Communications of the Association for Information Systems

Volume 53 Paper 45

12-12-2023

Ethical Hacking for a Good Cause: Finding Missing People using Crowdsourcing and Open-Source Intelligence (OSINT) Tools

Ersin Dincelli
University of Colorado Denver, ersin.dincelli@ucdenver.edu

Craig Van Slyke
Louisiana Tech University

Alper Yayla
University of Tampa

Recommended Citation

Dincelli, E., Van Slyke, C., & Yayla, A. (2023). Ethical Hacking for a Good Cause: Finding Missing People using Crowdsourcing and Open-Source Intelligence (OSINT) Tools. Communications of the Association for Information Systems, 53, 1052-1071. https://doi.org/10.17705/1CAIS.05345

Ethical Hacking for a Good Cause: Finding Missing People using Crowdsourcing and Open-Source Intelligence (OSINT) Tools

Cover Page Footnote

This manuscript underwent peer review. It was received 12/11/2022 and was with the authors for five months for one revision. Lee Freeman served as Associate Editor.

Communications of the Association for Information Systems

Education Article DOI: 10.17705/1CAIS.05345 ISSN: 1529-3181

Ethical Hacking for a Good Cause: Finding Missing People using Crowdsourcing and Open-Source Intelligence (OSINT) Tools

Ersin Dincelli
Information Systems
University of Colorado Denver
ersin.dincelli@ucdenver.edu
0000-0002-8773-4714

Craig Van Slyke
Computer Information Systems
Louisiana Tech University
0000-0003-3924-1859

Alper Yayla
Information and Technology Management Department
University of Tampa
0000-0002-0785-0601

Abstract:

Over 600,000 people go missing every year in the US alone. Despite the extensive resources allocated to investigating these cases, the high volume of missing person cases constitutes one of the biggest challenges for law enforcement agencies. One approach to tackle this challenge is using crowdsourcing. That is, volunteers use freely available tools and techniques to aid the existing efforts to investigate missing person cases. Open-Source Intelligence (OSINT) refers to gathering information from publicly available sources and analyzing it through a comprehensive set of open-source tools to produce meaningful and actionable intelligence. OSINT has been applied to address various societal challenges and crimes, including environmental abuse, human rights violations, child exploitation, domestic violence, disasters, and locating missing people. Building on this premise, this case examines a crowdsourced initiative called Trace Labs that aims to assist law enforcement agencies in solving missing person cases using OSINT tools. The case emphasizes socio-technical aspects of cybersecurity, highlighting both the bright and dark sides of technology. It demonstrates the potential of information systems to serve the public good by examining topics such as open-source software, crowdsourcing, and intelligence gathering, while acknowledging that the very same underlying technology can be used for malicious purposes.

Keywords: Cybersecurity, Ethical Hacking, Open-Source Intelligence, OSINT, Intelligence Gathering, Bright Side, Dark Side, Reconnaissance, Open-Source Software, Crowdsourcing, OSINT for Good.

This manuscript underwent peer review. It was received 12/11/2022 and was with the authors for five months for one revision. Lee Freeman served as Associate Editor.

1 Introduction

Contrary to the general perception, cybersecurity is not a highly technical field (Cram & D'Arcy, 2016). In fact, cybersecurity is a socio-technical field that demands instruction through a multi-disciplinary approach that requires a combination of human, social, and technical factors (Østby et al., 2019). Moreover, cybersecurity skills are best acquired with hands-on exercises that employ real-world scenarios within a collaborative setting (Dark, 2014; Plachkinova & Maurer, 2018), such as case studies that bring real-world issues and challenges into the classroom (Farhoomand, 2004; Hackney et al., 2003; Sipior et al., 2021). However, there is a limited number of teaching cases that specifically focus on the socio-technical dimensions of cybersecurity. This teaching case seeks to bridge this gap by emphasizing both the social and technical aspects of cybersecurity, focusing on the bright and dark sides of the technology following a hands-on approach to enrich the learning experience.

In this teaching case, students use information technology for the public good in the context of cybersecurity and intelligence gathering. The case is based on *Trace Labs*[1], a nonprofit organization with a mission to help find missing people through passive reconnaissance using open-source intelligence (OSINT). Trace Labs gamifies the crowdsourced search processes through its *Search Party Capture the Flag (CTF)* events. The case is structured as follows. First, students are introduced to the Trace Labs and *OSINT Framework*[2], a web-based interface that focuses on open-source intelligence-gathering tools. Afterward, students utilize various OSINT tools to collect information on missing people listed in law enforcement databases. Alternatively, students can choose to use the tools to collect information on themselves, their friends, or families, and various other alternatives. Finally, students reinforce their knowledge from hands-on activities with case questions on the public good, the bright and the dark sides of technology, open-source software, crowdsourcing, and intelligence gathering.

There are several learning objectives associated with this teaching case. First, it enhances students' technical skills that are necessary for becoming cybersecurity professionals. Second, it increases students' understanding of how technology can be used for the public good and sheds light on the potential for misuse and malicious intent that exists within the same technology. Third, it introduces students to several concepts relevant to information systems (IS), such as OSINT, open-source software, crowdsourcing, and intelligence gathering. Fourth, the case helps students increase their understanding of threats to their personal privacy from publicly available data sources. Finally, the activities in the case will help students better understand ethical issues related to OSINT tools by appreciating that they can be used for productive and nefarious purposes.

One of the unique characteristics of the intelligence gathering tools, and the majority of the cybersecurity tools (Yue et al., 2019), is that the same tool can be used by cybersecurity professionals to help individuals and organizations as well as malicious users to attack them since these tools are open-source and they can be accessed, used, and abused by anyone (Ball et al., 2012; Hribar et al., 2014). While interacting with the OSINT tools, students are not only exposed to the bright side of technology (i.e., intelligence gathering for the public good) but also acquainted with the dark side of technology (i.e., how others can gather information for malicious purposes). Thus, an indirect learning objective is to inform students on how these tools can be used for malicious purposes to increase their awareness of and resilience to future attacks.

Although the case is designed for cybersecurity and digital forensics classes, the multifaceted nature of the case allows it to be used in other IS classes that cover topics such as open-source software, crowdsourcing, business intelligence systems, digitalization, or ethics. In addition, we believe that the case holds benefits for any information systems student by helping them gain insights into the threats to their own privacy. By completing the case, students will have a greater appreciation of these threats. The *teaching notes* provide information on how students can better protect their privacy by requesting data removal. The increased understanding of threats to personal privacy will also help IS students better appreciate the importance of protecting users' privacy. Overall, the case provides students with a foundation on these critical IS concepts and how they can be applied to a real-world case. In the next section, we provide background information to familiarize readers with the concepts related to the case.

[1] Trace Labs: https://www.tracelabs.org/
[2] OSINT Framework Website: https://osintframework.com/

2 Background

2.1 Open-Source Software

Open-source software (OSS) is software that is released under a license that allows users to use, modify, develop, and distribute the software free of charge and without any restriction (O'Reilly, 1999). OSS is created and maintained mainly by developers, dedicated communities, and companies. While a sustainable business model is still challenging for smaller OSS projects, larger projects mostly use the freemium strategy. Host companies like RedHat, Mongo, and Canonical generate revenue through add-ons, professional support services, hosting services, software-as-a-service licensing, or similar business models (Gewirtz, 2016). However, the OSS projects have a low likelihood of success without voluntary participation. In other words, the success of OSS heavily depends on the number of developers and the effort they put into the project (Stewart & Gosain, 2006).

Despite the increasing interest, the adoption of OSS is still limited due to a lack of expertise and difficulty in assessing its quality (Lenarduzzi et al., 2020). Moreover, OSS can be less user-friendly compared to commercial software products. Furthermore, the development and updates of OSS may require more time, given its voluntary nature. Despite these drawbacks, the overall cost reduction has been the main driver for OSS adoption in the past. Today, the main reason for choosing OSS is access to innovation and the latest technology (Perez, 2022). Because OSS is free, it has allowed collaborative rather than competitive dynamics among its developers and users. Consequently, OSS had a positive impact on various industries, particularly in education, nonprofit organizations, and state and federal governments (Ahmad, 2021). Additionally, previous research has shown that gaining experience in OSS enhances the career development of IT students (Long, 2009). This case study gives students an opportunity to gain experience with OSS tools. Although this particular use of OSS is likely to be outside the scope of most IS workers' jobs, the experience will still benefit IS students by demonstrating some of the range of OSS capabilities.

The overall success of the OSS movement led commercial software companies like Microsoft to support this initiative (Barnes, 2020). One of the areas OSS has been heavily leveraged is cybersecurity. There is a wide range of OSS tools for cybersecurity professionals for penetration testing, vulnerability assessment, digital forensics, and other security assessment and analysis tasks. Some of the popular tools are Shodan, Nmap, Maltego, Recon-ng, and theHarvester. While most of these tools are available as standalone software, security-focused operating systems based on Linux (e.g., Kali Linux, Parrot OS) provide access to a collection of hundreds of cybersecurity tools. There are a myriad of tools available for intelligence gathering as well (Pastor-Galindo et al., 2020). These tools mainly utilize public data to collect, analyze, and present information on individuals and organizations. The next section focuses on open-source intelligence-gathering tools.

2.2 Open-Source Intelligence

Open-source intelligence (OSINT) refers to gathering information from publicly available sources and analyzing it through a variety of OSS to produce actionable intelligence. OSINT tools are mainly designed to find information using publicly available sources on the Internet, such as news articles, press releases, books, reports, images, and videos, as well as more restricted resources in the Deep Web and the Dark Web. Information gathering through OSINT has attracted people from diverse backgrounds, such as military personnel, journalists, human resource departments, law enforcement agencies, business analysts, penetration testers, and cybersecurity professionals.

There are a few websites that provide a list of OSINT tools, such as *Bellingcat's Online Investigation Toolkit*[3] created by a Netherlands-based investigative journalism group (Bellingcat, 2023) and the *OSINT Framework* developed by Justin Nordine in 2016[4]. The OSINT framework provides a structured categorization of the OSINT resources and tools based on task domains (Figure 1). These domains include email address, malicious file analysis, documentation, public records, business records, and people search engines. The framework provides one or more information gathering tools in each of these domains.

[3] Bellingcat's Online Investigation Toolkit: bit.ly/bcattools
[4] OSINT Framework Project on GitHub: https://github.com/lockfale/osint-framework/

The most common uses of OSINT include intelligence gathering, penetration testing (or ethical hacking), and malicious hacking. For example, intelligence agencies use OSINT to track events, weapon systems, and groups or people of interest. Similarly, law enforcement agencies use OSINT to gather information to help identify and rescue victims of crimes. While cybersecurity professionals use OSINT to identify technical vulnerabilities in information systems to find potential areas of weakness, malicious hackers use it to identify and exploit vulnerabilities for malicious purposes.

According to Sharma et al. (2021), there are three important functions that the OSINT tools provide. The first function is to *discover public-facing assets*. This function involves helping users discover information and map out what the information possesses and how it can contribute to a search task. The second function is to *discover information outside the organization*. This function looks for relevant information from outside the organization or network, such as social media communications. The third function is to *collect and combine the discovered information into an actionable intelligence*. Using OSINT tools on a specific target may result in vast amounts of unstructured data so it is important to convert the data discovered into a meaningful format that may lead to specific actions (Sharma et al., 2021). By serving these three functions, OSINT tools play a crucial role in intelligence gathering and can aid in digital investigations and other cybersecurity-related tasks.

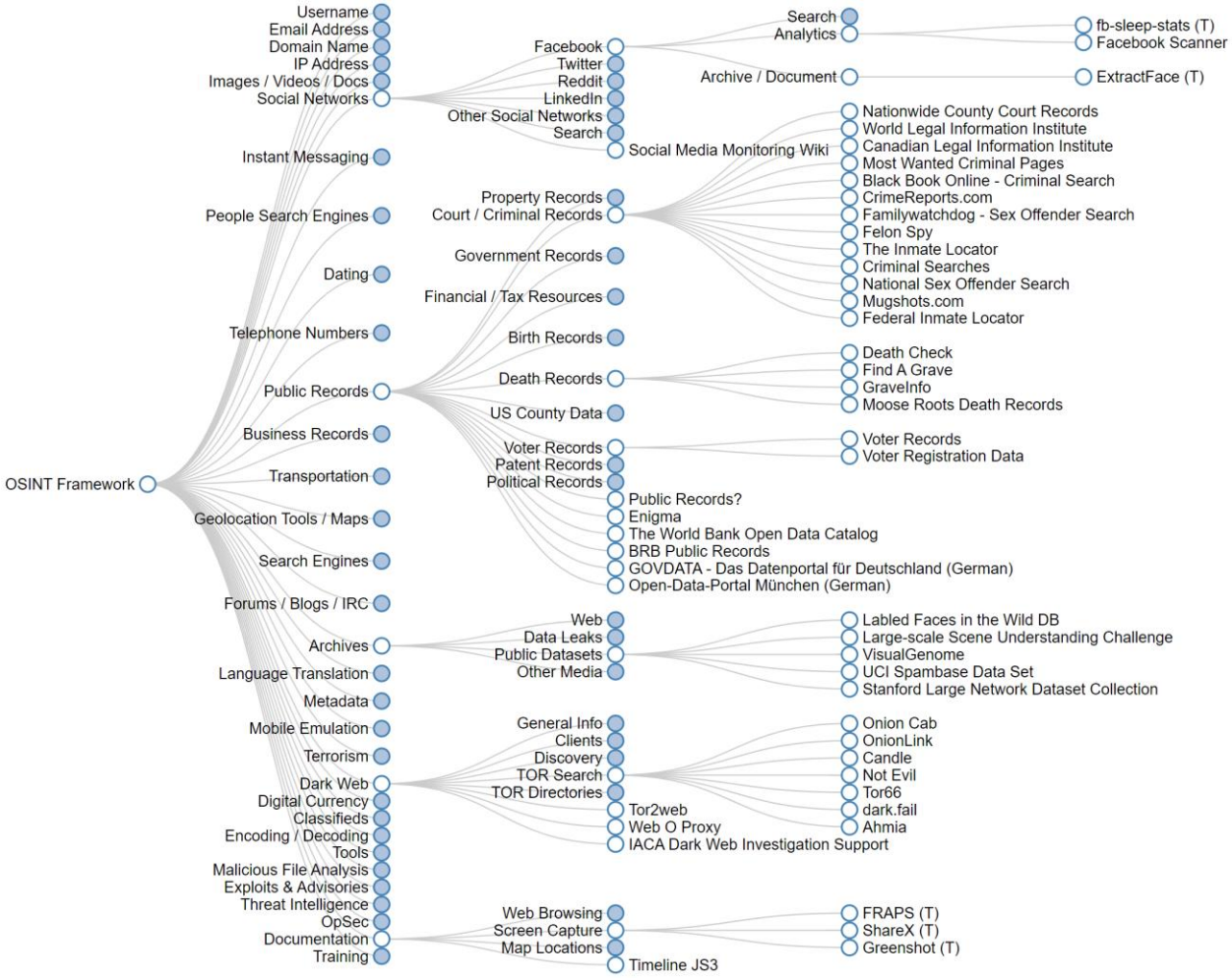

Figure 1. Sample Tools and Resources in the OSINT Framework

2.3 The Bright Side and the Dark Side of OSINT

OSINT has been used beyond its traditional application areas as well. For instance, one application of OSINT tools for the public good is in the public health context for early warning of diseases. *Global Public Health Intelligence Network (GPHIN)* is an event-based early warning system that scans open-source international news sources, reports, and rumors for potential chemical, biological, radiological, and nuclear

public health risks. *EpiWatch* is a similar tool that uses an AI-based surveillance system that searches open-source data to detect early signs of epidemics worldwide.

Nonprofit organizations also use OSINT for various causes, such as ensuring children's online safety and locating missing people. *The Internet Watch Foundation* identifies and removes child sexual abuse imagery and videos using OSINT. *The Innocent Lives Foundation* identifies child predators using OSINT and reports them to law enforcement agencies. *The BADASS Army* fights against revenge porn and image abuse. *The Stop the Traffik* fights against human trafficking. *The Environmental Investigation Agency* collects information to identify international environmental crimes and abuse, such as illegal logging, hunting, trade in wildlife, and pollution, using advanced OSINT techniques. *Trace Labs* assists law enforcement agencies in finding missing people using capture the flag (CTF) events. Table 1 presents some of the organizations that utilize OSINT for the public good.

Table 1. Nonprofit Organizations that Utilize OSINT for the Public Good

Initiative	Cause	Web Site
Trace Lab	Missing people	www.tracelabs.org
Locate International		www.locate.international
Night Owl Reconnaissance		www.nightowlrecon.org
Bellingcat	Human rights violations	www.bellingcat.com
Citizen Evidence Lab		www.citizenevidence.org
OSR4Rights		www.osr4rights.org
Innocent Lives Foundation	Child exploitation	www.innocentlivesfoundation.org
Internet Watch Foundation		www.iwf.org.uk
National Child Protection Task Force		www.ncptf.org
Global Emancipation Network	Human trafficking	www.globalemancipation.ngo
Stop the Traffik		www.stopthetraffik.org
The BADASS Army	Revenge porn	www.badassarmy.org
Environmental Investigation Agency	Environmental crimes	www.eia-international.org
Operation: SafeEscape	Domestic violence	www.safeescape.org

The line between the bright and the dark sides of OSINT can be very thin as the same type of information-gathered through OSINT can also be used for malicious purposes. For example, one of the main dark side applications of OSINT is reconnaissance for social engineering (Sood & Enbody, 2012). Hackers can leverage OSINT tools to gather and analyze information on their victims for targeted social engineering attacks. Information gathered through OSINT can help attackers compose more convincing attacks (Uehara et al., 2019), such as spear phishing (Ball et al., 2012). Another example is using public databases, search engines, and social networks to find, filter, and sort confidential data from organizations (Edwards et al., 2017). In addition to passive reconnaissance for gathering personal (e.g., social media profiles, contact details) and corporate information (e.g., employee details, usernames), attackers can use OSINT tools for active reconnaissance to collect information on corporate networks, devices, software, operating systems, and vulnerabilities (Kabanov & Madnick, 2021). After the initial information gathering phase, hackers can use OSINT tools to understand the security posture of the target organization, map out the organization's network structure, automate attacks, and exploit vulnerabilities. Other dark side applications of OSINT include espionage (Hribar et al., 2014), doxing (Khanna et al., 2016), and advanced persistent threats (Marchetti et al., 2016).

2.3.1 Trace Labs

Trace Labs is a nonprofit organization with the mission of training its members in the use of OSINT for finding missing people and uniting them with their families. Trace Labs works with law enforcement agencies to teach volunteers how to use OSINT tools to find information on missing people and help uncover new leads in both present and past cases through *search parties*. Trace Labs' search parties are a good example of how OSINT could be applied and scaled up using crowdsourcing. The goal of the search party is to harness the *Wisdom of the Crowd* through gamified capture the flag (CTF) events. These events are held at conferences such as Def Con and bring together researchers, analysts, hackers,

and other volunteers. Later, the Trace Labs intelligence officers triage the data collected from these CTF events and ongoing operations to generate actionable intelligence to be handed over to law enforcement agencies for further investigation. In addition, Trace Labs has partnered with industry and law enforcement agencies to provide OSINT education and awareness. Over ten thousand community members support the mission of Trace Labs and have contributed to 320 missing person cases through 35 search parties as of 2022 (Trace Labs, 2022).

2.3.2 Missing People

A missing person is defined as an individual who is missing either voluntarily or involuntarily. According to the National Missing and Unidentified Persons Systems (NamUS), over 600,000 people of all ages go missing in the United States every year (NamUS, 2022). Although the majority of missing people are quickly found, as of the end of 2021, the National Crime Information Center registered over 93,000 active cases, of which 42 percent involved individuals under 21 years of age (FBI, 2021). Moreover, there are also "missing" missing people, which are not accounted for in these statistics since they are not reported despite being missing. These unaccounted individuals include victims of human trafficking, illegal immigrants, homeless people, and sex workers (Quinet, 2012).

The large volume of missing people is one of the greatest challenges to local and state law enforcement agencies. Finding missing people is a demanding and resource-intensive task that involves multiple agencies and the families of the missing individuals (Fyfe et al., 2015). Enlisting volunteers to support the searches and using technological innovations may provide the needed assistance to law enforcement agencies and increase the success chance of the searches (Quinet, 2012). For example, social media (Tsoi et al., 2018), video surveillance (Vaquero et al., 2009), and face recognition (Sajjad et al., 2020) play a significant role in locating missing individuals. However, the sheer volume of missing person cases and limited resources to find them require sourcing models that can improve the process of finding missing people.

2.3.3 Crowdsourcing

Crowdsourcing is a form of outsourcing where a large number of participants produce a service or product using their competence and expertise (Howe, 2006; Zhao & Zhu, 2014). Howe (2006) coined the crowdsourcing term in 2006 and drew its similarities to the open-source principles. An online platform is generally used as an intermediary to attract the crowd and divide the task. The nature of the task varies from idea generation to funding. For their contribution, participants may receive monetary awards, nonmonetary awards like products or recognition, or no awards at all (Estellés-Arolas & González-Ladrón-de-Guevara, 2012). In other words, crowdsourcing is driven by the economic and philanthropic motivation of the participants (Lei et al., 2017).

Today, many popular applications of crowdsourcing exist from Wikipedia to KickStarter, Waze, and Amazon Mechanical Turk. One example of crowdsourcing in the context of missing people is the TrafficCam mobile app, which requires users to take photos of the hotel rooms they stay in when they travel. Since most traffickers advertise their victims using photos taken in hotel rooms, analysts can use image recognition to compare the hotel room of victim photos to the crowdsourced hotel room photos to identify possible matches (Stylianou et al., 2017).

3 Case Text: Finding Missing People Using OSINT

Open-source intelligence (OSINT) tools have become increasingly important for cybersecurity professionals. By successfully completing the activities in this case study, you will be able to:

1. *Discuss key concepts related to OSINT, intelligence gathering, footprinting and reconnaissance, open-source software, and crowdsourcing*.
2. *Understand how information systems and ethical hacking can be used for the public good.*
3. *Compare and contrast the bright side and the dark side of technology.*
4. *Perform intelligence gathering through various OSINT tools for finding publicly available information.*
5. *Apply ethical hacking techniques and OSINT tools to solve real-life problems.*
6. *Critically evaluate the reliability and validity of information obtained on the Internet.*

Technology allows us to weave privacy and security into the devices and applications we use. Yet, people often share more sensitive personal information on the Internet than they would in face-to-face communications. Given the tracking capabilities of electronic devices (e.g., smartphones and fitness trackers) and the growing trend of sharing personal information through social media and other online platforms, finding personal information, such as names, emails, home addresses, and geolocations, on the Internet has become trivial, which can have both positive and negative consequences, depending on how it is used and the context in which it is shared. Most people would probably be very surprised by the amount of information about them that can be found online through publicly available sources. This case will help you gain a better understanding of these sources, how they can be used for the public good, and how they represent a threat to personal privacy.

OSINT refers to the collection and analysis of information from publicly available sources on the Internet to produce intelligence. This type of intelligence gathering is facilitated by various open-source software tools, which are mainly designed to locate and extract information from publicly available sources, including social media posts, online databases, news articles, press releases, reports, images, and videos. OSINT tools can even be used to access more restricted resources within the Deep Web and the Dark Web. Individuals equipped with OSINT knowledge and skills can easily locate the specific information they are looking for. Organizations and government agencies can gather valuable information using OSINT that can aid them in decision-making and other important activities. However, malicious actors like black hat hackers can use this information for malicious purposes, such as finding vulnerabilities in information systems to launch cyber attacks, finding sensitive personal information to tailor their social engineering techniques, or committing identity theft.

But why not utilize these skills for the public good? Some white hat hackers will do just that! A community of hackers and online detectives have decided to dedicate themselves to finding missing people reported in public databases. This group of ethical hackers works for a nonprofit organization called Trace Labs.

Trace Labs is a nonprofit organization that works on OSINT education and awareness and brings together ethical hackers to leverage crowdsourced OSINT through gamified *search party* events. These ethical hackers volunteer their time and expertise and participate in capture the flag (CTF) competitions, where they search for possible information about missing people within the *search party* using publicly available sources. While they search for a missing person, these volunteers can submit relevant information to gain points and win prizes if they find any information about the individual in question. The information collected is used to produce actionable intelligence reports on each ongoing missing person case. Once information is found, it is handed over to law enforcement agencies to aid in their search efforts. Law enforcement agencies examine these reports for new information on missing person cases. Trace Labs has been successful in locating missing people, and their efforts have gained recognition in the cybersecurity community. By using their OSINT skills to help find missing people, Trace Labs demonstrates the positive use of OSINT for the public good.

What these ethical hackers essentially do as part of their OSINT activities is reconnaissance. Reconnaissance is the first step of ethical hacking, during which white hat hackers and online detectives gather as much information as possible about the target. Ethical hackers use various OSINT tools and techniques to collect and analyze information from publicly available sources. Through reconnaissance, ethical hackers can gather valuable information that can aid in their search for missing people or help organizations improve their cybersecurity posture. The OSINT framework is a comprehensive collection of open-source intelligence-gathering tools that helps hackers and online detectives for performing automated reconnaissance. This framework provides a user-friendly interface that categorizes a variety of OSINT tools based on their functionality, such as social networks, people search engines, public records, and geolocation tools, in a tree structure.

In the following video, Nathalie shares the heartbreaking story of her father's disappearance in 1988. This case is an example of a missing person case that remains unsolved for years, despite the efforts of law enforcement agencies. Ethical hackers have participated in search parties in which they have tried to find information on missing people, such as Nathalie's father, using OSINT tools. However, cases like Nathalie's father's can be especially challenging to solve, as they have been active for years. Nonetheless, ethical hackers and organizations such as Trace Labs continue to play an essential role in finding new information about missing people and raising awareness about missing person cases.

Hackers Find Missing People For Fun: https://youtu.be/2puBmXfi9Z0

Please note that the intelligence gathering in this case involves real individuals. Therefore, it is crucial to handle the investigation with the utmost care. Please follow the rules listed in the "Search Party Rules of Engagement" strictly during your investigation. These rules are designed by Trace Labs to ensure there is no illegal activity or interference in law enforcement investigations and we are respectful to missing individuals and their families.

These rules are designed by Trace Labs to maintain the integrity of the search and ensure that all search party members adhere to ethical and legal standards. If you have questions about this assignment or the rules, please contact your instructor for guidance and clarification.

Some of you may feel uncomfortable using OSINT on real missing people. If this is the case, you can answer the alternative questions provided by your instructor instead.

3.1 Suggested Case Questions

You are part of a search party that seeks to find information about missing people in the State of Colorado. Visit the Colorado Bureau of Investigation's Missing Person(s) Resource Page[5]. On this website, you will find a list of missing people in Colorado. Click on the list of people currently missing in Colorado to download the PDF. Use the reconnaissance skills you acquired throughout the class and try to find as much information as possible about a missing person of your choice using at least four different OSINT tools[6]. Be aware, however, that you can spend an almost endless amount of time on this search activity. Your instructor will give you guidance on how much time you should spend on your search[7]. After completing these tasks, answer the following questions.

3.1.1 Case Questions: OSINT

1. In your opinion, which collection (i.e., category) of the OSINT framework would be a good starting point for gathering information on missing people? Please provide at least two reasons why you chose the collection. Refer to the OSINT framework for the collections.
2. What specific OSINT tools did you use to find information about the missing person(s)? Why did you choose those tools? You can refer to the OSINT framework to select appropriate tools.
3. Describe your search process in detail. For example, did you try a wide range of OSINT tools to find information, or did you conduct a deep search by focusing on a small number of tools and go more deeply into them? What search strategies did you utilize?
4. Did you find any information regarding the missing person(s)? Have there been any leads, theories, or sightings?
5. How old is the case? Do you think that the year they went missing contributes to the state of their investigation? Explain your answer.
6. Did you find the OSINT framework useful to find information on missing people? Please provide a detailed explanation for how the OSINT contributed to finding the information you found.
7. As you performed your search, what ethical considerations did you take into account and how did you ensure that your actions were in line with ethical standards and best practices?
8. What did you learn regarding protecting your own privacy online? Did the case lead you to consider taking any steps to better protect your privacy? If so, what steps should you take? If not, why not?

3.1.2 Case Questions: The Bright and the Dark Sides of Technology

9. What are the advantages and disadvantages of having an extensive digital footprint over the Internet? How would you interpret the trade-off between these advantages and disadvantages?

[5] To make the case more appealing to the students, we suggest instructors change the location to the city, state, or country of the university the students are enrolled. Instructors can use their city's missing people resource pages or other databases, such as National Missing and Unidentified Persons Systems (NamUS).
[6] We suggest instructors familiarize students with OSINT and OSINT Framework before exposing students to the case.
[7] We recommend that instructors provide students with a range of time that students should spend on their search. Without this guidance, some students may spend an inordinate amount of time on the search.

10. How can OSINT tools be used for malicious purposes? Explain in detail.
11. The impact of technology on individuals and society can be multifaceted, with specific technologies having both positive and negative impacts depending on how they are used. How did the activities you completed for this case study affect your thinking about how the use of technology positively and negatively affects individuals and society?

3.1.3 Case Questions: Open-Source Software

12. How do open-source projects incorporate sound security practices to ensure confidentiality, integrity, and availability, and what benefits have been observed as a result?
13. Find three other examples of open-source software that can be used for the public good. Briefly describe their purpose.

3.1.4 Case Questions: Crowdsourcing

14. How is crowdsourcing being used in the cybersecurity field?
15. Find three other examples of crowdsourcing initiatives that are used for public good. Briefly describe each example.

3.2 Alternative Case Questions for OSINT to Avoid Potential Discomfort

Searching for missing people might be stressful for some students. Additionally, in certain cultures, people may be more sensitive when it comes to searching for others' personal information (Dincelli, 2018). Instructors can provide alternative case questions for the first six questions (see section *3.1.1 Case Questions: OSINT*) so that students who feel uncomfortable using OSINT on actual missing people would avoid potential negative effects (e.g., stress, anxiety, negative mood, etc.). The alternative questions can prompt students to conduct a search using OSINT tools on (1) themselves, (2) family and friends, (3) celebrities, (4) public figures, (5) known criminals such as FBI's ten most wanted fugitives[8], (6) fictional characters, or (7) already solved cases with positive outcomes. By using these alternative case questions, students can still understand the main concepts and principles of OSINT while avoiding any potential discomfort or stress that may arise from searching for actual missing people.

We provided detailed information on two specific alternatives: conducting OSINT search on themselves and on a recent crypto fugitive Do Kwon in our teaching note. However, we encourage instructors to prioritize searching for actual missing people, as even a small piece of information can make a significant difference in people's lives. If instructors do decide to use alternative case questions, we suggest they ask students to conduct a search on themselves, found criminals, or an already solved case with a good outcome, respectively. Based on our experience, searching on oneself may be the best option as this can provide instructors the opportunity to teach students how they can prevent potential sensitive personal information disclosure, including identity monitoring and management, removing personal information, such as an inappropriate photo, from the Internet, and other preventive actions to protect personal information. In the case of a found criminal, we recommend instructors use the case of crypto fugitive Do Kwon. We provide detailed instructions for both cases in our teaching note. We recommend that instructors add a disclaimer at the end of the case as follows to ensure students understand the nature of the case and make their own choices regarding the alternative path:

> *If you are uncomfortable using OSINT on actual missing people, you can skip questions 1-6 above and answer the following questions instead. If you decide to answer the above questions, you don't need to answer the following questions.*

1. Perform a search on yourself using tools from the OSINT Framework. Please explain in detail what you were able to find. Is there any information that you were surprised to find?
2. In your opinion, which collection (i.e., category) of the OSINT framework was a good starting point for gathering information about yourself? Please provide at least two reasons why you chose the collection. Refer to the OSINT framework for the collections.

[8] FBI - Ten Most Wanted Fugitives: https://www.fbi.gov/wanted/topten

3. What specific OSINT tools did you use to find information about yourself and why? You can refer to the OSINT framework to select appropriate tools.
4. Describe your search process in detail. For example, did you try a wide range of OSINT tools to find information, or did you conduct a deep search by focusing on a small number of tools and go more deeply into them? What search strategies have you utilized?
5. Did you find the OSINT framework useful to find information? Please provide a detailed explanation of how the OSINT framework contributed to finding the information you found.
6. Why would it be easier to find a recently missing person (i.e., after the 2000s) than others who went missing before the 2000s?

Instructors can use the same questions for the bright and the dark sides of technology (section 3.1.2), open-source software (section 3.1.3), and crowdsourcing (section 3.1.4) as they do not involve controversial questions that would impose adverse effects on students.

4 Evaluation of the Teaching Case

In order to evaluate the teaching case comprehensively, we gathered feedback from stakeholders with various backgrounds and experiences in cybersecurity, including university-level instructors, cybersecurity professionals, and undergraduate and graduate students. Additionally, we conducted pilot tests across multiple cybersecurity classes over a three-year period to iteratively improve the teaching case and assess its effectiveness.

4.1 Pre-test

To ensure its validity, a teaching case should be pre-tested by instructors and other subject-matter experts who are knowledgeable about the topic (Cappel & Schwager, 2002). Our case was circulated among a group of six instructors who teach information security and IS courses to determine its suitability for classroom use. Additionally, we sought feedback from three cybersecurity professionals to gain a broader perspective. Based on the feedback we received, we made improvements to the case to ensure that it effectively conveys the key concepts of OSINT and meets the needs of instructors.

Teaching cases are often only evaluated from the perspective of the instructors. In order to understand the value of a teaching case and ensure it meets the needs of students, it is important to evaluate it from the perspective of students as well (Havelka & Neal, 2015). Thus, we tested a version of the case in an introductory-level cybersecurity class. 40 students completed the case and provided feedback, which we used to improve the case. For example, one of the main improvements we made was to provide alternative case questions to reduce potential emotional stress, given the nature of the case, as recommended by both instructors and students during the pre-test.

4.2 Post-test

We used a mixed-methods approach to data collection to gain a comprehensive understanding of students' experiences with the final version of the teaching case. We used the teaching case in an ethical hacking class that was offered to both undergraduate and graduate students at a public university in the US. A total of 139 students (47 in year 1 and 92 in year 2) completed the case and participated in the subsequent discussion. To evaluate the effectiveness of the case, we collected both quantitative and qualitative data using an anonymous survey. Out of the 139 students who completed the case, 108 students (77.7%) completed the survey.

4.2.1 Quantitative Results

We used single-item measures to capture students' experiences and examined some of the important performance metrics, including *learning*, *interest*, *usefulness*, *curiosity*, *enjoyment*, and *relevance* (Lewis, 1992). We also assessed the constraints that students encounter while working on the assignment, such as *ease of learning* (Wetzlinger et al., 2014) and *mental demand* (Hart & Staveland, 1988). The scales were measured on a 7-point Likert scale. Appendix A includes the survey items. Table 2 shows the results of the evaluation survey. All performance metrics were above 6, stating that the teaching case performed well in all six different areas. Learning progresses fast and participation to the learning activity is maximized when the instructional content is neither too easy nor too difficult (Wilson et al., 2019). Our findings regarding ease of learning (M=4.26) indicate that students found the teaching case neither easy

nor difficult. The amount of mental demand (*M*=4.85) required to complete the teaching case was also deemed moderate. These results suggest that students perceived the teaching case as appropriately challenging and effective in learning the content.

Table 2. Teaching Case Evaluation Results (n=108)

Performance Metrics						Constraint Metrics	
Learning	Interest	Usefulness	Curiosity	Enjoyment	Relevance	Ease of Learning	Mental Demand
6.49	6.44	6.36	6.29	6.31	6.40	4.26	4.85

4.2.2 Qualitative Results

Out of the 108 students who participated in the survey, 69 students (63.89%) provided feedback by responding to a set of open-ended questions (see Table A2 in Appendix A). In this section, we identify important themes based on students' responses and highlight some of the feedback we received.

One of the primary goals of the teaching case was to demonstrate how some of the important aspects of information systems (e.g., crowdsourcing, open-source software, and cybersecurity skills) could be used for the public good. Students had the opportunity to put their technical skills into practice and realized the importance of cybersecurity for serving society. Accordingly, the first theme we identified was the potential of the teaching case to address societal issues and contribute to the public good:

> *Student 64: The case highlights the **intersection of technology, ethics, and community** engagement, showcasing how a **collective effort**, in this case, ethical hackers and law enforcement agencies, can be a powerful force for good in **addressing critical societal issues**.*
>
> *Student 75: Utilizing OSINT tools for the purpose of **assisting in the search for missing people** is one of the more **positive uses** for ethical hacking that I have encountered.*

The second theme we identified highlights the capacity of the teaching case to promote creativity and critical thinking through hands-on learning experiences grounded in a real-life scenario. This is particularly important for cybersecurity education as cybersecurity skills are best acquired through experiential learning within a collaborative classroom setting that uses engaging real-life examples students can relate to (Dark, 2014). Students stated that they were able to apply the skills they have gained throughout the course (i.e., utilizing open-source tools for information gathering) to a real-world and meaningful issue:

> *Student 3: The discussion case allowed us to think **creatively** and get a perspective of **real-world applications**.*
>
> *Student 11: I thought the discussion case was **interesting** and gave us the opportunity to **apply creative** and **critical thinking** to everyday issues.*
>
> *Student 94: The discussion case was **engaging** and made me **think**.*

The third theme highlights the potential of the teaching case in increasing the interest and curiosity towards learning more about cybersecurity. Given the growing cybersecurity workforce gap (ISC2, 2023), this theme highlights the potential of employing teaching cases as a strategic opportunity to bridge this gap. By leveraging engaging cases that increase curiosity about the cybersecurity field, educators can remove perceived barriers to cybersecurity, increase students' confidence, and ultimately increase their interest in pursuing a cybersecurity career (Giboney et al., 2021).

> *Student 31: The greatest strength of the case was **inciting the interest** of the students in cybersecurity. I personally gained a lot of knowledge. This class/case introduced me to a full new world with new tools. I have thoroughly enjoyed the assignment.*
>
> *Student 44: I got an opportunity to use OSINT tools for a real case which increased my **curiosity** about cybersecurity.*
>
> *Student 50: The case increased my **curiosity** to learn new tools.*

Relevance is a key criterion in the selection of teaching cases in order to actively engage students (Hackney et al., 2003). A teaching case that is relevant reinforces the key concepts and promotes the development of skills being taught more effectively (McFarlane, 2015). Relevancy emerged as the fourth

theme as students found the case not only relevant to cybersecurity and the concepts they learned in the classroom, but also to real life.

> *Student 38: I found the case so **fascinating** and very **relevant** to the world we live in, unfortunately.*
>
> *Student 88: The case provides a **unique approach** to learn cybersecurity and it is super **relevant**.*

The immersion and realism of the teaching case emerged as the fourth theme, which included two important elements for education and training applications (Dincelli & Chengalur-Smith, 2020). In contrast to traditional teaching cases where students often act as passive observers, our teaching case facilitated an immersive experience, enabling students to actively participate in and learn concepts as integral components of the case.

> *Student 38: Overall, I think this case study was incredible. It made me **feel like I really was on the job** of finding missing people and **felt like I was part of the team**, even though it was kind of like a simulation of trying out a career in cybersecurity.*
>
> *Student 57: It was very **realistic** to proceed with the investigation based on data from actual missing people. I was able to proceed with the investigation while maintaining a **high level of motivation**, with the thought that if I was lucky, I might be able to make a **contribution to society**.*

As discussed, we developed the case iteratively based on the feedback we received from instructors, cybersecurity professionals, and students. One vital piece of feedback we received was the potential adverse effects of the case. We included alternative questions to eliminate this issue as explained above. Students appreciated the alternative questions showing that the feedback we received and the way we improved the case were effective:

> *Student 65: I **appreciate** that alternative questions were provided. Although I think what Trace Labs does is an amazing use of technology and hacking skills, I **don't completely feel comfortable** searching for actual missing people myself. So, I will be answering the alternative questions.*

5 Discussion

The use of open-source tools is essential to cybersecurity professionals; familiarity with OSINT tools is similarly important (Pastor-Galindo et al., 2020). OSINT tools are useful for performing various cybersecurity-related tasks, such as penetration testing, vulnerability assessment, network analysis, threat intelligence, incident response, and identifying potential threat vectors, among other uses (Ball et al., 2012; Hribar et al., 2014). This teaching case provides students with a hands-on, socially-relevant, real-life opportunity to learn about OSINT and some of the available tools. Human trafficking is a significant social problem, and numerous nonprofit organizations use crowdsourced OSINT to help address the problem. In this case, students are asked to explore OSINT tools to find information about a real person. Alternative assignments are also provided for students who may find the context of the task upsetting. After engaging in their intelligence-gathering tasks, students answer a variety of questions designed to enhance their learning through critical assessment of tools and reflection on their experiences. Critical reflection is an example of reflection in action, which helps students expand their knowledge by solidifying their experiences and knowledge into a cohesive whole (Nonaka, 1994). In addition, students are asked to extend their learning by identifying potential risks to themselves through their online exposure. The context of the case not only helps students enhance their technical skills but also illustrates how technology can be used for the public good. In addition, the case introduces students to the concepts of open-source software and crowdsourcing. The activities embedded in the case also help students gain and enhance their intelligence-gathering skills, which will be useful for careers in cybersecurity and other related fields.

Although the case is especially well suited for students interested in cybersecurity, it is also beneficial to other IS students. Even if non-cybersecurity students may not need practical skills in OSINT and intelligence gathering, they should be aware of them conceptually. Open-source software is clearly an important part of many organizations' IT infrastructures and services. Conceptual knowledge of OSINT helps IS students understand important threats to information and personal privacy, such as spear

phishing that relies on personal information about the target (Goel et al., 2017). Crowdsourcing is an important IT-enabled phenomenon. Ethical hacking is an important social trend; all IS students should at least be familiar with the concept (Ulrich et al., 2023). In addition, IS students should have some appreciation for how IS can be used for both good and evil. Finally, all IS students need strong critical thinking skills and the ability to critically evaluate information reliability and validity. This case study can help IS students in all of these important areas.

An important element of the case is that it illustrates that OSINT, like many technologies and tools, can be used for good or evil (Hribar et al., 2014). The same tools that nefarious actors use to identify, stalk, and ensnare victims are also useful in tracking down and helping victims (Ball et al., 2012; Uehara et al., 2019). There are ongoing "bright side and dark side" conversations related to IT-enabled systems and related phenomena, such as artificial intelligence (AI) (e.g., Ågerfalk et al., 2022), social media (e.g., Baccarella et al., 2018), virtual worlds (Dincelli & Yayla, 2022), technostress (e.g., Califf et al., 2020), technology-related addictions (e.g., D'Arcy et al., 2014), sensor-based technologies (e.g., Marabelli et al., 2017), among others. Students may be unaware of the bright side/dark side nature of many technologies and practices. This case helps them gain an appreciation for this increasingly important dichotomy.

The case also provides a concrete example of how information systems can be used for an important public good. IS education is often focused on the use of information systems for economic benefit. Less attention is given to the use of information systems for public benefit, which is an important socio-technical aspect of IS (Zhang et al., 2010). This case illustrates in a dramatic fashion how information systems, OSINT specifically, not only can be used but are being used to address a critical social problem, which can be a starting point for discussion of additional means of using IS to address social challenges. Further, the bright side/dark side aspect of this case allows faculty to discuss ethical issues related to other important IS topics, such as AI, data collection and surveillance, telework, and others. In an era in which information technology is increasingly pervasive, it is important for students to understand the nuanced, grey areas of the societal effects of information technology.

By emphasizing the fact that open-source tools can be used to attack individuals, the case provides a secondary benefit of helping students understand the capabilities of OSINT tools. This may help reduce students' vulnerability to attacks that utilize such tools. Finally, this case provides a useful hands-on real-world unstructured cybersecurity task that requires students to engage in self-directed learning to address a real-world problem while enhancing their technical and critical thinking skills. Such hands-on experience is useful not only for building explicit knowledge of OSINT tools and processes but also important for accumulating related tacit knowledge (Nonaka, 1994). Students are required to make informed decisions and evaluations regarding the tools they use and the processes they employ. Due to the ever-evolving nature of cybersecurity, the ability to learn tools and techniques independently, and the ability to critically evaluate tools and processes are important for career success (Goles et al., 2008).

6 Conclusion

Every day, our society faces a growing number of challenges. While emerging technological innovations help us in addressing these challenges, their potential for misuse and abuse introduces new concerns. In other words, there is a thin line between the good (i.e., the bright side) and malicious uses of technology (i.e., the dark side), as the very same technology can be used for both positive and negative purposes (Salisbury et al., 2011). This is particularly true in the field of cybersecurity. Cybersecurity tools are prone to such misuse, given their capabilities; this is exemplified by the OSINT tools (Hribar et al., 2014; Ball et al., 2012). Cybersecurity professionals, law enforcement agencies, and volunteers from nonprofit organizations utilize OSINT to address various societal challenges and crimes, including environmental crimes and abuse, human rights violations, child exploitation, human trafficking, and domestic violence. Yet, the use of OSINT tools, like many other tools used by hackers (Ulrich et al., 2023), may still be considered a questionable activity due to their association with malicious activities perpetrated by black hat hackers and other criminals. This negative association can impact the overall reputation of such tools, leading to a decrease in their adoption within educational settings.

This teaching case provides a real-world and hands-on opportunity to explore the bright side applications of information technology. Simultaneously, it emphasizes the importance of ethical considerations and cautions against the potential dark side applications of information technology. By immersing students in an investigative process that leverages OSINT tools for intelligence gathering, it prompts them to reflect on the broader societal implications of cybersecurity and encourages critical thinking in navigating the

ethical considerations of cybersecurity tools widely used by professionals. In doing so, it aims to equip students not only with technical proficiency but also with an ethical framework for their future careers in the field of cybersecurity.

References

Ågerfalk, P., Conboy, K., Crowston, K., Eriksson Lundström, J., Jarvenpaa, S., Mikalef, P., & Ram, S. (2022). Artificial intelligence in information systems: State of the art and research roadmap. *Communications of the Association for Information Systems, 50*(1), 420-438.

Ahmad, R. (2021). A critical review of open source software development: Freedom or benefit libertarian view versus corporate view. *IEEE IT Professional, 23*(1), 16-26.

Baccarella, C. V., Wagner, T. F., Kietzmann, J. H., & McCarthy, I. P. (2018). Social media? It's serious! Understanding the dark side of social media. *European Management Journal, 36*(4), 431-438.

Ball, L., Ewan, G., & Coull, N. (2012). Undermining: Social engineering using open source intelligence gathering. In *Proceedings of the 4th International Conference on Knowledge Discovery and Information Retrieval* (pp. 275-280). Barcelona, Spain.

Barnes, H. (2020). Microsoft and open source: An unofficial timeline. *Box of Cables*. Retrieved from https://boxofcables.dev/microsoft-and-open-source-an-unofficial-timeline

Bellingcat. (2023). *Bellingcat's online investigation toolkit*. Retrieved from bit.ly/bcattools

Cram, W. A., & D'Arcy, J. (2016). Teaching information security in business schools: Current practices and a proposed direction for the future. *Communications of the Association for Information Systems, 39*(1), 32-51.

Cappel, J. J., & Schwager, P. H. (2002). Writing IS teaching cases: Guidelines for JISE submission. *Journal of Information Systems Education, 13*(4), 287-294.

Califf, C. B., Sarker, S., & Sarker, S. (2020). The bright and dark sides of technostress: A mixed-methods study involving healthcare IT. *MIS Quarterly, 44*(2), 809-856.

D'Arcy, J., Gupta, A., Tarafdar, M., & Turel, O. (2014). Reflecting on the "dark side" of information technology use. *Communications of the Association for Information Systems, 35*(1), 109-118.

Dark, M. (2014). Advancing cybersecurity education. *IEEE Security & Privacy, 12*(6), 79-83.

Dincelli, E. (2018). The role of national culture in shaping information security and privacy behaviors. In S. Goel (Ed.), *Innovation in Information Security, Vol. 4* (pp. 47-68). World Scientific Publishing.

Dincelli, E., & Chengalur-Smith, I. (2020). Choose your own training adventure: Designing a gamified SETA artefact for improving information security and privacy through interactive storytelling. *European Journal of Information Systems, 29*(6), 669-687.

Dincelli, E., & Yayla, A. (2022). Immersive virtual reality in the age of the Metaverse: A hybrid-narrative review based on the technology affordance perspective. *Journal of Strategic Information Systems, 31*(2).

Edwards, M., Larson, R., Green, B., Rashid, A., & Baron, A. (2017). Panning for gold: Automatically analysing online social engineering attack surfaces. *Computers & Security, 69*, 18-34.

Estellés-Arolas, E., & González-Ladrón-de-Guevara, F. (2012). Towards an integrated crowdsourcing definition. *Journal of Information Science, 38*(2), 189-200.

Farhoomand, A. (2004). Writing teaching cases: A reference guide. *Communications of the Association for Information Systems, 13*(1), 103-107.

FBI. (2021). 2021 NCIC missing person and unidentified person statistics. *FBI*. Retrieved from https://www.fbi.gov/file-repository/2021-ncic-missing-person-and-unidentified-person-statistics.pdf

Finneran, C. M., & Zhang, P. (2005). Flow in computer-mediated environments: Promises and challenges. *Communications of the Association for Information Systems, 15*(1), 82-101.

Fyfe, N. R., Stevenson, O., & Woolnough, P. (2015). Missing persons: The processes and challenges of police investigation. *Policing and Society, 25*(4), 409-425.

Gewirtz, D. (2016). Nothing good is free: How Linux and open source companies make money. Retrieved from https://www.zdnet.com/home-and-office/networking/nexuslink-ethernet-over-coax-adapter-kit-review

Giboney, J. S., McDonald, J. K., Balzotti, J., Hansen, D. L., Winters, D. M., & Bonsignore, E. (2021). Increasing cybersecurity career interest through playable case studies. *TechTrends, 65*, 496-510.

Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human vulnerability. *Journal of the Association for Information Systems, 18*(1), 22-44.

Goles, T., White, G. B., & Dietrich, G. (2008). Dark screen: An exercise in cyber security. *MIS Quarterly Executive, 4*(2), 303-317.

Hackney, R., McMaster, T., & Harris, A. (2003). Using cases as a teaching tool an IS education. *Journal of Information Systems Education, 14*(3), 229-234.

Hart, S. G., & Staveland, L. E. (1988). Development of NASA-TLX (Task Load Index): Results of empirical and theoretical research. In Hancock P. A., & Meshkati N. (Eds.), *Human Mental Workload*. North Holland.

Havelka, D., & Neal, C. (2015). A basic set of criteria for evaluation of teaching case studies: Students' perspective. *Information Systems Education Journal, 13*(4), 41-50.

Howe, J. (2006). *The rise of crowdsourcing*. Wired. Retrieved from https://www.wired.com/2006/06/crowds

Hribar, G., Podbregar, I., & Ivanuša, T. (2014). OSINT: A "grey zone"? *International Journal of Intelligence and CounterIntelligence, 27*(3), 529-549.

ISC2. (2023). *Cybersecurity workforce study 2023*. ISC2. Retrieved from https://www.isc2.org/research

Kabanov, I., & Madnick, S. (2021). Applying the lessons from the Equifax cybersecurity incident to build a better defense. *MIS Quarterly Executive, 20*(2), 1-17.

Khanna, P., Zavarsky, P., & Lindskog, D. (2016). Experimental analysis of tools used for doxing and proposed new transforms to help organizations protect against doxing attacks. *Procedia Computer Science, 94*, 459-464.

Lei, Y., Yayla, A., & Kahai, S. (2017). Guiding the herd: The effect of reference groups in crowdfunding decision making. In *Proceedings of the 50th Hawaii International Conference on System Sciences (HICSS)* (pp. 1912-1921). Waikoloa Village, HI.

Lenarduzzi, V., Taibi, D., Tosi, D., Lavazza, L., & Morasca, S. (2020). Open source software evaluation, selection, and adoption: A systematic literature review. In *Proceedings of the 46th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)* (pp. 437-444). IEEE.

Lewis, J. R. (1992). Psychometric evaluation of the post-study system usability questionnaire: The PSSUQ. In *Proceedings of Human Factors and Ergonomics Society Annual Meeting* (pp. 1259-1263). Los Angeles, CA.

Long, J. (2009). Open source software development experiences on the students' resumes: Do they count? - Insights from the employers' perspectives. *Journal of Information Technology Education: Research, 8*(1), 229-242.

McFarlane, D. A. (2015). Guidelines for using case studies in the teaching-learning process. *College Quarterly, 18*(1).

Marabelli, M., Hansen, S., Newell, S., & Frigerio, C. (2017). The light and dark side of the black box: Sensor-based technology in the automotive industry. *Communications of the Association for Information Systems, 40*(1), 351-374.

Marchetti, M., Pierazzi, F., Guido, A., & Colajanni, M. (2016). Countering advanced persistent threats through security intelligence and big data analytics. In *Proceedings of the 8th International Conference on Cyber Conflict (CyCon)* (pp. 243-261). IEEE.

National Missing and Unidentified Persons Systems (NamUS). (2022). The nation's silent mass disaster. Retrieved from https://namus.nij.ojp.gov/#the-nations-silent-mass-disaster

Nonaka, I. (1994). A dynamic theory of organizational knowledge creation. *Organization Science*, *5*(1).

O'Reilly, T. (1999). Lessons from open-source software development. *Communications of the ACM, 42*(4).

Østby, G., Berg, L., Kianpour, M., Katt, B., & Kowalski, S. J. (2019). A socio-technical framework to improve cyber security training: A work in progress. In *Proceedings of the 5th International*

Workshop on Socio-Technical Perspective in IS Development (STPIS) (pp. 81-96). Stockholm, Sweden.

Pastor-Galindo, J., Nespoli, P., Mármol, F. G., & Pérez, G. M. (2020). The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. *IEEE Access, 8*, 10282-10304.

Perez, J. (2022). *10 reasons why companies choose OpenLogic for OSS support*. OpenLogic. Retrieved from https://www.openlogic.com/blog/why-companies-choose-openlogic-oss-support

Plachkinova, M., & Maurer, C. (2018). Security breach at Target. *Journal of Information Systems Education, 29*(1), 11-20.

Quinet, K. (2012). *Missing persons. Problem-oriented guides for police. Problem-specific guides series No. 66*. Department of Justice. Retrieved from https://popcenter.asu.edu/content/problem-specific-guides-web-guide-number

Sajjad, M., Nasir, M., Muhammad, K., Khan, S., Jan, Z., Sangaiah, A. K., Elhoseny, M., & Baik, S. W. (2020). Raspberry Pi assisted face recognition framework for enhanced law-enforcement services in smart cities. *Future Generation Computer Systems, 108*, 995-1007.

Salisbury, W., Miller, D. W., & Turner, L. C. J. M. (2011). On contending with unruly neighbors in the global village: Viewing information systems as both weapon and target. *Communications of the Association for Information Systems, 28*(1), 20.

Sharma, A., Breeden, J., & Fruhlinger, J. (2021). 15 top open-source intelligence tools. *CSO Online*. Retrieved from https://www.csoonline.com/article/3445357/what-is-osint-top-open-source-intelligence-tools.html

Sipior, J. C., Granger, M., & Farhoomand, A. (2021). Writing a teaching case and teaching note: A reference guide. *Communications of the Association for Information Systems, 49*(1), 659-667.

Sood, A. K., & Enbody, R. J. (2012). Targeted cyberattacks: A superset of advanced persistent threats. *IEEE Security & Privacy, 11*(1), 54-61.

Stewart, K. J., & Gosain, S. (2006). The impact of ideology on effectiveness in open source software development teams. *MIS Quarterly, 30*(2), 291-314.

Stylianou, A., Schreier, J., Souvenir, R., & Pless, R. (2017). TraffickCam: Crowdsourced and computer vision based approaches to fighting sex trafficking. In *Proceedings of Applied Imagery Pattern Recognition Workshop (AIPR)* (pp. 1-8). IEEE.

Trace Labs. (2022). Trace labs. Retrieved from https://www.tracelabs.org

Tsoi, K. K., Zhang, L., Chan, N. B., Chan, F. C., Hirai, H. W., & Meng, H. M. (2018). Social media as a tool to look for people with dementia who become lost: Factors that matter. In *Proceedings of the 51st Hawaii International Conference on System Sciences (HICSS)* (pp. 3355-3364). Waikoloa Village, HI.

Uehara, K., Mukaiyama, K., Fujita, M., Nishikawa, H., Yamamoto, T., Kawauchi, K., & Nishigaki, M. (2019). Basic study on targeted e-mail attack method using OSINT. In *Proceedings of the International Conference on Advanced Information Networking and Applications (AINA)* (pp. 1329-1341). Matsue, Japan.

Ulrich, F., Müller, S. D., & Flowers, S. (2023). The professionalization of hackers: A content analysis of 30 years of hacker communication. *Communications of the Association for Information Systems, 52*(1), 556-585.

Vaquero, D. A., Feris, R. S., Tran, D., Brown, L., Hampapur, A., & Turk, M. (2009). Attribute-based people search in surveillance environments. In *Proceedings of Workshop on Applications of Computer Vision (WACV)* (pp. 1-8). Snowbird, UT.

Wetzlinger, W., Auinger, A., & Dörflinger, M. (2014). Comparing effectiveness, efficiency, ease of use, usability and user experience when using tablets and laptops. In *Proceedings of the 3rd International Conference of Design, User Experience, and Usability* (pp. 402-412). Crete, Greece.

Wilson, R. C., Shenhav, A., Straccia, M., & Cohen, J. D. (2019). The eighty five percent rule for optimal learning. *Nature Communications, 10*(1), 1-9.

Yue, W. T., Wang, Q. H., & Hui, K. L. (2019). See no evil, hear no evil? Dissecting the impact of online hacker forums. *MIS Quarterly, 43*(1), 73-95.

Zhang, W., Gutierrez, O., & Mathieson, K. (2010). Information systems research in the nonprofit context: Challenges and opportunities. *Communications of the Association for Information Systems, 27*(1),1-12.

Zhao, Y., & Zhu, Q. (2014). Evaluation on crowdsourcing research: Current status and future direction. *Information Systems Frontiers, 16*(3), 417-434.

Appendix A: Assessment of the Case

After students completed the case assignment, we asked them to evaluate it using a survey and open-ended questions:

> *You completed a case assignment called "Ethical Hacking for a Good Cause: Finding Missing People using Crowdsourcing and Open-Source Intelligence (OSINT) Tools" in the previous week. The following questions will ask about your learning experience related to the case assignment so that we can improve it for future classes based on your feedback.*
>
> *There are no right or wrong answers to the questions in this survey. We simply ask for your opinion about the case assignment you completed. Please read each statement carefully and choose the best answer that applies to you. This survey is completely anonymous. There is no way to link your name with the answers. Please provide your honest opinion about the case.*
>
> *Please think about "Ethical Hacking for a Good Cause: Finding Missing People using Crowdsourcing and Open-Source Intelligence (OSINT) Tools" case assignment that you completed last week and answer the following questions.*

Table A1. Case Evaluation Questions

	Metric	Question	Source
Performance Metrics	Learning	I gained new knowledge from the case assignment.	Lewis (1992)
	Usefulness	The case assignment was useful to learn about cybersecurity and/or related topics.	Lewis (1992)
	Relevance	Overall, the case assignment was relevant to cybersecurity and/or related areas.	Havelka and Neal (2015)
	Enjoyment	Overall, I enjoyed the case assignment.	Finneran and Zhang (2005)
	Curiosity	The content of the case assignment piqued my curiosity.	Self-developed
	Interest	Problems posed in the case assignment increased my interest in cybersecurity and/or related topics.	Self-developed
Constraints	Ease of Learning	Overall, how difficult, or easy was it to complete the case assignment?	Wetzlinger et al. (2014)
	Mental Demand	How mentally demanding was the case assignment?	Hart and Staveland (1988)

Table A2. Open Ended Evaluation Questions

Question	Source
What are the strengths of the case assignment?	Havelka and Neal (2015)
What are the weaknesses of the case assignment?	
What could be done to improve the case assignment?	
Do you have any additional comments or suggestions about the case assignment?	

About the Authors

Ersin Dincelli is an Assistant Professor of Information Systems in the Business School at the University of Colorado Denver. Dr. Dincelli received his MBA and Ph.D. in Informatics from the University at Albany, State University of New York, where he received the *Distinguished Dissertation Award 2018-2019*. Dr. Dincelli's research concerns the behavioral aspects of information security and human-computer interaction (HCI). In particular, he studies individuals' decision-making processes and behaviors in the context of information security and privacy, social engineering attacks, privacy-invasive technologies (e.g., social media and wearable devices), designing innovative security education, training, and awareness (SETA) programs, and HCI design for emerging technologies (e.g., AI, blockchain, and virtual reality). Dr. Dincelli has published in academic journals, such as the *Journal of the Association for Information Systems*, *European Journal of Information Systems*, *Journal of Strategic Information Systems*, *Government Information Quarterly*, *Information Systems Frontiers*, *Behaviour & Information Technology*, *IEEE IT Professional*, and in the proceedings of leading information systems and security conferences.

Craig Van Slyke is the Mike McCallister Eminent Scholar Chair in Information Systems at Louisiana Tech University. Prior to joining Tech, he was professor and dean of the W.A. Franke College of Business at Northern Arizona University, and before that, professor, associate dean and department chair at Saint Louis University. He has also held faculty positions at the University of Central Florida, and Ohio University. He holds a Ph.D. in Information Systems from the University of South Florida. His current research focuses on behavioral aspects of information technology, cyber security, and privacy. Dr. Van Slyke has published over fifty articles in respected academic journals including Communications of the AIS, Decision Sciences, Communications of the ACM, European Journal of Information Systems, The DATA BASE for Advances in Information Systems, and Journal of the Association for Information Systems. The fifth edition of his fourth co-authored textbook, Information Systems in Business: An Experiential Approach, will be published in 2024.

Alper Yayla is an Associate Professor and the Director of the Cybersecurity Programs in the Sykes College of Business at The University of Tampa. He earned his Ph.D. degree in Management Information Systems from Florida Atlantic University. His research interest is the impact of technology on organizations and individuals, with a focus on cybersecurity and emerging technologies. His work has been published in several academic journals, including *Decision Sciences*, *European Journal of Information Systems*, *Journal of Information Technology*, *Journal of Strategic Information Systems*, *International Journal of Electronic Commerce*, *Information Systems Management,* and *IEEE IT Professional,* as well as in the proceedings of various academic conferences.