A DECEPTICON and AUTOBOT walk into a bar: A new Python tool for enhanced OPSEC

Joe Gray

Senior OSINT Specialist, QOMPLX; Principal Trainer, The OSINTion

A DECEPTICON and AUTOBOT Walk into a Bar

A new Python tool for enhanced OPSEC

About Me

- Senior OSINT Specialist at QOMPLX by day
- Some experience with Python scripting
- Extremely interested in Data Science (Machine Learning and Natural Language Processing specifically)
- Frequent competitor in the Trace Labs Missing Persons OSINT Search Party (on 2nd place team for Global Search Party V in July)
- Passionate about OPSEC and OSINT
- Volunteer/Advisory positions with National Child Protection Task Force and **Operation: Safe Escape**

I am not…

- A programmer or developer
- A mathematician or data scientist
- An expert when it comes to trafficking or domestic violence

Definitions

- OSINT (Open Source Intelligence): intelligence gathered from overt or public sources
- OPSEC (Operations Security): the act or activities of masquerading one's own information presence (attack surface) and takes steps to obscure or eliminate the data or use disinformation/deception to make the data unreliable
- DECEPTICON: A term I applied to OPSEC through disinformation and deception in presentations over the past few years
- ML (Machine Learning): Study of math and algorithms to improve automation via 'learning' from a test dataset that enables the model and influences predictions and decisions
- Data Science: An amalgam of several disciplines that seek to use processes, programs, structures, and mathematic algorithms to gain insight from data
- AI (Artificial Intelligence): Study of 'intelligence' shown by machines through programming to attempt to mimic natural intelligence to reach desired outcomes or cognitive results
- GPU (Graphics Processing Unit): specialized system to accelerate the processing of images or video; commonly used in ML to speed up processing

The Problem:

One of the leading ways that adversaries find their ways into the lives of their victims is via social media.

Examples of “Adversaries”

- Malicious people seeking financial gain
- Nefarious people seeking to harm the victim
  - Abusers
  - Traffickers
  - Nation-States
  - Political Opponents
- Adversaries “of opportunity”

Examples of Victims:

- Public Figures (Politicians and Executives)
- Victims of domestic abuse and/or trafficking
- People with poor or misguided OPSEC

Dissecting possible advice from an OPSEC perspective:

- Simply abandoning the account is not always feasible
  - It could cue the adversary in on this and encourage them to find any alternative accounts
  - Some people have to use social media for work
  - Why should a victim have to live their life in fear?
  - Some victims are not aware of the adversary until it’s too late

More Dissection

- Even if the victim blocks the abuser, there are methods for them to continue to cause trauma:
  - The Abuser using fake accounts
  - Friends and Friends of Friends
  - Reporting alternate accounts for being fake
  - Passwords can still be reset
  - Companies can still be exploited

As an OSINT investigator, I am more skeptical of OSINT subjects that do not have any social media presence than of those with some

Why not have autonomy and agency over what is posted with minimal effort?

The Code

GitHub Repo (same link; 1 is just shorter if you need to jot it down):

- https://github.com/jocephus/DECEPTICON_Bot
- https://osint.mobi/2OzkCyG

The code

- Written in Python
- One version leverages Tensorflow and Keras (as written now, the NVIDIA port of Tensorflow 2.20); the other uses PyTorch, but is not discussed in this presentation
- Uses Pandas Python package to organize the data in data frames
- Within the implementation in the code, a Long Short Term Memory model (LSTM) is used to generate the text
- The Keras Python package is the vehicle for the LSTM

What is a Long Short Term Memory model?

An LSTM is a type of Recurrent Neural Network (RNN)

What is an RNN?

- An RNN is a type of Neural Network that takes into account past decisions and those decisions influence the outcome. They also have the capability to remember previous things learned. (*Source: Towards Data Science*)
- Unlike a traditional Neural Network, RNNs are not of a fixed vector size, which is ideal for processing text, speech, and images.

- An LSTM is a type of RNN that learn order dependencies and perform sequence prediction. (*Source: Machine Learning Mastery)*
- LSTMs are popular for Natural Language Processing because of the sequence prediction and dependency analysis

How Does This Work?

- We use a set of Twitter API keys and the Python-Twitter package to authenticate to Twitter and pull down all of the tweets for the user. By default, the tool only reads the tweets of the owner of the API keys, but could be modified to read anyone's tweets as long as the account tied to the API can view them.
- From here, we capture the text and time of the tweet and measure lexical diversity (LD). Lexical diversity is the ratio of the words used to the length of the text (this will become more import in subsequent iterations and forks). The time, text, and LD are written to the data frame.
- The tweets are tokenized (separated into words; an alternative method would be to tokenize the sentences) and added to the corpus (Bag of Words)
- We collect more stats on the text of the tweets (standard stats as well as **post_interval**) and move into the generate module

How Does This Work? (cont.)

- In the generate module, we establish our vector sizes and sequences. We also measure the number of unique patterns in the corpus (Bag of Words)
- In premodeling, we set up files associated with the model (so the tool can learn from it). We also define the model and the associated parameters.
- We move into the trainer module to establish a pseudorandom seed to begin the tweet generation from.
- We use the tweet_creator module to execute the model and assess the predictions
- Next, we have the logic check, this is where we ensure that the text is short enough to be able to tweet and we also remove links and known characters to occur (those not common to normal written text).
- After this, we tweet.

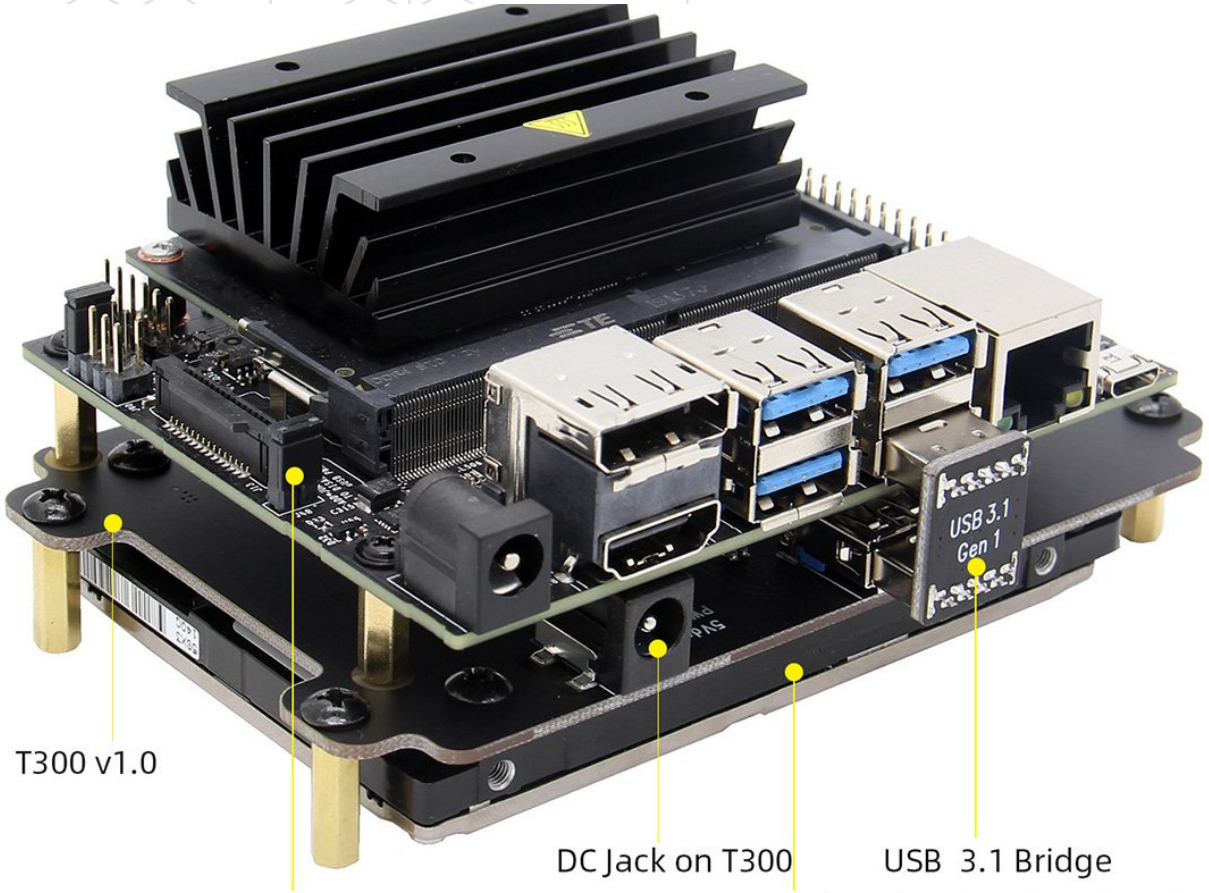
Demonstration

The Project

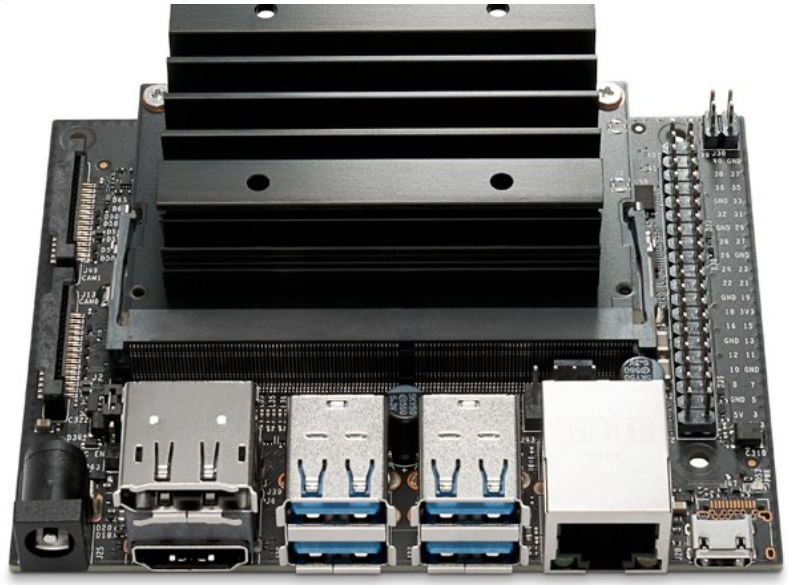
- Started around December 2019
- Many hurdles, shiny objects, delays, etc.
- I had written some tools in Python (i.e. WikiLeaker and associated Recon-ng module)
- I had been reading about NLP and ML and how to implement the disciplines in Python
- Started doing some work with Operation: Safe Escape

The Project (cont.)

- Around March, the project stalled.
- I was introduced to the NVIDIA Jetson platform for AI and Machine Learning
- I ported the code over and resumed developing the tool
- The VM I was developing it in wasn't 'weak' but it wasn't efficient either
- 3 cores, 8GB RAM, Radeon GPU
- Running on 2017 Macbook Pro 15"

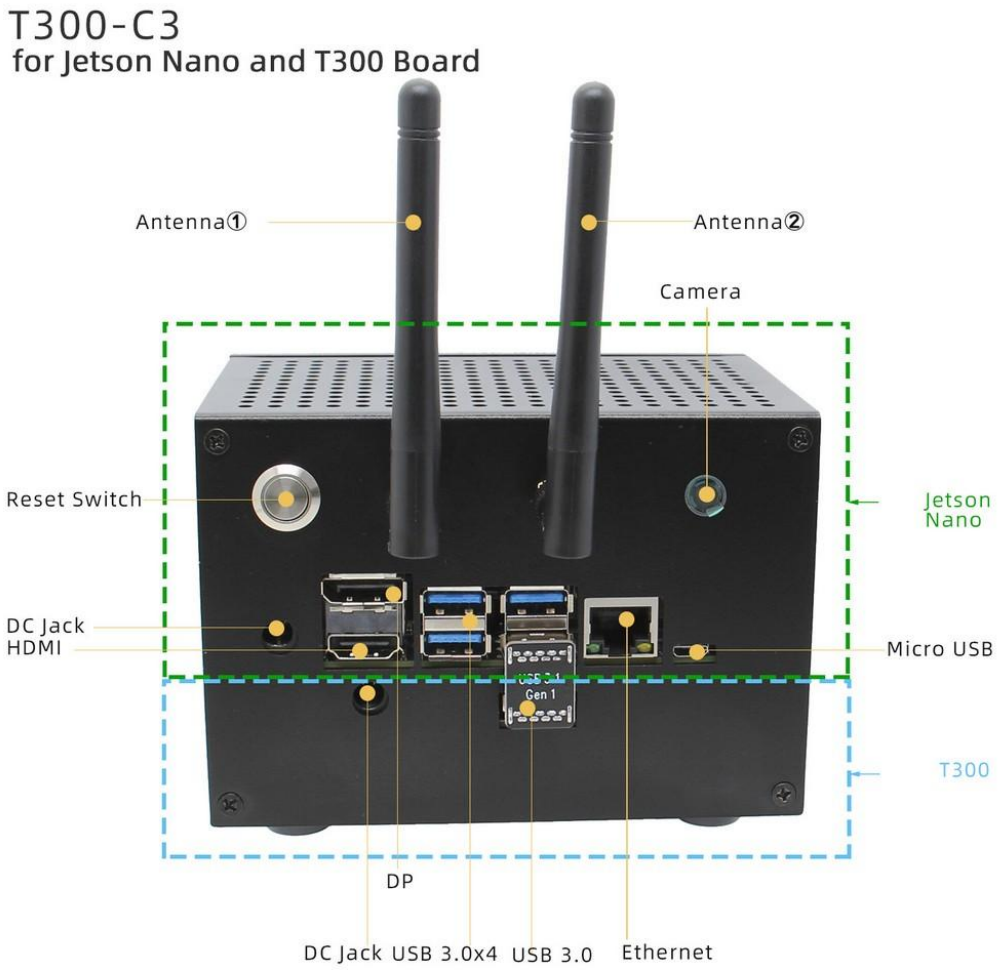

USB 3.1
Gen 1
T300 v1.0
DC Jack on T300
USB 3.1 Bridge


JETSON NANO
DEVELOPER KIT



Specs:

- Quad Core 64-bit ARM processor
- 4GB 64-Bit DDR4 RAM
- Linux Tegra Support
- 128-core (Cuda) Maxwell GPU



Why the Jetson platform?

- External to my regular host
- Has the enhanced GPU with cuda cores to expedite the analysis
- Recommended by a friend for other data science research

Lessons Learned

- Data Science is no walk in the park – especially if you lack a heavy math background
- PyTorch is faster than Tensorflow, but less reliable in output
- If testing such a bot on your regular account, ensure that you have tweeted some things of substance as of late
- If you don’t want to have to make modifications to the code, tweet fairly regularly
- People often get confused when you start tweeting poems and song lyrics to influence your corpus (Songs: All Star and Never Gonna Give You Up; Poems: Jabberwocky, The Raven, Still I Rise, Waste Land, and We Wear The Mask)
- When dealing with NLP and ML, there is a lot of A/B testing and hypothesizing
- ~200 tweets at around 280 characters each is a VERY SMALL data set for an LSTM

Limitations:

- As of right now, the code is written to make use of GPUs and cuda cores. Running this on a VM or server will be very time consuming. Leasing GPU processing in the cloud is VERY expensive
- The LSTM model is dependent upon what your account has posted. If you wiped the account or just set it up, you will need to get something posted for it to work off of.

Questions?

Contacting Me

- Contacting Me:
  - Twitter: @C_3PJoe
  - Email: jgray@theosintion.com
- Jetson Nano Amazon Idea List:
  - https://a.co/eZeJagi
- GitHub Repo (same link; 1 is just shorter if you need to jot it down):
  - https://github.com/jocephus/DECEPTICON_Bot
  - https://osint.mobi/2OzkCyG

Training Opportunities

- People OSINT
  - 2-day format
  - (7/30-31 6-9PM EDT)
  - 7/31-8/1 6-9AM SGT)
    - https://osint.mobi/32FGSQ0
  - 1-day format
  - (8/1 8PM-2AM EDT)
  - (8/1 8AM-2PM SGT)
    - https://osint.mobi/2OFKlWx

- Use code HITB1337 for 25% off

Thank You!

HITB LOCKDOWN 002
livestream

Joe Gray, jgray@theosintion.com