DEVELOPING & MAINTAINING AN OPEN SOURCE INVESTIGATION CAPACITY FROM SCRATCH

Workshop Report

United Nations

International, Impartial and Independent Mechanism الآليّة الدوليّة المحايدة والمستقلة
to Assist in the Investigation and Prosecution of Persons Responsible for the Most Serious Crimes under International Law Committed in the Syrian Arab Republic since March 2011

TABLE OF CONTENTS

FOREWORD BY THE DEPUTY HEAD OF THE IIIM

The International, Impartial and Independent Mechanism (IIIM) was established by a Resolution of the United Nations General Assembly in December 2016. Resolution 71/248 created a new type of institution—the first in a new generation of bodies with a 'quasi-prosecutorial' function—to assist in the investigation and prosecution of persons responsible for the most serious crimes under International Law committed in the Syrian Arab Republic since March 2011.

The GA mandated the IIIM to carry out three essential yet interconnected tasks:

- Collect, consolidate and preserve information and "evidence of violations of international humanitarian law and human rights violations and abuses";
- Analyze this collected evidence and prepare "files in order to facilitate and expedite fair and independent criminal proceedings"; and
- Share information and evidence collected and analytical work produced with national, regional and international courts.

Since its creation in 2016, the IIIM has grown from a small start-up team to an indispensable source of support for a broad range of justice actors working on cases concerning core international crimes in Syria. The interests of victims/survivors are the compass guiding all of the IIIM's work and their views and priorities inform the IIIM's vision and are the measure of its success.

To achieve this vision, each section of the IIIM works collaboratively to fulfill the mandate, guided by a Victim/Survivor-Centered Approach (VSCA) and commitment to inclusive justice.

In 2018, when we started our operations, the IIIM faced a high level of disillusionment among victims/survivors and affected community civil society organizations (CSOs), who felt that little had been done to stop the violations in Syria and deliver justice. The IIIM had an additional layer of challenge in giving meaning to victim/survivor-centeredness in the context of its novel mandate, requiring fresh thinking. We devised platforms for two-way dialogue and supplemented these engagements by developing thematic strategies on gender, children and youth, and broader justice objectives.

Each section within the IIIM is responsible for integrating these strategies and inclusive approaches into core daily workflows. We have been testing, piloting and adjusting approaches and our internal architecture in support of our inclusive justice objective. Aspects of this are quite novel, and present challenges for the teams.

While the benefits of using open source information to investigate international crimes and human rights violations are well understood, the question of how—how to effectively and efficiently utilize open sources in support of inclusive justice—has received little attention. What must be considered? And how do we build up this organizational capacity?

Our October 2024 closed workshop on developing open source capacity from scratch was designed to take a look back at the "how" of this process, to address the operational gaps, to share lessons learned from IIIM's "start-up" days, and to foster continued collaboration amongst a growing community of practitioners. We encouraged participants to share their experiences, insights, acquired knowledge, and still-unresolved challenges.

We hope the workshop promoted more inclusive justice outcomes for historically marginalized communities and made a positive mark on the ever-expanding accountability ecosystem. A heartfelt thank you goes out to all panelists and participants for joining us.

Michelle Jarvis
Deputy Head
IIIM-Syria

PURPOSE OF THE WORKSHOP

The benefits of open source information in investigations of violations of international criminal, human rights, and humanitarian law are widely acknowledged and well-documented.

However, issues relating to establishing dedicated open source investigation operational capacities have garnered less attention, particularly in defining relevant processes and building the necessary infrastructure to support open source investigators. These issues are not unique to any one organization, but impact investigative and accountability bodies involved in open source activities worldwide.

Over the years, open source investigations have gained significant traction among organizations with accountability and and investigative mandates. These investigations rely heavily on publicly available information. While anyone can use freely available information at little to no cost, entities often struggle with developing and maintaining the operational capacity to conduct such investigations at an organizational level. To that end, the workshop aimed to fill that gap by shifting the focus from the benefits of open source investigations to the "how"—that is, the operational issues related to developing and maintaining the necessary infrastructure to conduct open source investigations and manage the underlying information and evidence.

To address this gap, the IIIM invited international organizations focused on accountability and investigations, non-governmental organizations (NGOs), and CSOs to a closed workshop on information and evidence management in the context of open source investigations. The event itself was situation-neutral and did not involve sharing substantive information about any open source investigations or analyses. It was held online on Wednesday, 23 October 2024.

This workshop provided participants with a unique opportunity to share best practices and lessons learned from leading organizations in the field. Case studies and panel discussions addressed the following topics:

- Identifying the right infrastructure and skills needed.
- Investigators versus infrastructure: which comes first?
- Understanding the Electronic Discovery Reference Model (EDRM) in the context of open source investigations involving large volumes information and evidence.
- Information management: why it is important, how to do it, what works, and what does not?
- Managing multimedia content.
- The analyst's dilemma: what constitutes evidence? How does it differ from information? How to collect and preserve online material?
- Generating value from a large volume of collected data.

This report outlines the fundamental concepts covered in each of the three panels, with an eye toward capturing key takeaways and lessons learned. The workshop followed the Chatham House Rule to encourage open discussion amongst participants. For this reason, no participant names will be used in this report. Everything that follows is simply a summary of the proceedings and points discussed by participants during the workshop.

PANEL 1: BUILDING AN INFRASTRUCTURE TO SUPPORT AND CONDUCT OPEN SOURCE INVESTIGATIONS

Infrastructure is a core component of any open source investigation capacity. Why? Because it enables investigators to securely access the web while also allowing for the effective collection, preservation, and analysis of information and evidence. This infrastructure must be governed by strict processes and policies.

Infrastructure is a varied, core component of open source investigation capacity, which must be tailored to mission requirements. It should not be perceived as a commercial solution, but rather as a customized set of hard- and software that forms an integrated system. This system in turn allows organizations to carry out their mission in a safe, secure, and efficient manner by providing secure access to the world wide web, and appropriate tools to collect and preserve data. In other words, having the right infrastructure in place makes information and evidence easily accessible to colleagues for review, analysis, and more.

Open source investigations refer to the systematic collection and analysis of publicly available data. One of the primary challenges many organizations face is the sheer volume of data in multiple formats. Organizations must also verify the accuracy of that data, which can be time consuming and lead to inefficiency and ineffectiveness. This can sometimes make working with open sources feel like filling a cup from a firehose: the hose keeps expanding, pushing out more and more water, until the cup eventually overflows. Similarly, the amount of data available can be overwhelming at times. To overcome such data saturation—to stop the proverbial cup from spilling over—organizations should consider investing in robust infrastructure.

Infrastructure constitutes a core component of an open source investigation capacity. As mission requirements differ between organizations, the underlying infrastructure must be tailored accordingly. For example, there is a difference between organizations that have a broad mandate to collect vast amounts of various data types, and smaller organizations that might only require the collection of a single data type, such as text documents. Nevertheless, there are fundamental principles that apply across the board. These principles inform the development and maintenance of infrastructure that aligns with an organization's mission and vision.

Key Factors to Consider

Custom versus Off-the-Shelf Solutions

Workshop participants agreed that there is no single off-the-shelf solution for every organization. The infrastructure should be tailored to each organization's mission. Developing and maintaining this infrastructure requires professionals with the right skillset and expertise.

The Team

A successful team should include professionals with a strong technical background for custom development and demonstrated experience in information and evidence management, data analysis and open source investigation. The combined expertise lays the foundation for a strong open source investigation capacity.

The Fundamentals

Participants agreed that a robust infrastructure must encompass everything from providing safe and secure internet access to acquiring the appropriate tools for collecting and managing information and evidence. What follows are six fundamentals discussed during the panel.

- **Agreeing on mission requirements:** A critical step when designing infrastructure is to determine and agree on the overall objectives, with an understanding that the design needs to be tailored to the specificities of an organization's mission. For example, some entities may need to preserve potential evidence to a specific evidentiary standard, while other entities may not. Similarly, some entities may have a broad mandate, while others may focus on more narrowly defined issues. Understanding these requirements determines the necessary infrastructure capabilities.

- **Safe and secure internet access for investigators**: Participants agreed that safe and secure access to the internet is critical for any open source investigation. This includes, but is not limited to, adhering to strict operational security protocols to protect both the investigator and the organization as a whole.

- **Mental health protections:** There was also consensus on the importance of protecting the mental health of open source investigators, who often encounter distressing material. Any infrastructure needs to include tools and facilitate processes and policies to mitigate mental health risks.

- **Chain of custody:** For entities that collect and preserve evidence for eventual use in a criminal investigation or at trial, maintaining a documented and unbroken chain of custody is key. Chain of custody refers to the detailed documentation of transferring, handling, and processing of information to preserve its integrity. Considering this, every open source item that could potentially become evidence should always be under strict control, with a transparent audit trail from the moment it was collected to the moment it is presented in court.

- **Confidentiality, integrity, and availability:** Security was another element highlighted in discussions. The confidentiality, integrity, and availability of all preserved information and evidence must be ensured. The infrastructure must also be secured against unauthorized access using physical and technical measures.

- **Scalability and flexibility:** Regardless of the mission scope, infrastructure must be scalable and flexible. Organizations that focus on narrowly defined issues need to carefully consider this as their mission requirements may change over time. Should the infrastructure not allow for any scaling of operations or not be easily adjustable, the organization may have to build a new infrastructure from scratch. Likewise, infrastructure that is overly broad may introduce unnecessary cost and risk.

Hardware and Software Considerations

Setting up a dedicated open source investigation capacity can be achieved with a small budget, but operational security should never be compromised. The following hardware and software components were discussed during the workshop.

Hardware

- **Dedicated open source investigation machines:** Participants agreed that open source investigation activity should be carried out on dedicated machines. This includes also the use of dedicated mobile devices as some social media is only accessible via a mobile app or a device associated to a phone number. There must also be a clear distinction between machines used for day-to-day operations and those used for open source investigations. More technically mature organizations may choose to explore enterprise solutions that provide a software solution (including virtual machines), which can be accessed from any machine, including those used for day-to-day operations.

- **Internet access:** As with machines and mobile devices, workshop participants recommended not using the same IP address for everyday activities (such as routine internet browsing or checking emails) and investigations (such as accessing sensitive or investigation-relevant online information).

- **SIM and eSIM:** SIM or eSIM cards are necessary for obtaining phone numbers to use during open source investigations. In some countries, SIM cards can be purchased without the need to present any proof of identity, while in others, proper identification is required. Participants discussed the necessity to adhere to local law.

Software

- **Virtual Private Network (VPN):** VPNs are a cost-effective solution for masking IP addresses and accessing websites restricted to certain physical locations, participants suggested. For example, if a website blocks visitor access from Germany, a VPN might be used as a workaround for accessing the same website from the United Kingdom.

- **Virtual machines:** Participants also discussed the use of freely and commercially available software to allow users to set up a virtual environment within their physical device, e.g., a desktop computer, such that if anything that happens within the virtual environment, the physical device will remain unaffected. In other words, if open source investigators infect their virtual machine with malware, the actual device will remain uncompromised. Investigators can quickly delete any infected virtual environment and set up a new one with just a few clicks. For larger organizations, enterprise solutions do exist.

- **Documentation software:** Participants also discussed the use of documentation software to automatically capture online investigative activities for the purpose of keeping an audit trail. Free software solutions also exist, and while some of these are not primarily designed to capture everything an investigator does online, they can still be used for notetaking. Larger organizations can seek out enterprise solutions within the e-discovery domain.

- **Tools:** Software can also include the use of free and paid tools, but participants agreed that open source investigations are not about having access to any tool, but the methodology. Similarly, the importance of keeping up with continued change in open source investigation was stressed. In that regard, it was recommended to keep abreast of any updates by engaging with colleagues and/or online communities.

A Case Study from the Internet Resources Unit at the IIIM

During the workshop, the IIIM presented on the Internet Resources Unit (IRU) and its approach to integrating complex data into its central repository. The IRU was established to address the lack of standards and tools for collecting and analyzing large, complex datasets, and has maintained a focus on skills, workflows, and infrastructure since its foundation.

Among other things, the presentation emphasized the importance of developing customized processes and tooling (i.e., scaffolding) to automate and normalize data structures. It also addressed common misconceptions about digital forensic standards, such as the gap between commercial promises and practical realities, and the lack of appropriate industry standards. There was also mention of the complexity of data analysis, the limitations of artificial intelligence (AI), the challenges of large-scale text searches, and the importance of cultivating an open culture for digital investigations within and amongst communities.

The presentation also laid out the IIIM's growing need to handle large amounts of multimedia and complex, unstructured data, and introduced participants to the in-house development of a media processing pipeline designed to meet this need. This pipeline includes modules for deduplication, content moderation, machine transcription and translation, semantic search, and reverse image search, along with a multimedia library for storing processed data. The pipeline uses machine learning and other advanced technologies to cluster, classify, identify, transcribe, translate, and index. In doing so, it enhances searchability and comprehension, and facilitates review and analysis. Limitations of the pipeline were also discussed.

PANEL 2: BUILDING AND MANAGING TEAMS TO SUPPORT AND CONDUCT OPEN SOURCE INVESTIGATIONS

The quality of open source investigation and analysis is only as good as the team behind it. Therefore, building and managing a team that is effective, diverse, and well-trained is essential, even if it is often overlooked in capacity-building. To that end, it is important for an organization to consider how it wants its teams to be structured and what skillsets are required of its investigators.

Key Skills

One important aspect of building an effective team lies in determining the skillsets an organization wants each of its team members to possess. The following considerations were discussed during the second panel and ensuing discussion:

- **Expertise:** What kind of expertise is necessary for the team? Does the organization need investigators skilled in locating individuals? What about geolocation specialists? Perhaps the subject of the investigation requires expertise in event-mapping or timeline-analysis.

- **Attention to detail:** How detail-oriented should each team member be in an ideal scenario? Is it important that team members thoroughly scrutinize text, audio recordings, videos, maps, and other visuals for irregularities? What about investigators who consistently cross-reference content with the metadata behind it?

- **Differing viewpoints:** Consider how to mitigate various biases and manage disagreements that may arise amongst team members. How important is cultural and contextual diversity to the team? Differences of opinion should not necessarily be seen as a negative as they can help advance the investigation. Consider, as well, having any analyses peer-reviewed to mitigate bias.

Design Elements

Once an organization has identified the kind of skills necessary to build a perfect team, it is important to consider structure. This should be done even before the recruitment process begins. To that end, workshop participants highlighted the following key points:

- **Organization and structure:** Determine whether the organization would like to hire a fully remote team, or whether it would prefer an in-person or hybrid setup. Consider whether the teams should be organized by geography, themes (e.g., human rights), specific conflicts or hostilities, or any combination of these or other factors.

- **Managerial positions:** What kind of supervisors should lead the team? Consider establishing positions for project directors, leads, and managers who can help ensure workload balance and staff well-being. Participants pointed out that the best open source investigators might not make the best project leaders, and the best project leaders may not make the best open source investigators, but it is important to have both on any given team to ensure balance.

- **Supporting roles:** Team investigations require more resources and nuance than investigators working alone. Think about taking a holistic approach to open source investigations. What kinds of roles would enhance the team dynamic? Consider including localized specialists, subject matter experts, data analysts and scientists, as well as other support staff.

- **Consultancies:** If an organization does not have the resources to hire the necessary experts, think about creating project-specific consultancies. External providers can help build an in-depth product where a team may lack expertise.

- **Training and networking:** When designing a team, think about approaches to knowledge-sharing within and across the organization. This might include developing platforms for communication, building out and expanding digital libraries and datasets, documenting policies and processes, and fostering a culture of change management. Likewise, learn to leverage external partnerships. Outside collaboration might come through participating in trainings, such as hackathons and workshops, and seeking out ways to expand networks.

Recruitment

Participants explored the recruitment process for open source analyst positions, discussing what organizations look for when hiring for these positions and what candidates can expect during the interview phase. Below are some considerations raised by participants.

- **Transparency:** First and foremost, participants emphasized the need for transparent, open, and collaborative recruitment processes. This includes everything from posting jobs on public platforms such as Reddit, to making sure that potential candidates are kept informed every step of the way.

- **Curiosity:** Organizations often seek out open source investigators who are curious, love solving complex puzzles, trust their instincts, and exhibit persistence—those who do not shy away from a good challenge. Why? Because open source analysis is often one big puzzle, with each investigator contributing a small part towards the collective goal of solving that puzzle. To this end, even while open source intelligence is gaining popularity as a field of study, the best investigators will not necessarily acquire their curiosity and desire to be challenged from a professional, formal degree.

- **Knowledge and skills:** Recruiters look for candidates who understand open source mechanics and can effectively use tools to analyze information. To assess this, interviews for open source positions will often include a live skills test. This allows the recruiters to observe the candidate at work, understand their thought process, and gauge their level of open source proficiency.

- **Focus on diversity:** Increasing diversity and parity within teams has become a priority for recruiters. To that end, participants noted the importance of addressing disparities in gender and geographical representation. To help remedy these gaps, recruiters should focus on hiring staff from various backgrounds and nationalities. With diverse perspectives represented amongst its staff, an open source team can build a strong and lasting foundation. Participants also discussed the need to remove structural impediments in recruitment processes, such as the requirement for a candidate to have a specific degree or background (e.g., a master's degree or experience in digital forensics), and to adapt job descriptions to prevent unfair disqualification of candidates at the initial stages of recruitment, especially when AI is involved in screening applications.

Lessons Learned

Participants discussed lessons learned in building open source teams from scratch. Many of these lessons are reflected in the commentary raised earlier in this report, including the importance of developing a diverse, well-trained team. Additional key lessons are outlined below.

- **Security considerations:** Open source teams must also consider concerns related to operational security. How can organizations protect the identity of their investigators? If, for example, a team is investigating war crimes in a particular country, the organization should be fully aware of its threat model. Only then can it implement strategies to safeguard both itself and its investigators from potential retaliation or attacks by malicious actors.

- **Preventing and managing burnout and fatigue:** As outlined above, open source teams need effective managers and project leads who can build trust with their staff and who recognize early signs of burnout and fatigue. Managers should endeavor to be as honest as possible with their teams and to openly seek support when necessary. Resources such as hotlines and peer-to-peer support groups can be helpful in prioritizing staff wellbeing.

- **Secondary trauma:** Due to the nature of open source investigation, trauma can be challenging to prevent and manage. Nonetheless, there are a number of mitigation strategies that can help ensure investigators are appropriately supported day-to-day. As with preventing burnout and fatigue, establishing 24/7 support hotlines and providing access to mental health services such as counselling sessions can go a long way in making sure staff stay resilient and healthy. Managers again need to foster an environment where staff feel comfortable reporting trauma, seeking help, and stepping back when needed. Additional attention should also be paid to cultural and individual sensitivities here. Free resources are available to help navigate these issues.

PANEL 3: EVIDENCE AND INFORMATION MANAGEMENT - FROM THEORY TO COURT

One of the biggest challenges with open source investigations and the collection of digital information from the web is how to preserve and store it; how to make it retrievable, analyzable, and sharable with third parties; and eventually, how to make it usable in court. The following topics were mentioned and discussed among workshop participants.

Despite attempts to regulate the management of information and evidence, a unified international criminal law standard has yet to emerge. Nonetheless, the Electronic Discovery Reference Model (EDRM) has proven to be a valuable starting point for addressing this issue.

The Electronic Discovery Reference Model (EDRM) versus The EDRM 2.0

The EDRM provides an adaptable, legally compliant framework for standardized workflows and cross-functional collaboration. It allows teams to work together in a project-based manner, with, for example, the investigative team identifying information and evidence for preservation and collection, the e-discovery team overseeing processing, review and analysis, and the legal team producing the work product. Its relevance cuts across many different sectors, including legal, business, information technology, and can be adapted to the user's interface and infrastructure.

Panelists gave participants a preview of the upcoming EDRM 2.0, the next iteration of the model. The latest version takes a fresh, bottom-up approach to e-discovery. It is being developed through collaboration with stakeholders from around the world in different fields. It hopes to integrate AI and open source investigation and analysis in new and innovative ways.

Admissibility of Audiovisual Content

Another aspect that was discussed during the panel was audio-visual evidence. Like any other type of evidence, it must be relevant and reliable before being admitted into a court of law.

To start, the proffered evidence must be relevant. It must make a fact in the case more or less probable than it would be without the evidence. Second, it must be reliable, considering authenticity, the characteristics of the evidence, such as chain of custody, and the balance between the probative value versus the prejudicial effect. Once these two criteria are established, the court can then determine how much weight to give the evidence.

The discussion here centered around two cases of international law involving audio-visual evidence. In one, issues with chain of custody, methodology, and metadata extraction were eventually overcome using online tools. In the other, targeted satellite imagery was used to circumvent crime scene access issues. In both instances, convictions were secured and upheld.

The key lesson from these scenarios is the importance of using audio-visual evidence to build strong, winning cases. Adaptability, working with multilingual teams, getting help from experts, and establishing partnerships with local organizations are all necessary to make sure that the criteria of relevance and reliability are met, and that the evidence is weighed carefully once made part of the record.

Applying the EDRM – Lessons Learned

The EDRM is a pioneering approach to managing information and evidence. Nonetheless, working with digital evidence, in particular from open sources, presents unique challenges. Workshop participants identified several lessons that can carry us forward:

- **Standards:** Not having clearly defined standards can be problematic. To overcome this, organizations need to prioritize documentation and transparency, using international standards (e.g., ISOs) as a starting point. The EDRM is useful in that it can help scale, plan, and design investigations.

- **People power:** The rule of four is helpful: a lawyer, investigator, analyst, and legal technologist all have roles to play in building a strong, multi-talented team. Organizations need to make sure this team is equipped to handle data wrangling, information retrieval, contextual knowledge, and technology.

- **Data types:** Unstructured data and different data types present significant challenges in e-discovery under international criminal law. Overcoming these challenges requires organizations to invest in people with unique skillsets and develop robust processes for analyzing and organizing data.

- **Technology strategy:** The complexity and volume of data vary with any given collection type. Narrowing data collections to specific types is easier than handling broad collections across multiple data types, which can be extremely challenging. To resolve this issue, organizations must develop the right processes, tools, and infrastructure to effectively manage and handle their data.

CONCLUDING THOUGHTS

Open source investigations have recently gained popularity among investigative and accountability-focused organizations. Numerous well-documented cases demonstrate their viability and utility while detailing how others can replicate past and current open source investigations.

Up until today, most of the discourse within the wider open source investigations community has focused on how to use open source investigations for particular purposes. Discussions that dominate the public discourse often center around new tools and technology, such as generative AI. This emphasis has led to a flawed understanding of what is necessary to conduct successful open source investigations, and most importantly, what tools cannot do.

As demonstrated by the panel discussions, organizations aiming to develop an in-house open source investigation capacity must understand that there is no single off-the-shelf solution. In fact, the absence of such a capacity is often seen as a "technology gap," where procuring new technology is perceived as filling this gap. However, technology is only one of three major components required for a successful open source investigation capacity. Because of this, betting only on technology will inevitably lead to failure. Instead, any capable open source investigation capacity must consider the complex interplay between three key components: **infrastructure**, **people**, and **processes**, which in turn are embedded within an open **culture** and a surrounding **community**.

Infrastructure

Infrastructure, which serves multiple functions, is the backbone of any open source investigation capacity. At its most basic level, it provides safe and secure access to the world wide web. As the number of staff grows, coordinating this function becomes more important and more challenging. Other core functions include managing information and evidence in accordance with relevant policies. This also becomes increasingly complex as additional data needs to be collected, processed, and enriched before ultimately being made available to teams of analysts and investigators.

People

The success of any organization depends on the diverse skill sets and expertise of its staff, tailored to its specific mission. Although open source investigation specialists are invaluable in specific situations, their expertise is not sufficient for certain critical technical functions, such as the information and evidence management of large volumes of different data types. Where those functions are prioritized, the contribution of evidence officers, data scientists, and data analysts is crucial. Each specialist brings key skills that, in combination, create an indispensable team on which any organization can rely to fulfill its mission.

Processes

The importance of well-defined processes and standards cannot be overstated, as they ensure consistency, reliability, and legal compliance, especially for entities that manage large amounts of information and evidence. Absent established processes, staff may approach problems without any consistency, only to create incongruent outcomes or potentially jeopardize the organization, contrary to the goals of open source investigations, which demand the highest level of operational security. Following a structured approach is also essential for maintaining the integrity and credibility of the organization.

Culture

Infrastructure, people, and processes are essential to building effective investigative capacities, but to truly maximize open source potential, it is important to consider the culture within an organization and its integration into the community at large. By nature, open source investigations rely on publicly available data and information, accessible to anyone, from anywhere, and at any time. It is this open community that makes the resultant investigations so powerful. Investigative outlets pioneering this new approach seek to promote a culture of transparency where everything, including methods, techniques, leads, and outcomes, is broadly shared. While it is true that some organizations cannot and must not share sensitive information, the fact remains that anyone can learn the tradecraft and take part in active online investigations. This openness and transparency must be promoted within an organization to overcome information silos and maximize the exploitation of public sources in support of a particular mission.

Community

Community refers to groups of people within and outside an organization. The goal of forming such communities is to encourage support and collaboration. Sharing tradecraft tips, methodologies, leads, and other useful information can be immensely powerful in that regard, and promoting such a practice within an organization undoubtedly leads to success, both internally and externally. While the mission and vision of each entity may differ, the underlying principle remains the same: forming communities is necessary to achieve ultimate success. That is, working together can drive better outcomes than working in isolation, especially when multiple entities are tasked with investigating the same atrocities.

Our workshop marked the first of its kind, bringing together leading organizations to share experiences and discuss best practices in building open source investigation operational capacities from scratch. What was discussed, and the conclusions that emerged, are only the beginning. We sincerely hope to continue the conversation, and begin new ones, with organizations involved in open source investigations in the future.

The IIIM extends its heartfelt thanks to every presenter and participant. A special thanks to ISMS Section Chief Keith Hiatt for his leadership, for pioneering the development of open source capacity at the IIIM, and for his invaluable contributions to the workshop, to Rayyan Ghuma for her insights and expertise, and to Wael Hattar for masterfully designing this report. Lastly, a huge thank you to all IIIM colleagues involved in the preparation and execution of the workshop. We could not have done it without your support.

Lorand Bodo
Internet Resources Analyst
ISMS