QUANTIFYING UNIFORMITY WITHIN FORENSIC TOOLS

Harm van Beek, PhD
Netherlands Forensic Institute
h.van.beek@nfi.nl

Christoph Lofi, PhD
Delft University of Technology
c.lofi@tudelft.nl

Roel van Dijk, MSc
Netherlands Forensic Institute
r.van.dijk@nfi.nl

Luuk van Campen, BSc
Delft University of Technology, NFI
l.van.campen@nfi.nl

GOAL

The capabilities of forensic search engine Hansken can be increased by integrating open-source forensic tools. While the CASE ontology is not widely adapted, a manual schema matching approach is the only way to create such integrations. However, this process is difficult due to a lack of uniformity within those tools; quantifying this lack of uniformity provides an insight into the difficulty of creating the matching. This helps Hansken's developers with making well-founded choices on what tool to prioritise.

RESEARCH QUESTION

- **How can uniformity of forensic tool output be quantified?**
- **How uniform is the output of commonly found open-source forensic tools?**

CHALLENGE

A lack of uniformity can manifest itself in several ways. We make the distinction between **semantic** and **syntactic** uniformity, and divide those up into three levels: **high**, **low**, and **structural**.

Open-source forensic tools generally do not come with an explicit schema or data-model that helps us understand what their output means or how it is structured, and what digital traces are returned and what not.

Although data integration has been a lively research topic for decades, to the best of our knowledge, the kind of uniformity metric described in this research has not been created before.

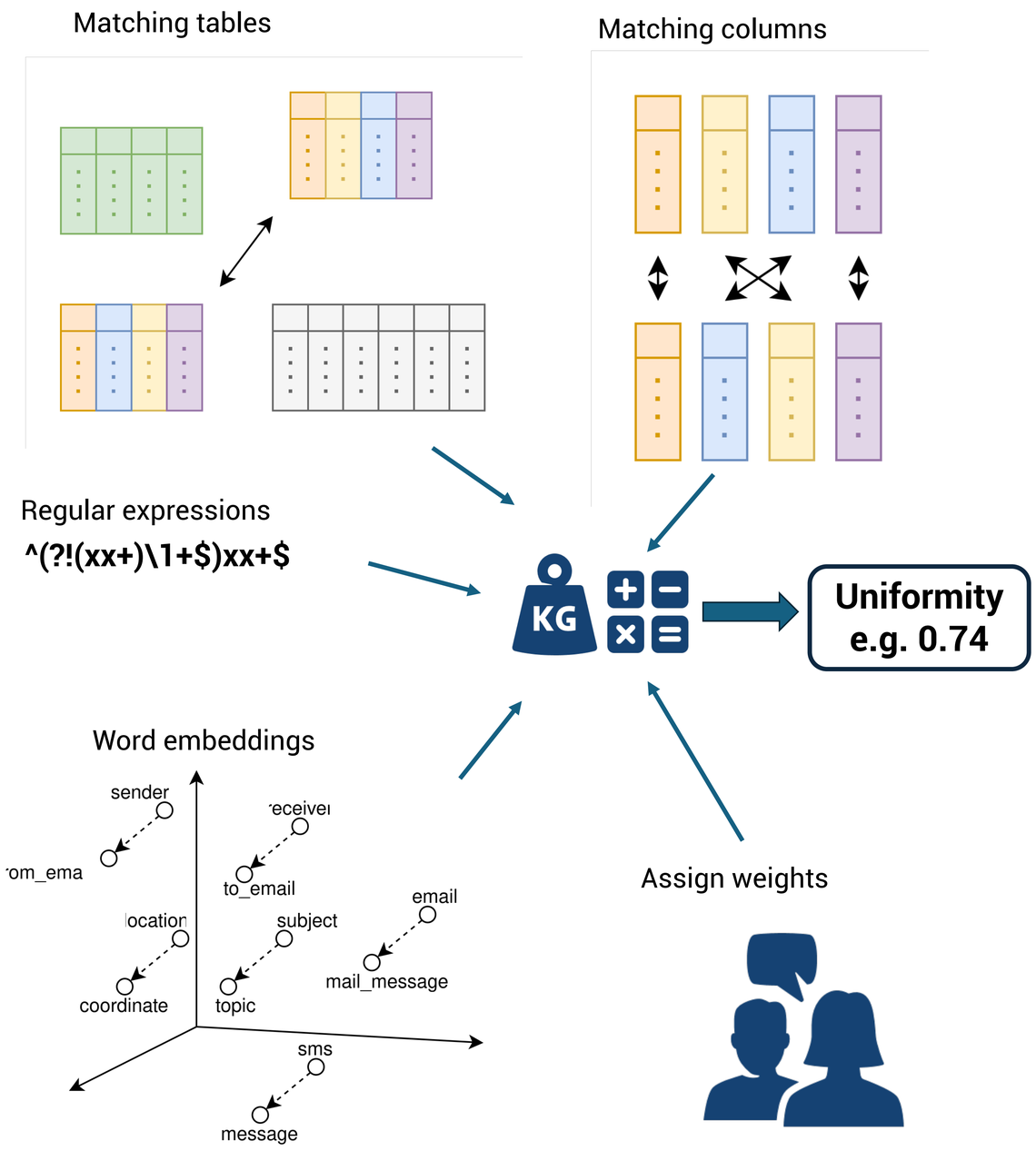
EXAMPLE FROM TOOL X

Outlook_mail_message				
Sender	**Receiver**	**Send_time**	**Subject**	**Content**
l.van.campen@nfi.nl	dfrws@dfrws.org	1708950804	"Poster presentation"	"Hello, I'm a poster!"

versus

apple_email						
Sender	**Receiver**	**From_email**	**To_email**	**Send_time**	**Subject**	**Content**
Luuk van Campen	DFRWS	l.van.campen@nfi.nl	dfrws@dfrws.org	Mon Feb 26 2024 12:33:24 GMT+0000	"Poster presentation"	"Hello, I'm a poster!"

METHOD



OPEN-SOURCE FORENSIC TOOLS

- Plaso
- IPED Digital Forensic Tool
- XLEAPP
- ILEAPP, ALEAPP, WLEAPP
- The Sleuthkit
- Mac-apt
- IOS_sysdiagnose_forensic_scripts
- APOLLO
- Tap-ir
- Dissect

MORE INFORMATION

Master's Thesis project, running from November 2023 until June 2024.

www.hansken.org
www.caseontology.org

Find this poster online: