THE RESPONSIBLE OPEN SOURCE INVESTIGATIONS WORKBOOK

A guide for open source investigators

# 

# CONTENTS

*WELCOME*

*GETTING SET UP*

[WHY ARE YOU DOING THIS?](#j899cjz78rs2)

[WHAT IS YOUR GOAL?](#uz6wyeusyodd)

[WHO ARE YOU WORKING WITH?](#dywo2sjhc9x)

[HOW WILL YOU WORK?](#ellc0y8x1bq9)

*THE INVESTIGATION*

[DISCOVERY](#v3fd53nc4kfp)

[PRESERVATION AND STORAGE](#vhica7g6m7u7)

[ANALYSIS AND VERIFICATION](#ojn1sxs9szcu)

[PUBLICATION](#mj7ua9ic1ak)

[AFTER THE DUST SETTLES](#lcgam5aq69z4)

*INDEX AND RESOURCES*

# WELCOME.

The Responsible Open Source Investigations Workbook is designed to support you – a human rights researcher using open source information – to make the best possible judgements in the particular context you’re working in.

Open source information has always been a part of the human rights researcher’s toolbox. In recent years, however, both the amount of information available and the number of people working with it have increased.

These developments bring with them a lot of opportunities. They also, however, introduce a lot of challenges, including the risk of negatively impacting the rights of people you are, through your investigation, seeking to protect.

Taking a human rights based approach, this workbook was designed to help guide you through difficult decisions so that such negative impacts can, as far as possible, be avoided.

This approach focuses on those who are most marginalised, excluded or discriminated against, and works to address power imbalances. It also encourages us to not just focus on the outcomes, but also on *how* these outcomes are achieved. (More on these principles and the human rights based approach to digital open source investigations can be found in the report that accompanies this workbook.)

Underlying this workbook are two principles:

* Just because you can, doesn't mean you should
* The ends do not necessarily justify the means.

The workbook is designed to help you to add intentionality to every step of your investigation.

|  |
| --- |
| *How to use the Responsible Open Source Investigations Workbook* |
| This workbook is available as a Word doc, Open Office doc, and as a PDF, and it includes spaces for you to fill in your own information.  Take this document and make it yours. Save it, edit it, remove the parts that aren’t relevant to your context. Translate it. Print it, draw on it, stick it to the wall. Work through it as a team or as an individual.  Ideally you would work through the workbook at the start of your investigation, but it’s designed to be useful at any stage, even if you’re already finished (in this case, use it to evaluate your current processes and ways of working).  At the end you will find an index and a list of supplementary resources, which include a report that provides more information on the human rights based approach to open source investigations and case studies that relate to each section of this workbook. If you are looking for more information and context, the report is a good place to start.  *Note: If you are using this workbook in Google Docs / Google Drive, or if you are sending it to collaborators via unencrypted email, be careful not to enter information that could put people at risk. Also make sure that any physical or digital copies are stored and shared securely.* |

*LET’S GET GOING.*

Not too fast.

Speed is often prioritised during an open source investigation, but here we encourage you to slow down. Stretch your body, take a breath, and grab a glass of water.

It’s important to stay hydrated.

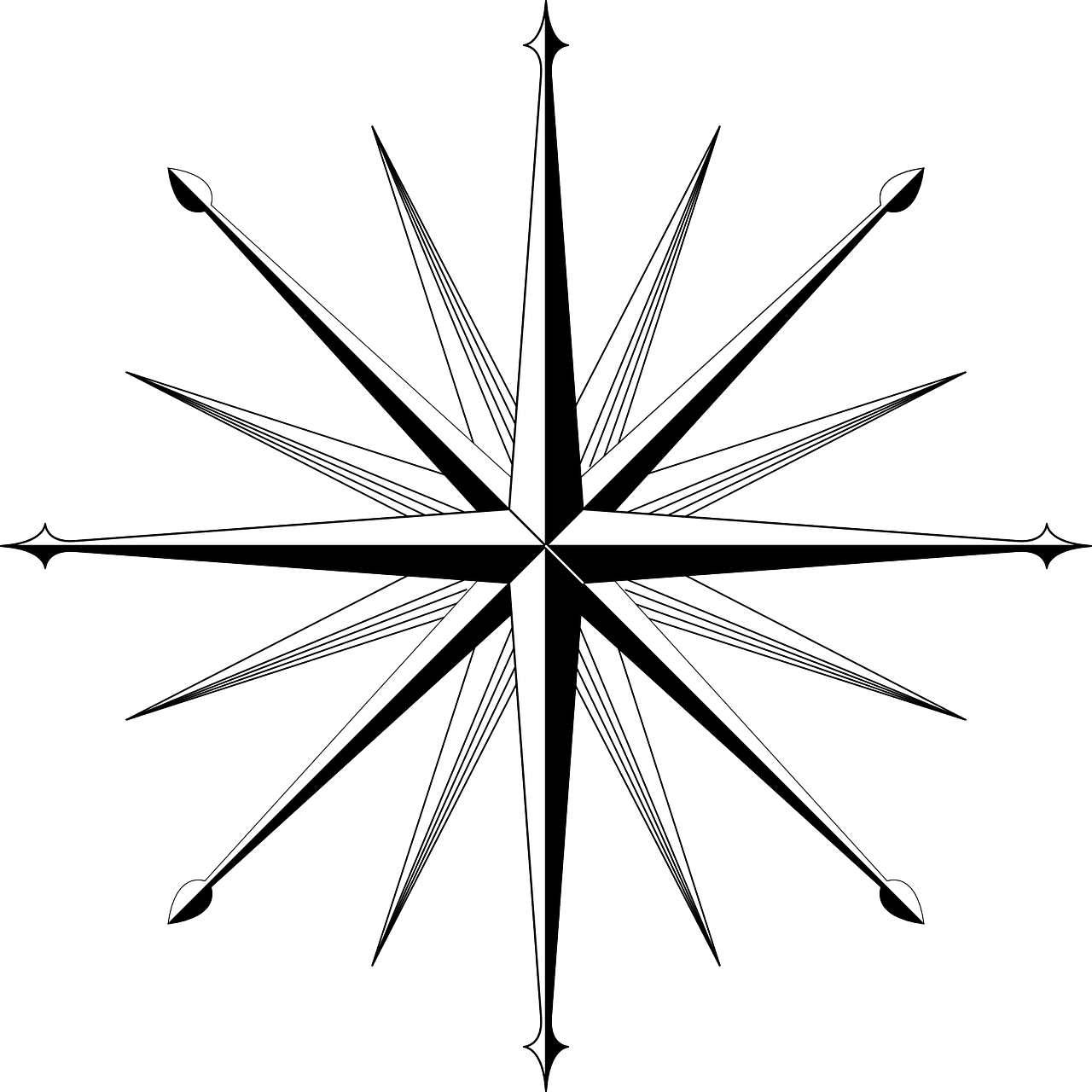
GETTING SET UP  
WHY ARE YOU DOING THIS?

Understand what motivates you and those you are working with.

Your investigation will be stronger if you answer two key questions upfront:

* What matters most to me?
* What matters most to those I am working with?

Conducting an investigation responsibly can mean different things to different people, depending on the beliefs, experiences, values, and motivations of everyone involved.

When you need to make a tough decision in the course of your investigation, it can help to be consciously aware of the values that guide you and those you’re working with – you can use them as your North Star, pointing you in the right direction. 

The exercise that follows is designed to help you get a clearer idea of what your values actually are.[[1]](#footnote-1)

*STEP 1: Pick your top six values**If doing this exercise as a team, each person should first complete this step individually – you will compare answers later on.*

* From the list of values below, circle, highlight or write down the six values that are most important to you.

|  |  |  |
| --- | --- | --- |
| Accountability | Diligence | Joy |
| Accuracy | Discipline | Justice |
| Achievement | Diversity | Leadership |
| Adventurousness | Efficiency | Legacy |
| Altruism | Empathy | Making a difference |
| Ambition | Enthusiasm | Obedience |
| Assertiveness | Excellence | Openness |
| Being the best | Excitement | Perfection |
| Challenge | Fairness | Positivity |
| Cheerfulness | Freedom | Professionalism |
| Commitment | Fun | Reliability |
| Community | Generosity | Rigour |
| Compassion | Growth | Sensitivity |
| Competitiveness | Hard Work | Speed |
| Consistency | Honesty | Structure |
| Control | Honour | Success |
| Creativity | Humility | Teamwork |
| Curiosity | Ingenuity | Trustworthiness |
| Decisiveness | Insightfulness | Truth-seeking |
| Determination | Intelligence |  |
|  |  |  |

*STEP 2: Put your top six values in order of importance*

* Rank your top six values in order of importance. *For tips on how to rank your values, see the box below.*

*1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 3. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*4. \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 5. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 6. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

|  |
| --- |
| ***Tip:*** It can help to consider values in pairs. Start by choosing any two values in your top six list and ask yourself, "*If I had to act according to only one of these values, which would I choose?*"  Try and visualise a concrete situation in which these two values might come into conflict. For example, for *speed* vs *truth seeking,* maybe you have obtained information about an event that has just occurred and must decide what to do with it. Do you report it quickly (*speed*)? Or do you delay reporting in order to verify the content and properly understand the risks involved in publishing (*truth-seeking*)?  If you report quickly, you risk publishing unverified or potentially harmful content. If you delay, you risk the report not being picked up by news outlets. Which of the two values would guide you in this situation?  Try and work through your list by comparing each value with each other value. |

*STEP 3: Share and discuss*

* If you are working with a group, share your lists with each other. Discuss why each value was chosen. *This will help each of you understand what is important to the people you are working with as you carry out your investigation together.*

*STEP 4: Repeat this exercise with potential partners or collaborators*

* Going forward, before entering into partnership with new collaborators, ask them to go through the same exercise. Compare their top values with yours, discussing your choices together. (More questions to ask potential partners will be covered later in this workbook).

|  |
| --- |
| ***What happens if our values vary greatly?***  Isn’t it great that you know this now rather than half way through the investigation? Understanding what values are important to your collaborators or partners, and gaining insight into *why* they are doing this work, will help you to better understand their approach as well as help them to better understand yours.  If there is an extreme values-mismatch between your team and others you’re planning to work with, and where this could negatively impact the investigation, then map out other potential allies, partners or collaborators that you could work with. |

# 

# WHAT IS YOUR GOAL?

*Be clear on what you are investigating, what impact you hope to have, and what unintended consequences your work could potentially have*

Being intentional about your goals will help your entire investigation. Not only will clear goals help you to establish the most appropriate methods to achieve them goals; they will also help you to identify potential risks.

Investigations focused on legal accountability, for example, will have different discovery, verification and publication processes and standards compared with investigations aimed at creating a big media splash.

*Try and answer the questions below as clearly and concisely as possible. You’ll come back to your answers again while working through this workbook.*

**What is the goal of your investigation?** *Describe your goals and your target audience.*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**How will you know if you have reached this goal?**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Why are you the right person or group of people to do this work?** *Think about, for example, whether you have the right existing knowledge, team and infrastructure in place.*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Having identified your values and goals, this workbook will now help you gain a deeper understanding of who you’re working with on your investigation, and who makes your work possible.  
WHO ARE YOU WORKING WITH?

Gain a deeper understanding of your team, your partners, and the individuals or groups who make your work possible

In a responsible open source investigation, it’s essential to have a clear understanding of who you’re working with, what skills or capacities everyone has, and whose work makes your work possible.

For teams, it’s also important to recognise any differentials in power, perks or privileges within the team. Not only is this key to building a sustainable and equitable team and, more broadly, a more sustainable and equitable field, it also lays essential groundwork for other aspects of responsible open source investigations, such as trauma mitigation plans and appropriately crediting all those involved (this workbook will deal with both these things later on).

|  |  |
| --- | --- |
| ***People involved in the investigation*** *List all the individuals involved in the investigation (anonymise names where listing them might put people at risk).* | |
| Your team |  |
| Partners |  |
| External organisations |  |
| Data creators |  |
| Other |  |
| *Skill mapping*  *Map out the skills that your team has, and any skills that might be missing. For example: contextual knowledge, archival knowledge, skills around handling data (storage, deletion, providing access, security), relevant language skills, expertise in secure communication, verification, analysis, etc.* | |
| What skills do the people in your team have, relevant to this investigation? |  |
| What skills is the investigation missing?   For each skill, consider:  > Can this be developed within the team? How? How long will it take?  > Are there partners or collaborators you need to bring in? |  |
| *Power, positionality and privilege* | |
| Does everyone involved in the investigation know what each other’s values are? Are these values complementary? |  |
| Who is working remotely? |  |
| Who has a personal connection to the issue? |  |
| In this work, what factors can create differences in people's structural power? (For example, gender, ethnicity, race, geographic location, age, affiliations). Think about your team in relation to these factors. |  |
| Who is being paid for their work on this investigation? Is anyone volunteering? |  |
| Who knows the context best? |  |
| How will you credit the individuals or groups you are working with? |  |
| What are the risks and/or opportunities that come with being credited? |  |
| *Whose shoulders are you standing on?* | |
| Who has made it possible for you to have access to the data you are using for the investigation? |  |
| Whose work has enabled you to get to this point? |  |
| How will you credit those who have made your investigation possible? |  |

The table below is designed to help you map out your investigation’s ecosystem of people.

## ASSESSING PARTNERSHIPS

Before collaborating on an investigation with another group or individual, it’s important to understand how your potential partners approach areas like security, verification, data sharing, bias and resiliency.

As mentioned earlier in the workbook, it’s also key to know which values are important to them.

|  |  |
| --- | --- |
| ***Values*** | |
| What values are most important to them?  > Do their values align with yours? |  |
| Who funds them?  > Do the values of their funders align with your values? |  |
| *Relationships* | |
| Who are their partners and/or collaborators?  > Do you share any partners/ collaborators? |  |
| Have you worked with them before? Was it a good experience?  > If you haven’t worked with them before, is there a small project you can work on together first, to establish trust? |  |
| ***Ways of working*** |  |
| Do you share the same verification standards? |  |
| How do they treat, store and process sensitive data? |  |
| Who do they typically share data with? |  |
| Do you agree on how to credit those who have worked on the investigation? |  |
| Are you both likely to stick to the timelines and deadlines set? |  |
| Do you share the same standards when it comes to dealing with the psychosocial health of team members working with distressing materials? |  |
| What tools are they using?  > Do these tools align with your security standards and risk assessment? |  |
| How will your work together be licensed? |  |

The following questions can help you assess partnerships you might already have, as well as partners you’re considering working with.

## MAKING IT OFFICIAL

Once you have considered these questions and want to go ahead with a partnership, use your answers to write a Memorandum of Understanding (MOU), Service Level Agreement (SLA) or Terms of Reference (TOR) document.

This document can be referred back to if the partnership is not developing as expected. Along with details on how you will work together (informed by the exercise above), also include details on the following:

* The background of the investigation
* What each partner’s role is
* What each partner will be responsible for
* How you will keep in touch
* Any important milestones or deadlines
* Data sharing
  + Who has access to what, why and for how long?
  + How will each partner be allowed to use the data collected as part of the investigation?
  + How will the data be shared? *This could include file format, method of delivery, and how often the data will be sent between partners.*
  + How will the data be treated? *This could include security measures, how often data should be deleted, whether data will be shared with third partners, and if so, how.*
  + Who should have access to what data at what point of the investigation?

# HOW WILL YOU WORK?

Think about the ways in which your investigation could possibly cause harm, and develop strategies to avoid this

Conducting a responsible investigation means actively seeking to understand the risks involved: risks to yourself, to those you are working with and to those you are working on behalf of.

This section looks specifically at *how* you are planning to conduct, or already conducting, your investigation. What harms could potentially be caused by your activities? What could be done to avoid causing these harms?

**Use the table below to map out risks and mitigation strategies.** Some examples have been included to help get you started.

|  |
| --- |
| ***A note on security*** When going through the table, think about how to set up your workstation to ensure it is as secure as possible and does not reveal personal information.  Measures might include setting up a separate browser profile, creating separate social media accounts for monitoring online activity, using a VPN and activating two factor authentication (2FA). These should apply to all team members and partners. |

|  |  |  |  |
| --- | --- | --- | --- |
| **What are you doing?** | **What are the risks involved, to yourself and to others?** | **What is the risk of this happening?** | **What steps could you take to stop this happening?  > What costs will this incur?** |
| Collecting data | Data could be lost or stolen (for example, through being hacked) | High: We are collecting sensitive and potentially damaging data about a well-resourced government. | > Back up the data regularly  > Store the data in encrypted hard drives |
| Viewing graphic and distressing videos and images | A team member could be traumatised |  |  |
| Sharing data with a partner | Our partner could publish unverified data |  |  |
| Publishing an investigation | We could get it wrong |  |  |
| Hosting data | We might not have enough funds to host it after the project ends |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Once you have filled in the table:

* Which of these risks are most likely to occur? Mark these with a star.
* From the starred risks: Which of these would be the most devastating if they happened? Circle these.

**Create Action Plans**

|  |  |  |
| --- | --- | --- |
| **Scenario:** | | |
| **Next steps** | | **Who will take action?** |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |
| 4 |  |  |
| 5 |  |  |
| 6. |  |  |

Starting with the risks you have circled, create an action plan for each worst-case scenario, using the table below as a guide.

**Create an Emergency Shutdown/ Project Termination plan**

|  |  |  |
| --- | --- | --- |
| **Emergency shutdown / project termination Action Plan** | | |
| **Next steps** | | **Who will take action?** |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |

* Make sure that you have an emergency plan that lays out steps for immediate shutdown or project termination.

**Assess your capacity**

* **Does everyone involved know what to do, and what others should do?**
* **Do you have the resources needed to manage the situation?** Are there any critical gaps? Do you need additional resources?
* Given your answers to all the questions above, assess: **Can you deal appropriately with the risks your project opens up?** If not, are there additional resources you should seek out first or, do you need to reconsider the project in its entirety?

## DECIDING WHICH TOOLS AND TECHNOLOGIES TO USE

When it comes to working on data that is very sensitive, it’s important to consider the tools you and your partners are using very carefully.

When evaluating tools, consider:

* **Costs:** Can you and your partners afford to use it?
* **Usability:** Will the tool work on your teams’ devices and with everyone’s internet connectivity? Is the tool within everyone’s skill sets, or too complex for some?
* **Online vs local:** Can you use the tool locally on your computer, to ensure that third parties don’t have access to the data you’re working with?
* **Data management:** How does the tool treat your data? Consider this question in terms of storage, third-party access, and portability.
* **Code:** Is the tool open source or proprietary? Do you know who made the tool, and who maintains it?
* **Ownership and trust:** Who built the tool, who funds it and who is the tool’s target audience? Are your peers using it?

|  |  |  |  |
| --- | --- | --- | --- |
| **Tool** | ***Benefits*** | **Limitations** | **Situation** *How will you use this tool?* |
| Online metadata viewer | >Easy to use >Free >Works in the browser | >Image is uploaded to an unknown server and results are viewed online | Only when the data we are analysing is not sensitive |
| Locally hosted metadata viewer | >Free  >Works on a computer, so no one else has access to it  >Code is open source | >It is not so easy to install, or to view the results | We will use this tool when the data we are analysing is sensitive |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Where possible, get in touch with and talk to the designers of the technology yourself. If helpful, use the table below to summarise your evaluations for the tools you are considering.

## MITIGATING THE RISK OF TRAUMA

Conducting digital open source investigations in a human rights context can be very traumatic. In doing this work you can be exposed – sometimes in a sustained way – to violent, graphic and distressing digital content. This can heavily impact your mental wellbeing, and frequent and repetitive exposure to this type of material can lead to vicarious trauma and even Post-Traumatic Stress Disorder (PTSD).

There are steps that you can take to mitigate the possibility that you and your team will experience trauma through your work. The questions below are designed to support you in creating a resiliency plan for your investigation; make sure there is an opportunity for all team members to give input.

### Creating a resiliency plan

Different content requires different approaches – there is no one-size fits all approach to creating a resiliency plan.

**Remind yourself of the goal of the investigation**. Does everyone on the team know what this goal is and what you are trying to achieve?

*Having a goal and connecting with your reasons for conducting this investigation can help psychologically – in particular with the feelings of helplessness that may arise.*

**What type of material will people on your team be seeing or hearing?**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Who on your team has a personal association to the material?**

*It can be more difficult for those who are reminded of a personal situation or who have a personal connection with the material. It is important to take this into consideration and to take extra care with this team member.*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**How will you or your team be receiving material?**

*For instance, via WhatsApp, through emails or through social media platforms. It is important to know what channels you or others in your team will be receiving material through. Surprise can make looking at distressing material a lot worse.*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**If members of your team are likely to encounter distressing material without warning, what steps can you take to reduce the shock or surprise?**

*Warning others in the team, adding descriptions and tagging content can all help.*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**How can you streamline your collection, discovery and verification process so that individuals don’t have to view the same material repeatedly?**

*Repeat exposure is damaging. Work on reducing this where possible. Avoiding needless repeat exposure could be done through measures such as analysing material only when necessary, writing robust notes so that you don’t have to revisit the material, not sending the material to more people than necessary, and so on.*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**How else can you create and maintain a healthy working environment?**

*Some strategies that can help include adjusting the viewing environment, turning off the sound, taking frequent breaks and encouraging others in the team to do the same, taking a walk, and drawing clear boundaries around when you are online and when you are off-duty.*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Encourage each member of the team to have a self-care plan. Where or what is your happy place?**

*Research shows that highly resilient individuals are more likely to exercise regularly, maintain outside interests and enthusiasms, and invest time in their social connections when challenged by trauma-related stress.*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**How can you make it easier for team members to talk with each other about stress and trauma?**

*It can be helpful to set up peer support networks within organisations or teams to talk about distressing material and stress. Create and support an organisational culture that normalises and makes space for conversations around self-care and trauma reduction.*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**What resilience and trauma reduction policies have been set up? What policies could be set up for your next investigation?**

*If you are leading an investigation or managing the process, identify what support you can put in place and include allowances for therapy or other self-care approaches in your budget. Don’t forget to also look after yourself. Consider a rotation system for those looking at distressing, violent or graphic content so that they can rotate out and work on less distressing material. Consider limiting exposure to graphic content for more junior team members, and make sure that when they are exposed to this content, they have the guidance of more senior members.*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

THE INVESTIGATION

# DISCOVERY

At this point, you should be set up with a solid foundation: you know what you’re doing and why, you have a team in place as well as some policies, and you have considered, and created mitigation plans for, some of the risks and challenges that might arise.

Now it’s time to start looking more deeply at the investigation itself.

The first stage of any investigation involves gathering information. This section is designed to help you to think through your methodologies and ethical lines related to collecting and processing data.

It will also guide you through thinking about situations that could have adverse human rights impacts, and what approaches or measures you can take to avoid or mitigate these negative impacts.

Before getting started it’s also important to go back to the principles outlined at the beginning of this workbook. Throughout each stage of your investigation, ask: “Just because we *can,* does it mean we *should*?”

## SOURCES OF DATA

To start working through the ethical decisions you might need to make during the collection and preservation phases of your open source investigation, it can help to first get a clear idea on where you’re actually planning to gather information from.

In this workbook we use the definition that open source information concerns ‘publicly available information that anyone can lawfully obtain by request, purchase, or observation.’[[2]](#footnote-2)

**From the list below, select all the sources that apply to your investigation:**

* Social media platforms
  + YouTube
  + Facebook
  + Twitter
  + LinkedIn
  + Other \_\_\_\_\_\_\_\_\_
* Search engine results
* Online databases
* Government-published data
* Satellite imagery platforms
* Webcams
* Freedom of Information (FOI) requests
* Other \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Now select the types of information that you’re planning on collecting:**

* Visual documentation, such as videos and images
* Text data, such as documents
* Numerical data
* Audio recordings
* Geospatial imagery
* Coordinates
* Other \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## WHAT ARE YOUR ETHICAL LINES?

When it comes to using publicly available data, it can be tricky to know what is ‘okay’ to use, and what not to use. Even if a piece of information is publicly available, it does not necessarily mean that the person who uploaded the data or the people who might appear in it would consent to its use in your context. They might not even know that this data exists

The following exercise will take you through a number of common scenarios that come up in this work, and encourage you to think through how you would approach each scenario.

Before you start, revisit your core values and use them to guide you through the questions that follow.

|  |
| --- |
| Would you use data from a leak, hack or breach in your investigation? |
| *NEVER*- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*YES* |

**Look at the question below. Where on the line do you stand?** *For this exercise, each individual will need to answer the question for themselves first, before discussing as a group.*

***Example answers:***

* **Never:** This data was not meant to be publicly available in the first place, raising questions around the privacy, safety, and consent of individuals whose information is contained in the dataset.
* **In the middle somewhere**: This data was not meant to be public. However, if it’s useful for the discovery stage of the investigation and if we don’t use it in the publication phase, I feel ok using it.
* **Yes:** This data is useful and could aid in the investigation. However, I would make sure to verify it before publishing it or using it, and redact any personally identifiable or sensitive data. I might also put extra effort into explaining where the data came from for viewers of the data, ensuring that they understand the limitations and provenance of the data.

**Why have you chosen this position?** *What could go wrong if you don’t use these data sources? What could go wrong if you do?*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |
| --- |
| Would you use a fake name or account on a social media platform to obtain information? |
| *NEVER- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -YES* |

**Discuss your answers as a team. Do you all agree? What could go wrong?**

***Example answers:***

* **Never:** I would not do this as those I am investigating would not be properly informed.
* **Never**: I would not do this as I would risk the legal case I am preparing: if this information were to be used later in my legal claim, the chain of custody would have to be proven in a court of law and this could put the investigation and claim at risk.
* **Yes**:I would use a fake name in order to protect my privacy/identity but I am aware of the trade-off that those I am investigating are not giving their consent.
* **Yes:** I am violating the terms and services of the social media platform, but this is a justified trade-off if it means gaining access to a potentially vital piece of information.

**Why have you chosen this position?** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |
| --- |
| Would you create a Facebook profile under a pseudonym to gain access to a closed Facebook group? |
| *NEVER- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -YES* |

**Discuss your answers as a team. Do you all agree? What could go wrong?**

***Example answers:***

* **Never:** I would not do this as I am preparing to go to court – I know all the associated information I have found and used in the discovery phase will have to be released.
* **In the middle somewhere:** I would do this, but not if a victim or potential victim was involved – then I would never digitally trespass.
* **Yes:** Not using a pseudonym could alert a suspected perpetrator that I am investigating them and they could delete important information.

**Why have you chosen this position?** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |
| --- |
| Would you ask for more information from an online source? |
| *NEVER- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -YES* |

**Discuss your answers as a team. Do you all agree? What could go wrong?**

***Example answers:***

* **Never:**  I would be contacting them on an insecure platform, and if they were being monitored and surveilled then this could bring them into harm's way.
* **Never:** This is moving into the realm of closed source investigative techniques – I would not do this as part of this investigation.
* **In the middle somewhere:** This is valuable information: those who are at the scene know the context and geographic region the best. I have developed a process for how I will represent myself online, and I will try to move the communication to a more secure channel as soon as possible; for example, if I reach out to a source via direct message on Twitter, then I will try to move the conversation to WhatsApp or Signal as soon as possible, let them know how I will process the information they are providing, and make sure I know what level of anonymity they want.

**Why have you chosen this position?**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |
| --- |
| Would you track, monitor, or gather information from the friends and family of someone you are investigating? |
| *NEVER- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -YES* |

**Discuss your answers as a team. Do you all agree?** **What could go wrong?**

***Example answers:***

* **In the middle somewhere:** I would do this, but I would not monitor social media accounts of those under the age of 16 as minors should be treated differently to adults.
* **In the middle somewhere:** I would do this, but I would not publish any information about these people.

**Why have you chosen this position?**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Discuss your answers as a team. Do you all agree? What could go wrong?**

As you continue with your investigation, keep in mind that drawing ethical lines will be an iterative process. Be prepared to revisit this section, explore additional questions, and adjust your red lines as new challenges emerge.

## CROWDSOLVING

*Crowdsolving* campaigns often target a large, undefined group of people, tasking them with assignments ranging from identifying satellite imagery to categorising leaked documents.

Crowdsolving is a powerful method of collaboration – one that touches on the heart of the democratising potential of open source investigations. In practice, however, many things can go wrong, and have harmful consequences.

**If you are asking a group of strangers to collaborate on an investigation, there are a number of questions to consider.**

* Are the crowdsolvers tasked with identifying people? If so, what happens if they identify the wrong people? What happens if the investigation interferes with other active investigations or court cases?
* What standards must the crowdsolvers maintain? Who will be responsible for moderating and upholding these standards?
* Are you using gamification techniques as a way to attract, motivate and engage people to join your crowdsolving campaign? Consider what kind of motivation you are encouraging; for example, motivation based on prestige, rewards or points is extremely different to motivation based on justice and accountability.

# PRESERVATION AND STORAGE

Safeguarding the information you are collecting is crucial to any open source investigation.

Digital open source information can be ephemeral, and can disappear from online spaces for a host of reasons. Carefully storing and preserving online content such as photos and videos (including their metadata) will help ensure that you can access and understand it in the future, maintain research integrity, catalogue the data, and establish a chain of custody for use in legal settings.

All this allows for the possibility of using the information not just for use in your current investigation, but also in other contexts, including, where appropriate, in bringing perpetrators to account.

As individuals may have risked their personal safety to highlight particular human rights violations, memorialising and safely preserving their contributions can also be important to an investigation from an ethical standpoint.

However, when you start to take data from a public space and move it into a private setting, there are risks to consider.

**Thinking through your preservation plan**

**Step 1:** The preservation and archival standards you implement will depend on the goal of your investigation. Remind yourself of this goal by going back to the section of this workbook in which you defined it.

|  |  |
| --- | --- |
| What types of data are you preserving and why? |  |
| How long will you store the data you’re collecting? |  |
| What tools will you use? |  |
| Who will be responsible for making sure material is preserved? |  |
| Is the data sensitive? If yes, what will you do differently? |  |
| What are the relevant data protection regulations? |  |
| What security concerns are there around preserving this data? |  |

**Step 2**: Work through the questions below to create a data preservation plan.

## 

# ANALYSIS AND VERIFICATION

Once you’ve made a plan for preserving the material you’re planning to collect, you’ll need to decide how you’re going to analyse what you have, and how you’re going to verify it to assess its reliability. Part of this should involve working out how you will document and communicate the steps you’ve taken, after you’ve taken them.

The analysis and verification stage can be the point in an investigation where a decision is made as to whether the investigation is worth pursuing or not.

The analysis process can also bring to light new ways in which your investigation could potentially impact the human rights of others – as these emerge, adjust your investigative processes accordingly.

**Go back to your goal. What are you trying to do?** *Your reasons for carrying out this investigation will determine the level of verification and analysis you need to carry out.*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**How will you document what you’re doing?** *Taking notes as you go will help others follow your techniques and processes. These notes will also be helpful to you and your team later down the line, and could prove invaluable when you are writing up your methodology at the end of the investigation.*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**What are the key decisions you’ve made so far, and what were the considerations and assumptions around those decisions?**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**How might your own preferences or biases play into the way you’re planning to use, or are already using, data?** *For example, are you limited by the languages that you speak or understand, or the way in which you’re expecting a story to play out?*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**What are you missing? Whose perspective is not included in your investigation?** *For example, perhaps only people with access to the internet and digital technology will be contributing to the story that you’re seeing.*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Who on your team knows how to verify and analyse the content you’ll be collecting?***If no-one on the team has this expertise, talk to peers and experts on how to do this.*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**How confident are you in the veracity of the content you’re working with?**

There is no single method you can use to guarantee the veracity of content. Rather, verification is a process to be followed in order to give yourself and others *confidence* in the veracity of the material you are working with, and confidence that your conclusions can be trusted.

Verification processes can reduce the risk of harms being caused through the publication of unverified material. You should be as transparent as possible about what you do know, and what you don’t.

|  |  |
| --- | --- |
| *0%* | We found that the material had been posted years before the event we are investigating took place. |
| *20%* | We cannot find out where the material came from, and we only have a screenshot of it from before it was taken down. |
| *40%* | We found an article on the incident from an unknown blog, and a satellite image that could show destruction of a building, but cannot locate any other information. |
| *60%* | There is only one video of the incident online. We are pretty sure it’s authentic but cannot find any other information corroborating the incident. |
| *80%* | We have other material that corroborates this piece of information, we know where this material came from, we trust its authenticity, |
| *100%* |  |

How confident are you in the veracity of the material you have in front of you? How confident do you have to be before you publish something? The table below offers some hypothetical situations that might underpin different levels of confidence.

What are your degrees of confidence?

|  |  |
| --- | --- |
| *0%* |  |
| *20%* |  |
| *40%* |  |
| *60%* |  |
| *80%* |  |
| *100%* |  |

Fill in the table below with some hypothetical (or actual) situations relevant to your own investigation.

**How are you going to document and communicate uncertainty in your methodologies?**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Are there other ways to interpret the data you have?**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Writing out your methodology

If you answered the questions above, you now have an outline of your methodology.

**Why would you want to document your methodology?**

In an open source investigation, writing down your methodology can be important for a number of reasons:

* To increase transparency and trust in your work
* To provide more information to people who want to dig deeper
* To verify the accuracy of your investigation
* To help others replicate your investigation.

**How can you check your methodology?**

* Share the methodology you have created with trusted partners and allies for feedback – do they agree with the steps you’ve taken?
* Try to check your assumptions with others who might know more than you do.

The next section of the workbook, *Publication,* will look at how you can publish this methodology as part of your investigation.

# PUBLICATION

Now that you’ve worked through the discovery, verification, and analysis parts of your investigation, it’s time to think about how you’re going to publish and share the investigation. But not so fast. Publication is not just about exhibiting a creative technique you used, or making a beautiful graphic to illustrate it – it is also about communicating the details of your investigation, methodologies, approach and bias, protecting your sources, and correctly attributing those who took part in the investigation.

###### 

###### Deciding how, if, and what to publish

Step 1: Is it relevant?

Look at what you’re planning to publish. Is it actually necessary to make this content public? Or was it just useful for the discovery phase of the investigation? For instance, a graphic, distressing video might have informed the analysis stage of your investigation, but publishing this video might unnecessarily distress those who end up viewing it as part of your published investigation. If you lack the necessary local, political and cultural context to properly assess the risks of publication, then defer to people who do have this knowledge.

It’s also important to keep in mind that open source information is rarely published without other information gathered from interviews, expert testimonials, or other sources – these together help to reconstruct a full and accurate account of violations that might convince the public, policymakers, or judicial bodies to hold perpetrators to account. Consider how the open source information you’re planning to publish fits in with these other sources of information.

Step 2: Will it help to increase transparency and reproducibility?

In the previous section of this workbook, we explored a process for documenting your methodology. Publishing parts of your methodology can help others understand, build upon and reproduce your work.

**What might you want to publish?** Your answer to this question might include:

* Where and how you got the data
* How you analysed the data and how you came to the conclusions you did
* If appropriate, raw data downloads or scripts
* Explainer graphics or videos
* Your level of confidence with your findings – think about how to communicate any bias or uncertainty.

Step 3: Have you taken steps to gain consent? And how will you do this without putting people in danger?

When considering informed consent (which we explore more deeply in this same section), there are a number of factors to take into account. Some situations that illustrate the variety of factors informing the sensitivity of gaining consent include:

1. Contacting the producer of a video or other piece of content could easily put them in danger (from, for example, an authoritarian regime who is monitoring their communications)
2. On the other hand, a producer might have posted evidence of a human rights violation in order to share their story with a broader audience and with full awareness of the risks associated with doing so
3. Amplifying content to a different, or wider, audience than originally intended could bring more unforeseen risks to participants at every level of the investigation – even those that may not be fully aware of their inclusion

This is, in short, a complicated landscape to navigate. The steps below offer some guidance around navigating the decisions that will need to be made.

**Here are a few suggestions when getting in touch with people:**

* For making initial contact, locate a channel of communication that is non-public:
  + See if you can find an email address associated to the social media account the content was posted from
  + Send the poster a direct message or add them as a friend on social media accounts
* Be as clear and transparent as possible on why you are contacting them, including:
  + Where you are contacting them from
  + Why you want to be in touch
  + What the known risks are in being in contact with you
* Ask to move to a more secure channel, such as WhatsApp or Signal, as soon as possible.
* When communicating on a secure channel, explain what you want to use the material for, discuss what the associated risks might be now and in the future, ask if you have their permission to use their material and if and how they would prefer to be credited.

|  |
| --- |
| What constitutes informed consent? **Notice or Disclosure**: The consent process must ensure that the person is informed of the nature and purpose of the investigation, the expected benefits (if any), the reasonably foreseeable risks, how their information might be reused or shared, the option of not participating, and the procedures for confidentiality and anonymity.  **Capacity, or Understanding**: The information must be easily understood in that specific context (language, technical jargon) and the person must be given the opportunity to have any questions answered.  **Voluntariness**: Consent must be voluntary, free of any coercion or inflated promise, and not involve people who have power over those being asked to give consent. In the development context, however, it is difficult, if not impossible, to remove unequal power dynamics entirely.  **Competence:** The participant must be competent to give consent and not incapacitated due to mental status, disease, or emergency. |

Step 4: What are the risks involved in publishing certain content and what steps have you taken to understand and reduce these risks?

Write down relevant risks and mitigation strategies in the table below. Some examples have been given to help you get started.

|  |  |
| --- | --- |
| **Risk / Scenario** | **Mitigation strategies** |
| Risk: A video or image has been posted on social media, but you haven’t received consent to republish it. Publishing this media could go against the wishes of the poster and put them and others at risk. | Strategy: Embed or link to the source on social media, rather than using a screenshot or reuploading a video. This enables uploaders to choose to take the material down themselves if they wish to.  Strategy: Only republish material from social media accounts that have over a certain number of followers, as the poster will already have an understanding that what they post is public and visible to a large number of people. |
| Risk: The publication of certain material might infringe on an individual’s right to due process and a fair trial. | Strategy: Blur the faces not only of victims and bystanders but also of alleged perpetrators (who still have the right to due process and a fair trial). |
| Risk: A recent satellite image has been captured that shows people hiding in a particular area. Publishing this image could alert military forces to the whereabouts of these people. | Strategy: Consider delaying publication. Time delays are a useful tactic; in the case of this example, waiting for a period of time – whether that is a day, a week or a few months – will enable you to gain a better understanding of the situation and the risks involved. |
| Risk: Hostile actors could identify the person who has filmed a video or captured an image, or could identify the people who appear in the video. These people could become targets. |  |
| Risk: Though a video released by a terrorist group could be useful for verifying a timeline of actions and actors, publishing it could work to amplify the terrorist group’s message. |  |
| Risk: Through the verification phase of your investigation you have found the exact location a video was recorded from. If you published this location you could be, in turn, providing this information to local security forces. | Strategy: Working with local partners or researchers who know the area and context can help you determine whether the people living there would likely be targeted in retaliation or not. |
| Risk: You have to decide whether to publish a video of someone who is experiencing inhuman or degrading treatment. By doing so, you risk retraumatising, and further amplifying the trauma of, this person. |  |
| Risk: |  |

Step 5: How will you fairly assign credit and attribution?

Everyone involved in your investigation should be correctly, fairly and appropriately credited. It is important to attribute people’s work in order to acknowledge labour that is often overlooked, and for those involved in various aspects of an investigation to not feel exploited or miscredited. Power dynamics within a team can influence who receives credit, and how credit is assigned. Have conversations early on around who is doing what work, and how credit will be assigned.

**Options for those who don’t want to be credited**

It can be risky to name sources so be aware that some people might want to stay anonymous for very good reasons. In these cases, there are other possibilities that can be explored:

* Offer to credit them under a pseudonym
* Discuss alternative ways to negotiate and assign credit that do not compromise safety - for example, you could name an organisation instead of an individual.
* If you are not able to negotiate credit, consider alternative mediums through which investigators can be acknowledged for their work, for example in an independently published piece.

# 

# AFTER THE DUST SETTLES

This section of the workbook is for the end of your investigation. Hopefully, by the time you get to this you will have conducted and published a responsible and impactful investigation. Congratulations!

###### Measuring success

Go back to your goal and the measures for success you identified at the beginning of the workbook.

Did your investigation have the impact you expected it to have? If not, why not?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Investigation retrospective*

Now is the time to reflect on the processes you put in place, and to gather feedback from your collaborators in order to see what can be changed for next time.

|  |
| --- |
| Potential questions for a retrospective |
| * What were you most proud of? * What did you think you all did really well? * Did you feel icky at any point? * What would you like to change for next time? * Go back to the list of values you identified. Do you feel like those values helped to guide you during the process? Did you add or remove any values on your list along the way? * How well did the partnerships and collaborations go? What led to successes or difficulties? |

*When situations change*

In some cases, threat models change and content that was once fine to be published now puts people at risk. As mentioned earlier, when publishing social media posts, embedding or linking to the source on social media (rather than taking a screenshot or reuploading a video) gives the uploader the opportunity to take down material themselves. It will then automatically be removed from your online version of the investigation as well.

In other situations, having a plan for taking down content ahead of time and being able to communicate this to those who need to get in touch is an essential step.

###### Responding to removal requests

**How can people get in touch with you?**

* How can people get in touch with you in a secure and easy way?
* How often will someone be checking the communication channels?
* How quickly will you respond?

**What are your criteria for removing content?**

* Do you have criteria already established? For example:
  + If there are mistakes in what you have published
  + If someone is threatened by what you have published. *If the person asking for removal is a victim/survivor, or someone who was involved in capturing the data in the first place, then you should likely remove this content. If it is a company, government, perpetrator or a political figure, then you will need to make a decision based on context.*
* How transparent are you being about your decisions?

**What is your plan for removal?**

|  |
| --- |
| **That’s it!**  **You have reached the end of the Responsible Open Source Investigations Handbook - but it is really just the beginning. Take this workbook and make it yours.** |

Create a plan for how to change credit and attribution after an investigation is public, including how to remove names if a threat changes or add names if someone decides later that they wish to be credited.

Index

Choosing tools

* Section: [Deciding which tools and technologies to use](#d7w3bpdwflxw)

**Resources:**

* + [Technology Tools in Human Rights,](https://www.theengineroom.org/wp-content/uploads/2017/01/technology-tools-in-human-rights_high-quality.pdf) The Engine Room

Credit

* Section: [Who are you working with?](#dywo2sjhc9x)

Data protection

* Section: [How will you work?](#ellc0y8x1bq9)
* Section: [Deciding which tools and technologies to use](#d7w3bpdwflxw)

**Resources:**

* + Privacy Impact Assessment Process: [WFP Guide to Personal Data Protection and Privacy](https://docs.wfp.org/api/documents/e8d24e70cc11448383495caca154cb97/download/), pp 85-94.
  + For information on RAD policies, look at [the ELAN tipsheet on retention, archival and disposal](http://elan.cashlearning.org/wp-content/uploads/2016/06/Data-retention-tip-sheet.pdf).
  + If you’re curious to learn more about what goes into deleting data, check out [the UK National Archives data disposal checklist](http://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/disposal/disposal-checklist/).

Data sharing

* Section: [Making it official](#ufhyjsmxw8r0)

Feedback

* Section: [After the dust settles](#lcgam5aq69z4)

Harm reduction

* Section: [How will you work?](#ellc0y8x1bq9)
* Section: [Mitigating the risk of trauma](#lx6fiug6thgb)
* Section: [What are your ethical lines?](#dx37broik614)
* Section: [Analysis and Verification](#ojn1sxs9szcu)
* Section: [After the dust settles](#lcgam5aq69z4)

**Resources:**

* + [Making Secondary Trauma a Primary Issue: A Study of Eyewitness Media and Vicarious Trauma on the Digital Frontline](https://eyewitnessmediahub.com/research/vicarious-trauma), EyeWitness Media.
  + The Responsible Data basic [de-identification solution matrix](https://docs.google.com/spreadsheets/d/1rFgN61xBCUE5cidaCicZrx8DXtQYoHdOYXfWr1udk0w/edit%23gid=1520464066).
  + The [Responsible Data Handbook](https://the-engine-room.github.io/responsible-data-handbook/chapters/chapter-02c-sharing-data.html) includes a section on anonymising data, with tips for anonymising data.
  + Pages 111-120 of the [WFP Guide to Personal Data Protection and Privacy](https://docs.wfp.org/api/documents/e8d24e70cc11448383495caca154cb97/download/) lays out templates for a data protection notice and beneficiary consent form, a data access request form, and photo/video release form.

Impact

* Section: [After the dust settles](#lcgam5aq69z4)

Informed Consent

* Section: [What are your ethical lines?](#dx37broik614)
* Section: [Publication](#mj7ua9ic1ak)

Licensing

* Section: [Assessing partnerships](#udt1bpo3zg)

**Resources:**

* + [Creative Commons licensing](https://creativecommons.org/choose/)

Methodology

* Section: [Analysis and Verification](#ojn1sxs9szcu)

**Resources:**

* + [Tip sheet](https://docs.google.com/document/d/1bH5i2S-0IzmvwhcTn2jJsTV4uz5377CQ9XGONs_2fnY/edit) for how to write and publish your methodology

Partnerships

* Section: [Why are you doing this?](#j899cjz78rs2)
* Section: [Assessing partnerships](#udt1bpo3zg)

Power and privileges

* Section: [Who are you working with?](#dywo2sjhc9x)
* Section: [Analysis and Verification](#ojn1sxs9szcu)

**Resources**

* + [Anti-Oppression Training Resource](https://static1.squarespace.com/static/564be1d3e4b08e5f0e45876f/t/5c898d6c15fcc074e571f7f7/1552518509610/TYC+-+Anti-oppression+resource+2019+-+March+11+Export.pdf), March 2019, from the Toronto Youth Council

Preservation

* Section: [Preservation and Storage](#vhica7g6m7u7)

Resources:

* + Page 48 from [DatNav](https://www.theengineroom.org/wp-content/uploads/2017/01/en-datnav-report_high-quality_web_.pdf) on Preservation

Risk assessment

Resources:

* + [Risk Assessment Fundamentals](https://medium.com/@seamustuohy/risk-assessment-fundamentals-1b7b1b9e103f), by Seamus Tuohy
  + [Girl Effect’s sample GEM risk assessment matrix template](https://docs.google.com/spreadsheets/d/1qsbegV4uTfXdQKD-YdlpaCYyOabyZiZXn5AaTjsmXSI/edit?pref=2&pli=1%23gid=773614129)
  + [Data Innovation Risk Assessment Tools](http://unglobalpulse.org/sites/default/files/Privacy%2520Assessment%2520Tool%2520.pdf), UN Global Pulse

Security

* Section: [Deciding which tools and technologies to use](#d7w3bpdwflxw)

Resources

* + Getting started with Digital Security by [WITNESS](https://blog.witness.org/2016/11/getting-started-digital-security)

Social media platforms

* Section: [What are your ethical lines?](#dx37broik614)

Values

* Section: [Why are you doing this?](#j899cjz78rs2)

**Resources**

* + Value Mapping exercise, [Mind Tools](https://www.mindtools.com/pages/article/newTED_85.htm)

Verification

* Section: [What is your goal?](#uz6wyeusyodd)

*Thank you to* [Lorraine Chuen](http://lorrainechuen.com/) *for developing the layout of this workbook.*

1. Exercise adapted from <https://www.mindtools.com/pages/article/newTED_85.htm> [↑](#footnote-ref-1)
2. The Berkeley Protocol on Digital Open Source Investigations [↑](#footnote-ref-2)