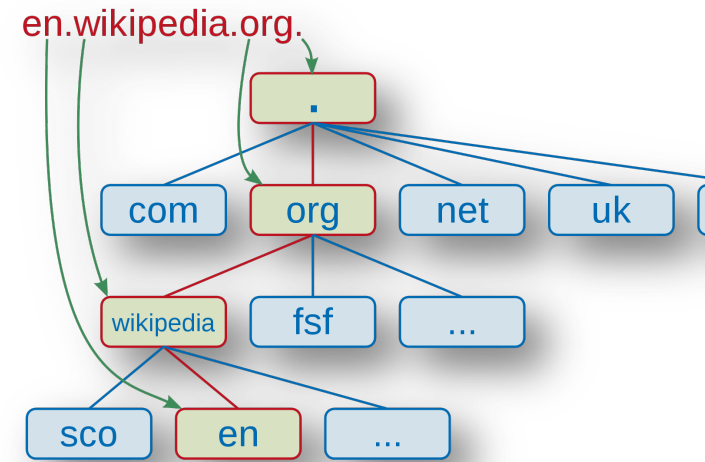
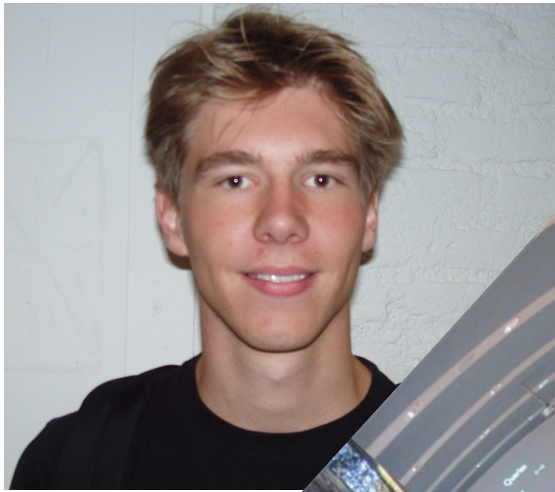


Operationalizing machine learning models for DNS security

Thymen Wabeke, Thijs van den Hout
SV CognAC

1 March 2023 18:00





2009
Intro

2011
CognAC board

2014
Graduated

2015
TNO

2018
SIDN Labs





2015
Start!



2018
BSc ✓



2020
Master Thesis
@UMC



Summer 2021
MSc ✓



Feb 2021 - now
@ SIDN



SIDN is the operator of the .nl TLD

- Provide secure and fault-tolerant registry services for .nl
 - Anycast DNS services with DNSSEC support
 - Registration and domain protection services
- Objective: increase the value of, and society's confidence in the internet
 - Enable safe and novel uses (SIDN Fund, IRMA)
 - Increase internet security and trustworthiness (SIDN Labs)
- Not-for-profit private organization with a public role based in Arnhem

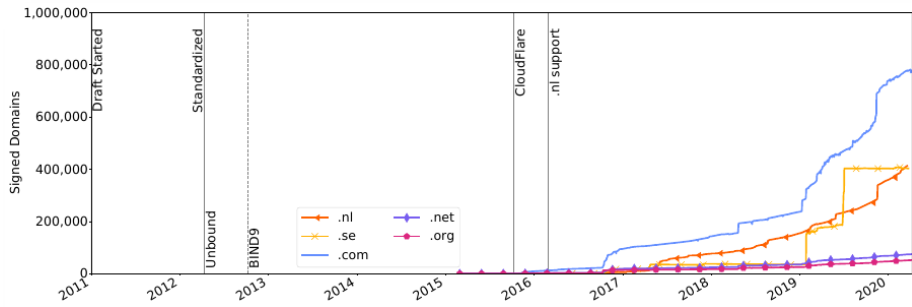


.nl = the Netherlands
~17M inhabitants
6.2M domain names
3.4M DNSSEC-signed
2.5B DNS queries/day
8.6B NTP queries/day

SIDN Labs = research team

- Goal: increase trustworthiness of our society's internet infrastructure, for .nl and the Netherlands in particular.
- Strategies:
 - Applied technical research (measurements, design, prototyping, evaluation)
 - Make results publicly available and useful for various target groups
 - Work with universities, infrastructure operators, and other labs
- Three research areas: network security (DNS, NTP, BGP), domain name & IoT security, secure future internet infrastructures

Example projects



Measuring the deployment of newly standardized DNSSEC algorithms



Provide well-managed and secure time services

securepaymentportal.nl WHOIS DRS Historie Website KASM

Risk score	90%
Name	Stichting Internet Domeinregistratie Nederland
Address	fake address, 12345AB Randomsterdam, NL
Email	support@sidn.nl
Phone	+31.263525555
Registrar	Stichting Internet Domeinregistratie Nederland
Reseller	-
Registration date	2022-12-07 12:00:00
Name servers	ns5.sidn.nl, ns3.sidn.nl, ns1.sidn.nl

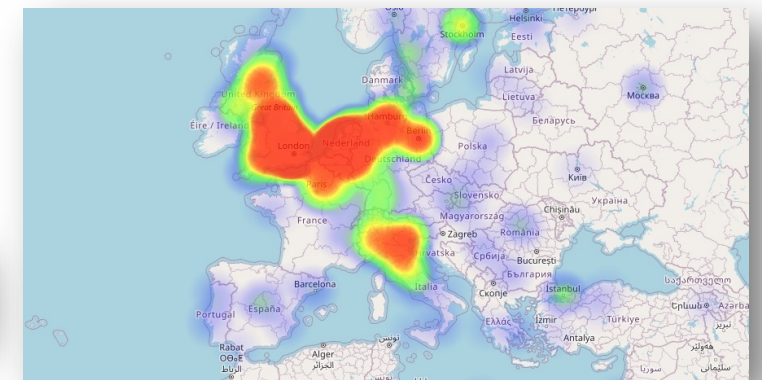
Comment: Could be a scam, given the word 'payment' and invalid address. I will verify registrant's identity.

Reset annotation Previous

Label: High-risk registration, Registration invalid

Status: Pending, Done

Detecting high-risk domain name registrations



Optimize anycast routing



EN | NL

Inloggen bij GGD Online

Hoe wilt u inloggen?

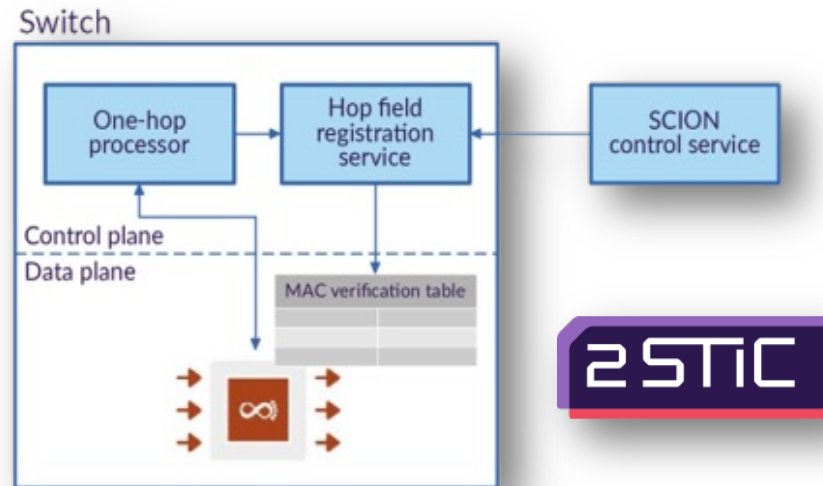
- Met de DigiD app: De makkelijkste manier om veilig in te loggen
- Met een sms-controle
- Met mijn identiteitskaart

Annuleren

Vraag en antwoord

- Ik ben mijn gebruikersnaam vergeten
- Hoe kan ik de sms-controle activeren?
- Waar download ik de DigiD app?

Logo detection technology to identify malicious .nl websites



Experimenting with secure future networks and programmable networks


Applying ML in a responsible way

- Human-in-the-loop
- Simple and interpretable models
- Collaborate and publish

Radboud University



Government of the Netherlands




menu sidn.nl

Home > SIDN Labs > News and blogs > Assessing the r...

Assessing the risk of new .nl registrations using RegCheck

Our system helps to identify potentially malicious domain name registrations and obtains 48% recall and 22% precision



Friday 27 January 2023
Article by: Thymen Wabeke, Thijs van den Hout



Search   Log in



International Conference on Passive and Active Network Measurement
↳ PAM 2020: **Passive and Active Measurement**
pp 158–174 | [Cite as](#)

Counterfighting Counterfeit: Detecting and Taking down Fraudulent Webshops at a ccTLD

[Thymen Wabeke](#)  [Giovane C. M. Moura](#),
[Cristian Hesselman](#) + Show authors

Conference paper |
[First Online: 18 March 2020](#)



UNIVERSITY OF TWENTE.



Graduation internships at SIDN Labs!

Project ideas:

- Resolver classification
- Anomaly detection in DNS traffic
- Representation learning
- Optimize anycast setup
- Estimate risk of terminated domains
- Domain name recommendations
- Estimate popularity of .nl-websites

Previous ML-projects:

- S. Thiessen (TU Delft):
Device Type Classification
- J. Prins (University of Twente):
Proactive Recognition of Domain Abuse
- R. de Heer (Radboud University):
Determine the economic activities associated with domain names
- T. van den Hout (Radboud University):
Using logo detection technology to identify malicious .nl websites

<https://www.sidnlabs.nl/en/afstuderen>

Mail us: sidnlabs@sidn.nl



Today's agenda


- ~~1. Intro [10 min]~~
2. Successful ML applications @ SIDN [20 min]
3. ML with an operational mindset [20 min]


Break

4. Train, evaluate and tune a fraud detection classifier [30 min]
5. Improve classifier using active learning [30 min]

Two successful machine learning projects at SIDN Labs



DamesHerenInloggen | Register | (0) Omschrijving




★★★★★

Hollister Ondergoed Heren Lage Taille Multipack Grijs Groen Camo Zwart 11859-FNX

15 Kleur **BROEK & KORTE BROEK**

~~€30.60~~ **€22.31**




★★★★★

Hollister T Shirt Heren Logo Graphic Korte Mouwen Donkerblauw 21170-HLT

15 Kleur **TOPS**

~~€30.70~~ **€22.38**




★★★★★

Hollister Jas Dames All-weather Stretch Sherpa-lined Zwart 45801-GXL

1 Kleur **JASSEN**

~~€98.35~~ **€69.73**




★★★★★

Hollister Joggingbroek Heren Advanced Stretch Cargo Twill Olijfgroen 97393-SXN

4 Kleur **BROEK & KORTE BROEK**

~~€50.11~~ **€35.98**




★★★★★


Hollister Blouses Dames Fluweel Off-the-shoulder Goud 49289-JQI

2 Kleur **TOPS**


~~€30.60~~ **€22.31**




★★★★★




★★★★★




★★★★★




★★★★★



★★★★★





SIDN's interest

- Consumer losses
- Trust in Internet may decrease

Perfect vantage point:

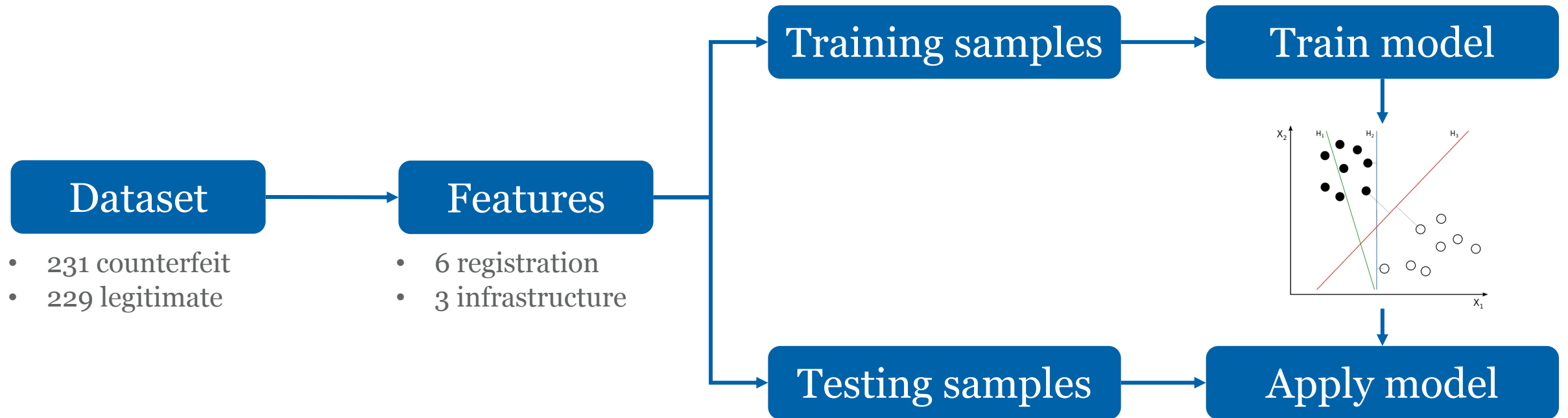
- List of *all* .nl - domains
- Passive and active measurements



Main results

- Detected thousands since 2016
- Protected users from being scammed
- PAM2020 paper:
 - BrandCounter (2018 Q1-2)
 - FaDe (2019 Q1)





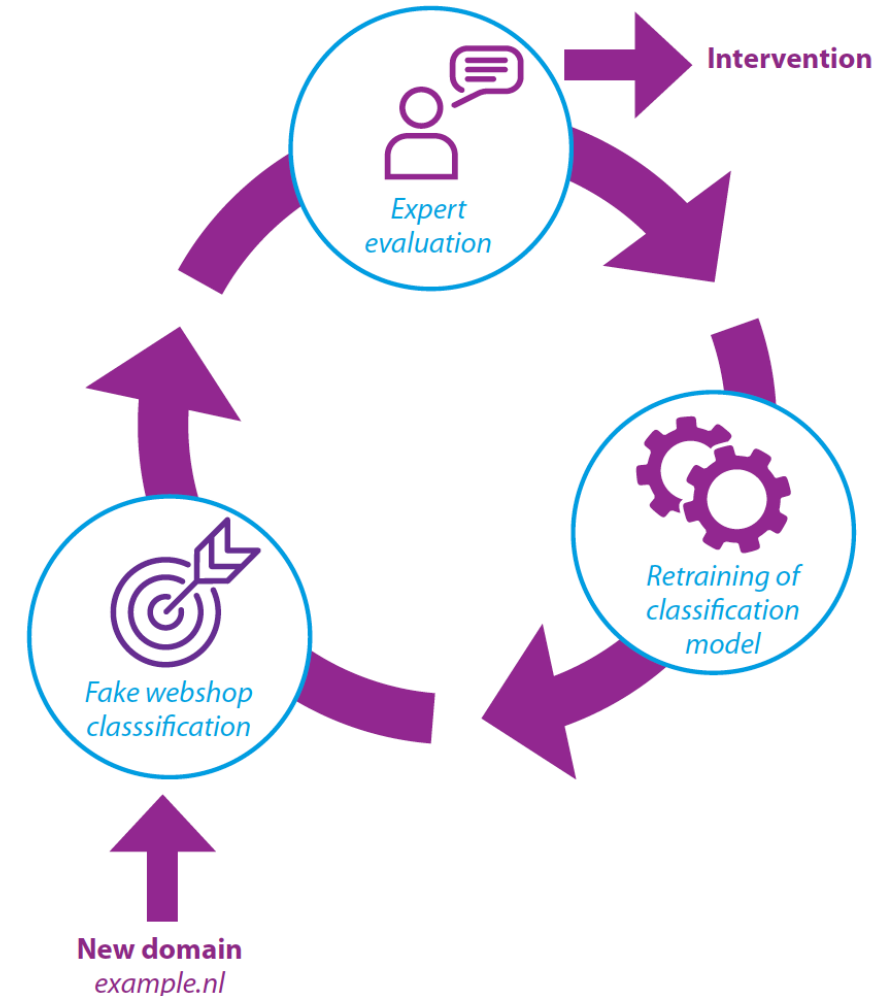
Samples	Precision	Recall
Train (cross-validation)	0.98	0.97
Test	1.0	1.0

Lessons learned

- Registrar and ICS collaboration was key
- Detectors are simple yet effective
 - Registries have perfect vantage point
 - Suggests little pressure

Year	Taken down
2018	~12,000
2019	4,340
2020	481

Number of counterfeit webshops taken down



LogoMotive: finding malicious .nl-domains with logo detection

Pagina's

- Home
- Problemen
- Vragen
- Nieuws
- Video's
- Quizen
- Over ons

Volg ons

- Facebook
- Twitter
- Instagram
- YouTube
- Vimeo

Privacyverklaring Cookieverklaring Responsible disclosure Disclaimer Ditoegankelijkheid

Een initiatief van:

- rijksoverheid 0.9
- rijksoverheid 0.98
- Ministerie van Economische Zaken en Klimaat
- Nationaal Cyber Security Centrum Ministerie van Justitie en Veiligheid
- ECP Platform voor de InformatieSamenleving

Mede mogelijk gemaakt door:

- kpn
- vodafone
- Ziggo
- Betaalvereniging Nederland
- sidn 0.97
- Google
- Microsoft
- thuiswinkel 0.95
- thuiswinke.org
- SENORWEB
- mediaspout
- SIC
- NLdigital
- FRAUDEHELPDESK.nl
- ACM ConsuWijzer
- Co-financed by the European Union Connecting Europe Facility
- veilig internetten.nl

EN | NL

rijksoverheid 0.98

Inloggen bij GGD Online

Hoe wilt u inloggen?

- Met de DigiD app
De makkelijkste manier om veilig in te loggen
- Met een sms-controle
- Met mijn identiteitskaart
- Annuleren

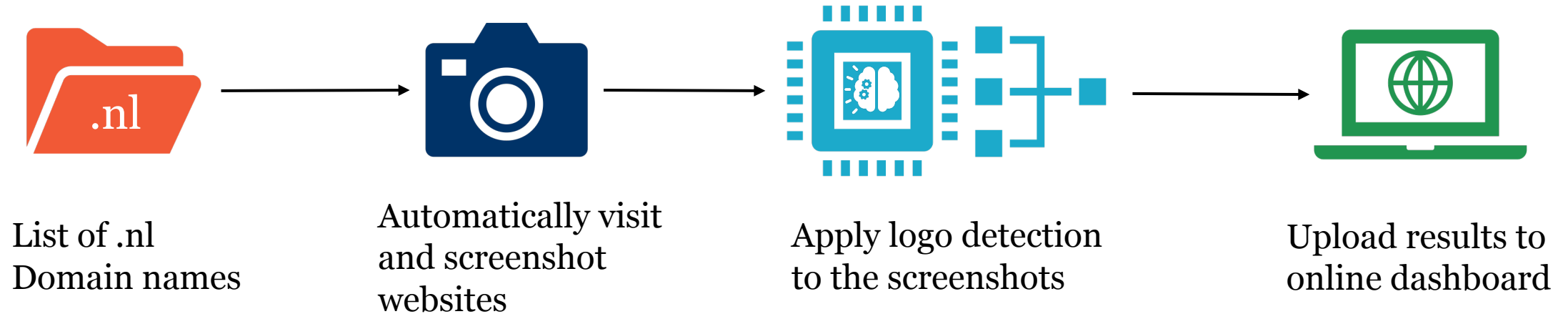
Kunt u niet verder? Download dan de DigiD app [opent in een nieuw venster] of activeer de sms-controle [opent in een nieuw venster]

Nog geen DigiD? Vraag uw DigiD aan

Vraag en antwoord

- Ik ben mijn gebruikersnaam vergeten

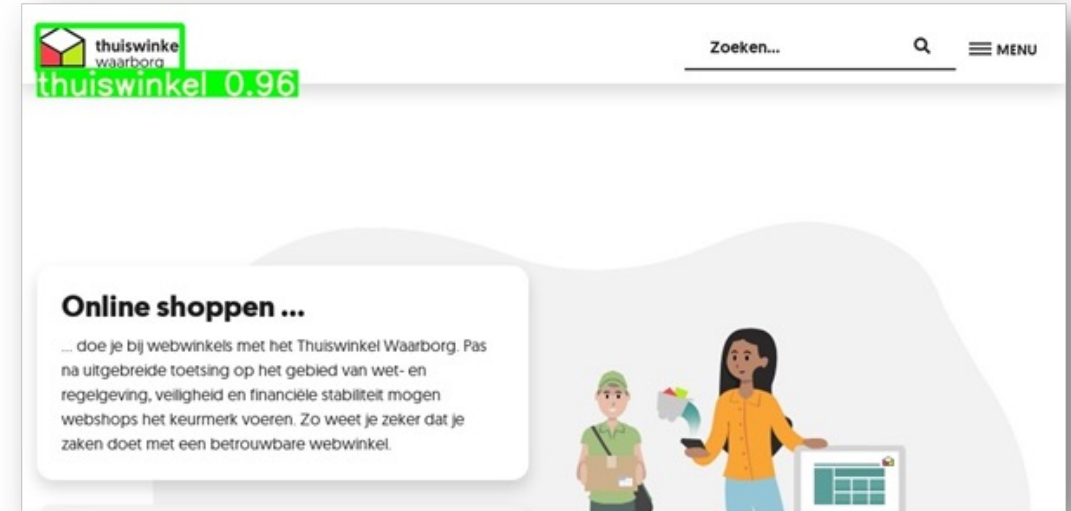
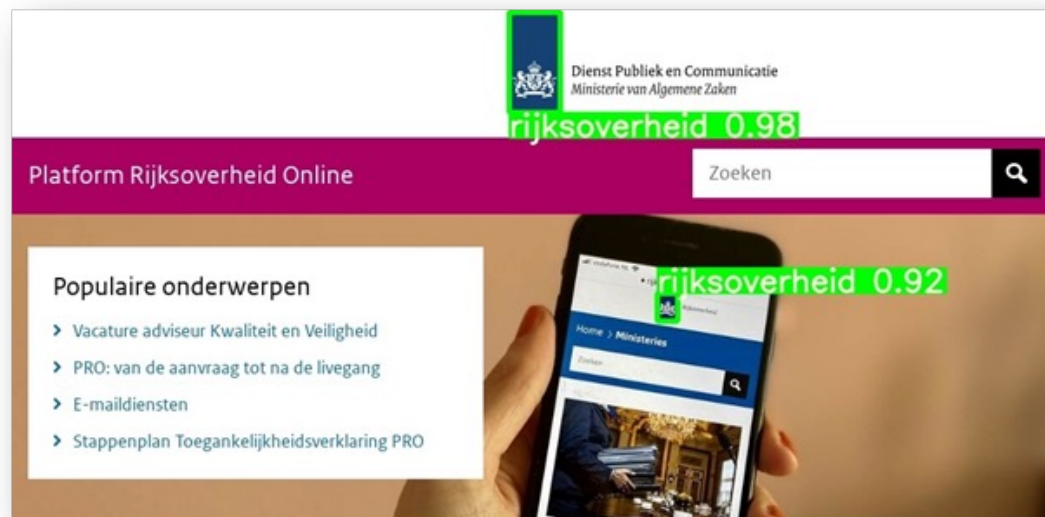
How does LogoMotive work?



Can logo detection contribute to a safe .nl-zone?

Case study with Dutch national government

Found: Phishing, suspicious redirects, security threats



Case study with Dutch webshop trustmark (Thuiswinkel.org)

Found: Trustmark abuse, improved domain portfolio

More info & paper: logomotive.sidnlabs.nl



Machine learning with an operational mindset



Part 2/4

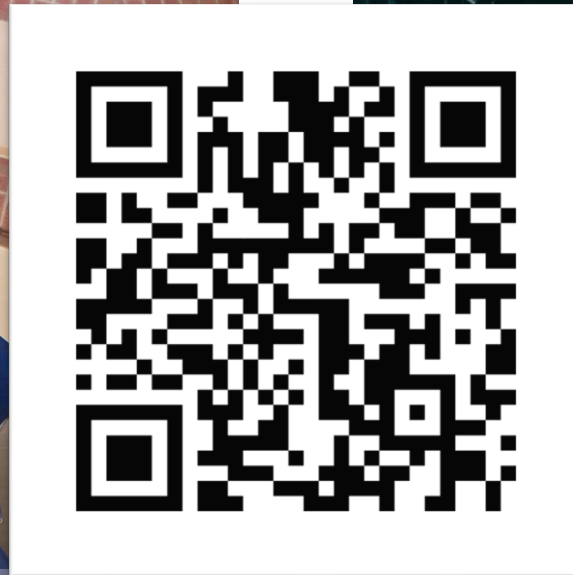
Use case: detect suspicious registrations

- 22%-62% of abusive domains were registered with malicious intents
 - Phishing, malware, DGAs
- Verifying new registrations could prevent malicious registrations
 - But: +/- 2500 registrations per day
 - But: reviewing a registration takes 5-20 minutes
 - But: only 3 (0.11%) reported at Netcraft within 30 days
- Goal: identify registrations that should be reviewed

Research vs. operational environment

- Project is suitable for:
 - Research project at a university (outcome = paper)
 - Operational project within an organization (outcome = deployed classifier)
- How will developing the classifier differ between these 2 environments?

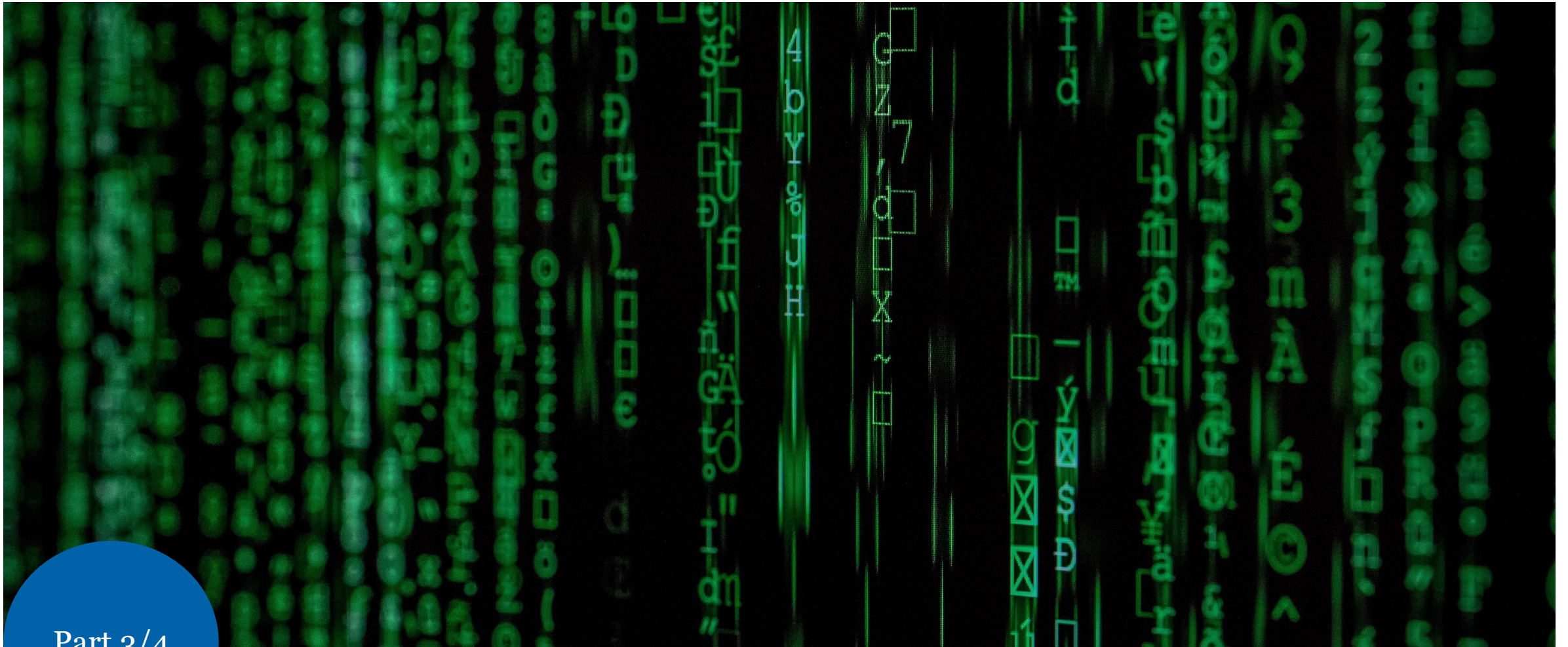
Research vs. operation: identify differences



Go to www.menti.com and enter 7167 3714



Train, evaluate & tune a fraud detection classifier



Part 3/4

10-minute break

Characteristics of classification problem

	RegCheck	TransactCheck
Row	New domain name registrations	Credit card transactions
Number of rows	~ 900k in 2021	~ 286k for a year
Class labels	Class 0: Not reported Class 1: Reported within 28 days	Class 0: Legitimate Class 1: Fraudulent
Goal	Detect malicious registrations	Detect fraudulent transactions
Abuse ratio	~ 0.11%	~ 0.17 %
Labelling costs	Strong labels expensive	Strong labels expensive
Input	Domain name, registrar, creation date, name servers, name and address details of registrant.	Transaction amount, 28 unnamed features which are components generated by a PCA
Sensitivity	Many PIDs	No PIDs due to PCA

Characteristics of classification problem

	RegCheck	TransactCheck
Row	New domain name registrations	Credit card transactions
Number of rows	~ 900k in 2021	~ 286k for a year
Class labels	Class 0: Not reported Class 1: Reported within 28 days	Class 0: Legitimate Class 1: Fraudulent
Goal	Detect malicious registrations	Detect fraudulent transactions
Abuse ratio	~ 0.11%	~ 0.17 %
Labelling costs	Strong labels expensive	Strong labels expensive
Input	Domain name, registrar, creation date, name servers, name and address details of registrant.	Transaction amount, 28 unnamed features which are components generated by a PCA
Sensitivity	Many PIDs	No PIDs due to PCA

Assignment 1: Develop a TransactCheck model

- Explore dataset
- Train 2 or more `scikit-learn` models using balanced dataset of 2 weeks
 - At least 1 interpretable model
- Tune and test models using holdout data
 - Precision vs. recall tradeoff
 - Choose a threshold

Instructions

1. Find a coding partner
2. Browse to <https://colab.research.google.com> and sign-in with a Google Account
3. New to Google Colab and/or Jupyter Notebook?
Browse to <https://colab.research.google.com/notebooks/intro.ipynb>
4. Ready for the real deal?
Browse to **github.com/SIDN/ml_workshop** and click on the Assignment1 link in the README

Results assignment 1



Go to www.menti.com and enter 7167 3714

Improve classifier using active learning

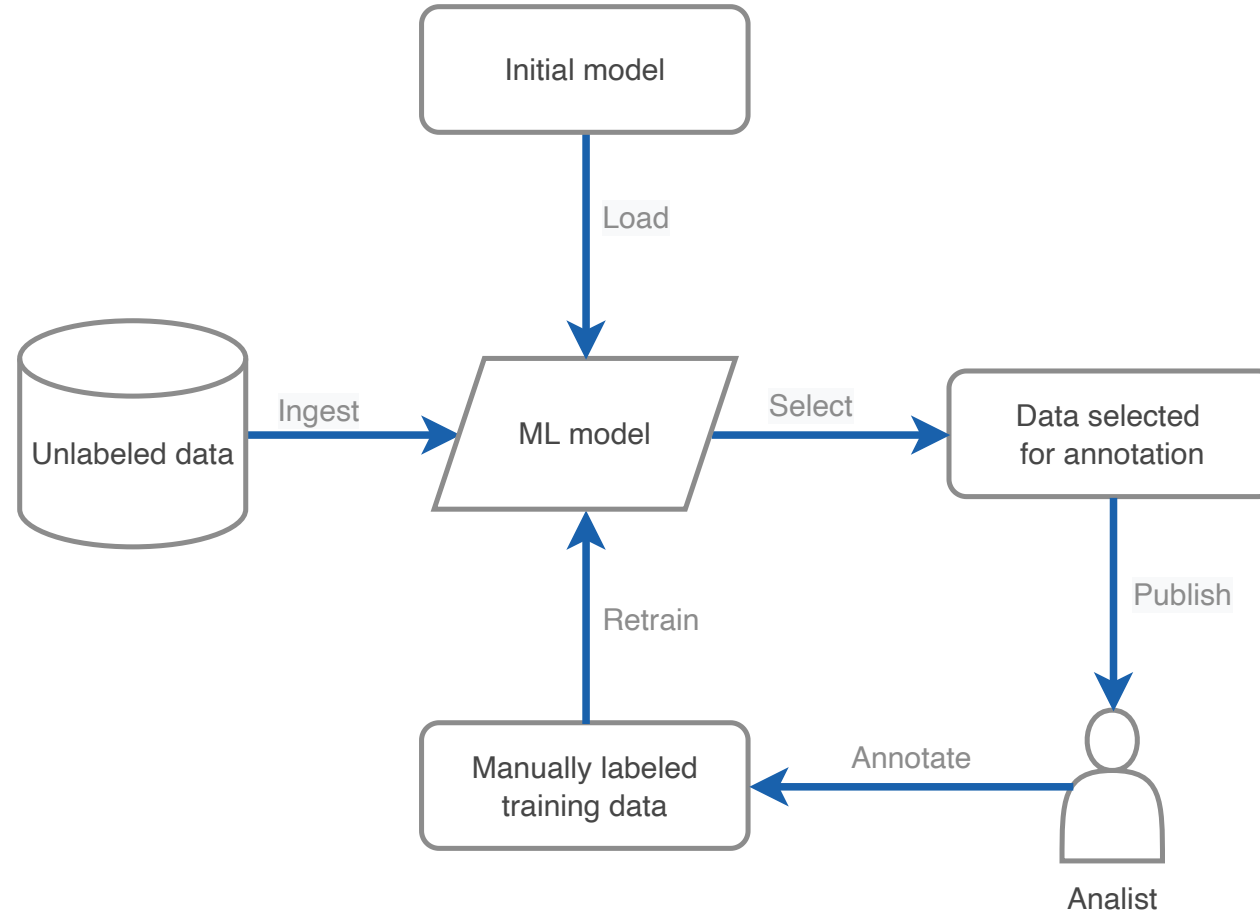


Part 4/4

Goals of active learning

- Minimize the labelling effort of human annotators
- Increase the accuracy of a machine learning model
- Reach the target accuracy of a machine learning model faster

Human-in-the-loop learning process

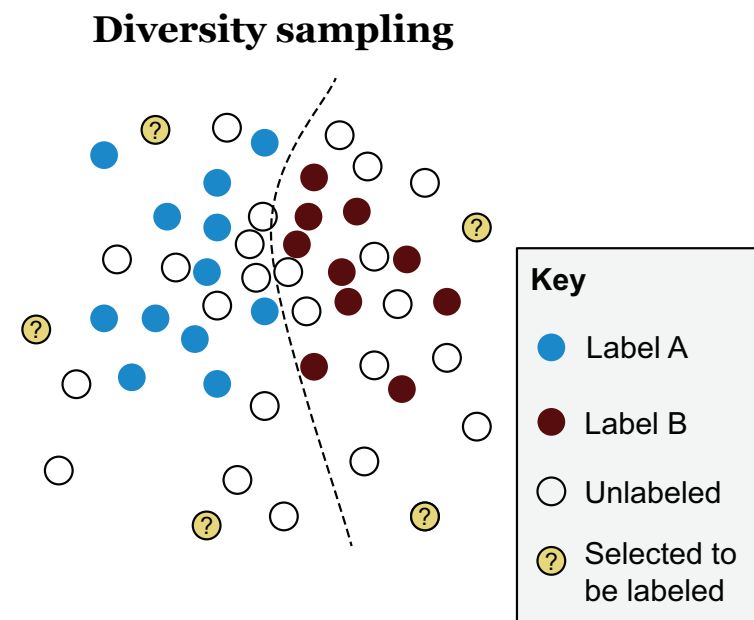
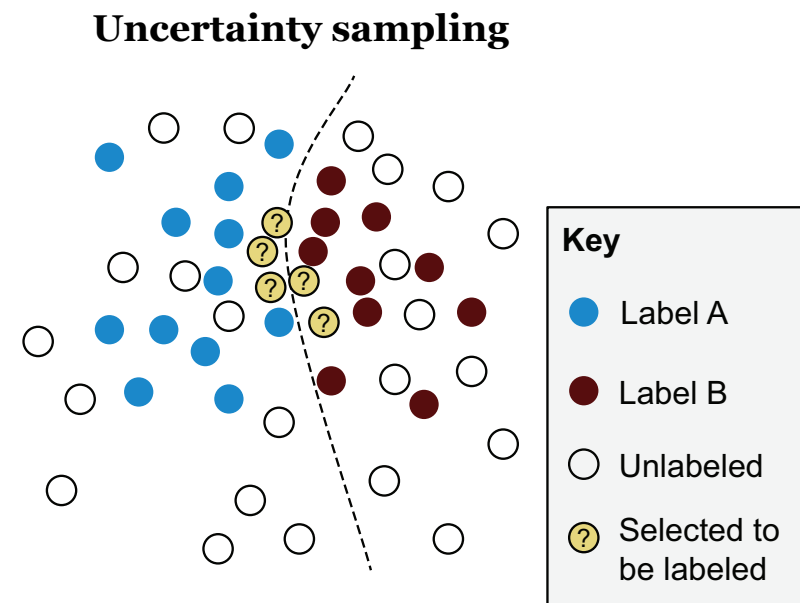


Active learning is no free lunch

- What is an informative datapoint?
- What if the model assumptions are wrong?
- How many informative datapoints should be labeled?
- Does model performance improve?

What is an informative data point?

- Random sampling: each item has a fair chance of being selected (unbiased)
- Uncertainty sampling: select items close to decision boundary of a model
- Diversity sampling: select items underrepresented or unknown to a model
- Community disagreement sampling: select items that a community of models classify differently



Assignment 2: improve model using active learning

- Explore implemented sampling strategies
- Find best sampling strategy to improve model performance
 - A training iteration every week
 - Annotation budget: 50 data points per iteration
 - Measure improvement using average precision (AP)
- Implement your own sampling strategy (if time permits)

Instructions

1. Find a programming partner
2. Browse to **github.com/SIDN/ml_workshop** and click on Assignment2 in the README

Results assignment 2



Go to www.menti.com and enter 7167 3714

Volg ons

 SIDN.nl

 @SIDN

 SIDN

Q&A

www.sidnlabs.nl | stats.sidnlabs.nl

Thymen Wabeke
Research engineer
thymen.wabeke@sidn.nl

Thijs van den Hout
Research engineer
thijs.vandenhout@sidn.nl

Thanks to Unsplash.com and its
photographers for beautifying these slides

