
Open Source Intelligence Training in Hacking-Lab

Technical Report

Bachelor Thesis

BSc – Computer Science
Eastern Switzerland University of Applied Sciences
Campus Rapperswil-Jona

Spring Term 2023

Authors	Damian Dasser & Florian Falkner
Version	15/06/2023
Advisors	Ivan Bütler
External Co-Examiner	Vanessa Procacci
Internal Co-Examiner	Markus Stolze

Contents

1. Abstract	5
2. Acknowledgments	6
3. Management Summary	7
4. Glossary	11
I. Technical Report	12
1. Introduction	13
1.1. The Problem at Hand	13
1.2. Aim and Scope of this Thesis	13
1.3. Administrative Framework	13
1.4. The Hacking-Lab System Context	14
1.4.1. Student's point of view	14
1.4.2. Teacher's point of view	14
2. Open Source Intelligence on OSINT	17
2.1. Definitions	17
2.1.1. Data and Information	17
2.1.2. Open Information and Intelligence Categories	17
2.2. OSINT - Open Source Intelligence	18
2.3. Behind the INT Acronyms	18
2.3.1. GEOINT - Geospatial Intelligence	19
2.3.2. HUMINT - Human Intelligence	19
2.3.3. IMINT - Imagery Intelligence	19
2.3.4. SIGINT - Signals Intelligence	19
2.4. A Picture is Worth a Thousand Words	19
2.4.1. Coordinates	19
2.4.2. Landmarks	19
2.4.3. Distances	19
2.4.4. Roads and Signs	20
2.4.5. Cars and Plates	21
2.4.6. Houses	21
2.4.7. Flags	21
2.4.8. Flora and Fauna	21
2.4.9. Biometrics	22
2.4.10. Others	22

2.4.11. Metadata	22
2.4.12. Reverse Image Search	22
2.5. Information About Businesses	22
2.5.1. Online Presence	23
2.5.2. Home Page	23
2.5.3. Social Media	23
2.5.4. Commercial Register	23
2.5.5. Stock Market	23
2.5.6. News	23
2.5.7. Reviews	23
2.6. Information About a Person	23
2.6.1. What defines a person	23
2.6.2. Names	24
2.6.3. Date of Birth	24
2.6.4. E-Mail Address	24
2.6.5. Tracking on Social Media	24
2.7. Other Information and the Internet	24
2.7.1. Satellite Imagery	24
2.7.2. Aerial Photography	24
2.7.3. User Created Content	24
2.7.4. Databases	25
2.7.5. Tracking Objects	25
2.7.6. Dark Web	25
2.7.7. Analysis of Code	25
2.8. Just Some Text?	25
2.8.1. Fonts	25
2.8.2. Writing Style	26
2.8.3. Meaning	26
2.8.4. Translation	26
2.9. What does this mean for OSINT?	26
3. Requirements	27
3.1. Challenge Requirements	27
3.2. Lecture Requirements	28
4. The Tale of Stories and Doings	30
4.1. Definition	30
4.1.1. Doings	30
4.1.2. Stories	30
4.2. Design Workflow	30
4.3. Creation	30
4.4. Matching	32
4.5. Categorisation and Rating	33
4.5.1. Categorising the Stories	33
4.5.2. Weighting the Doings	33
4.5.3. Rating the Stories	33
4.5.4. Selecting Ten Stories	34
5. Challenge Documentation	35
5.1. Challenge 01 - Scamming Personal Information	36
5.2. Challenge 02 - The Propagandist's Information	39
5.3. Challenge 03 - Time for Waste	43
5.4. Challenge 04 - Validate Internet Post	47
5.5. Challenge 05 - Third Party Software Contributions	49
5.6. Challenge 06 - Show What You Have Learned	52
5.7. Challenge 07 - Vulnerability Information	54

5.8. Challenge 08 - Run After Ransomware	56
5.9. Challenge 09 - A Car's History	59
5.10. Challenge 10 - Malicious Gamer	62
6. Testing	64
6.1. Testing Procedure	64
6.2. Test by the Author	65
6.3. Team Internal Testing	65
6.4. External Testing Group	65
6.4.1. The Feedback Form	65
6.4.2. Received Feedback Statistic	65
6.4.3. Feedback Form Review	66
6.4.4. Applied Changes Overview	67
7. Results	68
7.1. Desired Target	68
7.2. Optional Targets	68
8. Conclusion and Outlook	70
II. Appendix	71
1. List of Figures	72
2. List of Tables	73
3. Bibliography	76

CHAPTER 1

Abstract

In cyber security the topic of Open-source intelligence (OSINT) plays a major role. With OSINT security defender and researcher may find valuable information about cyber crime and attackers. OSINT helps to understand the effects of sharing public information. OSINT is not yet part of the curriculum at OST. An e-learning platform called Hacking-Lab already exists and is used at OST. In Hacking-Lab, students can apply what they have learned in the lecture in a controlled environment in the form of practical hands-on exercises.

The goal of this thesis was to create ten OSINT challenges in the Hacking-Lab for students to solve and practice. In every OSINT challenge, students are given a set of tasks and summative assessment questions. The students are guided through the proposed steps in order to answer the posed questions in form of a write-up.

Each OSINT challenge is framed by a story to make them more engaging. These stories were chosen in a way that many different OSINT techniques are applicable and can be practiced by the students. In OSINT there is not only one way to find the correct answer hence the students are also encouraged to find their own way to reach the expected solution. To guarantee a high quality of the challenges, multiple quality assurance tests were conducted with students and colleagues working in IT. The results of these quality tests are an indicator whether the goal was reached.

As a result of this work, the goal of creating ten OSINT challenges in Hacking-Lab was achieved. These challenges provide some insight into the topic of OSINT without getting lost in details and technicalities.

This project provides a foundation which a lecturer can build upon by creating a lecture on OSINT. This lecture could be integrated in a course on cyber security. Social media was purposely neglected in this project because social media is difficult to maintain and make future-proof, which makes it incompatible with the project's requirements. Therefore, it could also be a future project to expand upon these challenges with a focus on social media as it is an indispensable part of OSINT.

CHAPTER 2

Acknowledgments

We would like to express our gratitude to all the supporters of this thesis.

First of all, we thank our supervisor Ivan Bütler for the exciting and challenging work as well as his valuable contributions and ideas.

A thank you goes to our testers as well, who took time to go through our work and give valuable feedback which we gladly incorporated in our work.

Last but not least, we would like to thank our families, partners and friends for their time and support.

CHAPTER 3

Management Summary

The main goal of this project was to create exercises as a foundation to enable teaching the topic of Open-source intelligence (OSINT).

Why OSINT?

In today's digital landscape, where cyber threats are becoming increasingly sophisticated and pervasive, effective cyber security measures have become a necessity for individuals, organizations, and nations. To protect critical systems and sensitive data, cyber security professionals rely on various tools and techniques, one of which is OSINT.

What is OSINT?

OSINT involves gathering information from publicly available sources, such as websites, social media platforms, forums, news articles, and other online repositories. The categories used in this thesis can be seen in Figure 3.1 It focuses on collecting and analysing data that is accessible to anyone, without requiring any specialized access or permission. This wealth of openly accessible information serves as a treasure trove for cyber security professionals, providing valuable insights into potential vulnerabilities, threat actors, attack patterns, and emerging risks.

Importance of OSINT

OSINT allows cyber security professionals to monitor the digital landscape proactively and detect potential threats at an early stage. This enables swift response and mitigation, preventing or minimizing the impact of cyber incidents.

Cyber security incidents rarely occur in isolation. They are often part of a larger landscape influenced by geopolitical events, emerging technologies, or industry-specific factors. OSINT allows cyber security professionals to contextualize their findings and understand the broader environment in which threats operate. This contextual understanding is crucial for developing effective response strategies, anticipating future threats, and staying one step ahead of adversaries.

When a cyber incident occurs, OSINT can be instrumental in conducting post-incident analysis and investigations. By leveraging publicly available information, it can help with the reconstruction of the timeline of events, the identification of the attack vector, and tracing the origin of the attack. This information not only helps in understanding the incident's scope and impact but also aids in attributing the attack to specific threat actors or groups.

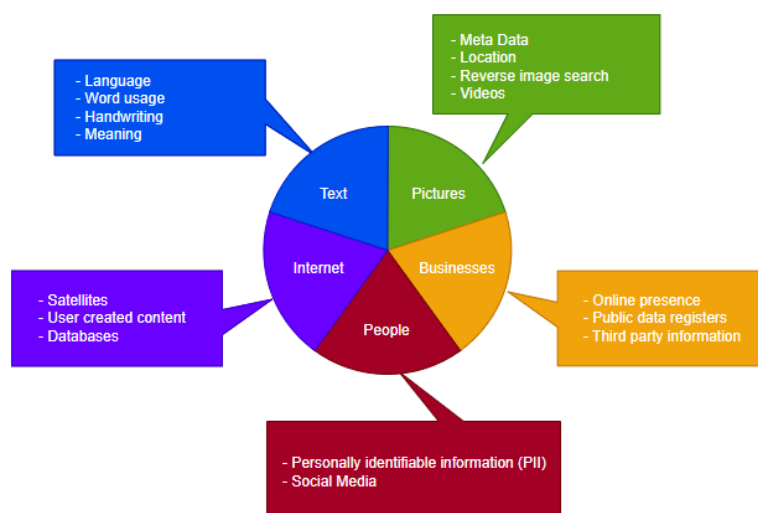


Figure 3.1.: OSINT topics in this thesis

OSINT at OST

OSINT is not yet part of the curriculum at "Ostschweizer Fachhochschule" (OST). Nevertheless, there are already multiple lectures focusing on cyber security. These lectures occasionally use the e-learning platform Hacking-Lab. In Hacking-Lab, students can apply what they have learned in the lecture in a controlled environment in the form of practical hands-on exercises.

Requirements

The goal was to create 10 challenges in Hacking-Lab. Challenges in Hacking-Lab are structured in sections and steps. The sections in turn are structured with some titles. The first section must include an introduction, a goal or story, and tasks and is usually followed by multiple steps guiding students through the challenge by giving instructions, background information, hints and posing questions. At the end of the challenge, there is a description of what the students need to hand in in order to complete the challenge. In this project it is always a flag in addition to a write-up where students should explain how they were able to answer the questions posed. Each challenge shall take around 30 minutes to solve. The challenges are created to be sustainable, meaning that they should be solvable in a similar manner in the years to come. The challenges shall be interesting to solve while still teaching the students the ins and outs of OSINT.

In addition to the challenge students can see, each challenge must also come with so-called grading instructions. These grading instructions should contain detailed instructions as to how the solution was reached when creating the challenge. In OSINT there is not only one way to find the correct answer hence the students are also encouraged to find their own way to reach the expected solution.

Choosing Challenges

In order to satisfy the requirement of interesting challenges, each challenge was framed by a story. The team brainstormed some ideas which were then divided into stories and doings. Stories describe a situation which could happen in real life where OSINT could be used to gather information surrounding the situation. For example, a person is stopped at the boarder because their newly bought used car is missing an important form. The owner of the car now wants to find out about the car's history and why the form is missing. Doings are tasks which could be associated with many different stories. For example, finding the exact location where a picture was taken. These doings were linked to each story where it was deemed possible. Then the doings were ranked by importance consequently also giving a ranking to the different stories they were linked to. After a preselection to eliminate stories with missing relevance for IT students, the top 10 stories were chosen to create exercises from.

Iterative Testing

During the creation of the challenges, the team members each solved the others challenge and gave feedback. The initial team member revised the challenge according to the feedback and it was tested again before being uploaded to the external testing platform of Hacking-Lab. There are other students from OST and colleagues working in IT tested the challenges again and gave feedback through a feedback form. The challenges were adjusted based on that feedback before being tested again. Figure 3.2 shows this procedure visually.

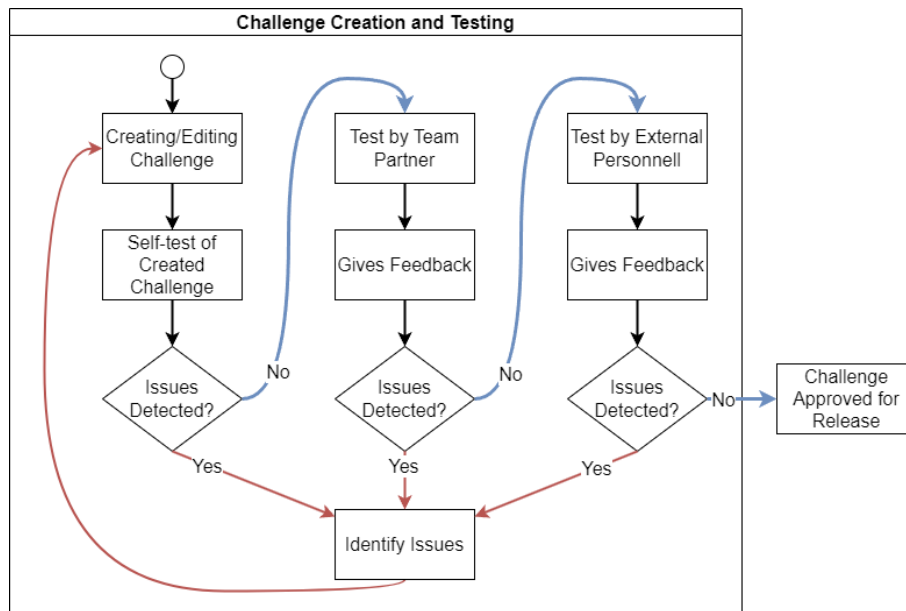


Figure 3.2.: Iterative testing procedure

Results

10 challenges were created as seen in Figure 5.1 meeting the requirements. The challenges provide some insight into the topic of OSINT without getting lost in details and technicalities. Classic OSINT topics like geolocating pictures or research on certain people are covered as well as exercises which require translation or research on standards like VIN or container numbers. All labs are deployed on the Hacking-Lab platform and were tested by Cyber Security students at the OST and people outside OST to cover more expert opinions on specific topics like geolocation or translation. In essence, the result of the thesis provides a foundation to build upon for teaching OSINT at OST.

Outlook

Using the thesis as a basis, a teacher can create a lecture on the topic of OSINT. This lecture can be integrated in a course on cyber security. The lecturer then has a pool of challenges to choose from to give the students to solve during the exercise session. Social media was purposely neglected in this project because it is difficult to maintain and make future-proof, which makes it incompatible with the project's requirements. Therefore, it could also be a future project to expand upon these challenges with a focus on social media as it is an indispensable part of OSINT.





















#	Name	Categories	Level	#	Name	Categories	Level
1	 01 - Scamming Personal Information b39b6263-141a-4fb0-8927-30201f0059b9		easy	6	 06 - Show What You Have Learned 69d55549-87ad-40fa-bb2a-08bee8fcd0d2		medium
2	 02 - The Propagandist's Information 825a0db6-5474-40d2-aa3f-2911a4e6c829		medium	7	 07 - Vulnerability Information 45432888-540a-49be-8684-2b4873490c76		novice
3	 03 - Time for Waste 00dc1eea-5b05-4e04-ad34-9c0d325c845e		easy	8	 08 - Run After Ransomware 3306164a-5b4a-4ce6-b1fc-79d2998ed956		medium
4	 04 - Validate Internet Post 88df05bc-aaa3-4c2c-84f6-8985dc076fa		easy	9	 09 - A Car's History 65033668-4b98-4b22-b790-1dbbee6a7e		novice
5	 05 - Third Party Software Contributions 8be49b45-5efe-490c-9477-5bb6808763a7		easy	10	 10 - Malicious Gamer 73e9cb77-ffff-43c4-883f-3141d8e9e0d8		easy

Figure 3.3.: Challenges overview

Glossary

- COMINT** Focus on the content of transmitted messages inside electromagnetic signals. 18
- ELINT** Geolocation of foreign electromagnetic signals. For example, radars or radioactive materials. 18
- Exif** Standardised format for metadata of images. 21
- FISINT** Deals with signals created through telemetry or beacons from deployed systems. 18
- flag** A specific string which has to be found during a task. It must match perfectly with the master solution.
13, 26
- GEOINT** Mapping geospatial information to locate any position precisely. 18
- google dorking** Using the Google search with advanced operators like 'filetype:' or 'allinurl:'. 27
- HUMINT** Information acquisition through human sources. Usually called spy or agent. 18
- IMINT** Information acquisition through pictures. 18
- Kookarai** Based on Kali Linux this distribution contains additions like a VPN specially for Hacking-Lab.com.
26
- MPEG-7** Standardised format for metadata of audio-visuals. 21
- OSINT** Information gathering using publicly available sources. 12, 16
- SIGINT** Intelligence on both raw data and products of its analysis. Subcategories are COMINT, ELINT and FISINT. 18
- write-up** A description of an approach to solve the task at hand. It contains the steps taken and can be used to replicate the findings. 13

Part I.

Technical Report

CHAPTER 1

Introduction

1.1. The Problem at Hand

Cyber security is a versatile, exciting and time-consuming topic. No matter how much time one spends on it, there is always a stone unturned, from Phishing, buffer overflows, side channel attacks, denial of service, ransomware to supply chain attacks. All of them are huge topics on their own and most of the time they rely on information that is publicly available. Nowadays we take this information and its gathering for granted and do not think about it very much. However, this information procurement and accumulation on its own is a topic of cyber security called Open Source Intelligence (OSINT). While OSINT is such an essential subject it finds little coverage in computer science education.

1.2. Aim and Scope of this Thesis

The paper deals with the topic of OSINT. Ten tasks are to be created, which will be solved by future students in the context of a cyber security lecture. The tasks shall be integrated in the Hacking-Lab e-learning platform already used at the OST. In addition, the tasks should require as little maintenance as possible. This means that the content should be stable over time so that it does not require regular maintenance.

1.3. Administrative Framework

This thesis is partially a student research project thesis and a bachelor thesis. The time budget therefore varies between the team members. In combination this thesis has a budget of 600 hours of work and a reward of 20 ETCS as seen in Table 1.1.

Student	ETCS	Required total hours
Florian	8	240
Damian	12	360
<i>Total</i>	<i>20</i>	<i>600</i>

Table 1.1.: ETCS and time budget per team member

OST policy requires that a Bachelor thesis with a term paper component, the respective work credits be listed, and the bachelor thesis part is graded independently from the semester thesis part. The work distribution can be seen in Table 1.2.

Written by Florian, Proof-read by Damian	Collaboratively Written and Proofread	Written by Damian, Proof-read by Florian
<i>Preamble</i>	<i>Preamble</i>	<i>Preamble</i>
3. Management Summary	1. Abstract	2. Acknowledgments
<i>Chapter I</i>	<i>Chapter I</i>	<i>Chapter I</i>
8. Conclusion and Outlook	2. Open Source Intelligence on Open Source Intelligence	1. Introduction
<i>Chapter II</i>	3. Requirements	4. The Tale of Stories and Doings
2. Project Plan	5. Challenge Documentation	6. Testing
5. Time Management	<i>Chapter II</i>	7. Results
<i>Chapter III</i>	1. Project Management	<i>Chapter II</i>
Meeting Minutes	4. Risk Analysis	3. Quality Assurance
Interview Minutes	<i>Chapter III</i>	<i>Chapter III</i>
<i>Hacking-Lab Challenges</i>	Conducted Interviews	Feedback Form
01 - Scamming Personal Information		<i>Hacking-Lab Challenges</i>
04 - Validate Internet Post		02 - The Propagandist's Information
06 - Show What You Have Learned		03 - Time for Waste
07 - Vulnerability Information		05 - Third Party Software Contributions
10 - Malicious Gamer		08 - Run After Ransomware
		09 - A Car's History

Table 1.2.: Work distribution

1.4. The Hacking-Lab System Context

The Hacking-Lab is an online platform used for e-learning. As the name suggests it focuses on the topic of hacking and thus cyber security. The Hacking-Lab contains various events which contain one or more so called challenges. These challenges cover a certain topic and always contain a description which states what one has to do and submit to solve this challenge. The submission of a challenge can consist of a specific string, called flag, which has to exactly match the solution or a description of the steps taken while solving the task and thus documenting the process which is called a write-up.[34]

It is developed and maintained by Compass Security AG whose co-founder Ivan Bütler is this project's advisor.

1.4.1. Student's point of view

A student can participate in multiple courses, called events, in the Hacking-Lab menu. An event consists of multiple challenges as seen in Figure 1.1. In the overview the students see the level of difficulty, the required hand-ins and the current grading points achieved. Coloured squares at the top of the page indicate the current status of the challenges and of the event as a whole.

A challenge itself again states its properties as in the overview, a list of resources, if available, and finally the description of the task at hand.

1.4.2. Teacher's point of view

The teacher receives a list of student submissions and their grading status. Each submission can be graded separately. The grading view displays the solution history of a student for this challenge together with the master solution on the right side as seen in Figure 1.4. In this example the solution was submitted as a PDF file and is thus not directly visible.

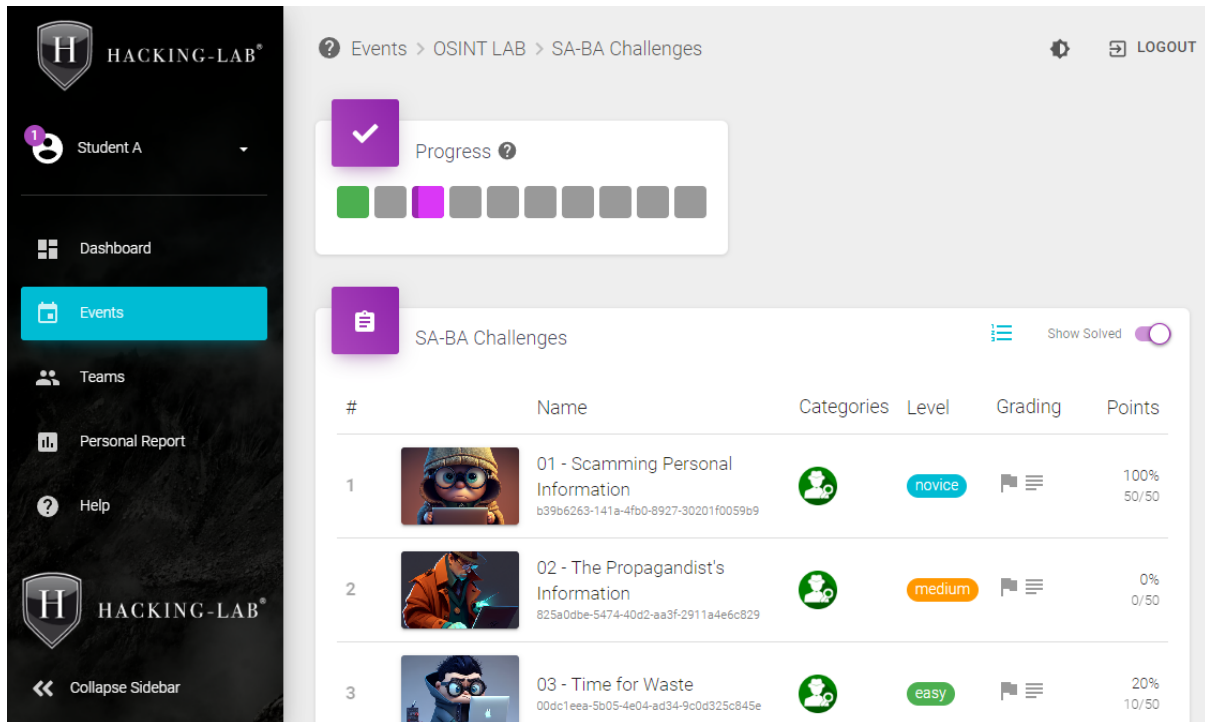


Figure 1.1.: Overview of the challenges to solve

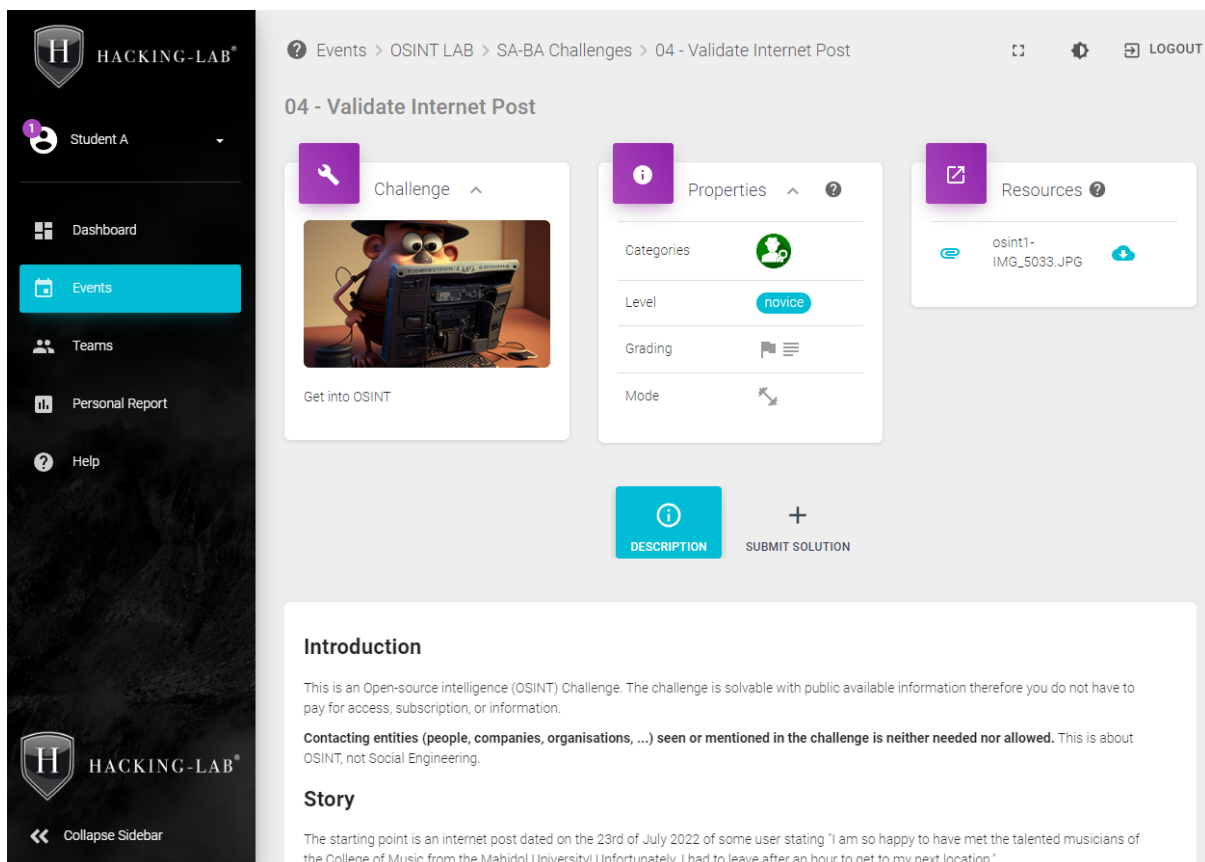


Figure 1.2.: View of a challenges

The screenshot shows the Hacking-Lab teacher interface. On the left is a sidebar with navigation options: Mr. Teacher, Inbox, Account, Profile, Logout, Dashboard, and Collapse Sidebar. The main content area is titled 'Teacher > SA-BA Challenges'. It features three summary cards: 'Event Status Running' (with a green clock icon), 'Open Solutions 4' (with an orange checkmark icon), and 'User 19' (with a purple person icon). Below these is a 'Challenge Solutions' table with columns for Name, Title, Status, Pct, and Date. The table lists three entries, all with a 'GRADED' status.

Name	Title	Status	Pct	Date
Student F (username-f)	01 - Scamming Personal Information	GRADED	0%	02.06.2023
Student B (username-b)	10 - Malicious Gamer	GRADED	20%	31.05.2023
Student B (username-b)	06 - Show What You Have	GRADED	20%	31.05.2023

Figure 1.3.: Student submissions in an overview for a teacher

The screenshot shows the Hacking-Lab teacher interface for assessing a student submission. The sidebar on the left is identical to Figure 1.3. The main content area is titled 'Disable Markdown' and features a vertical timeline of events. The events are: 'FLAG SUBMITTED' (bottom), 'FLAG ACCEPTED' (middle), and 'COMMENTED' (top). The 'COMMENTED' event includes a message: 'Submit a writeup to receive full grade', 'Current Solution State: Graded', and '28 May 2023 16:43 system'. To the right of the timeline is a 'Grading Instructions' panel. It contains a 'Valid Flags' section with a barcode and the text '28 May 2023 16:43'. Below this is a 'Write-up' section with two questions: '① How old is the PHP repository and who is the owner? Is this repository a fork and if yes from where?' and '② Write down if you find something suspicious in the commits between 2021-05-31 and 2021-05-27 and describe why.' Below the second question, there is a partial sentence: 'On the 2021-05-III we find suspicious entries.' and a barcode.

Figure 1.4.: Assessment of a student submission (master solution redacted)

Open Source Intelligence on OSINT

This chapter covers the research done on and around OSINT during this thesis. It outlines the OSINT term and discusses various aspects which seemed essential to be used in Hacking-Lab challenges.

2.1. Definitions

Before going into OSINT, some terms need to be defined to ensure a proper understanding.

2.1.1. Data and Information

The main difference between data and information is the context, which is missing in data and being provided by information.

Data state a fact without context nor analysis. For example, "the autonomous car was travelling at 10km/h at the time of impact." It is not clear if the car was breaking or accelerating at that time.

Information on the other hand provides context and meaning. Using the same example, information could look like "the autonomous car accelerated from 5km/h to 10km/h in the 2 seconds before the impact."

2.1.2. Open Information and Intelligence Categories

The *NATO Open Source Intelligence Handbook V1.2* [3] defines four distinct categories for open information and intelligence:

- Open Source Data (OSD)
 - Raw data coming from a primary source.
 - Examples: photograph, recordings, oral communication
- Open Source Information (OSIF)
 - Various pieces of data can be put together and some sort of filtering is applied to ensure specific criteria, it is labelled as OSIF.
 - Examples: newspapers, books, broadcasts
- Open Source Intelligence (OSINT)
 - Intentionally sought or obtained information to meet certain needs and answer certain questions.
- Validated OSINT (OSINT-V)
 - OSINT information validated through non-OSINT sources and thus having a high certainty and trustworthiness.

2.2. OSINT - Open Source Intelligence

According to Nihad and Rami [18] open source intelligence describes information specifically searched for and available to the public. The sources are not limited to the internet and can consist of books, newspapers, television and radio broadcasts and many other sources too. Even weather and geographical data can be searched for while still conducting OSINT.

The term OSINT is mostly used in cyber security or by governmental agencies. Most people will "google" for information or "look something up", while state and intelligence agencies would rather use the word OSINT to describe the same task. Beside the wording there is a major difference between googling around and conducting OSINT. In the latter, collected information must be stored and enriched with additional information like timestamps and sources. Proper handling of the information is critical to the success of an OSINT operation.

The data gathered using OSINT can be used in many different scenarios such as financial or criminal investigations, but also in more mundane tasks such as analysing business competitor, running background checks or just gathering information about specific individuals or entities in general. Nihad and Rami estimate that around 90 percent of useful information gathered by intelligence services comes from public sources.

Why is OSINT so popular and important? OSINT provides a multitude of benefits. It is cost-effective especially when compared to other intelligence sources such as a private investigator. It is easy to get started. OSINT sources are always available and up to date. This is especially true when using social media. Using OSINT rarely incurs legal issues. Since all information is already publicly available, there is no worry of copyright infringement. Of course, there are grey areas, so it is still important to be cautious. [18]

In the field of cyber security, OSINT can be instrumental in conducting post-incident analysis and investigations. By leveraging publicly available information, it can help with the reconstruction of the timeline of events, the identification of the attack vector, and tracing the origin of the attack. This information not only helps in understanding the incident's scope and impact but also aids in attributing the attack to specific threat actors or groups. [35]

Gathering information with OSINT is usually done secretly to avoid revealing the searcher's identity. Even when conducting OSINT, the searcher leaves behind trace which could in turn be traced back to them. Because of this, it is best practice to use so called sock-puppet accounts when searching for information. These accounts are created in a way that they are not traceable back to the searcher. If done correctly, this means using separate hardware, a VPN and other countermeasures to prevent revealing anything about the searcher's identity. [27]

2.3. Behind the INT Acronyms

Due to the sheer number and size of the various fields requiring their respective experts, more names became established. While everybody can practise OSINT, some OSINT tasks benefit from experts analysing the data. Mapping a mountain by experts might deliver not only better, but even more information as they are more likely to comprehend found data and adjust their methods and searches to it.

To get an idea of the subcategories there are, some examples are highlighted below.

- Open Source Intelligence (OSINT)
- Geospatial Intelligence (GEOINT)
- Human Intelligence (HUMINT)
- Imagery Intelligence (IMINT)
- Signals Intelligence (SIGINT)
 - Communication Intelligence (COMINT)
 - Electronic Intelligence (ELINT)
 - Foreign Instrumentation Signals Intelligence (FISINT)

2.3.1. GEOINT - Geospatial Intelligence

Mapping the world and being able to locate positions is in the realm of Geospatial Intelligence (GEOINT). The idea is to collect as much geospatial information in such a manner that it can be used to precisely locate positions on a map. The data collected can range from measured height differences to distance relations of objects or soil information such as Scotland's soil database. [36] [46]

2.3.2. HUMINT - Human Intelligence

Information received from humans during interviews or interrogations belong to the Human Intelligence (HUMINT) category. Colloquially, such human sources are called spies. The cooperation of these people with intelligence services is usually a secret and thus requires additional resources to keep it that way. [47]

2.3.3. IMINT - Imagery Intelligence

Imagery Intelligence (IMINT) revolves around satellite images and aerial views. Optical or infrared images can be analysed for known signatures or to monitor activities on the ground. [47]

2.3.4. SIGINT - Signals Intelligence

Intelligence on both raw data and products of its analysis is called Signals Intelligence (SIGINT). Three subtopics exist called Communication Intelligence (COMINT), Electronic Intelligence (ELINT) and Foreign Instrumentation Signals Intelligence (FISINT). COMINT puts the focus on the content of transmitted messages. ELINT specialises on geolocation of foreign electromagnetic signals. For example, radars or radioactive materials. FISINT deals with signals created while deploying systems through telemetry or beacons. [11] [9]

2.4. A Picture is Worth a Thousand Words

A picture can feature landmarks, buildings, flora, fauna, people and a lot more. Every single one of these objects can give away information. The objects stand in relation to each other since they were photographed at the same time and from a specific position. Thus, they are linked by a photo or video.

2.4.1. Coordinates

Geolocation is a fundamental part of image analysis. The best way to accurately describe a location anywhere in the world is with the geographic coordinate system. This system uses latitude and longitude to describe a point on earth. In the ISO 19111 standard, additional geodetic datums have been added as well to account for the more elliptical shape of the earth. [23]

2.4.2. Landmarks

Localisation of a spot can be done by identifying landmarks and comparing angles. While this can be done by hand, today there exist many algorithms in machine learning to help find results quickly. However, it is not yet a solved problem, as there are annual competitions to find new and improved machine learning algorithms for this problem. [26]

2.4.3. Distances

It is possible to calculate the distances in a picture provided you know the size of two objects in said picture. It is also possible to calculate the distance based on the size of one object and the focal length to the image alone. [29]

2.4.4. Roads and Signs

Just by looking at a road, it is possible to narrow down the location of an image. There are two main factors that go into this: the condition of the road and the line markings. The condition can be an indicator to the wealth of a country. The richer the country, the better maintained the road. The line markings are also different all across the world, making it easier to make an educated guess about the region using the map in figure 2.1. [22]

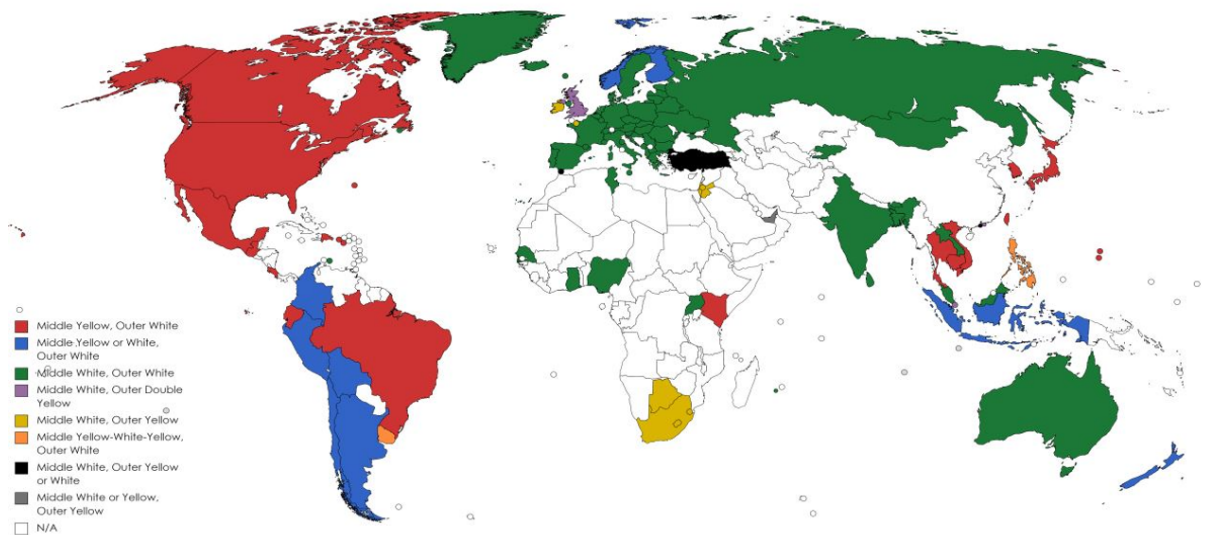


Figure 2.1.: Road line markings around the world [22]

The road signs can also give an indication as to where a picture was taken. Not only do road signs sometimes contain written text which reveals the language and sometimes even the name of a city, but also the shapes and designs of the signs are different all across the world. Even within a country the signs can sometimes look completely different depending on where you are, as shown in figure 2.2 below of highway signs in the United States of America. [22]

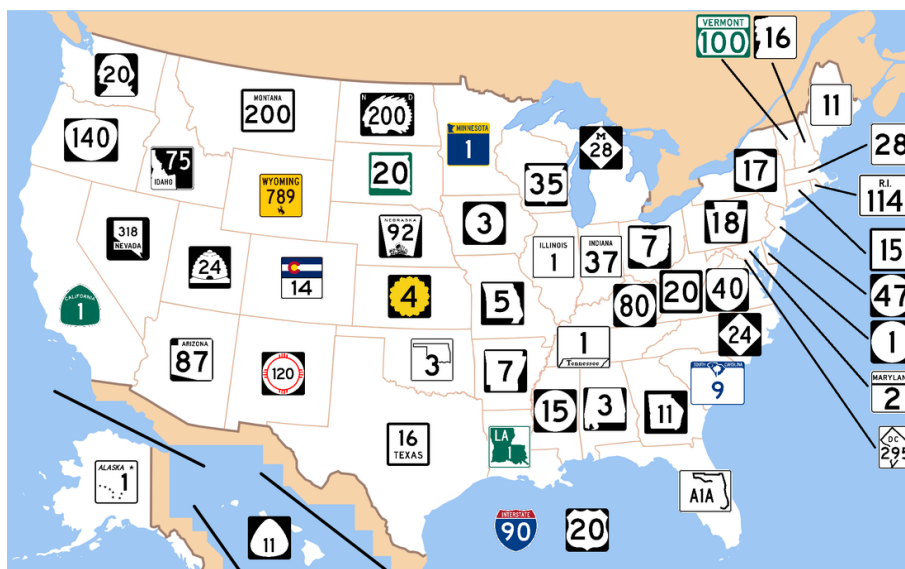


Figure 2.2.: North American state highway signs [22]

2.4.5. Cars and Plates

When a picture shows cars on the road, it is possible to narrow down the list of possible countries depending which side of the road they are driving on as seen in Figure 2.3. In addition to that, the make and model of the car can be an indicator to the country as well, as different kinds of vehicles are more popular in some countries compared to others. [8]

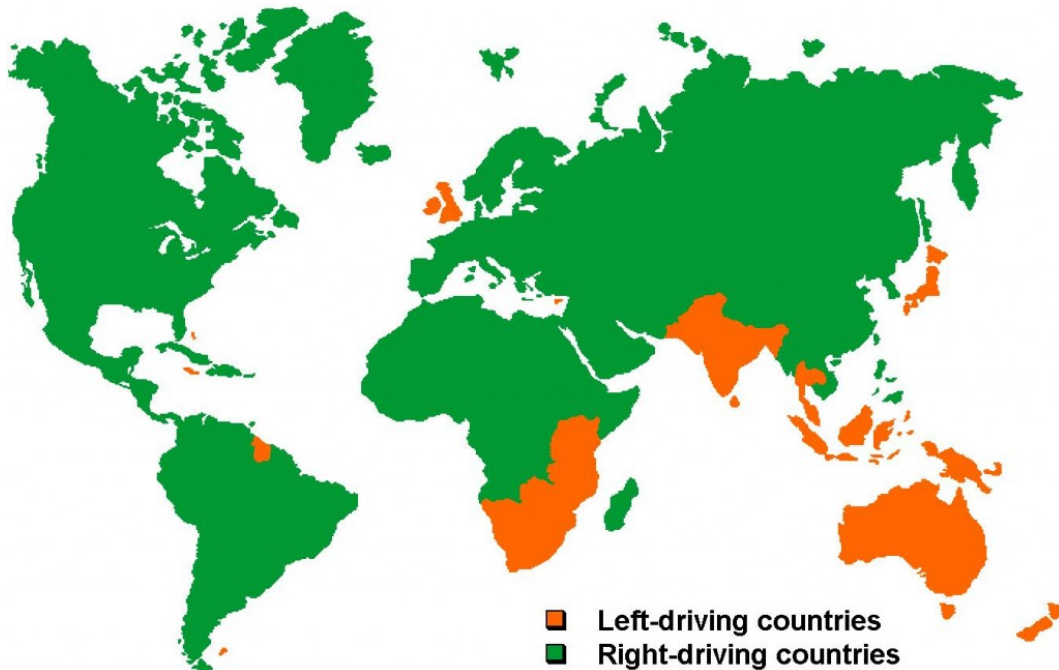


Figure 2.3.: Distribution of left and right side driving [8]

The colour, shape and position of a license plate can also be used to determine where an image was taken, even if the license plate is blurred for privacy reasons. For example, if a car does not have a license plate at the front, it is possible that it belongs to a car registered in the southern United States. [22]

2.4.6. Houses

The architectural style of houses can indicate both the location and the time in which the house was built. In combination with the condition of the house in the picture, it is possible to make an educated guess as to the picture's time and location. [22]

2.4.7. Flags

Although a country's flag may be obvious, there are also a lot of smaller flags that may be visible, for example a canton in Switzerland or a state flag in the United States of America.

2.4.8. Flora and Fauna

Flora and fauna are a good indication for geographical regions. The ability to identify species and their habitat allows the search area to be narrowed. For example, if there is a monarch butterfly in the picture, there is a high chance this picture was taken in the summer in North America because of the butterfly's lifecycle and natural habitat as seen in Figure 2.4. [43] The same strategy can also be pursued with plants. A picture with birch trees will most likely have been taken in the northern hemisphere, as birch trees naturally only occur there. [1]

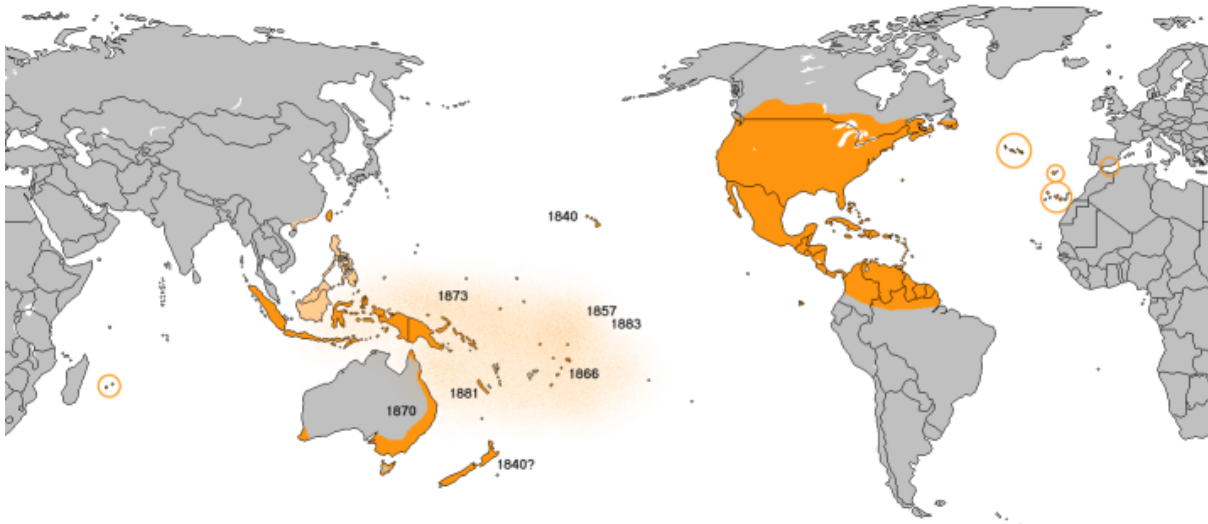


Figure 2.4.: Occurrence of the Monarch Butterfly [43]

2.4.9. Biometrics

Photos can also be used to acquire biometric information. If a picture's resolution is high enough, the extraction of fingerprints, irises, and veins could be possible as suggested in [12] and [19].

2.4.10. Others

The list of possible things that can be identified in a picture and that can give a clue as to where or when the picture was taken is almost endless. Utility poles, for example, can indicate a region as they vary in structure, materials, coloring, and guardrails. There is a wealth of data sets available for different characteristics around the world [39] and even country-specific ones [40].

2.4.11. Metadata

Metadata is information added to a file beside its actual content. It can hold information about the file, like timestamps on creation or modification. It can also include information on the software used to create the file or the hardware involved. The metadata standard applied usually depends on the file type.

The Exchangeable Image File Format (Exif) format was standardized to store information of the picture creation such as camera settings, GPS coordinates, date, time, image metrics, and more.

The Multimedia Description Schemes of MPEG-7 defines metadata structure for audio-visual content. [31]

2.4.12. Reverse Image Search

Reverse image search engines such as Google Lens [42] or Yandex Images [48] rely heavily on machine learning to filter out certain features of an image and provide the user with similar images. Ultimately, however, it is still up to the user to decide whether the search engine results are really what the user is looking for and whether the image the user uploaded matches the feedback from the machine learning algorithms. It is also the user's job to tell the reverse image search engines what to focus on in the image. Sometimes focusing on specific excerpts can lead to very different results than those reached when the entire image was given as input.

2.5. Information About Businesses

Information on business can help with tracking a local market or finding out more about a potential competitor.

2.5.1. Online Presence

Most businesses in the modern age have some form of online presence. This presence can come from the business itself, but also from third parties talking about the business. Information about businesses can be connected with other information to get a more complete picture about an event or a person.

2.5.2. Home Page

Already in 1997, more than two thirds of Fortune 500 companies had their own website. This number has only grown the closer we get to the present. These websites are usually a platform for businesses to connect to their customers. It can show products, reviews and does not necessarily have to be used to conduct the business itself. For OSINT, it is always important to remember that this content has been curated by the business itself. [2]

2.5.3. Social Media

Social Media has also become more popular with businesses to promote their business and products. They can have an official account posting news about the business, but it is also not unheard of these accounts posting jokes to try to resonate with younger audiences. As with a business home page, this content is curated by the business itself, although it is not as closely controlled as the content on a home page. [6]

2.5.4. Commercial Register

The commercial register is a publicly available database for business information such as its name, the owners, its address or financial statements. It can be a great tool to find leads for connected people. [50]

2.5.5. Stock Market

The stock market can also be a tool to find out if a company has changed hands. It can also give a rough estimate how well a business is doing. [44]

2.5.6. News

It can always be an asset to follow the news, as information about a company could be contained in a news article. Since journalists have made it their job to find information and make that information publicly available, why not profit from their work? News, whether on TV, radio, in the newspaper or on the internet, can contain the information one was are looking for. Sometimes even passwords like during an interview with the French news program 13 Heures[14].

2.5.7. Reviews

Reviews are a great way to find out what the public opinion is about a company. Some sources for such reviews can be the google maps reviews for general reviews by whoever wants to write them, or there are also sites like Glassdoor which can give you insider information from employees who work or have worked there and write a review about what it is like working for this company. [41]

2.6. Information About a Person

Every time a person uses the internet, some traces are left behind for a skilled OSINT professional to find and link back to the initial person.

2.6.1. What defines a person

A person is a complex being, so it is only natural that there are many different ways of finding information. What is information that can help us identify a person? The following sections show a non-exhaustive list of personally identifiable information that is most relevant for OSINT. [32]

2.6.2. Names

Every person in our modern society has at least one name, most people have two or more. While this information may not be enough to unquestionably identify a person, it can give an indication for many different aspects such as gender, nationality or age. [4]

2.6.3. Date of Birth

The date of birth alone does not carry much information, as there are only 365 days to a year and a person only lives for around 71 years on average. [10] In combination with a name however, this has a high chance of resulting in a unique connection.

2.6.4. E-Mail Address

Since in modern society, most people have multiple E-Mail addresses, a single E-Mail address can hold more information than a name, such as a year of birth or a workplace. However, it can also contain less if it just consists of random letters or numbers. An E-Mail address does not have to belong to one single person, it could also belong to a company.

2.6.5. Tracking on Social Media

Social media can be a very good source of information when looking for information about people. However, that is not the only thing it can be used for. It also offers information about businesses, trends and events. Through social media, you can sometimes get a person's location, their friends and family, their home or work address and interests.

2.7. Other Information and the Internet

The internet is a vast place and information can be found about almost anything. You just have to know where to look.

2.7.1. Satellite Imagery

Satellites can provide important information about the weather and the global geography. Using satellites, it is possible to predict the weather on earth more accurately, as a lot of information that influences the weather can only be measured from space. [25]

2.7.2. Aerial Photography

Satellite images and images from general aerial photography are used for most modern maps in existence today. Online maps such as Google Maps are a useful tool to look at the world at a glance. However, it must be remembered that the images are not always up to date. It is enriched with data about public transport, businesses, hospitals and other public areas. The team of engineers at Google preserve and analyse datasets including historic and real-time data, which is what makes Google Maps so progressive and accurate. [21] Different map providers can give different results as seen in Figure 2.5 which can also be useful for OSINT.

2.7.3. User Created Content

Social media, forums and blogs are all examples of user created content that can be the source of information for anything and everything. This does not have to be restricted to the internet either. It can also be something like a flyer given to you on the street that contains information.



Figure 2.5.: Different maps from left to right: Satellites Pro [45], Yandex maps [49], Bing maps [38]

2.7.4. Databases

The community is a huge asset for all OSINT related information gathering. There are databases for everything imaginable. If you need information on a specific topic, there is bound to be someone who was already interested in that topic and has compiled a database for that for everyone to use. For example, there is a database for all airline tails [51]. This could be combined with the route the airlines fly to find out which airport a picture was taken at. [37]

2.7.5. Tracking Objects

Like with databases, tracking objects across the globe can be done by an official instance or just a community. Staying with the example of airplanes, it is possible to look up commercial flights on the official website of airlines, but for smaller planes which do not appear on public websites, the community can still be helpful like with plane spotters. [52]

2.7.6. Dark Web

The dark web can be used to access websites that cannot be found via the 'normal' internet. These websites are not indexed by search engines like google and can only be accessed when using specific browsers that routes traffic through a series of other users' computers making it more difficult to track. The dark web may be used for legitimate purposes, but also to conceal criminal and otherwise malicious activities. [16]

2.7.7. Analysis of Code

A lot of code has been made public on sites like GitHub. When cloning a repository, always make sure to double check the code to make sure you understand what it does, and no malicious lines have been added by a third party. GitHub also allows to check the commit history to see who committed which changes and with what commit message. Comments by other users can also be a great source of information. It is also possible to automatically scan a repository to find security vulnerabilities and coding errors. [30]

2.8. Just Some Text?

Text does not only contain the meaning of its words but also sentence structure, punctuation, spelling errors and statistical information on frequency of letter, word or structure usage.

2.8.1. Fonts

Used fonts can also narrow down document creation dates as it was used 2017 in an incident called Fontgate where a document was predated to a date the used font was not created jet. [17]

2.8.2. Writing Style

The writing style of a text can give context clues as to when, where and for what purpose a text was written. It is also possible to identify the author of a text to a certain extent, given there are enough samples. [5] [13]

2.8.3. Meaning

Words can have different meaning depending on the context used. Therefore, it is always important to know in which situation or which circumstances a sentence or text was written. It is also important to remember that written text sometimes does not have the context clues that spoken language does. Consequently, it is more difficult to express feelings like sarcasm, although there exist projects to detect sarcasm in text. [15] There is also the possibility of a secret language, where different words have other meanings than what is written in the dictionary. [20]

2.8.4. Translation

When translating text from one language to another, some of the meaning can be lost. This is especially true for automatically translated text with translation engines like Google Translate. While automatic translation - even from images - can be helpful, it is important to remember that a translation can vary depending on the translation engine used. Even when people translate text, the translation can look different depending on the knowledge level of the translator. [7]

2.9. What does this mean for OSINT?

Since so many different things can provide almost endless amounts of information about a subject, it is only logical that many databases have been created to try and make the use of said information easier. It almost seems like for every aspect of information out there, there exists a database with information on that topic. On top of these databases many tools were created. Hence conducting OSINT to find new OSINT tools is a good idea when one starts with OSINT for the first time.

CHAPTER 3

Requirements

3.1. Challenge Requirements

The Hacking-Lab challenges created during this thesis fulfil the here described requirements.

Target Audience

Computer science students were selected as target audience. The challenges shall be suitable for lectures at OST.

Written Language

English will be the language of choice. It is the universal language for everything computer related. This includes the terms used in OSINT.

Programming Language

Python will be the programming language of choice. It is taught at OST in the first semester and besides that widely used for small scripts.

Time Expenditure

The students are expected to work either alone or in groups of two. In both cases a challenge should not require more than 45 minutes to be solved. Frequent rewards should be preferred over tedious and time-consuming tasks.

Exercise Grading

To track the students' progress the usage of flags is desired. Write-ups can be used as a second element of the solution since they provide more detail and can contain descriptions of the thought process.

Platform

The Kookarai Pentesting Linux is the reference platform. Every challenge must be completable using Kookarai. Additionally, students solving the challenges should be able to freely choose which operating system they use without any disadvantage. If a challenge is bound to a platform either by the software needed or the description of the steps, it has to be stated in the title of the challenge and contain an explanation in the description.

Maintainability

Challenges should be as sturdy over time as possible. Artefact maintenance shall not be a routine task to keep the labs working.

Content Restriction

Challenges must not feature content like drugs, nudity, human exploitation, violence, death. It is also prohibited to gloss over or encourage crime.

Challenge Structure

The structure of the challenge and its description shall be uniform in all the challenges and in accordance with the official Hacking-Lab challenge structure requirements[33].

3.2. Lecture Requirements

This chapter describes the requirements for a future lecture on the topic of OSINT which shall be held before the Hacking-Lab challenges created during this thesis are given to the students.

Scope

An integration into an existing cyber security module at OST seems fitting. It might also be beneficial for the general computer science student at OST, as the Hacking-Lab challenges teaches basic ideas, tools and techniques of OSINT which can be useful in daily life.

Duration

The lecture shall take the standard 90 minutes with at least 90 minutes of exercise sessions and additional time as homework.

Content

The lecture shall teach the basics of OSINT and should include following parts in order to prepare the students for the challenges.

Introduction

In the introduction, OSINT is described and its importance for the field of cyber security it shown with the help of some examples or personal anecdotes. It should describe the benefits and use cases of OSINT and how it has evolved over the years. It shall also include the definition and usage of a sock puppet for conducting research.

Tools and Techniques

Several of the most useful tools and techniques shall be shown. These should include the most useful techniques like google dorking and the most well-known tools like google lens, but could also show some lesser known tools and techniques the lecturer might find interesting. A select few tools and techniques shall be shown in practice, while others can just be mentioned in slides or by name. At least some of the tools that are used for the upcoming exercise session should be mentioned.

Practical Example

The lecturer shall choose an interesting challenge to solve collaboratively in class. This challenge could come from this thesis but also from the twitter bot or just a challenge found online. The challenge should promote creative thinking and show the power of OSINT. If the class is willing and there is enough time, it is also a possibility to search for information on a specific student just to show what can be found online.

Outlook and Resources

In the final part, should reiterate the importance of OSINT and give students resources to solve some challenges on the internet. Some examples are the OSINT twitter bot or more well-known internet sites where challenges can be found. It should motivate the students to try to solve some challenges in their free time. In the next lecture, the lecturer can ask the students if they have solved any additional exercises and if they are willing to share their experiences.

The Tale of Stories and Doings

This chapter covers the process of preparation and decision making with the goal to select ten stories and fitting doings.

4.1. Definition

At the beginning there were ideas. Every idea was categorised in either a story or a doing which are defined as follows:

4.1.1. Doings

A small task is called a doing. It describes a single step like analysing something for certain features. Some doings require very little time like reading a file's metadata, while others can result in very time-consuming tasks, like searching for a specific file on the internet.

4.1.2. Stories

A story describes the subject area of the narrative. It gives the challenge a meaning, such that doings are not strung together without reference. A story should also provide some motivation on why one should complete all doings and thus finish the challenge successfully.

4.2. Design Workflow

The workflow of the story creation and rating process consists of various consecutive and parallel tasks. It is visualised in Figure 4.1 and starts with the parallel task of brainstorming story and doing ideas, follows up with creating a match between the two groups. After categorising the stories and rating the doings the weight of each story idea is calculated. With this preparation ten stories were selected to be implemented as Hacking-Lab challenges.

4.3. Creation

Both stories and doings were compiled by both team members. The ideas came from various sources such as newspaper articles, documentaries, challenges once seen, interviews conducted and pure creativity. Only ideas contradicting the requirements were discarded. Table 4.1 lists the attributes for doings and stories which were used as a base for discussions during later steps.

Eventually, 22 doings and 16 stories were created and are shortly described in Table 4.2 and Table 4.3.

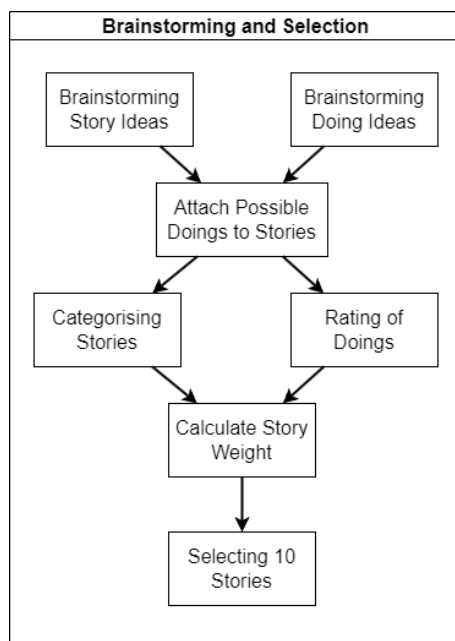


Figure 4.1.: Workflow of the story selection procedure

	ID	Description	Technical Needs	Arguments in Favour	Opposing Arguments	Related Doings
Doing	D00	Yes	Yes	Yes	Yes	No
Story	S00	Yes	No	Yes	Yes	Yes

Table 4.1.: Attributes of doings and stories

ID	Short Description
S01	Online scam investigation
S02	War in Ukraine
S03	Ransomware investigation
S04	Analyse trustworthiness of an internet post
S05	Investigating illegal waste disposal
S06	Authenticity of a job advertisement
S07	Anonymous informant's trustworthiness
S08	Business expansion
S09	Lobbying
S10	Blockchain analysis
S11	Investigating a car's history
S12	Investigate a company conglomerate
S13	Fraudster behind a pseudonym
S14	Gamer behind a pseudonym
S15	Analyse third party software repository
S16	Find a trustworthy key service abroad

Table 4.2.: List of stories

ID	Short Description
D01	Extract metadata from document
D02	Rate persons trustworthiness
D03	Detect usage of specific software
D04	Identify organisation structure
D05	Translate text
D06	Determine attacker by used methods/tools
D07	Obtain word dictionary
D08	Track physically moving object
D09	Image content analysis
D10	Create sock puppet
D11	Dark web research
D12	Video content analysis
D13	Find company balance
D14	Extract password from firmware
D15	Identify a company's IT partner
D16	Find contact information of person or position
D17	Find information about person
D18	Find information about company
D19	Examine older version of website
D20	Reverse image search
D21	Using advanced search features
D22	Locate position using map or satellite image

Table 4.3.: List of doings

4.4. Matching

At this point the doings were assigned to stories where they seemed reasonable or potentially doable. For example, it seems reasonable to assign the doing D11 *Dark web research* to the story S03 *Ransomware investigation*, but not the doing D14 *Extract password from firmware*. The result of all matchings can be seen in Figure 4.2. A story with more matchings has a higher flexibility as the creator can pick from a broader pool of doings to implement. Therefore, a coherent storyline is an expected target.

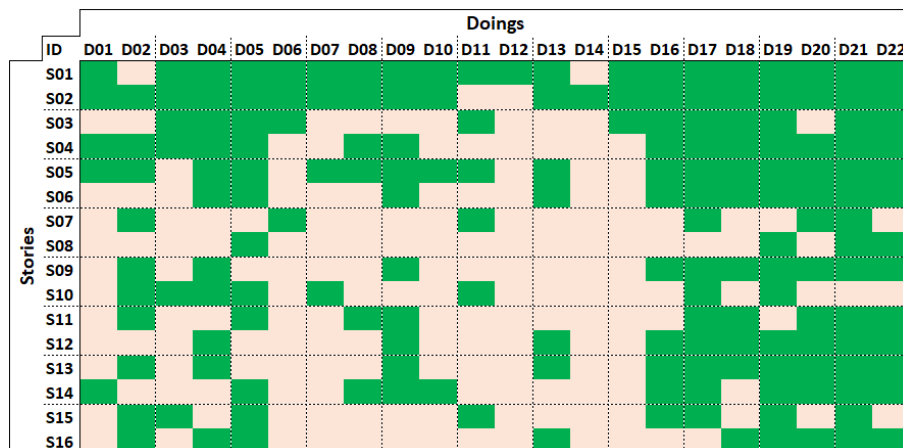


Figure 4.2.: Matching between doings and stories

4.5. Categorisation and Rating

To thin out the list of ideas, both stories and doings, a workshop with both team members and the stakeholder Ivan Bütler was set up. Each doing was introduced, discussed and then voted upon. In accordance with the Swiss democratic spirit, all participants had one vote and thus equal weight. Could no majority be reached, everyone was invited to explain their thinking and a discussion was started before the next ballot was held.

4.5.1. Categorising the Stories

All stories were categorised in one of five groups as shown in Table 4.4. Each group revolved around a question which should be answered in the story. The categorisation was introduced to guarantee a broader variety of storylines and to avoid an outcome where all challenges followed a similar question. It was expected to be too boring to only search for people in all the challenges.

Who is behind it? (Single person)	Who is behind it? (Company and people)	Verify authenticity	What happened?	Unsuited for target audience
S07	S01	S02	S03	S08
S14	S04	S06	S05	S09
S15			S10	S12
			S11	S13
				S16

Table 4.4.: Categorised stories

4.5.2. Weighting the Doings

Doings are weighted on how important the task and the learned knowledge is for a computer scientist. The scale applied ranged from 3 (very important) to 0 (better suited in other labs or for other target audiences). The distribution of weights is shown in Table 4.5. The weighting was conducted during the same workshop as the categorisation of the stories. Each person brought in work and school experiences as well as the research conducted up to this point.

Weight 3 (very important)	Weight 2	Weight 1	Weight 0 (unsuited)
D01	D06	D03	D04
D02	D11	D07	D10
D05	D19	D15	D13
D08	D22	D18	D14
D09			
D12			
D16			
D17			
D20			
D21			

Table 4.5.: Weighted doings

4.5.3. Rating the Stories

In an earlier step the stories got doings assigned which seemed reasonable or doable in the story. These assignments and weightings are now used for this next step.

So each story can include several doings weighted 3, some weighted 2 or 1 or 0. When all doings rated 3 were added up this sum was multiplied by 3. Then the 2-weighted doings were added and then multiplied by

2 and so on. These results were then summed up as the rating of the story. With this method a story gets a higher rating if it includes more high-rated doings than others.

An example of this calculation: the story S01 was matched with nine 3-rated doings, three 2-rated, four 1-rated and three 0-rated doings. Thus the story's rating is calculated with $(9 * 3) + (3 * 2) + (4 * 1) + (3 * 0) = 37$.

4.5.4. Selecting Ten Stories

The result of grouping, weighting and rating can be seen in Figure 4.3. The doings were matched as seen in Figure 4.2. A matched doing does not imply a required implementation. It is seen as a possible doing in this story and a final decision is made during the further story drafting.

Of the sixteen initial stories four were removed due to unsuited topics for computer science students. In addition, the two Blockchain like stories S03 and S10 were merged into S03. The S16 story was marked as an optional requirement.

ID	Story Description	Number of Doings of rating				Weight	Category
		3	2	1	0		
S01	Online scam investigation	9	4	4	3	39	Who is? (Company&Person)
S02	War in Ukraine	9	3	4	4	37	Verify authenticity
S05	Investigating illegal waste disposal	9	3	2	3	35	What happened?
S04	Analyse trustworthiness of an internet post	9	2	2	1	33	Who is? (Company&Person)
S14	Gamer behind a pseudonym	8	2	0	1	28	Who is? (Person)
S11	Investigating a car's history	7	1	1	0	24	What happened?
S03	Ransomware investigation	4	4	3	1	23	What happened?
S06	Authenticity of a job advertisement	6	2	1	2	23	Verify authenticity
S09	Lobbying	6	2	1	1	23	Unsuited
S13	Fraudster behind a pseudonym	6	2	1	2	23	Unsuited
S12	Investigate a company conglomerate	5	2	1	2	20	Unsuited
S15	Analyse third party software repository	5	2	1	0	20	Who is? (Person)
S16	Find a trustworthy key service abroad	4	2	1	2	17	What happened?
S07	Anonymous informant's trustworthiness	4	2	0	0	16	Who is? (Person)
S10	Blockchain analysis	3	2	2	1	15	What happened?
S08	Business expansion	2	2	0	0	10	Unsuited

Figure 4.3.: Stories ordered by weight

Challenge Documentation

The ten challenges shown in Figure 5.1 are described in this chapter. A brief description of the story and the various steps outlines the decisions made during the creation. The documented changes during the creation and already detected aspects which will probably require maintenance in the future are mentioned.

Each story has summative assessment questions which are expected to be answered by the students in their write-up. These questions are marked with circled numbers, like ①, ② and so forth, to be unique and thus distinguishable from step or hint numbering.

Pictures used in the challenges were selected to fit in at least one of the following categories:

- Licensed by the Hacking-Lab AG, like the small challenge pictures featuring AI generated detectives
- Public domain licensed
- Covered by Swiss Copyright law [24] Article 19, Paragraph 1, Literal b which allows work usage for educational purposes





















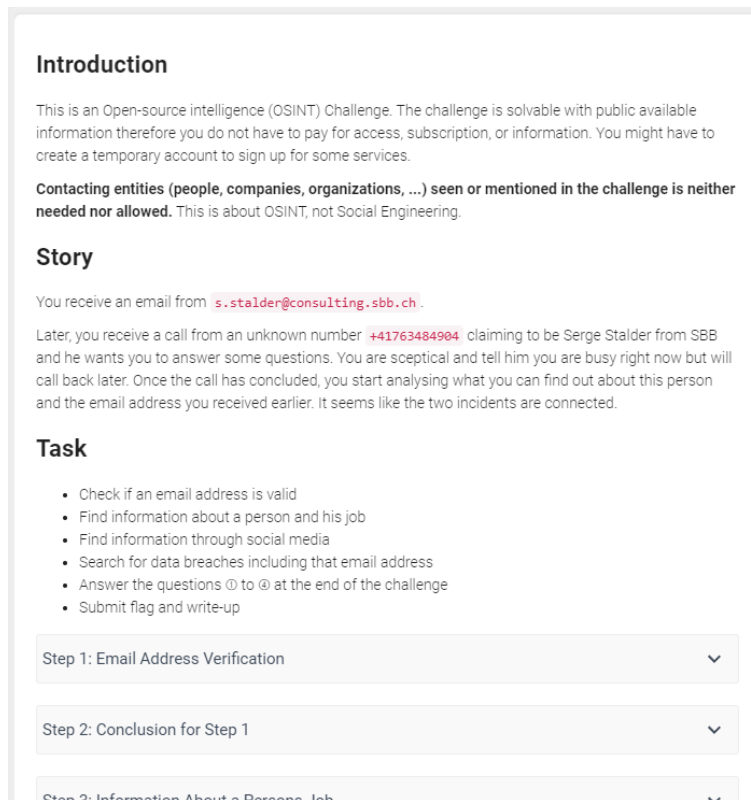
#	Name	Categories	Level	#	Name	Categories	Level
1	 01 - Scamming Personal Information b39b6263-141a-4fb0-8927-30201f0059b9		easy	6	 06 - Show What You Have Learned 69d55549-87ad-40fa-bb2a-08bee8fcd0d2		medium
2	 02 - The Propagandist's Information 825a0db6-5474-40d2-aa3f-2911e4e6c829		medium	7	 07 - Vulnerability Information 4543288b-540a-49be-8884-2b4873490c76		novice
3	 03 - Time for Waste 00dc1eea-5b05-4e04-ad34-9c0d3225c845e		easy	8	 08 - Run After Ransomware 330e164a-5b4a-4ce6-b1fc-79d2998ed956		medium
4	 04 - Validate Internet Post 88dfd5bc-aaa5-4c2c-84f6-8985dcb07bfa		easy	9	 09 - A Car's History 65033668-4b98-4b22-b790-1dbbee66a7e		novice
5	 05 - Third Party Software Contributions 8be49b45-5efe-490c-9477-5bb6808763a7		easy	10	 10 - Malicious Gamer 73e9cb77-ffid-43c4-883f-3141d8ee9e0d8		easy

Figure 5.1.: An overview of all ten challenges

5.1. Challenge 01 - Scamming Personal Information



Introduction

This is an Open-source intelligence (OSINT) Challenge. The challenge is solvable with public available information therefore you do not have to pay for access, subscription, or information. You might have to create a temporary account to sign up for some services.

Contacting entities (people, companies, organizations, ...) seen or mentioned in the challenge is neither needed nor allowed. This is about OSINT, not Social Engineering.

Story

You receive an email from `s.stalder@consulting.sbb.ch`.

Later, you receive a call from an unknown number `+41763484904` claiming to be Serge Stalder from SBB and he wants you to answer some questions. You are sceptical and tell him you are busy right now but will call back later. Once the call has concluded, you start analysing what you can find out about this person and the email address you received earlier. It seems like the two incidents are connected.

Task

- Check if an email address is valid
- Find information about a person and his job
- Find information through social media
- Search for data breaches including that email address
- Answer the questions ① to ④ at the end of the challenge
- Submit flag and write-up

Step 1: Email Address Verification

Step 2: Conclusion for Step 1

Step 3: Information About a Persons Job

Figure 5.2.: Hacking-Lab preview of Challenge 01

Meta Information

Desired Learning:

Be careful when accepting phone calls and answering email. Always double check to see if information given or requested is legit and if the person really is who they claim to be. The challenge also shows that even people who are not digital natives leave more traces on the internet than they themselves might suspect. It should raise awareness to what information can be found that might be unexpected. The challenge shows a different way of gathering information with just name and how one bit of information can lead to the next.

Time needed to solve:

30 - 45 minutes, derived from the average of the times taken by the test subjects.

Learning control:

A flag and a write-up is needed. The flag is the name of the company which probably dumped the waste illegally and is fictional. The write-up needs to answer the following questions:

- ① What are some methods to find out if an email address is valid?
- ② How did you find information about Serge Stalder. What sources did you use? Describe how you were able to find some answers in steps 3 onward.
- ③ How did you find his phone number? Did you also come across other phone numbers that can be associated with Serge Stalder?
- ④ Did the real Serge Stalder contact you and should you answer his questions?

Story Description

You receive a phone call and an email from someone claiming to be Serge Stalder. The goal is to find out information about this person ultimately deciding, if the person who contacted you is who they are claiming to be.

Steps

The steps are mostly built on each other. Each step is followed by another step containing hints to solve the previous step. The last step is a conclusion of the whole exercise.

Step 1: Email Address Verification

Build general knowledge of the different ways to check if an email address is valid. No link to a person yet in this step.

Step 2: Conclusion for Step 1

Shows four possible ways to check if an address is valid with the hint that more than one method should be tested because they could yield different results.

Step 3: Information About a Persons Job

Shows how much information can be found just on the business side of a person using search engines and social media. Since an account is needed to access some social media sites, a short instruction is given how to create a temporary account so that students do not have to use their own account or create a new one.

Step 4: Hints for Step 3

This step consists of two hints. Hint 1 directs students to social media to find information. Hint 2 directs them to hunter.io to find patterns of email addresses.

Step 5: Information About a Persons' Social Media

Asks students to find social media accounts as well as the email addresses used to sign up for the accounts.

Step 6: Hints for Step 5

Directs the students to haveibeenpwned.com which shows which email addresses were involved in data breaches.

Step 7: More Detailed Information About a Person

This step takes up the data breaches again, this time focusing on other data breaches than just the ones for social media.

Step 8: Hint

Hint that the phone number used for the flag is findable with hunter.io.

Step 9: Conclusion of the Challenge

Reiterates the importance of being aware how easy it is to leave a trail of information on the internet.

Adjustments During Creation

Initial Ideas

The first idea for this challenge was to find a phone number of some existing scammers online and track them through their website and maybe through their tools used. It became apparent that this approach only led to dead ends. Wherever a phone number was found which could be tied to a website, the website itself could not be tracked back to the scammers directly.

Another idea was to include a picture of a set of silverware a person wants to sell which is in reality just an item in a lesser-known museum. It would have been the student's job to decipher the inscription on the silverware to find the location of the museum. While this was interesting in practice, it also strayed too far from the original idea of trying to find out more information about a person or a business since after deciphering the name, the complete solution is trivial to find.

Adjustments due to feedback

When testing the challenge, the testers found other mobile numbers than the one needed for the flag which were not found initially. To make it more obvious which number was needed for the flag, the description changed indicating when this phone number was used and its second to last digit. The hint telling the user where to look for also came into existence as a result of the feedback.

The later testers also complained the temporary email services provided in the challenge did not work for hunter.io. This means in the short time since its creation and the later tests, the owners of hunter.io implemented a safeguard protecting against specific email addresses. In order to circumvent this, new temporary email services were evaluated and tested, and the links were replaced.

Lab Maintenance

Changing Data

Seeing that this challenge investigates a real person, the results of the analysis is subject to change depending on whether the affected person changes job, deletes their social media profile, or any other action that changes the information available at the moment.

External Websites

It should also be noted that this challenge relies heavily on third party sources. As already described in the previous section, it is possible that changes are made to how a website works, and information will maybe not be readily available anymore. It is also possible that websites themselves do not exist anymore.

5.2. Challenge 02 - The Propagandist's Information

Introduction


This is an Open-source intelligence (OSINT) Challenge. The challenge is solvable with public available information therefore you do not have to log in somewhere and certainly do not have to pay for access, subscription, or information.

This challenge is based on a real event. We have no proven information which tools or techniques were used, but we try to follow a path everybody could have followed to come to the same conclusion. After the incident there was a lot of media coverage, so you probably come across some articles or pictures. You can look at them, but you do not have to.

Contacting entities (people, companies, organisations, ...) seen or mentioned in the challenge is neither needed nor allowed. This is about OSINT, not Social Engineering.

Story

You come across an online image of a group of armed men posing in front of a building.



Your first thought is, they do not look like Ukrainian troops and... could it be that they took the picture in front of their accommodation?

Task

- Download the initial image seen above from [Resources](#) and start your analysis.
- Identify the journalist in the picture
- Geolocate the spot where the photo was taken
- Determine if the photo shooting was in the morning or in the afternoon
- Answer the questions ① to ④ at the end of the challenge
- Submit flag and write-up

Artifacts

- The photo to analyse: [C02 OSINT ORIGINAL Picture](#)

Step 1: Image Analysis

Figure 5.3.: Hacking-Lab preview of Challenge 02

Meta Information

Desired Learning

Open one's mind to see information hidden in plain sight. Search for information around images and their creator. Geolocate a position and determine the time of a picture. Stimulate a thought process of what information published images can reveal.

Time needed to solve

30 - 45 minutes, derived from the average of the times taken by the test subjects.

Learning control

A flag and a write-up is needed. The flag is the name of the journalist who published the picture. The write-up needs to answer the following questions:

- ① What does the unveiled guy from the image do for a living?
- ② Was the photo shooting in the morning or in the afternoon? How are you able to justify your choice? It is not required, but you might be able to narrow it down to a two-hour time frame.
- ③ At the time you saw the initial picture: What did you think was the information you could get out of it? Compare it with what you have found out at the end of the exercise.
- ④ Will you think of this exercise the next time you upload one of your photos on social media?

Story Description

An image of military personnel shall be analysed, and the ultimate goal is to localise the photo location and the time of the day it was taken.

Steps

The steps are mostly built on each other. Every step contains its solution at the end.

Step 1: Image Analysis

Write down information seen in the image, as the image does not contain useful metadata. One should train to analyse the content of an image and think of questions coming to mind.

Step 2: Conclusion for Step 1

In today's time images are barely studied in depth as the number of images is way too big and newspapers and chats create some sort of information overflow. The conclusion should give an idea on what information can be gathered. The range goes from basic information, like how many people can be seen to the conclusion that the picture is probably cropped as the picture's centre seems to be off.

Step 3: Reverse Image Search

Search for the image on the internet. There might be similar images or ones with a better resolution. Not every search engine will deliver the expected result and thus one has to know multiple tools for the same job.

Step 4: Conclusion for Step 3

This conclusion is to outline the benefits of multiple tools for the same job. One tool might not deliver the desired result and thus another has to be utilised.

Step 5: Identify the Guy

Identify the guy in the image. Search for the person's name. To find the initial creator or uploader of an information, in this case an image, is useful for checks on trustworthiness. In this step the name is just a data point to check if the initial social media post was found.

Step 6: Hint for Step 5

A hint directs the reader to news about the event as this incident spread quite far. The hint itself is probably not needed but keeps the structure of odd steps for questions and even steps for hints.

Step 7: Writing's on the Wall (Hard)

Try to identify the letters on the sign. They are in a foreign language and need translation. The language also uses the Cyrillic alphabet to make things harder. The incomplete picture of the sign and its blurriness increase the factor of difficulty. A first translation can be done which gives some meaning to the sign, with this information one can look for similar signs. With the similar sign the translation is easier. The combination of tools and the ability to check for other sources for the same information is the key learning here.

Step 8: Hints and Conclusion for Step 7

The text in the image is a bit blurry and written in Cyrillic. Text recognition is therefore hard even for native speakers. The hints are meant to lower the barriers one by one. The hints present a technique to recognise the letters, a similar placard in better quality and finally the text in Cyrillic is presented.

Step 9: Where was the Image Taken?

The sign mentioned an address. Locating the position on a map is still not easy. The street name is unknown to some Western map services and the house is not directly at that street. Hence the chosen tool has to be familiar with the region.

Step 10: Hint and Conclusion for Step 9

Most of the students are expected to use Google Maps which does not provide useful address location in this case. A hint directs them to other websites. The conclusion then gives concrete examples of various map services and the coordinates of the building in question. While this gives away part of the solution it helps students who are completely stuck to participate in the next step which provides interesting tasks and learnings.

Step 11: Was the Image Taken in the Morning or in the Afternoon? (Medium)

Determine the time an image was taken using information from the image like a shadow and a date. Not only is it necessary to identify a second image from the same photo shooting, but also that the second image features an information on the time it was taken, a shadow in this case. Determine the height of the building by finding a photo of it. To calculate its shadow length requires an open mind for new approaches.

Step 12: Hints and Conclusion for Step 11

The students might be lost on how to tackle this problem as it is not an everyday task. Therefore, the hints direct them toward the solution and show them how to find out where north is on the picture and how to calculate an object's shadow on a certain day of the year.

This peaks in the realisation that using two pictures of the same place it can then not only be geolocated, but one can also determine a time span when the pictures were taken.

Adjustments During Creation***Omitted Telegram Search***

At the beginning one step was planned to search on Telegram. This had to be cancelled for two reasons. Firstly, the journalist deleted his post and a search for it thus lapsed. Secondly during creation Telegram searches brought up various explicit content which was not appropriate. Both findings led to a move toward a search on news websites.

Lab Maintenance***Search Engine Adaption***

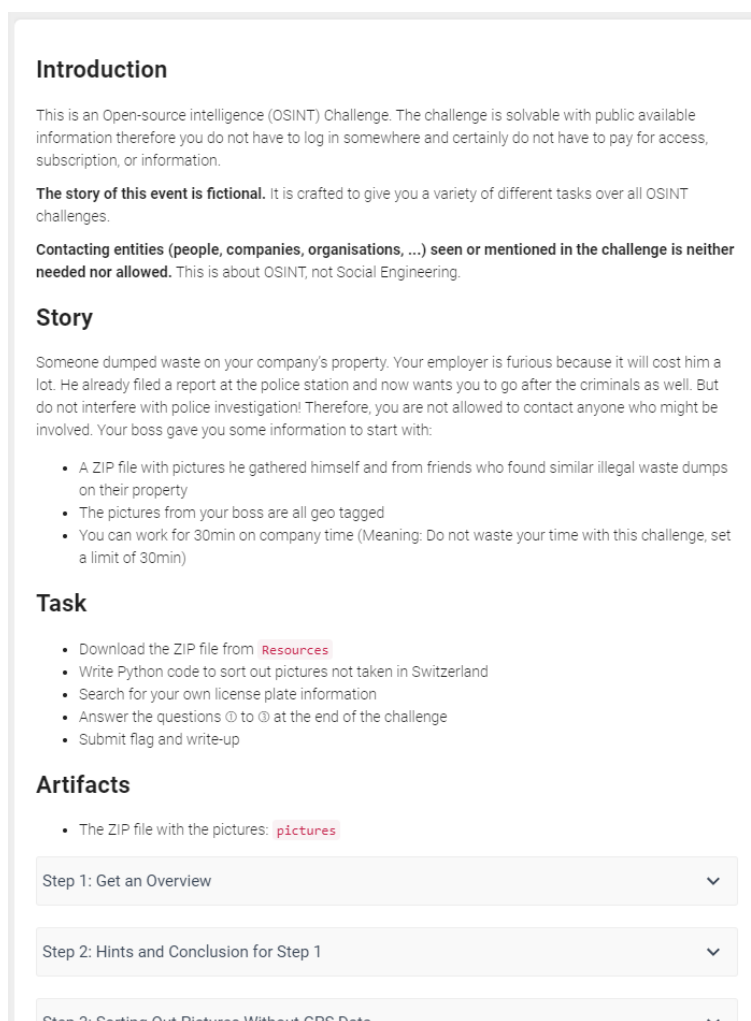
During the testing period a change in the results of the Google image search was recognised. Initially the cropped photo could not be identified, but over time there appeared some matches. This could nullify the main idea of the first step which was meant to show the difference between search engines.

Even if the image will be perfectly recognised the first step is not superfluous as a better and bigger version of the initial image has to be found.

External Websites

The challenge text, steps, hints and conclusions refer to external websites. It cannot be guaranteed that they do not change their functionality. To cushion possible changes no specific layouts or tasks on the sites were mentioned. Thus, an update of the lab is only needed for major functionality changes of these external sites.

5.3. Challenge 03 - Time for Waste



Introduction

This is an Open-source intelligence (OSINT) Challenge. The challenge is solvable with public available information therefore you do not have to log in somewhere and certainly do not have to pay for access, subscription, or information.

The story of this event is fictional. It is crafted to give you a variety of different tasks over all OSINT challenges.

Contacting entities (people, companies, organisations, ...) seen or mentioned in the challenge is neither needed nor allowed. This is about OSINT, not Social Engineering.

Story

Someone dumped waste on your company's property. Your employer is furious because it will cost him a lot. He already filed a report at the police station and now wants you to go after the criminals as well. But do not interfere with police investigation! Therefore, you are not allowed to contact anyone who might be involved. Your boss gave you some information to start with:

- A ZIP file with pictures he gathered himself and from friends who found similar illegal waste dumps on their property
- The pictures from your boss are all geo tagged
- You can work for 30min on company time (Meaning: Do not waste your time with this challenge, set a limit of 30min)

Task

- Download the ZIP file from [Resources](#)
- Write Python code to sort out pictures not taken in Switzerland
- Search for your own license plate information
- Answer the questions ① to ③ at the end of the challenge
- Submit flag and write-up

Artifacts

- The ZIP file with the pictures: [pictures](#)

Step 1: Get an Overview ▾

Step 2: Hints and Conclusion for Step 1 ▾

Step 3: Sorting Out Pictures Without GPS Data ▾

Figure 5.4.: Hacking-Lab preview of Challenge 03

Meta Information

Desired Learning:

Processing files depending on their metadata can not only be used in OSINT, but also in every company with huge amounts of data. To reduce the number of files which require further or even manual processing this can be a crucial part. In addition, it should rise awareness of databases maintained by governments: Namely the license plate database and the possibility to view people's tax declarations.

Time needed to solve:

15 - 30 minutes, derived from the average of the times taken by the test subjects.

Learning control:

A flag and a write-up is needed. The flag is the name of the company which probably dumped the waste illegally and is fictional. The write-up needs to answer the following questions:

- ① We used a very basic square to determine which points might be in Switzerland and which are outside. Name at least one software/library which can do much better.
- ② Assuming you found many license plates and you think of automating their queries on the official websites: Would this be clever, or could this have consequences? Explain your conclusion.
- ③ Could you view the most recent tax declaration of the company's boss using an official process? If so, explain how and if he could have had it blocked.

Story Description

One day an illegal waste dump appeared on the company's property. The task is to find the person or company responsible for this. The investigation starts with a folder containing many files the boss had already gathered. Mainly photos he found on the internet, got from friends with similar illegal waste disposal problems, screenshots of the company's surveillance cameras and random pictures seemingly unrelated.

After sorting out most of the pictures, the ones from the surveillance camera and some trash piles remain. With them the company dumping the waste can be identified. To complete the research a cantonal database for license plates should be searched to find information on a holder.

The task starts with the search for the needle in the haystack and ends with publicly accessible government databases storing personal information of its citizens.

Steps

The steps should be solved in a sequence, but it is not a necessity, as information retrieved during later steps is useful independent of the completeness of the python programme and vice versa.

Step 1: Get an Overview

The number of images is too large to handle them manually. It should encourage the students to automate some tasks. To do so some knowledge of the Exif format is required. This step is to familiarise the students with the Exif standard as this theoretical knowledge is required for further steps.

Step 2: Hints and Conclusion for Step 1

The first step may not trigger excessive euphoria in students. In an attempt to smoothen the transition from the theoretical preparation of the practical next step the hints give away some information to directly answer the question at hand.

Step 3: Sorting Out Pictures Without GPS Data

Knowing the standard, the students are now able to sort out some of the pictures. Namely the ones without GPS coordinates. The coordinates stored using the Exif standard are not in the format most maps use. Therefore, an existing method to transform the coordinates has to be created or a pre-existing one has to be identified.

Step 4: Hints for Step 3

Since the code framework given in the previous step was created with a certain library in mind, a hint gives away its name. It is not necessary, but it can prevent some students from drifting too far away with their own solution. The hint on different coordinate formats is meant for students who are not familiar with this subject and now have some words to search for on the internet.

Step 5: Sorting Out Pictures Abroad

A bounding box for the area of Switzerland has to be found. Either by approximation, measuring or by using knowledge found on the internet.

Step 6: Hint and Conclusion for Step 5

The hint is not essential but is used to give information to the students which otherwise might be overlooked. Other people had already taken care to define bounding box coordinates and even datasets with border coordinates are available. Last of which could be used together with Geopanda, a tool widely used in geography, to precisely determine whether a given coordinate lies within the border of Switzerland.

Step 7: Sifting the Remaining Images

The remaining photos show a street which story-wise leads to the company property and might thus show the vehicle dropping the waste. A reverse image search is required to identify the company logo of the vehicle with enough cargo space for the waste dumped.

The logo refers to a fictive company known from a video game and thus detectable by some wiki entry. Using the logo of a real company could lead to a defamation case which we wanted to avoid.

Step 8: Hint for Step 7

One of the problems with image recognition is the algorithms change over time and heavily depend on the input. The chances are that a student is not able to get a useful answer from those systems and would thus get stuck. The hint towards the game the fictional company in question appears in allows a manual search for the logo as the dataset is dramatically reduced.

Step 9: The License Plate

None of the license plates in the pictures is readable to enforce privacy. The student is asked to search his personal license plate number to avoid triggering anomaly alerts and to reduce the long-term maintenance of the challenge. A specifically selected license plate number might get an access restriction and the challenge would thus not work anymore. It is also possible that the license plate is registered by a new holder and thus creating a data privacy incident as we would expose a yet unknown entity.

Some cantons in Switzerland allow access to license plate registration data like the name of the person registering it. This step is meant to spread awareness of these databases and their publicly available information.

Step 10: Conclusion for Step 9

Similar to the variety of ways the different cantons use to publicly disclose license plate information the steps to protect one's own information are different. The conclusion is used to mention a few of these bureaucratic processes.

Step 11: Tax Declaration

The license plate database is not the only governmental database providing information about private individuals. Some cantons allow inspection of tax records of other people. Depending on the OSINT research conducted this could provide useful information. On the other hand, one might not want to share such information with one's fellow citizens and thus is made aware of one's situation by this step.

Step 12: Hint for Step 11

Changes in this domain might go undetected and thus change the students' answers over time. The hint therefore gives away an official link and an image of the current situation. This is done to reduce the maintenance needed for this step.

Adjustments During Creation**Flag Giveaway**

A first version mentioned the number of characters of the solution and thus allowed to skip the first steps since the flag could be found by crosschecking a list of company names from the Fallout game. The applied change thus clouded the flag format information.

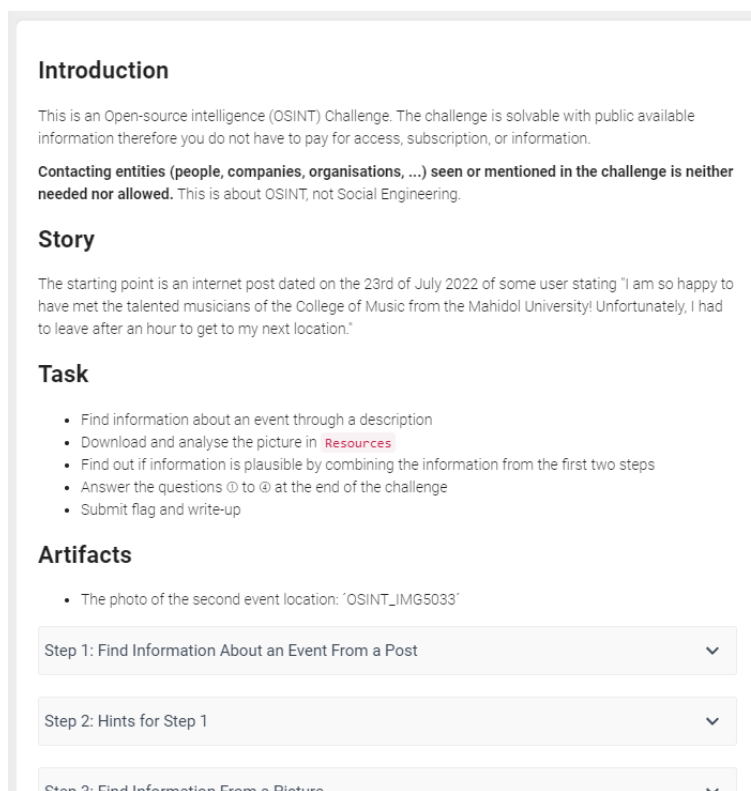
Governmental Databases

The addition of the tax declaration was not intended at first. With the incorporation of the license plate database, the question of whether there is not more private information being disclosed by government bodies became apparent. It was decided to include the possibility of inspecting tax returns, in the task as it is more of a surprise than finding one's name linked to a license plate.

Lab Maintenance

The stability of the challenge is expected to be high as the only external content is websites maintained by the Swiss government and thus expected to evolve very slowly. A reason for a faster change could be the upcoming data privacy regulation later this year. Depending on whether changes are made on the websites and to what extent the challenge might need some adjustments.

5.4. Challenge 04 - Validate Internet Post



Introduction

This is an Open-source intelligence (OSINT) Challenge. The challenge is solvable with public available information therefore you do not have to pay for access, subscription, or information.

Contacting entities (people, companies, organisations, ...) seen or mentioned in the challenge is neither needed nor allowed. This is about OSINT, not Social Engineering.

Story

The starting point is an internet post dated on the 23rd of July 2022 of some user stating "I am so happy to have met the talented musicians of the College of Music from the Mahidol University! Unfortunately, I had to leave after an hour to get to my next location."

Task

- Find information about an event through a description
- Download and analyse the picture in [Resources](#)
- Find out if information is plausible by combining the information from the first two steps
- Answer the questions ① to ④ at the end of the challenge
- Submit flag and write-up

Artifacts

- The photo of the second event location: 'OSINT_IMG5033'

Step 1: Find Information About an Event From a Post

Step 2: Hints for Step 1

Step 3: Find Information From a Picture

Figure 5.5.: Hacking-Lab preview of Challenge 04

Meta Information

Desired Learning:

Not everything you read on the internet is true. While this may seem obvious to most people working in IT, this challenge teaches how to find the relevant information to verify these statements.

Time needed to solve:

15 - 30 minutes, derived from the average of the times taken by the test subjects.

Learning control:

A flag and a write-up is needed. The flag is the name of the company which probably dumped the waste illegally and is fictional. The write-up needs to answer the following questions:

- ① What is the location and time of the first event?
- ② When did they leave to go to the next location?
- ③ Where and when was the picture in *Resources* taken?
- ④ Is the of the user plausible? Explain your reasoning with information you found in step 5.

Story Description

A post on social media claims to be at separate social events in a short timeframe. It is your job to verify if this is plausible.

Steps

The steps build on each other and should guide you through the task. Each step is followed by hints for the previous step. In the last step, results from the previous steps have to be combined to find new conclusions.

Step 1: Find information About an Event From a Post

Just given a description, students have to find an event taking place somewhere in the world. Since a search can yield multiple results, they have to find out which event is the most probable or if it even matters which event is the correct one for the following questions.

Step 2: Hints for Step 1

This hint describes that there are two events which fit the description and that it does not matter which one they want to follow up with for the next steps. This hint was added because students could easily get confused if it is important which event is chosen for the next step.

Step 3: Find Information From a Picture

Given just a picture, students have to find out where and when the picture was taken. This teaches them to look at several different sources and approaches to find information about the same picture.

Step 4: Hints for Step 3

These hints help students if they are stuck on a specific task giving ideas where else they could look for information.

Step 5: Combine Different Sources of Information to Reach a Conclusion

As described in the title, this step requires the solution of previous steps to answer the main question: Is it possible that the user making these posts really attended both events the way they described it?

Step 6: Hints for Step 5

These hints focus on the last question posed in the last step, because that is probably the most difficult one since it requires more information as to how flying private works.

Adjustments During Creation

User Feedback

It was not apparent at first that there are two events fitting the description perfectly. Since both of these events take place not too far apart from each other and they start at exactly the same time, nothing changed for the following steps. However, a note and hint was added that there are in fact two events that fit the description.

Lab Maintenance

Since this challenge focuses mainly on events from the past, not much should change for this challenge. Search engines alone are enough to solve this challenge and over time, depending on other events, only the difficulty of finding the relevant information should change.

Future Modes of Transport

In the future it could be possible that faster modes of transport are available, making the journey from one event to the other possible in the timeframe given. However, the results should not change, as the students would also have to find out when this faster mode of transport was created and come to the conclusion that this was not available at the time of this event taking place.

5.5. Challenge 05 - Third Party Software Contributions

Introduction

This is an Open-source intelligence (OSINT) Challenge. The challenge is solvable with public available information therefore you do not have to log in somewhere and certainly do not have to pay for access, subscription, or information.

This challenge is based on real events.

Contacting entities (people, companies, organisations, ...) seen or mentioned in the challenge is neither needed nor allowed. This is about OSINT, not Social Engineering.

Story

You are working as a software developer and your task for today is to analyse 3rd party software repositories your team thinks of implementing. Thus, you will analyse the `php` and the `colors.js` repository. May the writeup questions guide you, as your boss and your colleagues are very, very busy and cannot assist you.

Task

- Analyse the `PHP` and the `Colors` repository
- Answer the questions ① to ③ at the end of the challenge
- Submit flag and write-up

Step 1: Starting Sonatype Lift

Step 2: The PHP Repository General Analysis

Step 3: The PHP Repository Commits

Figure 5.6.: Hacking-Lab preview of Challenge 05

Meta Information

Desired Learning:

Third party software bears additional risks. To just look at the update frequencies and readmes is not enough to determine any sort of risk factor. Malicious code can be submitted with hijacked valid names or even by the original author. Code added to a software has to be reviewed and this is also needed for third party components.

Time needed to solve:

15 - 30 minutes, derived from the average of the times taken by the test subjects.

Learning control:

A flag and a write-up is needed. The flag is the name of the company which probably dumped the waste illegally and is fictional. The write-up needs to answer the following questions:

- ① How old is the PHP¹ repository and who is the owner? Is this repository a fork and if yes where from?
- ② Write down if you find something suspicious in the commits² between 2021-05-31 and 2021-05-27 and describe why.
- ③ What is *Zerodium*? Where does it come from and what does it do?

¹<https://github.com/php/php-src>

²<https://github.com/php/php-src/commits?after=0b4f83f68f93b2fc8fa164f4c8e3fb8cc8052c8c+0>

- ④ What are the dependencies and vulnerabilities found with Sonatype Lift?
- ⑤ Would you recommend the code of <https://github.com/Marak/colors.js> to your team and if yes under what conditions? Explain your reasoning.
- ⑥ Find the blog entry from 2021 and outline connections between its content and your findings from question ⑤.

Story Description

A software project would like to add the two projects *PHP* and *colors.js* to their code. They finally got the budget to have a look at these projects to determine whether it would really benefit their own project. The students receive the task to review the GitHub projects and deliver their suggestions to the rest of the team.

Steps

The steps build on each other and should guide you through the task. However, the solution can also be found without these steps.

Step 1: Starting Sonatype Lift

Sonatype Lift needs up to 15 minutes to inspect the repository given. The students are expected to start this process and then continue with the next steps in the meantime.

Step 2: The PHP Repository General Analysis

A first look should be taken at the metadata of the project. The owner must be determined to get an idea of whether it might be a trustworthy repository or a malicious fork. Depending on the outcome of this first check the later steps can be omitted and thus time is saved. Following a structured approach is the leading idea behind this step.

Step 3: The PHP Repository Commits

Once the repository seems to be the official one, a deeper analysis can be conducted. Instead of a full code review, which would obviously take way too long and cannot be expected to be done during this exercise, the focus lies on a handful of commits. The time frame of the commits to analyse is given and lies in the past to ensure a determined outcome. During this timeframe the repository was indeed attacked, and malicious commits were sent and merged. The students can therefore inspect a real attack.

Step 4: A Suspicious Commit

This step is meant for students who were lost and could not find the malicious code. It gives away the string to look at, which is also linked to one of the questions for the write-up.

Step 5: Sonatype Lift Report

In the meantime, the Sonatype Lift report might be completed and can now be analysed. This step is therefore meant as a reminder as now the related question can be answered. The report itself analysed the most recent state of the repository. Therefore, the report will change over time and different outcomes must be expected. Thus, the idea is to introduce a code analysis tool to the students and promote the idea to run them in order to detect bugs they overlooked themselves.

Step 6: Colourful

A second repository should be analysed, which was under attack as well, but this time the owner himself submitted the code. Many software projects wasted hours to find the bug in their code afterwards as too few checked the changes they merged.

Step 7: Prequel

At first the malicious commit in the colors.js repository was labelled by the owner as a test gone wrong. Conducting OSINT on his person reveals internet posts from the past which can be seen as a warning and contradict his theory of a failed test. The discovered information could therefore influence the decision whether to trust this person's code unseen in the near future or not. A code review therefore might benefit from a broader review.

Adjustments During Creation

No adjustments to the initial concept were made.

Lab Maintenance

Most of the research done for this challenge can be done on GitHub which is expected to last in the long run. The uncertainties are with the free-to-use status of Sonatype Lift and the private Blog used in step 7.

Sonatype Lift

The product is expected to remain free as nothing contradicting was published by the company. Nonetheless changes of plan can happen. As the software is not a critical part of the challenge it can either be replaced by another product or be omitted which would reduce the time needed for the challenge by approximately 5-10 minutes.

Private Blog of the Colors.js Owner

The blog has been operational for 10 years now and has changed its layout but not removed content. It is also archived by archive.org and thus the challenge could be updated with a hint for the archive to resolve issues of removed content.

5.6. Challenge 06 - Show What You Have Learned

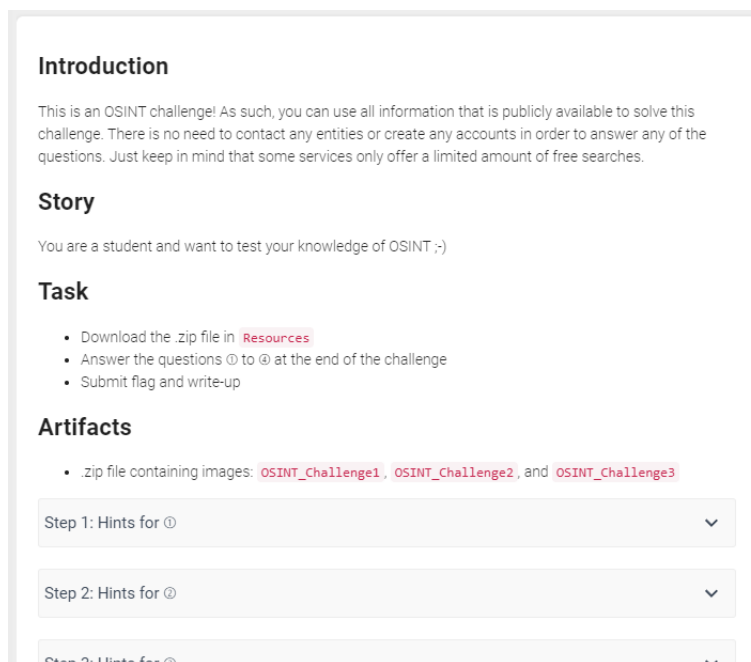


Figure 5.7.: Hacking-Lab preview of Challenge 06

Meta Information

Desired Learning:

Show what you have learned. This challenge combines several different topics and techniques learned in other challenges as well as introducing some new ones.

Time needed to solve:

15 - 30 minutes, derived from the average of the times taken by the test subjects.

Learning control:

A flag and a write-up is needed. The flag is the name of the company which probably dumped the waste illegally and is fictional. The write-up needs to answer the following questions:

- ① In the *OSINT_Challenge1* picture, what color were the flowers in the rightmost pot hanging from the lantern in August 2012?
- ② In the *OSINT_Challenge2* picture, what is the last name of this actress?
- ③ In the *OSINT_Challenge3* picture, what the last word on the sign this CCTV camera is mounted on (in 2018)?
- ④ Which degree course was first mentioned in the internal news after HSR became OST in 2020?

Story Description

You are a student wanting to practice your OSINT skills.

Steps

There are no steps guiding the students for this challenge. The hints are here to give the solution for each challenge in case they get stuck

Step 1: Hints for question ①

Teaches to look for clues in a picture and to look at history data on Google Maps.

Step 2: Hints for question ②

Teaches the use of Pimeyes and making decisions based on possibility of something being the correct result.

Step 3: Hints for question ③

Teaches to use of Insecam underlining the importance of data security of hardware connected to the internet. Requires creative thinking to open developer tools in the browser to get to an IP address. Also shows the use of shodan.io to find information about a domain.

Step 4: Hints for question ④

Teaches the use of archive.org.

Adjustments During Creation

The initial idea for this challenge was to create a fake job advertisement where students have to find out it is just a scam trying to get personal information. This idea was replaced with the current one for the following reasons: Even if we just included a picture of an advertisement from a newspaper, it would still have to include a name of a company or contact information. The first instinct of any cyber security professional would be to see what information is available on the internet about this company which means we would have had to maintain a whole fake website just for this one challenge and maybe even then, the website would be more difficult to find via Google and have little to no traffic because it is just a farce. It would also be maintained, which goes against our requirement of future-proof, low maintenance challenges.

User Feedback

At first the format of the flag was not really clear. An example was added to make it obvious what kind of input is expected.

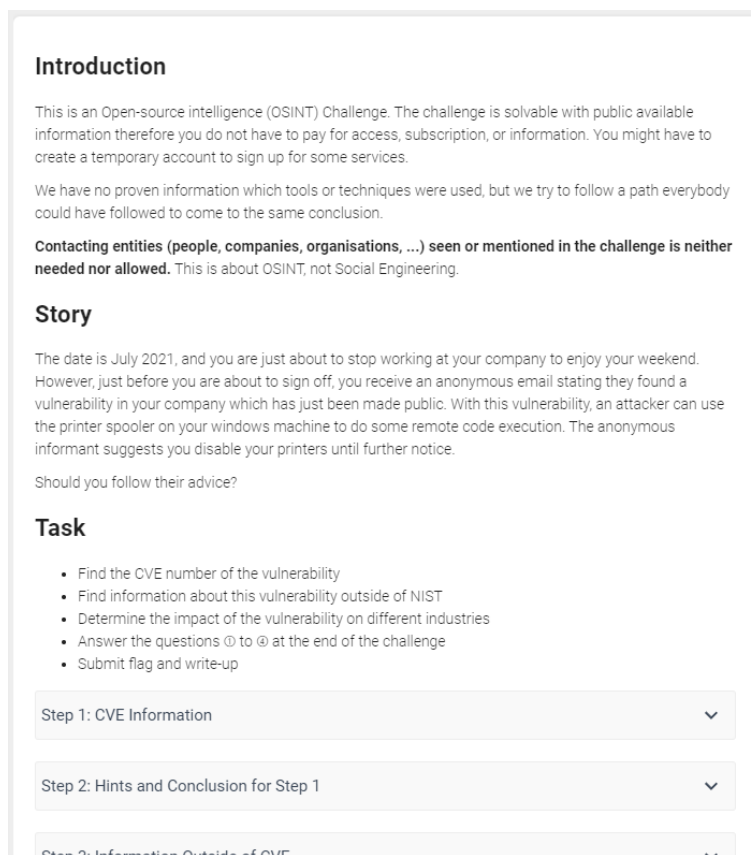
An additional paragraph was added stating that all questions except for ② can be solved without the use of reverse image searching. This was added in order to urge students to not always use the same tool to solve an exercise.

Lab Maintenance

Reliance on Third Party Services

Pimeyes, insecam.org as well as shodan.io are services that are available for free right now, but could charge for their use in the future. In the case of Insecam, it could also be that the CCTV camera is made safe and not accessible anymore from the web. If this was the case, the challenge description could be modified to also give the IP address to go on instead of just a picture.

5.7. Challenge 07 - Vulnerability Information



Introduction

This is an Open-source intelligence (OSINT) Challenge. The challenge is solvable with public available information therefore you do not have to pay for access, subscription, or information. You might have to create a temporary account to sign up for some services.

We have no proven information which tools or techniques were used, but we try to follow a path everybody could have followed to come to the same conclusion.

Contacting entities (people, companies, organisations, ...) seen or mentioned in the challenge is neither needed nor allowed. This is about OSINT, not Social Engineering.

Story

The date is July 2021, and you are just about to stop working at your company to enjoy your weekend. However, just before you are about to sign off, you receive an anonymous email stating they found a vulnerability in your company which has just been made public. With this vulnerability, an attacker can use the printer spooler on your windows machine to do some remote code execution. The anonymous informant suggests you disable your printers until further notice.

Should you follow their advice?

Task

- Find the CVE number of the vulnerability
- Find information about this vulnerability outside of NIST
- Determine the impact of the vulnerability on different industries
- Answer the questions ① to ④ at the end of the challenge
- Submit flag and write-up

Step 1: CVE Information

Step 2: Hints and Conclusion for Step 1

Step 3: Information Outside of CVE

Figure 5.8.: Hacking-Lab preview of Challenge 07

Meta Information

Desired Learning:

How to efficiently find information about vulnerabilities.

Time needed to solve:

15 - 30 minutes, derived from the average of the times taken by the test subjects.

Learning control:

A flag and a write-up is needed. The flag is the name of the company which probably dumped the waste illegally and is fictional. The write-up needs to answer the following questions:

- ① What is the main CVE number of the vulnerability and when was it published?
- ② Determine the best workaround that does not include stopping all printing.
- ③ Find a code example that exploits this vulnerability.
- ④ Why did this vulnerability become such a big problem so quickly?

Story Description

You receive a tip-off about a new vulnerability so now you want to find out as much as possible about this vulnerability. When is it fixed. What are temporary measures to be taken until it can be fixed? How plausible is it that this affects your company?

Steps

The steps build on each other and should be solved accordingly, one after the other.

Step 1: CVE Information

Find a vulnerability by a description and a date. Since there are multiple vulnerabilities that could fit, the student has to decide which one is meant by the tip-off.

Step 2: Hints and Conclusion for Step 1

These hints are made to eliminate any uncertainty for when the student is on the right track.

Step 3: Information Outside of CVE

Find the best ways to deal with a vulnerability before it is patched, which is very realistic to happen in real life.

Step 4: Hints for Step 3

Knowing that there are separate official records of vulnerabilities can help find more information.

Step 5: Impact

Looking beyond official records is helpful to understand the impact a certain event has.

Step 6: Conclusion for Step 5

Gives a name of a ransomware group to do further research on if nothing else was found.

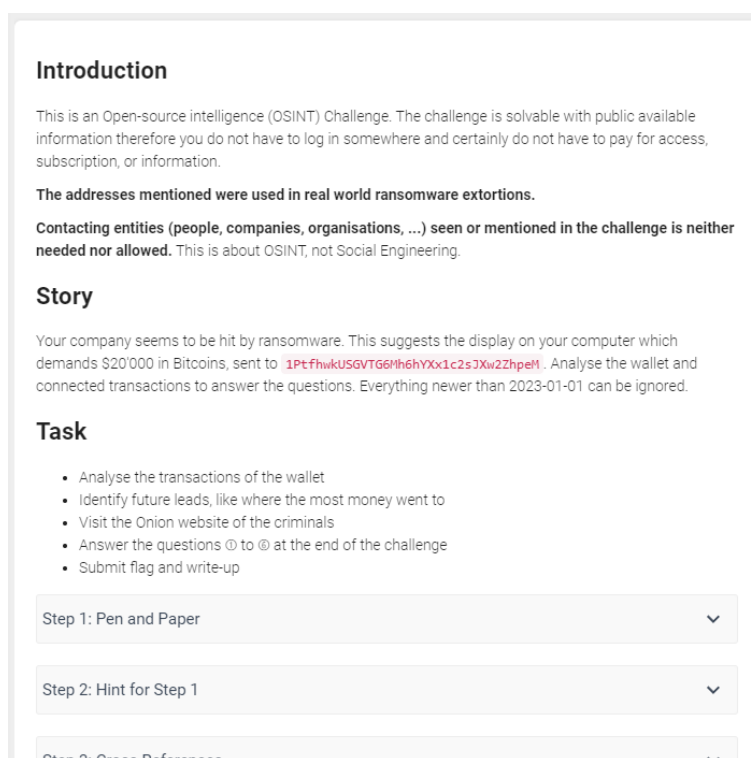
Adjustments During Creation

The only adjustments that were made were some clarifications where the wording was inexact.

Lab Maintenance

Since this challenge is purely based on historic events, no maintenance should be needed.

5.8. Challenge 08 - Run After Ransomware



Introduction

This is an Open-source intelligence (OSINT) Challenge. The challenge is solvable with public available information therefore you do not have to log in somewhere and certainly do not have to pay for access, subscription, or information.

The addresses mentioned were used in real world ransomware extortions.

Contacting entities (people, companies, organisations, ...) seen or mentioned in the challenge is neither needed nor allowed. This is about OSINT, not Social Engineering.

Story

Your company seems to be hit by ransomware. This suggests the display on your computer which demands \$20'000 in Bitcoins, sent to `1PtFhwkUSGVTG6tH6hYXx1c2s3Xw2ZhpEi`. Analyse the wallet and connected transactions to answer the questions. Everything newer than 2023-01-01 can be ignored.

Task

- Analyse the transactions of the wallet
- Identify future leads, like where the most money went to
- Visit the Orion website of the criminals
- Answer the questions ① to ⑥ at the end of the challenge
- Submit flag and write-up

Step 1: Pen and Paper

Step 2: Hint for Step 1

Step 3: Cross-References

Figure 5.9.: Hacking-Lab preview of Challenge 08

Meta Information

Desired Learning:

Transactions stored in the blockchain can be used to link contracting parties even after years. While it is out of scope and reach to identify each party it still gives hints on their activity. The goal is to compare the expectations with the real world.

Time needed to solve:

30 - 45 minutes, derived from the average of the times taken by the test subjects.

Learning control:

A flag and a write-up is needed. The flag is the name of the company which probably dumped the waste illegally and is fictional. The write-up needs to answer the following questions:

- ① Name the date of the first and last transaction involving this address. Are you able to spot a pattern in the transactions (holding the shares or fast forward)?
- ② Identify the wallet 1 hop away, where the largest share was forwarded to.
- ③ Identify the wallet 1 hop away, where most outgoing transactions from the initial wallet are linked with. Document your finding with a screenshot.
- ④ What services do the LockBit criminals advertise on their website?
- ⑤ Which country does LockBit name to be their current location?
- ⑥ Did the website match your expectations? Was there something that surprised you?

Story Description

The company finds itself with ransomware screens on their computers. Not much is clear, and the daily work cannot be done. Therefore, research on the new topic should be conducted. Analysing the wallet address and the ransomware gang's website might reveal new information.

Steps

The steps build on each other and should be solved accordingly, one after the other.

Step 1: Pen and Paper

Current websites analysing the blockchain for free mainly print its content as a table. The coin flow has to be tracked manually and possibly even with pen and paper as the websites do not offer such services for free.

Step 2: Hint for Step 1

Some sites provide some sort of report. As this service is not provided by everyone and is not located too prominently the hint points a finger on it. Sometimes the printable report is even more readable than the websites default layout.

Step 3: Cross-References

3D visualisation can reveal connections overlooked with the table representation. The gamification aspect also supports the motivation to explore, a core property when doing OSINT.

Step 4: Hints for Step 3

The hints given direct the students toward the desired target as there are so many transactions that getting lost in the data is just a matter of time.

Step 5: Visiting the Criminal's Website

While this is the only step mentioning the name of the ransomware gang, the challenge is solvable without the step as the Bitcoin wallet address can be linked to them when searching for it on the internet. A list of current onion addresses is also provided since a ransomware warning on a computer would feature it as well. Leaving it away completely would therefore break with the story.

Adjustments During Creation

The idea of a broader search through the darknet was planned, but was rejected later, as most sites which could have been incorporated into the story promoted many other crimes beside the ransomware topic. To promote criminal activities was never a desired effect of the challenges and thus the dark web research was limited to the site of the ransomware gang. While a broad dark web research would be an interesting topic this challenge setting is not the best framework for it as it might need closer care for the students conducting it.

Lab Maintenance

Blockchain 3D Explorer

The Blockchain 3D Explorer is a handy tool to inspect transactions in a joyful way. Its funding however is unclear even though the project has been up for 6 years. Should the website ever close down, it has to be replaced for this challenge as the visualised exploration of the blockchain is a key part of the challenge.

LockBit Onion Address

LockBit is a criminal organisation thus will be taken down for good at some point. This will mainly affect step 3 and questions regarding the LockBit website. Since the number of ransomware gangs is high it could be swapped with another gang's website. Changing the Bitcoin wallet address in earlier steps is optional but would serve the story.

5.9. Challenge 09 - A Car's History

Introduction

This is an Open-source intelligence (OSINT) Challenge. The challenge is solvable with public available information therefore you do not have to log in somewhere and certainly do not have to pay for access, subscription, or information.

This challenge is based on a real event.

Contacting entities (people, companies, organisations, ...) seen or mentioned in the challenge is neither needed nor allowed. This is about OSINT, not Social Engineering.

Story

You found a car dealership in Germany selling the car you always desired. A slightly used 2018 Audi RS5 for € 56'000. You inspect the car on site. It looks all clean and polished and it even got TUF (Swiss pendant is MFK, Motorfahrzeugkontrolle) recently. You decide to buy it and drive it back home.

At the border you hand over all documents you received from the dealer. The Swiss border custom still requests an EORI-Number you cannot find. None the less you are allowed to enter Switzerland with your new car, but you have to register it within 14 days.

You decide to go to your local mechanic and let them do it. They call you later and request you to look for more forms as the car could not be registered otherwise. These documents do not exist and now you want to know what happened.

Task

- Download the ZIP file from [Resources](#)
- Conduct a search for information on the car with the VIN number shown in the picture
- Answer the questions ① to ③ at the end of the challenge
- Submit flag and write-up

Artifacts

- The ZIP file `osint-pictures.zip` containing
 - The first image was taken from the car's driver door
 - The second picture is needed for step 3

Step 1: Decoding the VIN ▼

Step 2: Car History ▼

Step 3: A Detailed History ▼

Figure 5.10.: Hacking-Lab preview of Challenge 09

Meta Information

Desired Learning:

Understand vehicle identification numbers as possible starting points for OSINT. An OSINT task does not have to be on a person. Objects have a past, too and sometimes even a history which is accessible on the internet.

Time needed to solve:

15 - 30 minutes, derived from the average of the times taken by the test subjects.

Learning control:

A flag and a write-up is needed. The flag is the date on which the car was auctioned off. The write-up needs to answer the following questions:

- ① Describe the structure of the VIN number.

- ② The car was sold in the year 2019, but under what circumstances? Would you have bought the car if you had this information earlier?
- ③ Where does the information sold by websites like Carfax and AutoDNA come from?
- ④ Does a clean history (sold by those sites) guarantee that the car has had no accident resulting in a write-off?
- ⑤ Assume you found the container numbers *CLHU2158110*, *TGHU2918158* or *TEXU1070110* linked with the car. Is it possible that the car was shipped to Europe in one of these containers?
- ⑥ Add a picture of a (random) container with its number highlighted by you.

Story Description

A second-hand car was bought in Germany. On the way back home the Swiss border customs requested forms not present in the papers received from the seller. An internet search shall be conducted to find out where the car is from and what had happened to it.

Steps

The steps are independent and could theoretically be solved in a random order. Nonetheless it is structured to lead from the understanding of the VIN toward a lengthy car history report and thus creates some sort of leitmotif.

Step 1: Decoding the VIN

The VIN in full length can uniquely identify any car. It is structured and encodes country, company and name of the car's production plant.

Step 2: Car History

The search with the given VIN reveals a part of the car's story. Namely that it had an accident in the United States of America and was given the Salvage Certificate. Despite the write-off the car was auctioned off.

Step 3: A Detailed History

A detailed car history can only be accessed for money. To overcome this limitation this step uses an example report from one of the companies selling these. The original history has surprisingly many similarities with the example history. Both cars had an accident resulting in a write-off, were auctioned off, shipped to Lithuania, sold in Eastern Europe, marginally fixed and then sold a in Germany as second-hand vehicle in good condition. This is not an uncommon tactic and thus considered important learning. [28]

Step 4: Conclusion to Step 3

The conclusion is used to share information the students were not able to find online due to paywalls. It tells the story of the real buyer of the car who only found the true history of his car once he was denied registering his car.

Step 5: Your Car

While the chances are lower in Switzerland, thanks to the import regulations it might still be interesting to know what is publicly known about one's car. Thus, this step is meant for the students to find information on objects closely related to them.

Step 6: Container Tracking

Shipping containers have identification numbers as well and beside tracking their current or last travel it is sometimes possible to find their history from creation to decommission, too. To draw attention to these various identification numbers is one goal. Another goal is to crosscheck various clues the students receive to sort out false trails before following them too far.

Adjustments During Creation

Detailed History

During creation it became clear that with the requirements given a detailed history was not available. An account would have to be created and the report would have to be bought and was nowhere available for free. This alone would not have been a problem as the single information bits might be available as independent pieces. These pieces could complete the puzzle well and would even give a broader understanding of where information is collected and stored. Unfortunately, this information is not publicly available and thus not within the OSINT realm we set for these challenges.

The story was still considered interesting and thus an alternative history was needed. A surprisingly similar history report of the car was found in the example report given from one of the companies specialised in this type of information. The workaround to avoid the login and paywall thus is a reference to this example report. While this is not an ideal solution it avoids this topic going to waste.

Shipping Container

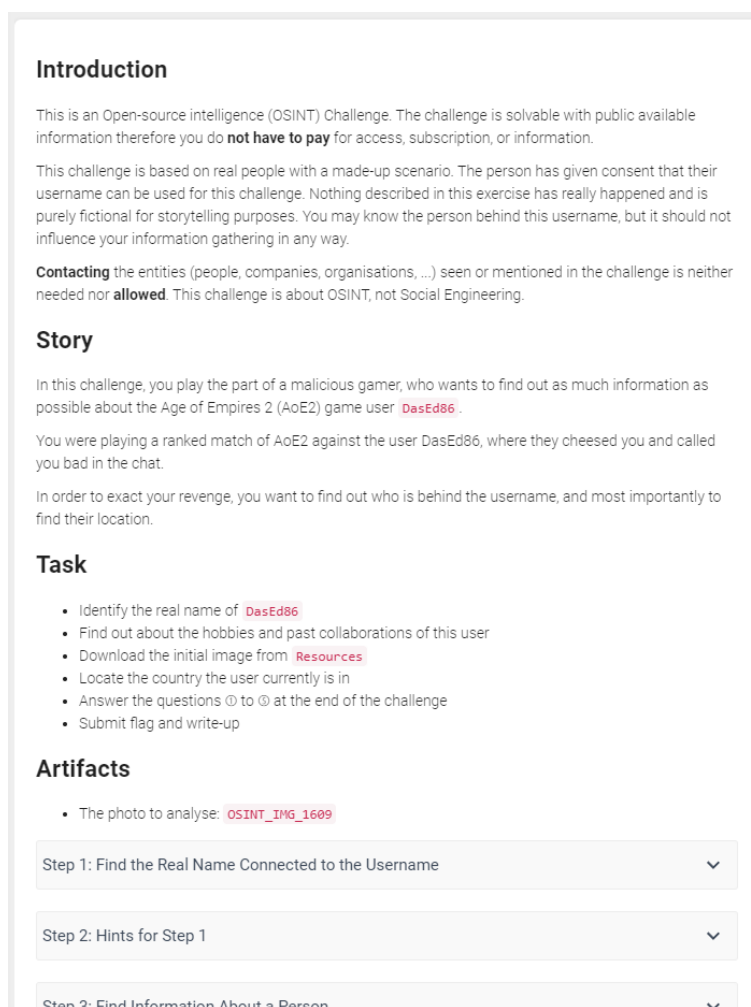
The blocked car history led to a much shorter challenge than expected. To counteract the tracking of three shipping containers was added together with the question whether one of them could have been used to transport the car over the Atlantic.

Lab Maintenance

External Websites

The challenge text, steps, hints and conclusions refer to external websites. It cannot be guaranteed that they do not change their functionality. To cushion possible changes no specific layouts or tasks on the sites were mentioned. Thus, an update of the lab is only needed for major functionality changes of these external sites.

5.10. Challenge 10 - Malicious Gamer



Introduction

This is an Open-source intelligence (OSINT) Challenge. The challenge is solvable with public available information therefore you do **not have to pay** for access, subscription, or information.

This challenge is based on real people with a made-up scenario. The person has given consent that their username can be used for this challenge. Nothing described in this exercise has really happened and is purely fictional for storytelling purposes. You may know the person behind this username, but it should not influence your information gathering in any way.

Contacting the entities (people, companies, organisations, ...) seen or mentioned in the challenge is neither needed nor **allowed**. This challenge is about OSINT, not Social Engineering.

Story

In this challenge, you play the part of a malicious gamer, who wants to find out as much information as possible about the Age of Empires 2 (AoE2) game user [DasEd86](#).

You were playing a ranked match of AoE2 against the user DasEd86, where they cheated you and called you bad in the chat.

In order to exact your revenge, you want to find out who is behind the username, and most importantly to find their location.

Task

- Identify the real name of [DasEd86](#)
- Find out about the hobbies and past collaborations of this user
- Download the initial image from [Resources](#)
- Locate the country the user currently is in
- Answer the questions ① to ③ at the end of the challenge
- Submit flag and write-up

Artifacts

- The photo to analyse: [OSINT_IMG_1609](#)

Step 1: Find the Real Name Connected to the Username ▾

Step 2: Hints for Step 1 ▾

Step 3: Find Information About a Person ▾

Figure 5.11.: Hacking-Lab preview of Challenge 10

Meta Information

Desired Learning:

OSINT can work both ways. Be aware of what information is available about you and how this information can be linked to your accounts and yourself and used against you.

Time needed to solve:

30 - 45 minutes, derived from the average of the times taken by the test subjects.

Learning control:

A flag and a write-up is needed. The flag is the name of the company which probably dumped the waste illegally and is fictional. The write-up needs to answer the following questions:

- ① What is the real name of the user *DasEd86*?
- ② Which country do they live in? Can you narrow it down to a region? Explain your reasoning

- ③ Who did they collaborate with in 2014 that went on have a fairly popular song (in Germany) in 2021?
- ④ Which country was the picture in *Resources* taken in?
- ⑤ What are the next flights landing in the user's home country from their current location? Include a screenshot of the flights

Story Description

You take the role of a malicious gamer who wants to find out information about their opponent in order to threaten them.

Steps

The steps build on each other and should be solved accordingly, one after the other, except for the step 5 which could be solved independently.

Step 1: Find the Real Name Connected to the Username

Find a persons' name starting with a username. This involves checking multiple sources to see if they line up and can connect back to the same user.

Step 2: Hints for Step 1

Sources to help finding information to connect to each other to verify that the name is correct.

Step 3: Find Information about a Person

Find more personal information, also digging through earlier versions of a website.

Step 4: Hints for Step 3

Sources for information in case students get stuck. Especially crucial is the hint about earlier versions of a website.

Step 5: Find Information About a Person's Location

Geolocation using an image is always useful and the most common challenge in OSINT.

Step 6: Hints for Step 5

Hints how to approach analysing the image in case reverse image search does not yield any results.

Adjustments During Creation

User Feedback

In the beginning the flag was just the user's real name. Since this was too easy, it was changed to the name of the person the collaborated with in 2014.

Lab Maintenance

Changes in the Personal Life

Especially for question ②, the answers could change if *DasEd86* ever changes job or moves away from where they currently live. The other parts of this challenge are future proof and require no maintenance.

To ensure the quality of each challenge a mandatory test routine was implemented.

6.1. Testing Procedure

Every challenge will be tested first by its author, then by the team partner and finally by a testing group, described in the next section.

The process follows an agile manner and creates continuous feedback which leads to improvements before entering the next stage of maturity. A challenge has to pass three stages consisting of a test by the challenge's author himself, then by the team member and finally by an external testing group. A visual representation of the testing workflow can be seen in Figure 6.1.

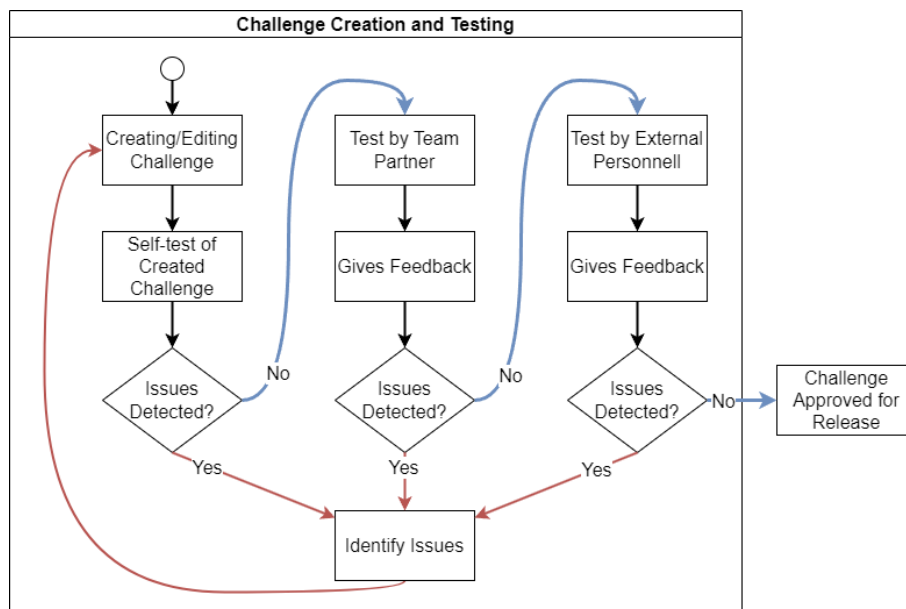


Figure 6.1.: Workflow of the testing procedure

6.2. Test by the Author

The challenge author will play through his own challenge to ensure the following:

- Requirements are met
- Required resources are provided
- Steps are in the correct order
- The flag is working
- Grading instructions are provided
- Spellcheck detects no errors

After this check the author passes his challenge to the other team partner to do the same.

6.3. Team Internal Testing

The partner will try to solve the challenge as a student would. This provides a first outside view as the ideas and texts written might be new to him. At this stage the same checks are applied as in the stage before. Spelling mistakes can be corrected right away, while bigger issues and feedback has to be sent to the author. He then updates his challenge accordingly and resubmits it to his partner. Only after this the tests with testing groups can be lined up.

6.4. External Testing Group

To test the challenges in a more realistic environment, tests with students, colleagues and friends were set up. Tests with personnel outside OST were focused on specific aspects of a challenge. For example, geolocation exercises were tested by geography students as they have better knowledge in this field and can thus provide detailed feedback.

The participants got a short introduction on OSINT, the web address to the challenges to test and a survey link to provide feedback back to the authors.

6.4.1. The Feedback Form

Blocksurvey.io was used to create and publish the feedback form. It was selected due to its privacy promise, functionality and clean style.

The feedback form comprised nine questions which were mostly answerable by clicking to encourage a submission.

The questions asked can be categorised in three groups: administrative, overview and build.

Administrative questions were used to classify the knowledge of the submitter and to match the submission to a challenge. Overview questions were to give a broad assessment like how much they liked the challenge, how difficult it was and how much time they needed. Questions regarding the build explore the structure and for detailed feedbacks. The task description could be rated on its ability to clearly state the subject, task and goal and if it aroused curiosity. A similar rating for the steps to rate their structure and usefulness was added. Two possibilities for free text entries were also given to receive feedback on topics the form did not cover.

6.4.2. Received Feedback Statistic

By the time of writing, we received 33 feedbacks through our feedback form and some through other media. The average challenge rating is 3.9 on a scale from 1 (bad) to 5 (great). This score even increases once the feedback for older versions is sorted out due to the suggested improvements being incorporated. The statistics of the feedback is shown in Figure 6.2.

The average time needed is around 25 minutes which does not include the writing of the write-up. Hence this number will increase once these challenges are solved during exercise sessions of future lessons, as the process of thoughts usually needs more time and might reveal uncertainties which need further research or OSINT in this case.

Challenge	Number of Feedbacks	Average		
		Rating	Difficulty	Time Needed
01 - Scamming Personal Information	6	3.2	2.3	30
02 - The Propagandists Information	4	4.5	3	35
03 - Time for Waste	2	4	2.5	30
04 - Validate Internet Post	3	3.3	2.7	20
05 - Third Party Software Contributions	4	4.3	2.5	25
06 - Show What You Have Learned	3	3.3	2.7	20
07 - Vulnerability Information	2	4	2	15
08 - Run After Ransomware	2	4.5	3	30
09 - A Car's History	4	3	1.5	15
10 - Malicious Gamer	3	5	2.7	35
Average	3.3	3.91	2.49	25.5

Figure 6.2.: Statistics for feedback received by external testing personnel

6.4.3. Feedback Form Review

Over all the testers gave valuable feedback and were engaged stating their opinion as 24 out of the 33 forms came gave additional findings. The high number suggests that the feedback form questions might not have been detailed enough to cover all the topics and thus forced the testers to write text. An alternative reason could be that they were keen to give useful feedback.

Free-Text Answer Evaluation

An evaluation of the free-text answers resulted in a classification of the statements into the following groups:

- Asking for more pictures (3 times)
- Description of
 - alternative approaches (3 times)
 - uncertainties (2 times)
 - problems while solving the challenge (4 times)
- Suggesting changes
 - less hints (5 times)
 - more or more specific hints (2 times)
 - certain wordings (5 times)
- Various unique points

Take-aways

While the unique points and descriptions of things cannot be covered by a specific question without bloating the form to an unappealing size, the other groups could benefit from separate questions.

Asking about Pictures

A new question asking whether a specific step is in need of more or less pictures. The design of the answer options has to be evaluated as with the growing number of steps the question might need, the space required could grow as well.

Suggested changes

The suggested changes were either less hints, more/more specific hints or a certain wording. While the wording cannot be asked for a question on the hints might be feasible. Similar to the question asking about pictures the design needs to be evaluated to not use the most space of the form.

6.4.4. Applied Changes Overview

This section lists meaningful changes applied to the challenges. The detailed descriptions are available in the documentation part of the corresponding challenge.

01 - Scamming Personal Information

A confusion around the number needed for the solution had to be resolved. Additionally, some linked services providing temporary email addresses had to be replaced as the websites where these mail addresses were needed blocked them and thus an account creation was not possible.

02 - The Propagandist's Information

Some hints were removed to give the students more space for their own OSINT.

03 - Time for Waste

Hints initially given made it possible to offline brute force the flag. Hence the flag format information was reduced.

04 - Validate Internet Post

One conclusion was in need of a rewrite to not spoiler too much.

05 - Third Party Software Contributions

Textual adjustments were made to guide the students since the feedback suggested a too open environment and thus a frustrating searching process.

06 - Show What You Have Learned

Minor changes in wording were made.

07 - Vulnerability Information

The feedback was very positive and no changes to the challenge were made.

08 - Run After Ransomware

Minor changes in wording were made.

09 - A Car's History

Feedback clearly suggested that the challenge was too short. As a result, the first question was reworked, and new question and step were added on container tracking/information gathering.

10 - Malicious Gamer

The feedback was very positive and no changes to the challenge were made.

7.1. Desired Target

The target of ten publishable and tested OSINT challenges has been achieved. Our testing personnel needed 25 minutes on average per challenge without writing a write-up, which could increase the total solving time beyond 30 minutes. The testing process also ensured the accordance to the official Hacking-Lab challenge structure requirements which were also improved and published during this thesis.

During the thesis ten challenges with different exercises were created. Classic OSINT topics like geolocating pictures or research on certain people are covered as well as exercises which require translation or research on standards like VIN or container numbers. All labs are deployed on the Hacking-Lab platform and were tested by Cyber Security students at the OST and people outside OST to cover more expert opinions on specific topics like geolocation or translation.

The documentation covers the process of the challenge creation from the initial ideas to the finally tested state the challenges have today.

7.2. Optional Targets

The optional target of covering all doings with a weight score of 3 was reached, while the optional target of an eleventh challenge was not.

On the basis of the initial matching between doings and stories the coverage of doings with a weight of 3 was tracked. In Figure 7.1 the realised matchings are marked with "R" on dark a green background while the possible, yet not realised matchings are marked with "p" on a light green background.

An eleventh challenge could not be realised. The first ten required more time than initially thought and brought up uncertainties which required a more cautious planning.

Story ID	Challenge ID	Doing ID	Doing Rating																					
			D01	D02	D03	D04	D05	D06	D07	D08	D09	D10	D11	D12	D13	D14	D15	D16	D17	D18	D19	D20	D21	D22
			3	3	1	0	3	2	1	3	3	0	2	3	0	0	1	3	3	1	2	3	3	2
			Extract meta data from document	Rate persons trustworthiness	Detect usage of specific software	Identify organisation structure	Translate text	Determine attacker by used methods/tools	Obtain word dictionary	Track physically moving object	Image content analysis	Create sock puppet	Dark web research	Video content analysis	Find company balance	Extract password from firmware	Identify a company's IT partner	Find contact information of person or position	Find information about person	Find information about company	Examine older version of website	Reverse image search	Using advanced search features	Locate position using map or satellite image
S01	C01		p		p	p	p	p	p	p	p	R	p	p	p	p	R	R	p	p	p	R	R	p
S02	C02		p	R	p	p	R	p	p	p	R	p					p	R	p	p	p	R	R	R
S05	C03		R	p		p	p		p	p	p	p					p	p	p	p		R	p	p
S04	C04		R	R	p	p	R			p	p						p	p	R	p		p	p	R
S15	C05			R	R		p						p				p	R		R		p		p
S06	C06		p	p	p	p	p	p	p	p	R	p	p	R	p	p	p	p	R	p	R	R	p	R
S07	C07			p	R		p						p					p				p	p	
S03	C08				R	p	p						R				p	p	p	R	p		p	p
S11	C09			p			p			R	p							p	p	p		p	R	p
S14	C10		p				p			p	p	p					p	R		R	p	p	p	p
Doing was integrated at least once:			Yes	Yes	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Figure 7.1.: Realised doings per challenge

Conclusion and Outlook

We Conclude

Our first goal was to create ten challenges for the Hacking-Lab with an additional goal of an eleventh challenge if the time allows it. While we were able to create ten challenges meeting our primary requirement, we were not able to create the eleventh challenge due to each challenge taking longer to create than expected. Nevertheless, the quality of the challenges was more important to us than the quantity and we feel like we reached a good standard of quality for each challenge which is reflected in the feedback we have received from the reviewers.

When selecting our challenges, we brainstormed ideas and made a selection of stories and doings that we wanted to implement in our challenges. We were able to create nine of the ten selected stories, with one being changed to a kind of summary of all topics instead of the original idea. The story that was cancelled was to check if a job advertisement is authentic. Here we wanted to have a fake job offer from a newspaper or a website which asks for a CV in order to phish for personal information. The idea was good in theory but turned out to be very difficult to implement and maintain in practice.

We ranked each different doing that we had after a brainstorming session with a priority ranging from 0 to 3. 0 being this is not important to include in our project to 3 being a must have. A secondary goal was to implement each doing that we rated to be the highest priority into a challenge. This goal was also achieved. Only 6 out of the 22 doings were not implemented into any challenge at all. One of those is priority 2, two were priority 1 and the rest were priority 0. While it would have been nice to include all priority two doings as well, we are happy with the result.

Our Outlook

We find that the challenges we created can serve as a foundation for a lecture on OSINT in a cyber security module at OST. We think OSINT is an integral part of cyber security today and it is almost unavoidable to be confronted with it in the field of cyber security. With our work, the lecturer has a variety of challenges to choose from to give the students to solve during the exercise session following a lecture.

The challenges can still be expanded upon and may have to be revised in the future to adjust to websites changing. Even though the challenges were created with the goal of being maintainable with little to no effort, the internet is a fast-paced construct and even in the time when we created the challenges, different results are achieved with the same actions. It is impossible to know what the future holds, which new tools or datasets will appear, making it necessary to revise the current challenges or create new ones to reflect the changes in technology and the internet. Furthermore, more challenges could be created with a focus on social media, since this was purposely neglected in this project because it is difficult to maintain and make future-proof, which makes it incompatible with the project's requirements.

Part II.
Appendix

List of Figures

3.1. OSINT topics in this thesis	8
3.2. Iterative testing procedure	9
3.3. Challenges overview	10
1.1. Overview of the challenges to solve	15
1.2. View of a challenges	15
1.3. Student submissions in an overview for a teacher	16
1.4. Assessment of a student submission (master solution redacted)	16
2.1. Road line markings around the world [22]	20
2.2. North American state highway signs [22]	20
2.3. Distribution of left and right side driving [8]	21
2.4. Occurrence of the Monarch Butterfly [43]	22
2.5. Different maps from left to right: Satellites Pro [45], Yandex maps [49], Bing maps [38]	25
4.1. Workflow of the story selection procedure	31
4.2. Matching between doings and stories	32
4.3. Stories ordered by weight	34
5.1. An overview of all ten challenges	35
5.2. Hacking-Lab preview of Challenge 01	36
5.3. Hacking-Lab preview of Challenge 02	39
5.4. Hacking-Lab preview of Challenge 03	43
5.5. Hacking-Lab preview of Challenge 04	47
5.6. Hacking-Lab preview of Challenge 05	49
5.7. Hacking-Lab preview of Challenge 06	52
5.8. Hacking-Lab preview of Challenge 07	54
5.9. Hacking-Lab preview of Challenge 08	56
5.10. Hacking-Lab preview of Challenge 09	59
5.11. Hacking-Lab preview of Challenge 10	62
6.1. Workflow of the testing procedure	64
6.2. Statistics for feedback received by external testing personnel	66
7.1. Realised doings per challenge	69

List of Tables

1.1. ETCS and time budget per team member	13
1.2. Work distribution	14
4.1. Attributes of doings and stories	31
4.2. List of stories	31
4.3. List of doings	32
4.4. Categorised stories	33
4.5. Weighted doings	33

Bibliography

- [1] —. *dtv Lexikon*. 2. München: F. A. Brockhaus GmbH und Deutscher Taschenbuch Verlag GmbH & Co. KG, 1995. ISBN: 3-423-05998-2.
- [2] Chang Liu et al. “Web sites of the Fortune 500 companies: Facing customers through home pages”. In: *Information & Management* 31.6 (1997), pp. 335–345. DOI: [10.1016/s0378-7206\(97\)00001-3](https://doi.org/10.1016/s0378-7206(97)00001-3).
- [3] —. *NATO OSINT Handbook V 1.2*. 2001. URL: <https://archive.org/details/NAT00SINTHandbookV1.2/mode/2up>.
- [4] William Bright. “What IS a Name? Reflections on Onomastics”. In: *Language and Linguistics* 4 (Jan. 2003).
- [5] Fazli Can and Jon M. Patton. *Change of Writing Style with Time*. 2004. URL: <https://link.springer.com/article/10.1023/B:CHUM.0000009225.28847.77>. Accessed: 2023-06-04.
- [6] Steve Weber. *Twitter Marketing*. Weber Books, 2009. ISBN: 978-0-9772406-6-1.
- [7] Edith Grossman. *Why Translation Matters*. London: Louis Stern Memorial Fund, 2010. ISBN: 978-0-300-12656-3.
- [8] Daven Hiskey. *Why Some Countries Drive on the Right and Some Countries Drive on the Left*. 2010. URL: <https://www.todayifoundout.com/index.php/2010/06/why-some-countries-drive-on-the-right-and-some-countries-drive-on-the-left/>. Accessed: 2023-05-29.
- [9] —. *(U) Signals intelligence*. 2012. URL: <https://documents.theblackvault.com/documents/intellipedia/intellipedia-sigint.pdf>.
- [10] Max Roser, Esteban Ortiz-Ospina, and Hannah Ritchie. “Life Expectancy”. In: *Our World in Data* (2013). URL: <https://ourworldindata.org/life-expectancy>. Accessed: 2023-06-12.
- [11] David Omand. In: *Securing the State*. Oxford University Press, 2014. ISBN: 978-0-1993-2717-1.
- [12] Starbug. *Ich sehe, also bin ich ... Du*. 2014. URL: https://media.ccc.de/v/31c3_-_6450_-_de_-_saal_1_-_201412272030_-_ich_sehe_also_bin_ich_du_-_starbug. Accessed: 2023-04-01.
- [13] Chunxia Zhang et al. “Authorship identification from unstructured texts”. In: *Knowledge-Based Systems* 66 (2014), pp. 99–111. DOI: [10.1016/j.knsys.2014.04.025](https://doi.org/10.1016/j.knsys.2014.04.025).
- [14] —. *France TV5Monde passwords seen on cyber-attack TV report*. 2015. URL: <https://www.bbc.com/news/world-europe-32248779>.
- [15] Pooja Deshmukh and Sarika Solanke. “Review Paper: Sarcasm Detection and Observing User Behavioral”. In: *International Journal of Computer Applications* 166 (May 2017), pp. 39–41. DOI: [10.5120/ijca2017914119](https://doi.org/10.5120/ijca2017914119).
- [16] Kristin Finklea. *Dark Web*. 2017. URL: [https://a51.nl/sites/default/files/pdf/R44101%20\(1\).pdf](https://a51.nl/sites/default/files/pdf/R44101%20(1).pdf).
- [17] Secunder Kermani. *Pakistani corruption case hinges on a font*. 2017. URL: <https://www.bbc.com/news/blogs-trending-40571708>. Accessed: 2023-04-01.

- [18] Nihad A. Hassan and Rami Hijazi. *Open Source Intelligence Methods and Tools*. New York: Apress, 2018. ISBN: 978-1-4842-3212-5.
- [19] Starbug and Julian. *Venenerkennung hacken*. 2018. URL: https://media.ccc.de/v/35c3-9545-venenerkennung_hacken. Accessed: 2023-04-01.
- [20] Kan Yuan et al. "Reading Thieves' Cant: Automatically Identifying and Understanding Dark Jargons from Cybercrime Marketplaces". In: *27th USENIX Security Symposium (USENIX Security 18)*. Baltimore, MD: USENIX Association, Aug. 2018, pp. 1027–1041. ISBN: 978-1-939133-04-5. URL: <https://www.usenix.org/conference/usenixsecurity18/presentation/yuan-kan>.
- [21] Heeket Mehta, Pratik Kanani, and Priya Lande. "Google Maps". In: *International Journal of Computer Applications* 178 (May 2019), pp. 41–46. DOI: [10.5120/ijca2019918791](https://doi.org/10.5120/ijca2019918791).
- [22] Kyal Shepard. *Geoguessr: The Top Tips Tricks and Techniques*. 2019. URL: <https://somerandomstuff1.wordpress.com/2019/02/08/geoguessr-the-top-tips-tricks-and-techniques>. Accessed: 2023-05-29.
- [23] International Organization for Standardization. *ISO 19111:2019 - Geographic information*. 2019. URL: <https://www.iso.org/obp/ui/#iso:std:iso:19111:ed-3:v1:en>.
- [24] —. *Bundesgesetz über das Urheberrecht und verwandte Schutzrechte*. 2020. URL: https://fedlex.data.admin.ch/filestore/fedlex.data.admin.ch/eli/cc/1993/1798_1798_1798/20200401/de/pdf-a/fedlex-data-admin-ch-eli-cc-1993-1798_1798_1798-20200401-de-pdf-a.pdf.
- [25] World Economic Forum. *Six ways space technologies benefit life on Earth*. 2020. URL: https://www3.weforum.org/docs/WEF_GFC_Six_ways_space_technologies_2020.pdf. Accessed: 2023-06-01.
- [26] Andre Araujo et al. *Google Landmark Recognition 2021*. 2021. URL: <https://kaggle.com/competitions/landmark-recognition-2021>. Accessed: 2023-05-28.
- [27] Heath Adams. *Open-Source Intelligence (OSINT) in 5 Hours - Full Course - Learn OSINT!* 2022. URL: <https://www.youtube.com/watch?v=qwA6MmbeGNo>.
- [28] Marvin Mohr. *Achtung Autofalle!* 2022. URL: <https://www.zdf.de/dokumentation/zdfinfo-doku/achtung-autofalle-leichtes-spiel-fuer-abzocker-100.html>. Accessed: 2023-05-02.
- [29] Calculator Academy Team. *Image Distance Calculator*. 2022. URL: <https://calculator.academy/image-distance-calculator/>. Accessed: 2023-05-28.
- [30] —. *About code scanning*. 2023. URL: <https://docs.github.com/en/code-security/code-scanning/automatically-scanning-your-code-for-vulnerabilities-and-errors/about-code-scanning>.
- [31] —. *MPEG-7*. 2023. URL: <https://mpeg.chiariglione.org/standards/mpeg-7>. Accessed: 2023-04-01.
- [32] Bernstein. *Personally Identifiable Information (PII)*. 2023. URL: <https://www.techtarget.com/searchsecurity/definition/personally-identifiable-information-PII>. Accessed: 2023-05-23.
- [33] Ivan Bütler. *Challenge Requirements*. 2023. URL: <https://hacking-lab.atlassian.net/wiki/spaces/HLSD/pages/234881025/Challenge+Requirements>. Accessed: 2023-03-31.
- [34] Compass Security. *Hacking-Lab Cyber Range*. 2023. URL: <https://www.compass-security.com/de/produkte/hacking-lab>. Accessed: 2023-03-18.
- [35] Yadav, Kumar, and Singh. *Open-source intelligence: a comprehensive review of the current state, applications and future perspectives in cyber security*. 2023. DOI: [10.1007/s10462-023-10454-y](https://doi.org/10.1007/s10462-023-10454-y).
- [36] —. *About NGA*. URL: https://www.nga.mil/about/About_Us.html. Accessed: 2023-04-28.
- [37] —. *Airline Route Maps*. URL: <https://www.airlineroutemaps.com/>. Accessed: 2023-06-07.
- [38] —. *Bing Maps*. URL: <https://www.bing.com/maps>.
- [39] —. *Geo Hints*. URL: <https://geohints.com/>. Accessed: 2023-05-29.
- [40] —. *Geo Tips*. URL: <https://geotips.net/>. Accessed: 2023-05-29.

-
- [41] —. *Glassdoor*. URL: <https://www.glassdoor.com/>. Accessed: 2023-06-06.
- [42] —. *Google Lens*. URL: <https://lens.google.com/>. Accessed: 2023-05-31.
- [43] —. *Monarch Butterfly*. URL: https://en.wikipedia.org/wiki/Monarch_butterfly. Accessed: 2023-05-29.
- [44] —. *Openinsider*. URL: <http://openinsider.com/>. Accessed: 2023-06-06.
- [45] —. *Satellites Pro*. URL: <https://satellites.pro/>.
- [46] —. *Soils Maps of Scotland*. URL: <https://www.hutton.ac.uk/learning/natural-resource-datasets/soilshutton/soils-maps-scotland>. Accessed: 2023-04-28.
- [47] —. *Was uns besonders macht*. URL: https://www.bnd.bund.de/DE/Die_Arbeit/Informationsgewinnung/informationsgewinnung_node.html. Accessed: 2023-04-28.
- [48] —. *Yandex Images*. URL: <https://yandex.com/images>. Accessed: 2023-05-31.
- [49] —. *Yandex Maps*. URL: <https://yandex.com/maps>.
- [50] —. *Zefix*. URL: <https://www.zefix.ch/en/hra>. Accessed: 2023-06-06.
- [51] Bruce Drum. *Airline Tails*. URL: <https://airlinersgallery.smugmug.com/Airline-Tails/Airline-Tails/>. Accessed: 2023-06-07.
- [52] Perryworld Ltd. *The Planespotter Community*. URL: <https://www.planespotters.net>.