# Digital Enquirer Kit: Guidebook

Digital Enquirer Kit
Community Edition

Created in 2022 by Tactical Tech (Denisse Albornoz, Yiorgos Bagakis, Safa Ghnaim, Andira Hayder, Christy Lange, and Nikita Mazurov).



A product of

TACTICAL TECH

Co-funded by the European Union

german cooperation
DEUTSCHE ZUSAMMENARBEIT

Implemented by
giz

# Table of Contents



# Welcome to the Digital Enquirer Kit: Guidebook!

This is a how-to guide to equip educators, community leaders, and civil society organizations with tips on using and adapting the resource to train Digital Enquirers in their own local community.

In this guidebook, you'll also find an overview of the first four modules of the Digital Enquirer Kit e-learning course.

## About the Digital Enquirer Kit

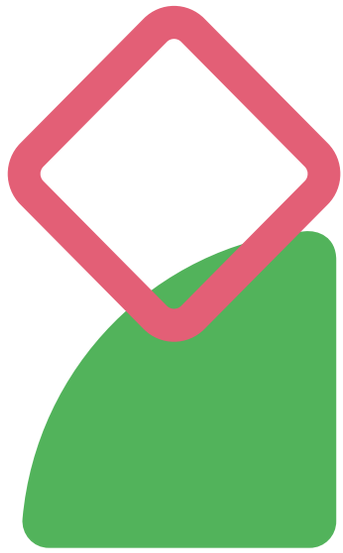
The Digital Enquirer Kit is an e-learning course focused on preventing the spread of misinformation. The course covers media literacy, verification, as well as how to navigate the internet and research safely.

◆ Track your progress and receive a certificate of completion at atingi.org ↗

This e-learning course was written for civil society activists, human rights defenders, investigators, citizen journalists, and consumers of online information and media—so-called 'Digital Enquirers'. The course contains simple explanations and real-world examples, illustrating secure research and information-gathering methods. The modules feature engaging and creative formats such as tutorials, quizzes, and interactive games.

## Dive into the Digital Enquirer Kit

The Digital Enquirer Kit follows characters who live in a diverse, multicultural, and multi-faith neighborhood at the edge of a city. Throughout the course, you'll meet Lina, her brother Junior, and their friends: Hana and Maarouf. They're all very inquisitive and use their digital skills to help their community unravel a series of challenges. As each character completes their journeys as Digital Enquirers, they pick up tips on how to investigate in an effective, responsible, and safe way. They also learn how to work together as a team, take care of their needs, and respect others.



## General Tips for Contextualization

The Digital Enquirer Kit was originally written in English with a global audience in mind. The characters are diverse in genders, ethnicities, and abilities, and have different levels of comfort with technology. The objective is that those new to, or familiar with digital investigations can see themselves reflected in the characters regardless of their background or identity. However, there are some additional considerations you may want to keep in mind if you're planning to adapt the content to your local or regional context:

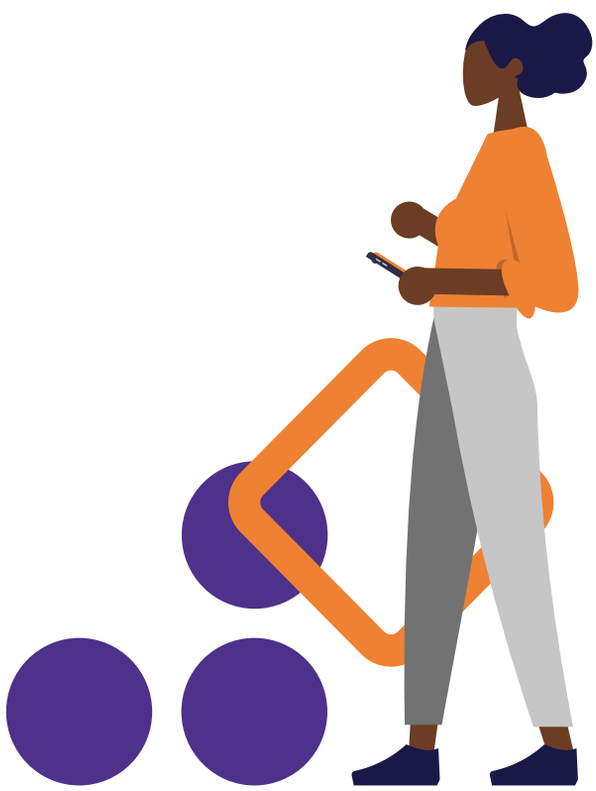
- The tone of the guide is friendly and calming. The goal is to make the Digital Enquirer Kit a space where people can explore, discover, and learn comfortably about topics that can cause confusion or fear. Refrain from using strong words such as 'threat', 'risk', or 'danger' whenever possible.
- Learners of the course are referred to as Digital Enquirers, rather than investigators, journalists, or researchers. It sends the message that anyone can learn the skills to gather credible information online safely.
- When translating specific words, consider the local jargon to avoid misinterpretation. The same word can have multiple meanings depending on the country.
- Use an abundance of caution when introducing new examples or situations for the characters. The Digital Enquirer Kit has refrained from using specific political scenarios or storylines to make it widely applicable and to ensure the learners' comfort and safety.
- When adapting scenarios, aim to remain inclusive of the different ethnic and religious minorities of your area.
- Certain avatars may be more representative of some regions of the world than others. Consider creating a backstory for those characters to provide context if needed.

**MODULE 1:**

# Identifying and Responding to Misinformation

Module 1 introduces some of the recurring cast of characters who will appear throughout the course, as they learn to deal with misinformation in their community.

Lina hears a rumor through social media that her brother, Junior, cheated on his exams. Lina follows the trail until she finds the source of the rumor. While Lina chats with everyone involved she keeps her **COWS (Challenges, Opportunities, Weaknesses, Strengths)** in mind.



## Learning Objectives:

- Develop an action plan that prioritizes **safety** in order to protect yourself, your data, and your sources.
- Discuss various facets of **misinformation** such as unreliable sources and visual misinformation.
- Identify different **sources** of information and evaluate their level of reliability and trustworthiness.
- Recognize **your role** in the information ecosystem.

## Included in Module 1:

**Lesson 1: Build Your Digital Enquirer Mindset** — the Do No Harm principle: prioritize the safety and well-being of yourself and others; risk minimization;
ABCs: Actions + Behaviors = Consequences; develop an action plan.

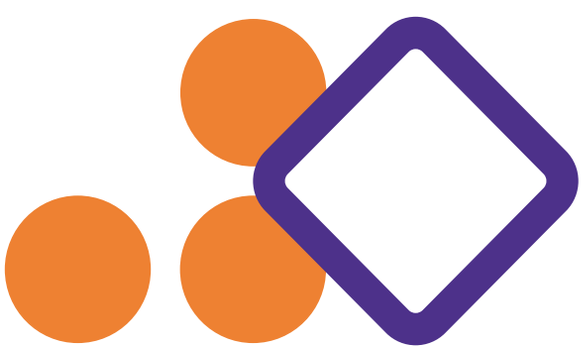
**Lesson 2: The Many Faces of Misinformation** — types of Misinformation; classify false Information; determine Levels of Harm.

**Lesson 3: Your Role in the Information Ecosystem** — find out how information spreads; your role in the information ecosystem; understand personality profiling; how your feeds are curated; craft your news feed; sharing is caring; don't let companies lure you in.

**Lesson 4: Spot Unreliable Sources** — catch the clickbait; find out if the URL is trustworthy; recognize tricky URLs; learn about trackers; whether or not to click links; exercise caution and make sure URLs are safe.

**Lesson 5: Explore Visual Misinformation** — examine a mislabeled photo; learn about "cheap fakes"; identify deepfakes.

**Lesson 6: Put It All Together** — a review of key takeaways.



## Tips for Contextualization of Module 1

◆ Terms like 'disinformation' and/or 'fake news' are used colloquially in various languages to refer to all types of false information. In some countries, there is no direct translation for 'misinformation' or 'malinformation' either. Find opportunities to explore the meaning of each word and offer examples on how each type is different from one another.

◆ Terms like 'cheap fakes', 'deepfakes', or 'clickbait' may not have a direct translation and are used by their English name in other languages. If this is the case in your context, offer clarifications if needed.

**MODULE 2:**

# Verifying Online Information

Module 2 follows Junior as he investigates a new medicinal drink called “Pandemic-Cure”. He becomes concerned about **clickbait headlines** calling the product a “miracle” and how they have persuaded Auntie, a beloved lady from his neighborhood, to purchase it. Junior decides to seek trustworthy information that confirms or denies the product’s safety. In these lessons, he learns to evaluate and verify a variety of sources and recognize which of those are **credible, authentic, and timely**. In the process, he learns how to use everyday devices like his smartphone and his laptop in a **private, safe, and secure** way.

## Learning Objectives:

- Conduct **research** using the Scientific Method principles.
- Discover **digital security fundamentals**.
- Identify characteristics of **credible**, **authentic**, and **timely** sources of information.
- Explore **verification methods** for visual information.

## Included in Module 2:

**Lesson 1: The Scientific Method** — introduction to the Scientific Method of researching; critical questions to ask; develop a working hypothesis.

**Lesson 2: Digital Security Basics Before You Get Started** — set up screen locks; boost your browsers; keep your findings safe and private; achieve password power.

**Lesson 3: Know Who You Can Count On** — credibility basics; your checklist for reliable information; neutrality in the news.

**Lesson 4: Asses Authenticity** — the trouble with bots; identify bot-like activity; learn about rewards for reviews; detect inauthentic engagement.

**Lesson 5: What's in a Picture?** — learn about and conduct a reverse image search; get creative with image searches.

**Lesson 6: When: It's a Matter of Time** — stay on top of updates; filter by date; find patterns within the dates; revisit your hypothesis.

**Lesson 7: Put It All Together** — a review of key takeaways.

## Tips for Contextualization of Module 2

◆ Identifying "inauthentic engagement" may require different strategies according to context and legislation (e.g., in some countries, it is mandatory to add a hashtag that indicates a post is advertising if there is a material connection between the poster and what is being promoted, while in others it is not).

◆ Double-check that the reverse-image search tools are available in your area.

◆ The use of VPNs may be illegal in some countries.

**MODULE 3:**

# Documenting and Collaborating on Your Digital Enquiry

In Module 3, Hana, Junior, Maarouf, and Lina examine a case of a polluted river. The company Lion Corp posted a video online which at first glance appeared to depict their friend Gemi dumping something in the river. The group gathers information, collecting and documenting their research, to determine whether the claims in the video are accurate or not. The team, composed of diverse members with complementary skills, sets **SMART (Specific, Measurable, Achievable, Relevant, and Time-Bound) goals** to help make sure that their research is successful, selects **collaborative tools** to use, and is sure to take **steps to protect** their main source, Jane, such as by not revealing identifying information about her in their notes.

## Learning Objectives:

- Find out how to set up an equitable **Digital Enquirer team**.
- Select and use the right **collaborative tools**, balancing security and usability.
- Evaluate your safety situation and **design a safety plan**.
- Document **verifiable information and evidence** with care.

## Included in Module 3:

**Lesson 1: Evaluate Your Unique Safety Situation** — revisit the Scientific Method; uncover the claims; assess whom you might be up against; figure out your safety plan.

**Lesson 2: Set Up Your Digital Enquirer Team** — build your team; align and set up goals; risk is inherited.

**Lesson 3: Select Your Collaborative Tools** — examine end-to-end encryption; balance security and usability; evaluate collaborative tools; set up a group chat.

**Lesson 4: Start Your Documentation** — record your journey; assess pros and cons; select pseudonyms; store your files; begin documenting.

**Lesson 5: Document with Care** — write lean documentation; seek informed consent; incident documentation; tips for collaborative documentation.

**Lesson 6: Put It All Together** — a review of key takeaways.

## Tips for Contextualization of Module 3

◆ Gemi is a non-binary character. When discussing their storyline, make sure that you refer to them using gender-neutral pronouns and conjugations that may be relevant in your context.

◆ Ensure that the recommended apps in this section are available and accessible in your areas (e.g., Signal). It's more productive to encourage the audience to learn how to conduct the usability-versus-security exercise with locally-relevant apps.

**MODULE 4:**

# Examining and Sharing Your Findings

Module 4 follows Maarouf as he realizes that surveillance cameras have been installed in his apartment building. Since then, the building owner, Mr. J. has started acting suspiciously, collecting information about tenants, and treating them unfairly. Maarouf wants to protect his neighbors and gathers a team to uncover if these events are connected. Throughout the Module, Maarouf and his team learn new techniques to **collect and visualize different types of data** and to become more **aware of their biases** when sorting and interpreting this evidence. After learning about appropriate techniques to report and share their findings, the team identifies **self-care strategies** to recharge before their next enquiry starts.

## Learning Objectives:

- Recognize your **thought patterns and biases** when dealing with evidence.
- Identify the **characteristics of metadata** and learn how and when to preserve or remove it from files, taking privacy and safety considerations.
- Apply **ethical considerations** to determine what data to use and document in your project.
- Report and **share digital enquiry findings** with care and with the right audiences.
- **Practice self-care** as a Digital Enquirer.

## Included in Module 4:

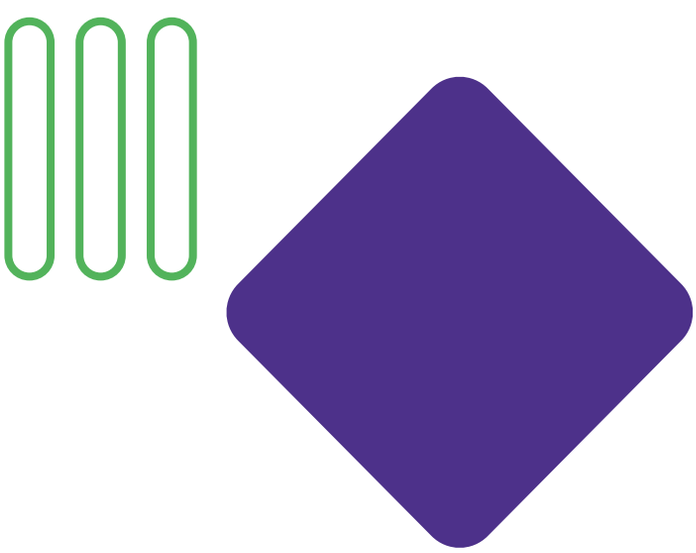
**Lesson 1: Be a Mindful Digital Enquirer** — qualities of reliable evidence; recognize your thought patterns; balance your biases; stick to the verifiable facts.

**Lesson 2: Expose the Invisible** — preserve the metadata; explore Exif data; get a grip on geolocation; view geolocation metadata.

**Lesson 3: Dive Deeper Into Data** — establish your limits; quantify your data; look into individuals and companies; save your digital evidence.

**Lesson 4: Report and Share Your Digital Enquiry** — reach your audience; publish and distribute your findings; give yourself a break.

**Lesson 5: Put It All Together** — a review of key takeaways.



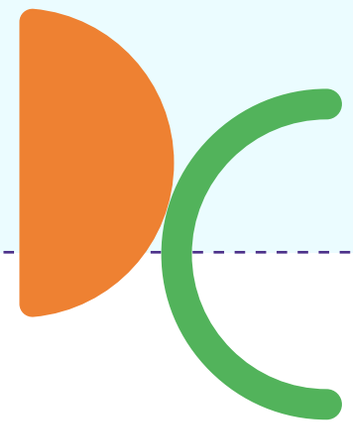
## Tips for Contextualization of Module 4

◆ Each country has different avenues and platforms to investigate criminal records. Make sure that your inquiry is rights-abiding and relies on publicly-available information. Recall the Do No Harm principle.

◆ Assess the local relevance and availability of tools used to search people and companies.

# Engaging with Digital Enquirers and Fostering Community

In addition to using the Digital Enquirer Kit e-learning course, there are various ways in which you can engage with learners and foster Digital Enquirer communities. We invite you to consider ways in which the Digital Enquirer Kit resources could fit into your local context and can fulfill a current need, starting with these suggestions.



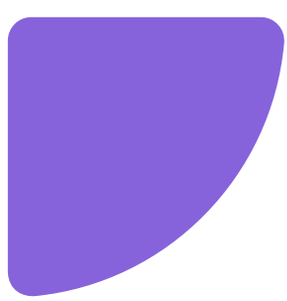
## Community Digital Enquirers

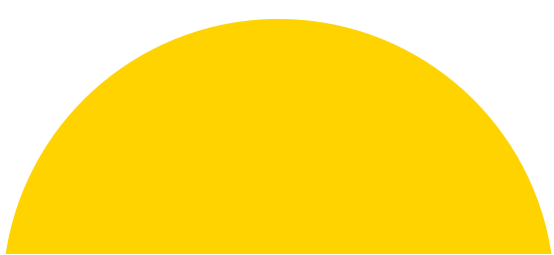
Community Digital Enquirers are leaders who support their local communities* by encouraging more individuals to be trained using the Digital Enquirer Kit and to regularly practice their Digital Enquirer skills. As a Community Digital Enquirer, your goal is to build networks and reach out to individuals or organizations in order to create opportunities for engagement, skills trainings, and dialogue exchanges.

* Your community could be your university class, work colleagues, or people around your neighborhood.

## What can you do as a Community Digital Enquirer?

- ↪ Provide educational services or curricula that educate about accessing, utilizing, and disseminating verified and verifiable information.
- ↪ Bring people together to discuss issues of common interest and build understanding across differences.
- ↪ Build institutional relations by liaising with schools, libraries, and organizations.





## Digital Enquirer Club

Community Digital Enquirers come together in the Digital Enquirer Club, which is a group for community leaders to develop a shared repository of ideas, experiences, and tools related to their practice.

The Digital Enquirer Club can be a space for Community Digital Enquirers to:

- Request information
- Exchange experiences
- Collaboratively solve problems
- Share and reuse assets
- Consult with peers before running a project
- Document a project

To start a Digital Enquirer Club:

↪ Research if there are existing clubs in your area to cooperate with or join.

↪ Clarify the membership policy and recruit community members (start small, with just a couple of reliable members).

↪ Design activities and processes, which include deciding on meeting frequency and choosing a communication channel.

↪ Develop a data collection plan and a legacy plan to ensure that the collective knowledge generated through the work of the club is made available to the broader community.

**Youth Digital Enquirer Club:** A Digital Enquirer Club could also be set up at a school or after-school space in order for young people to engage in topical issues and to uphold the tenets of the Do No Harm principle, as well as ensuring credibility, equitable and inclusive teamwork, and fact-checking.

# Digital Enquirer Activities

## Information Then and Now (30 minutes)

**Learning objectives:**

Compare and contrast the current information landscape to 50 years ago.

Discuss how technology (access, design, incentives) shapes information we receive.

**Description:** This activity gives participants the chance to share their knowledge about information access and exchange in the past and the present. This opens the chance for an exchange about what information sources we have access to and how our news feeds are shaped.

**Materials:**

- Worksheet (printed per group) [See Item 1 in the Appendix (p. 21)]
- Pens

**Instructions:**

1. Divide participants into small groups (3 to 5 people).
2. Each group fills out the diagram comparing the status of information today versus 50 years ago.
   - Encourage participants to think of information in terms of accessibility, reliability, quantity, quality, etc.
     - Example: Now, it's easier to access information of all kinds online. Then, diverse information required more effort to seek out.
   - Participants should also look for similarities which they can list where the two circles overlap in the middle.
3. Go back to the big group and share—in the first round of sharing, each group should only share one or two points so that the first group doesn't take all the ideas!

**Debriefing:**

The facilitator might need to highlight concepts like:

- 'Filter bubble' or an 'echo chamber' (and how these also existed pre-internet; the internet has mirrored/amplified existing societal issues).
- How information is complicated (not always clear at first which information is misleading, or if the source is truly credible).

## City Spotting Game (20 minutes)

**Learning objectives:**

Practice asking critical questions of visual information.

Identify the clues within visual information when verifying details.

**Description:** This activity allows participants to try some image verification skills using just their eyes and no digital tools. Look closely and carefully at the images and see if you can spot any clue as to which city these images are from. This activity works best with older teenagers and adults.*

**Materials:**

- Slides [See Item 2 (p. 22) in the Appendix]
- Optional: QR code [See Item 3 (p. 26) in the Appendix]

* You can recreate this activity with different images, but make sure your choices are neither too easy nor too difficult for your participants' age group.

**Instructions:**

1. Set the timer to allow one minute for participants to look at the photo quietly and notice clues.
   - In case the pictures are too hard to see, use the QR code so participants can bring up the images on their phones.
2. After the minute ends, participants can shout out the clues they see.
   - During this portion, ask participants to describe the clues, not only point them out. Ask: why is that worth paying attention to?
   - Encourage the participants to ask as many critical questions as possible. If they get stuck, help them (e.g., "What do you notice about the cars/signs/environment?").
3. The slide following the city image will reveal the clues and the facilitator can announce the answer; be careful not to give away the answers too soon.

**Answer guide:**

1. London's Chinatown

Clues:

- Language on the sign
- Architecture
- Office rental sign "Office to let"
- Casino name on banner

2. Tianducheng, China

(also called Sky City)

Clues:

- If you zoom in closely you can see the language on the business signs are all in Chinese
- Mountain ranges like this are not visible in Paris
- There is text on the ground that says Sky City
- High rises like these are not seen this close to the Eiffel Tower in Paris

**Debriefing:**

The facilitator might need to highlight concepts like:

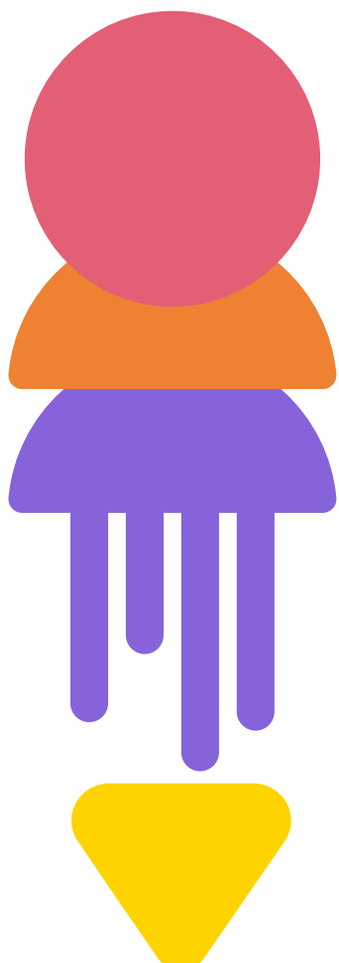
- What do you do when you don't immediately know the answer? (ask critical questions, research online—for example, using a reverse image search tool).
- Forms of visual misinformation, such as using a photo out of context and having an incorrect caption on an image, can be used to tell a misleading narrative.
- If a headline or image evokes a strong emotion like surprise, anger, fear, confusion, etc., take that as a sign that further research should be done to verify the details.

# Taking Care of Your Digital Enquirers

As facilitators of the Digital Enquirer Kit, one of your roles is to practice what you teach, and to above all abide by the Do No Harm principle—which means prioritizing the safety and well-being of yourself and others; in this case, the safety of your budding Digital Enquirers. Some key ideas surrounding this principle are:

## 1. Risk is inherited

A core principle of digital enquiries is that **risk is inherited**. This means that even if you carry little-to-no risk (e.g., living and working in a safe area), but you're teaming up with or interviewing someone who's experiencing high risk (e.g., living in a dangerous area or working on a controversial issue), the risk level of the entire group will become higher for a period of time before, during, and after collaborating with that person. Everyone in your team or group will also inherit your risk.



## 2. Safety and privacy considerations

As risk is inherited, safety and privacy precautions should be sufficient to **protect the most vulnerable** of participants. In other words, when weighing different safety and privacy considerations, always choose the options that will provide the requisite amount of safety and privacy to those in the group who would need it most. Be sure to proactively ask participants if they have any specific safety and privacy concerns, and to incorporate these into your **ground rules** from the start.

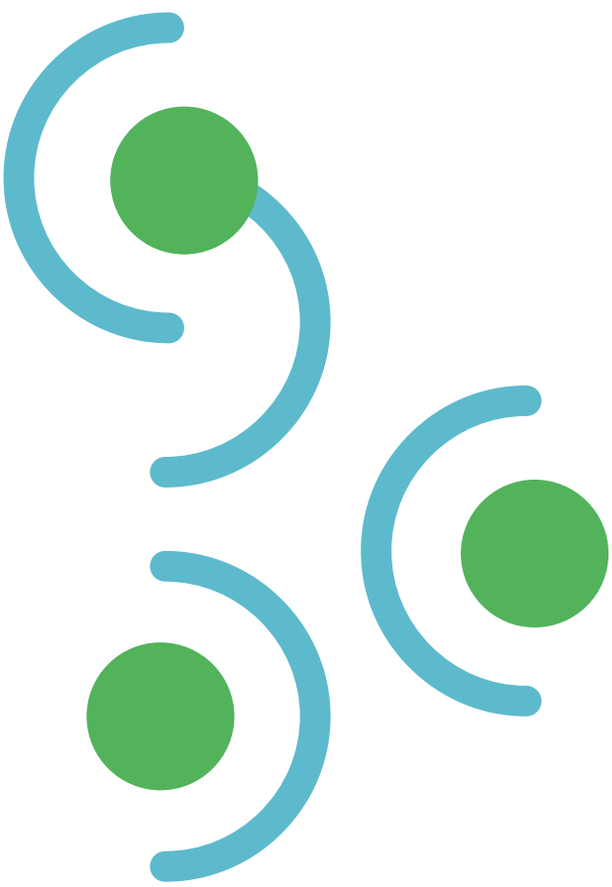
## 3. Informed consent

Make sure to always obtain informed consent in your projects or workshops. To ensure informed consent, you must:

- Use **plain and direct language** to explain the anticipated risks of the participation or collaboration.
- Provide your sources with **clear ways to refuse** to participate in your project.
- Make sure that your participants are aware that they're free to **change their mind and revoke their consent** at any time.

## Ground Rules for Your Event

Presentations, trainings, and workshops inspired by the Digital Enquirer Kit could take different formats, depending on the context they're delivered in and the audience you're trying to reach. However, there are a few ground rules you can follow to make sure that everyone feels safe, secure, and comfortable during these sessions. These include:



1. **Request the consent of participants** at different stages of the workshop. For example, before capturing any records of the session (e.g., photos, videos, or audio recordings), or before requesting that participants share any sensitive information.

a. Explain how these records will be used, if they will be shared and where, how long and where they will be stored, as well as when they will be deleted.

b. Photos of minors shouldn't be taken at all, especially without participant/parental (or guardian) consent. If they need to be taken for context-specific reasons, use tools to blur or hide their identities (e.g., Signal's blur function [https://signal.org/blog/blur-tools/ ↗], or craft physical masks).

c. Provide participants clear avenues to refuse to provide consent to these records or to participate in different moments of the workshop (e.g., in online workshops, recordings can stop when participants are sharing sensitive information; in offline workshops, participants can use red stickers to indicate they would rather not be photographed).

2. When documenting the workshop, **record the ideas** raised but don't identify your participants by name, unless you think that attribution is both necessary and safe in your context.

3. Provide a **point of contact** during the workshop that can be approached if a participant is feeling unsafe, **anxious**, or confused.

## Communication Tools and Tips

Much like the Digital Enquirers do throughout the modules, use safe communication tools and practices when organizing Digital Enquirer Kit events. You can do this by:

- **Assessing the risks** that both you and various Digital Enquirers might face, and adjust your communication methods accordingly. For example, if undergoing the Digital Enquirer Kit training may expose participants to heightened risk, **use pseudonyms** instead of actual names in your phone contacts.

- **Using a secure messaging platform** such as Signal or Wire, being sure to **test** the selected communications tool beforehand to make sure that it works in your region.

- **Having a backup communication channel** in place, so that in case your primary tool stops working you can seamlessly transition to another one without any disruption.

- **Selecting an innocuous name** for your group and setting up **disappearing messages** when you first create the group, prior to inviting people into it.

- Keeping in mind that not everyone who participates in your project may be who they say they are, so remind everyone to **not share any private or sensitive information** in your group which could increase their risk.

## Tips on Promoting and Outreaching Your Event

Decide how you will advertise the Digital Enquirer Kit sessions. Is it safe to advertise the events via public venues like community bulletin boards (both online and physical boards), or is it best to stick to private invite-only social media groups? If you're going to be posting in groups in which you’re not an active, established member or a moderator, make sure you get permission from the group administrators to post about the event. Be sure to **establish trust** with community leaders to make sure that you have their support.

# Resources

There are a number of additional related resources available from Tactical Tech (tacticaltech.org ↗) if you want to dive into many of the topics covered in the Digital Enquirer Kit in more depth.

**Exposing the Invisible** is a project about the techniques, tools, and methods of digital and non-digital investigations. Using activities, films, guides, and a bank of resources, ETI aims to encourage transparency and accountability and to make investigation accessible to everyone. exposingtheinvisible.org ↗

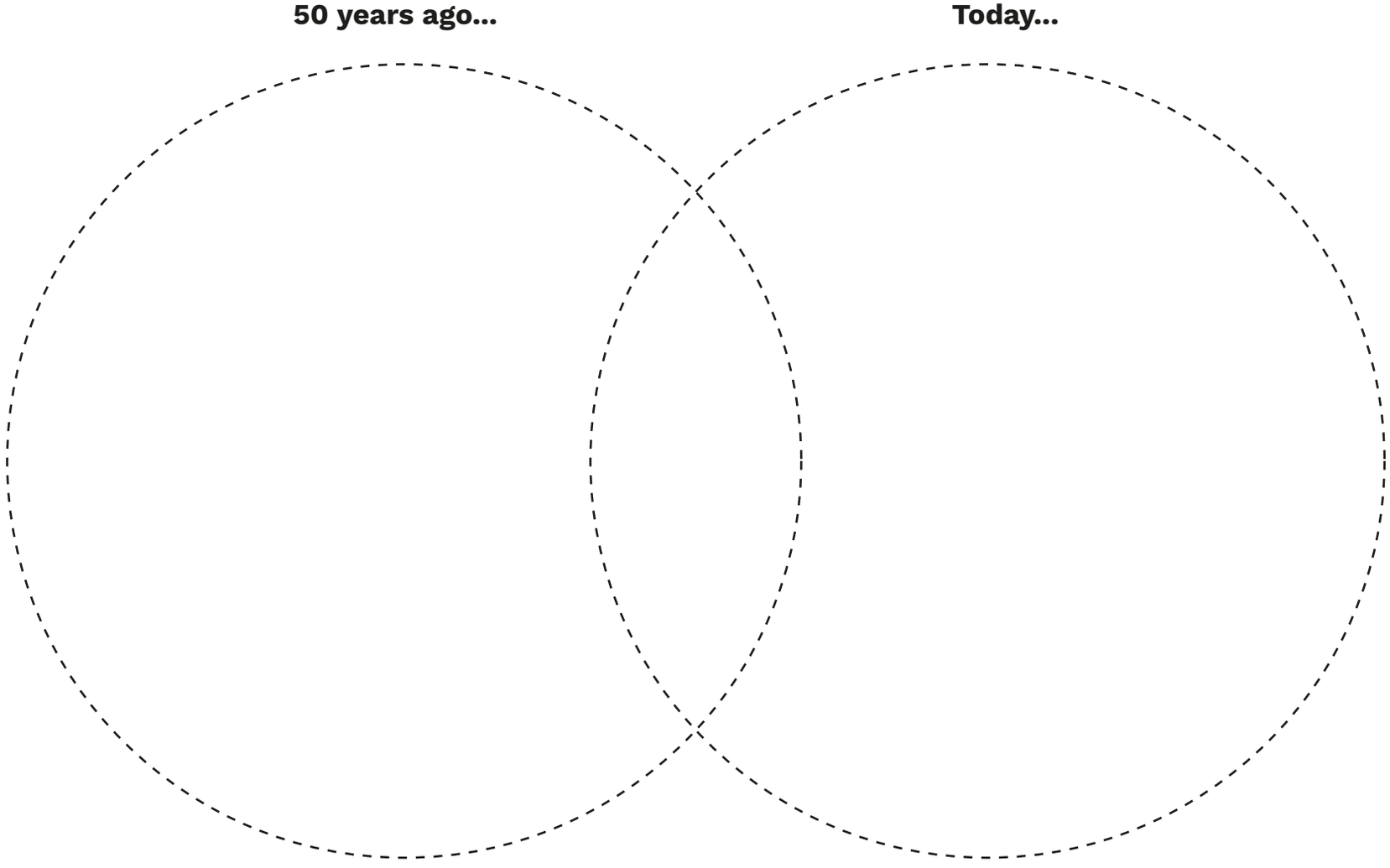
**The Data Detox Kit** provides everyday steps you can take to control your digital privacy, security, and well-being in ways that feel right to you. datadetoxkit.org ↗

**The Glass Room - Misinformation Edition** explores different types of misinformation, teaches you how to recognize it, and how to combat its spread. theglassroom.org/misinformation ↗

**The Gender and Tech Resources** project provides a number of resources gendersec.tacticaltech.org ↗, such as the “Zen and the art of making tech work for you” manual gendersec.tacticaltech.org/wiki/index.php/Complete_manual ↗

# Appendix - Item 1

## INFORMATION THEN AND NOW



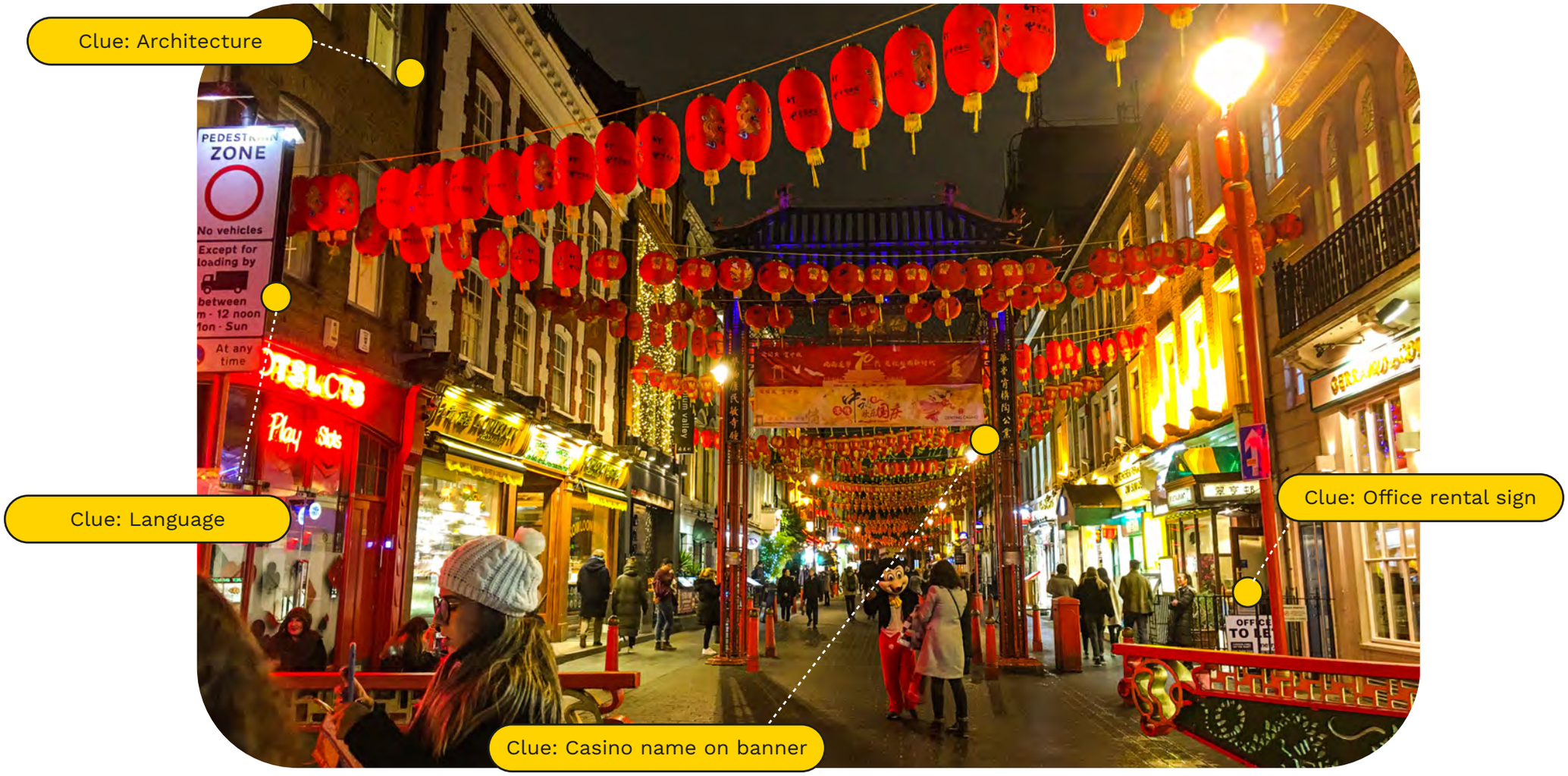
# Appendix - Item 2

## CITY #1

# Appendix - Item 2

## CITY #1: CLUES

Photo credit: cattan2011 on Flickr (CC BY 2.0)



# Appendix - Item 2

## CITY #2

# Appendix - Item 2

## CITY #2: CLUES

Photo credit: MNXANL on Wikipedia (CC BY-SA 4.0)

# Appendix - Item 3

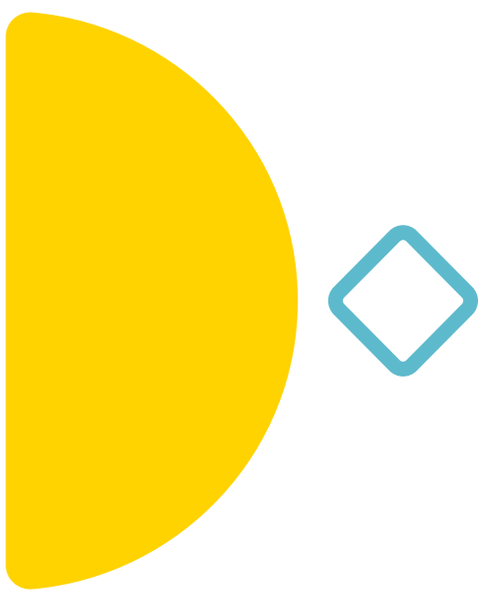
## City Spotting Game Photos

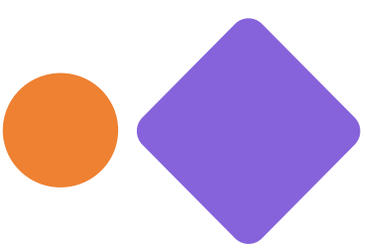
https://cdn.ttc.io/s/digital-enquirer-kit/activity/city-spotting-game/Digital-Enquirer-Kit_City-Spotting-Game_Guidebook.pdf ↗

atingi.org

Digital Enquirer Kit

Community Edition





A product of

TACTICAL TECH

Co-funded by the European Union

german cooperation
DEUTSCHE ZUSAMMENARBEIT

Implemented by
giz