Hansken

The open digital forensic platform
investigate - innovate - share

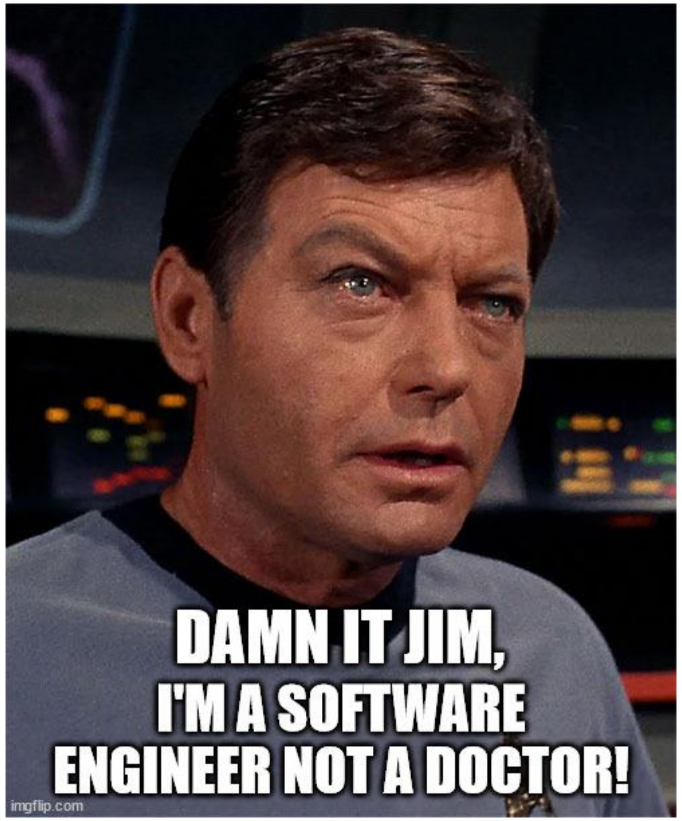
Hansken extraction plugins

Walkthrough

Introduction

- 👩‍🏫 My name: remco
- 🐘 I am part of the Hansken development team
- 🧑‍🚀 One of the main code contributors to the Extraction Plugin SDK
- 👩‍🔧 I am a software engineer
- ⚠ not a
  - case investigator
  - authority on digital forensics
  - …

Introduction



Our fictional case

- We are investigating a case
- Our suspect mentions that he/she was not at home and was not using his/her phone at a given time. **Is that True?**
- Evidence item: iPhone 15

- Imaginary & creative solution:
  - Find out when the phone is charging, and at what rate?
  - Find out when is the phone discharging, how fast is the phone discharging?
  - Can we use the charging/discharging rate to prove our hypothesis?

- So…
  - How can we know this?
  - And if we know this, how can we add this knowledge to Hansken?

Our fictional case: background research

- Iphone file: knowledgeC.db

KnowledgeC.db is a **SQLite file on recent iOS** versions **that tracks lots of different activity on the device** ranging from **Battery Level** and **Bluetooth connections** to **which speaker is in use** and **what it is playing at any given time** (…)
The database is located at **/private/var/mobile/Library/CoreDuet/Knowledge/knowledgeC.db** and is made up of 12 tables.

- For this walkthrough: **we will only focus on battery events!**

- **Background reading:**
  - https://www.doubleblak.com/knowledgec2
  - http://www.mac4n6.com/blog/2018/8/5/knowledge-is-power-using-the-knowledgecdb-database-on-macos-and-ios-to-determine-precise-user-and-application-usage

Talking points for today

- **(3 min) Our fictional case…**
- (2 min) Extracting knowledgeC.db in Hansken
- (3 min) Extraction plugin concepts
- (5 min) Write logic: parse knowledgeC.db and transform to Hansken types
- (5 min) Extraction plugin template
- (5 min) Add logic to plugin
- (5 min) Run with Hansken.py
- (5 min) Run the plugin during an extraction
- (3 min) Add tests to our code
- (3 min) Wrap up and questions

Talking points for today

- (3 min) Our fictional case…
- **(2 min) Extract knowledgeC.db in Hansken**
- (3 min) Extraction plugin concepts
- (5 min) Write logic: parse knowledgeC.db and transform to Hansken types
- (5 min) Extraction plugin template
- (5 min) Add logic to plugin
- (5 min) Run with Hansken.py
- (5 min) Run the plugin during an extraction
- (3 min) Add tests to our code
- (3 min) Wrap up and questions

Talking points for today

- (3 min) Our fictional case…
- (2 min) Extract knowledgeC.db in Hansken
- **(3 min) Extraction plugin concepts**
- (5 min) Write logic: parse knowledgeC.db and transform to Hansken types
- (5 min) Extraction plugin template
- (5 min) Add logic to plugin
- (5 min) Run with Hansken.py
- (5 min) Run the plugin during an extraction
- (3 min) Add tests to our code
- (3 min) Wrap up and questions

Extraction plugin concepts

Hansken.py

Standalone scripts

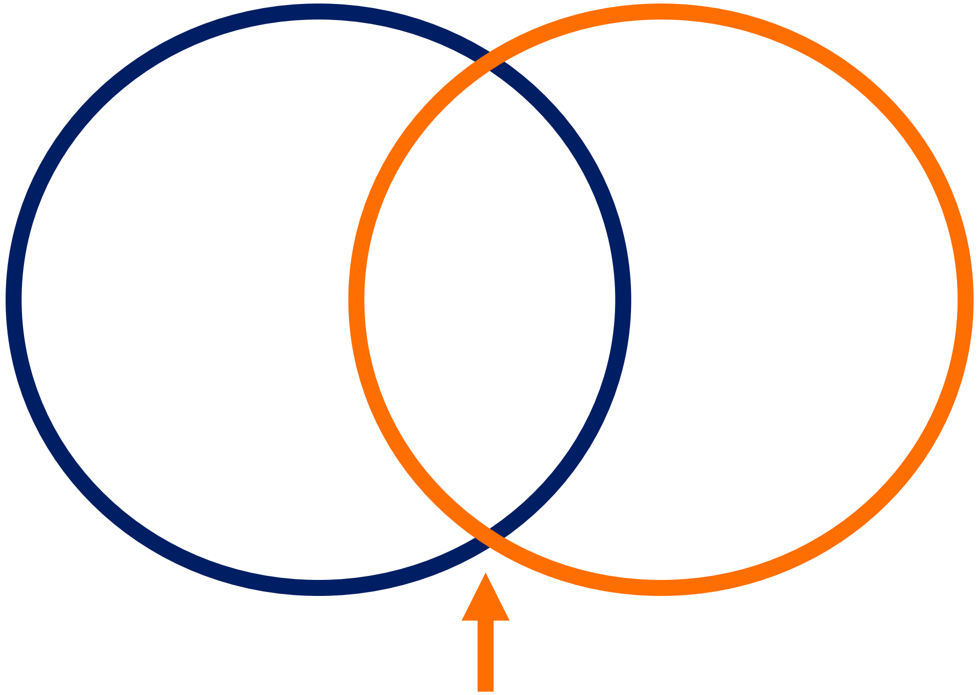
Interfaces over REST

Relatively slow ←

Easy to run

Manual invocation

Great for visualisations and analysis



Extraction Plugins
***can* run as Hansken.py scripts**

Extraction Plugins

Installed scripts

Runs distributed inside Hansken

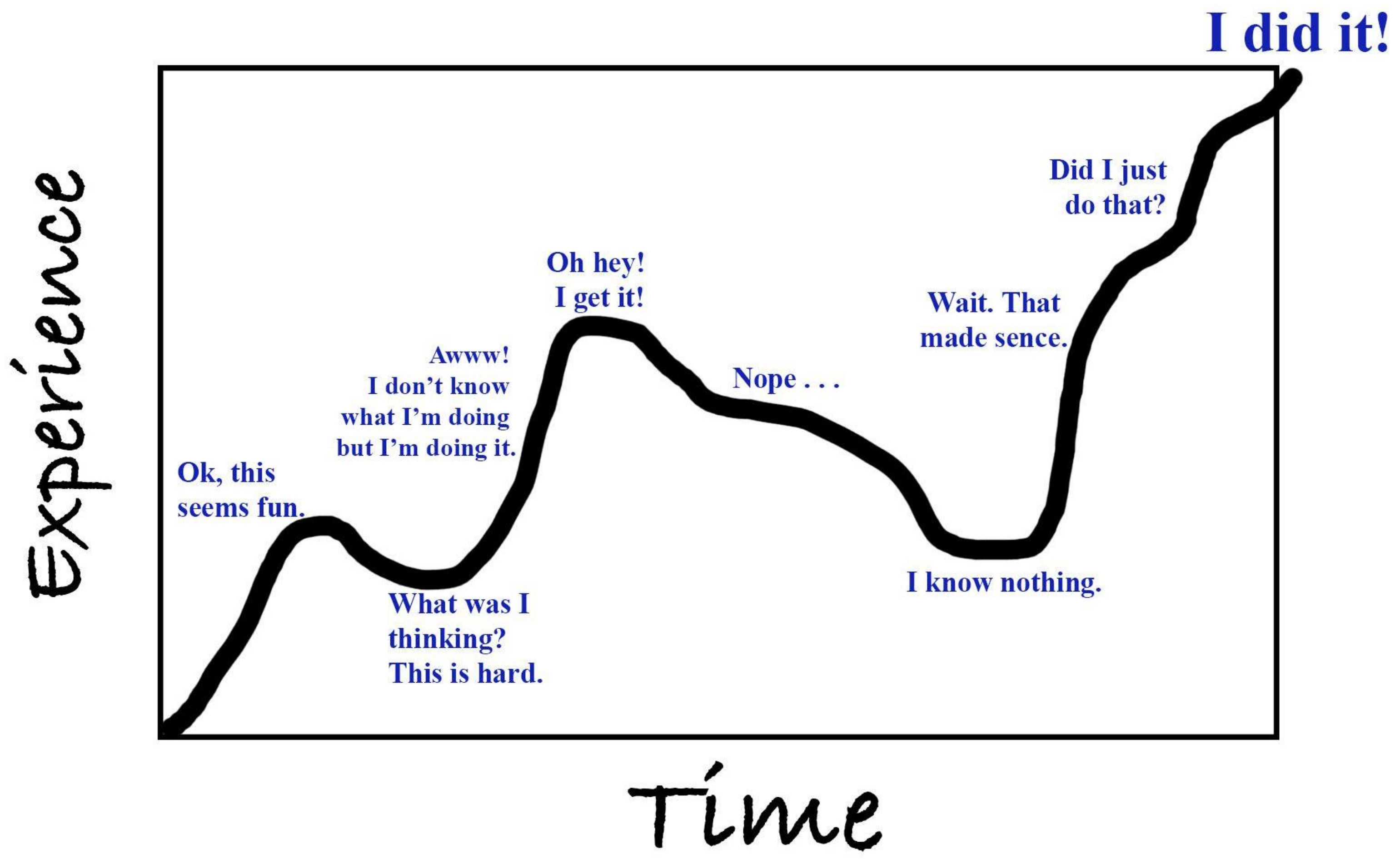
→ Relatively fast

Small learning curve

Automatic invocation on all cases

Great for ‘forensic formats’ processing and individual trace enrichment

The Learning Curve



www.theexcitedwriter.com

Extraction plugin concepts

- **Extraction plugin Software Development Kit (SDK):**
  - Java API and tooling, to be able to write an extraction plugin with the Java programming language
  - Python API and tooling, to be able to write an extraction plugin with Python programming language
  - Test framework, to be able to test extraction plugins before they are used production
  - Documentation
  - Examples (Github)

- Community: Extraction plugins made by the community on Gitlab

Talking points for today

- (3 min) Our fictional case…
- (2 min) Extract knowledgeC.db in Hansken
- (3 min) Extraction plugin concepts
- **(5 min) Write logic: parse knowledgeC.db and transform to Hansken types**
- (5 min) Extraction plugin template
- (5 min) Add logic to plugin
- (5 min) Run with Hansken.py
- (5 min) Run the plugin during an extraction
- (3 min) Add tests to our code
- (3 min) Wrap up and questions

Write logic: parse knowledgeC.db and transform to Hansken types

Steps

1. Determine how to store battery events in Hansken (trace model)
2. Write scripts:
   read battery events from database(SQLite query)
   and convert them to the Hansken model

Write logic: parse knowledgeC.db and transform to Hansken types

knowledgeC.db

Python script

traces of type “event”

Talking points for today

- (3 min) Our fictional case…
- (2 min) Extract knowledgeC.db in Hansken
- (3 min) Extraction plugin concepts
- (5 min) Write logic: parse knowledgeC.db and transform to Hansken types
- **(5 min) Extraction plugin template**
- (5 min) Add logic to plugin
- (5 min) Run with Hansken.py
- (5 min) Run the plugin during an extraction
- (3 min) Add tests to our code
- (3 min) Wrap up and questions

Extraction plugin template

Steps

1. Clone an template plugin from Github
2. Build the template plugin
3. (Upload the plugin to Hansken)
4. Refresh the plugin list in Hansken

Talking points for today

- (3 min) Our fictional case…
- (2 min) Extract knowledgeC.db in Hansken
- (3 min) Extraction plugin concepts
- (5 min) Write logic: parse knowledgeC.db and transform to Hansken types
- (5 min) Extraction plugin template
- **(5 min) Add logic to plugin**
- (5 min) Run with Hansken.py
- (5 min) Run the plugin during an extraction
- (3 min) Add tests to our code
- (3 min) Wrap up and questions

Add logic to plugin

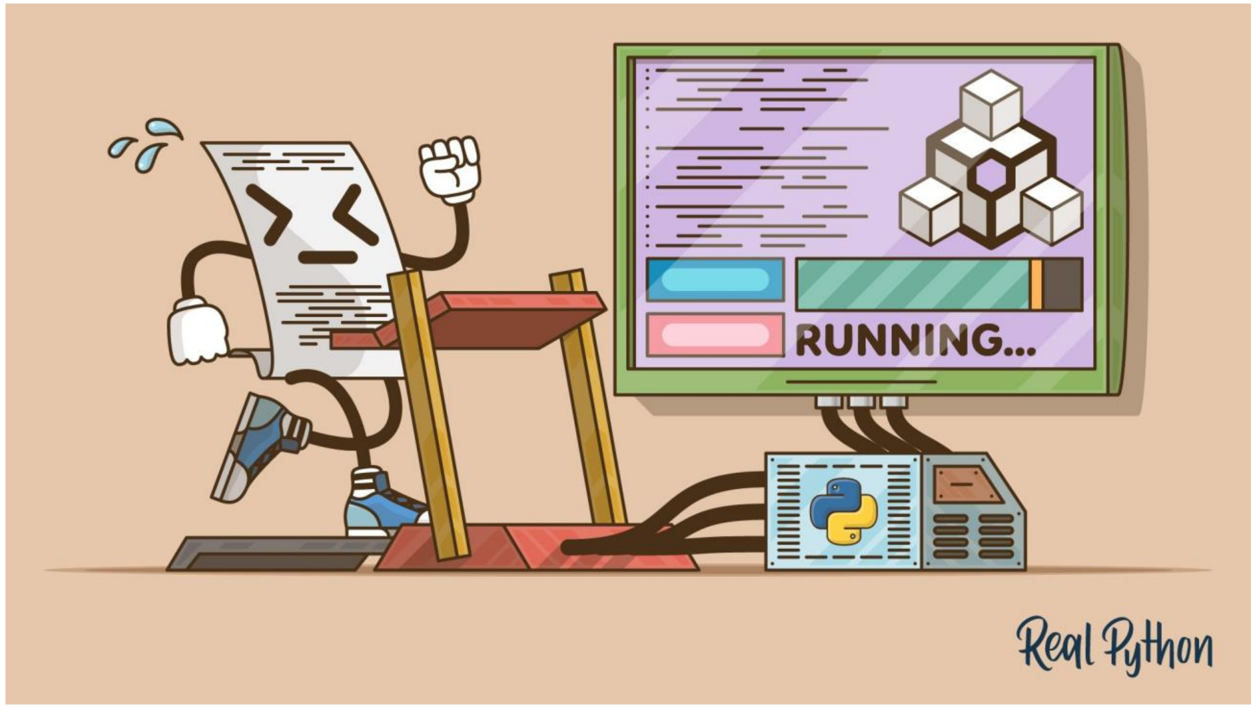
Steps

1. Update plugin info
   1. Naming convention
   2. Matcher (common PITA)
   3. Plugin resources (common PITA2)
2. Implement process method

Talking points for today

- (3 min) Our fictional case…
- (2 min) Extract knowledgeC.db in Hansken
- (3 min) Extraction plugin concepts
- (5 min) Write logic: parse knowledgeC.db and transform to Hansken types
- (5 min) Extraction plugin template
- (5 min) Add logic to plugin
- **(5 min) Run with Hansken.py**
- (5 min) Run the plugin during an extraction
- (3 min) Add tests to our code
- (3 min) Wrap up and questions

Run plugin with Hansken.py



Steps

1. Run plugin from the IDE:
   1. Determine program arguments (projectId, URLs)
   2. Define run profile
   3. Run!
2. Verify results

Talking points for today

- (3 min) Our fictional case…
- (2 min) Extract knowledgeC.db in Hansken
- (3 min) Extraction plugin concepts
- (5 min) Write logic: parse knowledgeC.db and transform to Hansken types
- (5 min) Extraction plugin template
- (5 min) Add logic to plugin
- (5 min) Run with Hansken.py
- **(5 min) Run the plugin during an extraction**
- (3 min) Add tests to our code
- (3 min) Wrap up and questions

Run the plugin during an extraction

Steps

1. Package the plugin (tox –e package)
2. Refresh plugin list in Hansken
3. Run an extraction
4. Inspect results
5. Inspect chain of evidence

Talking points for today

- (3 min) Our fictional case…
- (2 min) Extract knowledgeC.db in Hansken
- (3 min) Extraction plugin concepts
- (5 min) Write logic: parse knowledgeC.db and transform to Hansken types
- (5 min) Extraction plugin template
- (5 min) Add logic to plugin
- (5 min) Run with Hansken.py
- (5 min) Run the plugin during an extraction
- **(3 min) Add tests to our code**
- (3 min) Wrap up and questions

Add tests to our code

Steps

1. Why?
2. Have a look at the documentation on GitHub
3. Add test data to plugin
4. Generate & verify baseline resuts

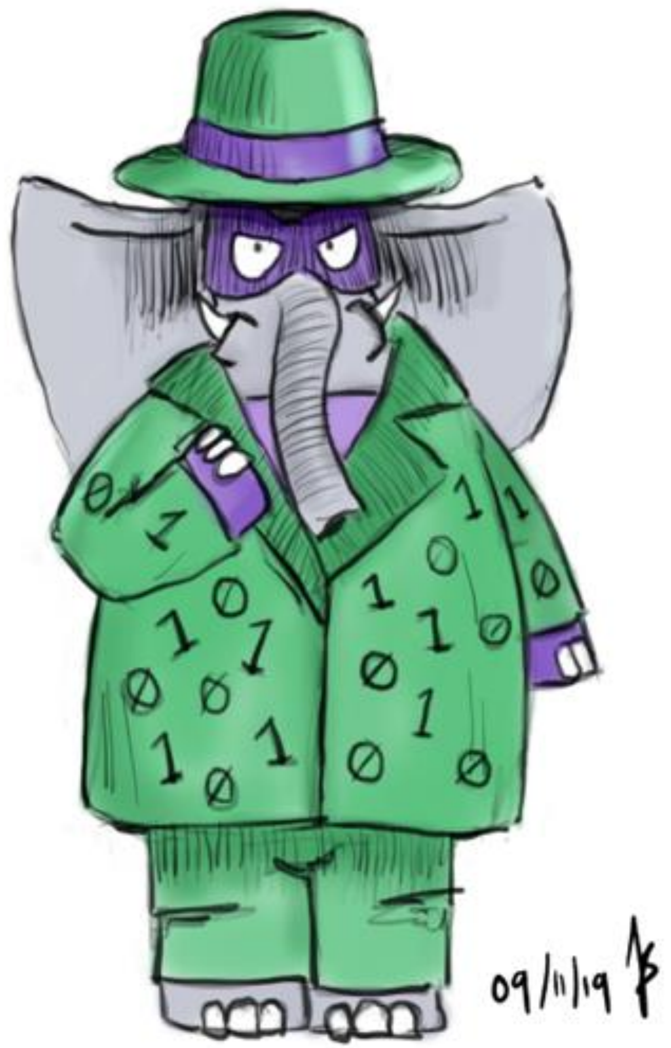
Talking points for today

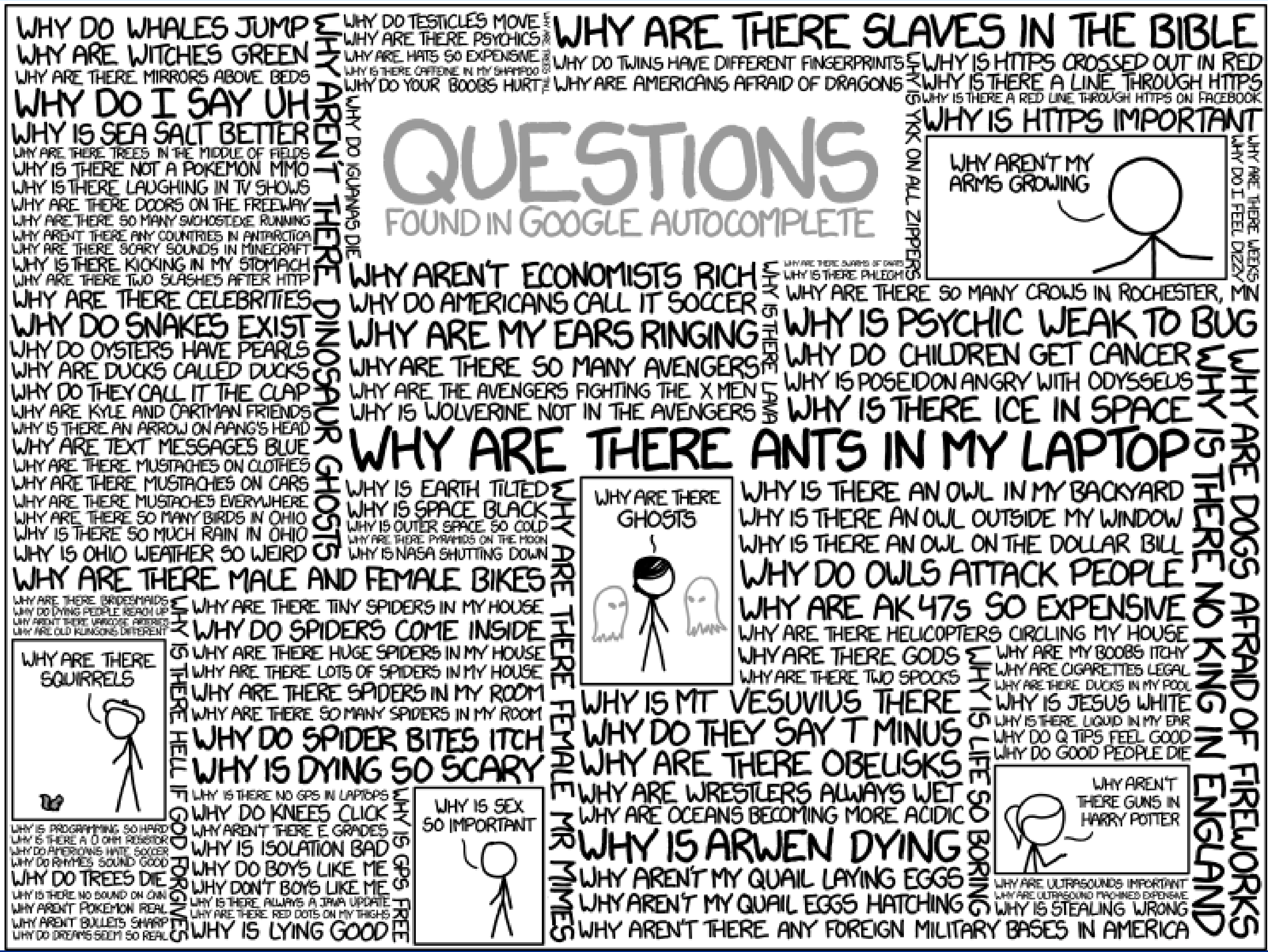
- (3 min) Our fictional case…
- (2 min) Extract knowledgeC.db in Hansken
- (3 min) Extraction plugin concepts
- (5 min) Write logic: parse knowledgeC.db and transform to Hansken types
- (5 min) Extraction plugin template
- (5 min) Add logic to plugin
- (5 min) Run with Hansken.py
- (5 min) Run the plugin during an extraction
- (3 min) Add tests to our code
- **(3 min) Wrap up and questions**

Wrap up

1. **We learned:**
   1. What extractions plugins are,
      how they relate to Hansken.py
      use cases
   2. Where to find plugins created by other community members
   3. How to create, test, and run a new plugin
      by downloading a plugin template and add an actual implementation

2. **A note on extraction plugins in practice:**
   1. Starting to prove itself in action
   2. Technology preview
      please report bugs, and share your experience!
   3. Debugging can be difficult -> “why does my plugin not work”?
   4. Needs to grow!


09/11/19


QUESTIONS
FOUND IN GOOGLE AUTOCOMPLETE
WHY DO WHALES JUMP
WHY ARE WITCHES GREEN
WHY ARE THERE MIRRORS ABOVE BEDS
WHY DO I SAY UH
WHY IS SEA SALT BETTER
WHY ARE THERE TREES IN THE MIDDLE OF FIELDS
WHY IS THERE NOT A POKEMON MMO
WHY IS THERE LAUGHING IN TV SHOWS
WHY ARE THERE DOORS ON THE FREEWAY
WHY ARE THERE SO MANY SVCHOST.EXE RUNNING
WHY AREN'T THERE ANY COUNTRIES IN ANTARCTICA
WHY ARE THERE SCARY SOUNDS IN MINECRAFT
WHY IS THERE KICKING IN MY STOMACH
WHY ARE THERE TWO SLASHES AFTER HTTP
WHY ARE THERE CELEBRITIES
WHY DO SNAKES EXIST
WHY DO OYSTERS HAVE PEARLS
WHY ARE DUCKS CALLED DUCKS
WHY DO THEY CALL IT THE CLAP
WHY ARE KYLE AND CARTMAN FRIENDS
WHY IS THERE AN ARROW ON AANG'S HEAD
WHY ARE TEXT MESSAGES BLUE
WHY ARE THERE MUSTACHES ON CLOTHES
WHY ARE THERE MUSTACHES ON CARS
WHY ARE THERE MUSTACHES EVERYWHERE
WHY ARE THERE SO MANY BIRDS IN OHIO
WHY IS THERE SO MUCH RAIN IN OHIO
WHY IS OHIO WEATHER SO WEIRD
WHY AREN'T THERE DINOSAUR GHOSTS
WHY DO IGUANAS DIE
WHY DO TESTICLES MOVE
WHY ARE THERE PSYCHICS
WHY ARE HATS SO EXPENSIVE
WHY IS THERE CAFFEINE IN MY SHAMPOO
WHY DO YOUR BOOBS HURT
WHY ARE THERE SLAVES IN THE BIBLE
WHY DO TWINS HAVE DIFFERENT FINGERPRINTS
WHY ARE AMERICANS AFRAID OF DRAGONS
WHY IS HTTPS CROSSED OUT IN RED
WHY IS THERE A LINE THROUGH HTTPS
WHY IS THERE A RED LINE THROUGH HTTPS ON FACEBOOK
WHY IS HTTPS IMPORTANT
WHY IS YKK ON ALL ZIPPERS
WHY AREN'T MY ARMS GROWING
WHY ARE THERE WEEKS
WHY DO I FEEL DIZZY
WHY AREN'T ECONOMISTS RICH
WHY DO AMERICANS CALL IT SOCCER
WHY ARE MY EARS RINGING
WHY ARE THERE SO MANY AVENGERS
WHY ARE THE AVENGERS FIGHTING THE X MEN
WHY IS WOLVERINE NOT IN THE AVENGERS
WHY IS THERE LAVA
WHY IS THERE PHLEGM
WHY ARE THERE SO MANY CROWS IN ROCHESTER, MN
WHY IS PSYCHIC WEAK TO BUG
WHY DO CHILDREN GET CANCER
WHY IS POSEIDON ANGRY WITH ODYSSEUS
WHY IS THERE ICE IN SPACE
WHY ARE THERE ANTS IN MY LAPTOP
WHY ARE DOGS AFRAID OF FIREWORKS
WHY IS THERE NO KING IN ENGLAND
WHY IS EARTH TILTED
WHY IS SPACE BLACK
WHY IS OUTER SPACE SO COLD
WHY ARE THERE PYRAMIDS ON THE MOON
WHY IS NASA SHUTTING DOWN
WHY ARE THERE GHOSTS
WHY IS THERE AN OWL IN MY BACKYARD
WHY IS THERE AN OWL OUTSIDE MY WINDOW
WHY IS THERE AN OWL ON THE DOLLAR BILL
WHY DO OWLS ATTACK PEOPLE
WHY ARE AK 47s SO EXPENSIVE
WHY ARE THERE HELICOPTERS CIRCLING MY HOUSE
WHY ARE THERE GODS
WHY ARE THERE TWO SPOCKS
WHY ARE THERE MALE AND FEMALE BIKES
WHY ARE THERE BRIDESMAIDS
WHY DO DYING PEOPLE REACH UP
WHY AREN'T THERE VARICOSE ARTERIES
WHY ARE OLD KLINGONS DIFFERENT
WHY ARE THERE SQUIRRELS
WHY IS THERE HELL IF GOD FORGIVES
WHY ARE THERE TINY SPIDERS IN MY HOUSE
WHY DO SPIDERS COME INSIDE
WHY ARE THERE HUGE SPIDERS IN MY HOUSE
WHY ARE THERE LOTS OF SPIDERS IN MY HOUSE
WHY ARE THERE SPIDERS IN MY ROOM
WHY ARE THERE SO MANY SPIDERS IN MY ROOM
WHY DO SPIDER BITES ITCH
WHY IS DYING SO SCARY
WHY ARE THERE FEMALE MR MIMES
WHY IS MT VESUVIUS THERE
WHY DO THEY SAY T MINUS
WHY ARE THERE OBELISKS
WHY ARE WRESTLERS ALWAYS WET
WHY ARE OCEANS BECOMING MORE ACIDIC
WHY IS ARWEN DYING
WHY AREN'T MY QUAIL LAYING EGGS
WHY AREN'T MY QUAIL EGGS HATCHING
WHY AREN'T THERE ANY FOREIGN MILITARY BASES IN AMERICA
WHY IS LIFE SO BORING
WHY ARE MY BOOBS ITCHY
WHY ARE CIGARETTES LEGAL
WHY ARE THERE DUCKS IN MY POOL
WHY IS JESUS WHITE
WHY IS THERE LIQUID IN MY EAR
WHY DO Q TIPS FEEL GOOD
WHY DO GOOD PEOPLE DIE
WHY AREN'T THERE GUNS IN HARRY POTTER
WHY ARE ULTRASOUNDS IMPORTANT
WHY ARE ULTRASOUND MACHINES EXPENSIVE
WHY IS STEALING WRONG
WHY IS PROGRAMMING SO HARD
WHY IS THERE A 0 OHM RESISTOR
WHY DO AMERICANS HATE SOCCER
WHY DO RHYMES SOUND GOOD
WHY DO TREES DIE
WHY IS THERE NO SOUND ON CNN
WHY AREN'T POKEMON REAL
WHY AREN'T BULLETS SHARP
WHY DO DREAMS SEEM SO REAL
WHY IS THERE NO GPS IN LAPTOPS
WHY DO KNEES CLICK
WHY AREN'T THERE E GRADES
WHY IS ISOLATION BAD
WHY DO BOYS LIKE ME
WHY DON'T BOYS LIKE ME
WHY IS THERE ALWAYS A JAVA UPDATE
WHY ARE THERE RED DOTS ON MY THIGHS
WHY IS LYING GOOD
WHY IS GPS FREE
WHY IS SEX SO IMPORTANT

Thank you for your attention