https://doi.org/10.2352/ISSN.2470-1173.2020.3.MOBMU-278

Conception and implementation of professional laboratory exercises in the field of open source intelligence (OSINT)

Klaus Schwarz, Franziska Schwarz, Reiner Creutzburg

Technische Hochschule Brandenburg, Department of Informatics and Media, IT- and Media Forensics Lab, Magdeburger Str. 50, D-14770 Brandenburg, Germany

Email: klaus.schwarz@th-brandenburg.de, franziska.schwarz@th-brandenburg.de, creutzburg@th-brandenburg.de

Abstract

A large amount of personal and very incriminating data is currently stored on websites, apps and social media platforms. Users often update these data daily, and this data is open source. This information can become evidence for citizens, governments, and businesses to use in solving real financial, employment, and crime problems with the help of a professional information collector. To respond to this new situation, it is important to have well-trained staff. The fact that many authorities and companies work with very sensitive data makes it necessary to train their employees in Open Source Intelligence (OSINT). Motivated by these facts, a practical training concept is developed that enables the creation of practical exercises. The focus is on the practical implementation of OSINT tools and methods. In the new course, participants learn legitimate and effective ways to find, collect, and analyze this data from the Internet. We have developed an introductory course for a Master level program in Open Source Intelligence (OSINT). Students learn up-to-date, hands-on skills, techniques, and tools that law enforcement, private detectives, cyber attackers, and defenders use to search the vast amount of information on the Internet, analyze the results, and build on interesting data to find other areas for investigation. Our goal is to provide the OSINT knowledge base for students to succeed in their field, whether they are cyber defenders, threat intelligence analysts, private detectives, insurance inspectors, intelligence analysts, law enforcement, or just someone curious about OSINT. Throughout the course that consists of 11 exercises, students will participate in numerous hands-on exercises using the OSINT tools and techniques that form the basis for collecting free data from the Internet.

Keywords

Open Source Intelligence, OSINT, Cybersecurity, Shodan, PassiveTotal, Censys, Maltego.

Introduction and Motivation

Open Source Intelligence or OSINT, for short, is the collection of data and information from freely accessible and open sources. Magazines, radio, television, publicly available, and openly accessible sources can be anything. Still, most of all, the Internet and web-based applications are used with OSINT to gain useful insights by analyzing various data and information. The internet consists of a vast amount of data, which is growing every year, as the following statistics show. For example, the amount of data produced annually was 33 Zettabyte in 2018, and it is assumed that this number will increase almost sixfold to 175 Zettabyte by 2025 (cf. fig. 1).

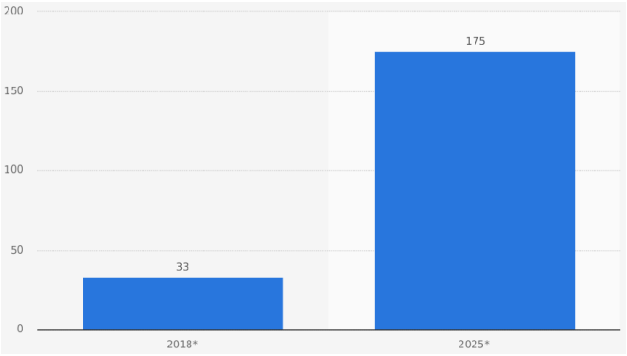


Figure 1. *Forecast of the volume of annually generated digital data worldwide in 2018 and 2025 (in Zettabyte)*

This huge amount of data holds great potential for a variety of analyses, which are summarized under the term Open Source Intelligence. Social networks with freely accessible private information such as Facebook and Instagram have 3.2 billion visitors daily, which corresponds to about 42% of the world' s population (see Fig. 2). However, Facebook and Instagram are by far, not the only networks of interest for OSINT data analysis. Figure 4 shows the Social Media Prism 2017/2018, the top 250 social media networks, apps, and tools. These and many other sources offer huge amounts of freely available data that can be used and analyzed for information gathering.

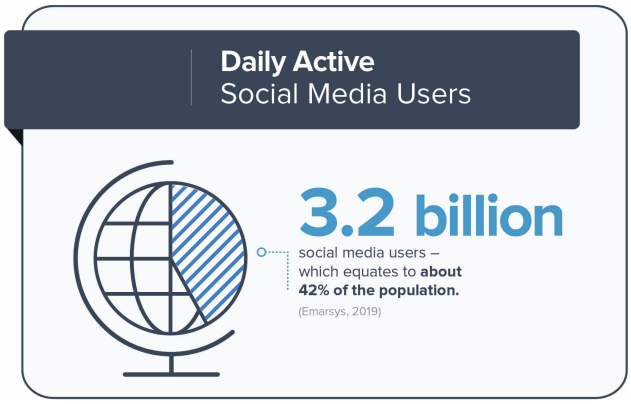


Figure 2. *Usage of social media around the world*

Not only a large amount of available data offers an interesting advantage over other types of intelligence gathering. The procurement of data by techniques and analyses of Open Source Intelligence, i.e., the acquisition of data from public and freely accessible sources, does not pose any particular risk and, in addition, causes only low costs for aggregation. However, a large amount of data also results in difficulty that should not be neglected. The targeted collection of data and the aggregation of knowledge from precisely this large amount of data. How data can be collected in a targeted manner, which tools, ways, and means are available and how usable insights can be gained from a lot of small information, is the goal of the course developed in the context of this work. The course consists of eleven exercises that start with setting up a working environment and teach how to work efficiently in it. Afterward, freely available tools are presented, and the use of these tools is trained. This is followed by the presentation of the most common commercial tools, which are worked out step by step in the individual exercises. Finally, it will be shown how all these tools can be used to aggregate search results from many individual data.

Definition of Objectives and Goals

This work aims to give participants a comprehensive overview of the topic of Open Source Intelligence and to enable participants to work independently with the newly learned tools, to collect data from freely accessible sources, and to aggregate them into investigation results. For this purpose, tasks are designed for several lab exercises. These should first impart knowledge of a Linux working environment specially created for investigations in the OSINT area and then teach the data acquisition in dealing with the presented free and commercial tools, as well as the subsequent analysis and aggregation of the data into investigation results. The participants learn the exact procedure in eleven practical exercises, which enable them to work independently in the Open Source Intelligence world step by step.

All exercises are designed to meet the requirements of a laboratory internship. The knowledge acquired in this course is deepened by the tasks and practiced in practical scenarios. Specific free and commercial tools are presented and offered for practice. The accompanying theory is intended to explain the exact technical and functional relationships of the given steps of data acquisition so that these can then be better understood.

The practical exercises allow participants to familiarize themselves with the tools presented; the exercises are accompanied by a teacher. This allows the participants to independently memorize and understand the theoretical content of the course, but if there are any questions or problems, participants will be addressed directly and individually. In this way, the interest of the participants in the topic of Open Source Intelligence is to be awakened, and thus more specialists in this area are trained. The acquired knowledge will be retained for a longer period of time due to the embedding of practical tasks and the independent but accompanied learning experience. This should motivate the participants more and help them to experience a sense of achievement.

By combining theory and practice in practical scenarios, the participants expand their specialist knowledge and learn how to apply what has been learned directly in a work-related environment. The participants will not only learn the steps for obtaining data but also how to aggregate data on a case-specific basis and how to choose the right methods and tools for obtaining and aggregating data. In this way, the participants will learn the basics of Open Source Intelligence and how to apply them.

Further competencies can be improved and strengthened, e.g., logical thinking, evaluation of clues, and concentrated and thorough approach to the use of search tools. The tasks are designed in such a way that they can be carried out by a group as well as by a single participant.

Delimitation

The field of Open Source Intelligence, like the vast amount of freely available data, is particularly extensive and, depending on the definition, is also made up of a variety of different components. This work is about learning OSINT techniques and tools in a Linux environment with free and commercial tools. In addition, mainly online tools like the search engine Google and other tools that have proven themselves in practice will be used to provide a particularly practical training. Especially the search for persons, although it belongs to the field of Open Source Intelligence, is not considered in this work. Furthermore, only the Internet serves as a data source for all exercises presented in this work. Although the collection of data from free and open available sources includes many more potential sources for analysis, the related concepts and theoretical foundations exceed the scope of this work.

OSINT

Open Source Intelligence, the collection of data from freely accessible sources, has a whole range of definitions. Robert D. Steele, one of the most cited authors when it comes to the definition of OSINT, describes Open Source Intelligence as follows: ”OSINT is intelligence derived from public information–tailored intelligence which is based on information which can be obtained legally and ethically from public sources.” in his whitepaper of 1997. The US ”National Defense Authorization Act for Fiscal Year 2006” Open Source Intelligence is defined as follows: ”produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement.” In addition, security researcher and publicist Mark M. Lowenthal, who also works for the CIA, defines OSINT as follows: ”any and all information that can be derived from overt

collection: all types of media, government reports and other documents, scientific resarch and reports, commercial vendors of information, the Internet, and so on. The main qualifiers to open-source information are that it does not require any type of clandestine collection techniques to obtain it and that it must be obtained through means that entirely meet the copyright and commercial requirements of the vendors were applicable." Common to all definitions is the following list of requirements:

- Overt collection
- Publicly available
- Open sources
- Disseminated
- Purpose is to address an intelligence requirement
- Copyright and commercial requirements
- Legally and ethically

These seven requirements reflect the core characteristics of Open Source Intelligence very well. The smallest pieces of information are collected from all conceivable open and freely available sources to obtain targeted knowledge and then put together to form this knowledge.

Course Overview and Introduction

The OSINT course created in this work attempts to give an interested person an introduction to the topic of Open Source Intelligence. After a short introduction into the world of Open Source Intelligence, the participants will get an overview of the basics of OSINT and an insight into the historical background. This is followed by the three main parts of the course, which consist of exercises covering various topics of Open Source Intelligence. In the three main parts, the participants learn all relevant skills for collecting and assembling everything from the smallest information to the creation of compound knowledge.

The first part of the course starts simply. It gradually provides participants without much previous knowledge with advanced skills of the Unix shell, thus introducing participants to the Linux working environment that has been specially prepared for this course. In addition to knowledge of the Unix shell, basic understanding of simple operations and knowledge of the file system hierarchy will be taught. The first chapter concludes with an exercise that shows how to work with Linux pipes and how to search and organize large amounts of data with simple means.

In the second part, these skills are then used to collect and aggregate the most complex data sets from the Internet using the freely available tools learned in the course. In addition to the simplest Linux shell tools, the Google search engine is also used, whose many buttons and options can dramatically improve searches and their results. Forensic methods are also taught to teach the participants how to work, think independently, and bring responsibility in complex systems as well as proper documentation to an understanding.

The third part of the course provides advanced knowledge of the most common commercial tools currently available. With the knowledge acquired in the first part, participants will learn how to search, evaluate successfully, and aggregate knowledge from large amounts of data or massive databases. In each exercise, a commercial tool is always presented, and the participants get to know it online on the respective platform. Afterward, however, all participants use the interfaces of the respective tool to search, prepare, and enrich large amounts of data. In this way, the knowledge imparted in the first parts of the exercise is used and what has already been learned is combined with new knowledge.

All three parts together offer a comprehensive overview and advanced knowledge in the field of Open Source Intelligence and enable the participants to work independently in this area.

Course Structure

The new OSINT course consists of the following 5 sections with 11 exercises:

1. Introduction
2. OSINT - Basics and History
3. Linux Fundamentals for OSINT
   (a) Preparation
   (b) Exercise 1: Linux Shell Fundamentals
   (c) Exercise 2: Linux File System Hierarchy Fundamentals
   (d) Exercise 3: Linux Pipe Fundamentals
4. OSINT Basics
   (a) Preparation
   (b) Exercise 4: Advanced Google Search
   (c) Exercise 5: Linux Networking Tools
   (d) Exercise 6: Linux Forensics Tools
5. OSINT Commercial Tools
   (a) Preparation
   (b) Exercise 7: Hacking-Lab Environment Preparation
   (c) Exercise 8: PassiveTotal
   (d) Exercise 9: Censys
   (e) Exercise 10: Shodan
   (f) Exercise 11: Maltego

Detailed Course Description

The OSINT course created in this work has five parts in total. The first part of the course offers a short introduction to the topic of Open Source Intelligence, followed by an insight into the basics and history of OSINT. With the third part, the three exercise parts of the course begin. After a short preparation part that precedes each of the three exercise parts, the first of the three exercise parts introduces the participants to work with the Linux environment created for all exercises. Besides working with the Linux command line, many other essential skills are taught, which will be assumed as basics in the later course of the activities. The second part of the exercise part of the work is about the basics of Open Source Intelligence. The knowledge from the first part is directly applied here and is expanded step by step in the exercises of this part. The third and last part of the exercise part introduces five different commercial tools that have proven themselves in practice.

1. Introduction

The first chapter introduces with a short introduction into the world of Open Source Intelligence, here the motivation and the objective of the exercises are described. The introduction conveys the importance and the explosiveness of the topic Open Source Intelligence and gives a clear overview of what can be learned and

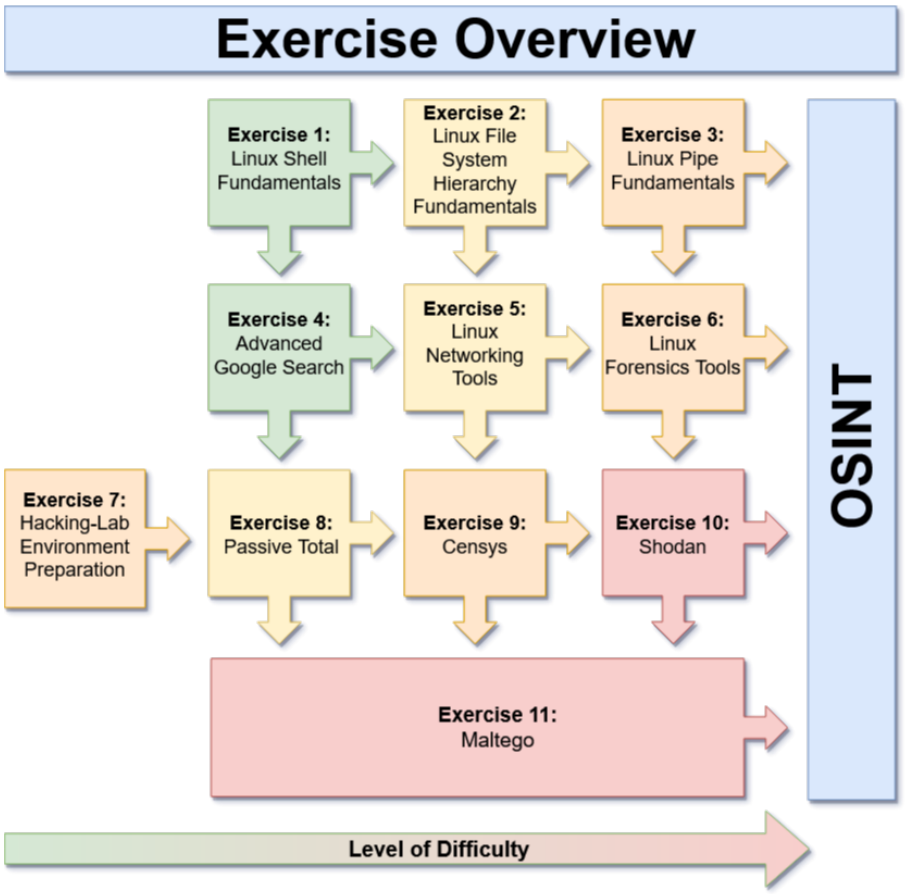


Figure 3. *OSINT Course Overview with 11 Exercise*

what is not covered in the course. It also describes how learning goals are to be achieved.

2. OSINT - Basics and History

This chapter defines and describes the beginnings of open source intelligence. It explains what OSINT is used for and in what way. This chapter also defines the use cases and goals for the use of OSINT. In particular, it discusses the function of authorities and secret services and which sources are most commonly used to obtain information.

3. Linux Fundamentals for OSINT

In this part of the course, the basics but also the knowledge for advanced users should be imparted, thus creating a solid foundation for the following parts of the course. This part of the course is designed in such a way that the participants can find an easy introduction to the topic even without a great deal of previous knowledge. Gradually, advanced knowledge of the Unix shell will be taught during this section of the course. In addition to the knowledge gained about the Unix shell, basic understanding of simple operations and knowledge of the file system hierarchy are also taught. This chapter concludes with an exercise in which working with Linux pipes and searching and organizing large amounts of data with simple means is practically practiced and learned.

Preparation

At the beginning of each of the three parts of the OSINT course, there is an introduction that explains all the steps necessary to set up the tools required in the course on the participants' computers. The preparatory part of the Linux Basics for OSINT section explains in easy-to-follow steps how to set up the Linux environment using a virtual machine, where to download it, and how to set up individual user accounts. It also explains how to set up the correct language and keyboard layout for working in the virtual machine.

Exercise 1: Linux Shell Fundamentals

This exercise is designed to introduce the Linux shell. A shell describes the traditional user interface in Unix operating systems. Basically, a shell is a program that receives commands from the user, forwards them to the operating system to be processed, and then displays its return. In this exercise, participants are introduced to the Linux shell step by step to gradually gain all the necessary knowledge to work independently. In this exercise essential basics for all later exercises are learned.

Exercise 2: Linux File System Hierarchy Fundamentals

Everyone knows what a file is. It is the photo, document, or piece of music that everyone uses. Even programs are made up of files, and in fact, the whole Linux operating system is just a col-

lection of files. In the case of a digital photo stored on a computer, it is still obvious but the monitor is also a file in a Linux operating system. In Linux, everything is a file. This exercise is designed to help participants understand how the file system is structured under Linux and where essential data can be found. Although there is a filesystem hierarchy standard, many Linux distributions follow it only partially. The Filesystem Hierarchy Standard is intended to help ensure that more Unix/Linux filesystem trees will match more closely in the future. This exercise serves as an introduction to the basics of the Linux filesystem hierarchy and contains important information on which all later exercises are based.

Exercise 3: Linux Pipe Fundamentals

Pipelines are an important tool when working on the Linux command line. A pipeline in unixoid operating systems consists of programs that are linked together via their standard data streams. A program "receives" the standard output (STDOUT) of the previous program in the chain via the standard input (STDIN). The individual programs are called one after the other by the previous one.

4. OSINT Basics

Building on the first part of this course, the knowledge of the Unix shell and the file system hierarchy under Linux that has been taught and learned will now be applied. In this part of the course, complex data sets from the Internet are collected and aggregated using the freely available tools that are taught in the course. Besides simple Linux shell tools, the search engine Google is also used. The numerous options and shortcuts offered by Google, when used correctly, can greatly improve a search and its results. Forensic methods are also taught within this course section. These are designed to teach participants to work in complex systems, to think for themselves, to take responsibility, and to document correctly.

Preparation

At the beginning of each of the three parts of the OSINT course, there is an introduction that explains all the steps necessary to set up the tools required in the course on the participants' computers. At this point, users already have a fully functional and operational system at their disposal. The preparatory part of this section briefly introduces the tools used in the following exercises. It then explains in easily understandable steps how to set up the tools and their environments.

Exercise 4: Advanced Google Search

This exercise is intended to provide an introduction to working with Google Advanced Search, focusing on the use of search operators. Google is the world's largest search engine provider. The phrase to google something is not only known in the English-speaking world, but the verb to google something is also listed in the German dictionary "Duden". The search for word groups is simple, intuitive, and well known. However, the results of most search engines are optimized for normal internet surfing for reasons of legality. Knowing some of the operators, the results of every search can, in many cases be dramatically improved by the correct use of the respective operator.

Exercise 5: Linux Networking Tools

This exercise is designed to introduce the essential Linux networking tools. With the help of these tools, a lot of information about the systems in the local network - or their access to external networks - can be collected quickly. Some of these tools make it possible to record the communication, and others help to see which way a request takes or how much time it takes. In this exercise, participants will cover the basic commands and use them in the Linux shell.

Exercise 6: Linux Forensics Tools

This exercise deals with the general principles of forensic investigation and is intended to show what means and possibilities there are in this field. Forensic investigations are complex. There is no standard case. At the beginning of an investigation, it is not possible to predict what an incident will entail. The various dates - the evidence - on the system are what the story of the event tells. The first person to respond to an incident has the responsibility to ensure that as little evidence as possible is damaged in order to contribute to a meaningful restoration of the incident.

5. OSINT Commercial Tools

The most common commercial tools and the advanced use of these are taught to the participants in this section. The knowledge acquired in the first parts of the course will now be applied, allowing the experience already learned to be interlinked and reinforced. The goal of this section is to teach the participants how to successfully search, evaluate, and aggregate knowledge from large amounts of data or massive databases. In every single exercise, a commercial tool is introduced, and the participants get to know and use it. Therefore the attendees look at the respective online platforms of different commercial tools that have proven themselves in practice. Afterward, each participant will use the respective interfaces of the tool in order to solve tasks that gradually become more complex. In this way, the knowledge imparted in the first exercise is used, expanded, applied practically, and consequently combined with new experience.

Preparation

At the beginning of each of the three parts of the OSINT course, there is an introduction that explains all the steps necessary to set up the tools required in the course on the participants' computers. In the preparatory part of the chapter OSINT Comercial Tools, the tools and environments of the following exercises are once more introduced in short form. Furthermore, the history of the individual tools and the possibilities of the interfaces of the respective tool are explained. Besides, it is discussed in detail which tool is particularly suitable in which area of Open Source Intelligence and where exactly the application areas of the respective tool are located.

Exercise 7: Hacking-Lab Environment Preparation

This exercise is intended to provide an introduction to working with the Hacking-Lab virtual hacking environment. The HACKING-LAB is a service of Security Competence GmbH, a Swiss subsidiary of Compass Security AG. Compass Security is a European company specializing in penetration testing, incident response, digital forensics, and security training. The HACKING-LAB provides a comprehensive attack/defense system for the "Eu-

ropean Cyber Security Challenge". The HACKING-LAB is licensed at numerous universities worldwide for educational purposes, to promote young cyber talents and encourage them to pursue a career in cybersecurity.

Exercise 8: Passive Total

Security and forensics experts today are confronted with extremely skilled, malicious, persistent threats and attacks. The good news for analysts is that there is data that can help expose the infrastructure used by attackers. In this way, attacks can be found, blocked, and prevented. PASSIVETOTAL accelerates investigations by linking internal activities, events, and indicators of threats to what is happening outside the firewall - making external threats, attackers, and associated infrastructure visible.

Exercise 9: Censys

CENSYS is often referred to as the most dangerous search engine in the world alongside SHODAN. CENSYS was developed by a group of researchers at the University of Michigan to make the Internet safer. Regular Internet-wide port scans across the entire public IPv4 address space can be used to identify vulnerable devices and networks and to generate statistics on usage patterns of specific protocols or certificates. The results can be retrieved with an advanced full-text search or via an API.

While similar search services of this kind focus on host discovery, CENSYS takes the path of performing complete protocol handshakes and analyzing the recorded data. This achieves a significantly higher hit rate without sacrificing accuracy.

The backend of CENSYS consists of the highly parallel application scanner ZGrab (part of the open-source project ZMap), which currently detects and analyzes numerous other application handshakes in addition to StartTLS, Heartbleed, and SSLv3 and makes them available as JSON objects. ZMap identifies the interesting hosts, and ZGrab initiates the handshakes and provides the corresponding structured data.

Exercise 10: Shodan

SHODAN is often referred to as the "most dangerous" search engine in the world. SHODAN attempts to catalog metadata about its targets, often they are the Internet of Things (IoT) devices. Hackers and security researchers use SHODAN every day to find endangered webcams, open traffic light systems, SCADA in production sites, and much more.

SHODAN users can attack systems such as traffic lights, surveillance cameras, home heating systems, and control systems for water parks, gas stations, water facilities, power grids, nuclear power plants, and particle-accelerating cyclotrons if they meet only low safety standards. Many devices use trivial authentication criteria such as the user name **admin** and passwords such as **1234**. The only software required to connect to these servers is a web browser of the participants choice.

The site searches the Internet for publicly available devices that focus on SCADA (monitoring and data collection) systems. SHODAN currently provides ten results to users with no account and 50 results to those with a free account. If users want to remove the restriction, they must provide a reason and pay a fee. The primary users of SHODAN are Internet security specialists, researchers and law enforcement agencies.

SHODAN collects data mostly on web servers (HTTP/HTTPS via ports 80, 8080, 443, 8443), FTP (port 21), SSH (port 22), Telnet (port 23), SNMP (port 161), SIP (port 5060), and Real-Time Streaming Protocol (RTSP, port 554). The latter are regularly used to access webcams and their video streams.

Exercise 11: Maltego

MALTEGO is a visual link analysis tool that comes with open-source Intelligence plugins called transformations. The tool offers real-time data mining. Collected information is displayed on a node-based graph that makes patterns and connections of multiple orders between the information easily identifiable. MALTEGO focuses on the analysis of real relationships between publicly accessible information about Internet infrastructures, individuals, and organizations.

MALTEGO uses the idea of transformations to automate the process of querying different data sources. This information is then displayed in a node-based graph suitable for performing connection analysis.
There are currently three versions of the MALTEGO client, namely MALTEGO CE, MALTEGO Classic and MALTEGO XL. All three MALTEGO versions will have access to a library of standard transformations for the discovery of data from a variety of public sources commonly used in online research and digital forensics.

Evaluation

The Open Source intelligence course created in this thesis has already been evaluated in several practical sessions with 20 test persons. The result is predominantly positive feedback; the participants thoroughly enjoyed the topic and the structure of the exercises. The clear structure and sequence of the exercises are also convincing. The participants further stated that the extent of the exercises and the general teaching material is appropriate to the requirements. All participants also praise the high practical part of the exercises. During the evaluation, the course always included all 11 practical exercises. On 14 training dates, a total of 64 contact hours of teaching were provided in 2 weeks (see Table in Appendix).

Summary and Outlook

The huge amount of data that the Internet represents has a great potential for a variety of analyses from the world of open-source intelligence. Social networks with freely accessible private information such as Facebook and Instagram have 3.2 billion visitors daily, which is about 42% of the world's population (see Figure 2). However, Facebook and Instagram are, by far, not the only networks of interest for OSINT data analysis. The course created in this thesis gives participants a comprehensive overview of the topic of Open Source Intelligence. It allows them to work independently with the newly taught tools, collect data from freely available sources, and aggregate it into investigation results. For this purpose, the tasks were designed for several laboratory exercises. These first teach knowledge about a Linux working environment specially created for investigations in the OSINT area

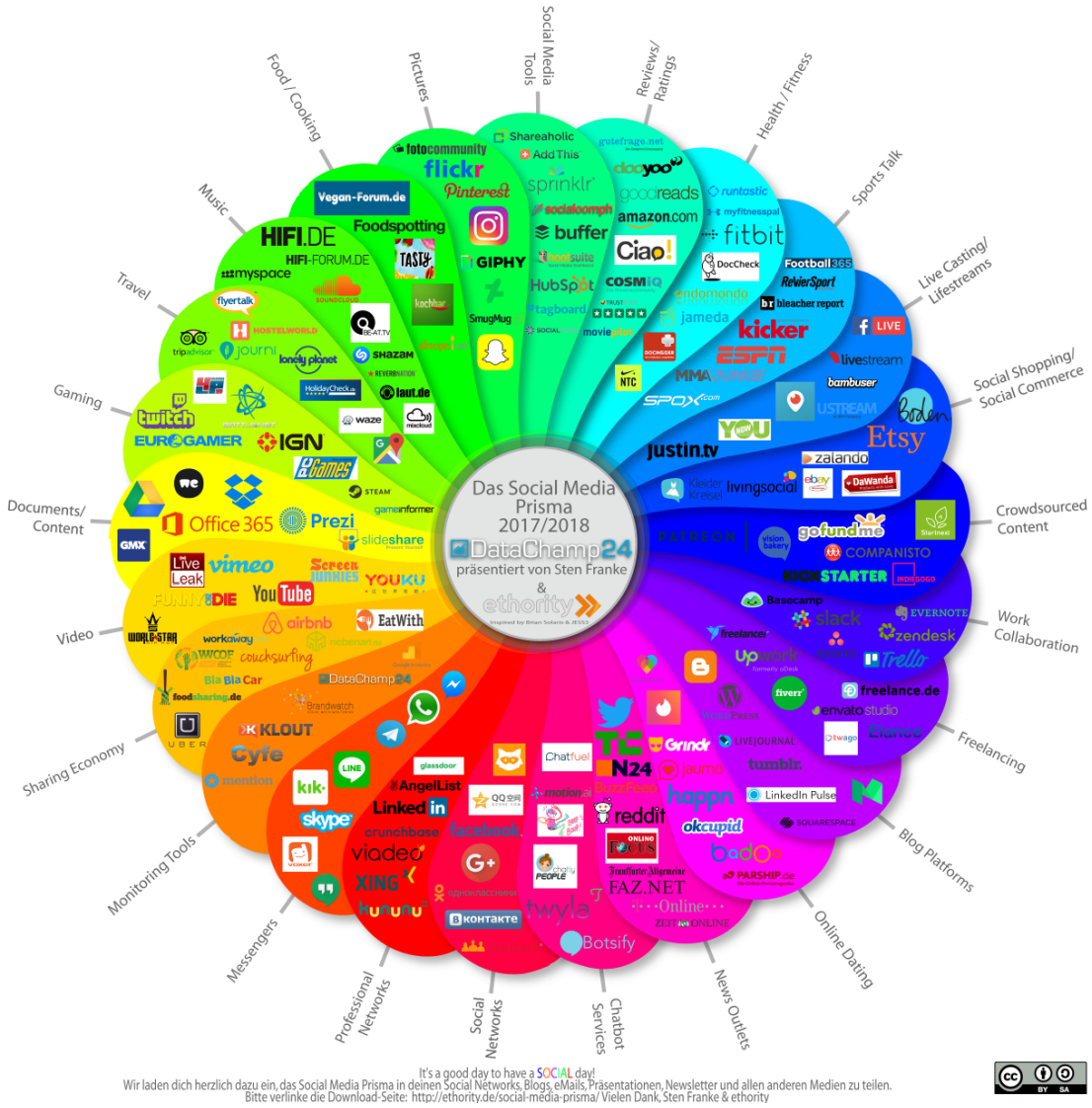


Figure 4. *Social Media Prisma 2017/2018*

and then the data acquisition in handling the presented free and commercial tools as well as the subsequent analysis and aggregation of the data to investigation results. In eleven practical exercises, the participants will learn the exact procedure that will enable them to work independently in the open-source intelligence world step by step. The first evaluations of the course showed consistently positive results. The OSINT methods were conveyed understandably. The encouragement of personal initiative is also highly praised. As the amount of work and time required to create the individual tasks was very high, not all ideas such as, for example, the search for personal data could be implemented. The creation of the sample solutions also required a lot of time and technical effort. Not all sources of error were foreseeable.

Future Work

It is planned to integrate the collection and enrichment of personal data from the most popular social networks into later versions of the open-source intelligence course. Besides, data mining, i.e., the enrichment of bulk data into investigation results, could also be dealt with in greater depth in a follow-up course.

Appendix

The appendix contains an illustrative timeline for information on the target audience, schedule, prerequisites, and objectives of the Open Source Intelligence Course.

Exercise No.	Target Group	Week No.	Time	Prerequisites	Objectives
1. Linux Shell Fundamentals	A, B, C, E	1	4 h	Independent	Introduction to the Linux shell
2. Linux File System Hierarchy Fundamentals	A, B, C, E	2	4 h	Exercise 1	Introduction to the Linux File System Hierarchy
3. Linux Pipe Fundamentals	A, B, C, D, F	3	4 h	Exercises 1-2	Organization, filtering and preparation of large amounts of data. Conversion of different formats into CSV.
4. Advanced Google Search	A, B, C, D, E, F	4	4 h	Independent	An introduction to working with Google Advanced Search
5. Linux Networking Tools	A, B, C, E	5	4 h	Exercises 1-3	Record communication, Collect information on systems in the LAN and WAN, Follow requests and analysis of communication.
6. Linux Forensics Tools	A, C, E, F	6	4 h	Exercises 1-3, 5	General principles of forensic investigations and related obligations.
7. Hacking Lab Environment (Preparation)	A, B, C, D, E, F	7,8	6 h – 32 h	Exercises 1-6	Modern sandbox environment to train the approach of Cybercriminals.
8. Passive Total	B, C, D, E, F	9-10	6 h	Independent, but Exercise 1,2,4 recommended	Detection of phishing, fraud, malware, and other online security threats with a cloud based tool.
9. Censys	B, C, D, E, F	10-11	6 h	Independent, but Exercise 1,2,4 recommended	Aggregation of bulk data on hosts and networks that make up the Internet.
10. Shodan	B, C, D, E, F	11-12	6 h	Independent, but Exercise 1,2,4	Getting to know the possibilities of banner grabbing. Introduction to working with the "most dangerous" search engine in the world.
11. Maltego	A, B, D (E, F)	12-16	16 h	Exercise 8,9,10 recommended	Introduction to real-time data mining.
			Total: 64 h		

Target Groups

A - Law Enforcement Investigator
B - Online Investigator
C - Preservation of Evidence Operator
D - Data Analyst
E - Bachelor Students of Cybersecurity
F - Master Student of Cybersecurity

References

[1] Mercado, Stephen C. "Sailing the Sea of OSINT in the Information Age." Secret intelligence: A reader 78 (2009).

[2] Best Jr, Richard A., and Alfred Cumming. "Open source intelligence (OSINT): issues for congress." December 5 (2007): 28.

[3] Glassman, Michael, and Min Ju Kang. "Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT)." Computers in Human Behavior 28.2 (2012): 673-682.

[4] Quick, Darren, and Kim-Kwang Raymond Choo. "Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINT+ OSINT): A timely and cohesive mix." Future Generation Computer Systems 78 (2018): 558-567.

[5] Williams, Heather J., and Ilana Blum. Defining second generation open source intelligence (OSINT) for the defense enterprise. RAND Corporation Santa Monica United States, 2018.

[6] Benes, Libor. "OSINT, new technologies, education: Expanding opportunities and threats. A new paradigm." Journal of Strategic Security 6.3 (2013): 22-37.

[7] Schaurer, Florian, and Jan Störger. "The evolution of open source intelligence (OSINT)." Journal of US Intelligence Studies 19.3 (2013): 53-56.

[8] Pringle, Robert W. "The limits of OSINT: Diagnosing the Soviet media, 1985-1989." International Journal of Intelligence and CounterIntelligence 16.2 (2003): 280-289.

[9] Gibson, Helen. "Acquisition and preparation of data for OSINT investigations." Open Source Intelligence Investigation. Springer, Cham, 2016. 69-93.

[10] Carroll, Jami M. "OSINT Analysis using Adaptive Resonance Theory for Conterterrorism Warnings." Artificial Intelligence and Applications. 2005.

[11] Best, Clive. "OSINT, the Internet and Privacy." EISIC. 2012.

[12] Casanovas, Pompeu. "Cyber warfare and organised crime. A regulatory model and meta-model for open source intelligence (OSINT)." Ethics and Policies for Cyber Operations. Springer, Cham, 2017. 139-167.

[13] Layton, Robert, and Paul A. Watters. Automating Open Source Intelligence: Algorithms for OSINT. Syngress, 2015.

[14] Steele, Robert David. "Open Source Intelligence (OSINT)."

[15] Berghel, Hal. "Robert David Steele on OSINT." Computer 47.7 (2014): 76-81.

[16] Weaver, Greg S. "Open Source Intelligence (OSINT)." The Police and the Military: Future Challenges and Opportunities in Public Safety 4.

[17] Revell, Quentin, Tom Smith, and Robert Stacey. "Tools for OSINT-Based Investigations." Open Source Intelligence Investigation. Springer, Cham, 2016. 153-165.

[18] Kalpakis, George, et al. "OSINT and the Dark Web." Open Source Intelligence Investigation. Springer, Cham, 2016. 111-132.

[19] Tabatabaei, Fahimeh, and Douglas Wells. "OSINT in the Context of Cyber-Security." Open Source Intelligence Investigation. Springer, Cham, 2016. 213-231.

[20] Danda, Matthew. "Open Source Intelligence and Cybersecurity." (2019).

[21] Steele, Robert D. "1997 OSINT What Is It Why Is It Important to the Military (White Paper)." Academia.edu - Share Research, Academia.edu, www.academia.edu/9817888/1997_OSINT_What_Is_It_Why_Is_It_Important_to_the_Military_White_Paper_.

[22] "Social Media Prisma 2017/2018, Ethority, ethority.de/social-media-prisma/.

[23] Mohsin, Maryam, et al. "10 Social Media Statistics You Need to Know in 2020 [Infographic]." Oberlo, Oberlo, 15 Jan. 2020, www.oberlo.com/blog/social-media-marketing-statistics.

[24] Tenzer: "Daten - Volumen Der Weltweit Generierten Daten 2025." Statista, Statista, 13 Feb. 2020, de.statista.com/statistik/daten/studie/267974/umfrage/prognose-zum-weltweit-generierten-datenvolumen/.

Author Biography

Klaus Schwarz received his B. Sc. in Computer Science from Technische Hochschule Brandenburg (Germany) in 2017. He is finishing his Master Thesis in 2020 and his research interests include IoT and Smart Home security, Embedded Systems, Artificial Intelligence, and Cloud Security.

Franziska Schwarz received her B.Sc. in Computer Science from Technische Hochschule Brandenburg (Germany) in 2019. Since 2019 she is working as scientific assistant in Technische Hochschule Brandenburg. Her research work is focused on IoT and Smart Home Security.

Reiner Creutzburg is a retired professor for Applied Informatics at the Technische Hochschule Brandenburg in Brandenburg, Germany. He is a member of the IEEE and SPIE and chairman of the Multimedia on Mobile Device (MOBMU) Conference at the Electronic Imaging conferences since 2005. His research interest is focused on Cybersecurity, Digital Forensics, Open Source Intelligence, Multimedia Signal Processing, eLearning, Parallel Memory Architectures, and Modern Digital Media and Imaging Applications.

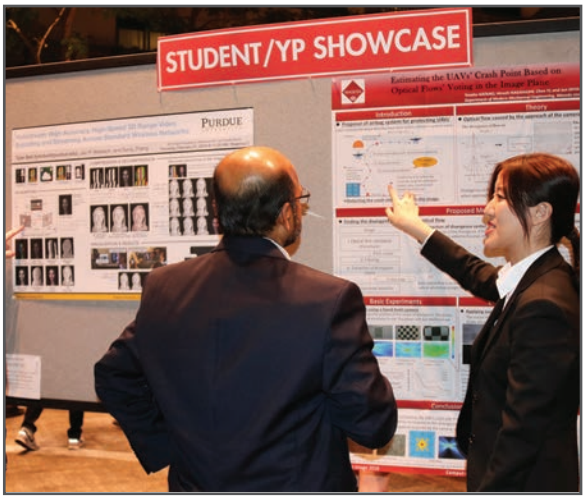
JOIN US AT THE NEXT EI!

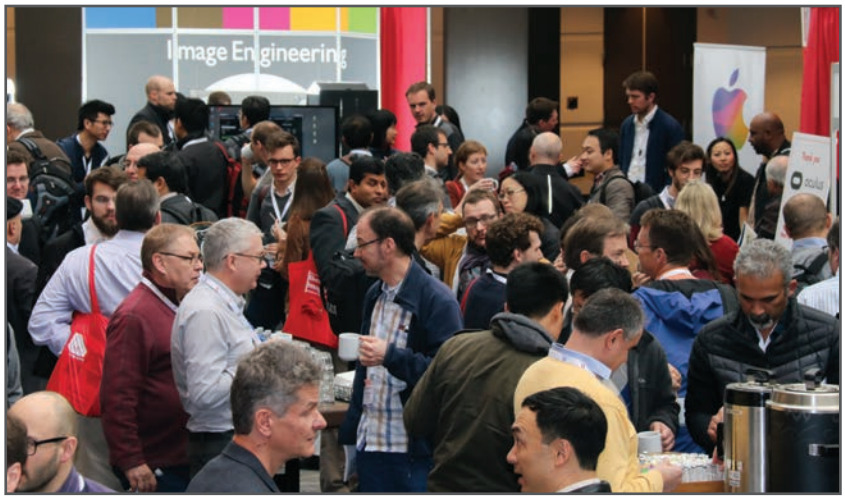
IS&T International Symposium on

Electronic Imaging

SCIENCE AND TECHNOLOGY

Imaging across applications . . . Where industry and academia meet!





• SHORT COURSES • EXHIBITS • DEMONSTRATION SESSION • PLENARY TALKS •
• INTERACTIVE PAPER SESSION • SPECIAL EVENTS • TECHNICAL SESSIONS •

www.electronicimaging.org

IS&T
imaging.org