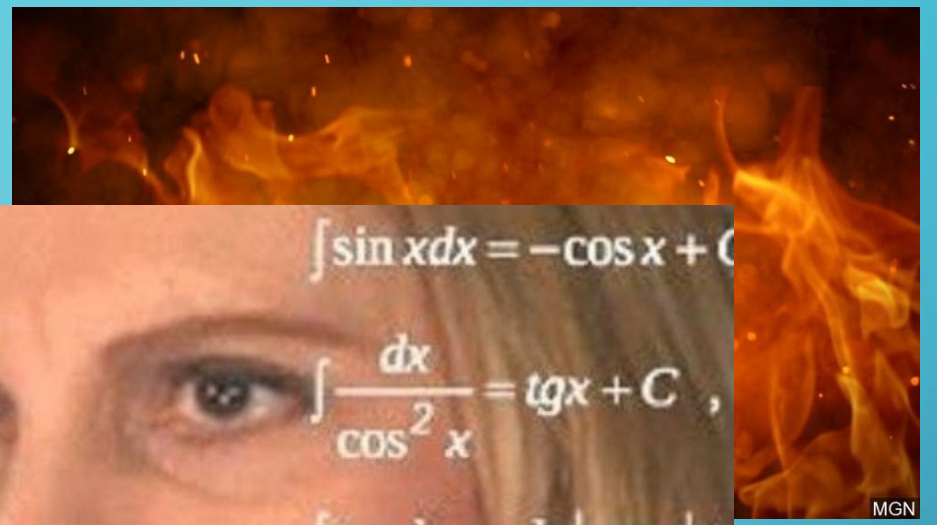
DOMAIN KNOWLEDGE

What is this?

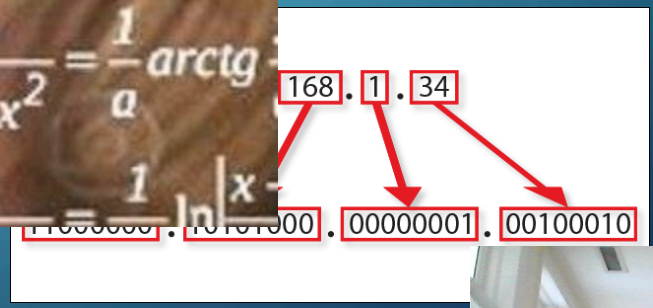


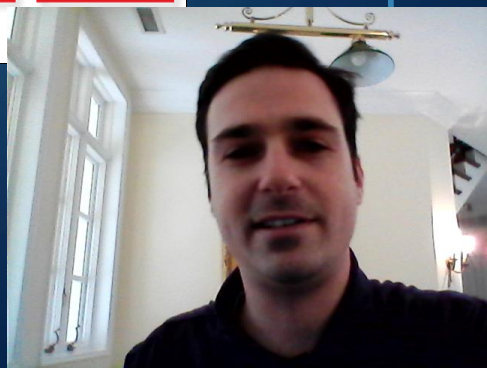



3 www.example.com
Go to name server for .com TLD
2 www.example.com
1
End user
7 192.0.2.44
8 http://www.
9


MGN

30° 45° 60°
sin 1/2 √2/2 √3/2
cos √3/2 √2/2 1/2
tan √3/3 1 √3
2x
60°
x
30°
x√3
45°
∫ sin x dx = −cos x + C
∫ dx / cos² x = tg x + C ,
∫ tg x dx = −ln|cos x| +
∫ dx / sin x = ln|tg x/2| + C
∫ dx / (a² + x²) = 1/a arctg
∫ dx = 1 ln|x


168 . 1 . 34
00000001 . 00100010



BENCHMARKS

- ML algorithms implemented
- Researched precision, accuracy, recall matched
- Neural Network implemented
- Attempt methods not available in research

REFERENCES

- UNSW-NB15 Dataset:
  - https://www.unsw.adfa.edu.au/unsw-canberra-cyber/cybersecurity/ADFA-NB15-Datasets/