Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Michael Cortes Birkeland

Analyzing and Reducing Vulnerability to OSINT

Master's thesis in Information Security
Supervisor: Basel Katt
Co-supervisor: Matija Puzar

June 2023

NTNU
Norwegian University of
Science and Technology

Michael Cortes Birkeland

Analyzing and Reducing Vulnerability to OSINT

Master’s thesis in Information Security
Supervisor: Basel Katt
Co-supervisor: Matija Puzar
June 2023

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

Abstract

The amount of data on the internet is immense, and a lot of the data is open and accessible to everyone. Open-Source Intelligence (OSINT) is the collection, processing, and correlation of publicly available data. To use OSINT in an investigation, one has to employ some tools or resources to make the investigation possible. Search engines and OSINT tools are the primary methods to do so.

In recent years OSINT has been a topic regarding uses and misuses. OSINT is a powerful resource for endless information that can be used against individuals, companies, and governments. Specifically for this thesis, there was a focus on how OSINT, and OSINT tools, can be used against individuals. The consensus is that OSINT is a tool prone to misuse and can be misused in cyberbullying, cyberstalking, and spear phishing contexts.

In this thesis, OSINT experiments were conducted to test the extent of OSINT tools. Four subjects were tested against various tools: search engines, Maltego, SpiderFoot, Recon-NG, and Sherlock. The experiment focused primarily on finding what types of information can be found only using real names and usernames. The thesis found that OSINT can be used in various threat scenarios: spear phishing, account hijacking, and cyberstalking. Moreover, the true power lies in the potential of profiling individuals. Information such as names, addresses, email addresses, phone numbers, pictures, relations, and social media profiles can be used to understand the individual to some extent which can be used in threat scenarios. However, there are countermeasures; OSINT heavily relies on the data being accessible, meaning if the data were to be removed, the tools could not gather the data.

Sammendrag

Mengden data på internett er enormt, og mye av dataen ligger åpent og er tilgjengelig for alle. Open-Source Intelligence (OSINT) er innsamling, behandling og korrelasjon av offentlig tilgjengelige data. For å bruke OSINT i en etterforskning bør man bruke noen verktøy eller ressurser for å gjøre undersøkelsen mulig. Søkemotorer og OSINT-verktøy er de primære metodene for å gjøre det.

OSINT har de siste årene vært omdiskutert angående bruk og misbruk. OSINT er en kraftig ressurs for endeløs informasjon som kan brukes mot enkeltpersoner, selskaper og myndigheter. Fokuset i denne oppgaven er hvordan OSINT, og OSINT-verktøy, kan brukes mot enkeltpersoner. Konsensusen er at OSINT er et verktøy som er utsatt for misbruk og kan misbrukes i sammenhenger med nettmobbing, cyberstalking og spearphishing.

I denne oppgaven ble OSINT-eksperimenter gjennomført for å teste omfanget av OSINT-verktøy. Fire forsøkspersoner ble testet mot ulike verktøy: søkemotorer, Maltego, SpiderFoot, Recon-NG og Sherlock. Eksperimentet fokuserte først og fremst på å finne hvilke typer informasjon som kun kan finnes ved å bruke ekte navn og brukernavn. Avhandlingen fant at OSINT kan brukes i ulike trusselscenarier: spydfisking, kontokapring og cyberstalking. Dessuten ligger den sanne kraften i potensialet til å profilere individer. Informasjon som navn, adresser, e-postadresser, telefonnumre, bilder, relasjoner og sosiale medier-profiler kan brukes til å forstå individet til en viss grad som kan brukes i trusselscenarier. Det finnes imidlertid mottiltak; OSINT er sterkt avhengig av at dataene er tilgjengelige, noe som betyr at hvis dataene skulle fjernes, kunne ikke verktøyene samle dataene.

Preface

The master thesis "Analyzing and reducing vulnerability to OSINT" concludes my Master of Science Degree in Information Security at the Norwegian University of Science and Technology in Gjøvik, Norway. I researched and wrote this thesis from November 2022 to 1. June 2023.

The thesis and topic are in collaboration with KPMG, my external supervisor Matija Puzar, and my internal supervisor Basel Katt. With their help, I could scope the project into something fit to be the conclusion of my academic journey.

Acknowledgements

I would like to thank my supervisors, Basel Katt and Matija Puzar, for the excellent guidance and inspiration for this thesis. Their knowledge, both academic and theoretical, was able to help me through the project.

I also want to thank my friends, family, and others who have helped me through my bachelor's and now master's degree for the last five years.

Michael Cortes Birkeland
Oslo, 20/05/2023

Contents

Figures

Tables

Acronyms

CLI Command Line Interface.

ICT Information and Communication Technology.

OSINT Open-Source Intelligence.

PoI Person of Interest.

SecOps Security Operations.

VM Virtual Machine.

Glossary

Accentruator data items which are used to enhance the effectiveness of an attack, by adding real-world context to the ploys, such as impersonation of a contact, or inclusion of an event or activity known to be of interest to the target[1]..

Bootstrap data which facilitate an attack, usually by allowing targeting of an individual or group of individuals. Consistently, experts reported that while target selection focused on those individuals who might be most susceptible to it, the focus was mainly to exclude individuals likely to be less vulnerable, such as IT or security personnel[1]..

Grey literature Grey literature is data, material, and research produced by companies outside of commercial or academic use. Common grey literature publications could be reports, working papers, government documents, white papers, and evaluations..

Chapter 1

Introduction

This chapter contains what topics the project covers, a problem description, justifications and motivation, research questions, and the planned contributions of the Master's thesis.

1.1 Topic covered by the project

Open-Source Intelligence (OSINT) is the collection and processing of publicly available data from sources such as the internet, media, news, social media, public government data, publicized academic, professional documents, and Grey literature as defined by [2]. The data collected can be used to identify targets, gain information about a target, explore ways of threatening a target, and use the information in a threat scenario. Due to this, there should be some awareness of what individuals can do to reduce their vulnerability and exposure to OSINT and OSINT threats. This issue has become an increasing problem as more and more people use social media and the internet, meaning a lot more data is publicly available than one may assume. According to [3], there are an estimated 5 billion internet users worldwide, and of those, 4.7 billion users are part of some form of social media. Hence, more people have more information about potential targets online than one may assume [4].

1.2 Keywords

CCS Concepts[1]:
• **Social and professional topics Computing / technology policy → Computer crime → Social engineering attacks;** Phishing
• **Information systems → World Wide Web → Web mining;** Data extraction and integration
• **Information systems → Information retrieval**

[1] `https://dl.acm.org/ccs#`

Additional keywords:
Information security, digital intelligence, open source software

1.3 Problem description

OSINT can potentially be used in attacks and threaten an individual's safety and well-being. Due to the nature of OSINT, anyone with motivation or a motive could attack a Person of Interest (PoI) using publicly available tools and resources. Analyzing and understanding how OSINT can be used in attacks and threat scenarios, knowing what data can be collected, what tools there are, and which resources the tools get their data from will be essential to understand the problem. Where the problem arises is a lack of awareness and countermeasures one can take to reduce risk to OSINT and OSINT tools. Creating a set of concrete countermeasures will reduce the potential risk and vulnerabilities tied to OSINT-based threats and threat scenarios.

1.4 Justification, motivation, and benefits

OSINT poses a real threat to individuals. Everyone who actively uses or is part of the internet will have some information open for everyone to see. However, this should be fine for most individuals. However, as soon as someone is a PoI, such as the director of an organization, politician, or other public figures, OSINT could lead to threat scenarios that could cause actual harm. Openness and public data are acceptable, but the problem is that there should be countermeasures when someone is a PoI. This thesis will focus on how OSINT can be used in threat scenarios, concrete countermeasures to OSINT, what OSINT tools are available, and what data can be collected.

1.5 Research questions

During the thesis, the following research questions will be answered:

- How vulnerable are we as individuals due to potentially too much openness?
- How problematic are OSINT tools?
- How to reduce vulnerability to OSINT-based attacks and threats?

1.5.1 Planned contributions

During the master's thesis, the following contributions will be produced:

- An assessment of different OSINT publicly available tools.
- Define some concrete countermeasures against OSINT and OSINT-based tools.

- Raise awareness of OSINT, OSINT tools, and what data lie readily accessible on the internet.

Chapter 2

Background

This chapter contains the context which is needed to present the results of the research. What OSINT is, how it can be used, and the advantages/disadvantages of such approaches will be presented in this chapter.

2.1 What is OSINT?

OSINT is the collection, processing, and correlation of publicly available information and open sources such as social media, forums and blogs, publications, news outlets, public government data, and commercial data [2]. OSINT is defined by the U.S. Director of National Intelligence and the U. S. Department of Defense as a type of intelligence "produced from publicly available information that is collected, exploited, and disseminated on time to an appropriate audience to address a specific intelligence requirement." [4, 5]. OSINT has been proven to work in investigations against specific individuals and organizations, where the investigation was performed by individuals, organizations, or government agencies such as law enforcement [6].

This thesis will focus on how someone can extract and use OSINT to find information about a Person of Interest (PoI) utilizing tools that extract publicly available information. What constitutes a PoI is someone that is of interest to someone; it could be a politician, company director, a university professor, or just someone the investigator has an interest in profiling. An internet presence is required in investigations such as this. A presence on the internet would be the person having some published data about themselves that are publicly available such as open social media profiles, published literature, and documents [7].

OSINT can be divided into three main principle use cases defined by Pastor-Galindo *et al.* [2]: *Social Opinion and Sentiment Analysis*, *Cybercrime and Organized Crime*, and *Cyber Security and Cyber Defense*.

- *Social Opinion and Sentiment Analysis* consists of data such as user interaction, messages, interests, and preferences. This data is primarily acquired through social media and publicly published posts. Mainly used for marketing and political campaigns.

- *Cybercrime and Organized Crime* is mainly used to detect crimes early. Adversary patterns and relationships with felonies are analyzed and studied to stop crimes from happening or to detect suspicious patterns.
- *Cyber Security and Cyber Defense*, as Information and Communication Technology (ICT) systems are continuously attacked, it is crucial to research how to defend them. Known attacks, vulnerabilities, and countermeasures can all be accessed using open sources and are crucial for protecting these systems. There are publicly available databases of known vulnerabilities and attacks, such as the CVE project[1].

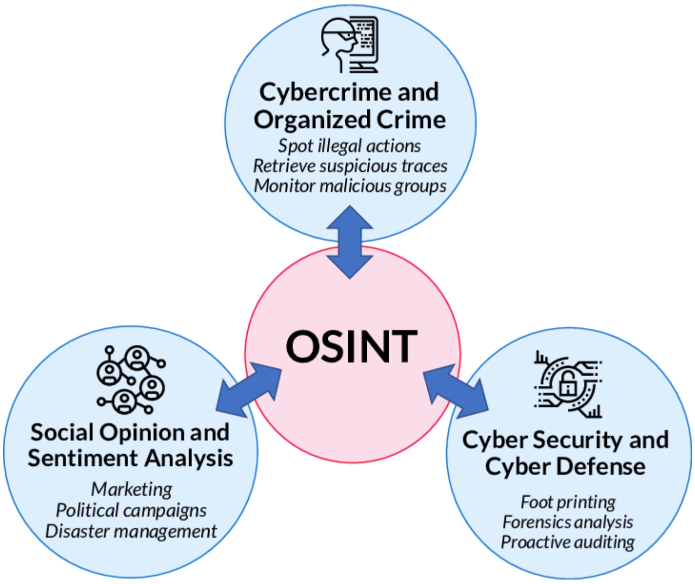


Figure 2.1: OSINT Principal use-cases [2]

2.2 Structure of OSINT

The structure of OSINT defines a primary method for collecting information using OSINT. Hwang *et al.* [7] describes a five-step process and methodology of OSINT data collection. This method involves identifying, collecting, processing, analyzing, and reporting data.

(Step 1) *Source identification:* Define the information the investigator wants to obtain about the target(s). The central questions the investigator has to answer are how the information will be obtained, where the information will be obtained from, and what data will be collected.

[1] `https://www.cve.org/`

(Step 2) *Data collection:* This is the step where the data is collected from the sources defined in the last step. One can classify two types of collection methods: either active or passive. Active collection is when data is directly collected using a tool such as a program or a script. The characteristic of this type of collection is that the investigator collects the data directly from the source, such as a social media service or database. This approach may leave some logs behind where the data was collected, which could be problematic in some investigations. Passive collection data is collected from sources such as Google and Shodan. The characteristic of this collection is that it makes it harder to track the investigator, as rather than directly accessing the data, it uses third-party applications instead to collect the data, meaning logs are not stored directly on the sources the data are collected from.

(Step 3) *Data processing and integration:* This step refines and processes the data gathered from the data collection step. OSINT data can be extensive; some or most could be redundant or irrelevant. Not processing the information could lead to data bloat and critical data being lost or not prioritized.

(Step 4) *Data analysis:* The data processed in the previous step is refined according to the criteria of the investigation. Steps 2 through 4 can be repeated to gather more data if needed.

(Step 5) *Results delivery:* This step summarizes steps 1 through 4 and makes the data produced presentable in a more readable way, such as a report or statistics.

2.3 OSINT data groups

OSINT investigators can gather many different types of data about their target. Using the tools and publicly available methods, the investigators can collect data about a person, organization, or the network of its target. Pastor-Galindo *et al.* [2] groups these types of data into three distinct information groups: *Personal, Organizational, and Network information*.

Category	**Description**	**Data**
Personal information	Personal information is all information and assessments that can be linked to you as an individual [8].	Name, age, gender, address, cellphone number, e-mail address(es), Career/Occupation, Education/University, published works, pictures
Organizational information	Organizational information is formed by team or a company composed of individuals.	The company, website(s), domain names, publicly available files and pictures, location, and GPS coordinates
Network information	Network information is the technical data of systems and communication technologies.	IP-address(es), Hostnames, Registration info, Operating System, DNS records, Subdomains

Table 2.1: Descriptions of the three OSINT information groups [2]

2.3.1 Difference between data and information

Data and information may seem synonymous at first glance. However, some concepts differentiate them from each other. Data refers to statistics and facts which lack context, while information is data that has been given context and processed. An example in OSINT would be a group of social media that could be considered data, but when the data has been correlated with a person becomes a piece of information.

2.3.2 Sensitive information

According to the Norwegian Data Protection Authority (Datatilsynet), sensitive personal data is a category that needs additional care and protection. They categorize this data into ten categories: ethnicity, political belief, religion, philosophical perception, union membership, genetic information, biometric information to uniquely identify someone, health information, sexual relations, and sexuality [8, 9].

This type of data should not be publicly available as it can cause harm to the individual. This could be harmful in places with political unrest, people with specific religious backgrounds are pursued, or some forms of sexuality are illegal. The services that treat such information are under strict guidelines on how to share and store such data to ensure that the individual's safety and privacy are kept. The Norwegian Data Protection Authority and GDPR could fine the organization with the information if such data were leaked or improperly stored. Which companies and organizations that receive these fines is also publicly available information and could be accessed on the Norwegian Data Protection Authority's website[2].

2.4 OSINT data sources

OSINT investigations gather information from a variety of sources. These sources have to be open to being counted as OSINT, even though the data could be seen as bordering on being confidential. Individuals willingly or unwillingly get information about them shared on these sources, and the investigator or tool aims to extract this information. The data sources can be summarized into six categories defined by the EU Open Data Portal. These data source categories are public media, the internet, public government data, professional and academic publications, commercial data, and Grey literature [10].

- *Public media:* Publicly available media such as print newspapers, magazines, and television.
- *Internet:* Online publications and blogs, discussion groups such as forums, and social media websites like Twitter, Facebook, LinkedIn, and Instagram.

[2] `https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/avgjorelser-fra-datatilsynet/`

- *Public government data:* Public government reports, budgets, press conferences, hearings, and speeches.
- *Professional and academic publications:* journals, conferences, academic papers, and theses.
- *Commercial data:* commercial imagery, business and financial assessments, and databases.
- *Grey literature:* technical reports, patents, business documents, unpublished works, and newsletters.

2.5 OSINT techniques

Pastor-Galindo *et al.* [2] summarizes eight of today's most popular OSINT techniques. These techniques utilize different types of information related to a person and OSINT services. They come in specific web pages, applications, or other services. The techniques mentioned are search engines, social networks, email address techniques, username techniques, real name techniques, location techniques, IP address techniques, and domain name techniques.

Search engines

Search engines such as Google, Bing, DuckDuckGo, and Yahoo are some of the most widely used tools on the internet, not only for OSINT investigations. Using queries, one can search the internet for information about someone or something and get that information instantly. However, the amount of information can be overwhelming as not all results are relevant for the investigation. This issue is remedied by some query techniques Google has implemented, such as using quotations or a symbol to refine the searches or searching after results from a specific website[3].

Social networks

Social media allows people to share life events and thoughts with friends and family. People worldwide widely use services such as Facebook, Instagram, and Twitter to interact with other people. The data shared could be used in OSINT investigations as the data shared can reveal the target's name, age, relations, occupation/employment, education, locations, and other valuable data. Using this information can be beneficial when doing OSINT investigations, and some tools use social media to their advantage.

Email address techniques

Emails are a core part of using services on the internet. It acts to identify, receive/send information, and create accounts on different online services. Each

[3] https://support.google.com/websearch/answer/2466433?hl=en

individual on the internet most likely has a personal and a professional email that they use daily or at least occasionally. This email can benefit an OSINT investigation as some publicly available tools and services check if the email address is legitimate or if there is any widely known information about that address. Services such as "*Have I been pwned?*" check if the email address in question has been part of any known public data breaches [11]. If this is the case, the investigator can use this information to get some information linked with the email, such as a password (either hashed or in plaintext), name, phone number, and other data.

Real name techniques

Searching for a real name can also be an effective way of finding information about a person. Searching after a real name will yield results from social media profiles, publications the name is associated with, news articles, and others. Online catalogs are also services that are widely used in Norway specifically. These online catalogs contain information about Norwegian citizens, such as phone numbers, addresses, and full names. The different telecom operators provide the data in Norway, and it is possible to reserve one's information from being shared with these. Still, it is something the individual has to do themselves.

Username techniques

A username is the form of identification often used on internet services. These can be categorized as pseudonyms and used to identify a specific person. Some social media, such as Facebook, often prefer the user to use a real name instead of a username, and other social media and forums let users choose their real name or username as they see fit. Some tools specifically search after usernames instead of real names, and if the real identity of the username is known, it can be used in OSINT investigations targeting individuals.

Location techniques

Knowing a target's location or movement patterns can benefit an OSINT investigation. One can find some information, GPS coordinates, and images of the target address using services such as Google Maps.

IP address techniques

An IP address is a unique identifier for devices connected to the internet. Each PC, smartphone, server, router, and whatever connects to the internet has a unique IP address. According to the Norwegian Data Protection Authority, an IP address is considered personal information as it can be used to trace back to a specific device, which could be associated with an individual[4]. The IP address provides some in-

[4] `https://www.datatilsynet.no/personvern-pa-ulike-omrader/internett-og-apper/webanalyse/`

formation for an OSINT investigation, such as what city/location the IP originates from. Going through the web also leaves some footprints, as every connection sends the IP address to the destination, which will be stored on a server if not deleted.

Domain name techniques

Web pages can also provide information that could be used in OSINT investigation. IP techniques share similar approaches and tools and will be intertwined. There are a lot of powerful tools associated with domain names; precisely for this thesis Wayback machine will be helpful as it is a service that allows the investigator to access earlier versions of websites.

2.6 Knowledge extraction and analysis

Pastor-Galindo *et al.* [2] also defines analysis and extraction techniques for the data produced by the previously mentioned OSINT techniques. For the data to be valuable and usable, the data need to be analyzed, extracted and understood.

2.6.1 Analysis techniques

- *Lexical analysis* raw data are examined to extract entities and relations from raw text. Redundant, irrelevant, and noisy data that bring no value or relevant data will be filtered from the analysis.

- *Semantic analysis* means drawing meaning from text. This analysis technique uses computer algorithms to extract knowledge and meaning from text using different methodologies, classification models, and approaches. The foundations create technologies such as chatbots and search engines [12].

- *Geospatial analysis* is a more location-based perspective of the data, looking at the target's locations, social networks, events, and IP addresses. Doing this could create a more in-depth look at connections between events and a person.

- *Social media analysis* looks at the features in people's social media. Doing this will create a network of events, people, places, and interactions around the target.

2.6.2 Knowledge extraction techniques

- *Correlation* is the detection of relationships. The relationships could be the link between people, events, and pieces of data. Doing this could extract more meaning from the data that lacked context or needed more supporting data to be valuable.

- *Classification* is the grouping and categorization of data. The features in the data can be classified with similar data according to previously defined categories. This technique is supervised, meaning the features and groups must be defined before the extraction. Machine learning technologies often use this simple yet effective way of handling massive data.

- *Outlier detection* is about detecting anomalies in the data. People usually create patterns; if some data does not follow this pattern, it could be important or interesting. This technique is more relevant in larger-scale OSINT operations that collect data from many different people, not just an individual.

- *Clustering* is similar to classification but is an unsupervised approach rather than the supervised approach of classification. Clusters bundle similar data without needing to create the groups beforehand. This technique could be relevant if the data include a lot of uncertainties and unknown diversities.

- *Regression* is about predicting numeric values and facts of data.

- *Tracking patterns* are the opposite of outlier detection, looking instead at the regularities of the data.

2.7 Relevant publicly available tools and resources for OSINT investigations

OSINT tools will be the primary method to gather the data in an OSINT investigation. These tools often specialize in one or more techniques that can get some information from the provided data. These tools vary from search engines to simple scripts that can be downloaded on a local workstation. This project only covers publicly available tools, not those used exclusively by police, states, and other government operations. Nevertheless, finding OSINT tools is no easy task, but it is made easier by publicly curated lists detailing different tools. One of the more well-known websites is OSINT Framework[5]. It focuses primarily on free OSINT tools and resources. Some require paying a sum to access the full extent of the tools but have at least the essential functions available.

2.7.1 Search engines

Search engines can be categorized into two categories based on their results. These are general-purpose and specialized search engines. The general purpose search

[5] https://osintframework.com/

engines are the usual and most well-known ones that give many varied results when given a prompt. These are search engines such as Google, Bing, Yahoo!, and DuckDuckgo.

Specialty search engines are more specialized search engines focusing on one group or type of data. These data types include pictures, network information, Internet-of-Things devices, news, and open-source code repositories. These are aimed explicitly towards finding one type of information and can often be better than the general-purpose counterpart.

2.7.2 Online catalogs

In Norway, online catalogs are services that share information, mainly data connections between names, phone numbers, and addresses. These catalogs get information from the telecom operators in Norway, such as Telenor, Telia, and Ice. If relevant, telecom operators give some information connected to a phone number, such as names, addresses, and associated companies or businesses. Anyone can search for a name, address, or phone number on these catalogs and see what data is associated with it. Some of Norway's most popular and well-known online catalogs are Gulesider, 1881, and 180 [13].

2.7.3 OSINT automation tools

OSINT automation tools are assortments of other external tools and their methods. These tools aim to generalize and compile the most similar tools to make an OSINT investigation as easy as possible. In this thesis, the focus will be on Maltego, SpiderFoot, Recon-NG, and Sherlock

Maltego is software used for OSINT investigations and forensics analysis, developed by Pretoria [14]. Maltego focuses on providing easy-to-use and expansive libraries for discovering and visualizing open-source information. Some of the primary applications of the software are to find relationships between people, groups, webpages, networks, and social media [15]. There are three versions of Maltego at the moment: Maltego CE, Maltego Pro, and Maltego Enterprise. Maltego CE will be used for this thesis as it is free compared to the 999 EUR annual fee (At the writing of this thesis). Furthermore, Maltego CE possesses the essential functions of the client but has some restrictions tied to it, such as only supporting 12 results per transform, which limits how much information one can find about a person [16]. The primary data types it can find relationships between are human names, phone numbers, email addresses, aliases, groups of people (social media and networks), companies, and websites. It can also find relationships between internet infrastructures outside the thesis scope.

SpiderFoot[6] is an example of a free-to-use open-source OSINT automation client. It arranges many different OSINT tools for data collection and analysis, and after collection, it presents its results inside an easy-to-read GUI if needed. It

[6] https://github.com/smicallef/spiderfoot

has a lot of different techniques available, such as using full names, IP addresses, emails, phone numbers, and usernames. SpiderFoot supports various modules and APIs such as Google, Bing, Shodan, Iknowwhatyoudownload, HaveIBeenPwned?, Hunter.io, and IntelligenceX. SpiderFoot also has a paid service named SpiderFoot HX. SpiderFoot HX provides a cloud-based solution for the user, including customer support and new features. This functionality is more geared towards professional investigations, and the free-to-use service should suffice.

Recon-NG is a fully automated reconnaissance framework used for OSINT investigations[7]. Recon-NG takes many notes from the Metasploit Framework, making it easy to use and implement into a system. It is entirely modular and makes it easy for any developers to contribute. It is written in Python and designed for Linux systems. Recon-NG is presented in a Command Line Interface (CLI); when needed, the investigator can set some parameters to start the process. The use cases for Recon-NG are vast, as many available modules exist and are downloadable. The "Profiler" module will be used for this thesis to find profiles associated with a name or username.

Similar to Recon-NG's Profiler, Sherlock[8] will be used to find accounts associated with a name or username. Sherlock searches after an alias at 407 different services and outputs whenever it finds a user.

2.8 Advantages and disadvantages of OSINT

OSINT appliances are both far and wide. However, despite its prevalent use and use cases, it has advantages and disadvantages [2, 7, 17].

Advantages

- The amount of available information. The scope of OSINT is vast, and it encompasses all data that is publicly available to use. Therefore it applies to everything publicly available on the internet, meaning thousands upon thousands of websites, documents, and articles from which data can be gathered.

- The different types of data. A massive variety of data can be collected when doing OSINT investigations. This data include and is not limited to Personal Information (Names, addresses, occupations, email) and different types of media containing that person (Pictures, videos).

- A lot of good publicly available tools and resources. OSINT is, by nature, open source, and many tools and resources that one can use in investigations are free to use or publicly available. There are exceptions, and these tools are often paid to use or utterly inaccessible to the public.

[7] https://github.com/lanmaster53/recon-ng

[8] https://github.com/sherlock-project/sherlock

- Ease of access and simplicity. Doing an OSINT investigation is something anyone could do. As previously mentioned, many tools are public and can be used by anyone. The investigator only needs a computer, internet connection, and potentially access to a virtual machine if the script or program cannot be run on the operating system the investigator uses.

- The low cost. Computers have reached a point where most newer hardware should be able to perform an OSINT investigation to at least some extent. There is no reason to use much money on hardware to be able to use some tools and resources online. In addition, many tools and resources are free to use, not needing a subscription or license.

Disadvantages

- Complexity of collected data. The data collected through tools and resources are not guaranteed to be relevant or readable, so extracting meaning could prove hard or impossible.

- Unstructured data. There is no guarantee that the data collected will be appropriately structured to be used. It is not as if public resources like social media were meant to be resources for OSINT.

- Reliability of data and sources. When collecting data from public sources, especially from the internet, there is no guarantee that the data are correct or reliable. It is crucial to be aware of this when collecting data from social media, forums, and other non-authoritative, not peer-reviewed, and untrusted sources.

Chapter 3

Related work

In this chapter, related work will be discussed and presented. Different chapters in the thesis will have related literature and existing work, and the chapter will be sectioned to differentiate the current work.

When answering the research questions, it is crucial to understand the domain that will be studied. Open questions, problems, definitions, and other available state-of-the-art publications are integral to answering the research questions. OSINT is not a new topic. With the rise of the internet and its integral part of ordinary people's lives, it has been a growing concern with what we publish publicly to others.

3.1 State of the art

In recent years OSINT has been a topic regarding openness and publicly available information on the internet. As technology advances, the amount of data that can be gathered from publicly available sources has increased dramatically. As such, OSINT has become a genuine threat to individuals, organizations, and governments. These technological advances have also sparked an increase in interest and research in the field of OSINT. The consensus is that the potential of OSINT is still unraveling, as the continuous development in technologies not only for corporate and organizational use but also for general use by individuals provides the means to create and use these technologies to use OSINT. The ease of access is also low, as a simple Google search after "OSINT tools" can give anyone, if interested, the methods needed to perform a simple OSINT investigation [2, 7, 18].

Much of the research focuses on how OSINT can be used in a more general sense or against companies and governments. Furthermore, as pointed out by Pastor-Galindo *et al.* [2], many of the issues regarding resources and research focus on a few specific nationalities and regions of the world, meaning that some parts of the world are not accounted for or are left more in the dark regarding OSINT.

This thesis focuses specifically on Norwegian individuals. Companies, governments, or other organized groups of individuals are not part of the scope. Focusing on Norwegian individuals creates a unique perspective into the world of OSINT, as what, how, and how much available data changes between different people with different nationalities [2]. Additionally, the focus will be on people searching, specifically real name and username techniques. IP, location, email address, and domain name techniques have tools, methods, and challenges that this thesis will not cover [19]. The research questions tackled in the thesis focus primarily on assessing and evaluating the performance of OSINT tools to do people searching.

3.2 How vulnerable are we as individuals due to potentially too much openness?

Open society, openness, and free flow of information are primarily good things; education, knowledge sharing, government transparency, and open-source software are all good for the betterment of society [20]. Our openness is primarily good, but can too much information be harmful? OSINT needs some transparency. If no information is shared publicly, OSINT can not work as it bases itself on open data from open sources. Hence, openness is why OSINT works; therefore, OSINT threats exist. This point of view is a black-and-white way of looking at things and does not account for the discussion about the nuances and the pros or cons of openness, transparency, and the free flow of information [1, 21, 22]. Rather than completely restricting the information flow, one could also look at the awareness of OSINT and people being more aware of what information they willingly share. If someone restricts what they publish online, OSINT tools should be restricted somewhat, making the data collected less than it could be [2].

Norway as a society has some differences compared to other countries, as is to be expected. If the openness in Norway differs, Norway also has unique challenges when discussing OSINT. Online catalogs, Skatteetatens public tax records, and some specific services such as Proff.no and Brønnøysundregistrene are examples of specific places where OSINT can be applied which does not cover other countries. This openness needs to be addressed in this thesis, not from an American or a British perspective. Most likely, some similar services apply to everyone, but these are unique as we have a different perceptions of what needs to be open.

3.3 How problematic are OSINT tools?

OSINT tools lay the foundation for doing an OSINT investigation. These tools include programs, scripts, simple browser plugins, websites, databases, and fully-fledged services. Either news is created, old is deprecated, or their service is shut down. The attack vectors these tools use are also different, but what is universal is that the investigator needs to feed the tool some information, such as a name, address, email, or phone number. If the investigator did not possess this information, no OSINT data could be collected [1, 2].

These tools become problematic when used in threat scenarios. The tools themselves do no damage or are of no threat but can be used to create the foundations or support a threat scenario. In a study by Edwards *et al.* [1], cyber security professionals specialized in penetration testing using social engineering were asked how OSINT and tools can be used in threat scenarios. They summarized that the data could go into one or the other information types: the Bootstrap or Accentruator. The bootstrap is the data that facilitates the attack, which usually allows for targeting a specific person or group of people. In comparison, the Accentruator is the data that amplifies the effectiveness of an attack. This amplification is often done by adding context to the attack. In cases of spear phishing, this could be adding a person, event, or activity known to the target.

OSINT affects how effective spear phishing can be in social engineering scenarios. Where tools are problematic is how more accessible it makes the collection and processing of the gathered data. Some may argue that OSINT tools should be restricted to only be able to be used by professionals and the government, limiting the possibility of someone with ill intentions misusing the open data. However, prohibiting people from making scripts and programs is impossible. There is the case to be made that services and websites which have data accessible publicly reduce what information can be gathered without having an account or some form of privileges [2, 23].

How effective a tool is can differ from one country to the other. This limitation is why assessing how tools work when different people from different parts of the world are tested is crucial. Gulesider and 1881 are not applicable in America, and similar services in America do not apply to Norwegians. If a tool is programmed to get their people searching from that one tool, it would only work on that one nationality, not others.

3.4 How to reduce vulnerability to OSINT-based attacks and threats?

Reducing the vulnerability to OSINT is knowing where the tools and resources are. If a person knows where these tools gather their data, one can start looking at possibilities of reducing their vulnerability to OSINT. Research points toward social engineering when discussing OSINT, specifically OSINT threats. Social engineering is communicating with a target and trying to get specific information out of them, which usually is information that can be harmful to the individual if leaked and abused by the one performing the social engineering. A spear-phishing method can be employed: targeted phishing attempts. Using OSINT, the person can get a general feel of interests, relations, and communication methods to get information from a target [1, 21, 24].

Furthermore, there is the case for the service provider to take some accountability, as pointed out by Pastor-Galindo *et al.* [2]. What information lies open is controlled by the different services, what information does the employer have accessible publicly, what data do online catalogs decide to share, and who can access that information is something the individual does not have a say in and is something the services has to take into consideration.

Nevertheless, finding international countermeasures to OSINT can be challenging, as what measures one can take changes between countries. For example, GDPR does not apply to the entire world, only to citizens of countries that are part of the EU/EEA. This thesis will specifically focus on Norway, meaning the countermeasures are created looking specifically at this. Norway has unique OSINT data sources, which only apply to Norwegians meaning specific countermeasures that apply to those sources.

Chapter 4

Methodology

This chapter will describe the different methods used in the thesis. The thesis follows a qualitative approach by gathering data from various published literature and conducting an experiment to measure the potential of these OSINT tools in threat scenarios.

4.1 Research design

The research design is the researcher's position when discussing the methods used. Busch [25] splits this into four principal questions: *The choice between intensive and extensive design, the choice between qualitative and quantitative methods, the choice of time perspective, and the choice of the main design* [25, p.52].

4.1.1 Choice of intensive or extensive design

Choosing whether intensive or extensive is appropriate for the data collection part of the thesis is based on the methods used. Data collection is done primarily through a literature survey and experiments. It will be a more intensive approach to reduce the time spent experimenting, allowing more time to dive deeply into the produced results. More subjects could lead to the results being too vast.

The literature survey will follow an extensive approach as there is a need to understand the domain of the problem and the state-of-the-art. Being too intensive could lead to a narrow understanding of the problem at hand, leading to biases and inaccuracies in the small amount of literature to misrepresent the thesis as a whole. A more extensive approach will avoid these problems and give a more unbiased look at the problems at hand [25, p.52-53].

4.1.2 Choice of qualitative and quantitative methods

A qualitative approach has been chosen to answer the previously defined research questions.

Quantitative methods are more appropriate for extensive research. However, as an intensive experiment and literature survey are used to gather data, this thesis will not use a quantitative approach. If the experiment were to be extensive, containing more subjects, then a quantitative approach would be more appropriate than a qualitative one.

Qualitative methods allow the researcher to go into more of a deep dive into the given data. The literature survey and experiments' data should provide abstract and complex data that a quantitative approach could not answer. Qualitative approaches crumble when the gathered data are too vast and not detailed enough, so the results do not contribute to the results [25, p.53].

4.1.3 Choice of time perspective

As defined by Busch [25], Time Perspective is whether all the data should be collected simultaneously or on separate occasions. The mentioned experiment will be a one-time data collection, as the orchestrations and permissions needed from the subjects could prove challenging to do multiple times throughout the allotted time for the thesis. Due to this, defining proper preparations and methods will be created before the experiment. The literature survey will be a continuous process as there will be a need to find information as the thesis expands correctly. Unforeseen problems and theories will be discovered and need proper research to continue the research [25, p.53-54].

4.1.4 Choice of main design

Based on these factors, the chosen main design will be evaluation research looking at causes and eventually concrete measures individuals can take to reduce their exposure and vulnerability to OSINT-based threats [25, p.54-56]. The literature survey and experiment will follow this design.

The method chosen will not focus on cultural factors, case studies, or phenomena regarding individuals but on the factual data gathered from the chosen studies and experiments. Of course, this does not exclude these types of data. Nevertheless, a literature survey will be conducted, as a survey or a set of interviews is not a part of the project's scope. This approach will further push the design into the mentioned evaluation research design.

4.2 Data collection

Answering the research questions will require data collection. A more extensive approach will be used for the literature survey to ensure that biases, inaccuracies, validity, and reliability of the data collected are up to standard. The chosen data collection methods will be a literature survey and an experiment.

4.2.1 Literature survey

Reviewing and studying relevant published research and literature will help understand the state-of-the-art and the problem. This will contribute to creating the theoretical foundations for the thesis by gathering relevant literature from various databases containing scientific and peer-reviewed literature [25, p.52-53]. Primarily Google Scholar will be used due to how accessible and extensive the literature database is. The accumulated literature will preferably be peer-reviewed. Appropriately cited and justified sources can be exempt from this.

4.2.2 OSINT experiments

During the thesis, experiments were conducted on a few selected subjects to test the effectiveness of the previously mentioned OSINT tools in chapter 2.7. The experiment will be intensive, meaning few subjects will be used to get qualitative data. The subjects will be chosen based on their experience, organizational role, background, and relevance. This is important as the thesis will mainly focus on people with a significant internet presence. The subject, however, will be anonymized in the thesis. The subjects could perceive the data as harmful or insensitive. Therefore, what the collected data contains must be announced and defined before any experiment. The data collected will help answer the research questions as the tools will output data that can be analyzed.

Identifying relevant OSINT tools

Identifying relevant tools to be used in the experiment will be a critical factor in how and if it is possible to answer the research questions. Choosing a tool that is not suitable will make analyzing the data a lot harder or even impossible. Therefore, much research has to go into the different potential tools and how relevant those are for the thesis. There are many requirements for a given tool to be relevant, which would be: how the tool uses OSINT, what the tool gathers, and how appropriate the produced output is for answering the research questions.

Selection of the participants

The selection of relevant subjects was made in collaboration with the external supervisor of the project. The subjects are chosen based on their career position, social media and internet presence, and willingness to participate in the experiment. A subject's role is limited to only providing personal information such as their full name, address, and relevant IP addresses, but only their name is required. A formal agreement has also been written regarding the storage and processing of the information and when the data will be deleted.

Setup of the experiment

The experiment will be done on a local virtual machine. One could argue for using a SkyHiGh server as NTNU provides them, but in this case, the extra power is unnecessary and would complicate the experiment as it is not too complex. The local virtual machine will run an instance of the Parrot Security 5.2 and Kali operating systems. The experiment will be done in the following order for each subject:

1. Identify what identification will be used. This could be the target's full name, phone number, or IP address. Based on this, different approaches will be conducted as different tools need different data work.
2. Choose the tools to be used. These were the primary tools and resources used:
    - Search engines: Google, Bing, DuckDuckGo, and Yahoo
    - Online catalogs: Gulesider, 1881, 180
    - Skattelisten, skatteetaten
    - Proff.no, Brønnøysundregistrene
    - Maltego Community Edition
    - SpiderFoot
    - Recon-NG
    - Sherlock
    - Others: Iknowhatyoudownload, HaveIBeenPwned
3. Run and use the tools to gather data
4. Process and filter out unnecessary data. Most data collected will likely be redundant, irrelevant, unnecessary, or even wrong. Due to this, it is important to filter out this data before the analysis begins to reduce the time used on unnecessary data.
5. Analyze the found data.
6. Present the data in the thesis, as well as anonymize the data.

4.3 Consequence-, probability-, and criticality-tables

The following tables measure the risk of a risk scenario or any threat in the results chapter. The following formula will be used to calculate the risk: $consequence * probability = risk$. The risk will be between 1 and 12, 1 being the least and 12 being the most.

4.3.1 Consequence table

Consequence level	Personal impact	Economical impact	Privacy impact
1 - Low	There is no measurable personal impact of the risk.	No impact on the target's economics. 0 NOK	The data is readily accessible, meaning that the knowledge does not change anything
2 - Medium	The impact of the risk may cause someform of discomfort or nuisance.	Some form of economical impact on the target. <1000 NOK	The data is not readily accessible and the knowledge of the data can be used for malicious intent but is not substantial enough to be used on its own.
3 - High	The impact is substantial and will cause discomfort and real-world consequences.	The impact of the person's economics is substantial. 1000-9999 NOK	The data that can be collected is substantial enough to be used in threat scenarios. The knowledge of the data itself has an impact
4 - Very high	The impact of the risk may cause real-world harm and extreme discomfort.	The cost of the risk is exceptionally high. >10000 NOK	The data is sensitive, and just the knowledge of the data may cause harm for the target.

Table 4.1: Consequence table, measured in different levels, 1 being the lowest, 4 being the highest

4.3.2 Probability table

Probability level	Description
1 - Not likely	Not probable at all. The probability of the risk happening is too low to be significant.
2 - Likely	The risk is probable. It has a high possibility of being carried out if the intention is there.
3 - Very Likely	The risk is guaranteed, if the intention is there any threat agent can execute the scenario

Table 4.2: Probability table, how probable is it that the scenario can be carried out, 1 is the lowest, 3 being the highest

4.3.3 Criticality and risk table

Criticality			
Low	**Low-Medium**	**Medium-High**	**High**
1-3	4-6	7-9	10-12

Table 4.3: Criticality table

4.4 Choice of variables

The chosen variables will be relevant to what is needed to answer the research questions. Variables are concrete questions, while a research question encompasses more of a theme for the question. The chosen variables for each of the research questions:

- How vulnerable are we as individuals due to potentially too much openness?
  - How vulnerable are individuals to OSINT?
  - What data lie accessible on the internet?

- How problematic are OSINT tools?
  - What data do the OSINT tools collect?
  - How are the OSINT tools problematic?
- How to reduce vulnerability to OSINT-based attacks and threats?
  - Is reducing one's vulnerability to OSINT possible?
  - What can individuals do to reduce their vulnerability to OSINT?
  - What OSINT-based threats are there to individuals?

4.5 Operationalization of variables

Choosing to operationalize the variables will help create a fundamental understanding of how to solve the given questions. Even as the project follows a qualitative method, it is crucial to ensure that the given variables are measurable and answerable. The operationalization will be as measurable concepts to which the variables can be attached. Exploring the following concepts:

Concept: How problematic are the OSINT tools

- **Description:** Assessment of the tools is one of the main focuses of this thesis, and to then present how problematic the tools are to, specifically, individuals. To answer this question, it is essential to understand how a tool can be problematic and how they work, looking specifically at: How the tools collect data, where they collect data, what data are collected, and how accessible the tools are.
- **Attached variables:** "*What data do the OSINT tools collect?", "What data lie accessible on the internet?" and "Is it possible to reduce one's vulnerability to these threats?*"

Concept: Reducing vulnerability to OSINT tools

- **Description:** To reduce vulnerability to OSINT, some concrete measures should be presented. To answer the research questions, the following needs to be addressed: What sources does the OSINT use, and if possible, can one request the data to be deleted? OSINT tools rely on getting their data from somewhere, often from an open, accessible source. And knowing where the tools access their data will be crucial to find some countermeasures.
- **Attached variables:** "*Is reducing one's vulnerability to OSINT possible?*", "*What can individuals do to reduce their vulnerability to OSINT?*",

Concept: Defining openness in society

- **Description:** Openness, or more accurately, what information do Norwegians share or with services? Looking at what types of data on what services will be

- **Attached variables:** "*How vulnerable are individuals to OSINT?*", "*What data lie accessible on the internet?*"

4.6 Data analysis

Data analysis will happen after the data collection. To use the data collected as they are not quantitative. They need to be analyzed to have any value or to be able to support any of the research questions or variables. The data collected will be associated with the different variables and operationalization concepts defined earlier, Busch [25, p.60-61] defines this as a systemic categorization approach to the analysis.

4.7 Handling potential problems

Problems are a certainty when writing a thesis at this scale. One has to deal with problems with data collection, chosen methods, data analysis, and even some unforeseen obstacles that can happen. Dealing with problems should happen before it affects the project as a whole. If a problem were to create a full stop of the project process, internal and external supervisors could be contacted to resolve the problems.

4.8 Ethical and legal considerations

As a lot of the data collection can be considered unethical, each subject has to be aware of what data will be collected by which tools. There should be no legal considerations with using these tools as they only operate on already open sources. As to storing this information, the collection and storage will only be locally on a virtual machine. After the thesis and project are finished, the Virtual Machine, including all remaining data, will be deleted. No personal information data will be uploaded to either Overleaf or any other cloud-based storage as they often operate or share data with countries and entities outside of the EU/EEA as requested by the external supervisor.

When conducting experiments, there is a need to submit a request for approval from the Norwegian Agency for Shared Services in Education and Research (SIKT) to use the subjects for the experiment. SIKT is one of the primary governmental agencies in Norway which approve requests when researchers need to perform experiments, create datasets, and conduct surveys. SIKT approved this project and data collection on 18.03.2023 (See Appendix A.2).

Chapter 5

Results

In this chapter, the execution and results of the literature review and experiment will be presented.

5.1 The experiment setup and environment

The experiment will be done in a local Virtual Machine (VM) using the VirtualBox hypervisor. The choice of Linux distribution is the security-oriented Parrot Security version 5.2. Parrot Security is specifically suited for use in Security Operations (SecOps) such as penetration testing, forensics, and incident response. Another relevant distribution to use in similar experiments would be Kali. Kali, as Parrot, is a Linux distribution that mainly focuses on its use in SecOps. Choosing one over the other is primarily due to the user's preferences. Kali is the more popular, and some error handling and issues may be more well-documented than Parrot-related issues. Nevertheless, Parrot was chosen due to personal preference regarding the User Interface and the Operating System being more lightweight than its counterpart. The experiment could be done on any Windows system as well. A simple Linux subsystem instance could be used if the Linux kernel is needed for a script or program. Some tools are also supported on Windows systems, such as Maltego. Some scripts, programs, and tools are written in languages that can be used universally: Python, C/C++/C#, and JavaScript, but some also use Linux/Unix Shell.

Parrot Security comes with some pre-packaged software. Specifically, Maltego, Recon-NG, and SpiderFoot have already been installed, as these are some of the most popular and well-known OSINT tools. However, the pre-installed SpiderFoot is an earlier version of the program, version 3, compared to the updated version 4; therefore, the newer version had to be installed. The Parrot VM will be as close to newly installed as possible; when tools are downloaded, an installation guide and, if needed, downloaded dependencies will be attached in the Appendix A.3.

The structure of the experiment is as follows. The steps are based on the structure of OSINT in chapter 2.2. All the steps have to be repeated for each of the subjects:

- Firstly, collect the necessary data from the subject to run the tools. This data would be some form of personal information linked to them. The only necessary information would be their real full name, as that is the experiment's focus. Any other information is a bonus, and some additional tools can be used if this information is to be utilized.

- Secondly, declare what tools will be used based on the information given to the subjects. Maltego, SpiderFoot, and the search engines are essential and will be run on all subjects. If a username were found, Recon-NG, Sherlock, and some additional Maltego and SpiderFoot functionality could be run to find profiles related to that username.

- When all preparations have been done, the data collection can start. There are different approaches to each of the different tools. After each tool or script has been run, all necessary screenshots of the results will be taken. In addition, any CLI commands listed in Appendix A.3 needed to install or run the scripts will be written down so the experiment steps can be repeated.

- When enough data has been gathered, and all necessary screenshots taken, the data should be ready to be analyzed. In addition to the literature survey, this data will be used to answer the research questions.

- Lastly, when the data has been analyzed, it should be ready to be presented in the thesis. All personal information, or any information that can be linked to the subject, will be anonymized to ensure their anonymity.

The following diagram has been created to visualize the OSINT workflow used in the experiment (Fig. 5.1).

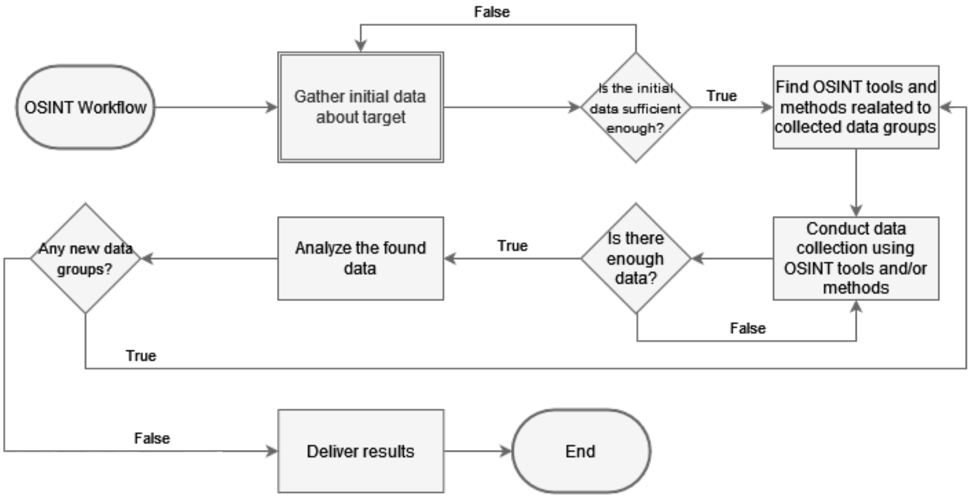

False
OSINT Workflow
Gather initial data about target
Is the initial data sufficient enough?
True
Find OSINT tools and methods realated to collected data groups
Conduct data collection using OSINT tools and/or methods
Is there enough data?
False
True
Analyze the found data
Any new data groups?
True
False
Deliver results
End

Figure 5.1: The OSINT workflow used in the experiment

5.2 Experiment results

Screenshots from the tools will be available in Appendix A.4.

5.2.1 Subject 1

Subject 1	**Description**
Provided personal data	Name, address, phone number, IP address, email, username(s)
Subject background	Subject 1 (S1) is a master's student. The subject understands Information Security, digital footprints, and has social media profiles on most popular social media.

Table 5.1: Subject 1 (S1) card

Choosing tools

As there is a lot of provided personal data about S1, most OSINT tools targeting individuals will work to some extent. Maltego, SpiderFoot, Recon-NG, and Sherlock will be the main tools to utilize, as these cover a lot of different areas, such as names, usernames, emails, phone numbers, and IP addresses. Search engines will also be used to see what data are easily accessible to anyone, looking at what social media, news articles, published works, and other data may be accessible. In addition, the name will be searched on Skatteetaten's tax list.

Running the tools

Starting with a simple search engine, the search gives some information about S1. Google, Bing, Yahoo!, and DuckDuckGo are the most popular search engines worldwide. Some outliers, such as Yandex and Baidu, focus on specific regions. These search engines will not be used in this experiment as neither S1 nor any of the subjects are from these regions. When searching using a query, it is essential to understand how the search engine works. Firstly it will search after the complete query, in this case, FULL NAME. These results will be displayed on the first pages of the search.

Furthermore, the search engine will start fragmenting the query into different strings meaning it will start searching after specific keywords in the query. So the next step for the search engine is to start using the first name in the full name as its query. This search will be less accurate as a first name is more common among many people than the complete full name. It will do this with the, if applicable, the middle name and last name(s). The queries can be further fragmented, specifically after specific keywords in the names or queries. As a result, the search engine can find everything from a couple of results up to millions or even billions of results, which are mainly irrelevant to whatever is being searched. Specific symbols and strings can filter most of the results to reduce the amount of bloat and irrelevant results. For S1, double quotation marks ("") were used only to look at results containing the full name and not the fragments. The used queries are as follows:

- "FULL NAME"
- "USERNAME"
- And to narrow the search, the following will be added on, `site:SITENAME.com`, where the SITENAME is replaced by some common websites such as Facebook, Instagram, LinkedIn, and online catalogs (Gulesider, 1881, 180). This syntax works for all of the search engines used in the experiment.

Using these queries in the previously mentioned search engines gives some results relevant to S1 and social media profiles such as Instagram, LinkedIn, and Pinterest. The results also showed the subject's place of work, its homepage, and a picture of S1. Searching using the subject's usernames, some more profiles such as a Reddit user and a private Twitter user.

After the Google searches, Maltego was used. The transforms were used on the entities: person (full name), alias, phone number, and email. Running Maltego is simple enough. All that is needed is an entity with the corresponding information. When the corresponding information has been entered, one can run the "all transform" option, which will go through all available transforms for that entity. Each transform generates data and tries to find data corresponding to the entity.

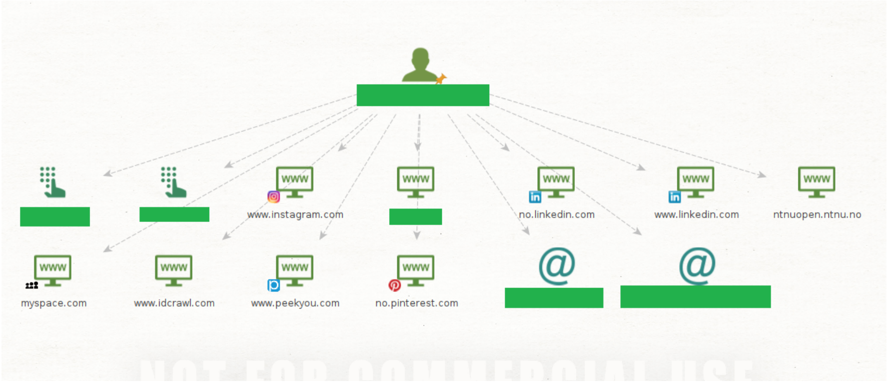
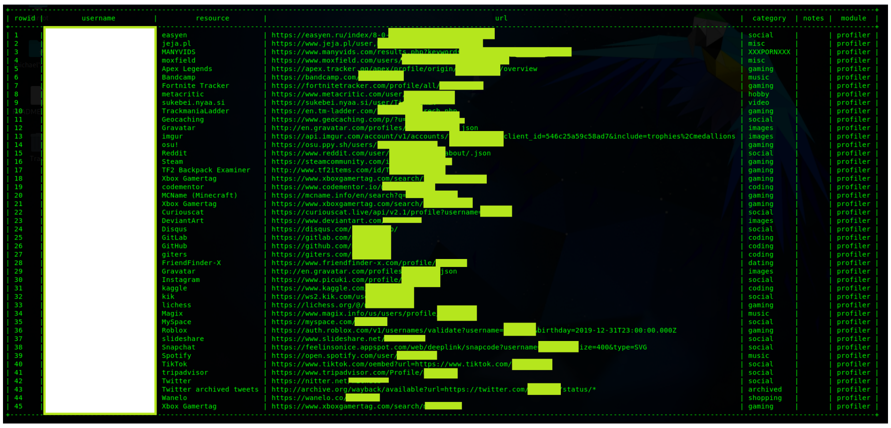


Figure 5.2: S1: Maltego person full transform

When the transform was run on S1's full name, Maltego could find some related data. These were primarily S1's social media profiles, such as Instagram, LinkedIn, and an inactive MySpace account. The subject's place of work was also shown, including their homepage. These entities linked directly to the subject's social media profiles, and all were legitimate. Some of the information found was false; however, mainly phone numbers and email addresses related to the found homepage of S1's place of work. Most likely, when Maltego fingerprints websites, it looks after valid email addresses and connects them to the entity. So when Maltego looked through the company website and found a user profile that matched the entity, it collected all email addresses it could find on that profile, which included some irrelevant mail addresses. It is afterward essential for the investigator to differentiate which emails are related or not.

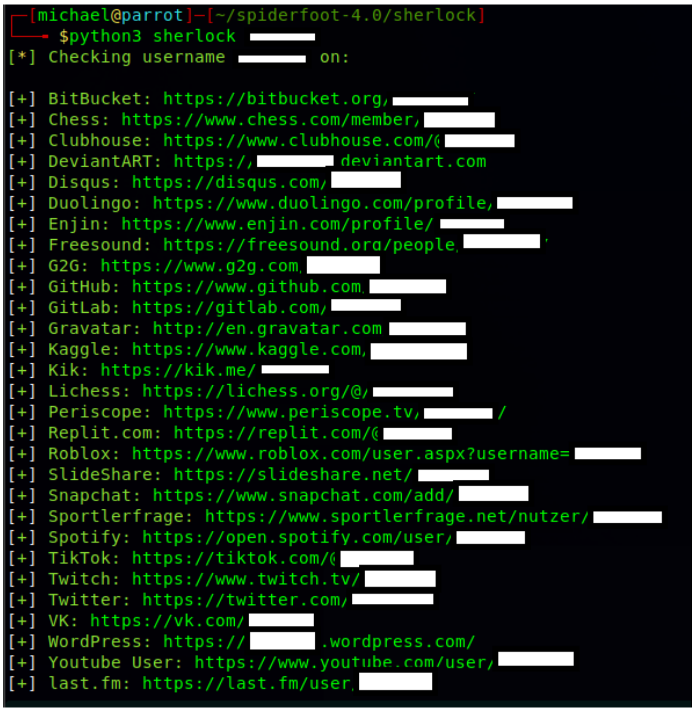
When using Recon-NG, the *Profiler* module was used. This module scans different sites and services after an alias, which can be the target's full name or username. It should be said that the profiler module used is best suited for username profiling, it works for people searching, but the success may vary from name to name. In this case, using the full name of S1 did not grant any usable data and only produced some bloat, as none of the found profiles are linked to S1. However, using S1's usernames, the results were a lot more interesting, finding profiles on different services such as Twitter, GitHub, Gitlab, TikTok, Reddit, and others, as shown in Figure 5.3.



```
+------------------------------------------------------------------------------------------------------------------------------------------------------------------------+
| rowid |       username        |         resource         |                                   url                                                       | category  | notes |  module  |
+------------------------------------------------------------------------------------------------------------------------------------------------------------------------+
| 1     | [redacted]            | easyen                   | https://easyen.ru/index/8-0-[redacted]                                                    | social    |       | profiler |
| 2     |                       | jeja.pl                  | https://www.jeja.pl/user,[redacted]                                                       | misc      |       | profiler |
| 3     |                       | MANYVIDS                 | https://www.manyvids.com/results.php?keywords[redacted]                                   | XXXPORNXXX |      | profiler |
| 4     |                       | moxfield                 | https://www.moxfield.com/users/[redacted]                                                 | misc      |       | profiler |
| 5     |                       | Apex Legends             | https://apex.tracker.gg/apex/profile/origin/[redacted]/overview                           | gaming    |       | profiler |
| 6     |                       | Bandcamp                 | https://bandcamp.com/[redacted]                                                           | music     |       | profiler |
| 7     |                       | Fortnite Tracker         | https://fortnitetracker.com/profile/all/[redacted]                                        | gaming    |       | profiler |
| 8     |                       | metacritic               | https://www.metacritic.com/user/[redacted]                                                | hobby     |       | profiler |
| 9     |                       | sukebei.nyaa.si          | https://sukebei.nyaa.si/user/[redacted]                                                   | video     |       | profiler |
| 10    |                       | TrackmaniaLadder         | https://en.tm-ladder.com/[redacted]                                                       | gaming    |       | profiler |
| 11    |                       | Geocaching               | https://www.geocaching.com/p/?u=[redacted]                                                | social    |       | profiler |
| 12    |                       | Gravatar                 | http://en.gravatar.com/profiles/[redacted]json                                            | images    |       | profiler |
| 13    |                       | imgur                    | https://api.imgur.com/account/v1/accounts/[redacted]client_id=546c25a59c58ad7&include=trophies%2Cmedallions | images |  | profiler |
| 14    |                       | osu!                     | https://osu.ppy.sh/users/[redacted]                                                       | gaming    |       | profiler |
| 15    |                       | Reddit                   | https://www.reddit.com/user/[redacted]about/.json                                         | social    |       | profiler |
| 16    |                       | Steam                    | https://steamcommunity.com/i[redacted]                                                    | gaming    |       | profiler |
| 17    |                       | TF2 Backpack Examiner    | http://www.tf2items.com/id/[redacted]                                                     | gaming    |       | profiler |
| 18    |                       | Xbox Gamertag            | https://www.xboxgamertag.com/search/[redacted]                                            | gaming    |       | profiler |
| 19    |                       | codementor               | https://www.codementor.io/[redacted]                                                      | coding    |       | profiler |
| 20    |                       | MCName (Minecraft)       | https://mcname.info/en/search?q=[redacted]                                                | gaming    |       | profiler |
| 21    |                       | Xbox Gamertag            | https://www.xboxgamertag.com/search/[redacted]                                            | gaming    |       | profiler |
| 22    |                       | Curiouscat               | https://curiouscat.live/api/v2.1/profile?username=[redacted]                              | social    |       | profiler |
| 23    |                       | DeviantArt               | https://www.deviantart.com[redacted]                                                      | images    |       | profiler |
| 24    |                       | Disqus                   | https://disqus.com/[redacted]/                                                            | social    |       | profiler |
| 25    |                       | GitLab                   | https://gitlab.com/                                                                       | coding    |       | profiler |
| 26    |                       | GitHub                   | https://github.com/                                                                       | coding    |       | profiler |
| 27    |                       | giters                   | https://giters.com/                                                                       | coding    |       | profiler |
| 28    |                       | FriendFinder-X           | https://www.friendfinder-x.com/profile/[redacted]                                         | dating    |       | profiler |
| 29    |                       | Gravatar                 | http://en.gravatar.com/profiles[redacted]json                                             | images    |       | profiler |
| 30    |                       | Instagram                | https://www.picuki.com/profile/                                                           | social    |       | profiler |
| 31    |                       | kaggle                   | https://www.kaggle.com[redacted]                                                          | coding    |       | profiler |
| 32    |                       | kik                      | https://ws2.kik.com/us                                                                    | social    |       | profiler |
| 33    |                       | lichess                  | https://lichess.org/@/                                                                    | gaming    |       | profiler |
| 34    |                       | Magix                    | https://www.magix.info/us/users/profile[redacted]                                         | music     |       | profiler |
| 35    |                       | MySpace                  | https://myspace.com/[redacted]                                                            | social    |       | profiler |
| 36    |                       | Roblox                   | https://auth.roblox.com/v1/usernames/validate?username=[redacted]birthday=2019-12-31T23:00:00.000Z | gaming |  | profiler |
| 37    |                       | slideshare               | https://www.slideshare.net/[redacted]                                                     | social    |       | profiler |
| 38    |                       | Snapchat                 | https://feelinsonice.appspot.com/web/deeplink/snapcode?username[redacted]ize=400&type=SVG | social    |       | profiler |
| 39    |                       | Spotify                  | https://open.spotify.com/user/[redacted]                                                  | music     |       | profiler |
| 40    |                       | TikTok                   | https://www.tiktok.com/oembed?url=https://www.tiktok.com/[redacted]                       | social    |       | profiler |
| 41    |                       | tripadvisor              | https://www.tripadvisor.com/Profile/[redacted]                                            | social    |       | profiler |
| 42    |                       | Twitter                  | https://nitter.net[redacted]                                                              | social    |       | profiler |
| 43    |                       | Twitter archived tweets  | http://archive.org/wayback/available?url=https://twitter.com/[redacted]/status/*          | archived  |       | profiler |
| 44    |                       | Wanelo                   | https://wanelo.co/[redacted]                                                              | shopping  |       | profiler |
| 45    |                       | Xbox Gamertag            | https://www.xboxgamertag.com/search/[redacted]                                            | gaming    |       | profiler |
+------------------------------------------------------------------------------------------------------------------------------------------------------------------------+
```

Figure 5.3: S1: Recon-NG profiler

Like Recon-NG's profiler, Sherlock will look after the username and see if it finds any usernames from a comprehensive social media and services list. Running Sherlock on S1's provided usernames, many different profiles were found. The results were similar to Recon-NG's profiler due to how similar they are and having the same objective.

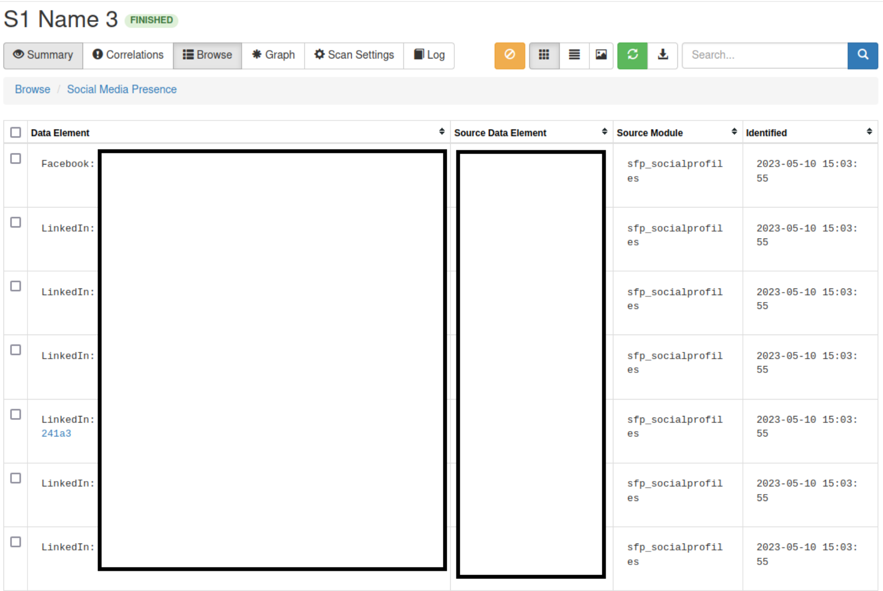


```
┌─[michael@parrot]─[~/spiderfoot-4.0/sherlock]
└──╼ $python3 sherlock [redacted]
[*] Checking username [redacted] on:

[+] BitBucket: https://bitbucket.org/[redacted]
[+] Chess: https://www.chess.com/member/[redacted]
[+] Clubhouse: https://www.clubhouse.com/@[redacted]
[+] DeviantART: https://[redacted].deviantart.com
[+] Disqus: https://disqus.com/[redacted]
[+] Duolingo: https://www.duolingo.com/profile/[redacted]
[+] Enjin: https://www.enjin.com/profile/[redacted]
[+] Freesound: https://freesound.org/people/[redacted]
[+] G2G: https://www.g2g.com/[redacted]
[+] GitHub: https://www.github.com/[redacted]
[+] GitLab: https://gitlab.com/[redacted]
[+] Gravatar: http://en.gravatar.com/[redacted]
[+] Kaggle: https://www.kaggle.com/[redacted]
[+] Kik: https://kik.me/[redacted]
[+] Lichess: https://lichess.org/@/[redacted]
[+] Periscope: https://www.periscope.tv/[redacted]/
[+] Replit.com: https://replit.com/@[redacted]
[+] Roblox: https://www.roblox.com/user.aspx?username=[redacted]
[+] SlideShare: https://slideshare.net/[redacted]
[+] Snapchat: https://www.snapchat.com/add/[redacted]
[+] Sportlerfrage: https://www.sportlerfrage.net/nutzer/[redacted]
[+] Spotify: https://open.spotify.com/user/[redacted]
[+] TikTok: https://tiktok.com/@[redacted]
[+] Twitch: https://www.twitch.tv/[redacted]
[+] Twitter: https://twitter.com/[redacted]
[+] VK: https://vk.com/[redacted]
[+] WordPress: https://[redacted].wordpress.com/
[+] Youtube User: https://www.youtube.com/user/[redacted]
[+] last.fm: https://last.fm/user/[redacted]
```

Figure 5.4: S1: Sherlock results

SpiderFoot supports a lot of different inputs. For this investigation, the following inputs will be used: Full name, email address, and username. To start a scan using SpiderFoot, one can click on the "new scan" button and choose a name for the scan. Afterward, the investigator must write down what will be searched in the "Scan Target" input field. SpiderFoot will automatically detect what type of information the input data are. One can also choose what data are relevant and what modules will run on the scan. For simplicity's sake, running the following scans, all modules will be run, and bloat will be filtered after the scan has been run. The primary purpose of choosing specific modules is to save time running the scans. Running a scan on S1's full name resulted in some social media profiles being found, specifically on LinkedIn and Facebook, as seen in Figure 5.5.



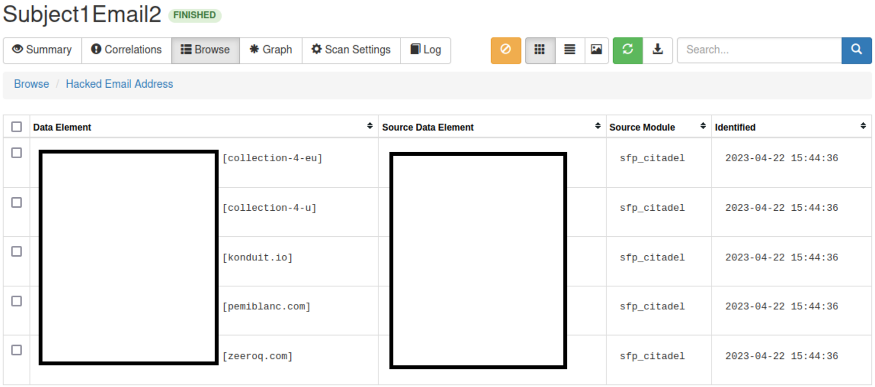
S1 Name 3 FINISHED

Browse / Social Media Presence

□	Data Element	Source Data Element	Source Module	Identified
□	Facebook: [redacted]	[redacted]	sfp_socialprofiles	2023-05-10 15:03:55
□	LinkedIn: [redacted]	[redacted]	sfp_socialprofiles	2023-05-10 15:03:55
□	LinkedIn: [redacted]	[redacted]	sfp_socialprofiles	2023-05-10 15:03:55
□	LinkedIn: [redacted]	[redacted]	sfp_socialprofiles	2023-05-10 15:03:55
□	LinkedIn: [redacted] 241a3	[redacted]	sfp_socialprofiles	2023-05-10 15:03:55
□	LinkedIn: [redacted]	[redacted]	sfp_socialprofiles	2023-05-10 15:03:55
□	LinkedIn: [redacted]	[redacted]	sfp_socialprofiles	2023-05-10 15:03:55

Figure 5.5: S1: SpiderFoot full name scan

In addition to a full name scan, an email scan was performed on the subject's email address. The results were some data breaches and usernames associated with the account. For example, Collection 4 (Part of Collection 1 through 5) is a known document containing millions of login credentials originating from the dark web [26]. These credentials were sold and distributed on the dark web and the MEGA file-sharing services and contain data from earlier breaches such as Yahoo!, LinkedIn, and Dropbox [27]. In this breach S1's email was found, it is not stated what credentials other than the email was found, but it is assumed that either a plaintext or hashed password is there as well.



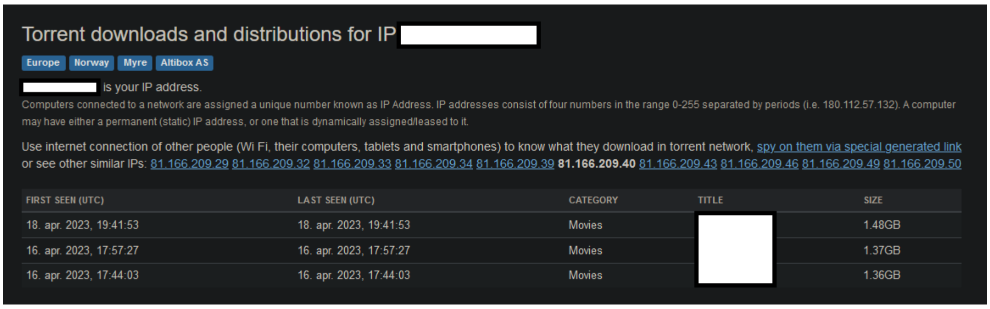
Subject1Email2 FINISHED

Browse / Hacked Email Address

□	Data Element	Source Data Element	Source Module	Identified
□	[redacted] [collection-4-eu]	[redacted]	sfp_citadel	2023-04-22 15:44:36
□	[redacted] [collection-4-u]	[redacted]	sfp_citadel	2023-04-22 15:44:36
□	[redacted] [konduit.io]	[redacted]	sfp_citadel	2023-04-22 15:44:36
□	[redacted] [pemiblanc.com]	[redacted]	sfp_citadel	2023-04-22 15:44:36
□	[redacted] [zeeroq.com]	[redacted]	sfp_citadel	2023-04-22 15:44:36

Figure 5.6: S1: SpiderFoot email scan, found some data breaches

The other tools used were *Iknowwhatyoudownload* and *HaveIBeenPwned?*. Iknowwhatyoudownload is a tool that shows IPs using the P2P torrenting network used on the internet to share and download files. Torrents are public, and it needs to be public to be able to share the files with others. Iknowwhatyoudownload displays this in an easy-to-read way, so one can search after an IP on the site to look at a specific IP address's torrenting history. Each entry has information about it, such as what was downloaded, when, and a general category of the downloaded files. S1 had no recorded recent history of using torrenting to download files. However, figure 5.7 is an example of what information is displayed about the torrenting history of an IP.



Torrent downloads and distributions for IP [redacted]

[redacted] is your IP address.

Computers connected to a network are assigned a unique number known as IP Address. IP addresses consist of four numbers in the range 0-255 separated by periods (i.e. 180.112.57.132). A computer may have either a permanent (static) IP address, or one that is dynamically assigned/leased to it.

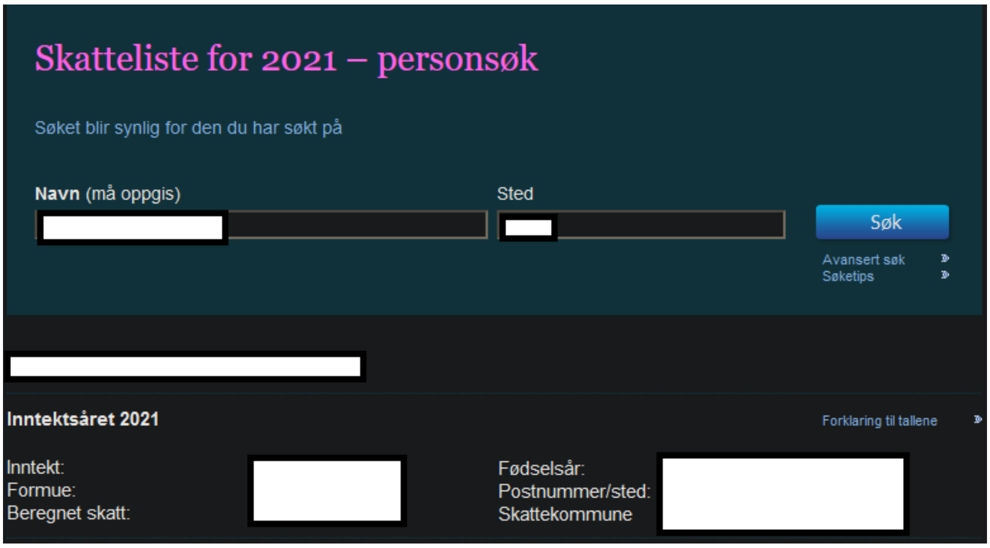
Use internet connection of other people (Wi Fi, their computers, tablets and smartphones) to know what they download in torrent network, spy on them via special generated link or see other similar IPs: 81.166.209.29 81.166.209.32 81.166.209.33 81.166.209.34 81.166.209.39 **81.166.209.40** 81.166.209.43 81.166.209.46 81.166.209.49 81.166.209.50

FIRST SEEN (UTC)	LAST SEEN (UTC)	CATEGORY	TITLE	SIZE
18. apr. 2023, 19:41:53	18. apr. 2023, 19:41:53	Movies	[redacted]	1.48GB
16. apr. 2023, 17:57:27	16. apr. 2023, 17:57:27	Movies	[redacted]	1.37GB
16. apr. 2023, 17:44:03	16. apr. 2023, 17:44:03	Movies	[redacted]	1.36GB

Figure 5.7: example of an IP search on Iknowwhatyoudownload

HaveIBeenPwned is a well-known service where email addresses can be looked up in known security breaches. When searching using S1's email addresses, breaches such as *MyHeritage*, *Gervatar*, *Kayo.moe*, and *Pemiblanc* were discovered. The email was also found in a database containing breaches and credential stuffing lists. This list could be a problem if the subject was unaware of the breach and used the leaked password on other important social media or email services, making it so a credential-stuffing attack could be performed. A credential stuffing attack uses a credential stuffing list, which is a list with combinations of credentials, often email or usernames, combined with the corresponding password to the account [28].

Skatteetaten, Proff.no, and Brønnøysundregistrene were tested to test some specific Norwegian services. Skatteetatens has a public tax list, which any Norwegian with an income can be searched after. Searching after S1 on the tax lists, there came up with some information about S1's income, fortune, and estimated tax in 2021. Additionally, S1's date of birth, zip code, and municipality the person is located. However, searching the tax lists is not anonymous. The Norwegian parliament decided that to search these lists, one needs to log into Skatteetaten, and when a name is searched, the person searched can look into who has seen their tax records.



Skatteliste for 2021 – personsøk

Søket blir synlig for den du har søkt på

Navn (må oppgis) [redacted]

Sted [redacted]

[redacted]

Inntektsåret 2021

Inntekt:
Formue:
Beregnet skatt: [redacted]

Fødselsår:
Postnummer/sted:
Skattekommune [redacted]

Figure 5.8: S1: Skattelistene, which is the public tax list in Norway

Proff.no and Brønnøysundregistrene are similar to those searching online catalogs such as Gulesider. Still, rather than only focusing on people, it is more for searching after companies and organizations that operate in Norway. There are no companies connected with S1. However, if there were any registered on S1, some information could be found, such as which companies the person is a part of, some information about owned stocks, and some direct relations connected through the listed company. The same can be said about Brønnøysundregistrene as it primarily focuses on making information about companies open for everyone to see (See fig. A.15 and A.16)

5.2.2 Subject 2

Subject 2	**Description**
Provided personal data	Full name
Subject background	Subject 2 has no background in cyber- or information security. The subject has social media profiles on the most popular social media services and uses them regularly.

Table 5.2: Subject 2 (S2) card

Choosing the tools

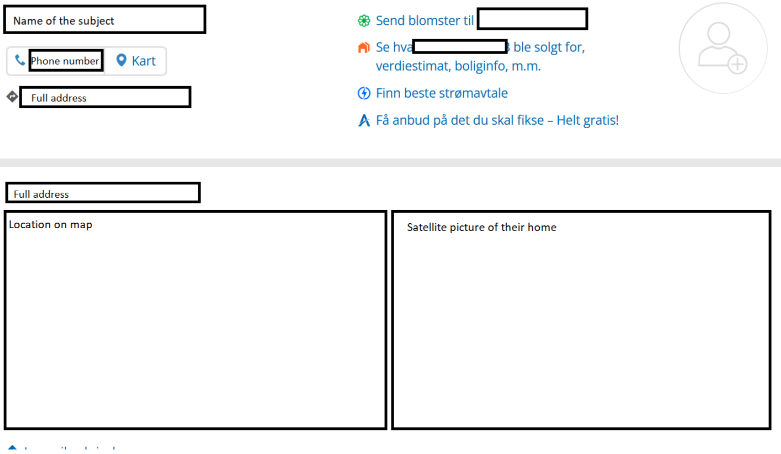
As only the name is accessible from the start, Maltego, SpiderFoot, and the search engines will be used. If a username were to be found, Recon-NG and Sherlock would be used to find accounts tied to that username, including some basic permutations of that username.

Running the tools

Subject 2 (S2) has no background in information security, meaning the subject likely needs to understand digital footprints and how their internet presence is available to others. The reasoning for choosing a subject with no background in cyber security is mainly to contrast the results, which differ between someone with an understanding and someone who knows less about information security.

Using search engines resulted in information about S2, such as social media profiles from LinkedIn, Instagram, Facebook, Instagram, and YouTube. There was also a Tise, an online marketplace similar to Finn.no, public profile. Additionally, there were hits on different online catalog services, specifically Gulesider and 1881. These results give basic profiling for S2, containing pictures, addresses, phone numbers, social media profiles, and even a username used for the YouTube profile.

When running Maltego, connections were made when running a "full transform" on the S2's name, specifically towards some social media profiles and internet catalogs such as Gulesider and 1881. The social medias found were as follows: LinkedIn, Instagram, and Pinterest. The subject's Instagram profile was private, meaning there is no way of seeing what content has been posted, but the username and profile picture are available for all to see. Gulesider and 1881 had more information about the subject, as seen in figure 5.9. This information would be their phone number, home address, GPS coordinates, and a satellite picture of their home.



Name of the subject

☎ Phone number Kart

Full address

Send blomster til [redacted]

Se hva [redacted] ble solgt for, verdiestimat, boliginfo, m.m.

Finn beste strømavtale

Få anbud på det du skal fikse – Helt gratis!

Full address

Figure 5.9: Screenshot of S2's 1881 page, containing personal information such as full name, address, phone number, GPS coordinates, and picture of their home

A username was found on the YouTube channel using the search engines and Maltego. Furthermore, due to this, Sherlock and Recon-NG can be used on the found username. Running Sherlock and Recon-NG on the username resulted in similar results as S1. Some permutations were used to find more profiles, such as removing the numbers at the end of the found username and trying "FIRST-

NAME.LASTNAME" as a username. Some profiles were discovered, but many bloat and irrelevant profiles were found, as with S1. Nevertheless, some profiles were explicitly found on TikTok, Twitch, VSCO, Spotify, and Snapchat, which often do not appear on search results on search engines during the tests done searching after the username in quotation marks.

5.2.3 Subject 3

Subject 3	**Description**
Provided personal data	Name
Subject background	Subject 3 (S3) has an extensive background in Information security, and is an industry professional spanning multiple years.

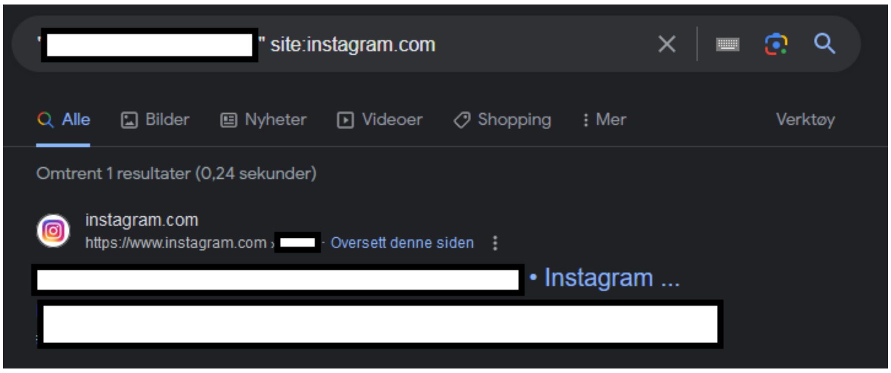
Table 5.3: Subject 3 (S3) card

Choosing the tools

Similar to S2, only the subject's name is available, and therefore to start Maltego, SpiderFoot, and search engines will be used. Furthermore, if a username is found, Recon-NG and Sherlock will be used to find accounts tied to that username and similar username permutations.

Running the tools

Using search engines resulted in information about S3, such as the place of work, social media profiles from LinkedIn and Instagram, online catalogs, and relevant news articles. As usual, the online catalogs contained information about S3's home address, phone number, and GPS location of their home. Furthermore, on Instagram, a username was found related to S3. This username will later be used with Sherlock and Recon-NG.



"[redacted]" site:instagram.com

Omtrent 1 resultater (0,24 sekunder)

instagram.com
https://www.instagram.com › [redacted] · Oversett denne siden

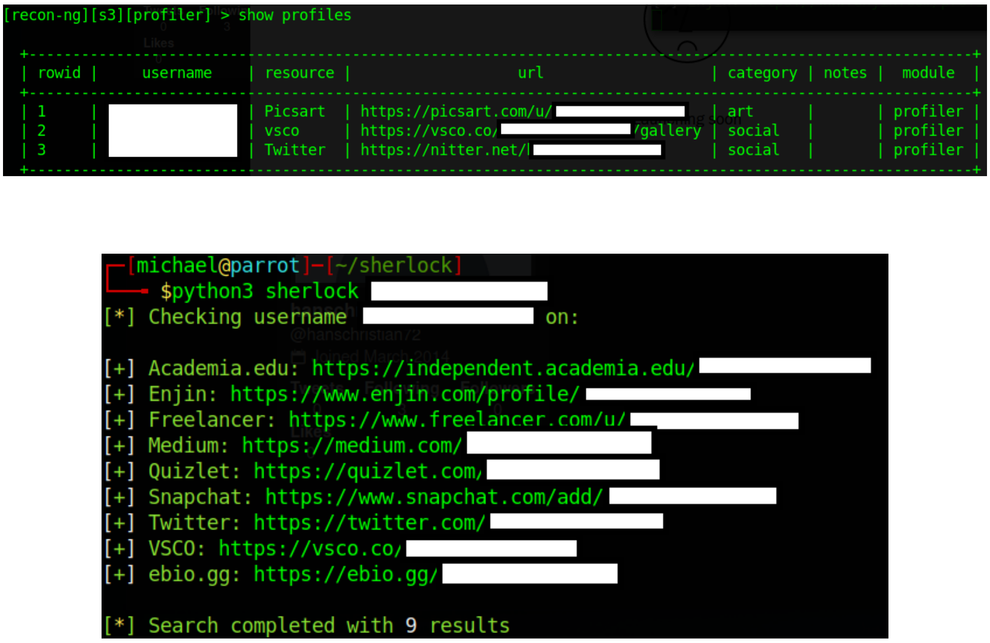
[redacted] • Instagram ...

[redacted]

Figure 5.10: S3: Search result on Google, "site:Instagram.com" used to filter out bloat data

After this, Maltego was run. Running a "full transform" on S3's name led to discoveries similar to the search engine results—specifically S3's LinkedIn, the online catalogs, and related news articles. Maltego Community Edition limits the data found to 12 results per transform. This limitation is an issue as S3 had many data related to them when using the search engines as Maltego relies on search results from Bing. Nevertheless, some information was found that is related and highly relevant. After this, a "full transform" of S3's phone number was run, found in the online catalogs. This transform led to similar findings, such as the subject's place of work and some telecom operator information.

Furthermore, using the username found to run Recon-NG and Sherlock led to some new findings, such as an account on Twitter, Snapchat, Medium, Academia.edu, and VSCO, as seen in Figure 5.11. These are accounts that share the username found on the Instagram profile.



```
[recon-ng][s3][profiler] > show profiles

  +-----------------------------------------------------------------------------------------------------------+
  | rowid |     username     | resource |                        url                        | category | notes |  module  |
  +-----------------------------------------------------------------------------------------------------------+
  | 1     | [redacted]       | Picsart  | https://picsart.com/u/[redacted]                  | art      |       | profiler |
  | 2     |                  | vsco     | https://vsco.co/[redacted]/gallery                | social   |       | profiler |
  | 3     |                  | Twitter  | https://nitter.net/[redacted]                     | social   |       | profiler |
  +-----------------------------------------------------------------------------------------------------------+
```

```
┌─[michael@parrot]─[~/sherlock]
└──╼ $python3 sherlock [redacted]
[*] Checking username [redacted] on:

[+] Academia.edu: https://independent.academia.edu/[redacted]
[+] Enjin: https://www.enjin.com/profile/[redacted]
[+] Freelancer: https://www.freelancer.com/u/[redacted]
[+] Medium: https://medium.com/[redacted]
[+] Quizlet: https://quizlet.com/[redacted]
[+] Snapchat: https://www.snapchat.com/add/[redacted]
[+] Twitter: https://twitter.com/[redacted]
[+] VSCO: https://vsco.co/[redacted]
[+] ebio.gg: https://ebio.gg/[redacted]

[*] Search completed with 9 results
```

Figure 5.11: S3: Recon-NG and Sherlock results

The results from SpiderFoot could have been better, only being able to find the LinkedIn profile of S3 and a Facebook post related to the subject. All the other information found was an inactive account on a video-sharing site and some usernames derived from the full name, meaning they are only suggestions of potential usernames the name can have, as some usernames are permutations of one's name.

5.2.4 Subject 4

Subject 4	**Description**
Provided personal data	Name
Subject background	Subject 4 (S4) is a public figure with all social media profiles open.

Table 5.4: Subject 4 (S4) card

Choosing the tools

This subject is a more particular case as S4 relies highly on its public perception and online presence. The reasoning for choosing a public figure is to look into how and what the tools will be able to find about someone that is the most likely to be a PoI for someone as their names are more well-known.

Running the tools

Searching after S4 on search engines leads to many varied results, primarily social media profiles and news articles, blogs, and other related results. These results are expected as the person relies on their internet presence and wants as many relevant results as possible.

After the search engine searches, a "full transform" of S4's names was done in Maltego. S4 does not use its full name on social media as its primary alias. Therefore, the transform must be done three times, one for the birth name, one for the full, and one for the shortened handle. The results generated from this are varied but are relevant. Some bloat was to be expected, which in this case was a lot of irrelevant phone numbers. Other than that, some results were mainly from social media profiles, blogs, news articles, and related websites containing information about S4.

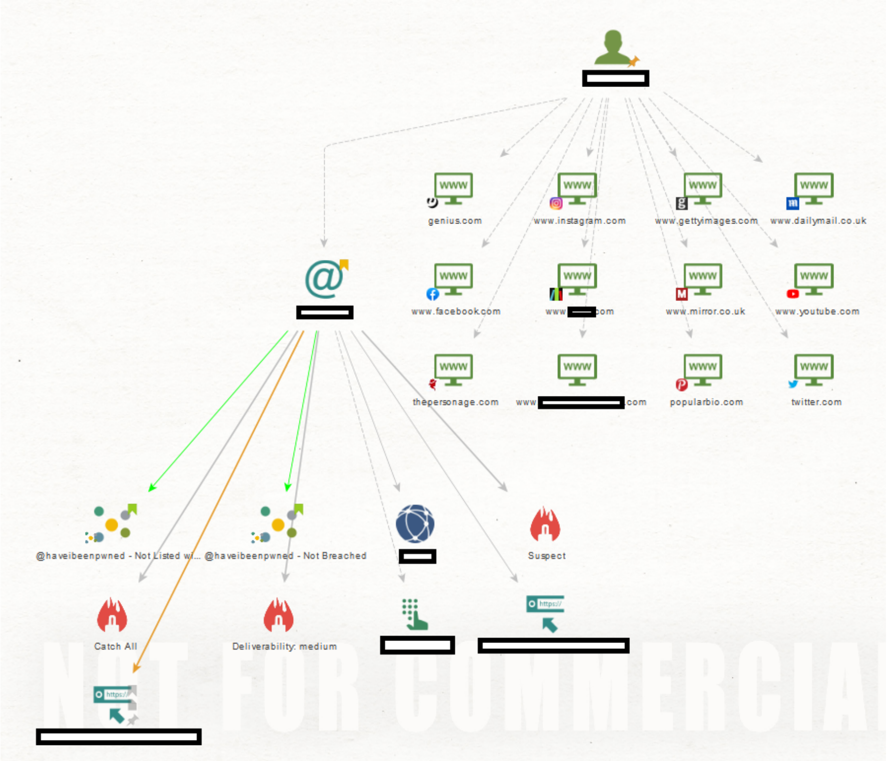
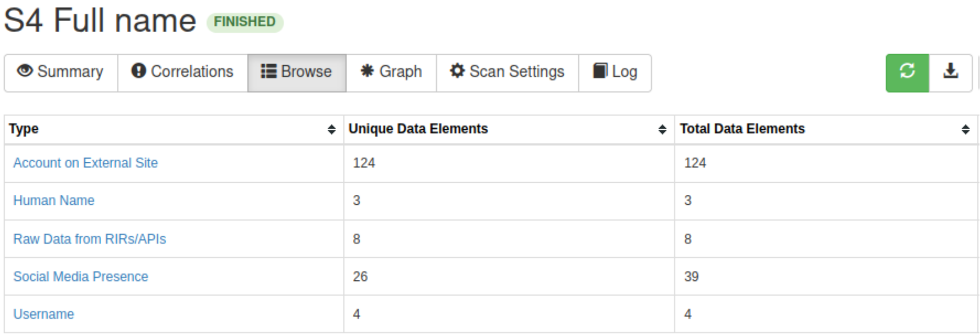


Figure 5.12: S4: Maltego results from running a full transform on the name and found email

SpiderFoot yielded some varied results but was able to link S4 to 148 different social media profiles and related social media posts. These results mainly were only related somewhat to the name, and 54 of the found accounts were connected to another person entirely. Nevertheless, some were relevant such as S4's Twitter, Instagram, and Facebook groups.



Type	Unique Data Elements	Total Data Elements
Account on External Site	124	124
Human Name	3	3
Raw Data from RIRs/APIs	8	8
Social Media Presence	26	39
Username	4	4

Figure 5.13: S4: SpiderFoot total results on the full name scan

5.3 Experiment results

The experiment was mostly successful, testing the tools and seeing how and what they could gather about people using their names, usernames, emails, and phone numbers. Maltego, SpiderFoot, Recon-NG, and Sherlock were exciting tools that were easy to use and could get varying results and information about the target. Each tool had varied results as each is made for specific purposes and uses. The most successful tool in this experiment was, without a doubt, Maltego CE. Maltego, even though it was limited by being the Community Edition license of the software, could profile the targets most accurately and provided the most diverse information about the target compared to the others, such as SpiderFoot. The collected data by Maltego mainly from social media profiles, news articles, online catalogs, and other sites related to the person. It also tried, and mostly was unsuccessful, to automatically scrape emails and phone numbers and display them with the corresponding person. The emails were primarily gathered from websites such as the person's place of work, not the online catalogs, which could mean that Maltego needs to recognize services as what they are. The issue could be that Maltego was not created to target Norwegian people and services, so it struggled with recognizing the websites. However, it could find the online catalogs, so just clicking on the provided link in Maltego did show the corresponding profile on these sites. Most of these tools are made for OSINT investigations abroad, not Norway, so specific services that only apply to Norway may get ignored or seen as spam. Furthermore, just like the Norwegian online catalogs, specific catalogs are made for finding people from the US, UK, and other countries, which some tools may have utilized, but as the subjects used were all Norwegian would not have worked.

SpiderFoot also worked to some extent but struggled with finding diverse information about the target, mostly only finding the associated LinkedIn and maybe some other social media profiles. Many of the found profiles were not even associated, so much bloat data was found about the target during the scan. The tool is also highly reliant on API access to work, and as there are over 200 different modules where each has its requirements or unique APIs. Managing and paying for each is not viable for a project like this one.

Recon-NG and Sherlock worked pretty well, but the Profiler module used with Recon-NG and Sherlock is aimed towards more of username OSINT, looking after users who share a username. When input with usernames, the tools could find many different users on dozens of services for each username. These accounts varied from inactive users to some that were more used by the subjects. Nevertheless, these results could not have been found using search engines, or tools using search engines as their data collection (Maltego), as these accounts do not appear on the search results.

In conclusion, the OSINT tools can profile targets using their real name, correlating data such as names, relations, phone numbers, email addresses, social media profiles, and news articles to a person. This profiling can be beneficial in many scenarios regarding law enforcement and more malicious activities.

5.4 Analysis of experiment results

Now that the experiment has concluded, the analysis will start, and the research questions will be answered.

5.4.1 What types of data were collected during the experiment?

Many OSINT tools act as glorified search engines, making it easier to organize data found and extract some specifics rather than bombarding the investigator with much bloat information. Much data can be collected from people when running OSINT tools. The tools run are created to gather data about people, aliases, locations, or other data types. Precisely for this experiment, the focus was on what can be found by only using a full name, and if that leads to more personal information, then testing what the newly gathered information can produce. In this case, social media profiles and internet catalogs were the main findings when running the tools, as these contain many data regarding the person. When running the tools, social media profiles such as LinkedIn and Instagram were found for each subject. These social media profiles have a lot of information about the person, such as place of work, occupation, name, relations, locations, and pictures. Using this as initial profiling can be made to understand what type of person the target is and how they behave. The experiment only focuses on personal information, focusing on full names and usernames. Some testing was done on other types of information, such as IP addresses, but more research was needed.

Asset	Description
Full name	A full name that is connected to an individual. Only a first- or last-name is not valuable in OSINT investigations, as many people share names. When using OSINT to investigate an individual, this information is required.
Address	An address connected to an individual or a group of people. Data in this group include address, zip code, and city. Addresses can be searched using online catalogs such as Gulesider, 1881, and similar services.
Phone number	A phone number connected to an individual. It can be a private number or a work number.
Email address	An email connected to an individual. Used for communication or registering on different services on the internet.
Username	An alias is used in different services on the internet. A username is connected to specific accounts used on the internet.
Social media profiles	A social media profile of an individual. It can be on services such as Facebook, Instagram, LinkedIn, and others. Social media profiles contain much extra information about an individual, such as: pictures, relations, life events, interests, names, and more.
Other profiles/accounts	Accounts on non-social media services. Often contain less information directly connected to an individual. Often found by using username OSINT techniques rather than searching a full name.
Pictures	Picture of an individual or related to an individual. Usually found on search engine searches and social media profiles.
News articles	News articles that are related or contain mentions of the individual.

Table 5.5: Table with what information was found during the experiment

5.4.2 OSINT is excellent for profiling a PoI

The experiment concludes that this OSINT investigation is excellent for profiling a potential PoI. OSINT is relevant for law enforcement, pen testing scenarios, phishing exercises, and malicious activities. If there is interest in profiling a PoI, these types of tools can be run to gather a lot of information, including names, friends, relations, pictures of the target, their home address, phone numbers, and place of work. There are limits to how exciting or unique the information found is, but the fact still stands, this information can be used to profile someone and create a general understanding of their behavior and life.

5.4.3 Great accessibility of tools

The tools used, and many more, are accessible to be used by anyone with some degree of technical understanding. Maltego and SpiderFoot are almost plug-and-play tools that do not need to configure many parameters and support an easy-to-use GUI, making using the tools easier than CLI-based tools such as Recon-NG and Sherlock. Usability aside, the main advantage of these tools is that they are available for everyone to use and, often, are free, even though some need subscriptions to use all the features, meaning everyone can use them if needed. In addition, the tools are designed to focus on data that is already accessible on the internet.

5.4.4 Threats of OSINT and risk scenarios

As OSINT can be accessible by everyone, there is bound to be some misuse of the tools and data. Many studies point toward spear phishing, a targeted phishing attempt toward someone or something [29].

Scenario 1: OSINT is used to perform a spear phishing attack

- **Description:** Someone has a person on their radar and is a PoI for some of their personal goal or agenda. They want to extort the person for money or at least try to get some personal information or a debit card number. The method the threat has decided on is social engineering and phishing. So they need to profile the person to make their attempt more believable for S1. They know S1's name, and that is what they have beforehand before starting any data collection. They decide to use Maltego to make the investigation as straightforward as possible, as Maltego supports an excellent tool for structuring much information. They then run the tool and get a lot of information about S1, such as their place of work, social media profiles, relations, address, phone numbers, usernames, and even email addresses related to their target. The threat can now communicate with the target through a direct social media message, email, or phone number. Additionally, now the threat has a lot more to go on. Phishing attacks often rely on the trust of the victim of the attack, impersonating famous people or companies to extract information. People should know that if a famous person asks about some personal information, it is most likely a scam and not legitimate. This dynamic changes when someone the target knows personally contacts them, and there are recent examples of this [30] where someone poses as a friend, family, or someone related to their phishing attack.

- **Impact:** 3
- **Probability:** 2
- **Calculated risk:** 6

Scenario 2: Threat agent uses data leak to hijack accounts to a target

- **Description:** A threat agent is interested in the target's accounts using their mail. The threat agent uses HaveIBeenPwned to determine whether the email has been in recent data breaches. There was a more recent breach, and after some time searching the web, the threat agent found the leak on a discussion board. The leaked credentials were plaintext, including the mail, username, and password. Using the username found on the leaked credentials, the threat agent can now use Sherlock and Recon-NG to find an account connected to the target. This finding led to the threat agent finding and being able to log into various accounts connected to the target, as the passwords had not been changed and there was no 2FA in place.
- **Impact:** 4
- **Probability:** 2
- **Calculated risk:** 8

Scenario 3: Stalker uses OSINT to find information about target

- **Description:** A stalker is interested in a public figure, and the public figure has all their data accessible online as they rely on social media presence for their career. The stalker knows the person's full name and social media usernames. Using Maltego, the stalker can find a lot of information about the target, such as all social media profiles, news articles, and some online catalogs. The target had not restricted their teleoperator from sharing personal information to the online catalogs, meaning their full name, address, and phone number are available online. The stalker knows where the target lives, their name, address, and phone number.
- **Impact:** 4
- **Probability:** 2
- **Calculated risk:** 8

Scenario 4: Someone uses the username to find the real identity of a person

- **Description:** Someone had a heated discussion on a forum, and the person wants to find the real identity of the other person in the discussion. Using their knowledge about Sherlock and Recon-NG, investigates what profiles that are connected with the same username. After running the tools, some profiles were found, including a social media profile that had their real name displayed. Using this newfound knowledge, uses Google searches after the name, finding their social media profiles and online catalog pages, which include the address and a phone number.
- **Impact:** 2
- **Probability:** 2
- **Calculated risk:** 4

Scenario 5: Scammer impersonates target to phish targets relatives

- **Description:** A scammer wants to seem more trustworthy during their phishing attempts. To do this, they chose a target and used OSINT tools to impersonate them. They have a name and use Maltego to get more information about the target. Maltego can find the target's Instagram and Facebook profiles, which are both public. Using this, the scammer downloads and uses pictures from the target's Instagram to create a fake profile on Instagram and Facebook. Using this profile, the scammer attempts to contact friends and family of the target with a phishing link. Most ignore and report the profile. However, someone falls for the attempt and gives away personal information as well as their debit card information [31].
- **Impact:** 4
- **Probability:** 2
- **Calculated risk:** 8

5.4.5 Risk matrix

	1 - Low	2 - Medium	3 - High	4 - Very high
3 - Very likely				
2 - Likely		4	1	2, 3, 5
1 - Not likely				

Table 5.6: Risk matrix before countermeasures, the impact- and probability tables can be found on Table 4.1, 4.2, and 4.3

5.5 Answering the research questions

5.5.1 How vulnerable are we as individuals due to potentially too much openness?

Transparency, truth, and trust are three fundamental ideas regarding openness in society. Steele and Bloom [20] explores the philosophical and cultural ideas of an Open-Source Everything society where transparency, truth, and trust lie in the center and where society works towards the betterment of society and humanity. Norway, which is the focus of this thesis, is regarded as one of the most developed countries in the world according to the United Nations Human Development Index [32] and considered as having one of the most transparent and least corrupt governments in the world according to the Open Government Partnership [33]. One can argue that the government is seen as less corrupt due to its transparency with its people. Tax records and online catalogs are also available publicly in Norway, where personal information is open to the public and part of a more transparent society [34]. The reason for the public tax records is to help society and uncover tax evasion or other tax fraud attempts. In addition, NRK argues that having this public shows where the taxes are going, how the economy works, and whether societal differences have changed [35].

However, openness can lead to misuse, as presented in this thesis. OSINT is the collection of open information directly from open sources on the internet. Maltego, SpiderFoot, Recon-NG, and Sherlock are potent tools that can profile people only using their names, usernames, and more. Knowing someone's address, relations, and phone numbers can lead to scenarios that may be uncomfortable, may cause unease, and even physical and financial harm [2]. There should be possibilities to reduce one's online presence and increase awareness about someone online. One should understand that one lays footprints on the internet; each account created, post published, and comment on a forum can potentially be traced back to an individual.

Although, this should not be the reason to make a less open society, and people should not have to worry about OSINT. OSINT is a tool to be used not only for malicious purposes but for positive things as well. Open source and transparency of information, knowledge, and data may help countries with development. It may as well be one of the reasoning's why Norway is as highly developed as it is [20]. Anonymous databases could also help with openness as well as not being a benefit to OSINT, as OSINT primarily relies on being able to associate information with something or someone [2].

5.5.2 How are OSINT tools problematic for individuals?

OSINT and OSINT tools make gathering publicly available much more accessible than a manual approach. With only a name, much information about each individual can be collected. What may be problematic with these tools is the amount of information that can be collected in a short amount of time. This information can and will lead to a threat being able to create somewhat accurate profiles of their targets, with data such as names, addresses, contact information, pictures, relations, locations, and social media profiles. Furthermore, to find this information, only the name is needed. If the one investigating the target has more details at the start, the results will be more extensive.

5.5.3 How to reduce vulnerability to OSINT?

Most OSINT tools use search engines or a preexisting database to do their searches and correlations to an individual. Maltego uses Bing, and some downloadable modules use Google, SpiderFoot uses either Bing or Google, and Recon-NG uses Google or Bing, meaning to reduce the amount of data that these tools can collect about someone one needs to be aware of what is available on the search engines. In 2014 the European Union's GDPR signed a new regulation so individuals can demand organizations to delete their data [36].

"The data subject shall have the right to obtain from the controller the erasure of personal data concerning them without undue delay, and the controller shall have an obligation to erase personal data without undue delay" [37]

This regulation has been named the *right to be forgotten* and applies to every organization that treats the personal data of EU citizens; this applies to the search engines like Google, Bing, Yahoo, and DuckDuckGo. To request that data be deleted from the search engines, each service needs to be able to delete specific results that appear when searching after a full name. A form can be filled out to request deletion, or some form of data protection officer can be contacted to request the deletion of data. This form is a proactive approach, meaning that this has to be done before someone uses OSINT tools or is investigating someone. If this happens after the data collection, it will not affect the investigation or the already produced data. Theoretically, if a person were to delete everything about themselves, or at least every result, on each of the search engines Maltego, SpiderFoot, and some modules on Recon-NG would not be able to produce any relevant data as they rely on the search engines to work and find data. In addition, one may ask to get deleted from any service. As for the subjects, one idea could also be to remove themselves from the online catalogs. However, to remove themselves from these, the person needs to contact their telecom operator to ask them to restrict sharing personal information to online catalogs, which is how the online catalogs get personal information connected to a name, address, or phone number [38].

These countermeasures only help with one part of the problem, making it so that little information can be gathered about someone. However, this is only part of the problem. If someone is the target of a spear phishing attack, the problem is not how accurate it is but how the target reacts. According to a study conducted by Halevi *et al.* [29], around 30 % of people tested on a spear phishing attempt fell for the attempt, downloading some malicious software that could have been malicious or did something similar to be considered "phished." The methodology used relied on exploiting the employees' trust, where the mail sent was from the internal systems and impersonated someone known from the IT staff. A similar approach could be made using OSINT by investigating some data about relations and people the target should know about, such as family or a colleague. What also was tested was if risk perception affected how likely the people were to be phished. This hypothesis was proven to have some effect, meaning people with better risk or phishing perception should be less likely to fall for a phishing attempt. Where the perception has to change is who one should be aware of, it is no longer just someone posing to be Microsoft or the boss of one's place of work. It can be family, friends, and other closer relations.

Countermeasures applied to the risk scenarios

Scenario 1: OSINT is used to perform a spear phishing attack

There are no solutions to "solve" spear phishing; everyone is susceptible and has the potential to be phished using it. However, as pointed out by Halevi *et al.* [29], cyber security training has a noticeable effect on likely someone is to get phished. Phishing has evolved. It is no longer a well-known company being impersonated; it now also has the potential to be someone related to someone. There should also ring some bells when a relative asks for personal information.

- Impact after measures: 2
- Probability after measures: 2
- Risk after measures: 4

Scenario 2: Threat agent uses data leak to hijack accounts to a target

People who know about data leaks can change passwords and credentials. A good password policy, or a routine of changing passwords every, or every other, year, should make it so this can not happen as often as one would assume. Passwords are just one part of credentials. As Two-Factor Authentication (2FA) has become increasingly popular, and most, if not all, websites use 2FA as an additional security measure. These measures make it near impossible for anyone to use a leaked password if the leak happened recently. Furthermore, the account hijacker cannot get through the 2FA even with a password. This measure does not change the risk's impact on someone, only the probability.

- Impact after measures: 4
- Probability after measures: 1
- Risk after measures: 4

Scenario 3: Stalker uses OSINT to find information about target

Restricting the available data on the web is the way to reduce what data can be found. Using the right to be forgotten is a start and should be applied to as many services as possible. Deleting search results are the most applicable for this scenario, as many of the tools tested and assessed during the thesis primarily use search engines as their sources. Suppose this is applied to a theoretical maximum of the most relevant pieces of information, such as online catalogs and social media. In that case, the amount of information will be much less impactful, and the profiling performed will be much less helpful in a cyberstalking scenario.

- Impact after measures: 2
- Probability after measures: 1
- Risk after measures: 2

Scenario 4: Someone uses the username to find the real identity of a person

Ensure that when creating usernames, not a username associated with a person. Please avoid using the same username on services that are not social media, making it so that a username search does not connect with a social media or service that can be traced back to an individual. Permutations are not enough; making unique usernames is vital in ensuring they can not be traced to an individual.

- Impact after measures: 1
- Probability after measures: 1
- Risk after measures: 1

Scenario 5: Scammer impersonates target to phish targets relatives

Similar to measures in scenario 1, awareness is vital. Being aware that phishing can also be from relatives is the knowledge that will be able to prevent phishing from happening.

- Impact after measures: 3
- Probability after measures: 1
- Risk after measures: 3

Risk matrix after measures

	1 - Low	2 - Medium	3 - High	4 - Very high
3 - Very likely				
2 - Likely		1		
1 - Not likly	4	3	5	2

Table 5.7: Risk matrix after countermeasures

5.6 Issues encountered during the execution of the experiment

Even though the experiment went reasonably well, some issues arose regarding API access, bloat, and the performance of SpiderFoot.

5.6.1 API access

Due to a change in attitudes towards free-to-use APIs, some APIs have chosen to go towards a more paid solution for their users and developers. One of the more recent examples would be Elon Musk announcing the Twitter API to become a paid service, needing its developers to pay a fee to use the API, which, In addition to being paid, is now a tiered service [39]. Following this, Reddit announced API changes as well following suit making a previously free-to-use API paid[1]. Nevertheless, many APIs are and have been paid and subscription-based since long before the project start, Bing, Pipl, IntelligenceX, and others are in this category and getting access to their premium features could be costly as they are most suited for professional use and companies and not for smaller projects such as this one.

5.6.2 A lot of bloat data

As expected, a lot of bloat data was created. This bloat is a well-known issue regarding OSINT investigations and was expected when running the tools [2, 17]. The bloat data came in different forms, such as data that were loosely correlated with the name, irrelevant or fake profiles, and generally false information. This data would be OK, but it makes it more difficult to profile different targets, especially when using Maltego Community Edition, where each transform, which is how we gather data, is rate limited to 12 results per transform. On average, two outcomes were irrelevant or wrong per subject, either linked to a similar profile or completely unrelated.

5.6.3 Lackluster SpiderFoot performance

SpiderFoot was one of the more anticipated tools to use in the experiment as it is one of the more well-known OSINT automation tools and is free to use. The official latest release, which was initially used, did not work as it got an error when doing the scan. This issue has been resolved, and downloading the latest main branch works without ending with an error. Furthermore, in practice, the tools struggled with gathering data when doing real-name techniques, which was the main focus of the experiment. When the tool worked, it could only find one or two social media, often only a LinkedIn- and Instagram profile. SpiderFoot,

[1] `https://www.reddit.com/r/reddit/comments/12qwagm/an_update_regarding_reddits_api/`

compared to Maltego and Sherlock, was highly reliant on API access, which can be tricky when there are 10-20 different APIs. Each API has unique requirements compared to the others, such as a subscription or equivalent paid tiered services for API access. Nevertheless, the username performance was on par with Recon-NG and Sherlock and likely used similar techniques to find relevant usernames.

The sample size may be too small as well. It has the potential to work better on other people. Many OSINT tools are also created to cater to specific parts of the world. SpiderFoot could work differently based on which part of the world the target is from, such as the US or Britain. SpiderFoot also has a paid version, SpiderFoot HX, that provides some premium features for its subscribers. It is advertised to come pre-installed and configured, which would take a lot of the headache of setting it up, and would also mean the tool would be set up correctly from the get-go.

Chapter 6

Discussion

6.1 Discussing the research questions

RQ1: How vulnerable are we as individuals due to potentially too much openness?

Openness applies to many aspects of OSINT, including government transparency, willingness to share information, accessibility of data, and specific types of information. Openness contributes a lot to society, and in the context of OSINT, openness is why there is OSINT. Some things should be openly accessible such as news articles and research papers, but there are limits. There are positives and negatives, and this thesis looks more at how openness can potentially harm an individual using OSINT tools to exploit openness.

This question does not have a definitive yes or no answer and is more for the individual to determine their perception of it.

RQ2: How are OSINT tools problematic for individuals?

The research done in this thesis points toward that OSINT tools may be problematic for individuals that are a person of interest to someone. OSINT tools utilize search engines and other data sources to collect as much data as possible about a person, making them susceptible to profiling. Furthermore, accurate profiling may lead to more harm, such as spear phishing, cyberstalking, and even account hacking. There is the case to be made that this is not a problem for most people, as a spear phishing attack using OSINT has to be targeted toward them, meaning a threat actor needs to have the motivation and intention to spear phish them. According to the research done by Halevi *et al.* [29], spear phishing is an effective method of phishing people, and this could also be done using OSINT; instead of impersonating a company, one can instead impersonate a friend, family member, or similar. What the OSINT tools do in this case is make the data gathering a lot easier and organize the data for the investigator, removing some of the potential bloat data. However, seeing the actual effect of making a spear phishing attempt like this has not been tested as it was not a part of the defined methodology and could be part of future work where this type of phishing is tested against a group of people.

RQ3: How to reduce vulnerability to OSINT?

Reducing vulnerability to OSINT is more of being aware of OSINT and taking the necessary steps to remove that content from the internet. The proposed countermeasure, the "Right to be forgotten," is a way for EU citizens to demand that some personal information be deleted from the service hosting the information, hence removing it from the internet. OSINT tools rely on the data being accessible. Making it inaccessible means the tools will no longer work on that information. Deleting the data is easier said than done, as removing "all" data from oneself could be a timely endeavor and may as well be almost impossible, especially as using the internet creates more footprints.

Other than removing the information that is accessible cyber security awareness and risk perception should affect OSINT. Being aware that, even if the person contacts a friend or family, someone may be impersonating them is critical to reducing one's vulnerability to OSINT. Seeing how this knowledge changes how one is vulnerable to OSINT-based phishing attempts is challenging but could be tested in some form of future work as well.

6.2 Discussing the results

The results do not fully represent what OSINT is and how it can be used. It looks into one specific part of OSINT: people searching, which was the thesis scope. When looking back, assessing other tools that use different techniques, such as IP addresses, locations, email, and domain names, to understand better how OSINT could be used and then use that information to answer the research questions. The risk scenarios were created using some real-world examples, specifically the more recent impersonation phishing attempts that have been affecting Norway; these cases have been covered by a lot of Norwegian publications such as NRK [40], and Tek.no [41].

6.2.1 Other OSINT tools?

The tools used only show parts of the research done. Some other tools were also tested to experiment with how different tools gather data. However, many tools collect data similarly, and the differences are marginal. SpiderFoot also covers various tools, as they are implemented modules or can be used with an API key. There is also the issue with the tools being able to only work on a specific group of people based on their location, and there are many OSINT tools specifically for American citizens.

6.3 Criticisms of the applied method

The applied method, specifically for the experiment, of answering the research questions may not have been suited as well as it may have seemed before starting the data collection. A literature survey was required to answer the research questions as it is needed to understand the state-of-the-art of OSINT and the tools used. It is an ever-expanding field that constantly changes, such as how openness and open source are perceived in Norway and worldwide. Furthermore, a literature survey was needed; however, the problem came with the conducted experiment. The reasoning for criticizing the applied methods may be that the experiment's results were not groundbreaking; the results were bland, at least in the grander scheme. The thesis might have had better results if some parts of the methods were changed or expanded upon, such as including interviews or surveys regarding people's perception of OSINT and openness to understand better how people perceive it. The tools run during the experiment did not work to the extent they advertised, only being able to find some basic information and social media profiles. Some more extensive tools that should cover more areas are either created to profile a specific country's people, which was the case with Pipl, which only covers Americans, or needs too significant of a price tag just for their license to use it, which was the case with Maltego Pro versions which cost 999 EUR for one year of the license. The issue can be made to ask for permission from Maltego to get a trial license for research purposes, but this was realized too late and needed to be accounted for way earlier in the data-collection process. Furthermore, some of the more exciting tools, which use Twitter, have been shut down or changed due to the changes in Twitter's API access. See Chapter 5.6.1. This change happened during the data collection and the support for the Twitter free API shutdown in March. There is a free-to-use alternative to Twitter's front-end named *Nitter*[1]. However, this did not change the impact of the API access changes. Furthermore, the number of different APIs was underestimated. Hundreds of various OSINT tools use some form of API; some are free, but most are paid. Those who were not often used a search engine API, such as Google's programmable search engine, which still is free, and some others used Bing's API, which is paid. There could have been a justification for paying and using Bing's API, as widely used by different OSINT tools. Again, if this were realized earlier in the data collection process how limiting this would be, another approach would have been chosen to suit this thesis and the research questions better.

[1] https://nitter.net/about

Chapter 7

Conclusion

OSINT is the collection, processing, and correlation of publicly available information. The amount of data from open sources is staggering, and being able to process this data can be used in investigations and threat scenarios. The research done in this thesis aimed to assess and understand how OSINT can be used against individuals, looking into how real names and usernames can be used with OSINT tools to profile individuals. To explore this, a literature review and an experiment were conducted to assess some popular existing tools and understand how OSINT could be used in threat scenarios.

This thesis finds that OSINT can be used in profiling individuals and spear phishing scenarios. A fair amount of information about an individual can be collected by only using their name, information such as addresses, phone numbers, relations, place of work, pictures, locations, social media profiles, other service profiles, and users. The amount of data collected is a double-edged sword, as processing a lot of information and filtering what is irrelevant or wrong could be difficult and time-consuming. Nevertheless, if done correctly, one can do a general profiling of a PoI.

The method chosen for this thesis may not have been perfect, as many questions are left unanswered. It could be interesting seeing more of an approach seeing how the general Norwegian citizens view OSINT and how their lack or not-lack of knowledge affects how OSINT can be used against them.

7.1 Future work

OSINT is a broad field containing a lot of different methodological approaches and scopes that were not covered in this thesis. Specifically, this thesis focused on OSINT tools using real name and username techniques and not on other techniques such as IP addresses, emails, location/GPS locations, pictures, and domain names. Each technique has its own approaches and set of relevant tools and could provide more insight into how these techniques work on individuals.

This thesis also focuses on which degree of effect OSINT has on individuals, meaning there is room for approaches that target nations, governments, organizations, or groups of people.

Other approaches could also focus on individuals, specifically in Norway, perceptions and understandings of OSINT and digital footprints. Rather than experimenting, an interesting approach would be a survey, or interview for that matter, regarding their perception of OSINT and diving deeper into if people even are aware of what is about them on the internet.

Bibliography

[1] M. Edwards, R. Larson, B. Green, A. Rashid, and A. Baron, “Panning for gold: Automatically analysing online social engineering attack surfaces,” *computers & security*, vol. 69, pp. 18–34, 2017.

[2] J. Pastor-Galindo, P. Nespoli, F. G. Mármol, and G. M. Pérez, “The not yet exploited goldmine of osint: Opportunities, open challenges and future trends,” *IEEE Access*, vol. 8, pp. 10 282–10 304, 2020.

[3] Statista, “Number of internet and social media users worldwide as of july 2022,” Jul. 2022. [Online]. Available: `https://www.statista.com/statistics/617136/digital-population-worldwide/` (visited on 11/02/2022).

[4] Wikipedia contributors, *Open-source intelligence — Wikipedia, the free encyclopedia*, [Online; accessed 8-December-2022], 2022. [Online]. Available: `https://en.wikipedia.org/w/index.php?title=Open-source_intelligence&oldid=1124226163`.

[5] *National defense authorization act for fiscal year 2006*, 2006. [Online]. Available: `https://www.govinfo.gov/content/pkg/PLAW-109publ163/html/PLAW-109publ163.htm`.

[6] F. Tabatabaei and D. Wells, “Osint in the context of cyber-security,” *Open source intelligence investigation*, pp. 213–231, 2016.

[7] Y.-W. Hwang, I.-Y. Lee, H. Kim, H. Lee, and D. Kim, “Current status and security trend of osint,” *Wireless Communications and Mobile Computing*, vol. 2022, 2022.

[8] *Hva er en personopplysning?* 2019. [Online]. Available: `https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/` (visited on 02/10/2023).

[9] *Lov om behandling av personopplysninger (personopplysningsloven)*, 2016. [Online]. Available: `https://lovdata.no/dokument/NL/lov/2018-06-15-38` (visited on 02/10/2023).

[10] *Open-source intelligence*, 2022. [Online]. Available: `https://data.europa.eu/en/publications/datastories/open-source-intelligence` (visited on 02/14/2023).

[11] T. Hunt. “Who, what & why - the background on the who, the what and the why of have i been pwned.” (), [Online]. Available: https://haveibeenpwned.com/About.

[12] “Semantic analysis, explained,” 2020. [Online]. Available: https://monkeylearn.com/blog/semantic-analysis/ (visited on 04/09/2023).

[13] “Topp 100 domener i norge.” (2022), [Online]. Available: https://www.iprospect.com/en/no/news-and-insights/news/liste/.

[14] “About us - maltego.” (), [Online]. Available: https://www.maltego.com/about-us/.

[15] Wikipedia contributors, *Maltego — Wikipedia, the free encyclopedia*, [Online; accessed 25-April-2023], 2022. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Maltego&oldid=1123556033.

[16] K. Schwarz and R. Creutzburg, “Design of professional laboratory exercises for effective state-of-the-art osint investigation tools-part 3: Maltego,” *Electronic Imaging*, vol. 2021, no. 3, pp. 45–1, 2021.

[17] T. Dokman and T. Ivanjko, “Open source intelligence (osint) issues and trends,” *The Future of Information Sciences*, vol. 1, no. 2020, p. 191, 2020.

[18] T. Riebe, T. Biselli, M.-A. Kaufhold, and C. Reuter, “Privacy concerns and acceptance factors of osint for cybersecurity: A representative survey,” *Proceedings on Privacy Enhancing Technologies*, vol. 1, pp. 477–493, 2023.

[19] A. Yadav, A. Kumar, and V. Singh, “Open-source intelligence: A comprehensive review of the current state, applications and future perspectives in cyber security,” *Artificial Intelligence Review*, pp. 1–32, 2023.

[20] R. Steele and H. Bloom, *The Open-Source Everything Manifesto: Transparency, Truth, and Trust* (Manifesto Series). North Atlantic Books, 2012, ISBN: 9781583944578. [Online]. Available: https://books.google.no/books?id=XbGVEHFh35IC.

[21] L. Ball, G. Ewan, and N. Coull, “Undermining: Social engineering using open source intelligence gathering,” in *4th International Conference on Knowledge Discovery and Information Retrieval*, Scitepress Digital Library, 2012, pp. 275–280.

[22] A. Yeboah-Ofori and A. Brimicombe, “Cyber intelligence and osint: Developing mitigation techniques against cybercrime threats on social media,” *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, vol. 7, no. 1, pp. 87–98, 2018.

[23] G. Hribar, I. Podbregar, and T. Ivanuša, “Osint: A “grey zone”?” *International Journal of Intelligence and Counter Intelligence*, vol. 27, no. 3, pp. 529–549, 2014.

[24] D. Quick and K.-K. R. Choo, “Digital forensic intelligence: Data subsets and open source intelligence (dfint+ osint): A timely and cohesive mix,” *Future Generation Computer Systems*, vol. 78, pp. 558–567, 2018.

[25] T. Busch, *Akademisk skriving for bachelor- og masterstudenter*, 2nd ed. 5068 Bergen: Fagbokforlaget, 2021, ISBN: 978-82-450-3722-7.

[26] T. Hunt, "The 773 million record "collection #1" data breach," 2019. [Online]. Available: `https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/`.

[27] Wikipedia contributors, *Collection no. 1 — Wikipedia, the free encyclopedia*, [Online; accessed 20-May-2023], 2023. [Online]. Available: `https://en.wikipedia.org/w/index.php?title=Collection_No._1&oldid=1144942191`.

[28] Wikipedia contributors, *Credential stuffing — Wikipedia, the free encyclopedia*, [Online; accessed 9-May-2023], 2023. [Online]. Available: `https://en.wikipedia.org/w/index.php?title=Credential_stuffing&oldid=1138246797`.

[29] T. Halevi, N. Memon, and O. Nov, "Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks," *Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks (January 2, 2015)*, 2015.

[30] D. J. Auby, "Ny facebook-svindel rammer mange norske brukere," 2021. [Online]. Available: `https://www.tek.no/nyheter/nyhet/i/pWdQXR/ny-facebook-svindel-rammer-mange-norske-brukere`.

[31] G. Stavrum, "Facebook-svindelen tapper brukere for tusenvis av kroner uten å bli stoppet," Jan. 2022. [Online]. Available: `https://www.nettavisen.no/norsk-debatt/facebook-svindelen-tapper-brukere-for-tusenvis-av-kroner-uten-a-bli-stoppet/o/5-95-376554`.

[32] *Human development index (hdi)*, 2023. [Online]. Available: `https://hdr.undp.org/data-center/human-development-index#/indicies/HDI`.

[33] A. Thurston, "Openness and information integrity in norway," 2013. [Online]. Available: `https://www.opengovpartnership.org/stories/openness-and-information-integrity-in-norway/`.

[34] M. Shaikh and E. Vaast, "Folding and unfolding: Balancing openness and transparency in open source communities," *Information Systems Research*, vol. 27, no. 4, pp. 813–833, 2016.

[35] H. Solberg, "Derfor publiserer nrk skattelistene," 2018. [Online]. Available: `https://www.nrk.no/norge/derfor-publiserer-nrk-skattelistene-1.14281716`.

[36] B. Wolford, "Everything you need to know about the "right to be forgotten"," 2014. [Online]. Available: `https://gdpr.eu/right-to-be-forgotten/`.

[37] General Data Protection Regulation (GDPR), *Art. 17 gdpr right to erasure ('right to be forgotten')*,
`https://gdpr.eu/article-17-right-to-be-forgotten/`, 2014.

[38] "Https://ks.1881.no/sporsmal-og-svar/artikkel/ka-01104/nb-no." (), [Online]. Available: https://ks.1881.no/sporsmal-og-svar/artikkel/KA-01104/nb-no.

[39] J. Weatherbed, "Twitter replaces its free api with a paid tier in quest to make more money," Feb. 2023. [Online]. Available: https://www.theverge.com/2023/2/2/23582615/twitter-removing-free-api-developer-apps-price-announcement.

[40] M. A. K. Marius Eriksen Guttormsen, "Ingrid ble brukt i pornosvindel på falsk instagram-profil," Mar. 2023. [Online]. Available: https://www.nrk.no/nordland/kvinner-far-bilder-misbrukt-i-falske-profiler-pa-instagram-som-lenker-til-porno-1.16330694.

[41] S. B. Buset, "Svindlere utga seg for å være jasmin (23) på instagram – nå advarer politiet," Mar. 2023. [Online]. Available: https://www.tek.no/nyheter/nyhet/i/wAR94M/svindlere-utga-seg-for-aa-vaere-jasmin-23-paa-instagram-naa-advarer-politiet.

Appendix A

Appendix

A.1 Task description

Analyzing and Reducing Vulnerability to OSINT

OSINT (Open Source Intelligence) is the method and the product of collecting information about a target by using open and publicly accessible sources. OSINT is typically used by threat actors to identify targets, to find out how targets can be attacked, and to be used as part of an attack. It is therefore obvious that organizations and individuals are interested in limiting or reducing the amount of information that OSINT can produce about oneself.

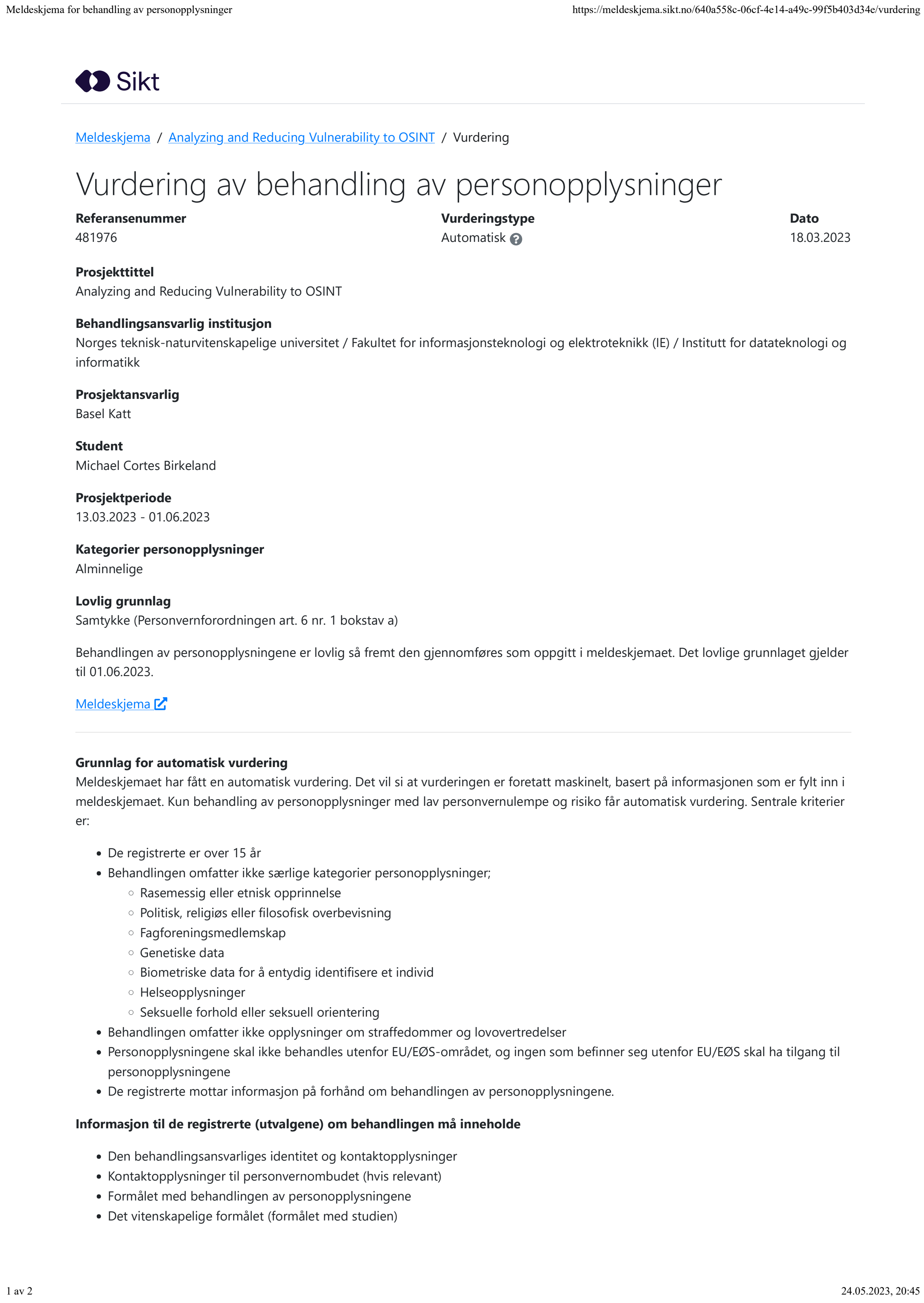
This project focuses on analyzing the potential for OSINT against specific targets, and on assessing how this could be used as part of threat scenarios. The project can also focus on how individuals and organizations can reduce the potential of OSINT against themselves, to mitigate threat scenarios and reduce vulnerabilities.

Aspects to consider include:

- Assess free tools and resources for OSINT.
- Open society and openness are good things, making a lot of things easier. But how vulnerable are we as individuals and nations due to potentially too much openness?

This project is in collaboration with KPMG.

A.2 SIKT confirmation



Meldeskjema for behandling av personopplysninger https://meldeskjema.sikt.no/640a558c-06cf-4e14-a49c-99f5b403d34e/vurdering

Sikt

Meldeskjema / Analyzing and Reducing Vulnerability to OSINT / Vurdering

Vurdering av behandling av personopplysninger

Referansenummer	Vurderingstype	Dato
481976	Automatisk ?	18.03.2023

Prosjekttittel
Analyzing and Reducing Vulnerability to OSINT

Behandlingsansvarlig institusjon
Norges teknisk-naturvitenskapelige universitet / Fakultet for informasjonsteknologi og elektroteknikk (IE) / Institutt for datateknologi og informatikk

Prosjektansvarlig
Basel Katt

Student
Michael Cortes Birkeland

Prosjektperiode
13.03.2023 - 01.06.2023

Kategorier personopplysninger
Alminnelige

Lovlig grunnlag
Samtykke (Personvernforordningen art. 6 nr. 1 bokstav a)

Behandlingen av personopplysningene er lovlig så fremt den gjennomføres som oppgitt i meldeskjemaet. Det lovlige grunnlaget gjelder til 01.06.2023.

Meldeskjema

Grunnlag for automatisk vurdering
Meldeskjemaet har fått en automatisk vurdering. Det vil si at vurderingen er foretatt maskinelt, basert på informasjonen som er fylt inn i meldeskjemaet. Kun behandling av personopplysninger med lav personvernulempe og risiko får automatisk vurdering. Sentrale kriterier er:

- De registrerte er over 15 år
- Behandlingen omfatter ikke særlige kategorier personopplysninger;
  - Rasemessig eller etnisk opprinnelse
  - Politisk, religiøs eller filosofisk overbevisning
  - Fagforeningsmedlemskap
  - Genetiske data
  - Biometriske data for å entydig identifisere et individ
  - Helseopplysninger
  - Seksuelle forhold eller seksuell orientering
- Behandlingen omfatter ikke opplysninger om straffedommer og lovovertredelser
- Personopplysningene skal ikke behandles utenfor EU/EØS-området, og ingen som befinner seg utenfor EU/EØS skal ha tilgang til personopplysningene
- De registrerte mottar informasjon på forhånd om behandlingen av personopplysningene.

Informasjon til de registrerte (utvalgene) om behandlingen må inneholde

- Den behandlingsansvarliges identitet og kontaktopplysninger
- Kontaktopplysninger til personvernombudet (hvis relevant)
- Formålet med behandlingen av personopplysningene
- Det vitenskapelige formålet (formålet med studien)

1 av 2 24.05.2023, 20:45

- Det lovlige grunnlaget for behandlingen av personopplysningene
- Hvilke personopplysninger som vil bli behandlet, og hvordan de samles inn, eller hvor de hentes fra
- Hvem som vil få tilgang til personopplysningene (kategorier mottakere)
- Hvor lenge personopplysningene vil bli behandlet
- Retten til å trekke samtykket tilbake og øvrige rettigheter

Vi anbefaler å bruke vår mal til informasjonsskriv.

Informasjonssikkerhet
Du må behandle personopplysningene i tråd med retningslinjene for informasjonssikkerhet og lagringsguider ved behandlingsansvarlig institusjon. Institusjonen er ansvarlig for at vilkårene for personvernforordningen artikkel 5.1. d) riktighet, 5. 1. f) integritet og konfidensialitet, og 32 sikkerhet er oppfylt.

A.3 Experiment installation guides

A.3.1 Parrot Security 5.2 VM

The .iso file of Parrot Security 5.2 can be downloaded from the official Parrot website: `https://www.parrotsec.org/download/`. The version installed for this project is the *Security Edition* of Parrot.

A.3.2 Maltego

Maltego can be downloaded from their official website: `https://www.maltego.com/downloads/`. Maltego also comes pre-downloaded in Parrot Security 5.2. The only requirement to use Maltego is to create a user, which can also be done on their official website: `https://www.maltego.com/ce-registration/`. This is for the free Community Edition of Maltego.

A.3.3 SpiderFoot

SpiderFoot 3.0 (CLI and GUI versions) comes pre-installed on Parrot 5.2. This build is outdated and lacks some functionality compared to the newer SpiderFoot 4.0. SpiderFoot is dependent on Python3.

SpiderFoot 4.0 can be installed and run with the following commands:

```
git clone https://github.com/smicallef/spiderfoot.git
cd spiderfoot
pip3 install -r requirements.txt
python3 ./sf.py -l 127.0.0.1:5001
```

If SpiderFoot 4.0 has been downloaded, you can run it by setting your current directory as the Spiderfoot4.0 folder and running the following command: `python3 ./sf.py -l 127.0.0.1:5001`. This is for the GUI web interface. SpiderFoot can then be used inside of the web browser from `localhost:5001`

A.3.4 Recon-NG

Recon-NG differs from SpiderFoot and Maltego as it is designed to be customized by the investigator, so there are multiple ways of setting up the Recon-NG environment. Recon-NG is downloaded using the following command in the Linux terminal: `sudo apt install recon-ng`. To run the Profiler module one need to install the module, to this run the following commands:

```
# Start Recon-NG
recon-ng
# Install the module
marketplace install profiler
# Load the module
```

```
    modules load profiler
    # Set a SOURCE, which is the target’s username
    options set SOURCE targets_username
    # run the module
    run
    # After the module has been run, one can see the found profiles
    show profiles
```

A.3.5 Sherlock

Installation guide can be found on Sherlocks’s GitHub page[1].

```
# clone the repo
$ git clone https://github.com/sherlock-project/sherlock.git

# change the working directory to sherlock
$ cd sherlock

# install the requirements
$ python3 -m pip install -r requirements.txt
```

The tools can be run using the following command, replace ALIAS with the username of the target: `python3 sherlock ALIAS`

[1] https://github.com/sherlock-project/sherlock

A.4 Experiment screenshots and results from tools

A.4.1 Subject 1

Subject 1: Maltego

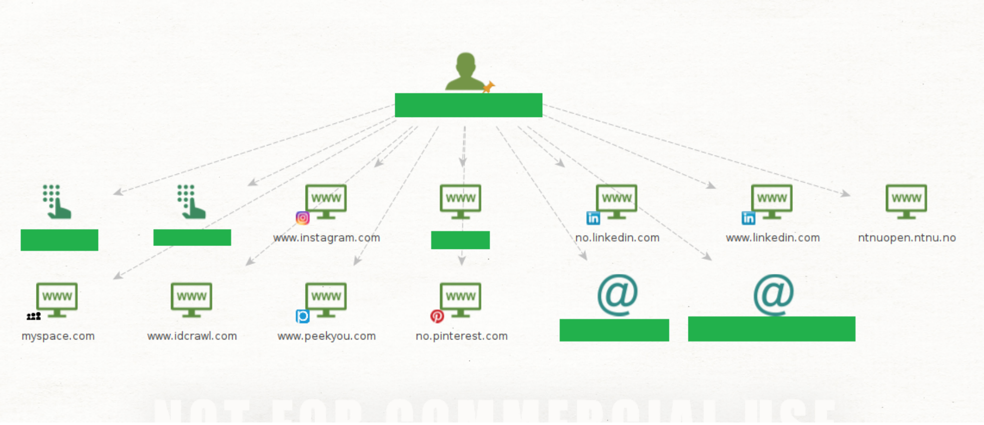


Figure A.1: S1: Maltego full name transform

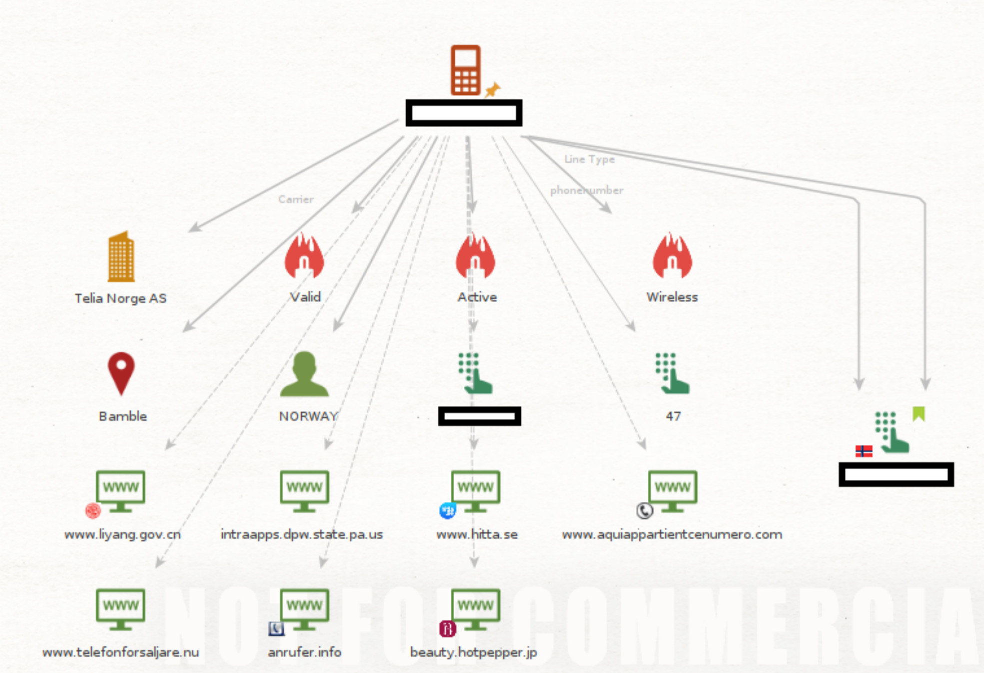


Figure A.2: S1: Maltego phone number transform

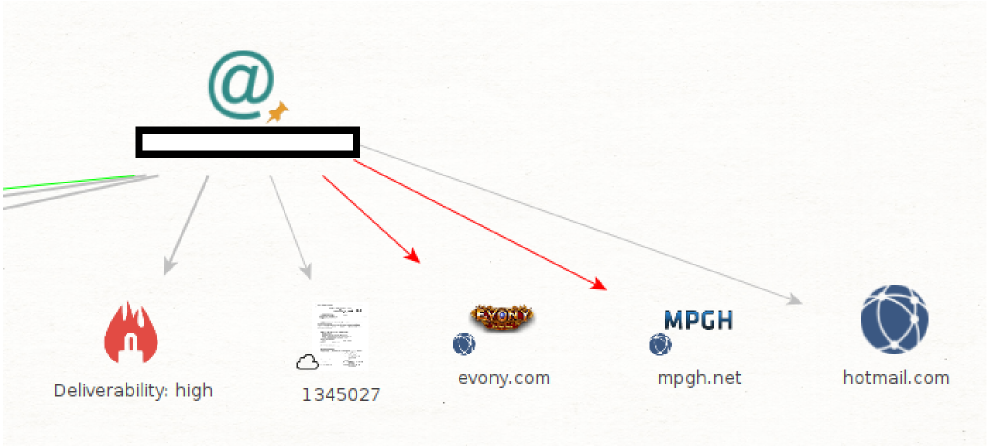


Figure A.3: S1: Maltego email transform

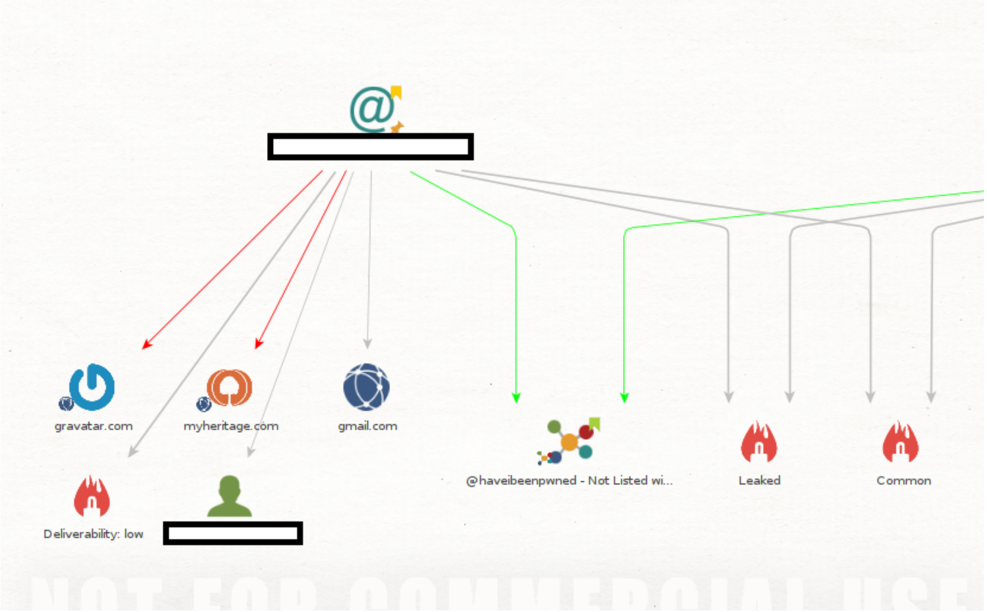
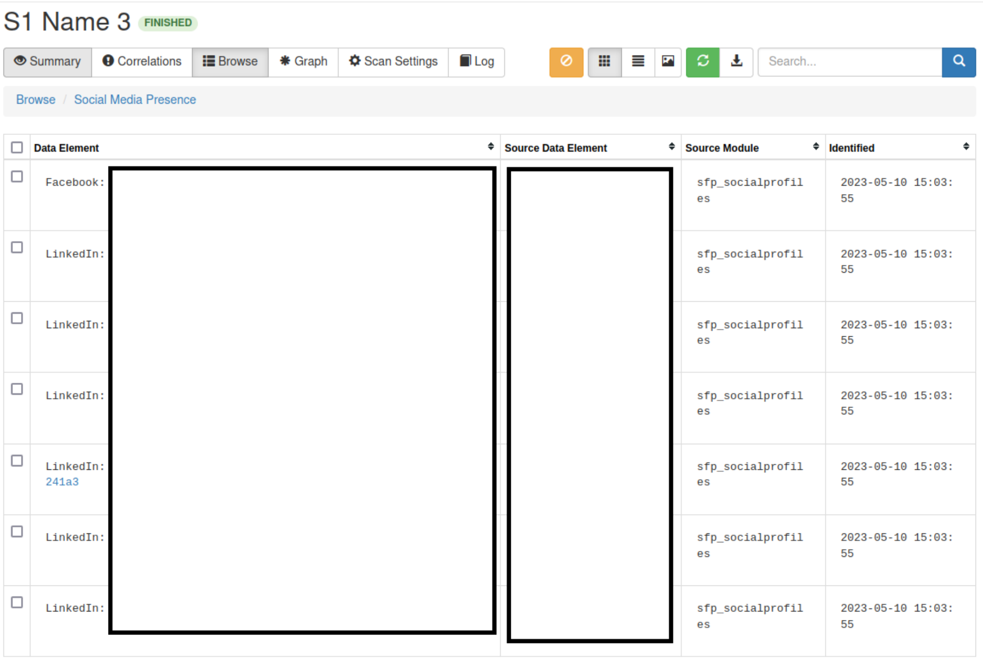


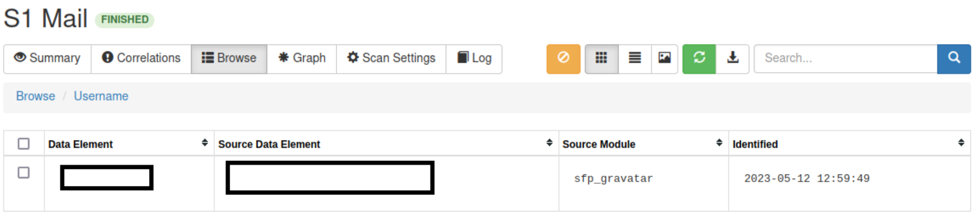
Figure A.4: S1: Maltego another email transform

Subject 1: SpiderFoot



☐	Data Element	Source Data Element	Source Module	Identified
☐	Facebook: [redacted]	[redacted]	sfp_socialprofiles	2023-05-10 15:03:55
☐	LinkedIn: [redacted]	[redacted]	sfp_socialprofiles	2023-05-10 15:03:55
☐	LinkedIn: [redacted]	[redacted]	sfp_socialprofiles	2023-05-10 15:03:55
☐	LinkedIn: [redacted]	[redacted]	sfp_socialprofiles	2023-05-10 15:03:55
☐	LinkedIn: [redacted]	[redacted]	sfp_socialprofiles	2023-05-10 15:03:55
☐	LinkedIn: [redacted]	[redacted]	sfp_socialprofiles	2023-05-10 15:03:55
☐	LinkedIn: [redacted]	[redacted]	sfp_socialprofiles	2023-05-10 15:03:55

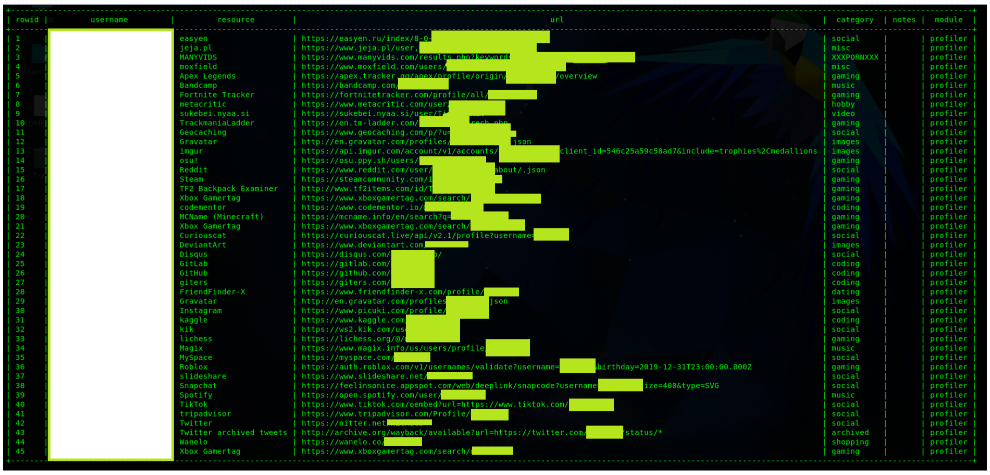
Figure A.5: S1: SpiderFoot Full name scan



☐	Data Element	Source Data Element	Source Module	Identified
☐	[redacted]	[redacted]	sfp_gravatar	2023-05-12 12:59:49

Figure A.6: S1: SpiderFoot found username using email

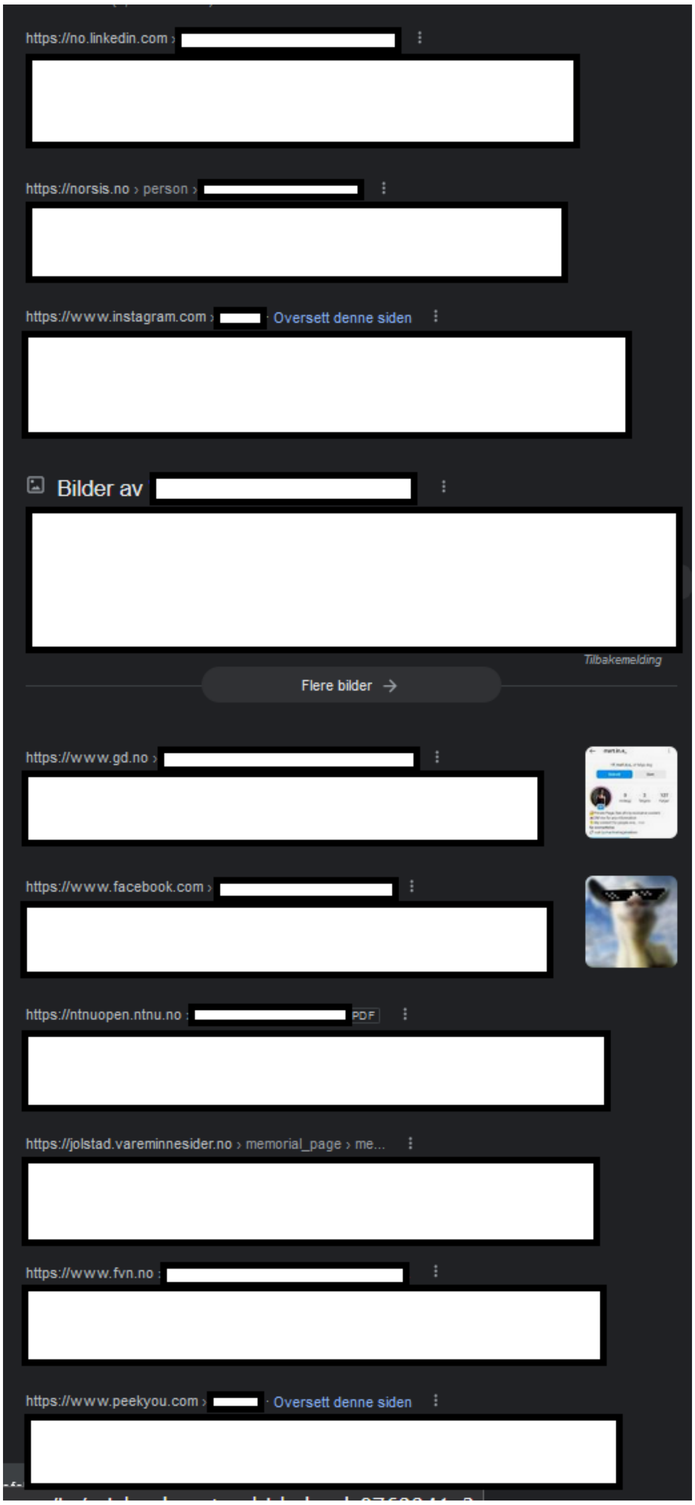
Subject 1: Recon-NG



```
+----------------------------------------------------------------------------------------------------------------------------------------------------------------------------+
| rowid |  username   |        resource          |                                          url                                                      |  category   | notes |  module  |
+----------------------------------------------------------------------------------------------------------------------------------------------------------------------------+
| 1     | [redacted]  | easyen                   | https://easyen.ru/index/8-0-[redacted]                                                                          | social      |       | profiler |
| 2     | [redacted]  | jeja.pl                  | https://www.jeja.pl/user,[redacted]                                                                             | misc        |       | profiler |
| 3     | [redacted]  | MANYVIDS                 | https://www.manyvids.com/results.php?keywords[redacted]                                                         | XXXPORNXXX  |       | profiler |
| 4     | [redacted]  | moxfield                 | https://www.moxfield.com/users/[redacted]                                                                       | misc        |       | profiler |
| 5     | [redacted]  | Apex Legends             | https://apex.tracker.gg/apex/profile/origin/[redacted]/overview                                                 | gaming      |       | profiler |
| 6     | [redacted]  | Bandcamp                 | https://bandcamp.com/[redacted]                                                                                 | music       |       | profiler |
| 7     | [redacted]  | Fortnite Tracker         | https://fortnitetracker.com/profile/all/[redacted]                                                              | gaming      |       | profiler |
| 8     | [redacted]  | metacritic               | https://www.metacritic.com/user/[redacted]                                                                      | hobby       |       | profiler |
| 9     | [redacted]  | sukebei.nyaa.si          | https://sukebei.nyaa.si/user/T[redacted]                                                                        | video       |       | profiler |
| 10    | [redacted]  | TrackmaniaLadder         | https://en.tm-ladder.com/[redacted]rech.php                                                                     | gaming      |       | profiler |
| 11    | [redacted]  | Geocaching               | https://www.geocaching.com/p/?u=[redacted]                                                                      | social      |       | profiler |
| 12    | [redacted]  | Gravatar                 | http://en.gravatar.com/profiles/[redacted]json                                                                  | images      |       | profiler |
| 13    | [redacted]  | imgur                    | https://api.imgur.com/account/v1/accounts/[redacted]client_id=546c25a59c58ad7&include=trophies%2Cmedallions     | images      |       | profiler |
| 14    | [redacted]  | osu!                     | https://osu.ppy.sh/users/[redacted]                                                                             | gaming      |       | profiler |
| 15    | [redacted]  | Reddit                   | https://www.reddit.com/user/[redacted]about/.json                                                               | social      |       | profiler |
| 16    | [redacted]  | Steam                    | https://steamcommunity.com/i[redacted]                                                                          | gaming      |       | profiler |
| 17    | [redacted]  | TF2 Backpack Examiner    | http://www.tf2items.com/id/T[redacted]                                                                          | gaming      |       | profiler |
| 18    | [redacted]  | Xbox Gamertag            | https://www.xboxgamertag.com/search/[redacted]                                                                  | gaming      |       | profiler |
| 19    | [redacted]  | codementor               | https://www.codementor.io/[redacted]                                                                            | coding      |       | profiler |
| 20    | [redacted]  | MCName (Minecraft)       | https://mcname.info/en/search?q=[redacted]                                                                      | gaming      |       | profiler |
| 21    | [redacted]  | Xbox Gamertag            | https://www.xboxgamertag.com/search/[redacted]                                                                  | gaming      |       | profiler |
| 22    | [redacted]  | Curiouscat               | https://curiouscat.live/api/v2.1/profile?username=[redacted]                                                    | social      |       | profiler |
| 23    | [redacted]  | DeviantArt               | https://www.deviantart.com[redacted]                                                                            | images      |       | profiler |
| 24    | [redacted]  | Disqus                   | https://disqus.com/[redacted]p/                                                                                 | social      |       | profiler |
| 25    | [redacted]  | GitLab                   | https://gitlab.com/[redacted]                                                                                   | coding      |       | profiler |
| 26    | [redacted]  | GitHub                   | https://github.com/[redacted]                                                                                   | coding      |       | profiler |
| 27    | [redacted]  | giters                   | https://giters.com/[redacted]                                                                                   | coding      |       | profiler |
| 28    | [redacted]  | FriendFinder-X           | https://www.friendfinder-x.com/profile/[redacted]                                                               | dating      |       | profiler |
| 29    | [redacted]  | Gravatar                 | http://en.gravatar.com/profiles[redacted]json                                                                   | images      |       | profiler |
| 30    | [redacted]  | Instagram                | https://www.picuki.com/profile/[redacted]                                                                       | social      |       | profiler |
| 31    | [redacted]  | kaggle                   | https://www.kaggle.com[redacted]                                                                                | coding      |       | profiler |
| 32    | [redacted]  | kik                      | https://ws2.kik.com/us[redacted]                                                                                | social      |       | profiler |
| 33    | [redacted]  | lichess                  | https://lichess.org/@/[redacted]                                                                                | gaming      |       | profiler |
| 34    | [redacted]  | Magix                    | https://www.magix.info/us/users/profile[redacted]                                                               | music       |       | profiler |
| 35    | [redacted]  | MySpace                  | https://myspace.com/[redacted]                                                                                  | social      |       | profiler |
| 36    | [redacted]  | Roblox                   | https://auth.roblox.com/v1/usernames/validate?username=[redacted]birthday=2019-12-31T23:00:00.000Z              | gaming      |       | profiler |
| 37    | [redacted]  | slideshare               | https://www.slideshare.net/[redacted]                                                                           | social      |       | profiler |
| 38    | [redacted]  | Snapchat                 | https://feelinsonice.appspot.com/web/deeplink/snapcode?username=[redacted]ize=400&type=SVG                      | social      |       | profiler |
| 39    | [redacted]  | Spotify                  | https://open.spotify.com/user/[redacted]                                                                        | music       |       | profiler |
| 40    | [redacted]  | TikTok                   | https://www.tiktok.com/oembed?url=https://www.tiktok.com/[redacted]                                             | social      |       | profiler |
| 41    | [redacted]  | tripadvisor              | https://www.tripadvisor.com/Profile/[redacted]                                                                  | social      |       | profiler |
| 42    | [redacted]  | Twitter                  | https://nitter.net/[redacted]                                                                                   | social      |       | profiler |
| 43    | [redacted]  | Twitter archived tweets  | http://archive.org/wayback/available?url=https://twitter.com/[redacted]/status/*                                | archived    |       | profiler |
| 44    | [redacted]  | Wanelo                   | https://wanelo.co/[redacted]                                                                                    | shopping    |       | profiler |
| 45    | [redacted]  | Xbox Gamertag            | https://www.xboxgamertag.com/search/[redacted]                                                                  | gaming      |       | profiler |
+----------------------------------------------------------------------------------------------------------------------------------------------------------------------------+
```

Figure A.7: Subject 1: Recon-NG profiler

Subject 1: Search engines



https://no.linkedin.com › [redacted] ⋮

[redacted]

https://norsis.no › person › [redacted] ⋮

[redacted]

https://www.instagram.com › [redacted] · Oversett denne siden ⋮

[redacted]

Bilder av [redacted] ⋮

[redacted]

Tilbakemelding

Flere bilder →

https://www.gd.no › [redacted] ⋮

[redacted]

https://www.facebook.com › [redacted] ⋮

[redacted]

https://ntnuopen.ntnu.no › [redacted] PDF ⋮

[redacted]

https://jolstad.vareminnesider.no › memorial_page › me... ⋮

[redacted]

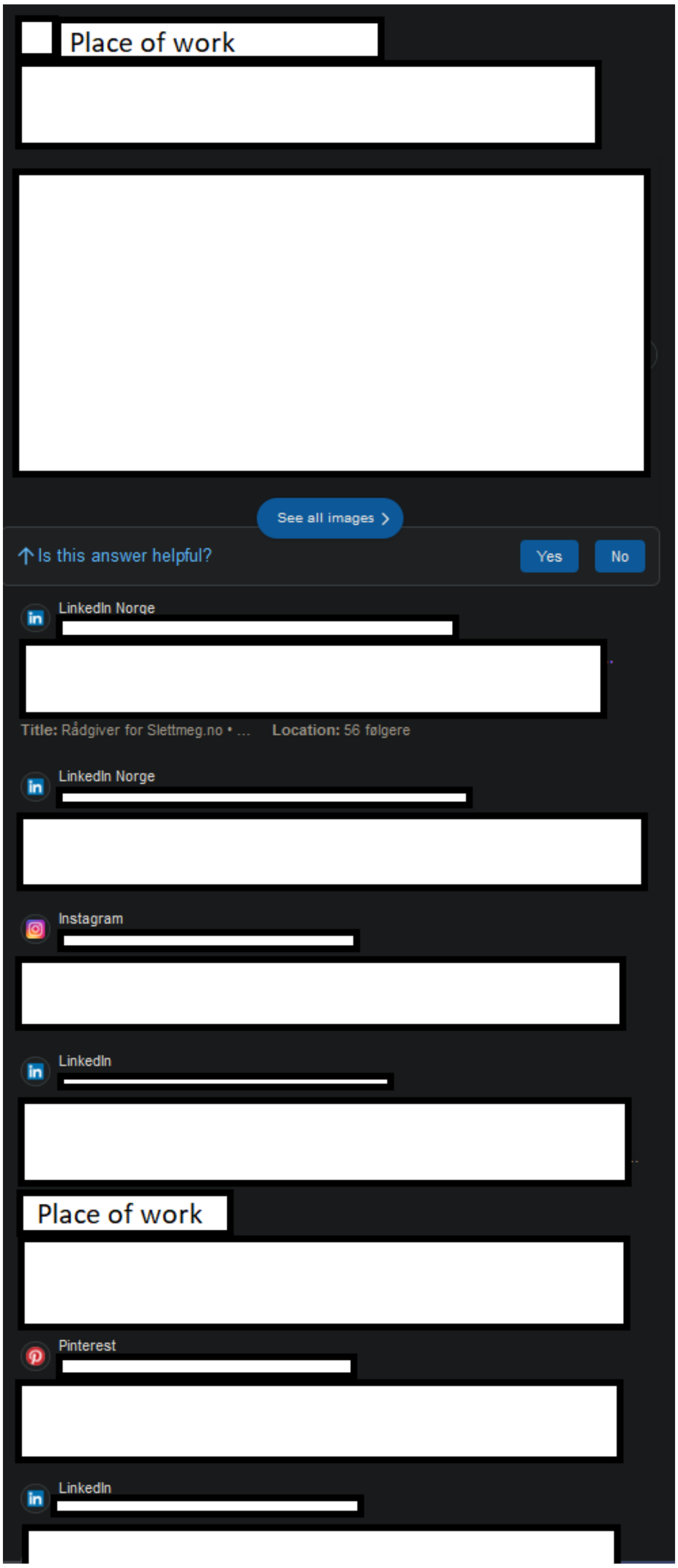
https://www.fvn.no › [redacted] ⋮

[redacted]

https://www.peekyou.com › [redacted] · Oversett denne siden ⋮

[redacted]

Figure A.8: Google search



[redacted] Place of work

[redacted]

[redacted]

LinkedIn Norge

[redacted]

[redacted]

Title: Rådgiver for Slettmeg.no • ... **Location:** 56 følgere

LinkedIn Norge

[redacted]

[redacted]

Instagram

[redacted]

[redacted]

LinkedIn

[redacted]

[redacted]

Place of work

[redacted]

Pinterest

[redacted]

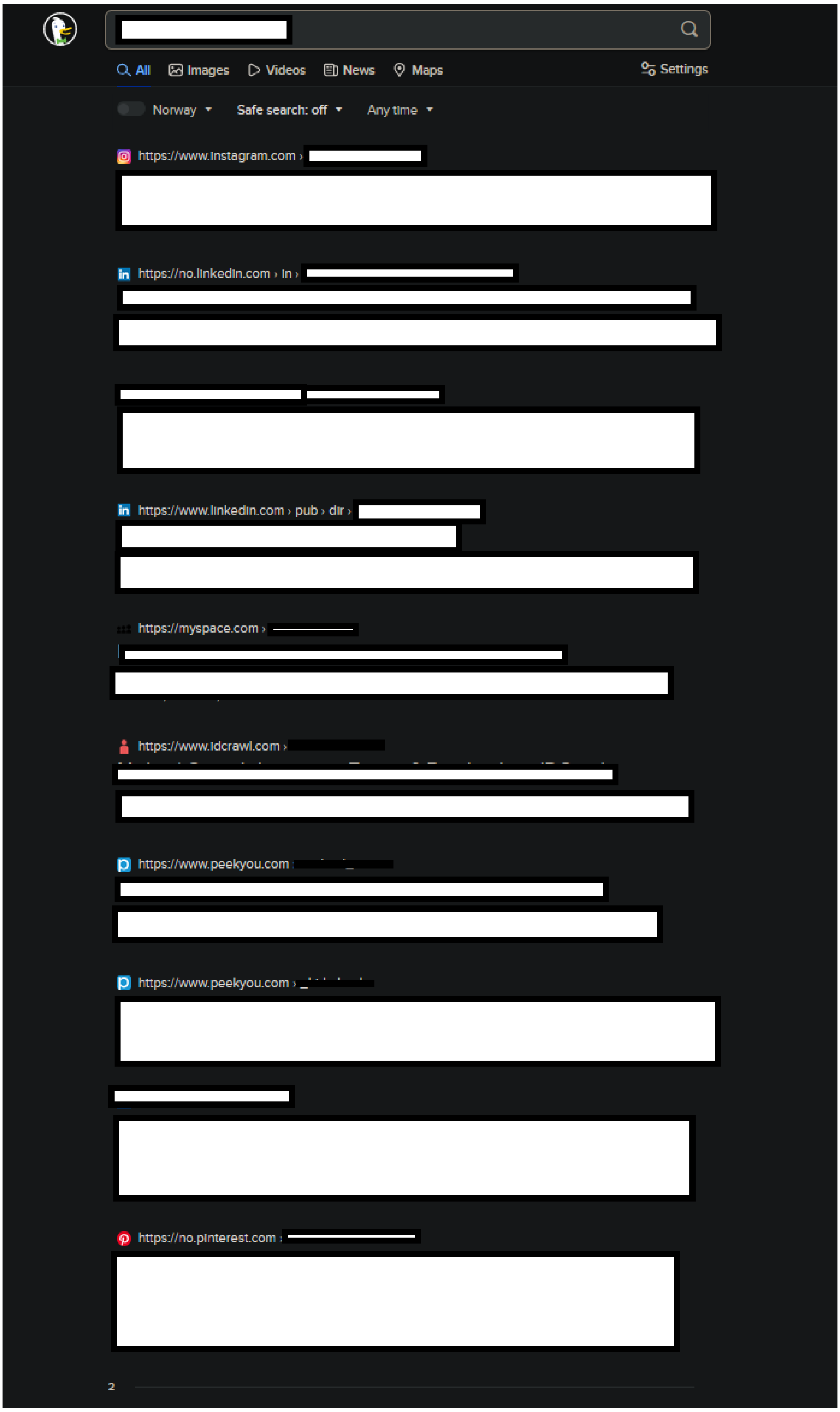
[redacted]

LinkedIn

[redacted]

[redacted]

Figure A.9: Bing search



[redacted]

Norway

Safe search: off

Any time

https://www.instagram.com › [redacted]

[redacted]

https://no.linkedin.com › in › [redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted]

https://www.linkedin.com › pub › dir › [redacted]

[redacted]

[redacted]

https://myspace.com › [redacted]

[redacted]

[redacted]

https://www.idcrawl.com › [redacted]

[redacted]

[redacted]

https://www.peekyou.com [redacted]

[redacted]

[redacted]

https://www.peekyou.com › [redacted]

[redacted]

[redacted]

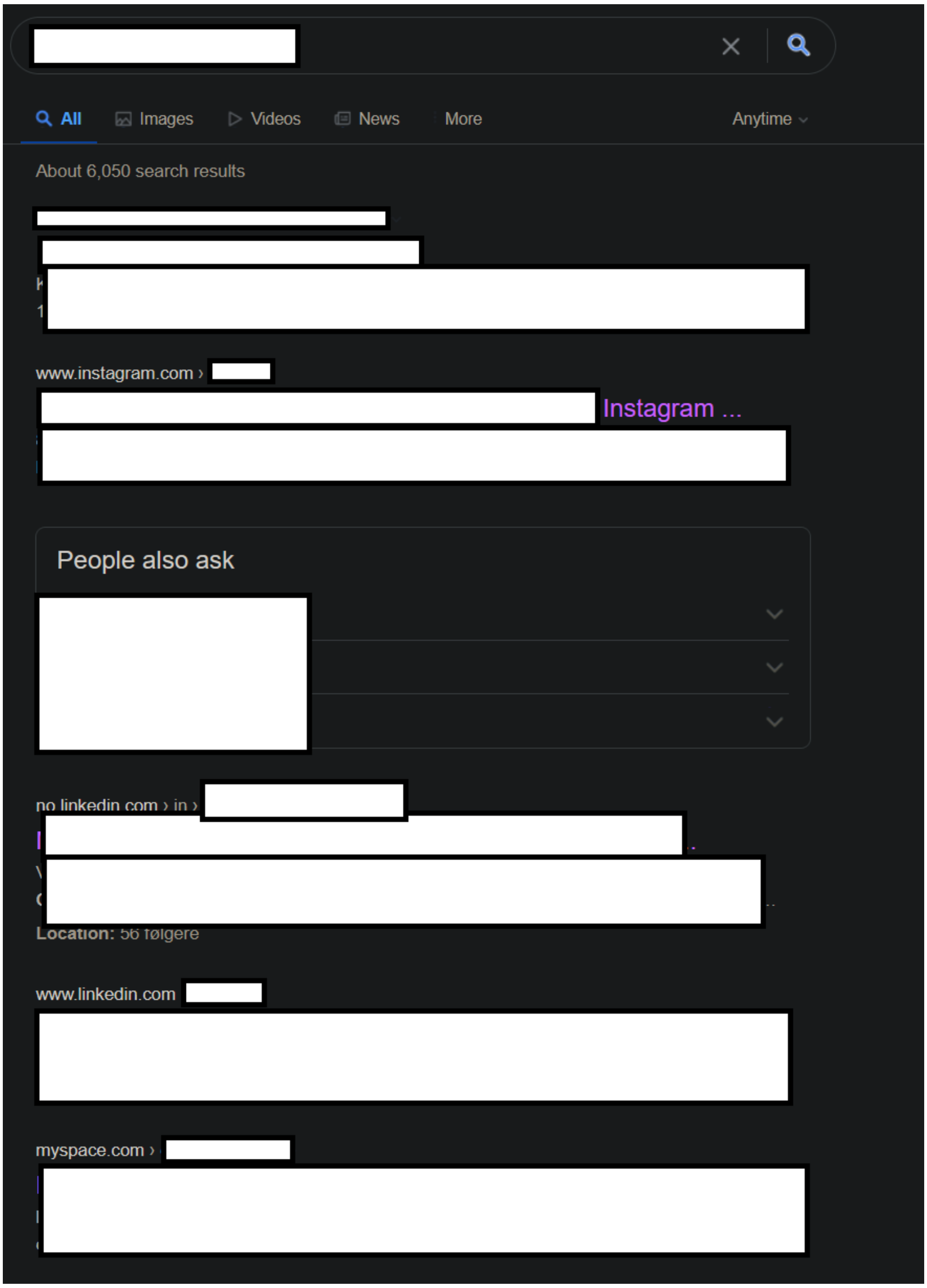
[redacted]

https://no.pinterest.com › [redacted]

[redacted]

2

Figure A.10: DuckDuckGo search



[redacted]

About 6,050 search results

[redacted]

[redacted]

[redacted]

www.instagram.com › [redacted]

[redacted] Instagram ...

[redacted]

People also ask

[redacted]

no.linkedin.com › in › [redacted]

[redacted]

[redacted]

Location: 56 følgere

www.linkedin.com [redacted]

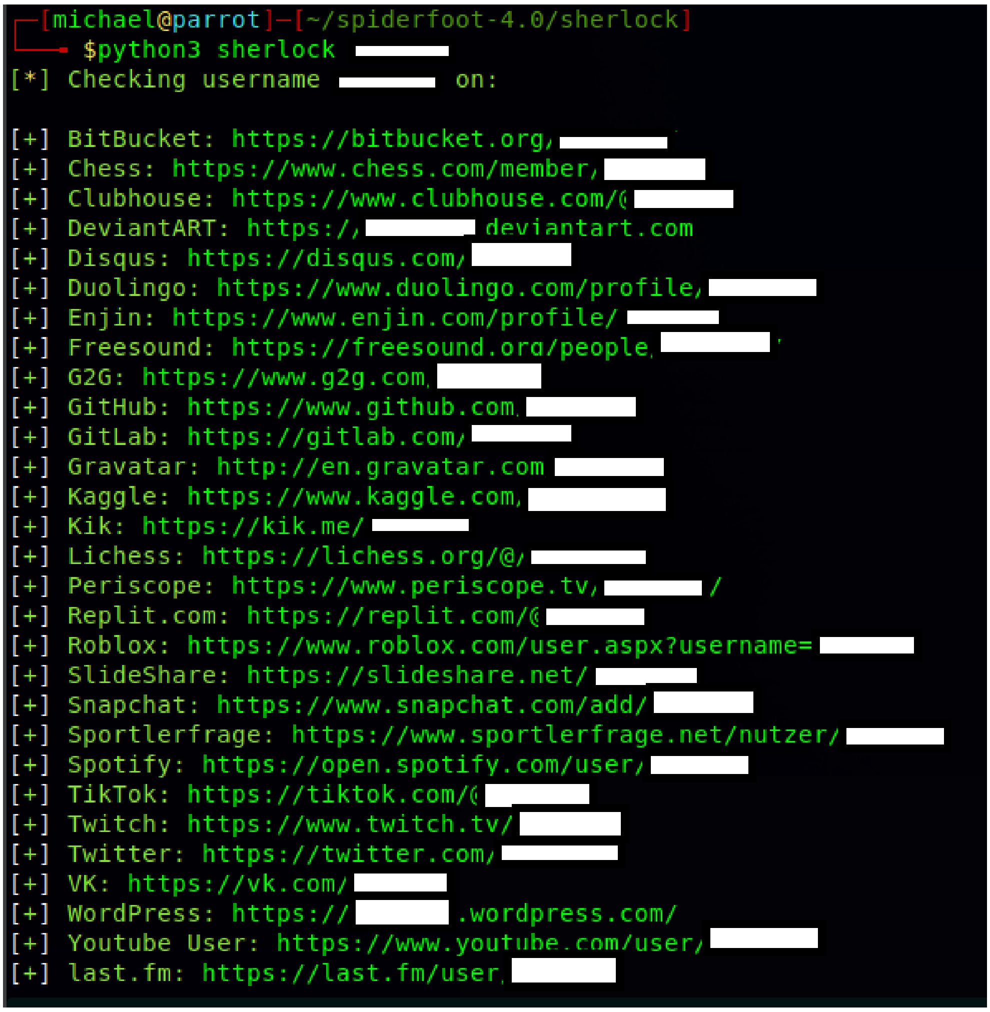
[redacted]

myspace.com › [redacted]

[redacted]

Figure A.11: Yahoo search

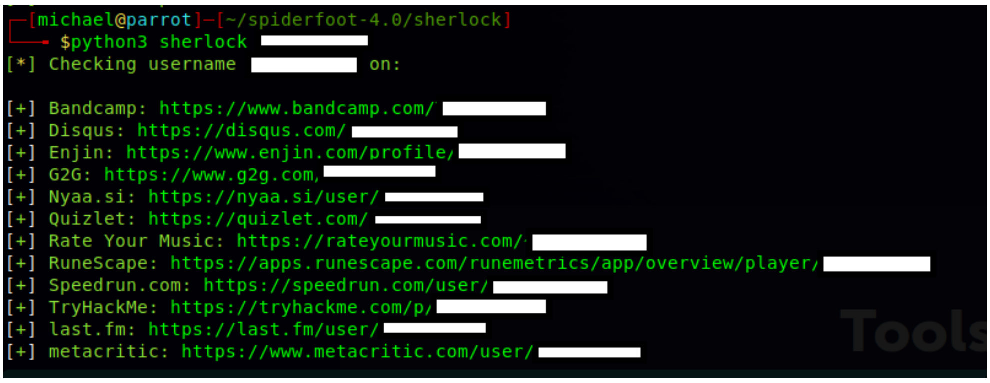
Subject 1: other tools and services



```
┌─[michael@parrot]─[~/spiderfoot-4.0/sherlock]
└──╼ $python3 sherlock [redacted]
[*] Checking username [redacted] on:

[+] BitBucket: https://bitbucket.org/[redacted]
[+] Chess: https://www.chess.com/member/[redacted]
[+] Clubhouse: https://www.clubhouse.com/@[redacted]
[+] DeviantART: https://[redacted].deviantart.com
[+] Disqus: https://disqus.com/[redacted]
[+] Duolingo: https://www.duolingo.com/profile/[redacted]
[+] Enjin: https://www.enjin.com/profile/[redacted]
[+] Freesound: https://freesound.org/people/[redacted]
[+] G2G: https://www.g2g.com/[redacted]
[+] GitHub: https://www.github.com/[redacted]
[+] GitLab: https://gitlab.com/[redacted]
[+] Gravatar: http://en.gravatar.com/[redacted]
[+] Kaggle: https://www.kaggle.com/[redacted]
[+] Kik: https://kik.me/[redacted]
[+] Lichess: https://lichess.org/@/[redacted]
[+] Periscope: https://www.periscope.tv/[redacted]/
[+] Replit.com: https://replit.com/@[redacted]
[+] Roblox: https://www.roblox.com/user.aspx?username=[redacted]
[+] SlideShare: https://slideshare.net/[redacted]
[+] Snapchat: https://www.snapchat.com/add/[redacted]
[+] Sportlerfrage: https://www.sportlerfrage.net/nutzer/[redacted]
[+] Spotify: https://open.spotify.com/user/[redacted]
[+] TikTok: https://tiktok.com/@[redacted]
[+] Twitch: https://www.twitch.tv/[redacted]
[+] Twitter: https://twitter.com/[redacted]
[+] VK: https://vk.com/[redacted]
[+] WordPress: https://[redacted].wordpress.com/
[+] Youtube User: https://www.youtube.com/user/[redacted]
[+] last.fm: https://last.fm/user/[redacted]
```

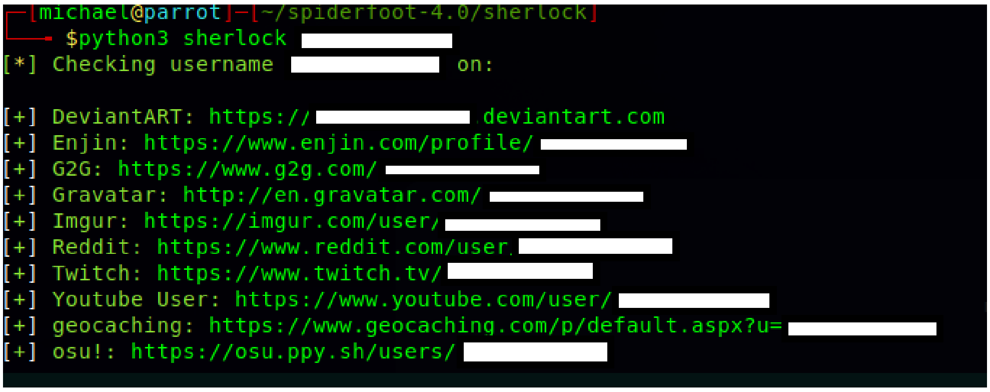
Figure A.12: S1: Sherlock username search



```
┌─[michael@parrot]─[~/spiderfoot-4.0/sherlock]
└──╼ $python3 sherlock [redacted]
[*] Checking username [redacted] on:

[+] Bandcamp: https://www.bandcamp.com/[redacted]
[+] Disqus: https://disqus.com/[redacted]
[+] Enjin: https://www.enjin.com/profile/[redacted]
[+] G2G: https://www.g2g.com/[redacted]
[+] Nyaa.si: https://nyaa.si/user/[redacted]
[+] Quizlet: https://quizlet.com/[redacted]
[+] Rate Your Music: https://rateyourmusic.com/~[redacted]
[+] RuneScape: https://apps.runescape.com/runemetrics/app/overview/player/[redacted]
[+] Speedrun.com: https://speedrun.com/user/[redacted]
[+] TryHackMe: https://tryhackme.com/p/[redacted]
[+] last.fm: https://last.fm/user/[redacted]
[+] metacritic: https://www.metacritic.com/user/[redacted]
```

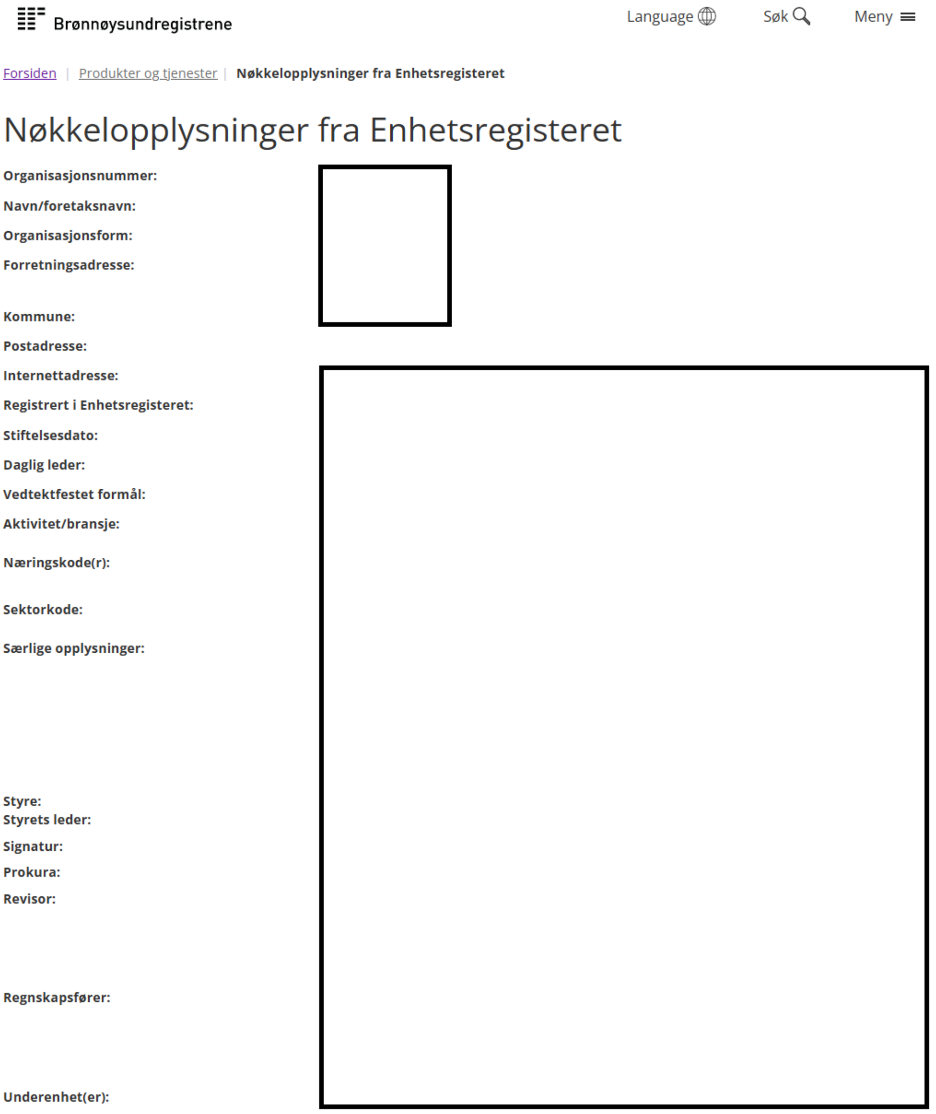
Figure A.13: S1: Sherlock username search



```
┌─[michael@parrot]─[~/spiderfoot-4.0/sherlock]
└──╼ $python3 sherlock [redacted]
[*] Checking username [redacted] on:

[+] DeviantART: https://[redacted].deviantart.com
[+] Enjin: https://www.enjin.com/profile/[redacted]
[+] G2G: https://www.g2g.com/[redacted]
[+] Gravatar: http://en.gravatar.com/[redacted]
[+] Imgur: https://imgur.com/user/[redacted]
[+] Reddit: https://www.reddit.com/user/[redacted]
[+] Twitch: https://www.twitch.tv/[redacted]
[+] Youtube User: https://www.youtube.com/user/[redacted]
[+] geocaching: https://www.geocaching.com/p/default.aspx?u=[redacted]
[+] osu!: https://osu.ppy.sh/users/[redacted]
```

Figure A.14: S1: Sherlock username search



Brønnøysundregistrene

Language Søk Meny

Forsiden | Produkter og tjenester | Nøkkelopplysninger fra Enhetsregisteret

Nøkkelopplysninger fra Enhetsregisteret

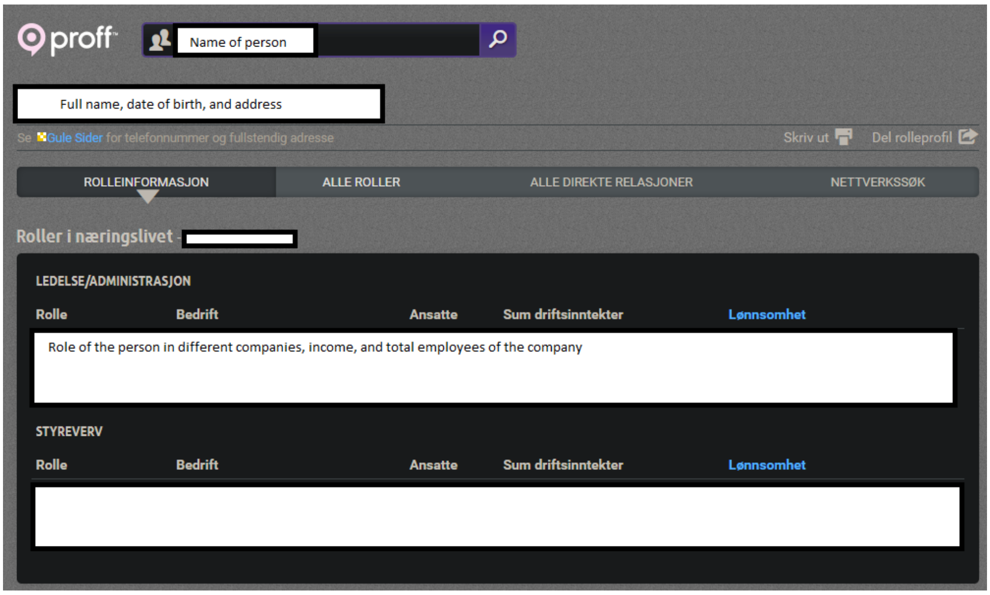
Organisasjonsnummer:
Navn/foretaksnavn:
Organisasjonsform:
Forretningsadresse:

[redacted]

Kommune:
Postadresse:
Internettadresse:
Registrert i Enhetsregisteret:
Stiftelsesdato:
Daglig leder:
Vedtektfestet formål:
Aktivitet/bransje:
Næringskode(r):
Sektorkode:
Særlige opplysninger:
Styre:
Styrets leder:
Signatur:
Prokura:
Revisor:
Regnskapsfører:
Underenhet(er):

[redacted]

Figure A.15: Example of Brønnøysundregistrene listing



proff

Name of person

Full name, date of birth, and address

Se Gule Sider for telefonnummer og fullstendig adresse

Roller i næringslivet - [redacted]

LEDELSE/ADMINISTRASJON

Rolle	Bedrift	Ansatte	Sum driftsinntekter	Lønnsomhet
Role of the person in different companies, income, and total employees of the company				

STYREVERV

Rolle	Bedrift	Ansatte	Sum driftsinntekter	Lønnsomhet
[redacted]				

Figure A.16: Example of Proff.no listing

A.4.2 Subject 2

Subject 2: Maltego

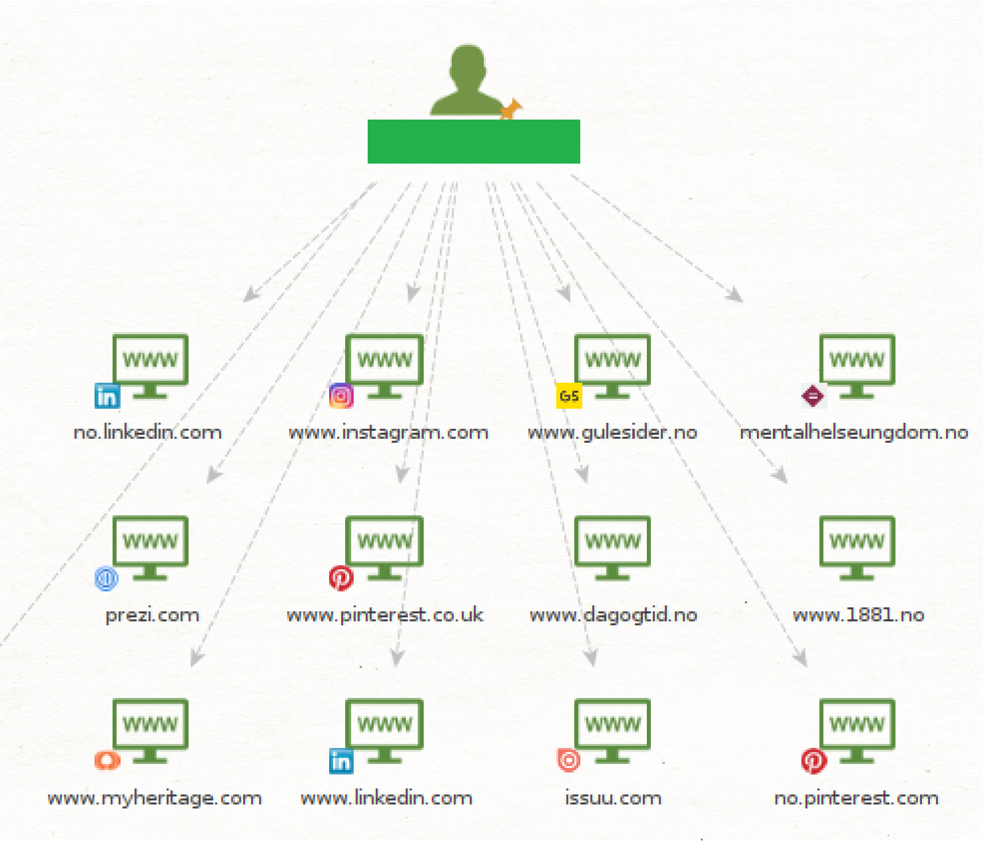


Figure A.17: Subject 2: Maltego all transform, full name

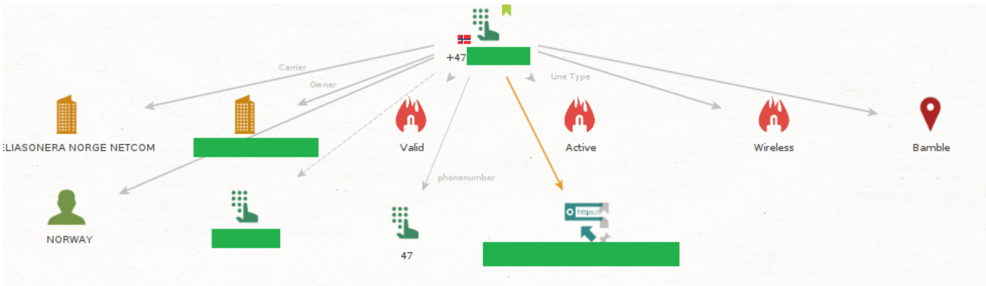
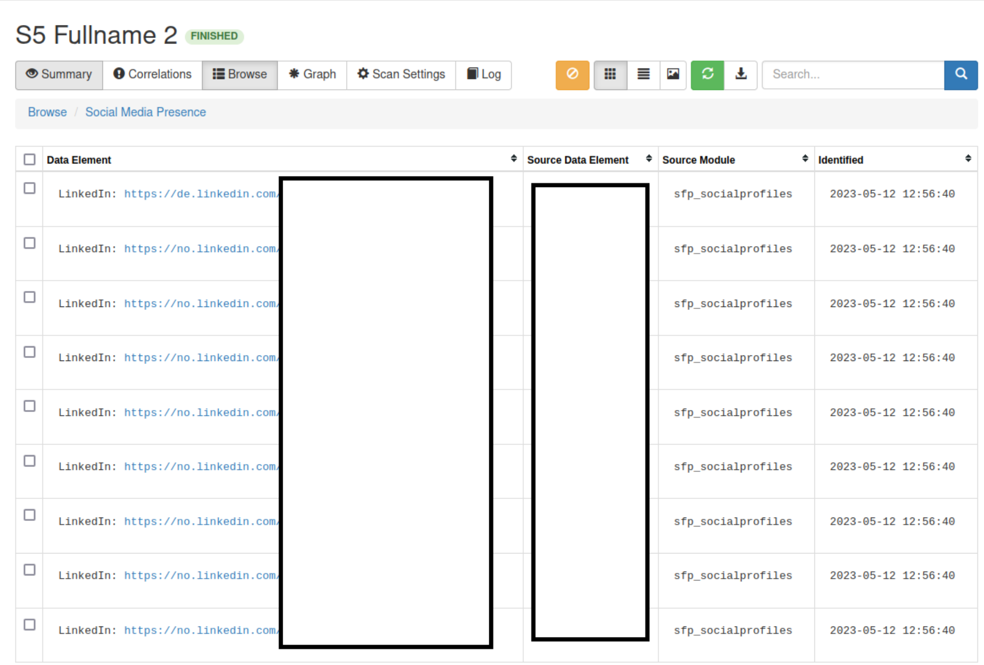


Figure A.18: Subject 2: Maltego all transform, phone number

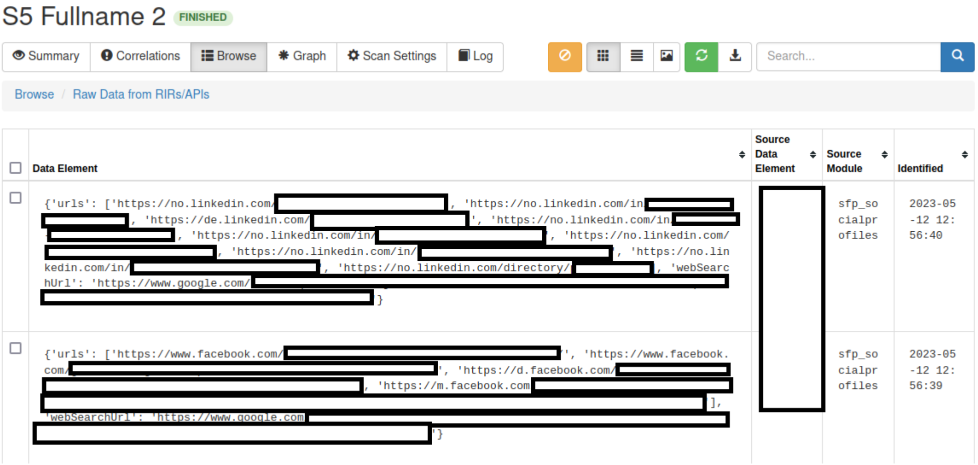
Subject 2: SpiderFoot



Browse / Social Media Presence

□	Data Element	Source Data Element	Source Module	Identified
□	LinkedIn: https://de.linkedin.com/[redacted]	[redacted]	sfp_socialprofiles	2023-05-12 12:56:40
□	LinkedIn: https://no.linkedin.com/[redacted]	[redacted]	sfp_socialprofiles	2023-05-12 12:56:40
□	LinkedIn: https://no.linkedin.com/[redacted]	[redacted]	sfp_socialprofiles	2023-05-12 12:56:40
□	LinkedIn: https://no.linkedin.com/[redacted]	[redacted]	sfp_socialprofiles	2023-05-12 12:56:40
□	LinkedIn: https://no.linkedin.com/[redacted]	[redacted]	sfp_socialprofiles	2023-05-12 12:56:40
□	LinkedIn: https://no.linkedin.com/[redacted]	[redacted]	sfp_socialprofiles	2023-05-12 12:56:40
□	LinkedIn: https://no.linkedin.com/[redacted]	[redacted]	sfp_socialprofiles	2023-05-12 12:56:40
□	LinkedIn: https://no.linkedin.com/[redacted]	[redacted]	sfp_socialprofiles	2023-05-12 12:56:40
□	LinkedIn: https://no.linkedin.com/[redacted]	[redacted]	sfp_socialprofiles	2023-05-12 12:56:40

Figure A.19: Caption

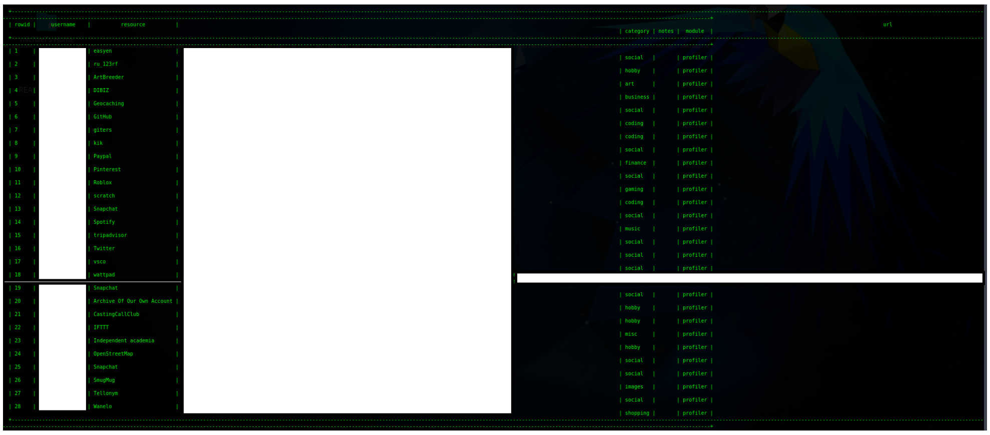


Browse / Raw Data from RIRs/APIs

□	Data Element	Source Data Element	Source Module	Identified
□	{'urls': ['https://no.linkedin.com/[redacted], 'https://no.linkedin.com/in[redacted], 'https://de.linkedin.com/[redacted]', 'https://no.linkedin.com/in[redacted], 'https://no.linkedin.com/in/[redacted]', 'https://no.linkedin.com/[redacted], 'https://no.linkedin.com/in/[redacted]', 'https://no.linkedin.com/in/[redacted]', 'https://no.linkedin.com/directory/[redacted], 'webSearchUrl': 'https://www.google.com/[redacted]}	[redacted]	sfp_socialprofiles	2023-05-12 12:56:40
□	{'urls': ['https://www.facebook.com/[redacted]', 'https://www.facebook.com/[redacted]', 'https://d.facebook.com/[redacted], 'https://m.facebook.com[redacted]], 'webSearchUrl': 'https://www.google.com[redacted]'}		sfp_socialprofiles	2023-05-12 12:56:39

Figure A.20: Subject 2: SpiderFoot, found URL

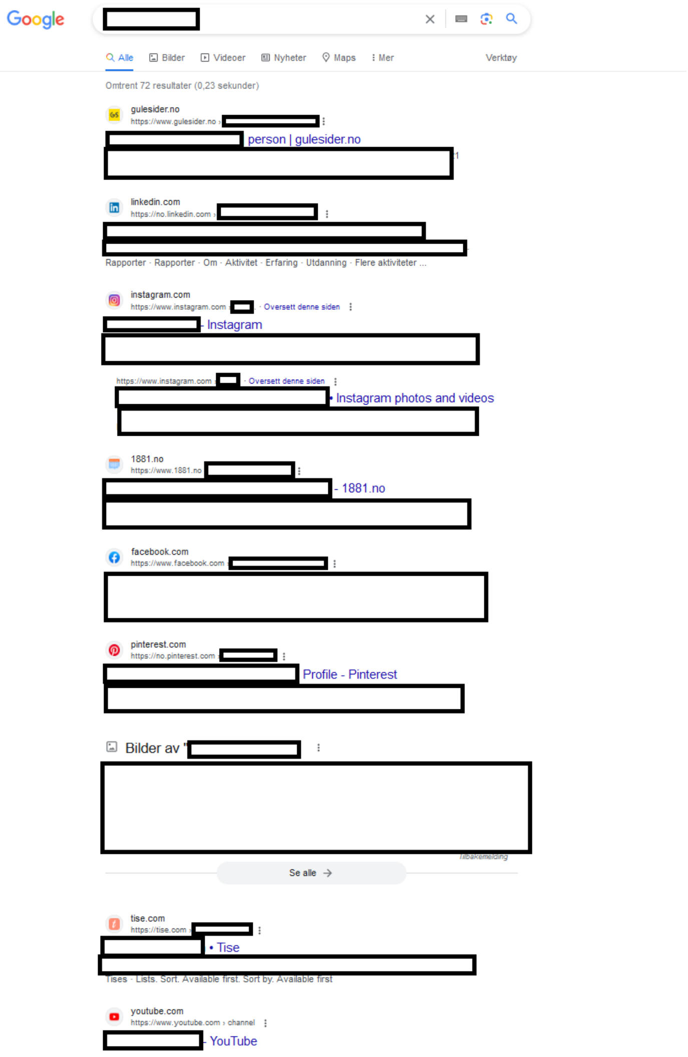
Subject 2: Recon-NG



```
+------------------------------------------------------------------------------------------------------------------------------------
------------------------------------------------+
| rowid |    username    |          resource          |                                                url
                                                 | category | notes |  module  |
+------------------------------------------------------------------------------------------------------------------------------------
------------------------------------------------+
| 1     | [redacted]     | easyen                     | [redacted]
                                                 | social   |       | profiler |
| 2     |                | ru_123rf                   |
                                                 | hobby    |       | profiler |
| 3     |                | ArtBreeder                 |
                                                 | art      |       | profiler |
| 4     |                | DIBIZ                      |
                                                 | business |       | profiler |
| 5     |                | Geocaching                 |
                                                 | social   |       | profiler |
| 6     |                | GitHub                     |
                                                 | coding   |       | profiler |
| 7     |                | giters                     |
                                                 | coding   |       | profiler |
| 8     |                | kik                        |
                                                 | social   |       | profiler |
| 9     |                | Paypal                     |
                                                 | finance  |       | profiler |
| 10    |                | Pinterest                  |
                                                 | social   |       | profiler |
| 11    |                | Roblox                     |
                                                 | gaming   |       | profiler |
| 12    |                | scratch                    |
                                                 | coding   |       | profiler |
| 13    |                | Snapchat                   |
                                                 | social   |       | profiler |
| 14    |                | Spotify                    |
                                                 | music    |       | profiler |
| 15    |                | tripadvisor                |
                                                 | social   |       | profiler |
| 16    |                | Twitter                    |
                                                 | social   |       | profiler |
| 17    |                | vsco                       |
                                                 | social   |       | profiler |
| 18    |                | wattpad                    |
[redacted]
| 19    | [redacted]     | Snapchat                   |
                                                 | social   |       | profiler |
| 20    |                | Archive Of Our Own Account |
                                                 | hobby    |       | profiler |
| 21    |                | CastingCallClub            |
                                                 | hobby    |       | profiler |
| 22    |                | IFTTT                      |
                                                 | misc     |       | profiler |
| 23    |                | Independent academia       |
                                                 | hobby    |       | profiler |
| 24    |                | OpenStreetMap              |
                                                 | social   |       | profiler |
| 25    |                | Snapchat                   |
                                                 | social   |       | profiler |
| 26    |                | SmugMug                    |
                                                 | images   |       | profiler |
| 27    |                | Tellonym                   |
                                                 | social   |       | profiler |
| 28    |                | Wanelo                     |
                                                 | shopping |       | profiler |
+------------------------------------------------------------------------------------------------------------------------------------
------------------------------------------------+
```

Figure A.21: S2: Recon-NG profiler

Subject 2: Search engines



Omtrent 72 resultater (0,23 sekunder)

gulesider.no
https://www.gulesider.no › [redacted]
[redacted] person | gulesider.no
[redacted]

linkedin.com
https://no.linkedin.com › [redacted]
[redacted]
Rapporter · Rapporter · Om · Aktivitet · Erfaring · Utdanning · Flere aktiviteter ...

instagram.com
https://www.instagram.com › [redacted] · Oversett denne siden
[redacted] - Instagram
[redacted]

https://www.instagram.com › [redacted] · Oversett denne siden
[redacted] • Instagram photos and videos
[redacted]

1881.no
https://www.1881.no [redacted]
[redacted] - 1881.no
[redacted]

facebook.com
https://www.facebook.com › [redacted]
[redacted]

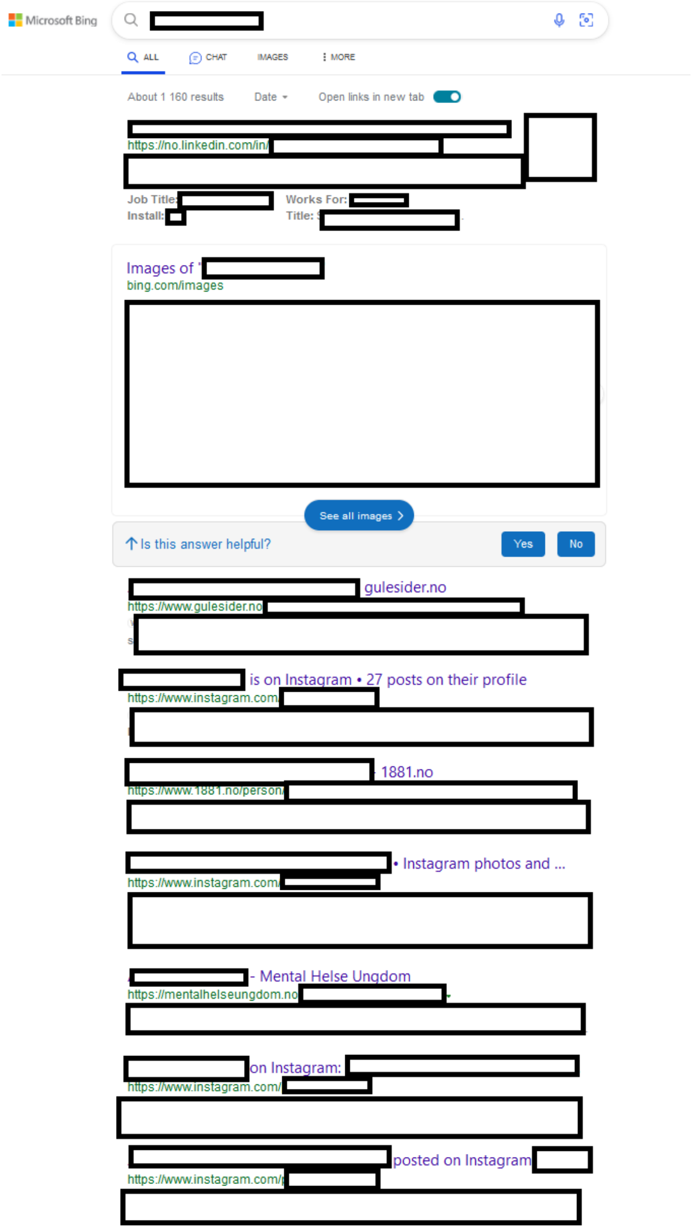
pinterest.com
https://no.pinterest.com › [redacted]
[redacted] Profile - Pinterest
[redacted]

Bilder av "[redacted]
[redacted]

tise.com
https://tise.com › [redacted]
[redacted] • Tise
[redacted]
Tises · Lists. Sort. Available first. Sort by. Available first

youtube.com
https://www.youtube.com › channel
[redacted] - YouTube

Figure A.22: Google search



[redacted]

About 1 160 results Date Open links in new tab

[redacted]
https://no.linkedin.com/in/[redacted]
[redacted]
[redacted]

Job Title: [redacted] Works For: [redacted]
Install: [redacted] Title: [redacted]

Images of [redacted]
bing.com/images
[redacted]

See all images

Is this answer helpful? Yes No

[redacted] gulesider.no
https://www.gulesider.no[redacted]
[redacted]

[redacted] is on Instagram • 27 posts on their profile
https://www.instagram.com[redacted]
[redacted]

[redacted] 1881.no
https://www.1881.no/person/[redacted]
[redacted]

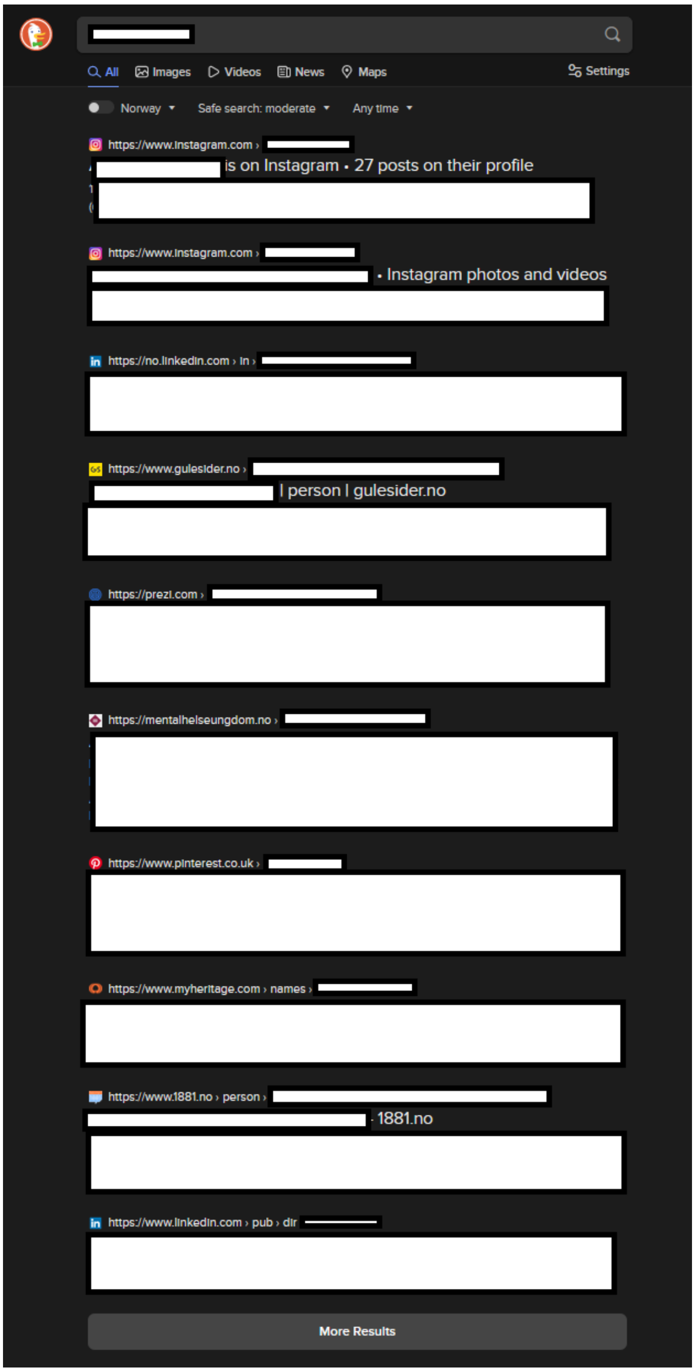
[redacted] • Instagram photos and ...
https://www.instagram.com[redacted]
[redacted]

[redacted] - Mental Helse Ungdom
https://mentalhelseungdom.no[redacted]
[redacted]

[redacted] on Instagram: [redacted]
https://www.instagram.com/[redacted]
[redacted]

[redacted] posted on Instagram [redacted]
https://www.instagram.com/[redacted]
[redacted]

Figure A.23: Bing search



[redacted]

Norway · Safe search: moderate · Any time

https://www.instagram.com › [redacted]
[redacted] is on Instagram • 27 posts on their profile
[redacted]

https://www.instagram.com › [redacted]
[redacted] • Instagram photos and videos
[redacted]

https://no.linkedin.com › in › [redacted]
[redacted]

https://www.gulesider.no › [redacted]
[redacted] | person | gulesider.no
[redacted]

https://prezi.com › [redacted]
[redacted]

https://mentalhelseungdom.no › [redacted]
[redacted]

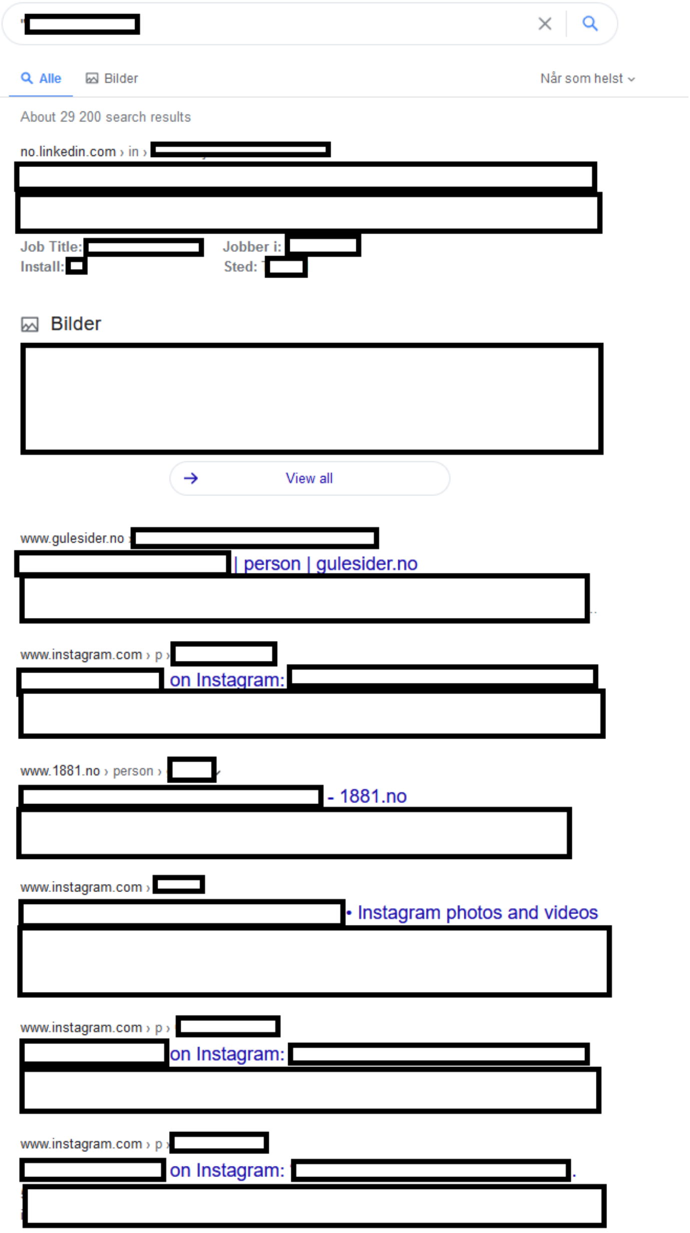
https://www.pinterest.co.uk › [redacted]
[redacted]

https://www.myheritage.com › names › [redacted]
[redacted]

https://www.1881.no › person › [redacted]
[redacted] · 1881.no
[redacted]

https://www.linkedin.com › pub › dir [redacted]
[redacted]

Figure A.24: DuckDuckGo search



[redacted]

About 29 200 search results

no.linkedin.com › in › [redacted]

[redacted]

[redacted]

Job Title: [redacted] Jobber i: [redacted]
Install: [redacted] Sted: [redacted]

Bilder

[redacted]

www.gulesider.no [redacted]

[redacted] | person | gulesider.no

[redacted]

www.instagram.com › p › [redacted]

[redacted] on Instagram: [redacted]

[redacted]

www.1881.no › person › [redacted]

[redacted] - 1881.no

[redacted]

www.instagram.com › [redacted]

[redacted] • Instagram photos and videos

[redacted]

www.instagram.com › p › [redacted]

[redacted] on Instagram: [redacted]

[redacted]

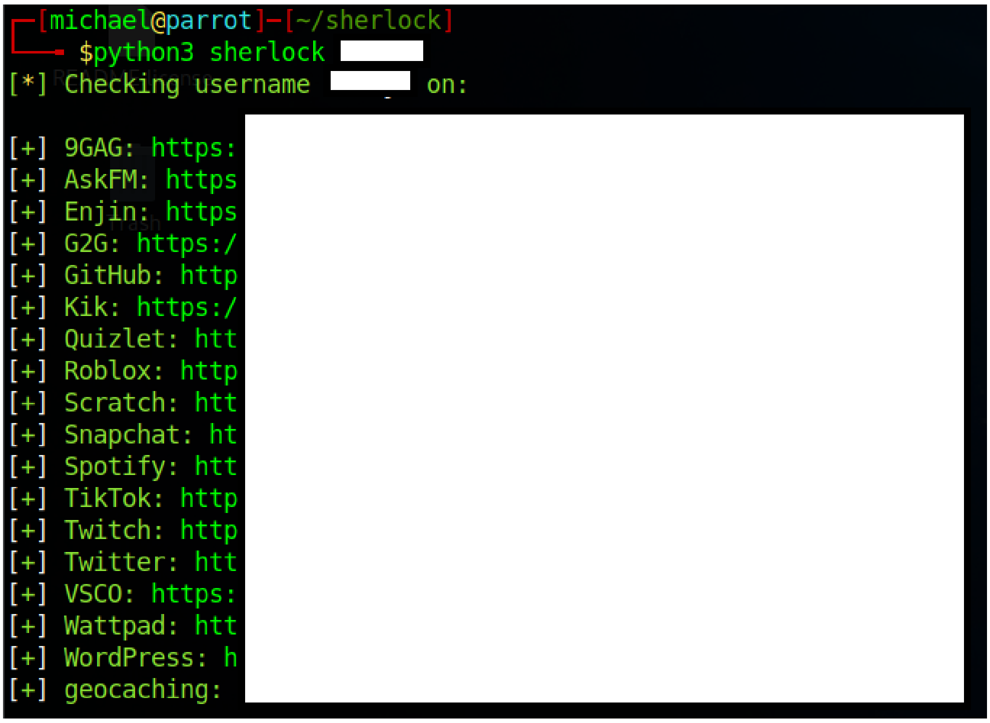
www.instagram.com › p › [redacted]

[redacted] on Instagram: [redacted].

[redacted]

Figure A.25: Yahoo search

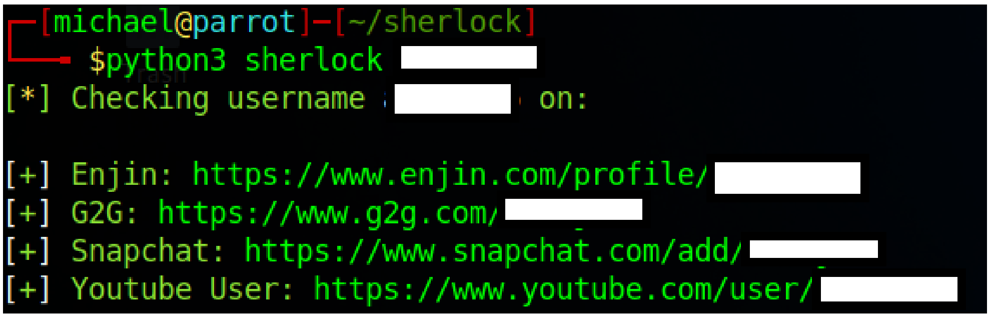
Subject 2: Others



```
┌─[michael@parrot]─[~/sherlock]
└──╼ $python3 sherlock [redacted]
[*] Checking username [redacted] on:

[+] 9GAG: https: [redacted]
[+] AskFM: https
[+] Enjin: https
[+] G2G: https:/
[+] GitHub: http
[+] Kik: https:/
[+] Quizlet: htt
[+] Roblox: http
[+] Scratch: htt
[+] Snapchat: ht
[+] Spotify: htt
[+] TikTok: http
[+] Twitch: http
[+] Twitter: htt
[+] VSCO: https:
[+] Wattpad: htt
[+] WordPress: h
[+] geocaching:
```

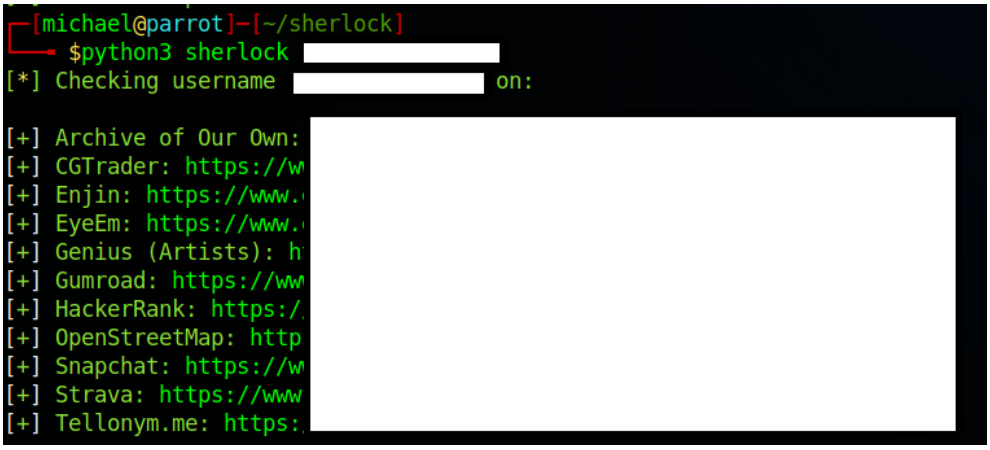
Figure A.26: S2: Sherlock username search pt.1



```
┌─[michael@parrot]─[~/sherlock]
└──╼ $python3 sherlock [redacted]
[*] Checking username [redacted] on:

[+] Enjin: https://www.enjin.com/profile/[redacted]
[+] G2G: https://www.g2g.com/[redacted]
[+] Snapchat: https://www.snapchat.com/add/[redacted]
[+] Youtube User: https://www.youtube.com/user/[redacted]
```

Figure A.27: S2: Sherlock username search pt.2



```
┌─[michael@parrot]─[~/sherlock]
└──╼ $python3 sherlock [redacted]
[*] Checking username [redacted] on:

[+] Archive of Our Own: [redacted]
[+] CGTrader: https://w
[+] Enjin: https://www.
[+] EyeEm: https://www.
[+] Genius (Artists): h
[+] Gumroad: https://ww
[+] HackerRank: https:/
[+] OpenStreetMap: http
[+] Snapchat: https://w
[+] Strava: https://www
[+] Tellonym.me: https:
```

Figure A.28: S2: Sherlock username search pt.3

A.4.3 Subject 3

Subject 3: Maltego

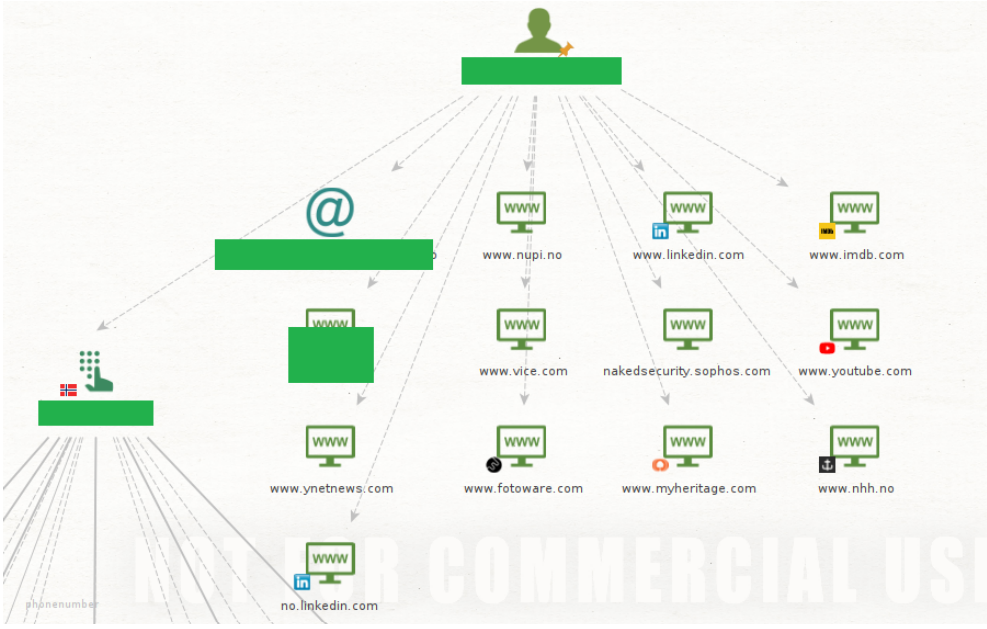


Figure A.29: Subject 3: Maltego all transforms, full name

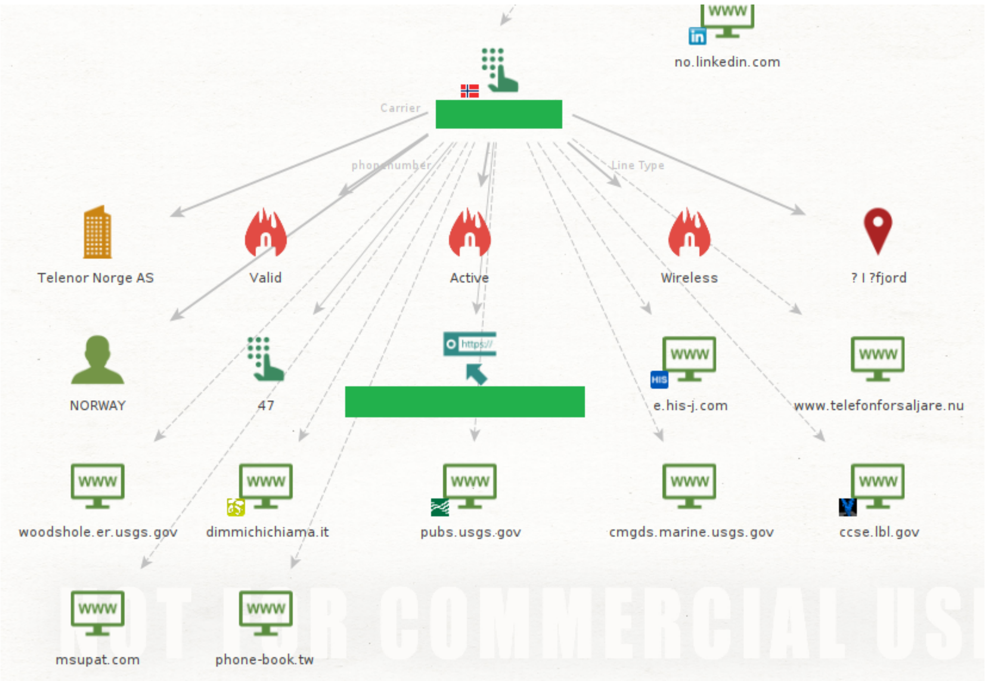
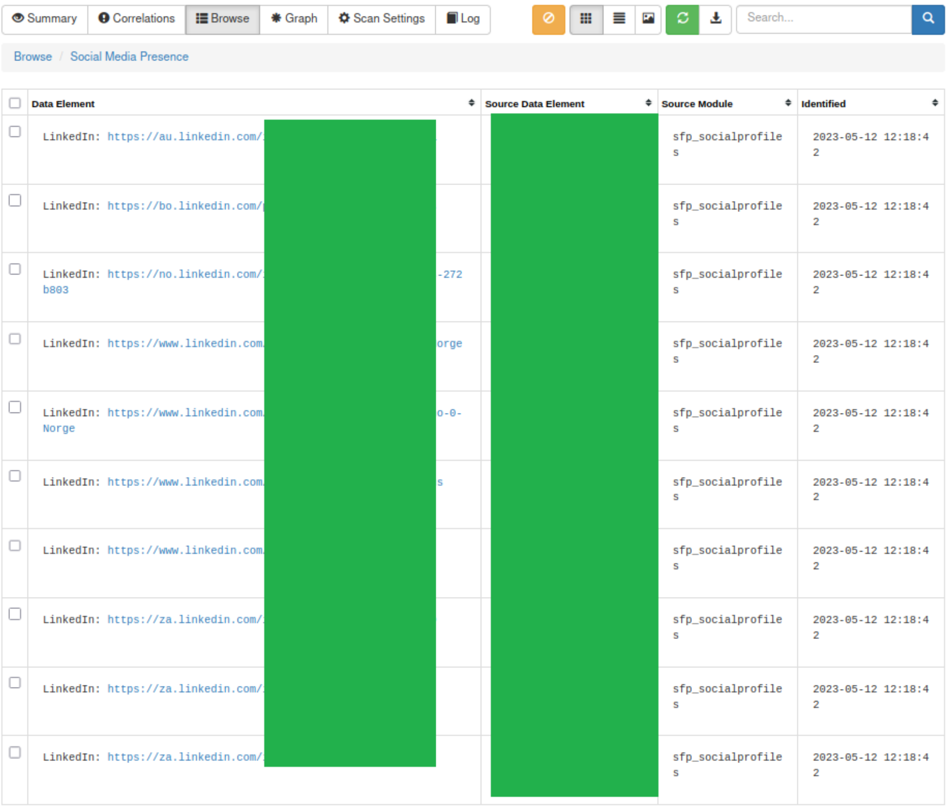


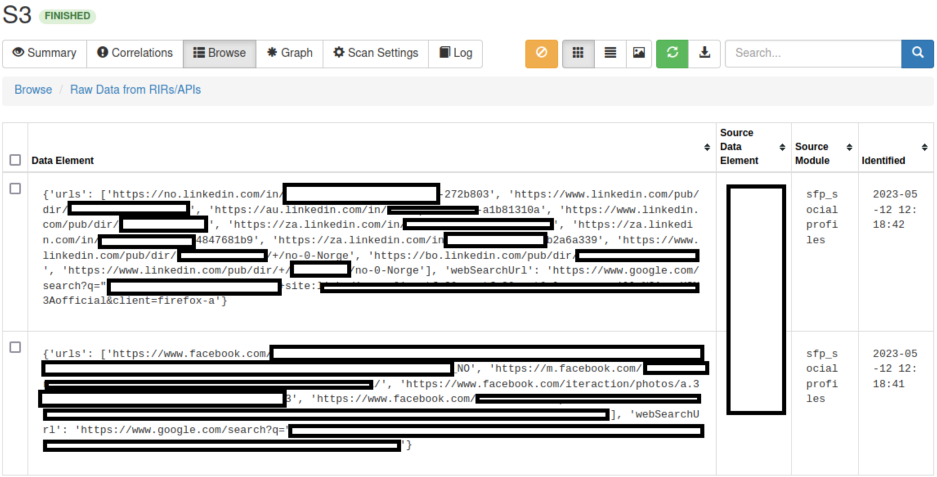
Figure A.30: Subject 3: Maltego all transforms, phone number

Subject 3: SpiderFoot



□	Data Element	Source Data Element	Source Module	Identified
□	LinkedIn: https://au.linkedin.com/[redacted]	[redacted]	sfp_socialprofiles	2023-05-12 12:18:42
□	LinkedIn: https://bo.linkedin.com/[redacted]	[redacted]	sfp_socialprofiles	2023-05-12 12:18:42
□	LinkedIn: https://no.linkedin.com/[redacted]-272b803	[redacted]	sfp_socialprofiles	2023-05-12 12:18:42
□	LinkedIn: https://www.linkedin.com[redacted]orge	[redacted]	sfp_socialprofiles	2023-05-12 12:18:42
□	LinkedIn: https://www.linkedin.com[redacted]o-0-Norge	[redacted]	sfp_socialprofiles	2023-05-12 12:18:42
□	LinkedIn: https://www.linkedin.com[redacted]s	[redacted]	sfp_socialprofiles	2023-05-12 12:18:42
□	LinkedIn: https://www.linkedin.com[redacted]	[redacted]	sfp_socialprofiles	2023-05-12 12:18:42
□	LinkedIn: https://za.linkedin.com/[redacted]	[redacted]	sfp_socialprofiles	2023-05-12 12:18:42
□	LinkedIn: https://za.linkedin.com/[redacted]	[redacted]	sfp_socialprofiles	2023-05-12 12:18:42
□	LinkedIn: https://za.linkedin.com/[redacted]	[redacted]	sfp_socialprofiles	2023-05-12 12:18:42

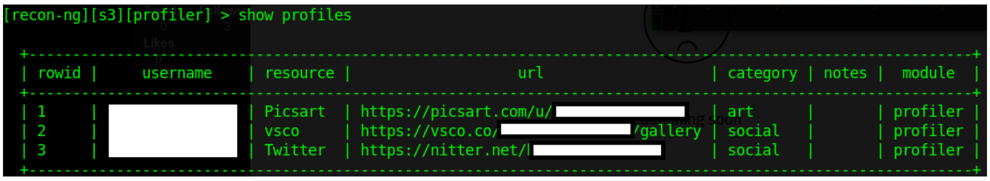
Figure A.31: Subject 3: SpiderFoot social media



□	Data Element	Source Data Element	Source Module	Identified
□	{'urls': ['https://no.linkedin.com/in/[redacted]-272b803', 'https://www.linkedin.com/pub/dir/[redacted]', 'https://au.linkedin.com/in/[redacted]-a1b81310a', 'https://www.linkedin.com/pub/dir/[redacted]', 'https://za.linkedin.com/in/[redacted]', 'https://za.linkedin.com/in/[redacted]4847681b9', 'https://za.linkedin.com/in[redacted]b2a6a339', 'https://www.linkedin.com/pub/dir/[redacted]/+/no-0-Norge', 'https://bo.linkedin.com/pub/dir/[redacted]', 'https://www.linkedin.com/pub/dir/+/[redacted]/no-0-Norge'], 'webSearchUrl': 'https://www.google.com/search?q="[redacted]+site:[redacted]3Aofficial&client=firefox-a'}	[redacted]	sfp_socialprofiles	2023-05-12 12:18:42
□	{'urls': ['https://www.facebook.com/[redacted]_NO', 'https://m.facebook.com/[redacted]/', 'https://www.facebook.com/iteraction/photos/a.3[redacted]3', 'https://www.facebook.com/[redacted]], 'webSearchUrl': 'https://www.google.com/search?q=[redacted]'}		sfp_socialprofiles	2023-05-12 12:18:41

Figure A.32: Subject 3: SpiderFoot urls

Subject 3: Recon-NG

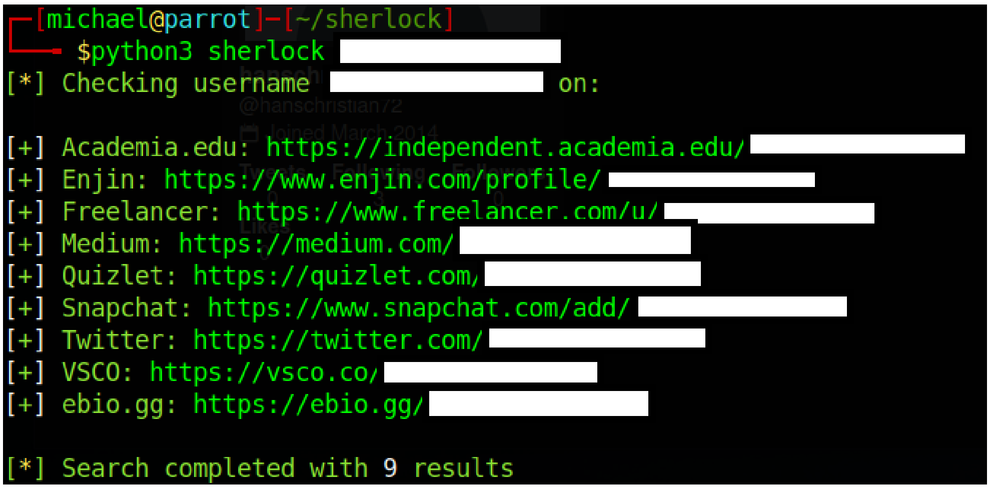


```
[recon-ng][s3][profiler] > show profiles

  +------------------------------------------------------------------------------------------------------------+
  | rowid |     username     | resource |                    url                        | category | notes |  module  |
  +------------------------------------------------------------------------------------------------------------+
  | 1     | [redacted]       | Picsart  | https://picsart.com/u/[redacted]              | art      |       | profiler |
  | 2     | [redacted]       | vsco     | https://vsco.co/[redacted]/gallery            | social   |       | profiler |
  | 3     | [redacted]       | Twitter  | https://nitter.net/[redacted]                 | social   |       | profiler |
  +------------------------------------------------------------------------------------------------------------+
```

Figure A.33: Subject 3: Recon-NG profiler

Subject 3: Others

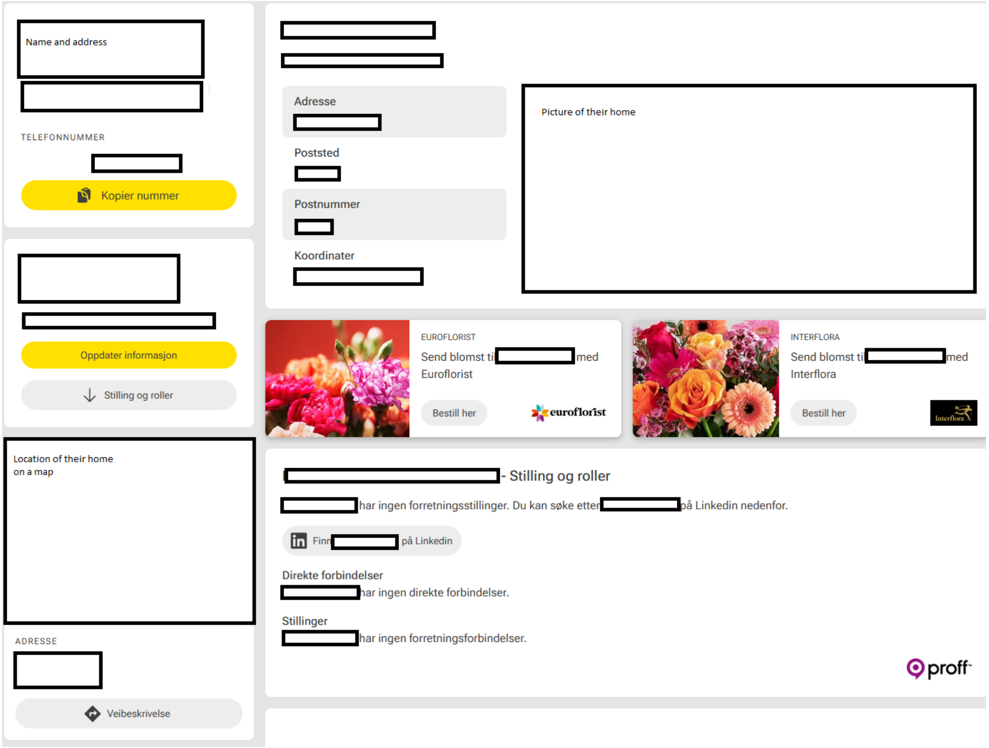


```
┌─[michael@parrot]─[~/sherlock]
└──╼ $python3 sherlock [redacted]
[*] Checking username [redacted] on:

[+] Academia.edu: https://independent.academia.edu/[redacted]
[+] Enjin: https://www.enjin.com/profile/[redacted]
[+] Freelancer: https://www.freelancer.com/u/[redacted]
[+] Medium: https://medium.com/[redacted]
[+] Quizlet: https://quizlet.com/[redacted]
[+] Snapchat: https://www.snapchat.com/add/[redacted]
[+] Twitter: https://twitter.com/[redacted]
[+] VSCO: https://vsco.co/[redacted]
[+] ebio.gg: https://ebio.gg/[redacted]

[*] Search completed with 9 results
```

Figure A.34: Subject 3: Sherlock username search



Name and address

[redacted]

[redacted]

TELEFONNUMMER

[redacted]

Kopier nummer

[redacted]

[redacted]

Oppdater informasjon

Stilling og roller

Location of their home on a map

ADRESSE

[redacted]

Veibeskrivelse

[redacted]

[redacted]

Adresse

[redacted]

Poststed

[redacted]

Postnummer

[redacted]

Koordinater

[redacted]

Picture of their home

EUROFLORIST

Send blomst ti[redacted]med Euroflorist

Bestill her

INTERFLORA

Send blomst ti[redacted]med Interflora

Bestill her

[redacted] - Stilling og roller

[redacted] har ingen forretningsstillinger. Du kan søke etter [redacted] på Linkedin nedenfor.

Finn [redacted] på Linkedin

Direkte forbindelser

[redacted] har ingen direkte forbindelser.

Stillinger

[redacted] har ingen forretningsforbindelser.

proff

Figure A.35: Subject 3: Gulesider

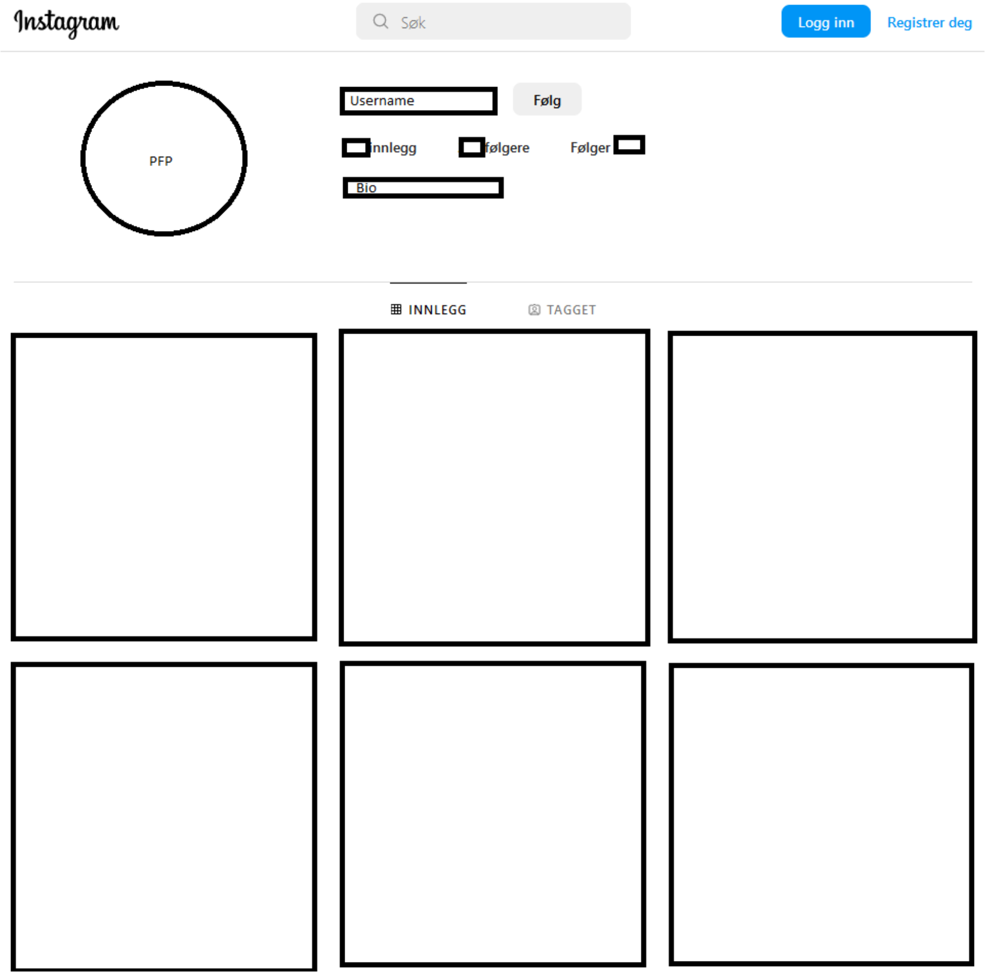


Figure A.36: Subject 3: Instagram-profile

A.4.4 Subject 4

Subject 4: Maltego

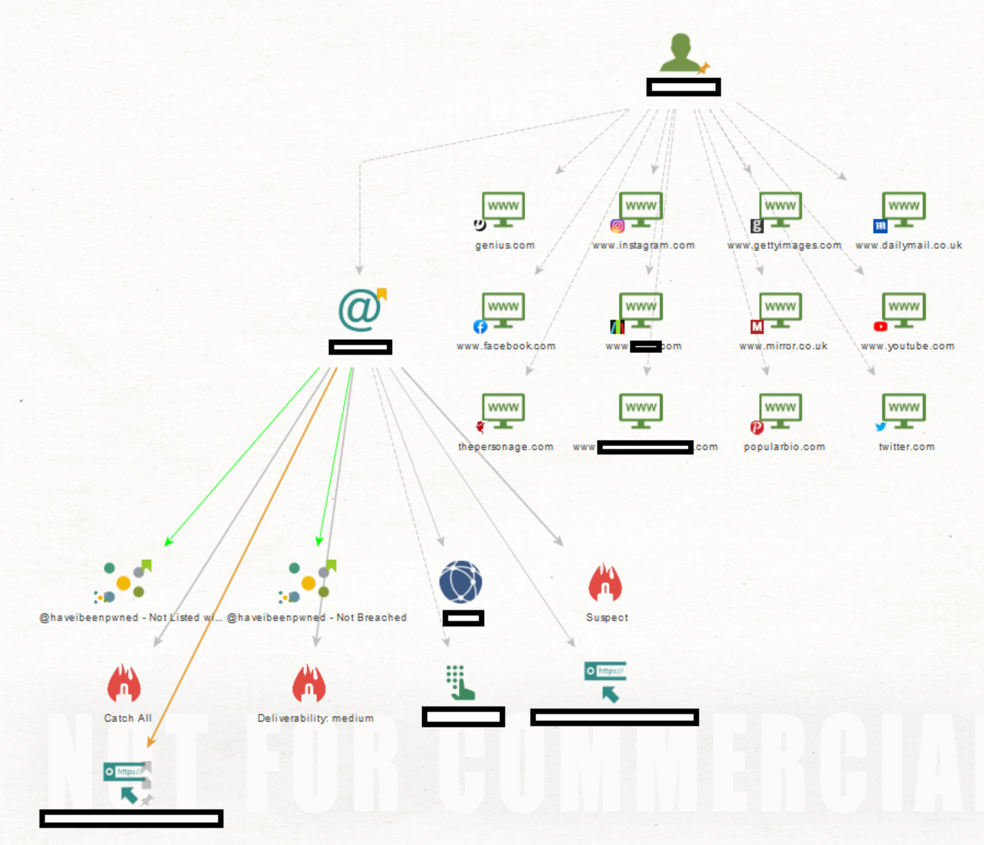


Figure A.37: Subject 4: Maltego full transform on name and email address

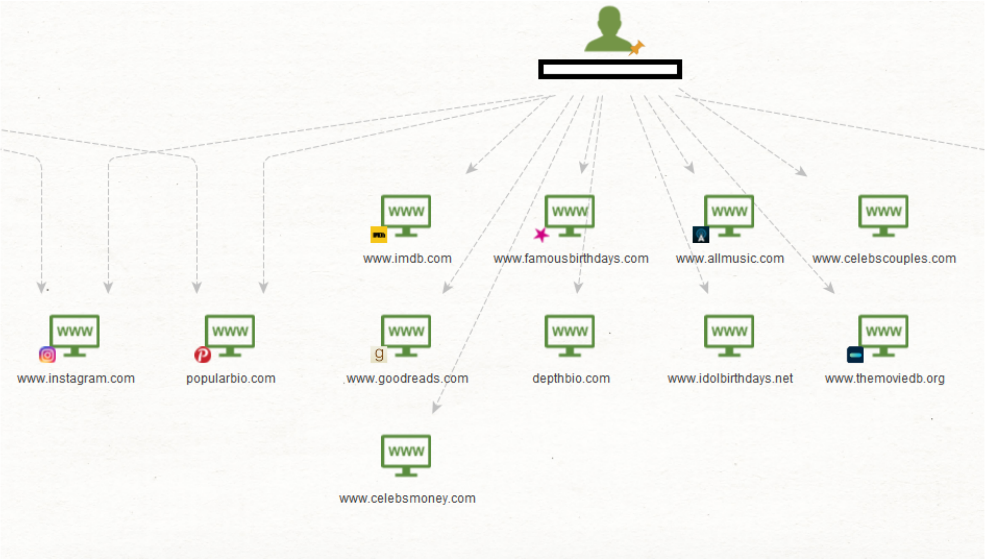


Figure A.38: Subject 4: Maltego full transform on full name

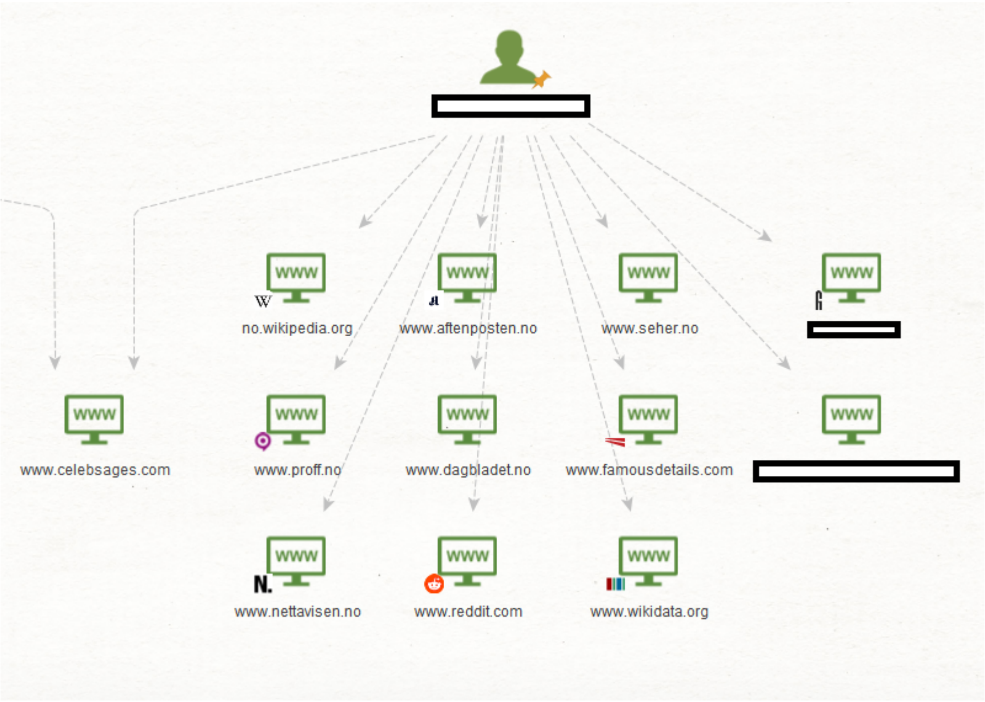
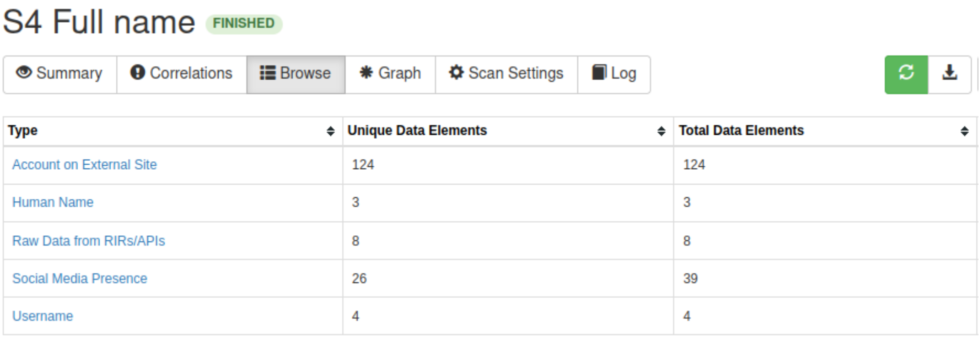


Figure A.39: Subject 4: Maltego full transform on full name

Subject 4: SpiderFoot



Type	Unique Data Elements	Total Data Elements
Account on External Site	124	124
Human Name	3	3
Raw Data from RIRs/APIs	8	8
Social Media Presence	26	39
Username	4	4

Figure A.40: Subject 4: SpiderFoot full name scan

NTNU

Norwegian University of
Science and Technology