

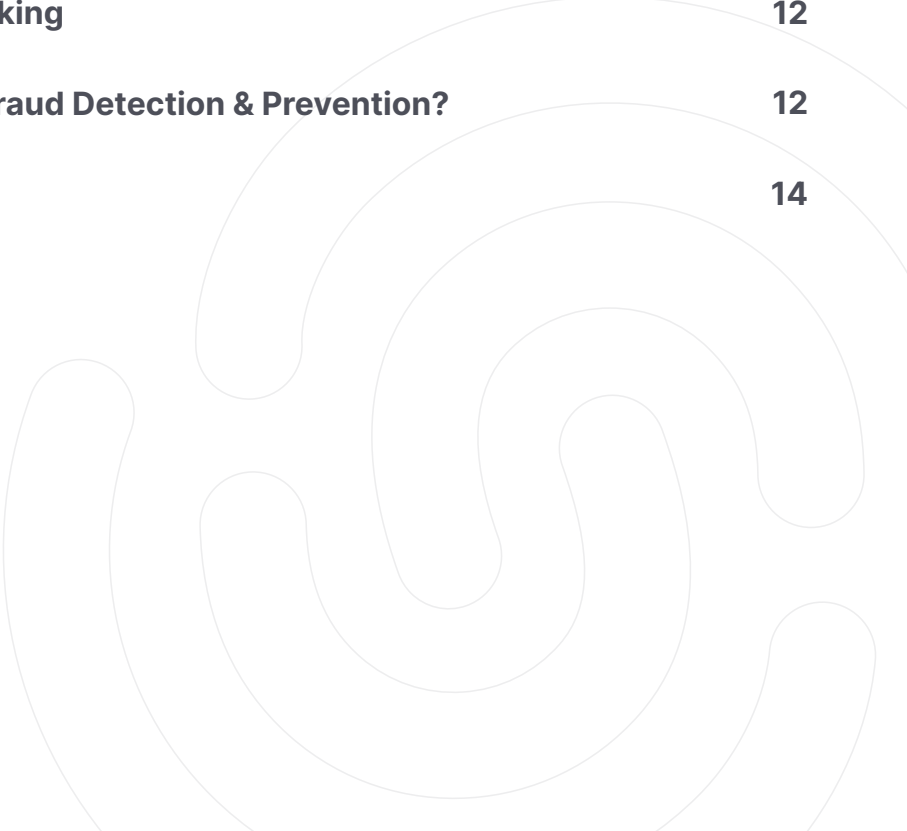


Guide

Open Source Intelligence Techniques (OSINT) for Fraud Prevention

Table of Contents

What is Open Source Intelligence (OSINT)?	2
How Does OSINT Work?	3
Who uses OSINT?	3
Why is OSINT Important?	4
Advantages of OSINT	4
Disadvantages of OSINT	5
Are OSINT investigations legal?	5
What are OSINT techniques?	6
What does an OSINT investigator do?	6
How can OSINT help with Fraud Detection & Prevention?	8
OSINT: Capturing evidence & notetaking	12
What OSINT tools are available for Fraud Detection & Prevention?	12
Conclusion	14



When one gets started in the world of fraud fighting, OSINT is one of the first - and scariest - acronyms to learn.

A shorthand for Open Source Intelligence, it covers not just a field, but almost a mindset. How do we utilize publicly available data to make sense of a situation at hand?

This guide aims to walk you through the core principles of OSINT, the most common techniques used, as well as tried and tested tips to help you fight fraud.

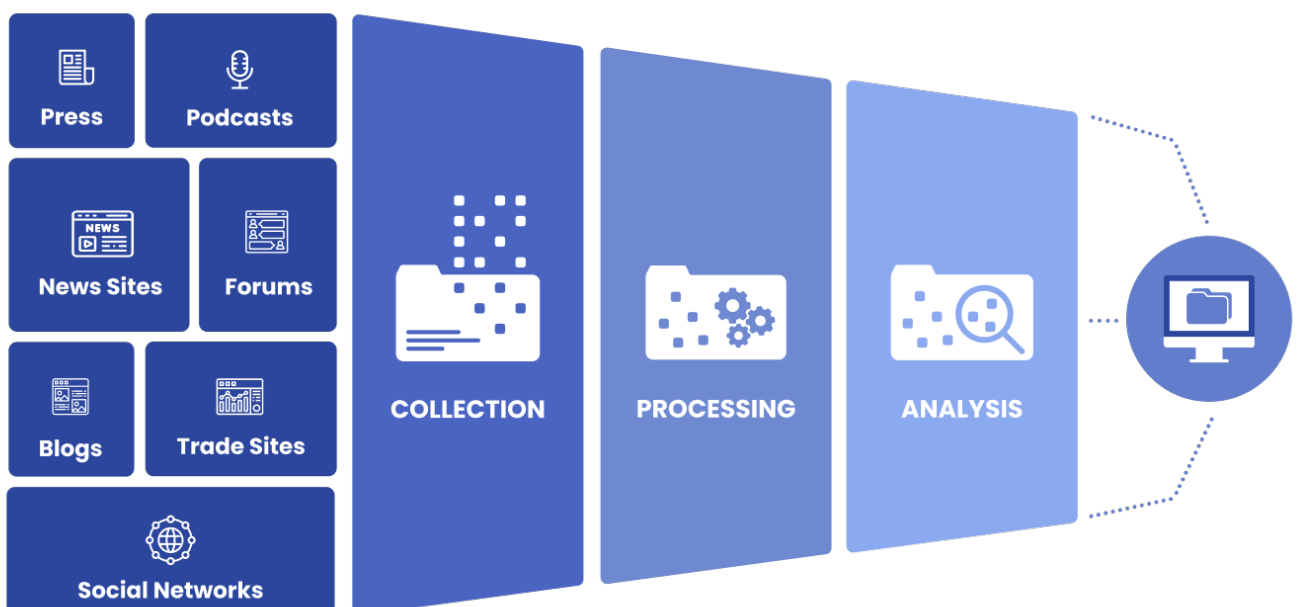
OSINT is used in a wide variety of fields from law enforcement to national security and even everyday business intelligence. Nowadays, most people who have grown up with the internet have stalking skills - but the scope of this guide is the field of fraud prevention and detection.

What is Open Source Intelligence (OSINT)?

Open Source Intelligence means gathering publicly available data from the internet, social media and traditional sources such as TV, news in order to assess a case or a situation.

The acquired information can range from text to images, videos and profiles, which once gathered needs to be processed, assessed and stored according to what's the end goal of the analyst.

As the CIA's website states: "Information does not have to be secret to be valuable."



How Does OSINT Work?

OSINT tools aggregate the information it collects from a range of publicly available sources and can help give a more detailed overview of a particular user / company.

Most publicly available sources can be used as OSINT and this includes:

- | **Blogs**
- | **Forums**
- | **Social media sites**
- | **Traditional media (TV, Radio, Publications)**
- | **Research papers**
- | **Government records**
- | **Academic journals**
- | **etc...**

In terms of fraud detection & prevention, it means gathering information on a given customer or case to determine what happened.

The most common scenario is verifying whether or not the user and the cardholder are in fact the same person, but it comes into play in more complex fraud cases where entities need to be analyzed (suspicious users, affiliates and the like). These are commonly called persons or points of interest (POI) - a term originally coined by the CIA.

Who uses OSINT?

OSINT is used by a variety of solution providers to provide further information on specific people / topics where further intelligence is needed.

It's commonly used in the following fields:

- | **Law enforcement**
- | **Risk & Fraud management**
- | **Human Resources**
- | **Cybersecurity**
- | **Military operations**

From businesses handling pay-in & pay-out systems, to law enforcement, OSINT can support any type of investigation.

Why is OSINT Important?

Reasons as to why using OSINT is important depends on the purpose of its usage however some reasons include:

- 1 **Identification of data breaches**
- 2 **Customer due diligence (CDD)**
- 3 **Uncover vulnerabilities**
- 4 **Back up decision making processes**
- 5 **Keep up to date with news**

Advantages of OSINT

OSINT can add an extra layer of security and improve your knowledge of potential users, without requiring any input from their side thus not impacting the user journey.

This extra layer can help improve your decision-making processes at a cheaper cost too, with many tools available for free.

There are many more tools out there, and we've collected some of them in our post - [the best tools for OSINT](#).

As well as this extra validation, another key upside of using OSINT for risk analysis is that it's often updated as public information is constantly being added to online.

Disadvantages of OSINT

Due to the nature of OSINT and the fact you're essentially accessing the internet's public library, filtering through the 'noise' can be pretty strenuous.

Without specialised tools your team can easily spend a lot of time sifting through thousands of pieces of information without any real direction / purpose.

There's not many direct 'plug and play' tools that support the analysis of the information and without the support AI, OSINT requires a lot of human input to verify the information collected.

OSINT has to be validated as sources of information need to be scrutinized or else you can easily be analysing false / useless information.

Are OSINT investigations legal?

OSINT is publicly produced and publicly available data that can be collected and shared without breaking laws or policies, needing a warrant, or participating in what would be commonly considered shady practices. They are perfectly legal to do in the context of fraud investigations, although the gathered and stored information needs to be handled in a compliant manner.

In the past few years it has gained notoriety in the widespread practice of 'doxxing': unveiling anonymous internet users by combining publicly available information.

What are OSINT techniques?

OSINT techniques cover the methodology on acquiring the aforementioned information - that is the knowledge of where to search or what tools to use for the job.

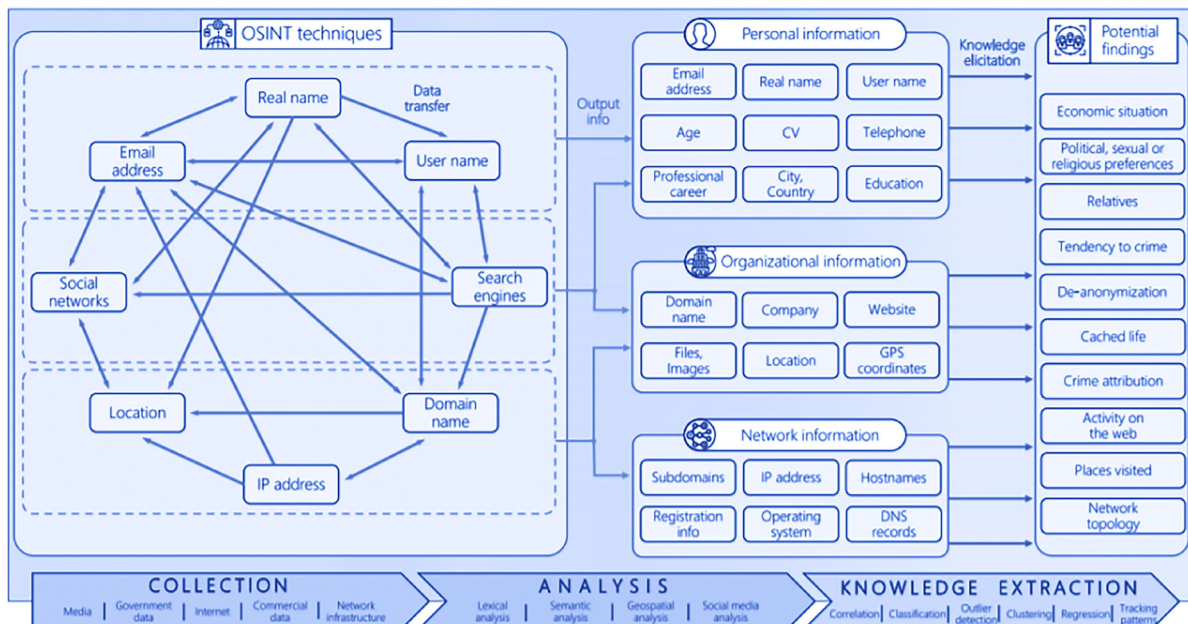
This distinction is crucial, as although most websites & social media platforms have some sort of search functionality, they treat some information (such as emails and phone numbers) as sensitive, and you need to know where to look for your search to yield results.

Sometimes it means working against the algorithm: Google orders the search results one way, but using special search operators means you can filter the result for a given file type, or only in a certain language or from specific domains. In fact it's useful to use different search engines - such as DuckDuckGo or Bing to counter the algorithmic bias.

Other queries require specialized search engines (such as people searches), and there are use case specific databases (such as the leaked email database of haveibeenpwned.com). Many of these sources are free (albeit time consuming) while specialist software is typically expensive.

Sources include things such as the [OSINT framework](#), while for mastering advanced search operators, we recommend Moz.com.

What does an OSINT investigator do?



An OSINT investigator is responsible for gathering and analyzing the information as well as extracting knowledge from their findings.

While everybody works differently and each organization will have different protocols on how exactly an investigation is conducted, there are certain frameworks which are typically followed.

Collecting information from open sources: Going by the mantra of "start with what you know / have" the investigator will search their sources with information such as emails, phone numbers, usernames, given names, addresses etc. to build up a file on the case at hand.

Filtering: Many of the findings will turn out to be either mismatches or irrelevant to the investigation, and must be set aside so the correct assessments can be made. Working with the wrong information will inevitably lead to making the wrong call on a case.

Analysis of information: using bottom up logic (or inductive reasoning), the analyst / investigator looks at the data, and builds up a theory based on what they see, working towards actionable insights. This can range from something simple (calling a spade a spade) to uncovering very elaborate plots and schemes.

Gaining insights: at the final stage the investigator can make a recommendation on what is to be done with the given case, and can present their reasoning with the relevant information. It's good practice to involve another investigator at this stage if needed to check against possible bias.

In short, intelligence is analysis **plus** information!

A note on OPSEC:

Operational Security (OPSEC) means being vigilant on what traces you leave while you conduct your activities. Within the OSINT context, this means that you need to be careful not to alert the target of your investigation. Depending on the system used, they may get notifications, or your IP address might show up in their analytics, etc. The best practice is to investigate as anonymously as possible, using virtual machines if necessary.

How can OSINT help with Fraud Detection & Prevention?

OSINT is typically associated with manual reviews in fraud detection, when the anti-fraud system's ruleset was insufficient to correctly assess the case.

The other main use case is staying up to date with what fraudsters are up to. OSINT techniques can be used to search carder forums or the dark web to see what's trending - and what you need to prepare for.

It follows a certain logic: the system couldn't make a correct assessment because risk scores are calculated based on what data is captured for a given action (or more commonly a transaction), and a human needs to step in and gather additional intelligence.

While OSINT typically covers the 5 W questions (Who, What, When, Where, Why + How?), for a fraud analyst the most typical question will be "Are you really who you say you are?". The second most common is "Is this too good to be true?". The third one is: "does this person really fit our user / customer profile?" And so on.

The catch is that fraudsters - the better ones anyway - are smart adversaries, and will not just look at the possible loopholes within your system - but also in your thinking.

Someone who just acquired stolen credit card details will do their research on their victim, and try to match the details of the transaction to what you may find out about the person as well, in addition to using a proxy that looks plausible on an address distance check.

Similarly, a shady affiliate will try to appear legitimate, and it's not unheard of for serious criminals to front their operations with LLC-s.

This means that while collecting information, you have to keep in mind a distinction. When it comes to fraud, the most common scenario is someone presenting themselves as someone else.

This means that information that you gain from the provided details might match that of an existing person - who might be a victim of identity theft or who is a money mule.

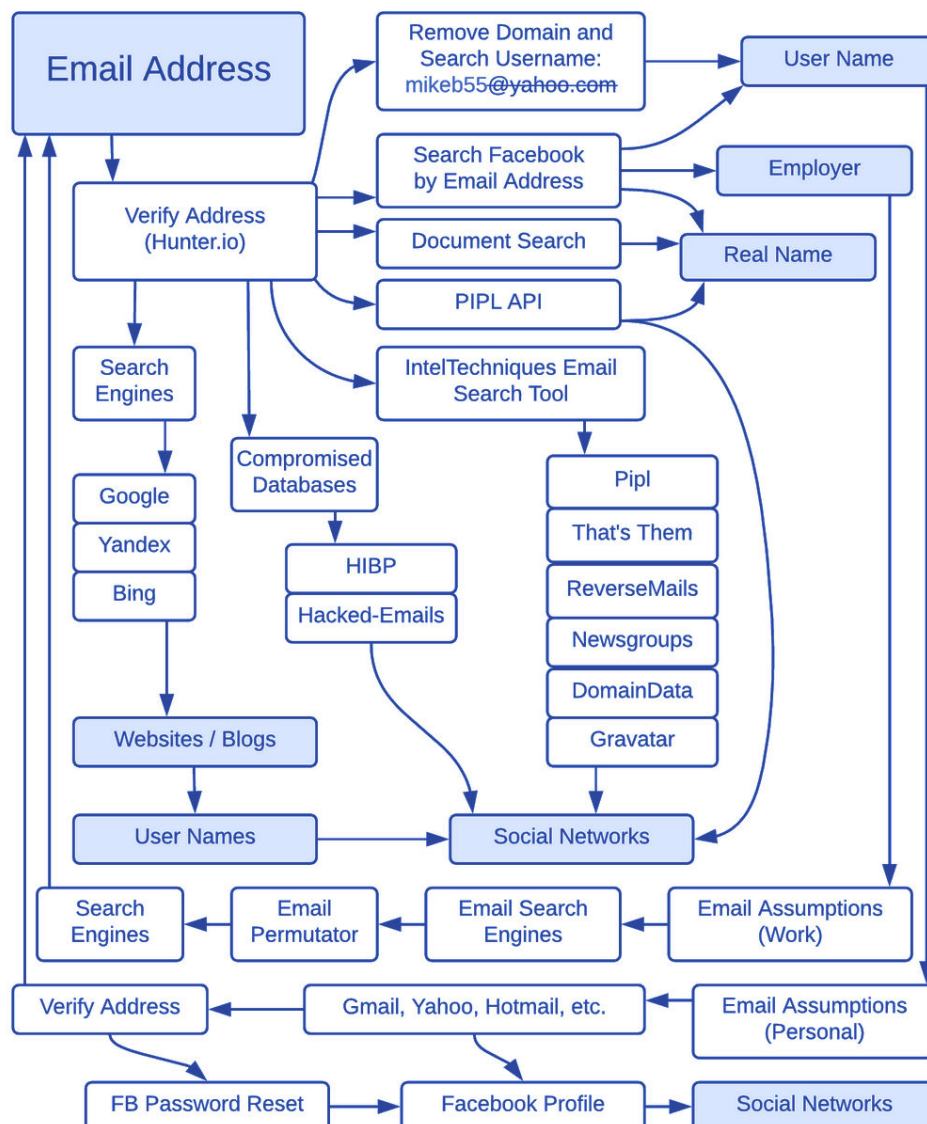
The other half of the puzzle is information related directly to the user: their device metadata, IP address, provided email and phone number.

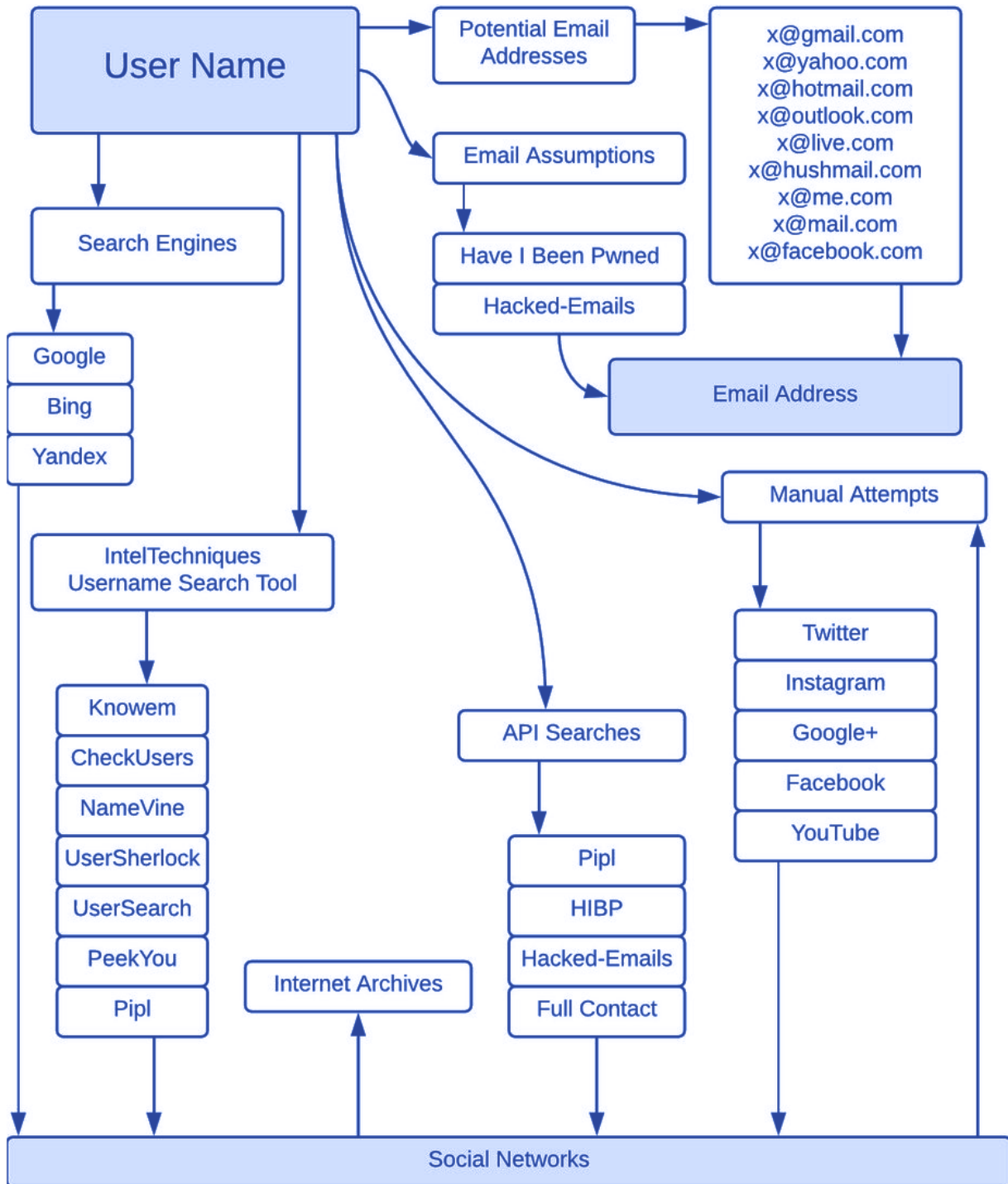
The question you're trying to answer is whether the two halves are linked together by anything other than the transaction / signup which you're looking at.

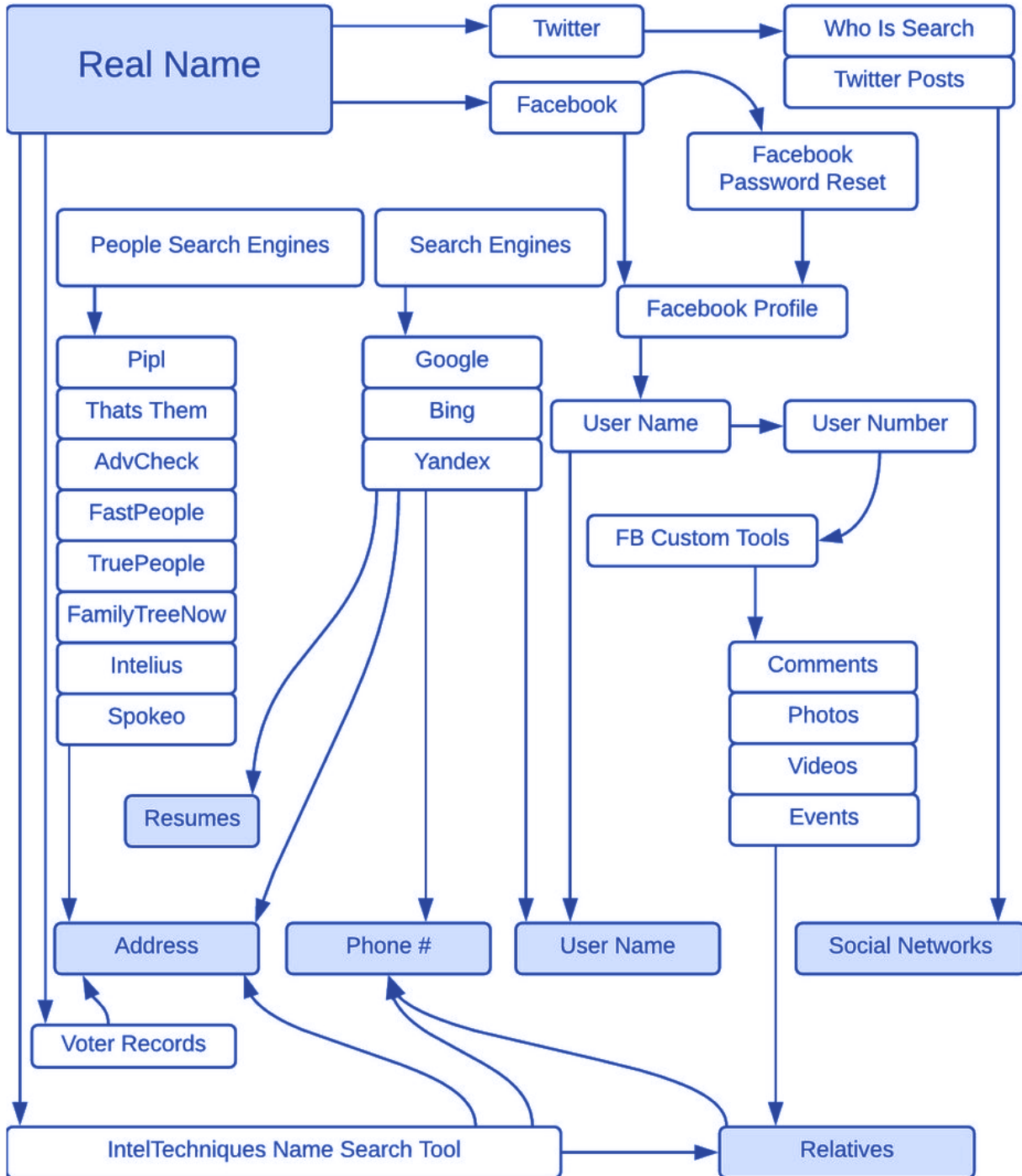
Secondly, while OSINT works mainly with publicly available information, even if it's hard to find, as a fraud manager you have a wealth of internal data at your disposal that can aid you. This means looking at connected users and entities in the system as well, conducting OSINT research on them.

Often you will find that links that are present internally can be found on the open web as well. And vice versa: by using intelligence gained via OSINT, you can discover new points of interest by searching internally, even if they weren't linked together originally by other data points. This is fairly common when dissecting fraud rings.

There are various OSINT workflows - originally collected by Michael Bazzell at IntelTechniques.com that you can memorize and practice until they become second nature.







OSINT: Capturing evidence & notetaking

For very basic investigations, collecting the links to the information found next to your notes and explanations should be enough. But not only is bitrot real, you'll be dealing with hints and evidence, and good cybercriminals don't just practice opsec, they'll also try to hide their tracks. This means that you need to use tools like archive.is or archive.org (The Wayback Machine), various screenshotting plugins for your browser of choice, or straight up the industry standard Hunchly extension (which has yearly licenses).

What OSINT tools are available for Fraud Detection & Prevention?

If you're reading this, you're probably thinking that this sounds like a lot of work. Doing it manually certainly is, and an analyst can only get so good & fast that services will start to think that they're bots.

At SEON, our manual lookup function allows you to quickly gather the digital footprints of a user using only their email address or phone number, supporting 35+ sites already (and growing).

You can use it as a chrome extension or an API, and it comes built into our fraud prevention stack where you can use it to automatically apply risk scores to transactions.

Other industry-grade tools include:

Maltego: the complex investigation power suit. While the community edition is free and very limited, licenses are steep - but the amount of transformations you can do make the price well worth it.

Skopenow: a more modern OSINT suite, designed for investigations of all kinds. Their strongest point is finding people, businesses and their associates, turning complex cases into open 'n shut ones.

Netwatch: priding itself as the #1 choice of online and social media intelligence, they work with a wide range of data partners for industrial grade investigations.

Effect Group: a sleek intelligence platform that's purpose built for OSINT investigations, paid on a per action basis, enabling analysts to compile profiles fast and relatively on the cheap.

balint.patkos@seon.io

0 / 100 SCORE

[Flag as suspicious](#)

Reasons

- Domain is custom and was registered more than 2 months ago. At least 1 online profile was found. It was not involved in a data breach

[Search on Google](#)

Deliverable
Yes

Data breaches

No. of breaches	First breach
0	Unknown

Registered ONLINE PROFILES

Skype

Balint Patkos

Skype ID: live:.cid.d8880dd82727b156
Handle: live:.cid.d8880dd82727b156

Not registered ONLINE PROFILES

Domain

Custom Free Disposable

Registered Yes	Marc enforced False
Created 1995-04-03 25 years ago	SPF strict True
Updated 2004-03-03 15 years ago	Valid MX False
Registrar NameCheap Ltd.	Accept all True
Registered to Sample company	Suspicious TLD False
	Website exists Yes

Lookup details

No. of hits 3	Customer hits 4
First seen 2017.04.05 11:45	Last seen 2019.06.24 15:50

36301234567

0 / 100 SCORE

[Flag as suspicious](#)

Reasons

- At least 2 online profiles were found

Valid Yes	Carrier Telekom HU
Type MOBILE	Country HU

Registered ONLINE PROFILES

Skype

John Doe
Hungary, Budapest

Facebook

Instagram

Yahoo

It's also worth noting that there are pre-made, purpose built [virtual machines available for OSINT](#) needs.

Conclusion

Open Source Intelligence is like a swiss army knife in the analyst's toolkit. It's essential in the context of fraud prevention as cybercriminals specialize in beating the automated security systems that we mount against them. Mastering the art can be summed up as being able to find information that someone doesn't want you to find.

While there are quite a few options available to automate the process, at the end of the day it's the mindset that matters, and being able to handle the information in the appropriate context, drawing the correct conclusions - and making decisions based on that.



