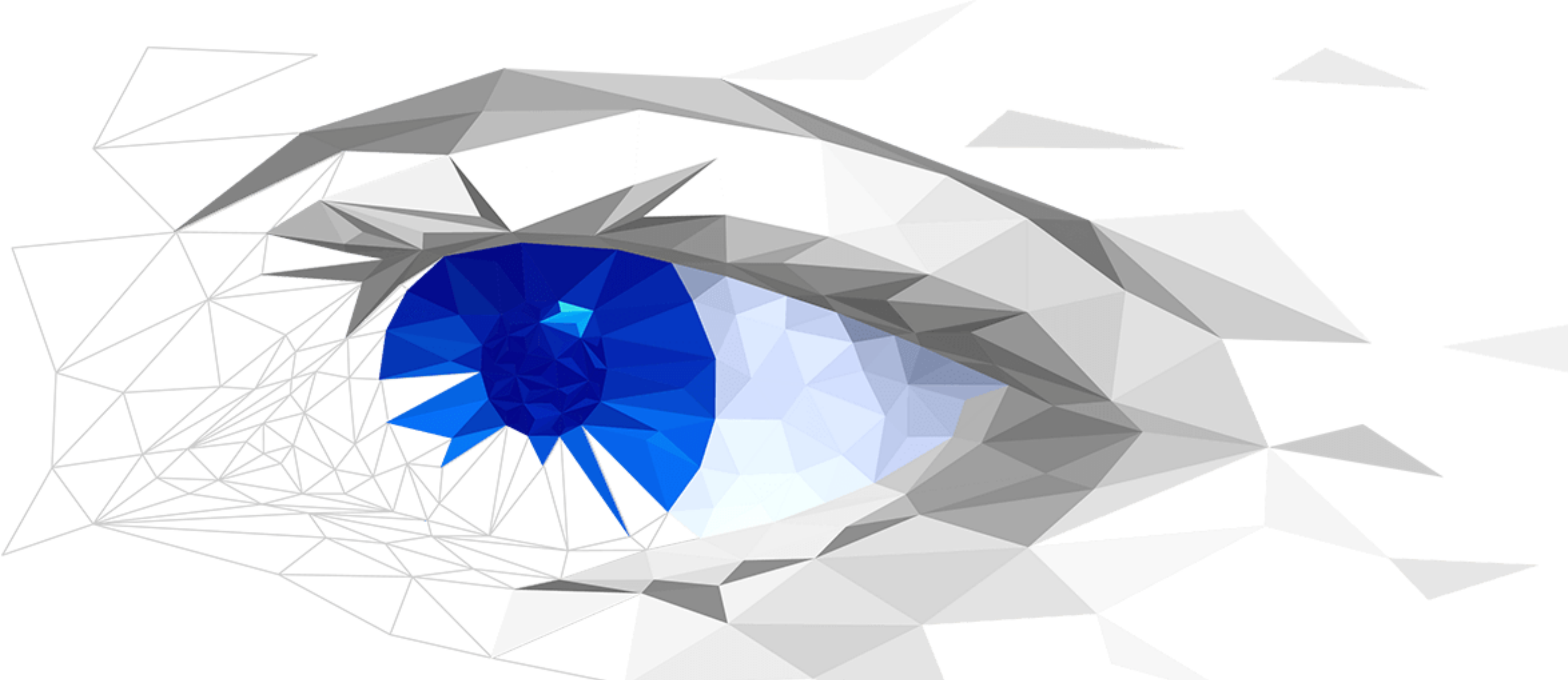


How I clone myself using AI

Tamaghna Basu, Co-Founder/CTO,

neoEYED Inc.

About Me

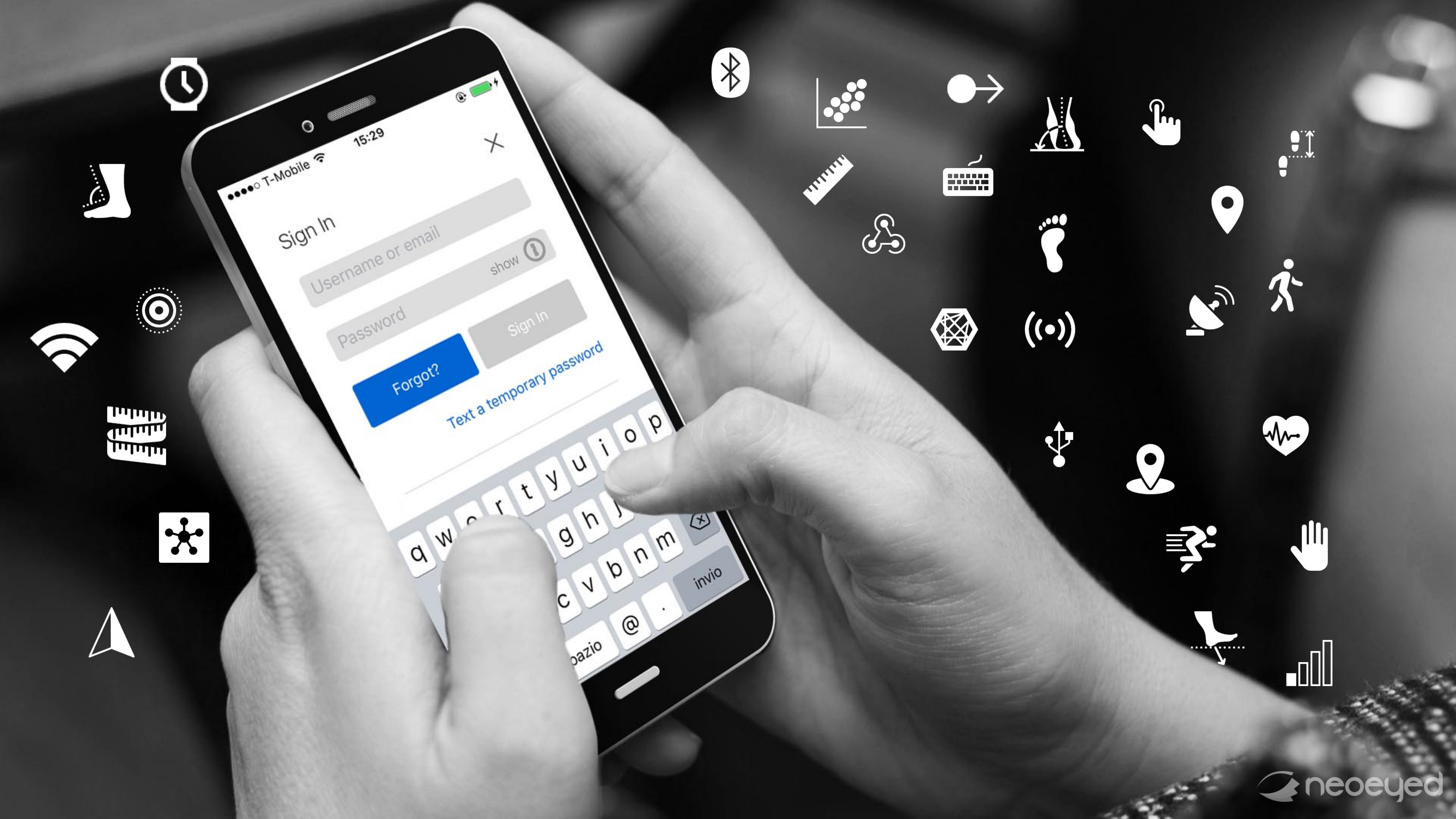
- *CTO/Co-Founder, neoEYED Inc. with 15+ years of experience*
- Startup Advisors, Mentor for Stanford cyber security course
- Cyber Security, Machine Learning, Python, java, .net, ruby etc. in domains like Finance, Insurance, Casino Gaming, eComm etc.
- Frequent speaker/trainer in international conferences like NULLCON, C0C0N, OWASP, ISACA, ISC2 etc.
- Member of NULL, DSCI and other communities.

Stanford University

GIAC CERTIFIED INCIDENT HANDLER
GCIH

OFFENSIVE® security

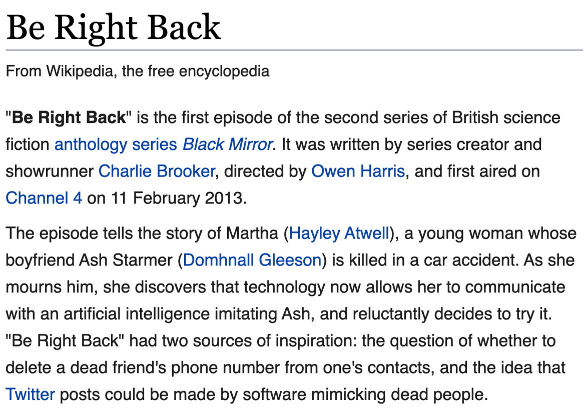
redhat.
CERTIFIED
ENGINEER


T-Mobile
15:29
Sign In
Username or email
show
Password
Sign In
Forgot?
Text a temporary password
invio
neoeyed

Agenda

- Background/Inspiration
- Demo – Text, Audio/Video
- Architecture: What’s happening behind the scene
- Code release – Notebook, Repository etc.
- What’s next – other approaches, future enhancements
- Our vision, invitation to contribute, support, learn
- References and Credits

Inspiration



Be Right Back

From Wikipedia, the free encyclopedia

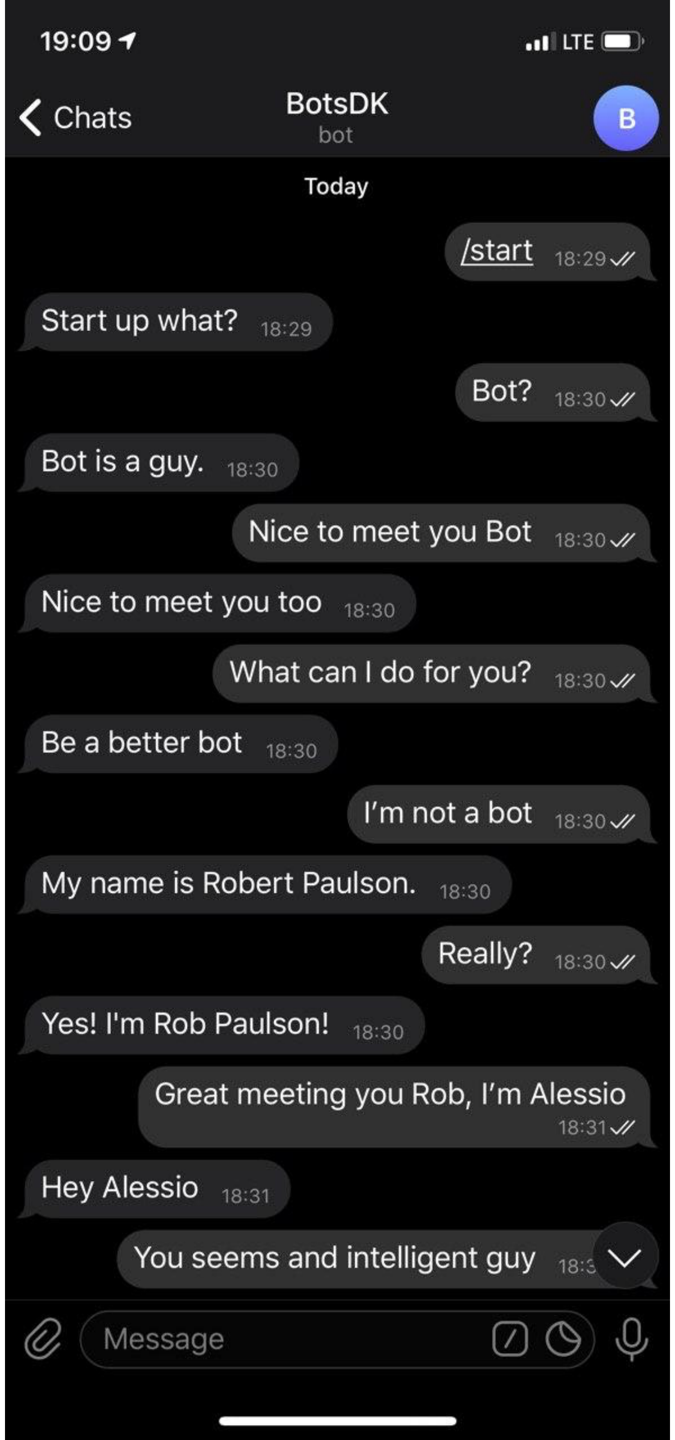
"**Be Right Back**" is the first episode of the second series of British science fiction anthology series *Black Mirror*. It was written by series creator and showrunner Charlie Brooker, directed by Owen Harris, and first aired on Channel 4 on 11 February 2013.

The episode tells the story of Martha (Hayley Atwell), a young woman whose boyfriend Ash Starmer (Domhnall Gleeson) is killed in a car accident. As she mourns him, she discovers that technology now allows her to communicate with an artificial intelligence imitating Ash, and reluctantly decides to try it. "Be Right Back" had two sources of inspiration: the question of whether to delete a dead friend's phone number from one's contacts, and the idea that Twitter posts could be made by software mimicking dead people.

https://www4.pictures.zimbio.com/mp/5b2LRQ2ouwsl.jpg

Chat Demo

Conversation - 1



/start 18:29

Start up what? 18:29

Bot? 18:30

Bot is a guy. 18:30

Nice to meet you Bot 18:30

Nice to meet you too 18:30

What can I do for you? 18:30

Be a better bot 18:30

I'm not a bot 18:30

My name is Robert Paulson. 18:30

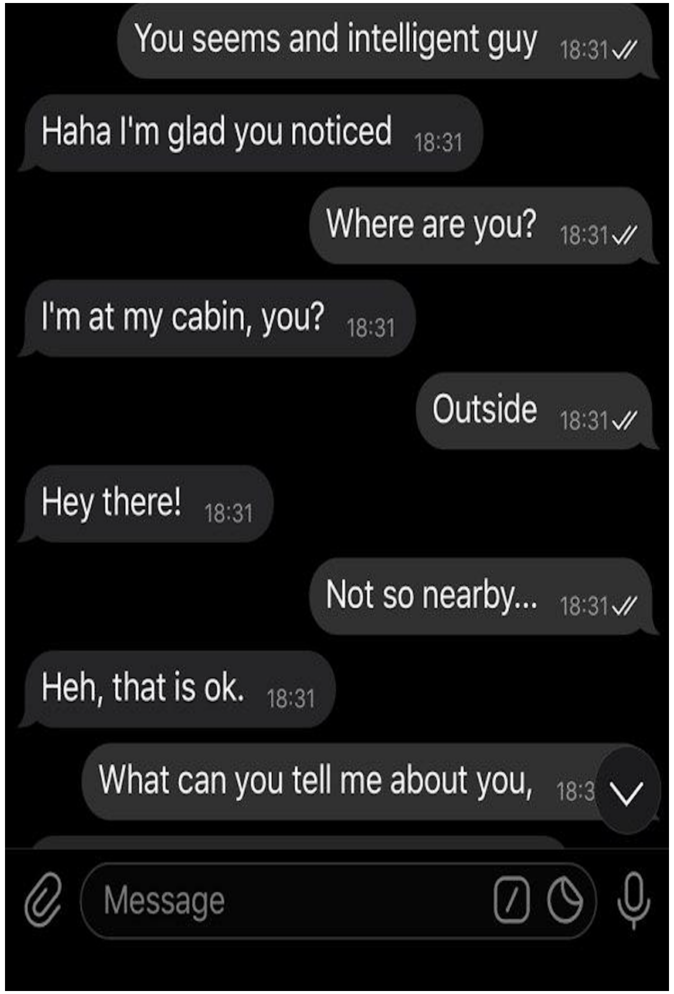
Really? 18:30

Yes! I'm Rob Paulson! 18:30

Great meeting you Rob, I'm Alessio 18:31

Hey Alessio 18:31

You seems and intelligent guy 18:3



You seems and intelligent guy 18:31

Haha I'm glad you noticed 18:31

Where are you? 18:31

I'm at my cabin, you? 18:31

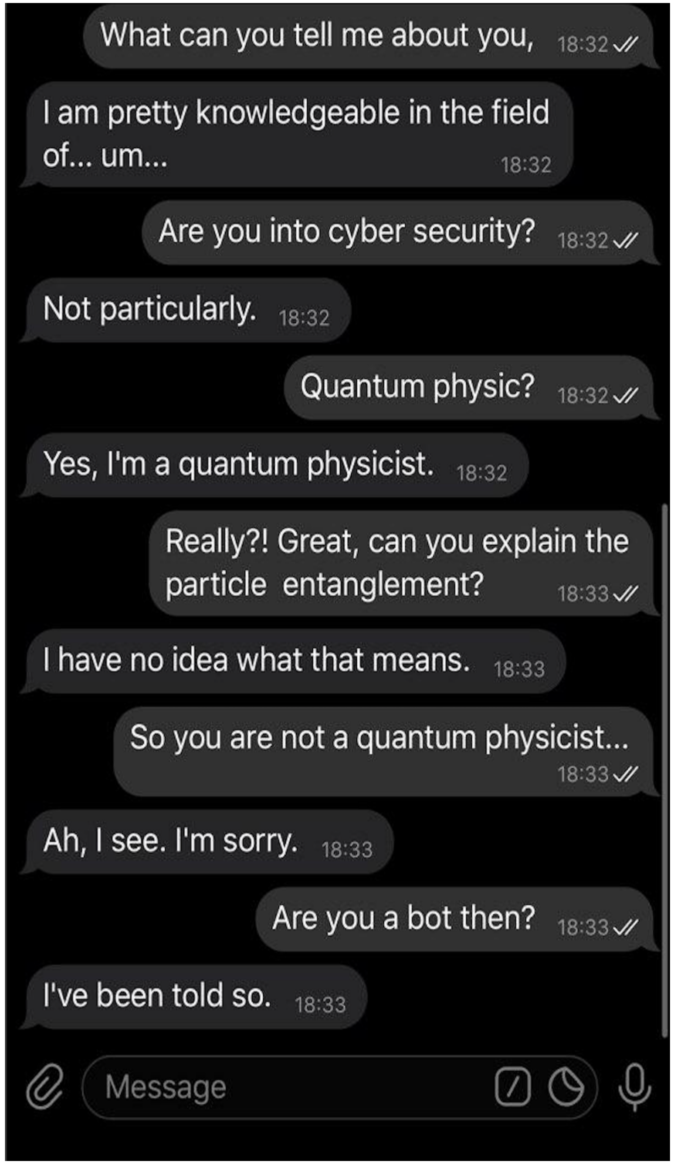
Outside 18:31

Hey there! 18:31

Not so nearby... 18:31

Heh, that is ok. 18:31

What can you tell me about you, 18:3



What can you tell me about you, 18:32

I am pretty knowledgeable in the field of... um... 18:32

Are you into cyber security? 18:32

Not particularly. 18:32

Quantum physic? 18:32

Yes, I'm a quantum physicist. 18:32

Really?! Great, can you explain the particle entanglement? 18:33

I have no idea what that means. 18:33

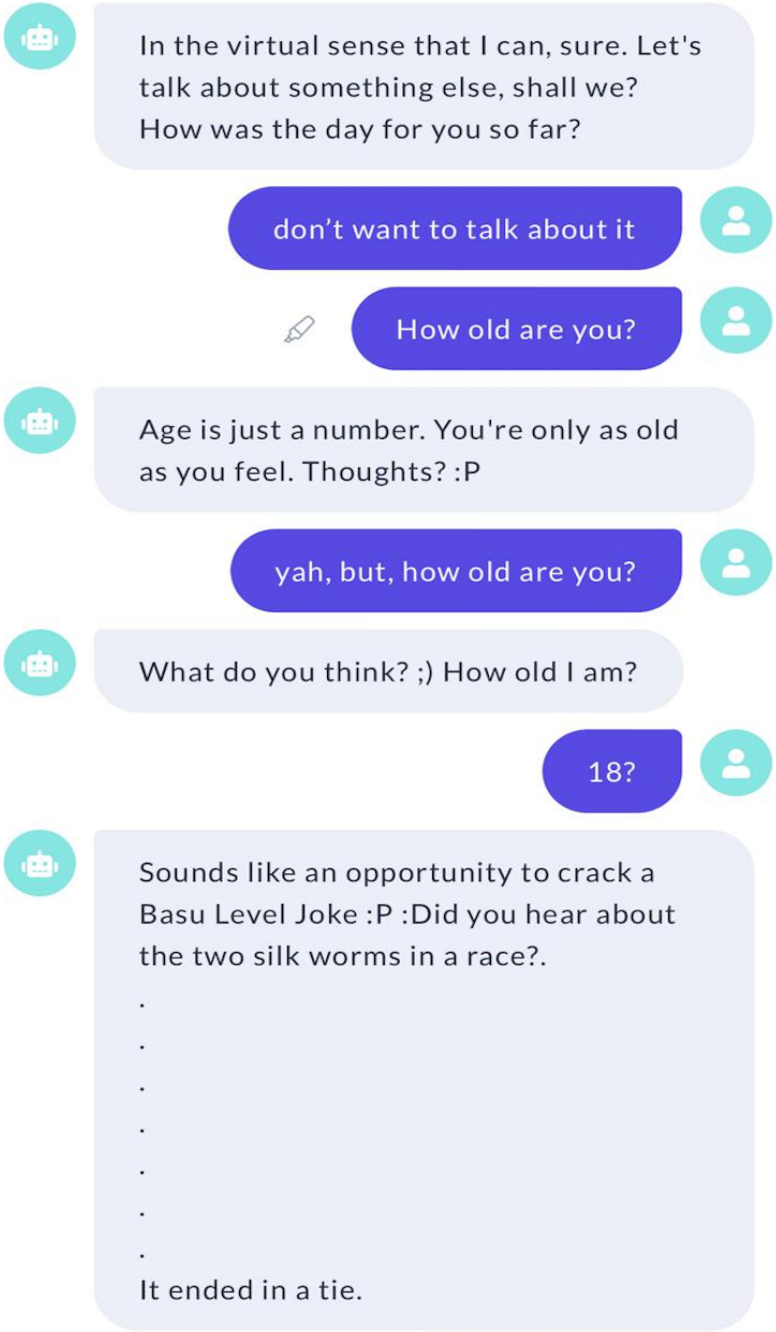
So you are not a quantum physicist... 18:33

Ah, I see. I'm sorry. 18:33

Are you a bot then? 18:33

I've been told so. 18:33

Conversation – 2, 3



In the virtual sense that I can, sure. Let's talk about something else, shall we? How was the day for you so far?

don't want to talk about it

How old are you?

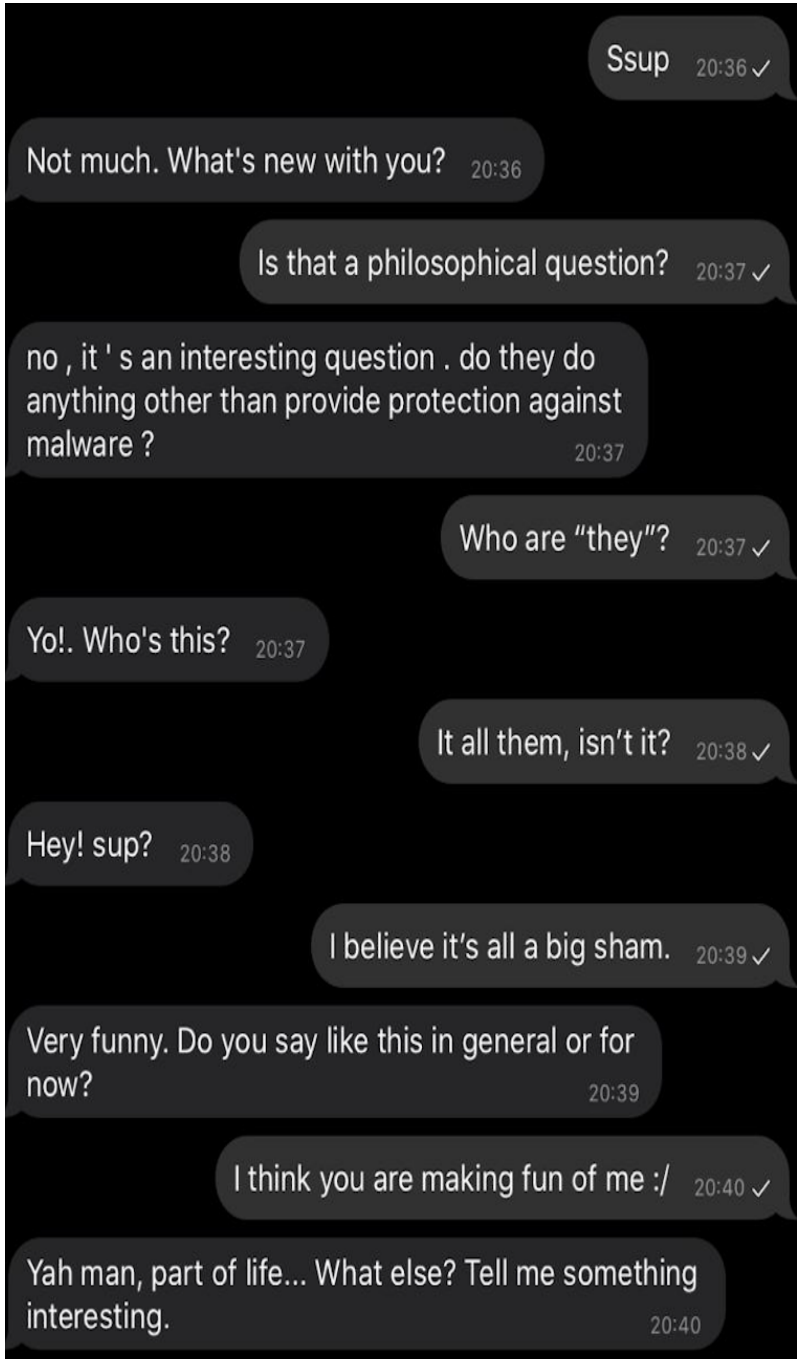
Age is just a number. You're only as old as you feel. Thoughts? :P

yah, but, how old are you?

What do you think? ;) How old I am?

18?

Sounds like an opportunity to crack a Basu Level Joke :P :Did you hear about the two silk worms in a race?.
.
.
.
.
.
.
.
It ended in a tie.



Ssup 20:36 ✓

Not much. What's new with you? 20:36

Is that a philosophical question? 20:37 ✓

no , it ' s an interesting question . do they do anything other than provide protection against malware ? 20:37

Who are "they"? 20:37 ✓

Yo!. Who's this? 20:37

It all them, isn't it? 20:38 ✓

Hey! sup? 20:38

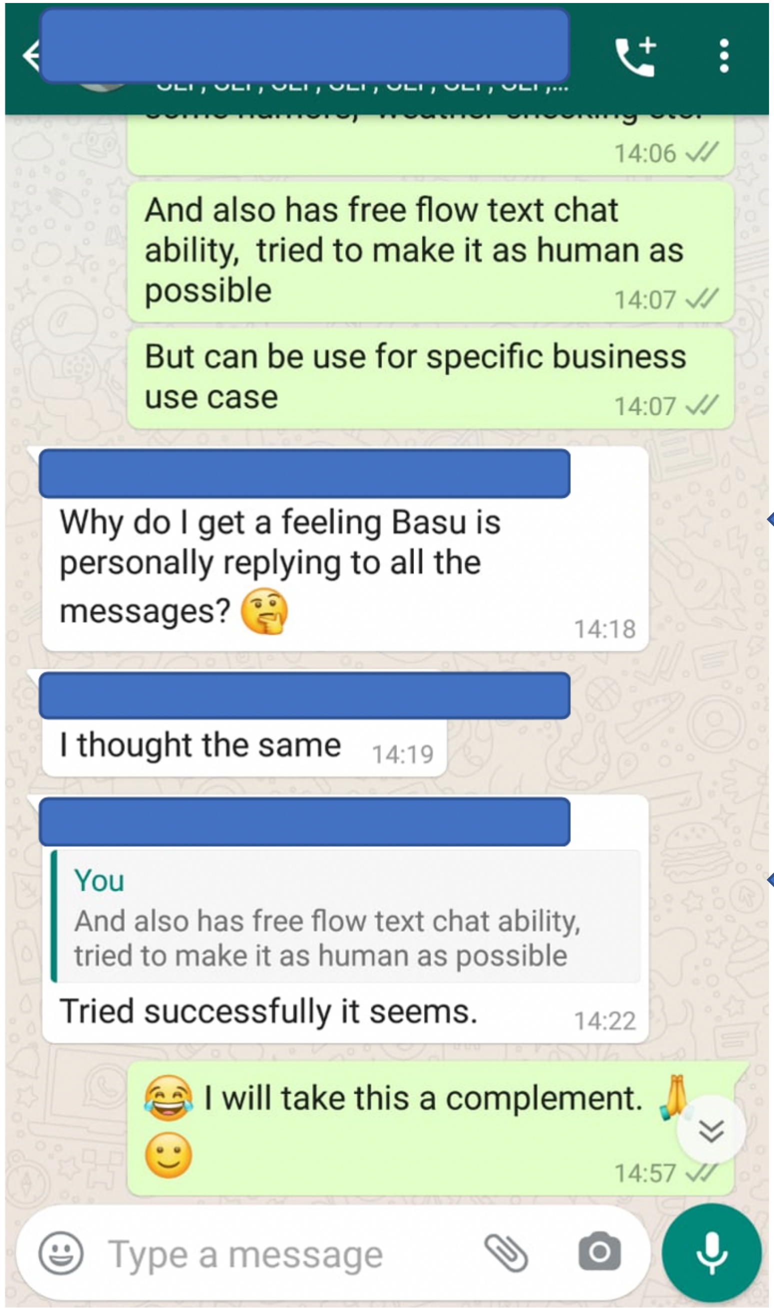
I believe it's all a big sham. 20:39 ✓

Very funny. Do you say like this in general or for now? 20:39

I think you are making fun of me :/ 20:40 ✓

Yah man, part of life... What else? Tell me something interesting. 20:40

Social Proof


[redacted]

14:06

And also has free flow text chat ability, tried to make it as human as possible 14:07

But can be use for specific business use case 14:07

[redacted]
Why do I get a feeling Basu is personally replying to all the messages? 🤔 14:18

[redacted]
I thought the same 14:19

[redacted]
> You
> And also has free flow text chat ability, tried to make it as human as possible

Tried successfully it seems. 14:22

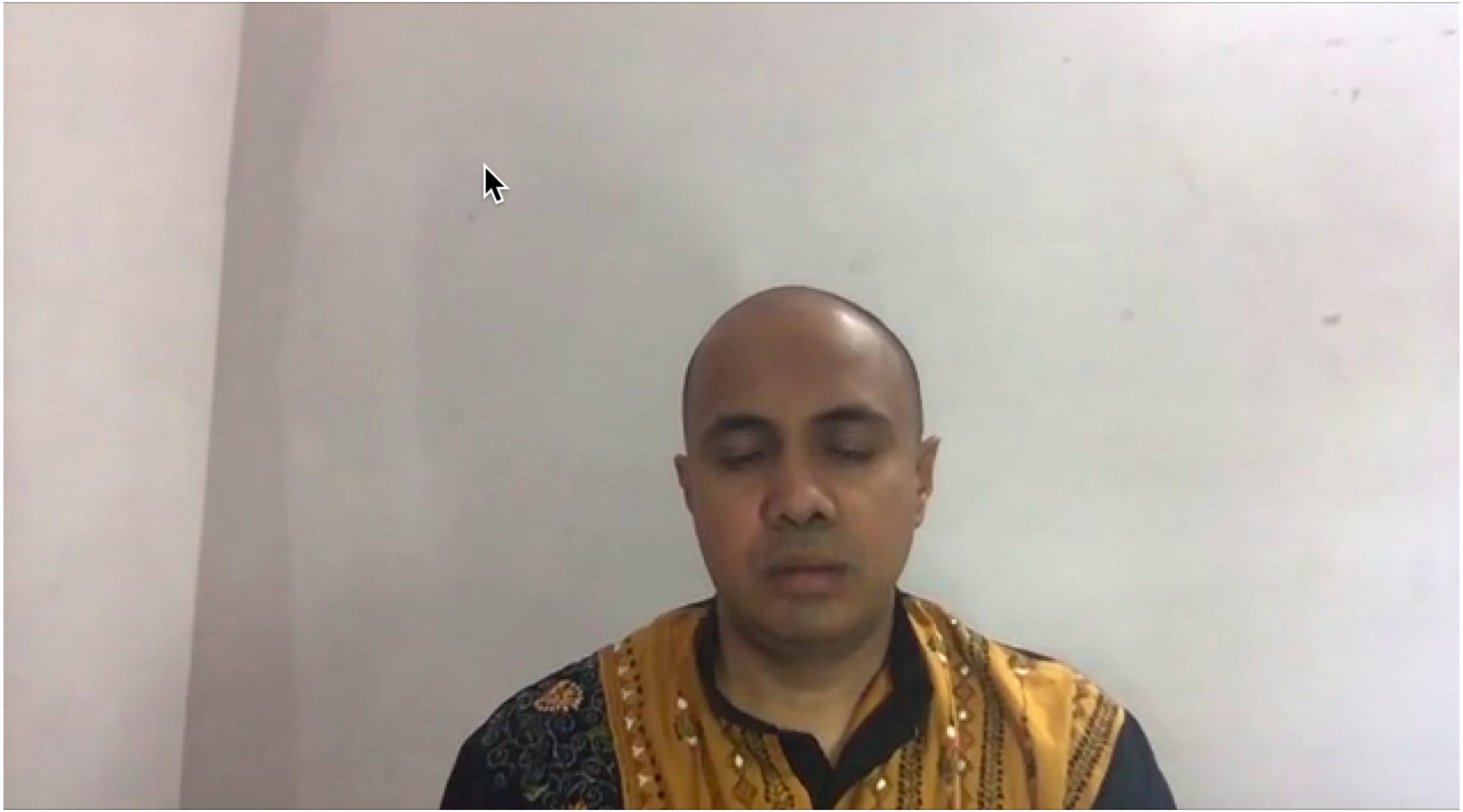
😂 I will take this a complement. 🙏
🙂 14:57

Person 1

Person 2

Person 3

Video Demo



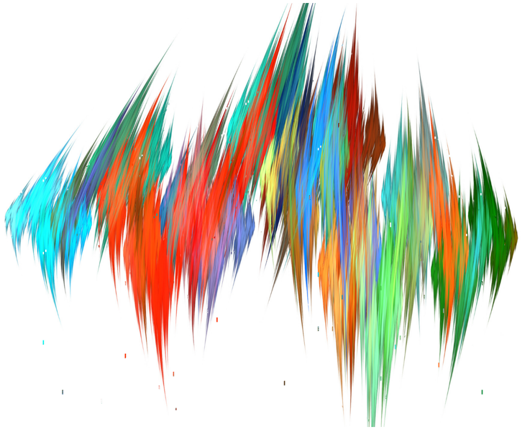
Architecture – What’s behind the scene

1. Flow Summary

The Brain

Text Chat Engine
(TCE)

The Voice



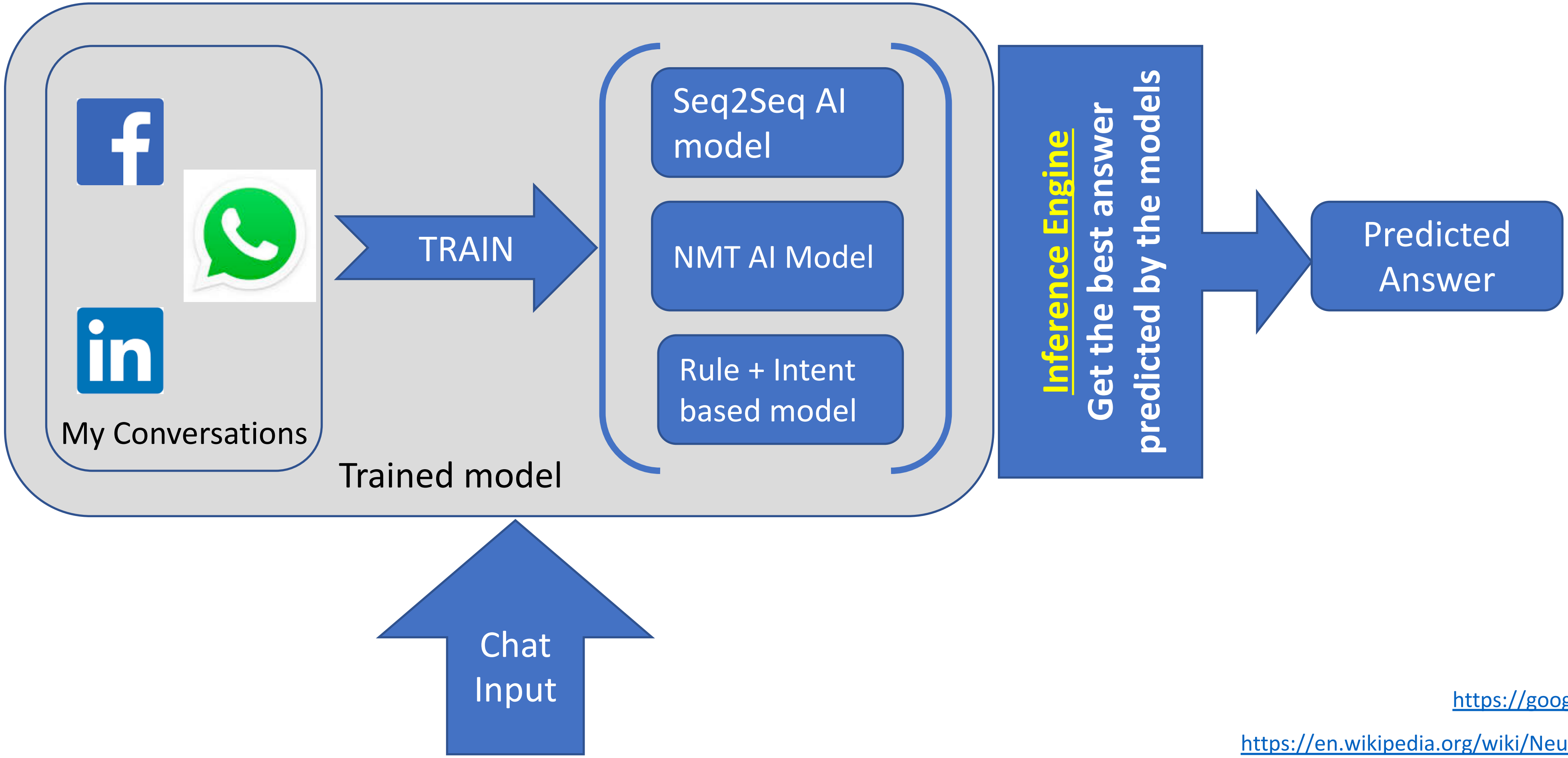
Audio Synthesis Engine
(ASE)

The Face

Video Synthesis Engine
(VSE)

The Brain

2. Text Chatbot Engine (TCE)



My Conversations

TRAIN

Seq2Seq AI model

NMT AI Model

Rule + Intent based model

Trained model

Chat Input

Inference Engine

Get the best answer predicted by the models

Predicted Answer

https://google.github.io/seq2seq/

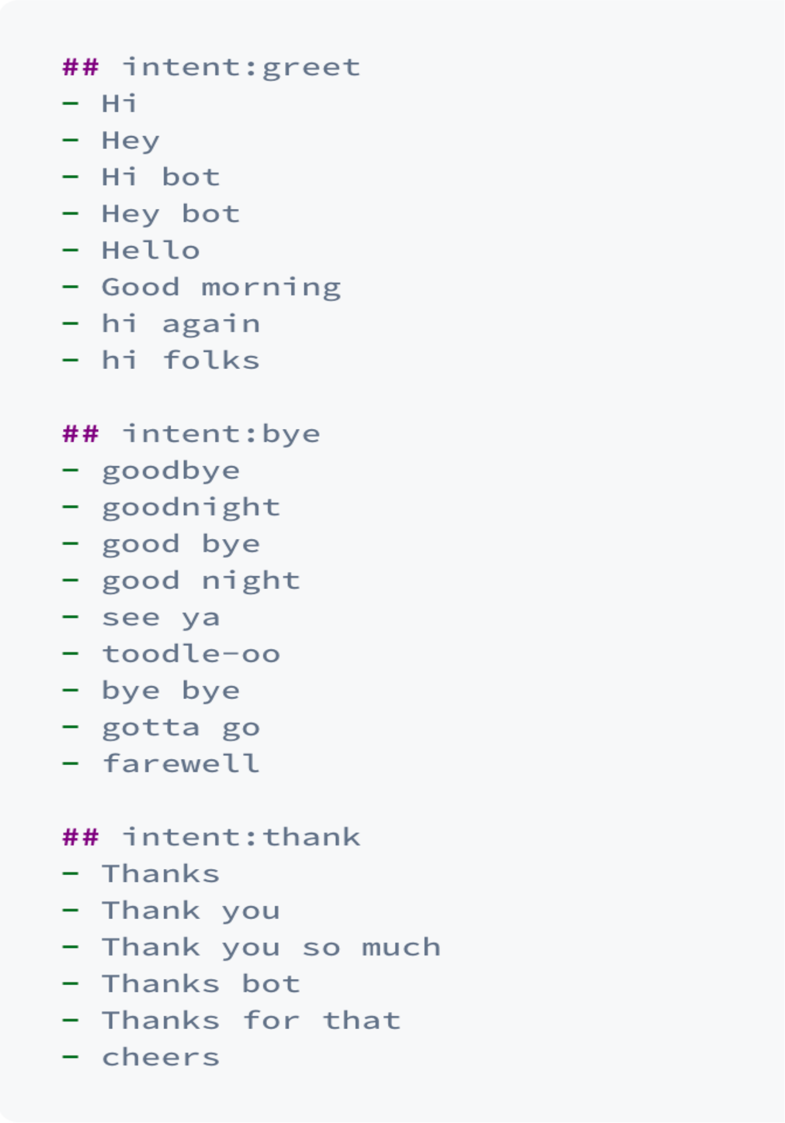
https://en.wikipedia.org/wiki/Neural_machine_translation

https://chatbotsmagazine.com/bot-talks-intent-based-vs-flow-base-conversations-798788dc9cf6

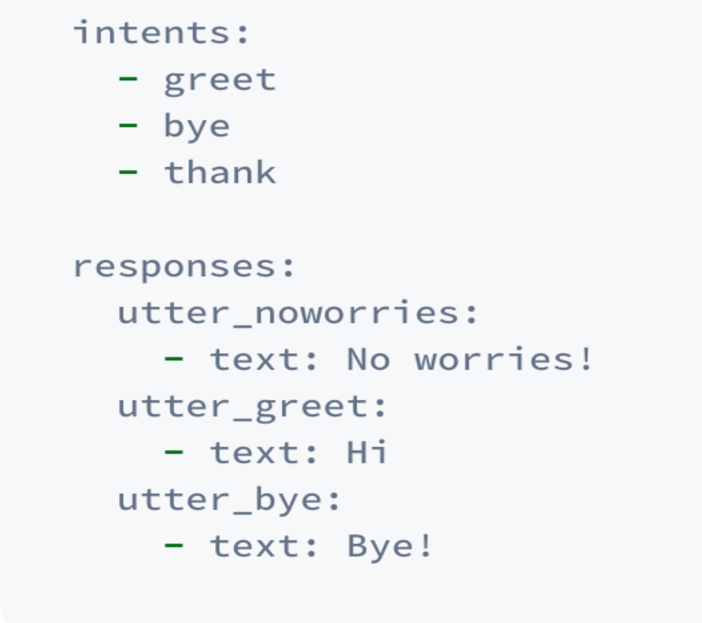
Categories of conversations

- Chit-chat **(CAT - I)**
- Historical **(CAT – II)**
  - “Can I come to your house today”
  - “Shall we meet tomorrow”
  - “Are you coming for the X meetup tomorrow”
- Topical, factual, asking for specific information **(CAT - III)**
  - How is the weather today?
  - What is SQLi
- Pure generative, philosophical, anything else aka free flow chat **(CAT – IV)**
  - What is love
  - What is the purpose of life etc.

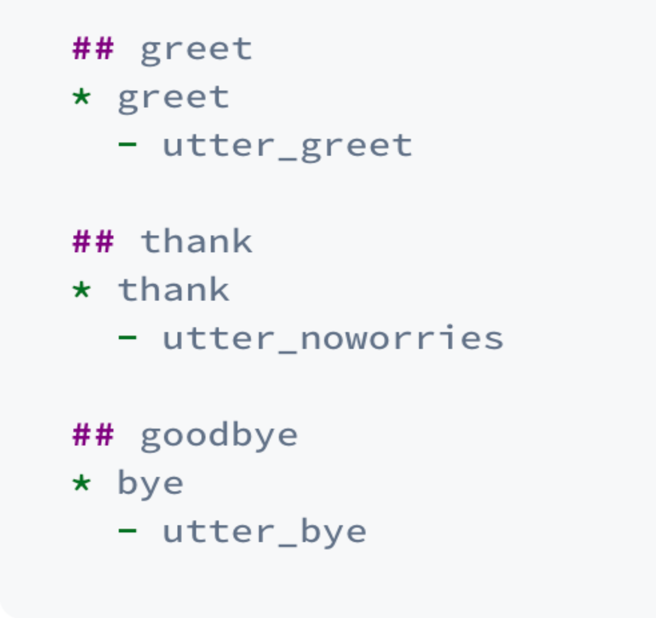
(CAT - I)



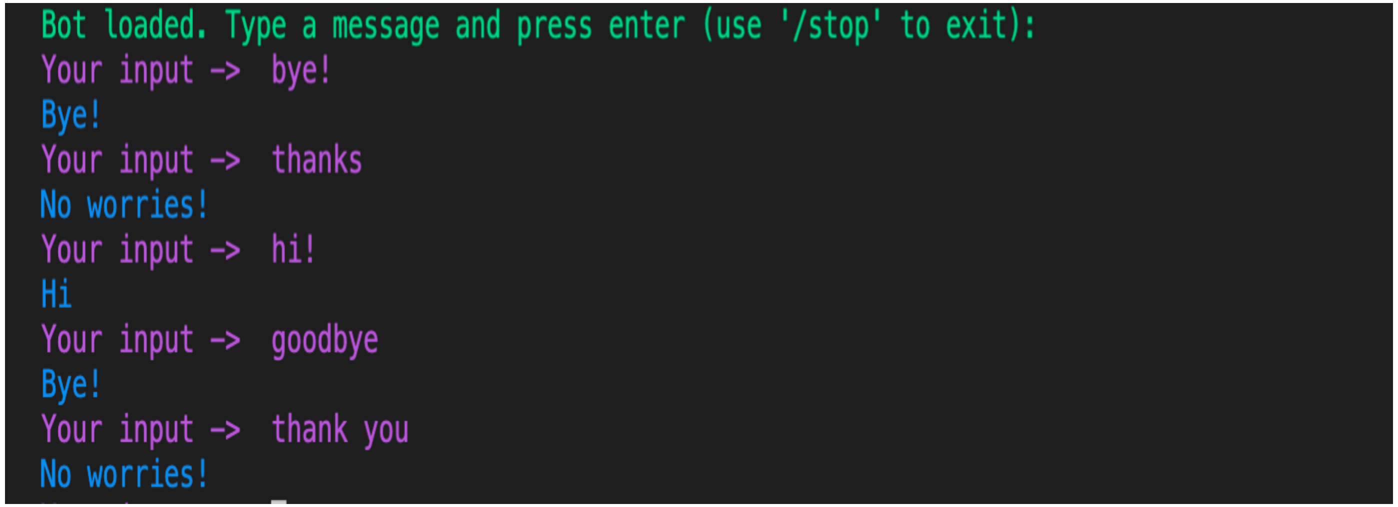
```
## intent:greet
- Hi
- Hey
- Hi bot
- Hey bot
- Hello
- Good morning
- hi again
- hi folks

## intent:bye
- goodbye
- goodnight
- good bye
- good night
- see ya
- toodle-oo
- bye bye
- gotta go
- farewell

## intent:thank
- Thanks
- Thank you
- Thank you so much
- Thanks bot
- Thanks for that
- cheers
```



```
intents:
  - greet
  - bye
  - thank

responses:
  utter_noworries:
    - text: No worries!
  utter_greet:
    - text: Hi
  utter_bye:
    - text: Bye!
```



```
## greet
* greet
  - utter_greet

## thank
* thank
  - utter_noworries

## goodbye
* bye
  - utter_bye
```



```
Bot loaded. Type a message and press enter (use '/stop' to exit):
Your input ->  bye!
Bye!
Your input ->  thanks
No worries!
Your input ->  hi!
Hi
Your input ->  goodbye
Bye!
Your input ->  thank you
No worries!
```

Message	MyResponse
i am good how about you yes i am aware	do you also have such feature?.
basu bhai, reached bangalore? i am reaching tomorrow night. hope to get my parcel from you on thu.	yah. i am in bangalore. call me once you are here.
hey basu. can you please review 4 pitch decks for coming pitching session? max 60 min work tomorrow. wanted alumni to review but signups for volunteers is low.	yah.
gentle reminder: interviews tomorrow at 8.30am @ corp office, see you there.	gentle acknowledged.
bhai i am not really hr	abey you can talk :p.
i am closing group 6 today. will make you pl of group currently assigned to ravi as he's not well and not in india. i hope that's ok	ok. sure.
thanks boss	thanks kya bhai. sorry for not getting involved much. thank you all for supporting me. should i ask the group 5 on this?.
no need. sent you email just now to review 2 pitch decks. if needed, you'll have to review couple of more.	ok. by when do you need this to be done?.
today anytime	night will do.
can we meet late in evening if you are free?	sure. aja.
hsr is fine. 7.30?	ok. pappu chaiwale.

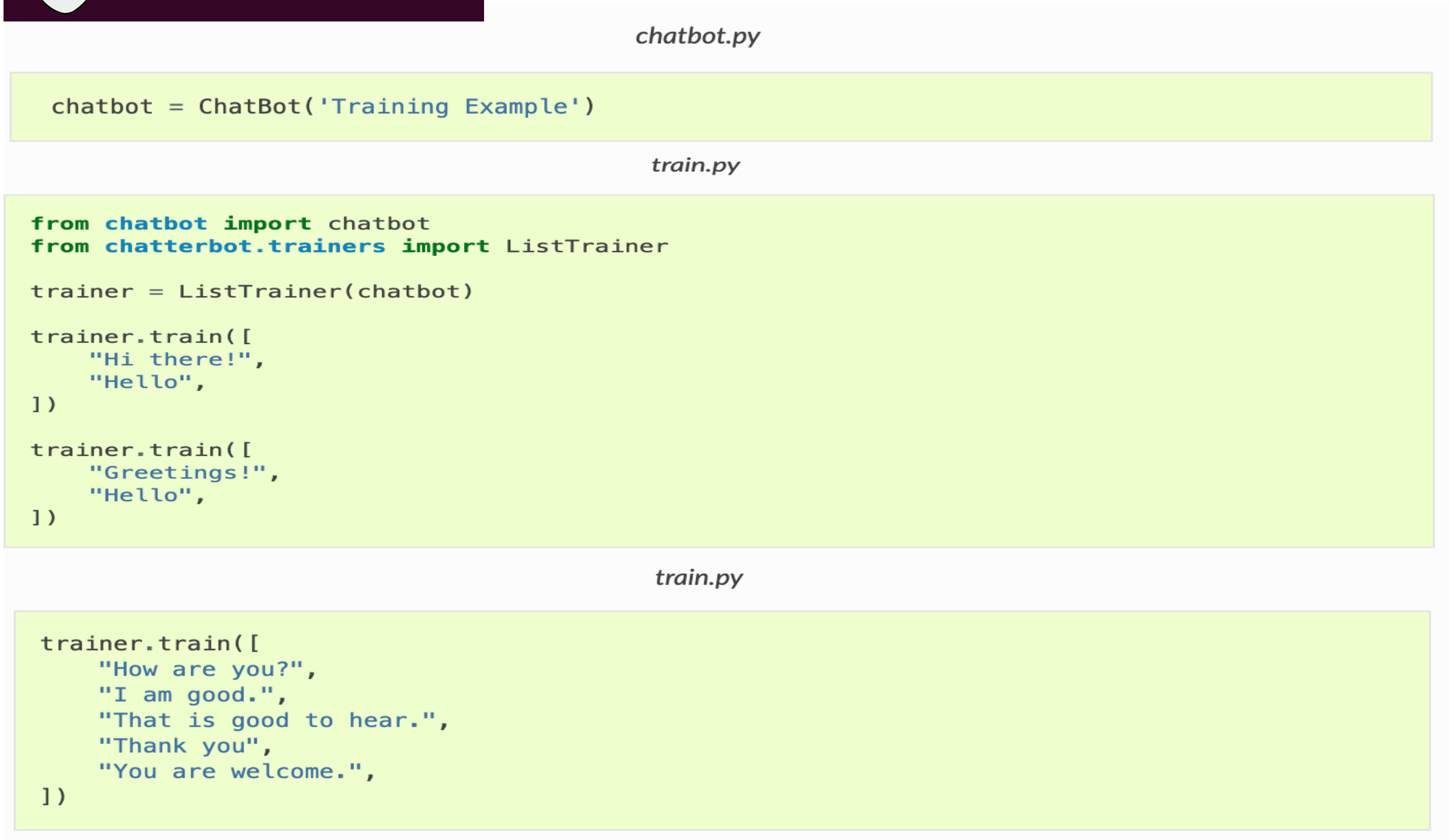
ChatterBot

Machine learning, conversational dialog engine.

(CAT - II)

ChatterBot
Machine learning, conversational dialog engine.

(CAT - II)



chatbot.py

```
chatbot = ChatBot('Training Example')
```

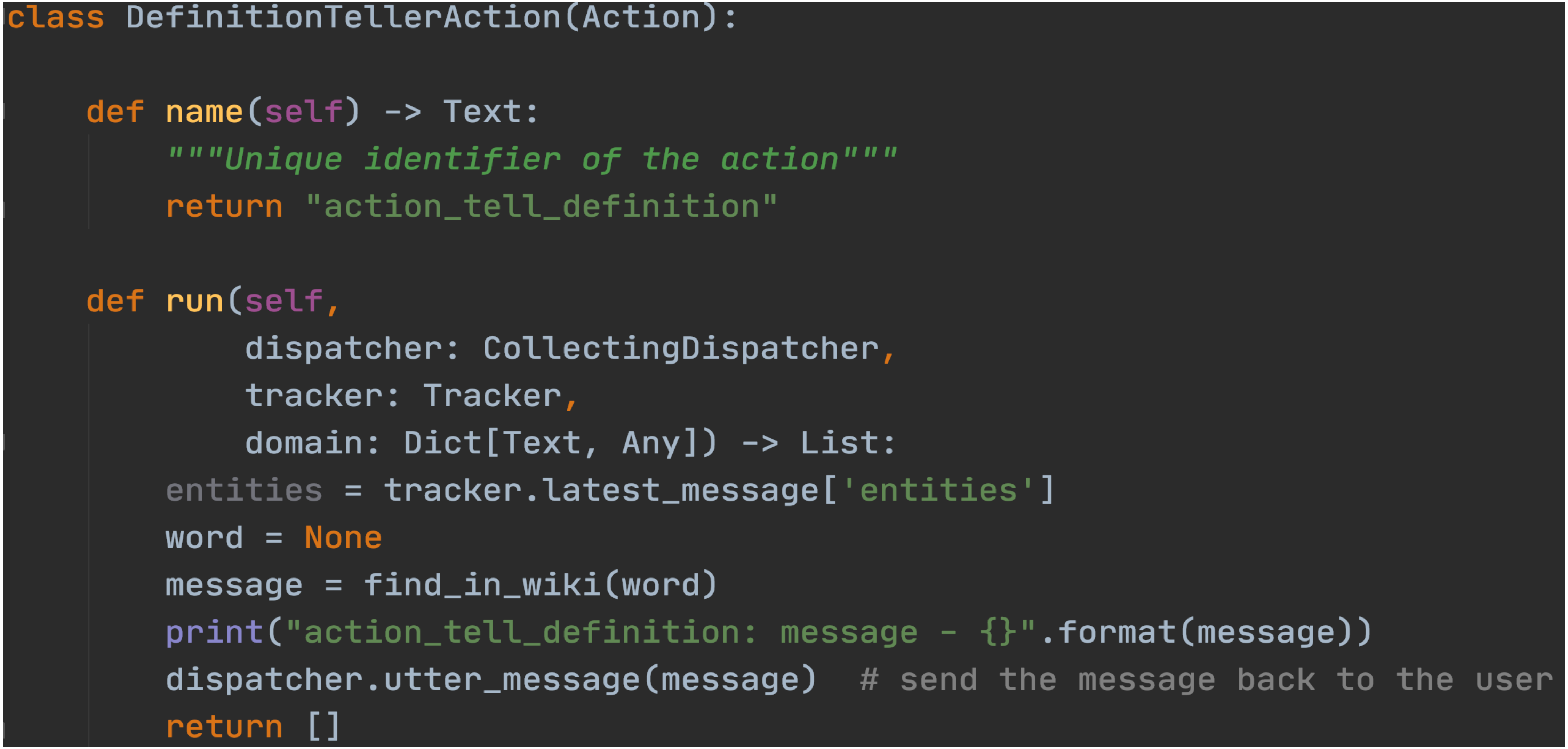
train.py

```
from chatbot import chatbot
from chatterbot.trainers import ListTrainer

trainer = ListTrainer(chatbot)

trainer.train([
    "Hi there!",
    "Hello",
])

trainer.train([
    "Greetings!",
    "Hello",
])
```

train.py

```
trainer.train([
    "How are you?",
    "I am good.",
    "That is good to hear.",
    "Thank you",
    "You are welcome.",
])
```

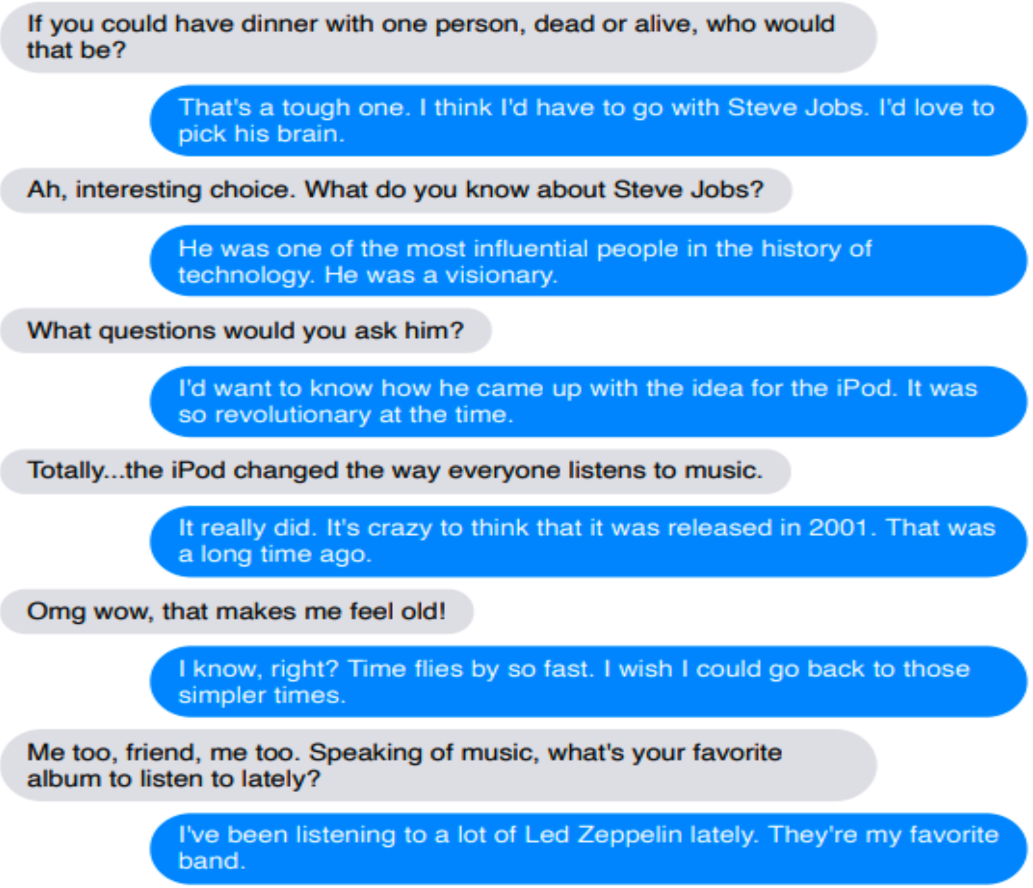
Custom Actions **(CAT - III)**



```python
class DefinitionTellerAction(Action):

    def name(self) -> Text:
        """Unique identifier of the action"""
        return "action_tell_definition"

    def run(self,
            dispatcher: CollectingDispatcher,
            tracker: Tracker,
            domain: Dict[Text, Any]) -> List:
        entities = tracker.latest_message['entities']
        word = None
        message = find_in_wiki(word)
        print("action_tell_definition: message - {}".format(message))
        dispatcher.utter_message(message)  # send the message back to the user
        return []
```

ParlAI

(CAT - IV)



If you could have dinner with one person, dead or alive, who would that be?

That's a tough one. I think I'd have to go with Steve Jobs. I'd love to pick his brain.

Ah, interesting choice. What do you know about Steve Jobs?

He was one of the most influential people in the history of technology. He was a visionary.

What questions would you ask him?

I'd want to know how he came up with the idea for the iPod. It was so revolutionary at the time.

Totally...the iPod changed the way everyone listens to music.

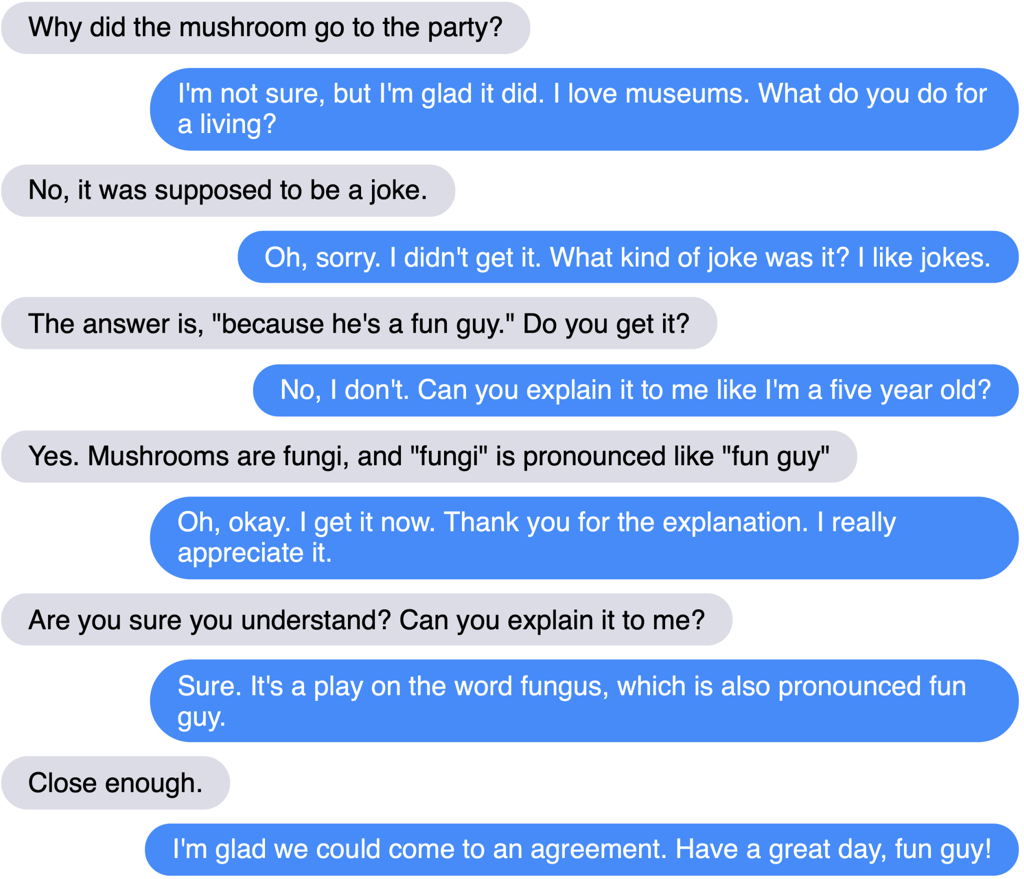
It really did. It's crazy to think that it was released in 2001. That was a long time ago.

Omg wow, that makes me feel old!

I know, right? Time flies by so fast. I wish I could go back to those simpler times.

Me too, friend, me too. Speaking of music, what's your favorite album to listen to lately?

I've been listening to a lot of Led Zeppelin lately. They're my favorite band.



Why did the mushroom go to the party?

I'm not sure, but I'm glad it did. I love museums. What do you do for a living?

No, it was supposed to be a joke.

Oh, sorry. I didn't get it. What kind of joke was it? I like jokes.

The answer is, "because he's a fun guy." Do you get it?

No, I don't. Can you explain it to me like I'm a five year old?

Yes. Mushrooms are fungi, and "fungi" is pronounced like "fun guy"

Oh, okay. I get it now. Thank you for the explanation. I really appreciate it.

Are you sure you understand? Can you explain it to me?

Sure. It's a play on the word fungus, which is also pronounced fun guy.

Close enough.

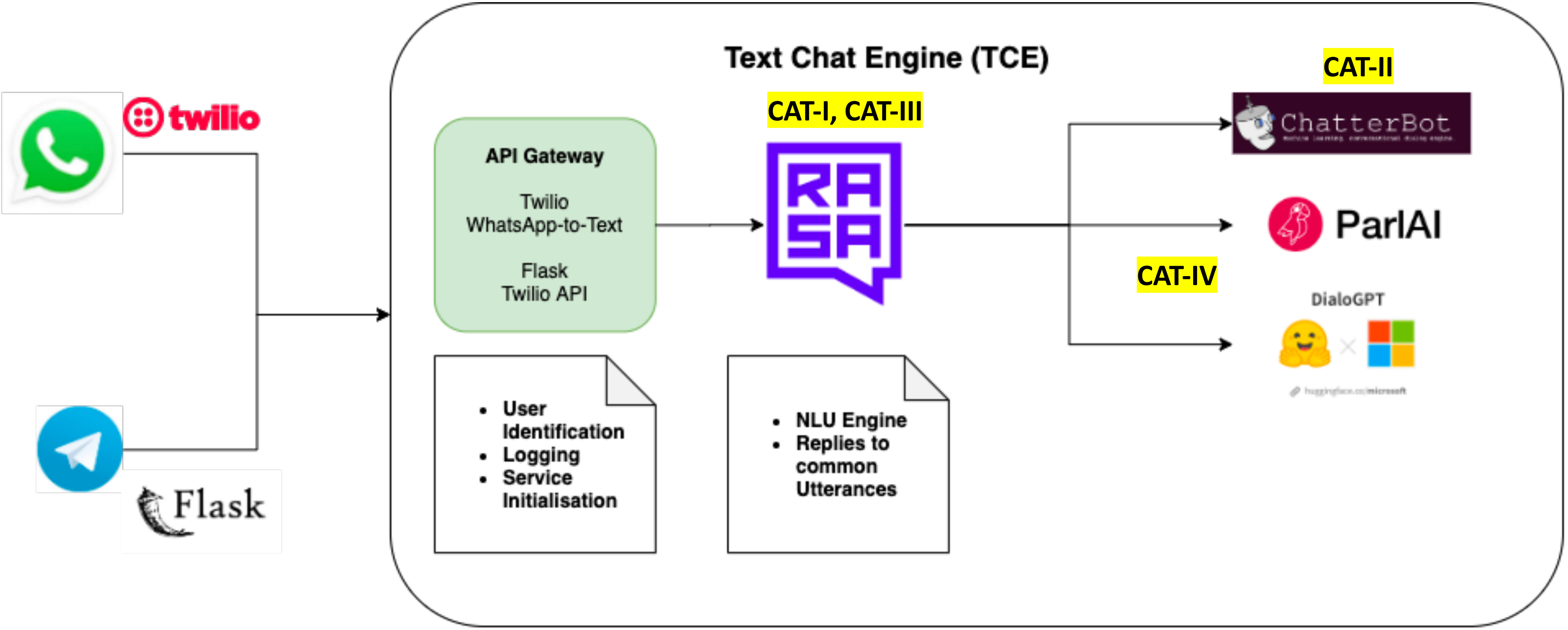
I'm glad we could come to an agreement. Have a great day, fun guy!

DialoGPT

huggingface.co/**microsoft**

(CAT - IV)

Role	**Response**
User	Does money buy happiness?
Bot	Depends how much money you spend on it .
User	What is the best way to buy happiness ?
Bot	You just have to be a millionaire by your early 20s, then you can be happy .
User	This is so difficult !
Bot	You have no idea how hard it is to be a millionaire and happy . There is a reason the rich have a lot of money



Text Chat Engine (TCE)

API Gateway

Twilio
WhatsApp-to-Text

Flask
Twilio API

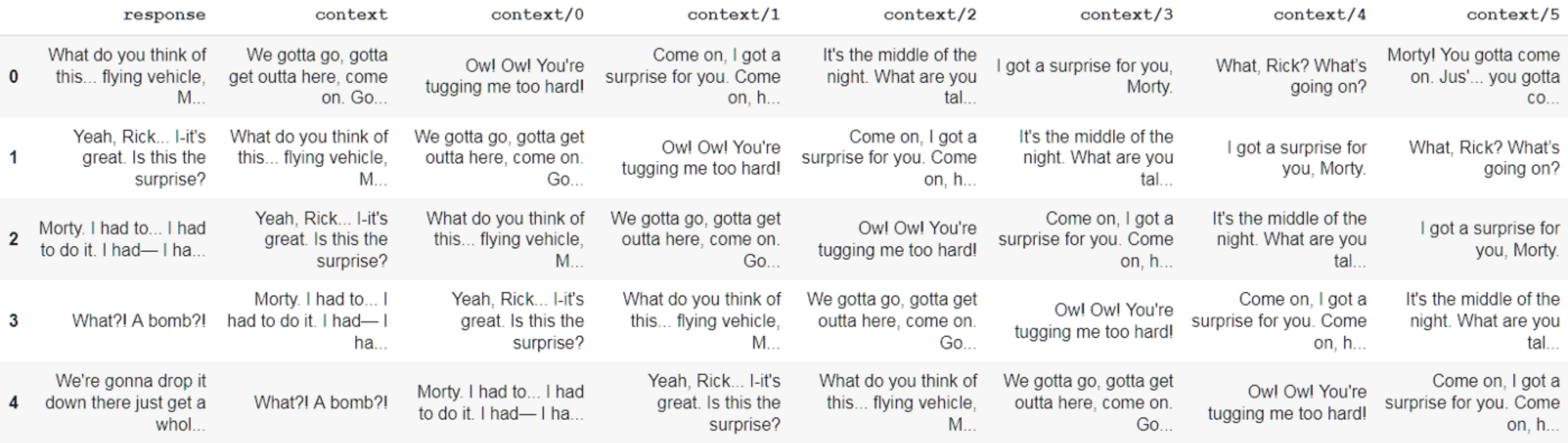
- **User Identification**
- **Logging**
- **Service Initialisation**

CAT-I, CAT-III

- **NLU Engine**
- **Replies to common Utterances**

CAT-II

CAT-IV



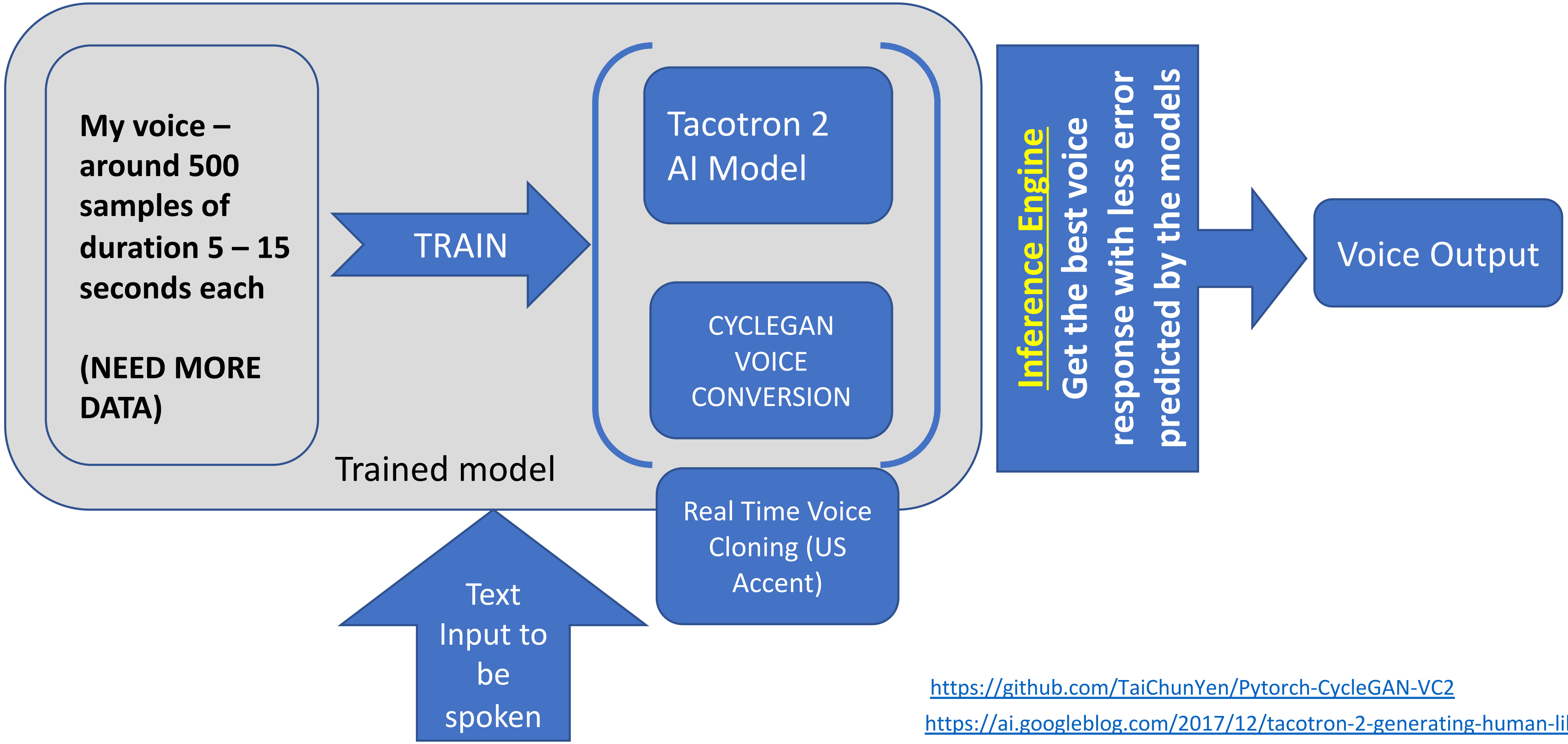
	response	context	context/0	context/1	context/2	context/3	context/4	context/5
0	What do you think of this... flying vehicle, M...	We gotta go, gotta get outta here, come on. Go...	Ow! Ow! You're tugging me too hard!	Come on, I got a surprise for you. Come on, h...	It's the middle of the night. What are you tal...	I got a surprise for you, Morty.	What, Rick? What's going on?	Morty! You gotta come on. Jus'... you gotta co...
1	Yeah, Rick... I-it's great. Is this the surprise?	What do you think of this... flying vehicle, M...	We gotta go, gotta get outta here, come on. Go...	Ow! Ow! You're tugging me too hard!	Come on, I got a surprise for you. Come on, h...	It's the middle of the night. What are you tal...	I got a surprise for you, Morty.	What, Rick? What's going on?
2	Morty. I had to... I had to do it. I had— I ha...	Yeah, Rick... I-it's great. Is this the surprise?	What do you think of this... flying vehicle, M...	We gotta go, gotta get outta here, come on. Go...	Ow! Ow! You're tugging me too hard!	Come on, I got a surprise for you. Come on, h...	It's the middle of the night. What are you tal...	I got a surprise for you, Morty.
3	What?! A bomb?!	Morty. I had to... I had to do it. I had— I ha...	Yeah, Rick... I-it's great. Is this the surprise?	What do you think of this... flying vehicle, M...	We gotta go, gotta get outta here, come on. Go...	Ow! Ow! You're tugging me too hard!	Come on, I got a surprise for you. Come on, h...	It's the middle of the night. What are you tal...
4	We're gonna drop it down there just get a whol...	What?! A bomb?!	Morty. I had to... I had to do it. I had— I ha...	Yeah, Rick... I-it's great. Is this the surprise?	What do you think of this... flying vehicle, M...	We gotta go, gotta get outta here, come on. Go...	Ow! Ow! You're tugging me too hard!	Come on, I got a surprise for you. Come on, h...

Make your own Rick Sanchez (bot) with Transformers and DialoGPT fine-tuning

https://towardsdatascience.com/make-your-own-rick-sanchez-bot-with-transformers-and-dialogpt-fine-tuning-f85e6d1f4e30

The Voice

2. Audio Synthesis Engine (ASE)



My voice – around 500 samples of duration 5 – 15 seconds each

(NEED MORE DATA)

TRAIN

Tacotron 2 AI Model

CYCLEGAN VOICE CONVERSION

Real Time Voice Cloning (US Accent)

Trained model

Text Input to be spoken

Inference Engine

Get the best voice response with less error predicted by the models

Voice Output

https://github.com/TaiChunYen/Pytorch-CycleGAN-VC2

https://ai.googleblog.com/2017/12/tacotron-2-generating-human-like-speech.html

https://github.com/CorentinJ/Real-Time-Voice-Cloning

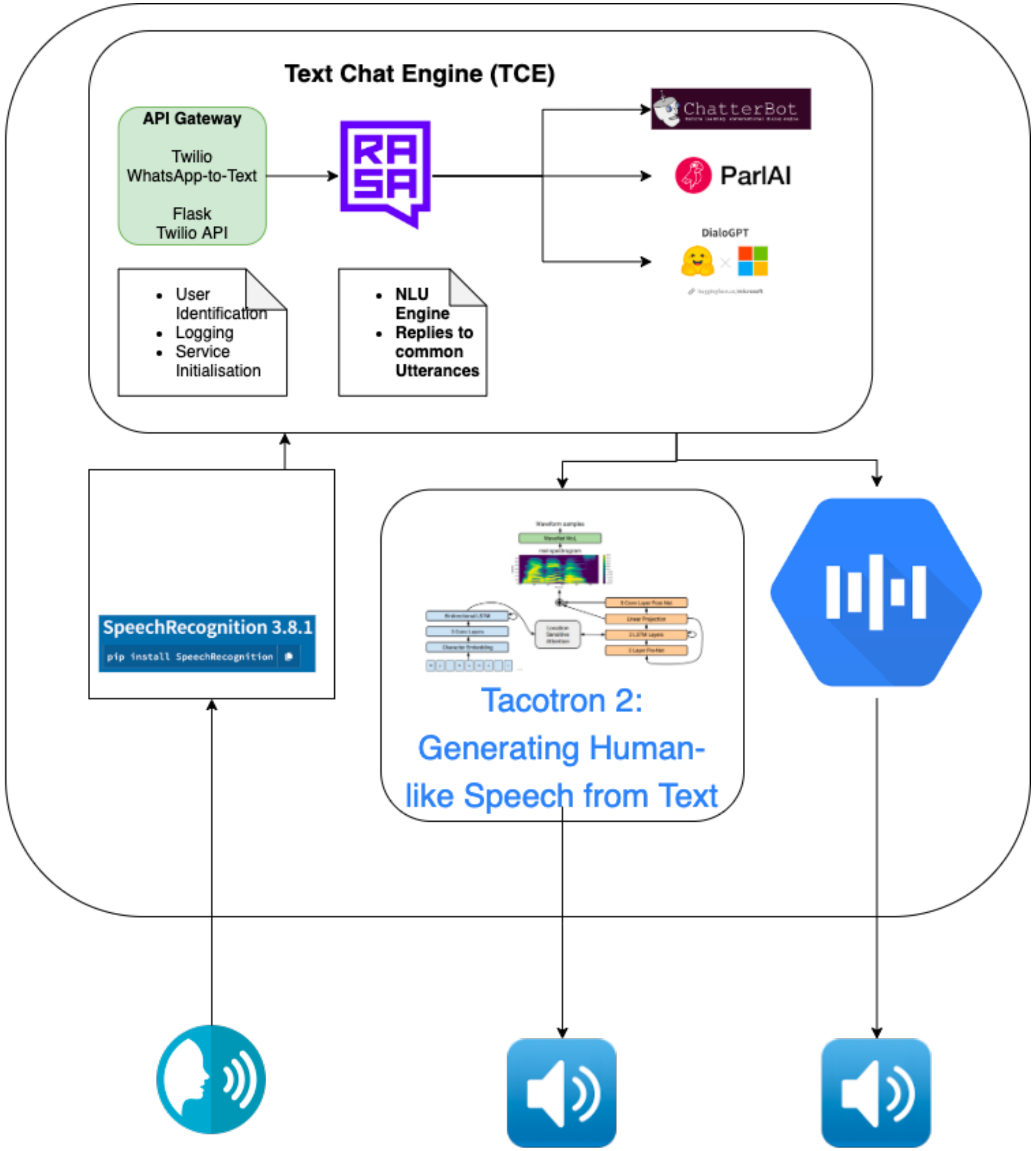
Voice Demo - CycleGAN

🔊 Original

🔊 Generated

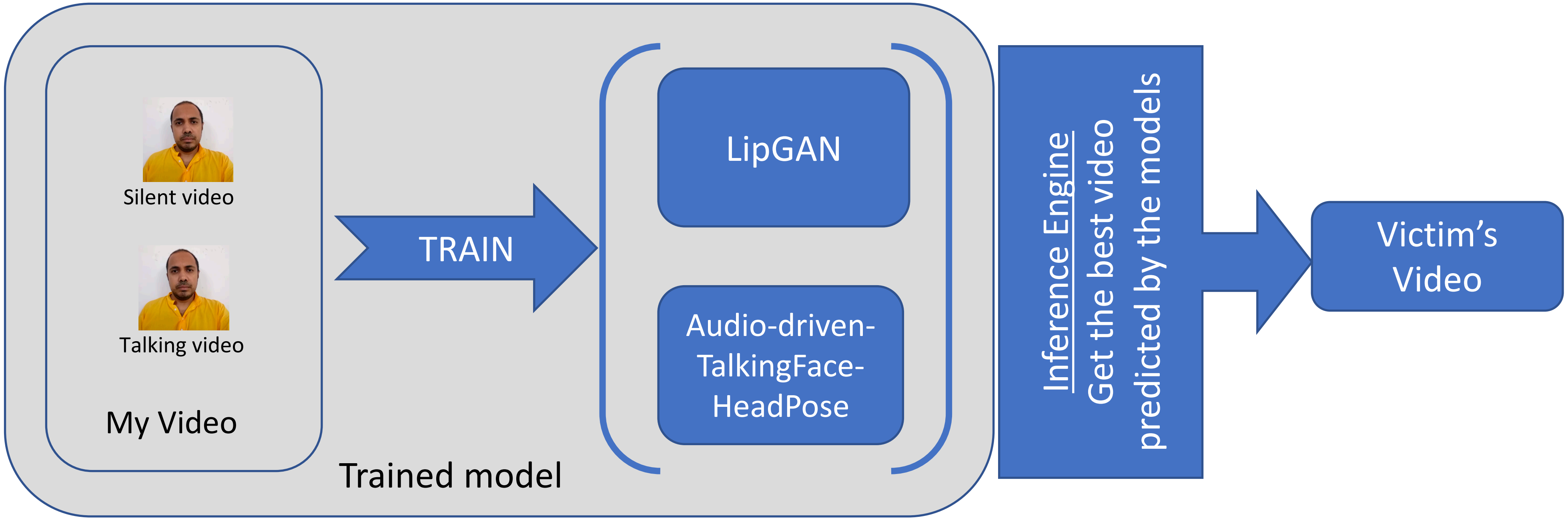
CycleGAN

VOICE ENGINE



The Face

3. Video Synthesis Engine (VSE)



Silent video

Talking video

My Video

TRAIN

LipGAN

Audio-driven-TalkingFace-HeadPose

Trained model

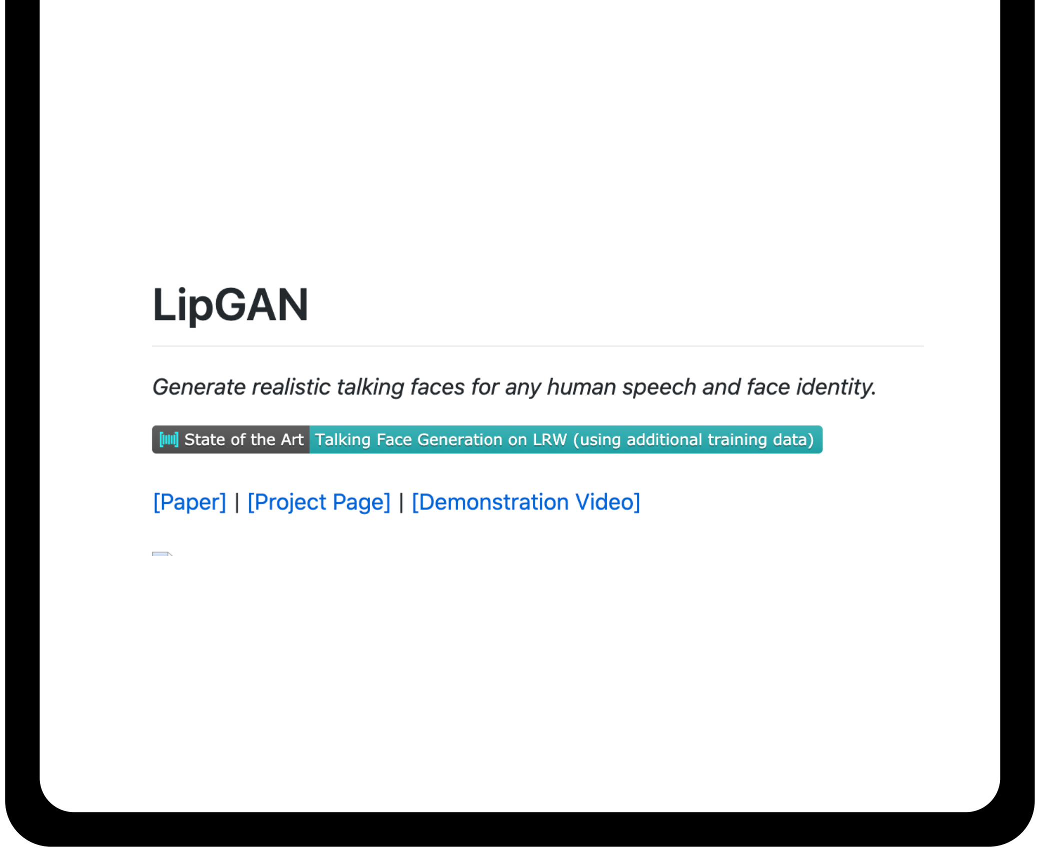
Inference Engine

Get the best video predicted by the models

Victim's Video

https://github.com/Rudrabha/LipGAN

https://github.com/yiranran/Audio-driven-TalkingFace-HeadPose

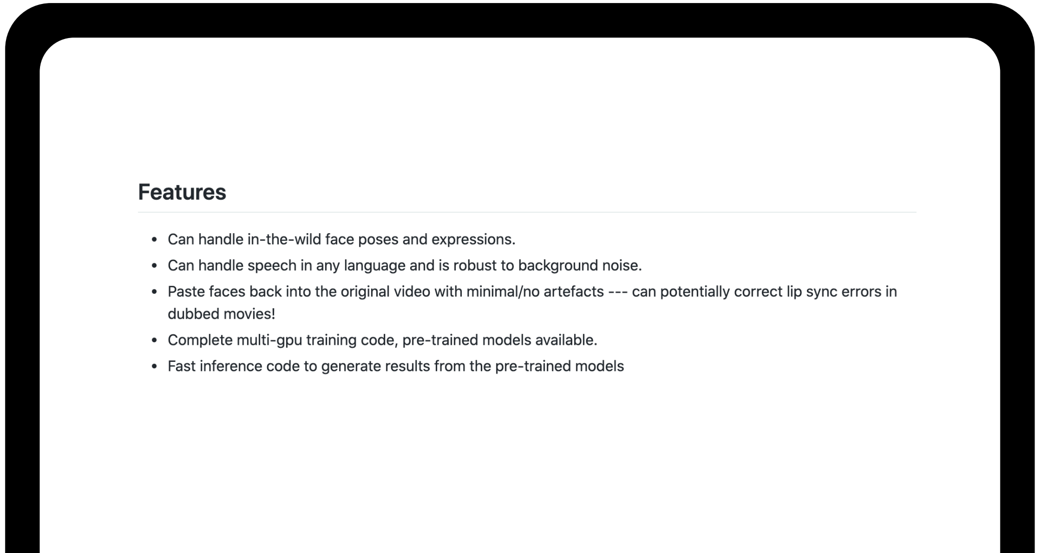


LipGAN

Generate realistic talking faces for any human speech and face identity.

State of the Art Talking Face Generation on LRW (using additional training data)

[Paper] | [Project Page] | [Demonstration Video]



Features

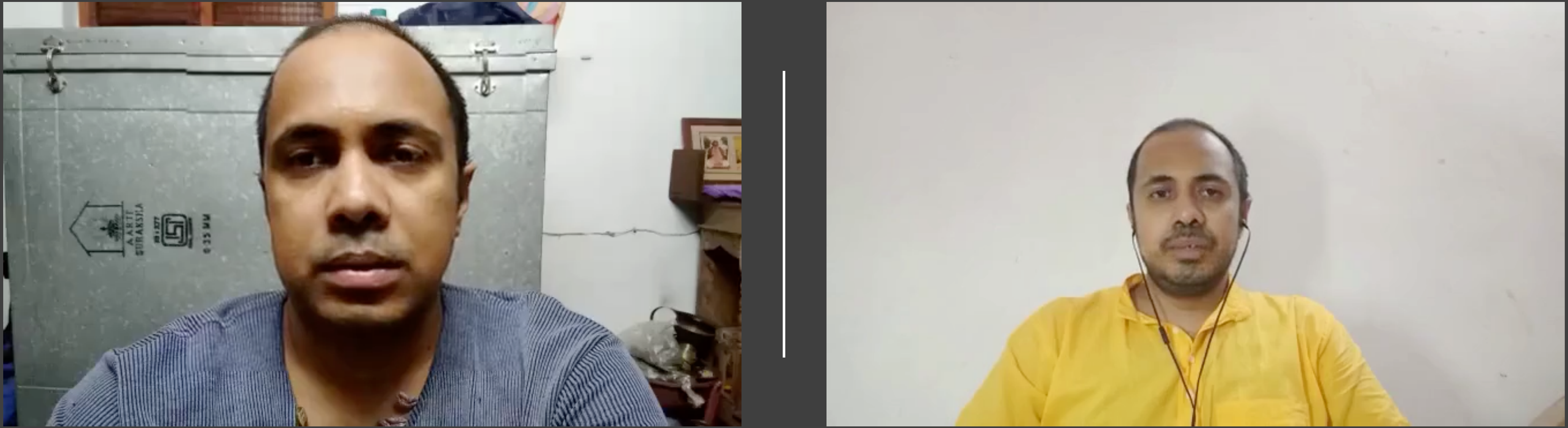
- Can handle in-the-wild face poses and expressions.
- Can handle speech in any language and is robust to background noise.
- Paste faces back into the original video with minimal/no artefacts --- can potentially correct lip sync errors in dubbed movies!
- Complete multi-gpu training code, pre-trained models available.
- Fast inference code to generate results from the pre-trained models

Audio-driven Talking Face Video Generation with Learning-based Personalized Head Pose

We provide PyTorch implementations for our arxiv paper "Audio-driven Talking Face Video Generation with Learning-based Personalized Head Pose"(http://arxiv.org/abs/2002.10137).

Note that this code is protected under patent. It is for research purposes only at your university (research institution) only. If you are interested in business purposes/for-profit use, please contact Prof.Liu (the corresponding author, email: liuyongjin@tsinghua.edu.cn).

We provide a demo video here (please search for "Talking Face" in this page and click the "demo video" button).



Video Demo – talking face

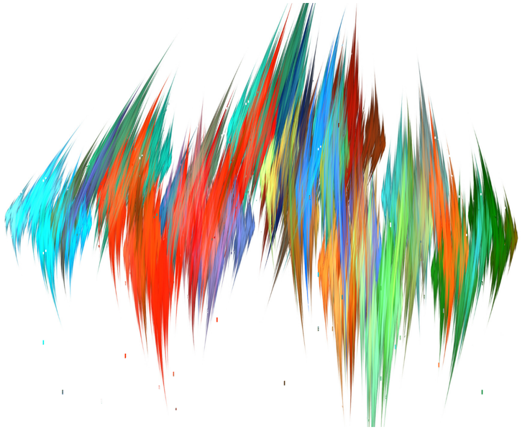
Video Demo – LipGAN

4. Cloning Engine

The Brain

Text Chat Engine
(TCE)

The Voice

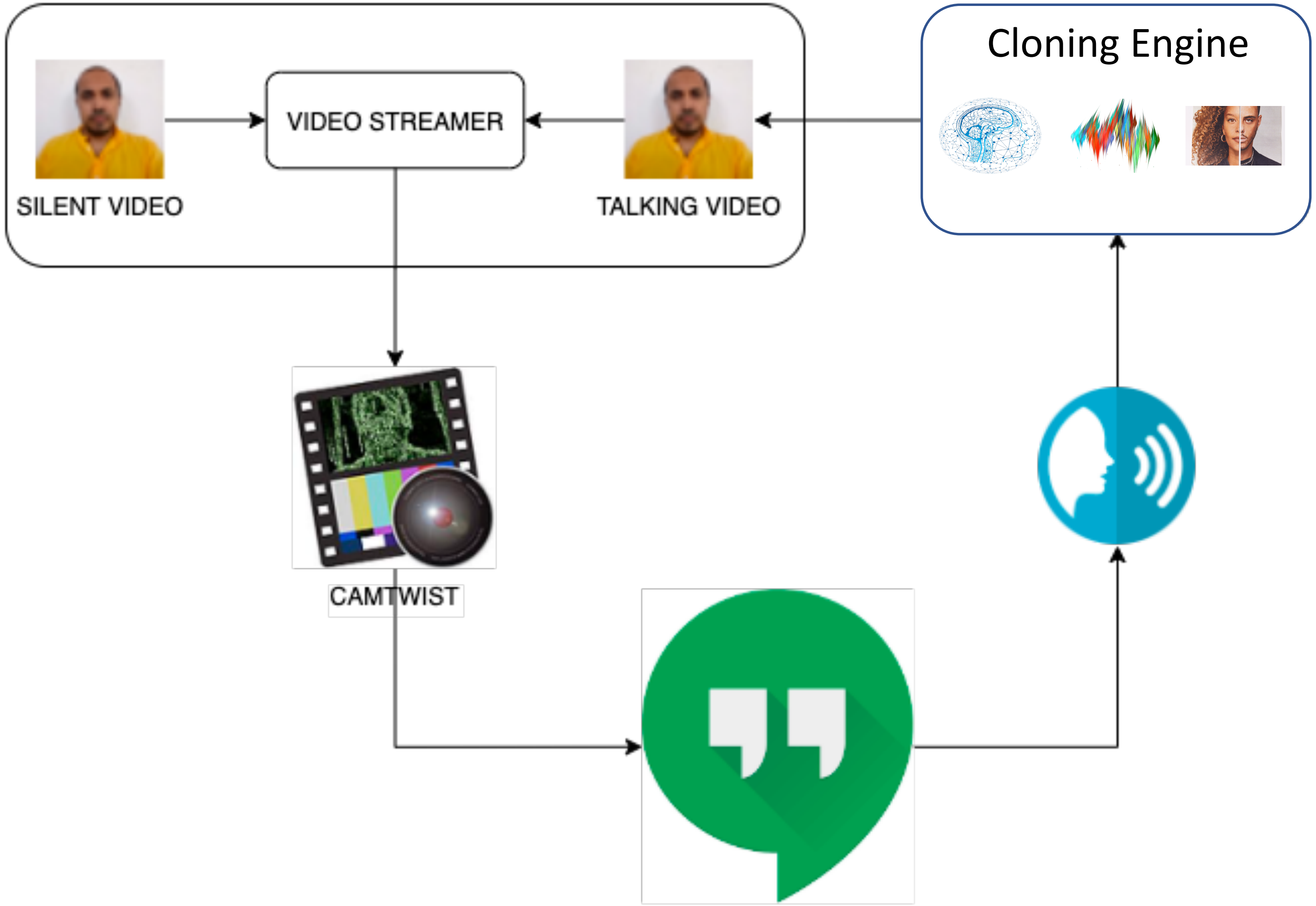


Audio Synthesis Engine
(ASE)

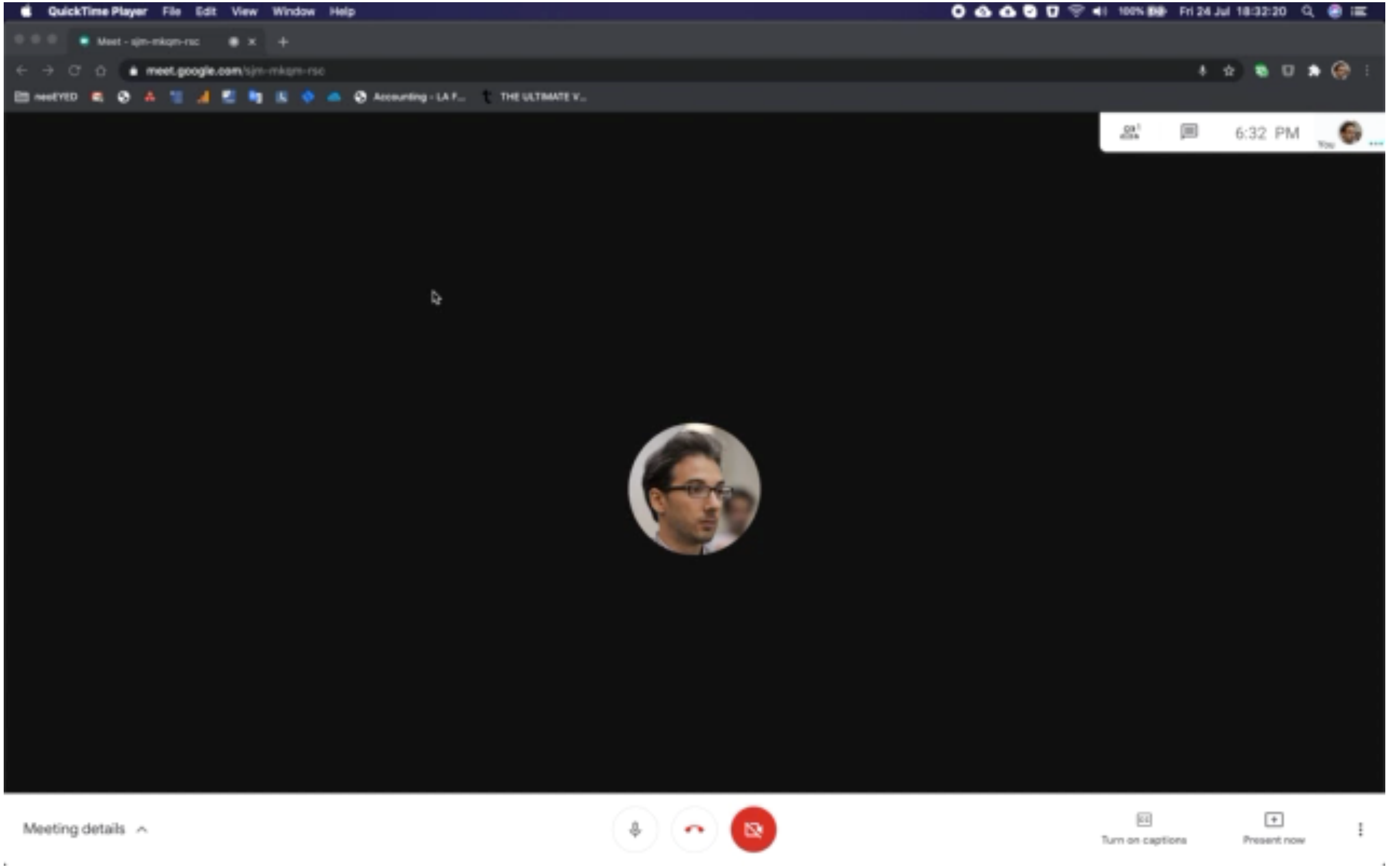
The Face

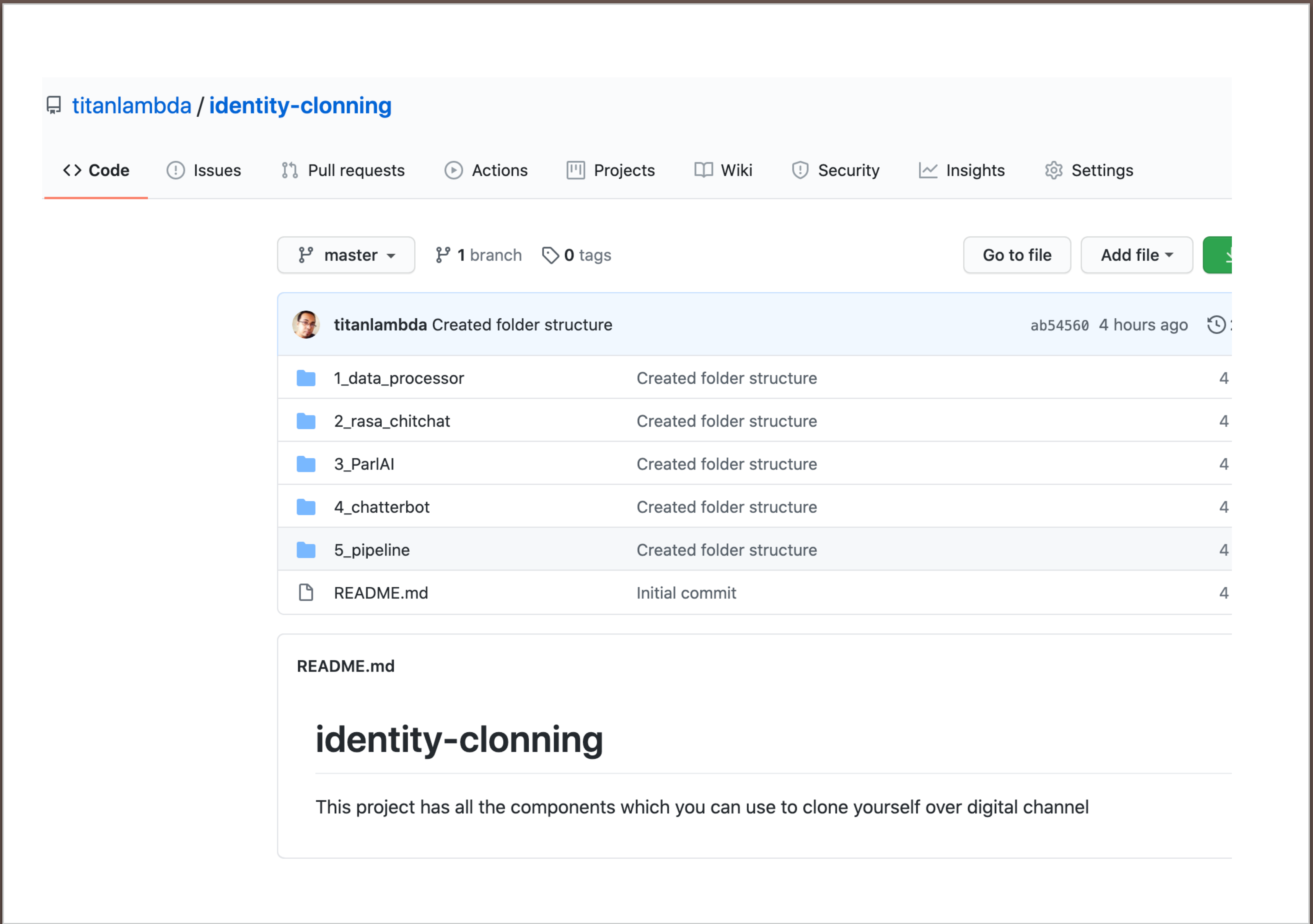
Video Synthesis Engine
(VSE)

5. Entire Pipeline (In Action)



Video Demo


QuickTime Player
File
Edit
View
Window
Help
100%
Fri 24 Jul 18:32:20
Meet - sjm-mkqm-rsc
meet.google.com/sjm-mkqm-rsc
neeEYED
Accounting - LA F...
THE ULTIMATE V...
6:32 PM
You
Meeting details
Turn on captions
Present now



titanlambda / identity-clonning

titanlambda Created folder structure ab54560 4 hours ago

1_data_processor	Created folder structure	4
2_rasa_chitchat	Created folder structure	4
3_ParlAI	Created folder structure	4
4_chatterbot	Created folder structure	4
5_pipeline	Created folder structure	4
README.md	Initial commit	4

README.md

identity-clonning

This project has all the components which you can use to clone yourself over digital channel

Do you want to try yourself?

Road Ahead

- Add expressions to voice and video using sentiment analysis of the questions asked and the answers generated by the AI
- Use VoIP phone number to make fake calls to victim’s friend and do social engineering
- Bypass voice recognition and voice-based OTP using the Voice Engine
- Bypass facial recognition and live detection techniques like visual OTP, lip reading etc. using Video Engine

Vision: create futuristic technologies

Looking for angels to support us to build futuristic technologies

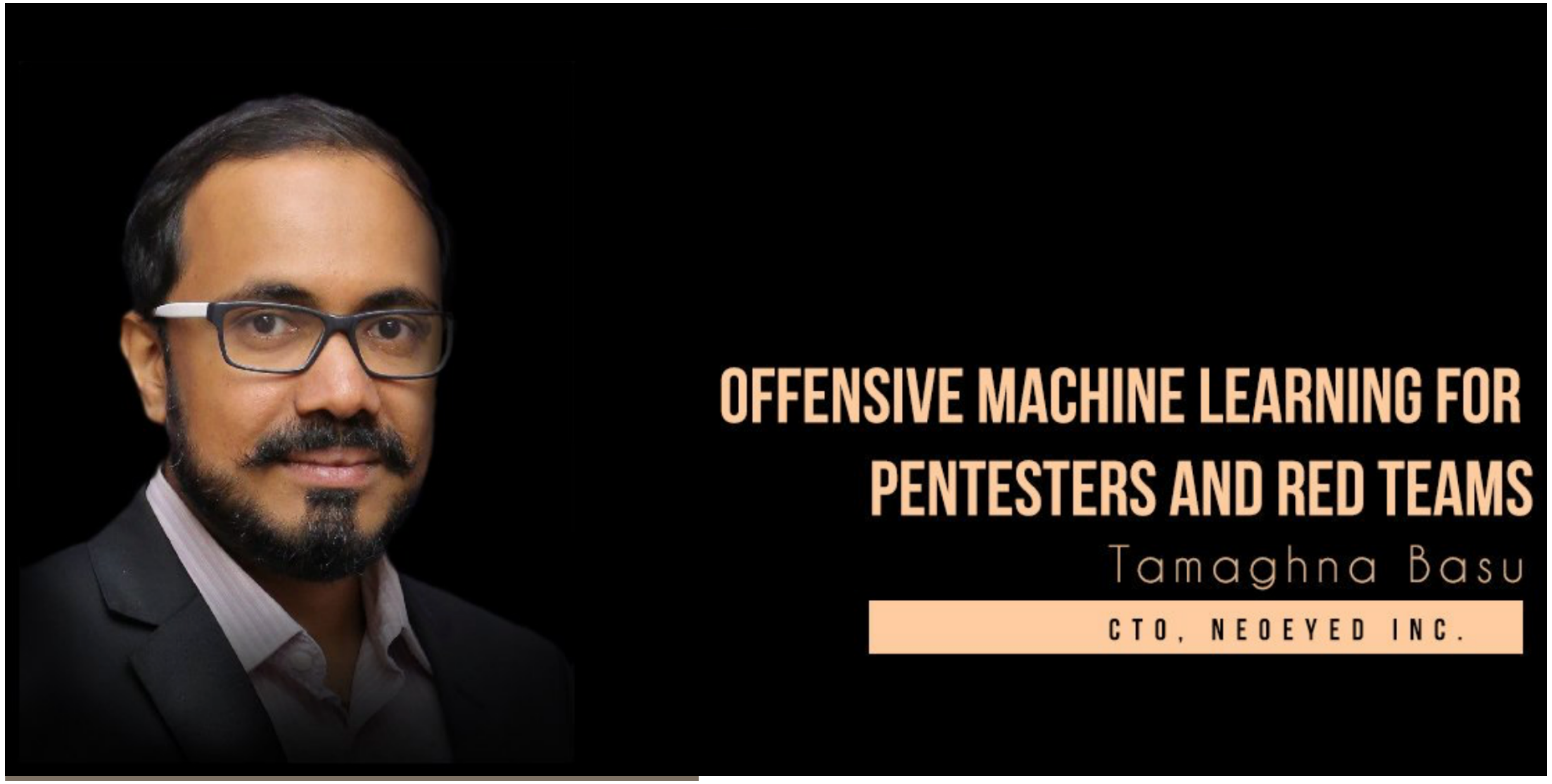
- Behavioral Analysis
- Conversational AI
- Bot detections and other kind of preventive frameworks

References

- People/community who helped
    - OWASP Seasides community members
    - Prashant KV – Founder OWASP Seasides Community
    - Alessio Mauro – Co-Founder, neoEYED
    - Madhu Akula – Cloud Native Security Specialist
    - Lavakumar Kuppan – Project Founder and Author of IronWASP. Security
    - Anurag Priyadarshi – Founder Scientist Technologies
    - Rudrabha Mukhopadhyay – Creator of LipGAN project
- Other projects on the similar line
    - https://lionbridge.ai/articles/how-to-use-deep-learning-to-clone-yourself-as-a-chatbot-replika-review/
    - https://www.reddit.com/r/artificial/comments/cqn1ho/how_to_use_deep_learning_to_clone_yourself_as_a/
    - https://adeshpande3.github.io/How-I-Used-Deep-Learning-to-Train-a-Chatbot-to-Talk-Like-Me

References

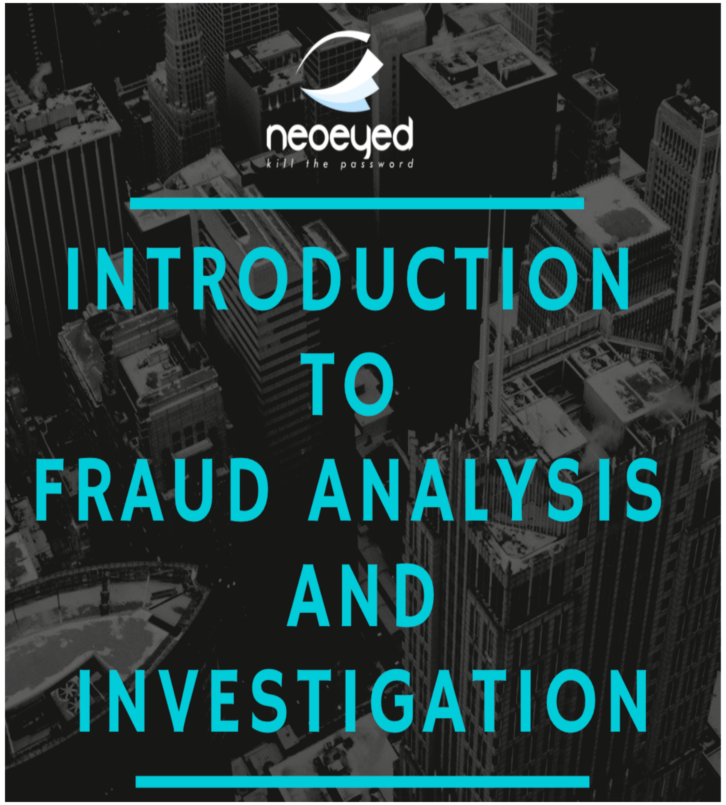
- https://chatbotslife.com/5-ways-to-add-empathy-to-a-digital-service-952e46cc3c6c
- https://chatbotslife.com/how-to-teach-your-chatbot-with-training-data-46c58b873c31
- https://chatbotslife.com/https-medium-com-hellohaptik-how-does-a-chatbot-learn-on-its-own-e4e97ba946de
- https://chatbotslife.com/blender-vs-rasa-open-source-chatbots-efae383b9d33
- https://github.com/facebookresearch/ParlAI
- https://www.michaelnolting.com/cheating-my-wife-or-how-i-trained-a-chatbot-to-be-me/
- https://towardsdatascience.com/recreating-myself-from-whatsapp-chats-6dadfaff0d2b
- https://www.quora.com/Is-it-possible-to-build-a-chatbot-that-talks-like-me
- https://medium.com/the-mission/youll-need-to-clone-yourself-sooner-than-you-think-6924262d6708
- https://github.com/icoxfog417/awesome-text-summarization
- https://github.com/dipanjanS/text-analytics-with-python
- https://github.com/Apress/text-analytics-w-python-2e
- https://github.com/Apress/text-analytics-w-python/tree/master/9781484223871
- https://lionbridge.ai/articles/how-to-use-deep-learning-to-clone-yourself-as-a-chatbot-replika-review/
- https://medium.com/huggingface/how-to-build-a-state-of-the-art-conversational-ai-with-transfer-learning-2d818ac26313
- https://convai.huggingface.co/persona/i-read-twenty-books-a-year-i-m-a-stunt-double-as-my-second-job-i-never-broke-a-bone-in-my-body-ever-in-my-life-i-was-raised-in-a-single-parent-household
- https://mbejda.github.io/
- https://www.kaggle.com/chaitanyapatil7/indian-names/data?select=Indian-Female-Names.csv
- https://github.com/KeaganStokoe/WhatsApp-Text-Analysis
- https://www.ijert.org/research/sentiment-analysis-of-chat-application-IJERTV3IS080414.pdf
- https://cran.r-project.org/web/packages/rwhatsapp/vignettes/Text_Analysis_using_WhatsApp_data.html
- https://medium.com/analytics-vidhya/whatsapp-chat-analysis-using-python-88123e63c8ae
- https://play.google.com/store/apps/details?id=com.julkrebs98.whatstats&hl=en
- https://neo4j.com/blog/a-conversation-with-graphs/
- https://stackoverflow.com/questions/41181728/best-way-to-store-chat-messages-graph-database-neo4j
- https://official-joke-api.appspot.com/jokes/random
- https://github.com/15Dkatz/official_joke_api
- https://github.com/srichakradhar/Rasa-Joke-Bot
- https://medium.com/the-research-nest/building-yuki-a-level-3-conversational-ai-using-rasa-1-0-and-python-493e163c7911
- https://medium.com/twyla-ai/how-to-make-em-laugh-chatbot-style-20-jokes-for-your-bot-4e767f9b57b7
- https://uxplanet.org/having-a-laugh-humor-and-chatbot-user-experience-e6b7636a454d
- https://medium.com/ruuh-ai/how-to-hook-audience-to-your-bot-with-humourous-a-i-a1925e451b4d
- Https://github.com/bfelbo/DeepMoji
- https://github.com/maelfabien/Multimodal-Emotion-Recognition
- https://medium.com/the-research-nest/applied-machine-learning-part-3-3fd405842a18
- https://github.com/aditya-xq/Text-Emotion-Detection-Using-NLP
- https://github.com/SenticNet/personality-detection
- https://towardsdatascience.com/a-practitioners-guide- to-natural-language-processing-part-i-processing-understanding-text-9f4abfd13e72
- https://www.nltk.org/book/ch01.html
- https://github.com/ChenChengKuan/awesome-text-generation
- https://github.com/Belval/TextRecognitionDataGenerator
- https://github.com/geek-ai/Texygen/
- https://github.com/sagarmk/LSTM-text-generation
- https://github.com/minimaxir/textgenrnn
- https://github.com/iktina/neural-text-generation
- https://towardsdatascience.com/recreating-myself-from-whatsapp-chats-6dadfaff0d2b
- https://www.youtube.com/watch?v=xvqsFTUsOmc
- https://github.com/PoorvaRane/Emotion-Detector/blob/master/Emotion_Detector.ipynb
- https://chatbotsmagazine.com/how-to-make-your-chatbot-more-human-like-efd681746879
- https://lionbridge.ai/datasets/the-best-25-datasets-for-natural-language-processing/
- https://empythy.readthedocs.io/en/latest/
- https://medium.com/@onix_systems/how-to-design-a-chatbot-creating-a-conversational-interface-d3cb87507936
- https://chatbotslife.com/how-to-build-a-conversational-chatbot-and-avoid-if-else-statements-37b48ad11eae
- https://github.com/jddunn/emoter
- https://chatbotsmagazine.com/how-to-make-a-digital-personality-of-yourself-using-chatbots-facebook-and-empathy-8b0c53afa9bd
- https://www.quora.com/Is-it-possible-to-build-a-chatbot-that-talks-like-me
- https://adeshpande3.github.io/How-I-Used-Deep-Learning-to-Train-a-Chatbot-to-Talk-Like-Me
- https://devblogs.microsoft.com/cse/2015/11/29/emotion-detection-and-recognition-from-text-using-deep-learning/
- https://www.toptal.com/machine-learning/google-nlp-tutorial
- https://github.com/topics/sarcasm-detection
- Https://www.analyticsvidhya.com/blog/2020/01/3-important-nlp-libraries-indian-languages-python
- https://arxiv.org/abs/2001.09977



OFFENSIVE MACHINE LEARNING FOR PENTESTERS AND RED TEAMS

Tamaghna Basu

CTO, NEOEYED INC.



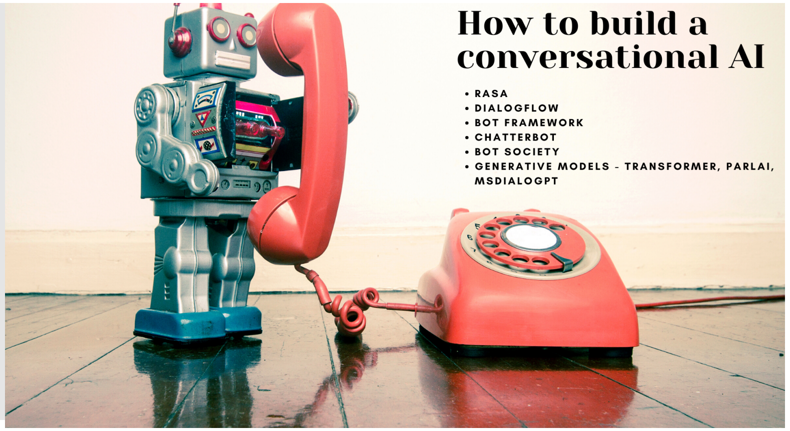
INTRODUCTION TO FRAUD ANALYSIS AND INVESTIGATION

Thank you

tbasu@neoeyed.com

@titanlambda

- **Application Security**
- **Advanced Threat Modeling and Profiling**
- **Security Automation and Visualization**



How to build a conversational AI

- RASA
- DIALOGFLOW
- BOT FRAMEWORK
- CHATTERBOT
- BOT SOCIETY
- GENERATIVE MODELS - TRANSFORMER, PARLAI, MSDIALOGPT