SANS

OSINT SUMMIT 2023

Free Live Online Summit:
Friday, September 22

sans.org/OSINT-Summit

OSINT AS AN INVESTIGATIVE TOOL

"Without a reproduceable investigative method, OsInt is nothing more than a bunch of cool tools that deep dive for data."

Craig Pedersen (CFE) FP(SA) CCCi

SANS OSINT SUMMIT 2023

INVESTIGATIVE METHODOLOGY

- WHAT IS INVESTIGATIVE METHODOLOGY?
- HAVE WE PROGRESSED FROM SHERLOCK HOLMES?
- WHAT METHODS ARE THERE FOR INVESTIGATION?
- HOW DO THEY TRANSLATE TO THE DIGITAL SPACE?

WITNESS ACCOUNT

- Who is a witness
- How many people interview a witness
- Cognitive behaviour
- Non-verbal indicators
- Speech patterns
- Time manipulation
- Lack of detail
- Overcompensation of detail
- Cross referencing witness accounts
- Statement analysis
- Finding additional witnesses and supporting data

TIMELINE

- Establish a fixed point from which to work
- Cast the line as broad as you feel necessary
- Create a fact board and an information board
- Move data between fact and information as it is verified
- What else can be used to verify the information
- Does verification as a fact lead to other data?
- What ancillary data could exist? Even if you don't have it
- Account for each hour/ minute on the timeline
- Analyse gaps – what could have happened before/ after
- Question inaccuracies in reported data and either confirm or suspect
- Data must always be cross referenced for confirmation

BASELINE

- “If you cannot measure it – you cannot manage it”
- If you cannot baseline it you cannot compare it!
- Locards principle – micro analysis
- Comparative Analysis

```
Received: from antivirus1.its.rochester.edu (antivirus1.its.rochester.edu
[128.151.57.50])
        by mail.rochester.edu (8.12.8/8.12.4) with ESMTP id h2OGQs9o002563;
        Mon, 24 Mar 2003 11:26:54 -0500 (EST)
Received: from antivirus1.its.rochester.edu (localhost [127.0.0.1])
        by antivirus1.its.rochester.edu (8.12.8/8.12.4) with ESMTP id
h2OGQrQx003450;
        Mon, 24 Mar 2003 11:26:54 -0500 (EST)
Received: from galileo.cc.rochester.edu (galileo.cc.rochester.edu
[128.151.224.6])
        by antivirus1.its.rochester.edu (8.12.8/8.12.4) with SMTP id
h2OGQrDC003447;
        Mon, 24 Mar 2003 11:26:53 -0500 (EST)
Received: (from majord@localhost)
        by galileo.cc.rochester.edu (8.12.8/8.12.4) id h2OGQq91029757;
        Mon, 24 Mar 2003 11:26:52 -0500 (EST)
Date: Mon, 24 Mar 2003 11:26:50 -0500 (EST)
From: somesender@mail.rochester.edu
Message-Id: <200303241626.h2OGQojt002507@mail.rochester.edu>
To: someuser@its.rochester.edu
Subject: My mail message is about:
```

FORENSIC

- Only concerned with facts
- No conclusion is often reached
- Substantiating data and cross referencing
- Establishing missing elements
- Creating links
- Meticulous attention to detail
- The use of science, mathematics and medicine
- Data science

APPLYING METHODS TO OSINT

Scope	Be very specific on what the scope of work is
Layer	Identify which data layer is most likely to yield a results
Toolsets	Identify which tools will aid your research
Research	Conduct your data research
Analysis	Analyze the data for accuracy and interpretation
Capture	Capture your results in the court approved method
Reporting	Be concise and factual in your outcomes

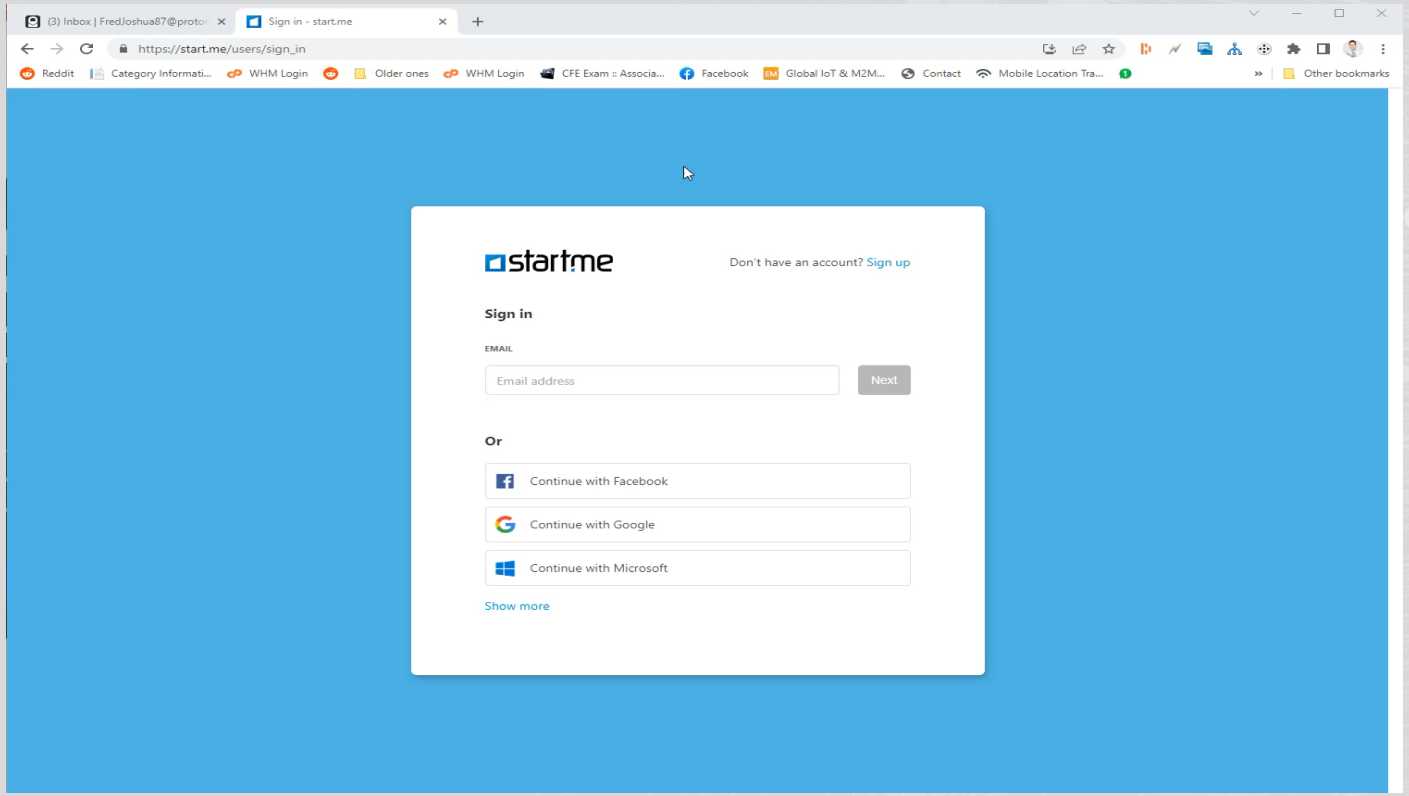
TOOL SUITABILITY AND SELECTION

- Fit to purpose
- Data retention if it's an online tool
- Patterning of you as an investigator
- Accuracy & Alternatives
- Availability

MINIMUM METHOD

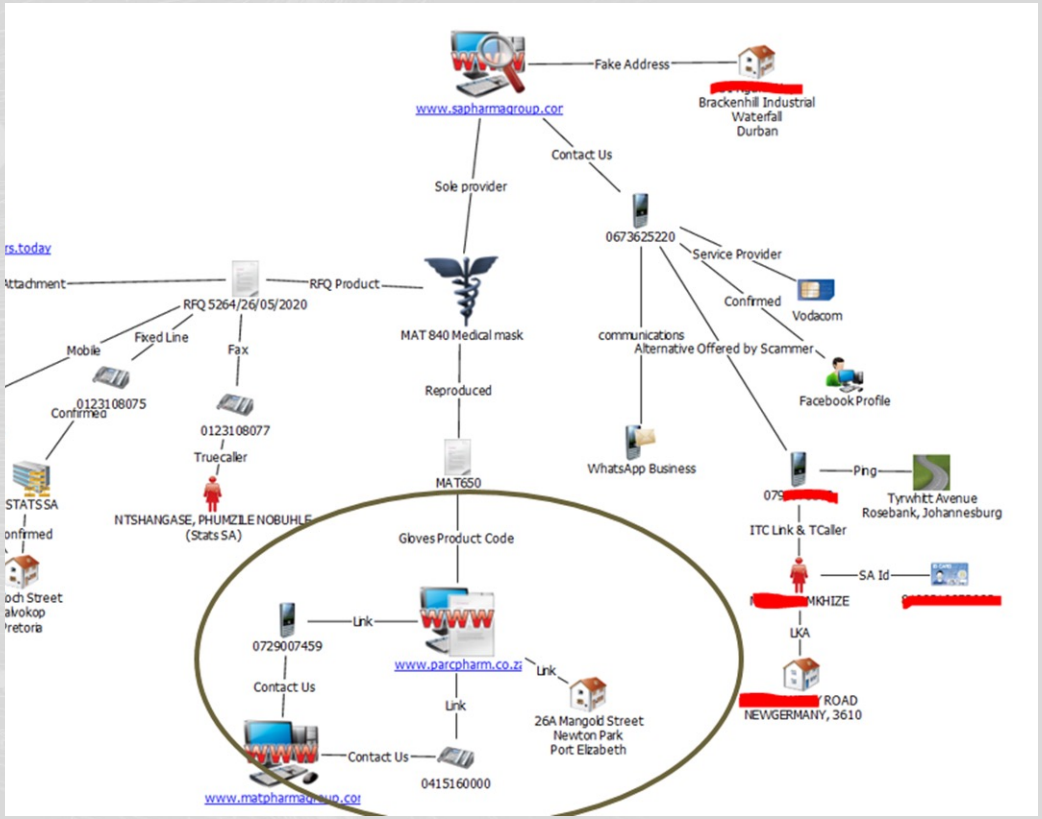
Use bookmark managers to control workflow.

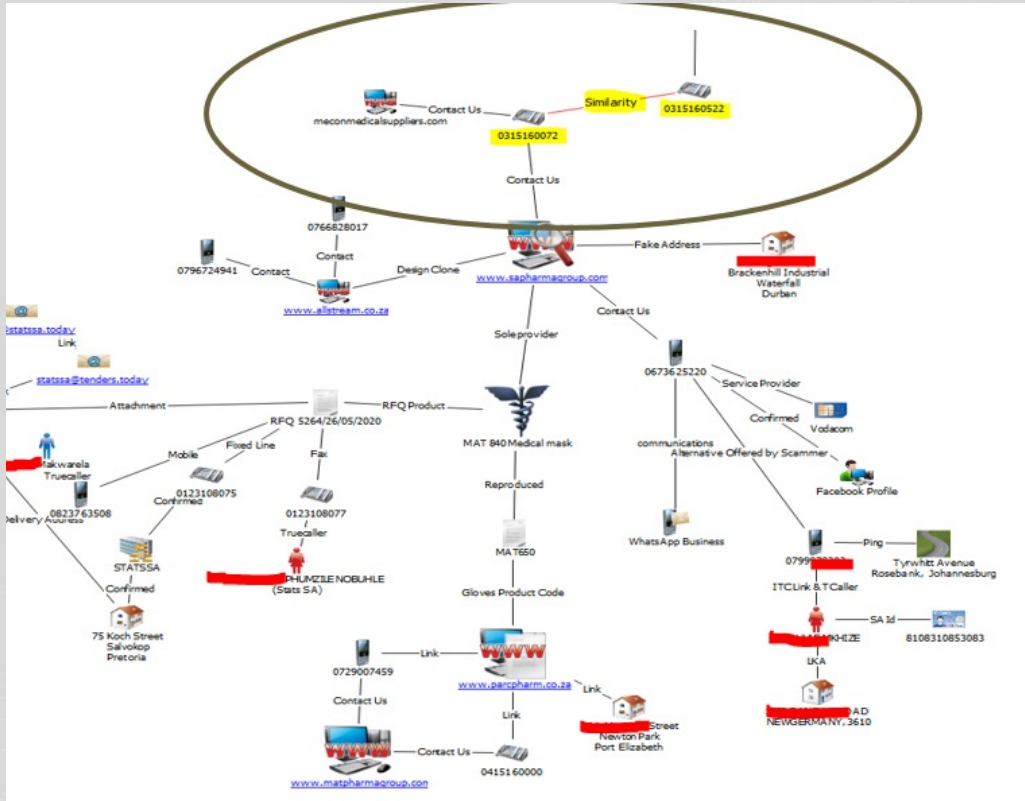
If you cannot reproduce the results- you can’t achieve consistency in your output.



SANS OSINT SUMMIT 2023

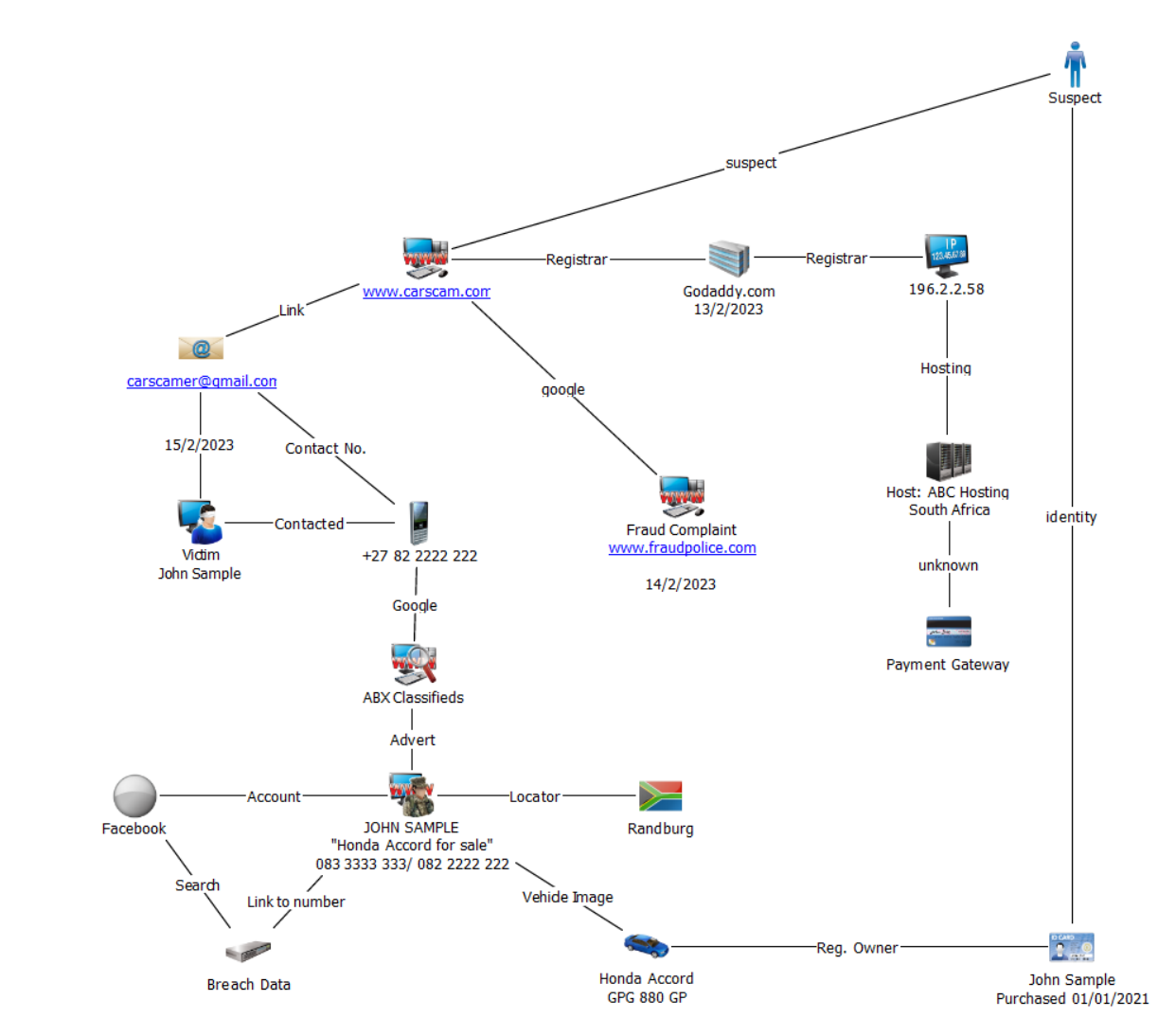
LATCHES AND PIVOTS





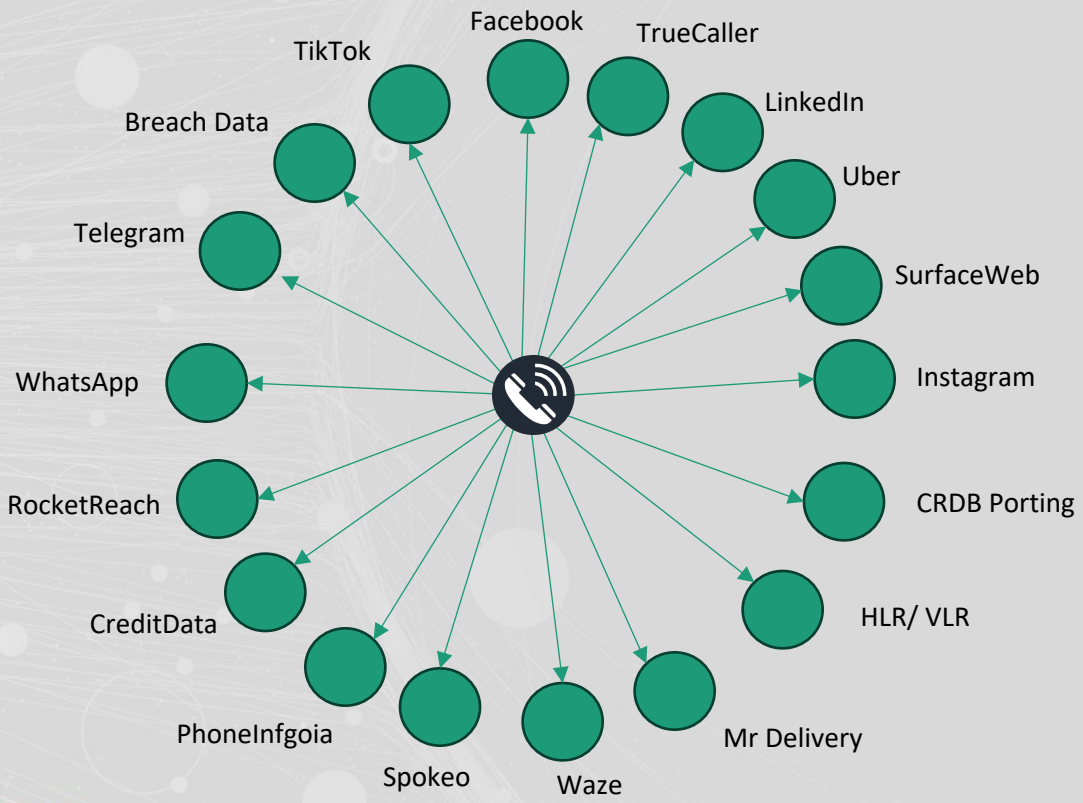
SANS
OSINT SUMMIT
2023

LATCHES AND PIVOTS

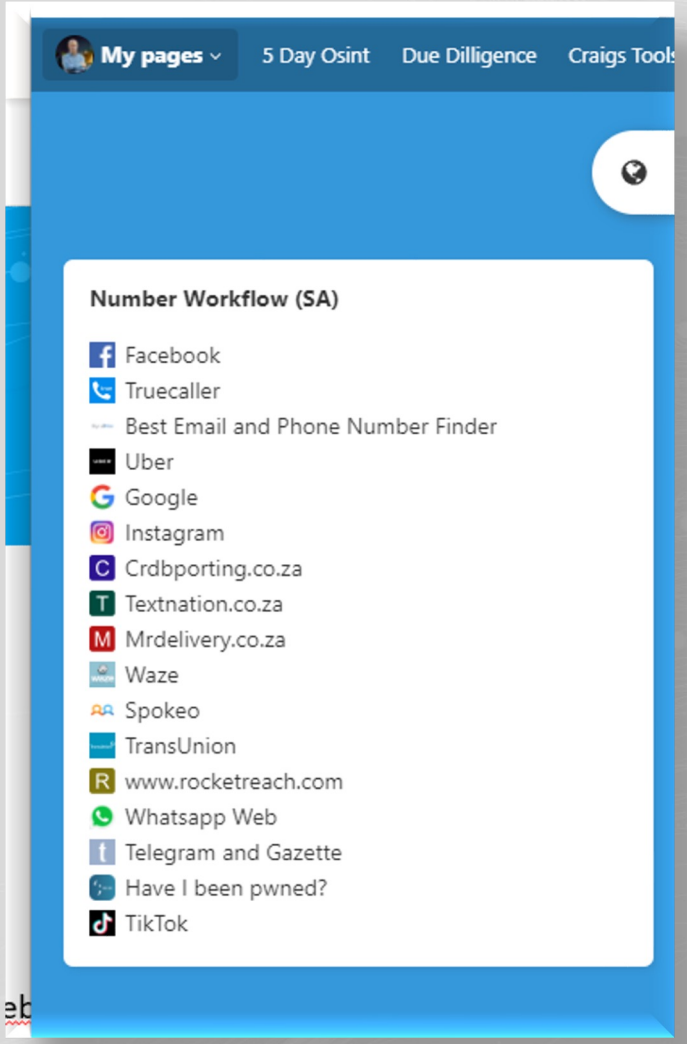


SANS OSINT SUMMIT 2023

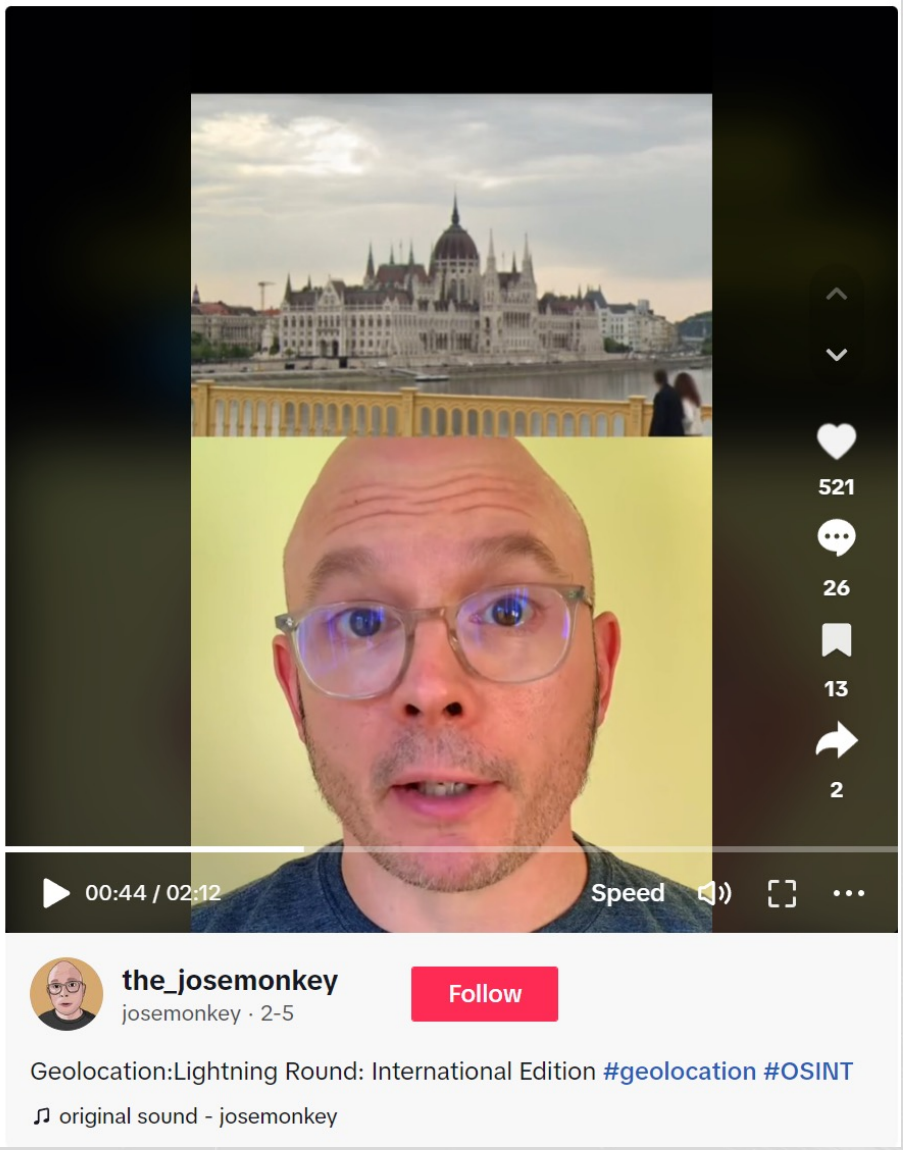
VISUALIZATION



SANS OSINT SUMMIT 2023

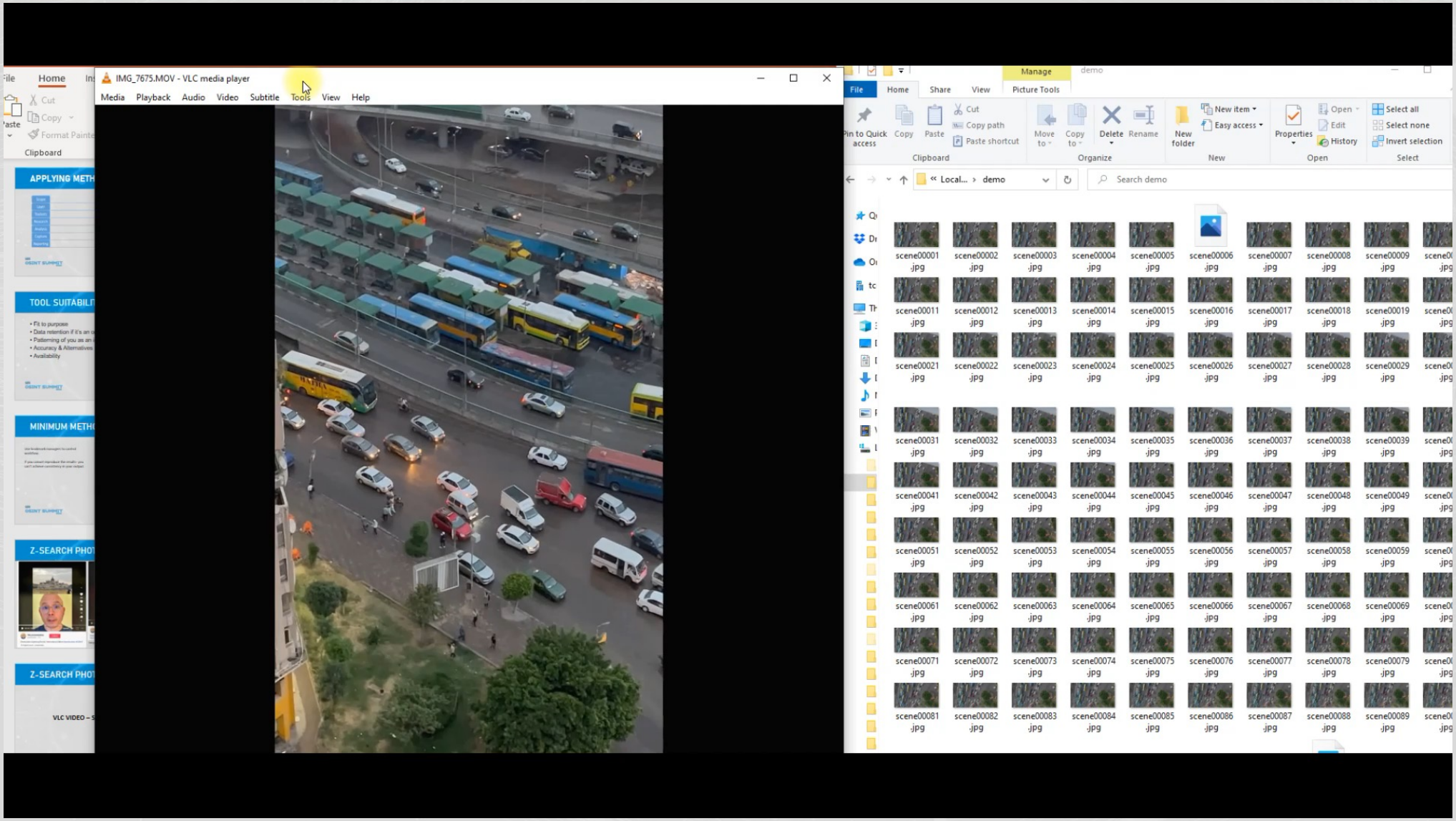


Z-SEARCH PHOTOS

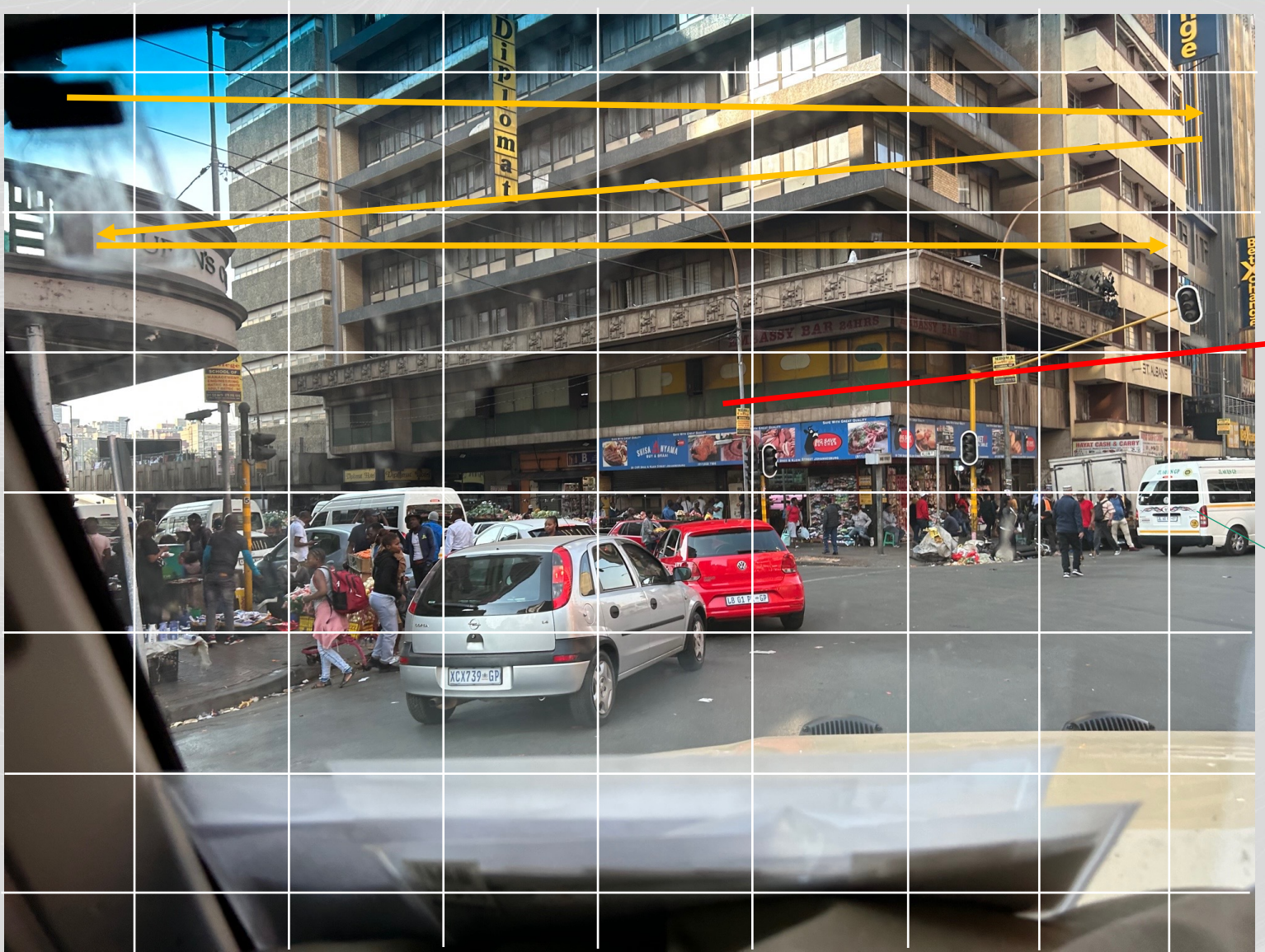


https://www.tiktok.com/@the_josemonkey

VLC PLAYER FOR IMAGE SLICING



Z-SEARCH PHOTOS



PRACTICAL APPLICATION

SCOPE & PLAN

Identify what data you need.

Which layer is the data most likely to be on?

Which tools will help you acquire the data/ answer?

What alternate tools can be used?

METHODOLOGY

Work to your own minimum method.
Use tools to enforce the method.

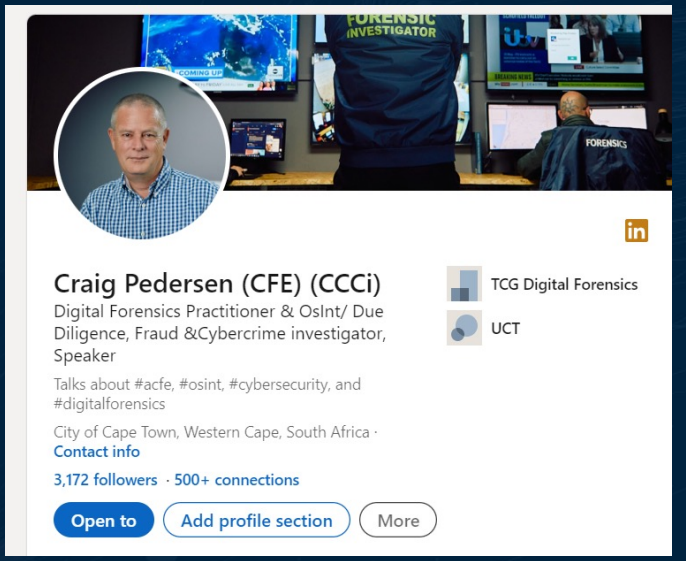
TECHNIQUE

Visualize and link your research.
Reduce video to slices.
Use the Z search method when working with images.

OSINT AS AN INVESTIGATIVE TOOL

"Without a reproduceable investigative method, OsInt is nothing more than a bunch of cool tools that deep dive for data."

Craig Pedersen (CFE) FP(SA) CCCi



SANS OSINT SUMMIT 2023