



TACTICAL
TECH

EXPOSING THE INVISIBLE

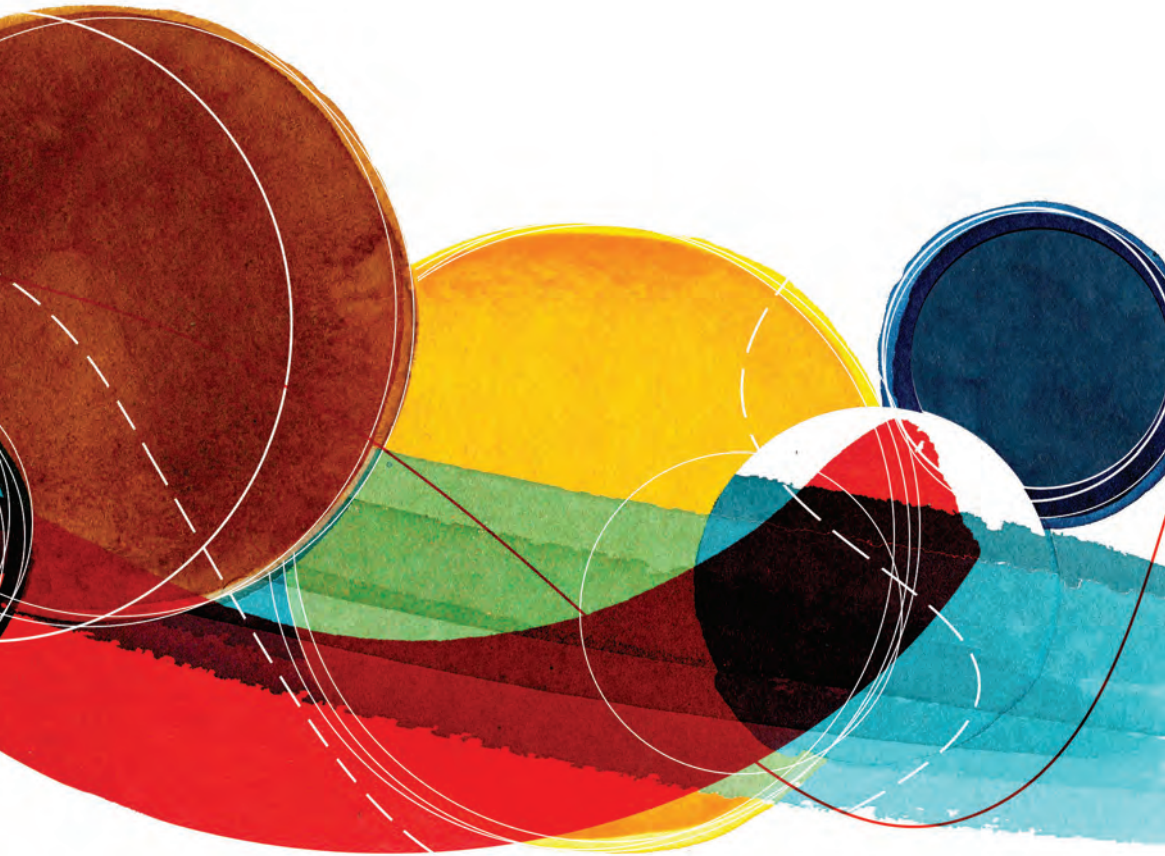
THE KIT

Investigation is a mindset. Get started.
kit.exposingtheinvisible.org

EXPOSING THE INVISIBLE

- 2 **THE KIT - AN INTRODUCTION**
- 6 **YOU ARE ALREADY AN INVESTIGATOR**
- 10 **WHAT MAKES AN INVESTIGATION**
- 20 **SEARCH SMARTER BY DORKING**
- 26 **RETRIEVING AND ARCHIVING INFORMATION
FROM WEBSITES**
- 34 **HOW TO SEE WHAT'S BEHIND A WEBSITE**
- 42 **USING MAPS TO SEE BEYOND THE OBVIOUS**
- 52 **AWAY FROM YOUR SCREEN, OUT IN THE FIELD**
- 60 **INTERVIEWS: THE HUMAN ELEMENT
OF YOUR INVESTIGATION**
- 68 **HOW TO MANAGE YOUR SOURCES**
- 74 **SUPPLY CHAIN AND PRODUCT INVESTIGATIONS**
- 82 **SAFETY FIRST!**
- 90 **GLOSSARY**
- 95 **CREDITS**

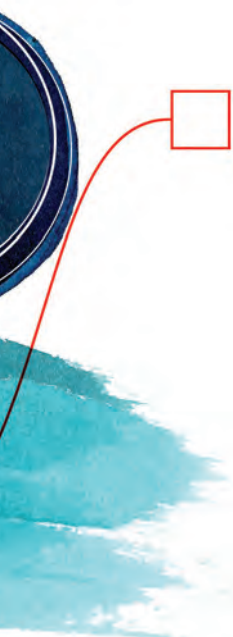
THE KIT



The Kit is a collaborative, self-learning resource that makes investigative techniques and tools used by experienced investigators more accessible.

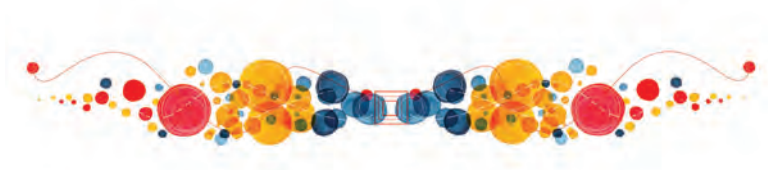
What is the Kit?

The Kit is a collaborative, self-learning resource that makes investigative techniques and tools used by experienced investigators more accessible to people and communities who feel motivated to start their own investigations, collect and verify information, build evidence and create a better understanding of issues without losing sight of ethical or safety considerations. The aim is to help people develop the ability to question information that they suspect is false, find information when it is scarce and filter information when it becomes overwhelming.



Here you can explore tools to access websites that have been removed from the internet, content that does not appear in search engines or data from videos and images that would otherwise remain invisible. You will discover ideas on how to approach investigations into companies and public funds or to find out how products you use and consume were made, and what abuses might have happened along the way. You can figure out how to use maps to investigate places and events, or how to prepare for field research. You will get tips about talking to people and observing places, assessing risks, collecting and using information safely and ethically, and making sure that you and others involved can stay out of harm's way. You will also see how to approach data from unexpected entry points or discover information resources and tools you didn't know about.

| This publication is a condensed version of the Exposing the Invisible Kit. |
| The complete kit is available online: kit.exposingtheinvisible.org |



Who is the Kit for?

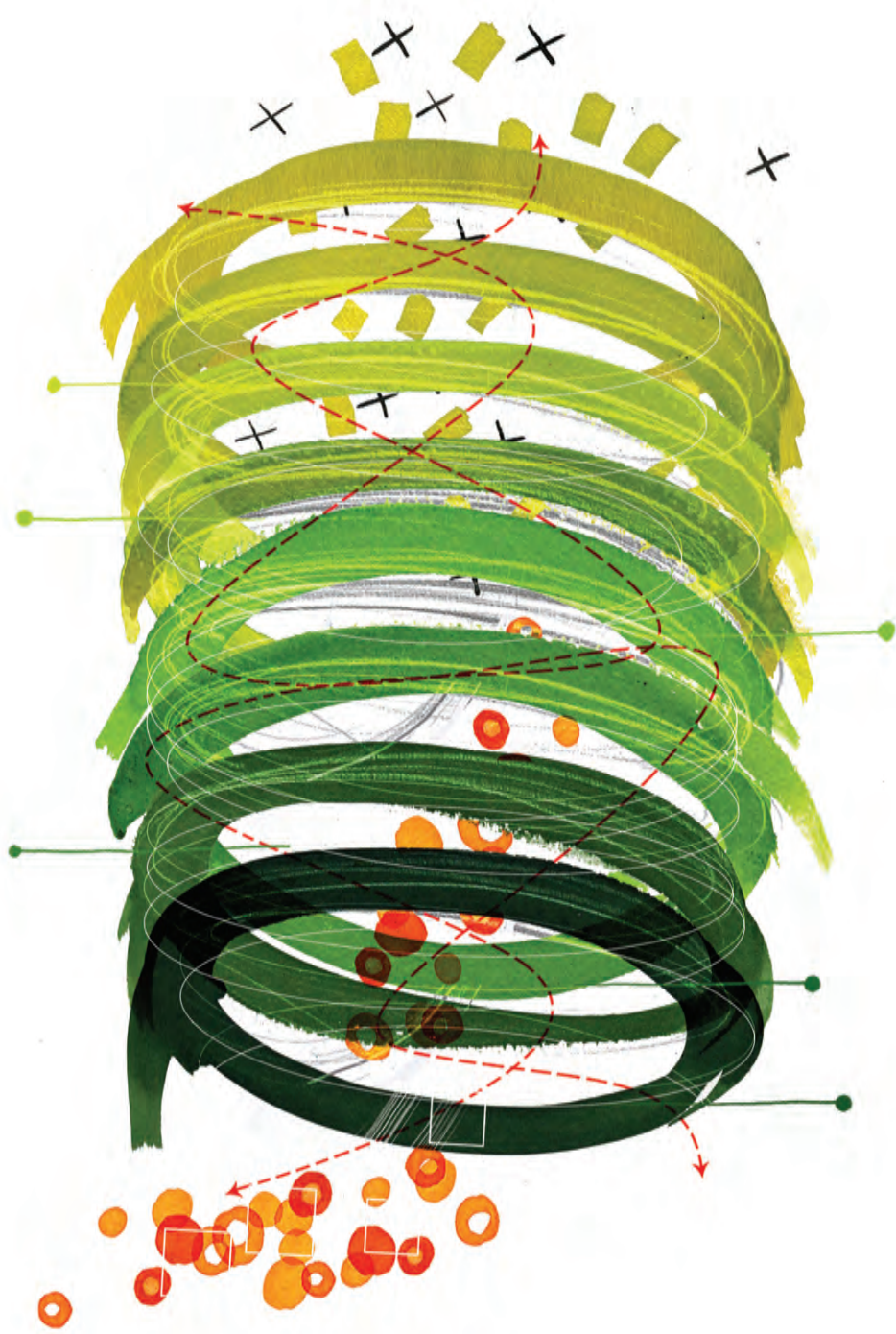
The Kit is meant for everyone. It does not matter what skills you may or may not have; it does not matter if you are just thinking of starting your first investigation or if you have already carried out several. As long as you have questions and curiosity, this is the kit for you.

This kit is issue-agnostic. It is not intended only for those who are challenging corruption or abuses of power. We believe that change happens all the time and everywhere. Neither the scope nor the scale of your investigation matters. Spending some time here will be worth your while even if all you are challenging is your own assumptions. This is meant to be a place where you can refine your thinking and determine how to go about your work in a thorough, step by step manner.

Who is behind this kit?

Tactical Tech launched the Exposing the Invisible project in 2010 with one simple goal: to showcase investigations that are sometimes outside the realms of journalism and law enforcement. Since then, we have made a number of documentary films, recorded hours of interviews, collected and analysed tools and tactics, run numerous trainings and workshops and hosted two larger events – a Data Investigation Camp, in 2017, and a ‘Kit’ Residency one year later, which gave us a starting point for this resource. Both the concept and the content of this kit owe much to many. Please visit the Credits section for more details.

| The Kit is a resource of Exposing the Invisible (ETI):
| exposingtheinvisible.org



YOU ARE ALREADY AN INVESTIGATOR



This kit will show you how to move from curiosity to investigation to action.

So you're here

You are already an investigator. That is why you are here. You have the curiosity, or the skills, or a problem that needs solving. You need to gather information, or you've already found information and you want to know how to use it.

The content of the online version of this Kit is being developed collectively by a group of researchers, activists, journalists, developers, artists and others eager to share knowledge on how to conduct investigations using a wide range of skills, tools and techniques. Like you, they are curious and motivated to learn about problems affecting their surroundings and to act on that information.

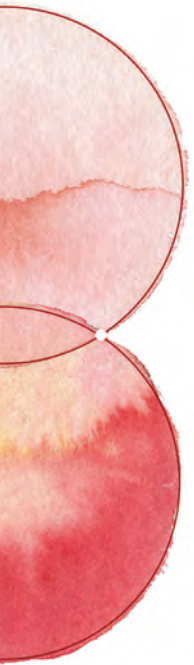
Using this kit, you will uncover different ways to build knowledge that can help you address an issue or simply to verify information instead of taking it for granted. Whether you are seeking to uncover corruption in local politics, document the manufacturing process of a product you consume, or map the scale of environmental damage in your neighbourhood, here you will find inspiration, useful techniques and important safety tips.

Investigating is like putting a puzzle together. The pieces are scattered around; some of them might be lost. You still want to find out what the big picture looks like, and you don't need all the pieces for that. That's what we want to show you here: how to collect relevant pieces, put them together and draw meaning from that incomplete picture.

Investigation is a mindset

An investigation is a process of collecting and analysing information from different sources and drawing conclusions that address an initial question, problem or assumption. This process allows you to build a body of knowledge about a person of interest, an organisation, a place, an event, a crime... you get the idea.

Investigations serve a clear purpose: it might be seeking the truth, understanding a pattern or creating – or countering – a narrative. The key to fulfilling that purpose is turning a body of knowledge into a body of evidence, an unbreakable proof, by interpreting and giving meaning to that knowledge. The process of setting your purpose, gathering information and extracting meaning is the central structure of any investigation.



Investigations are often non-linear, iterative processes. They involve a certain mindset to approach questions from different angles and with various tools and techniques. Be ready to rethink your strategies along the way if your current path reaches a dead end. You may need to consider alternative methods to interpret the same piece of information or search elsewhere for additional evidence that refines your understanding of the picture you're putting together.

Risks and rewards

As you start investigating you really don't know what you will find out there, so be cautious and aware. There may be safety concerns, legal risks or unexpected situations such as encountering challenges that go beyond your skills and abilities.

Before diving in, be mindful of your own safety and the risks involved in whatever tools, information sources and techniques you want to use. Consider the technology and devices that are most suitable for each investigation you plan and be aware of the physical environment you live and work in. Just as you can find traces of events or individuals that you are investigating, your own research can leave traces that can put you, your collaborators and your sources at risk.

Think of whether you need to work alone or collaborate with others, and whether you can find alternative ways of obtaining evidence if your initial plan seems too risky. Of course, you can't predict everything, and each investigative experience is unique in its own way.

But whether you are dealing with a low-tech environment, a conflict environment or simply the internet, you should be able to assess the risks you take and identify possible solutions by following the tips and techniques outlined in this kit.



This kit is yours

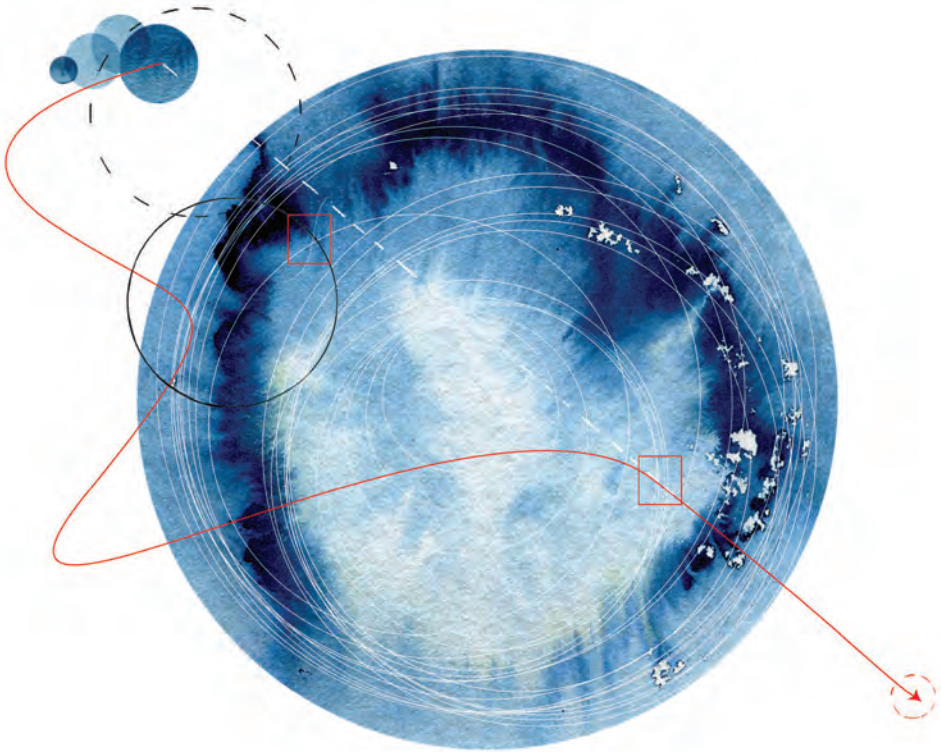
At a time when we are all saturated by data and confronted by misinformation, it's important on a personal and community level for us to be able to identify sources of problems and counter misleading narratives that are not based on facts and evidence. If facts are valuable in order to keep us away from unfounded rumors, then the process of uncovering and documenting these facts is also valuable.

The greater your arsenal of tactics the more you are able to grow and apply your investigative skills beyond what you are already doing.

Unfortunately, you can't always rely on others to determine the facts for you. Journalists, civil society organisations and others who investigate for a living are often unable to keep up with the speed at which misinformation and corruption currently spread and affect everyone. Sometimes you need to find out answers for yourself and conduct your own inquiries. Luckily, there is now an abundance of information of public interest that can be collected from offline and online resources with accessible tools and techniques. Also, for every technique developed to mislead you these days, there are more and more open-source tools and opportunities to verify or de-bunk.

This kit wants to take advantage of all these opportunities and amplify the investigator's mindset. Whether you are just starting, or you already have some experience, this resource can help you in many ways.

WHAT MAKES AN INVESTIGATION



Look at the most important elements of an investigation: what makes good evidence, how to develop a strong documentation process, the value of verification, and the key to a safe start.

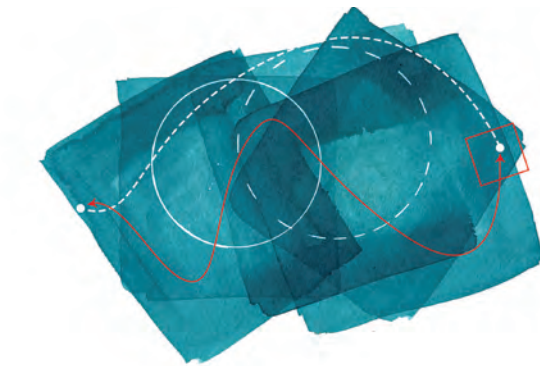
Building solid evidence

Throughout the kit, we use the generic meaning of evidence: information that is material to the question, problem, person or process you are investigating. There are legal definitions of evidence that can be much stricter, but this generic meaning serves more diverse investigations.

Evidence provides you with the confirmation of a claim or assumption. It is proof of something that happened, or of something that didn't happen. Interpreting and attributing meaning to information you collect produces a body of evidence. It's important to keep in mind that not every piece of information is, or can turn into, evidence.

An investigation is a process of organised evidence collection, which seeks to be as close to the truth as possible. The past leaves behind residue: dust, footprints, documents, videos, audio recordings, witnesses, scents, paperwork, the presence or absence of something that was or wasn't there before. Collecting evidence means finding and verifying these traces. While it's impossible to recreate history, these traces of events, relationships, transactions or places can be linked to prove that your story is based in reality.

Identifying links between pieces of information will bring you closer to the answers you seek, and the evidence to prove them. After all, you want a solid, unshakable foundation for your investigation.



Your checklist for good evidence

Not all evidence is good or relevant. There are some qualities that distinguish what is “good” and useful for your investigation. The best way to make sure you are on the right path is to test the strength, accuracy and integrity of your information, and to ask yourself a few guiding questions.

Good evidence:

is first-hand – information you find out yourself.

is documented and preserved – you can record and demonstrate the process that led you to the evidence.

is timely – collected and verified close to the date of the event.

can be verified by others – someone else than you should be able to confirm its source and content accuracy.

connects other pieces of information together – helps you build the bigger picture.

includes metadata – more information beyond the content, such as details on its author, date, location.

doesn't expose human sources to risk – ensures vulnerable people are not harmed.

may contradict you – it turns your initial assumptions or beliefs upside down.

speaks for itself.

Not every piece of evidence you discover will meet all these conditions. That's to be expected. But some of the evidence you find will meet a lot of them – those pieces are the ones you may want to prioritise.

Without documentation, it didn't happen

Documentation means keeping track of every step you make, every piece of data and evidence you collect with details such as what it is, where, when, why and how it was collected. Preserving this data in its initial form and features is crucial for your investigation.

The primary goal of documentation is to create a verifiable record of your investigation. Let's call it 'investigative hygiene' – regular maintenance of certain practices to ensure your investigation is healthy and can stand up to scrutiny and criticism if anyone tries to dismiss your evidence.

As you progress, documentation can help you remember prior conclusions or how you got leads or evidence that seemed useless before but now seems important. You might also find things you forgot to follow up on or problems you wanted to ask someone else to help with.

Your **documentation habits** are important if you intend to publish your findings, if you ever speak to law enforcement, if you pursue a case to court or offer your evidence to human rights defenders who represent cases of crime and abuse. Also, should personal or professional problems or changing socio-political conditions interrupt your work, it will be easier for someone else to interpret it and take on the rest of the investigation or use the evidence you managed to uncover. These habits are also useful if you end up collaborating with other partners.

While documentation is important, there are also risk factors. Your investigation logs may benefit potential adversaries – for example, someone determined to stop you from uncovering their wrongdoing – if the information falls into the wrong hands. Documentation can also put your sources at risk if it is not properly safeguarded.

It is crucial that you assess any potential risks at the start of and during your investigation. You need to take your safety and that of your sources seriously, as well as keep evidence and documentation safely, using encrypted storage and devices to protect it from unwanted access.

Security in-a-box is a Tactical Tech toolkit that covers essential digital safety principles, best practices and tools:

securityinbox.org

Make sure you always inform yourself about basic digital and physical security safeguards and learn about tools and skills you may need in order to stay safe and keep your data stored securely. We will address such issues through The Kit but you can also start checking available online resources such as Tactical Tech's *Security-in-a-Box* (securityinbox.org) or the tips from *Security Checklist* (securitychecklist.st). When working in particularly complex situations or environments, ask trustworthy people to advise you or look for safety trainings you may be able to attend if you feel that any of the investigations you pursue may pose even the slightest risk.

If it's not verified, it's not valid.

Verification is crucial not only in the media but for every one of us as the quality and trustworthiness of information available today is being challenged from multiple directions – from “fake news” creators and misinformation trolls to ill-informed social media users who spread news without checking sources first.

Whatever the goals of your investigation, it's important to be able to defend how you got to the information you are presenting as evidence. If something in your investigation is proven not to be true, it undermines your research and any narrative or conclusion you present.

Most of the investigation techniques in this kit can be used to uncover evidence as well as to verify it.

There are different levels of evidence during an investigation. Whatever path you follow, you're always trying to get closer to the first-hand evidence through techniques like verification. Here are some examples of sources of information you may need to address and verify throughout your investigations, listed from the less credible to the most credible ones :

Word of mouth. A neighbour heard that members of a minority group in your community are being denied service at a local authority. This sounds more like a rumour for now, so you will need to get closer to the facts.

Expert statements. A researcher who has tracked this sort of denial of service to minority groups tells you it's frequent. An expert statement is a good way to start validating the information, but you still need to collect some first-hand information or find more sources saying the same.

Second-hand accounts. You speak to people being denied this service. You are getting closer to the actual facts, but any personal experience and statement needs to be checked with other witnesses or existing documentation, if available.

Research documents or reports. A report from a credible NGO describes this occurrence based on interviews with directly involved community members. Documents from such research bring you a step closer but just as with the expert statements, you still need to corroborate them with witness accounts or at least another source stating the same.

Official documents. An official report documents the denial-of-service incident. Signed and dated official papers are very strong pieces of evidence as you can identify the institution and people responsible for documenting the case and follow-up with them if you have questions. Mind institutional bias, when an office may want to hide data rather than expose the truth, especially if it incriminates them. You have a good piece of evidence in your hands now but some witness or expert statements will make it stronger.

Photos, video, audio. A recording exists showing the situation occurring. This can be a treasure of evidence for you. If the images and audio are real, they can be linked to the location, time and people involved in the incident. Watch out for image and sound manipulation by checking EXIF data and metadata, verify the source and the contents and do not use it as evidence without reaching out to those involved to confirm its accuracy.

First-hand evidence. You are present while the situation occurs and maybe you even manage to film the incident. This is first-hand evidence and the strongest for your investigation. You have the opportunity and, at the same time, the responsibility to document the entire incident thoroughly. You also want to make sure you establish contact with others involved to be able to confirm your observations and evidence, should anyone doubt the accuracy of your investigation later on.

When to verify

The short answer is always.

Verification is an iterative process. You have to keep doing it over and over again. The process is not only related to one piece of evidence you uncover, but also to how all the pieces fit together.

Any new evidence you find may cast reasonable doubt on old evidence that you may have already verified. That is why documenting your evidence is important; so that you can retrace your steps and verify again and again.

Challenges of verification

Your assumptions about the credibility of your human sources can get in the way of proper verification if these assumptions are not true. It is essential not to take anything for granted since even the most trusted and reliable of sources can sometimes get it wrong, even if unintentionally.

Another challenge is finding creative ways of verification – to be ready to use sources of information in ways they were not intended. For example, if you want to verify whether a public official was somewhere despite him denying so, you may not only want to visit his social media accounts, but also those of his relatives and friends to find clues of messages, comments and images that may confirm or deny that.

How to verify

There are three main phases of verifying information:

Verifying the source. Where you got the information and where it originated.

Verifying the content. Whether it is exactly what it claims to be.

Verifying its relevance. Whether it fits in to your investigation.

In any investigation, you'll collect information from many different sources. Some will be obvious, while others may be less clear. You could get an anonymous email, an envelope of documents, see a video on social media or find a document on a random website. If there is any question about the origin of that information, it's important to verify where it came from - whether it was from the original source, whether it is from someone trustworthy, whether it is accurate or has been fabricated or tampered with, and whether there was some motive behind getting that information to you.

Information and evidence can take various forms and appear on various mediums. Images, videos, sound, written testimonies and webpages are just a few. For each medium there are tools, techniques and tricks that help with the process of verification, and you will find many of them explained in this kit. You do not need to learn everything about every medium before you start investigating. There will be plenty to discover as you go along, and you will also be able to learn through practice. Complex guides to verification written by experts in the field are also available for you to check if you wish to go in-depth, for example, *the Verification Handbook* (verificationhandbook.com), or the *Journalism, Fake News and Disinformation handbook* by UNESCO (en.unesco.org/fightfakenews.)

In order to rigorously test your evidence and keep your biases in check, you can document your research process and your findings and present them to other investigators to confirm that it makes sense to someone else. However, always make sure you trust those you are sharing information with at any stage of an investigation and that you – and any collaborators – are aware of ways to stay digitally and physically safe as you communicate and share information.



Take care of your emotions

Over the course of an investigation you will have to deal with your personal feelings, principles and values in addition to establishing your methodology, collecting and verifying information, building evidence, and so on. You will need to identify possible biases and also be careful not to undertake more than you can handle emotionally. These concerns are valid when working with any type of methods and resources, online and in the field, or with human sources and interviewees.

Personal emotions

Mental health issues like extreme stress, depression and trauma commonly affect investigators dealing with difficult topics.

Cumulative stress and the responsibility that you have for your subjects, your colleagues, family, and yourself shouldn't be underestimated. It is okay to feel low and frustrated, and to seek the counsel of more experienced investigators.

Speak up, and find effective therapy options if you feel that your investigation is taking a toll on you. Experiencing or hearing about trauma or investigating corruption or injustice, for instance, may put a lot of pressure on you. Often, investigators feel that people need them to keep investigating because they may need help right away. This can produce a sense of responsibility and may even convince some that taking the time to step back and deal with their reactions is a luxury they simply can't afford. Investigators, activists, human rights defenders, and many others who deal directly with issues affecting people around them may often feel this way. This is also one of the main factors that drives investigators to continue their work, so it might be something that drives you, too.

Your self-care, just as your safety, should always come first. If your capacities are dwindling due to your state of mind, that will influence your investigation. If at any moment you feel that you can't cope, you have every right to take a break or even let go of something that is harming your well-being. Moreover, even when you aren't feeling this kind of helplessness or stress, it's good to take breaks once in a while and to talk to others about how you feel. Look on the bright side and consider that even when your investigations might not be as successful as you want them to be, you are always trying.

Bias

It's natural to become emotionally involved with a story, particularly as you speak to sources you sympathise with. Our unconscious biases make us more interested in hearing some stories, and less interested in others. You should accept that you cannot remain a completely detached observer. But you should still strive to be mindful of your biases and seek to act in a fair and honest way as much as possible. Your investigation may fail if you push a certain point of view at the expense of others, or neglect important context due to your personal bias. This can also damage your reputation and trustworthiness.

Start where you are

There is no point in starting your first investigation by experimenting with a completely new or uncomfortable way of gathering information. Just start with what you are good at.

With the availability of digital devices and numerous sources of information on the internet, it is possible to conduct various tasks of an investigation from behind a desk. Digital investigations often mainly involve desk research, but they can also include basic offline research, such as going to the library and archives, making phone calls or a combination of all these.

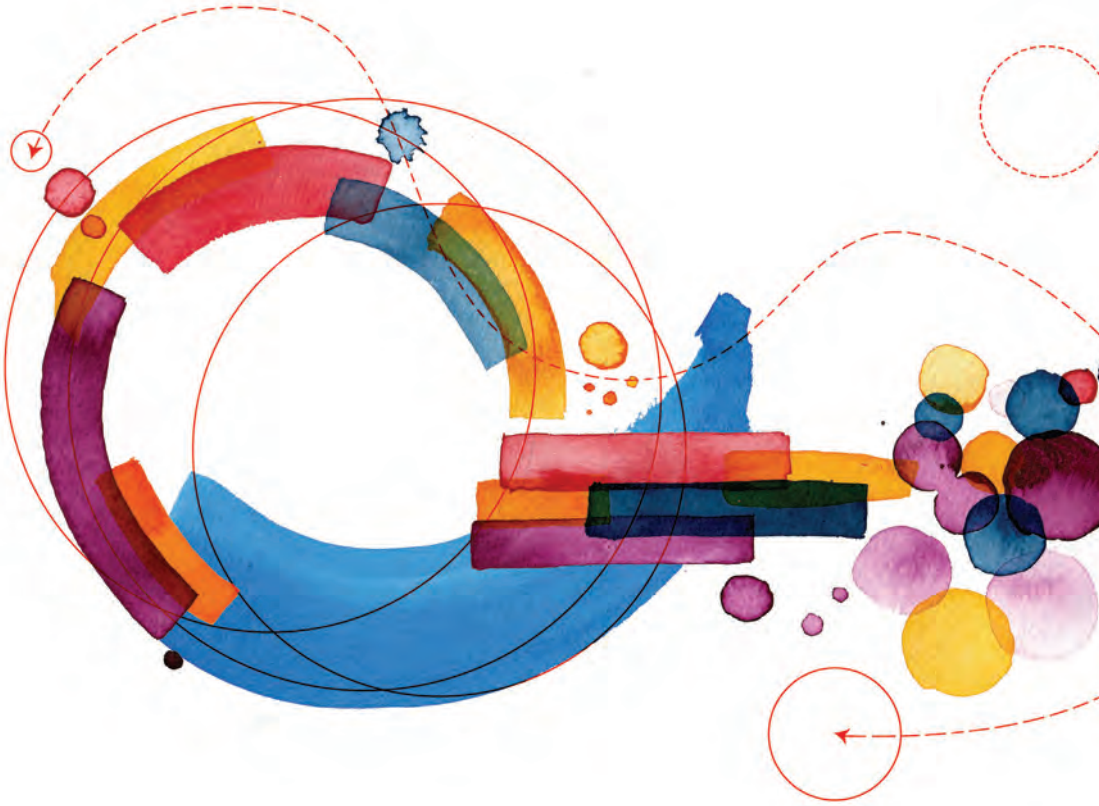
For other investigations, pen and paper is a more appropriate approach. A combination of traditional and new investigation techniques can be very effective.

Some cases will require you to conduct your own field work to gather evidence and verify it. Field research means that you identify and collect the information first hand and it is your responsibility to document it and confirm its accuracy. It can consist of recording testimonies, gathering samples, observing events and places.

Whether you are conducting digital or field research, there are important safety measures you need to be aware of in order to reduce the risks.

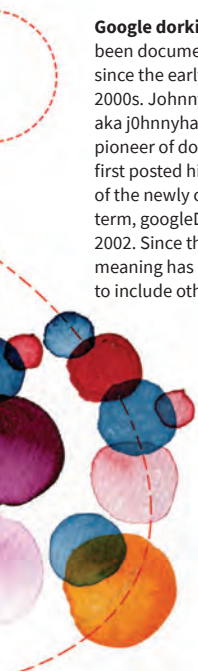
Knowing when to reconsider, ask for help, or set a project aside for a while if possible, is also a healthy attitude and asset to have as an investigator.

SEARCH SMARTER BY DORKING



Support your investigation with advanced internet searches by “dorking” across different search engines.

When investigating, you need to gather as much information as possible about a topic. Advanced search techniques can help to uncover files or leads that are relevant to the questions you are trying to answer. For example you may be able to find a company's tax returns or a local government's expenditure reports – information that may not appear on their websites or show up when you do a regular web search.



Google dorking has been documented since the early 2000s. Johnny Long, aka j0hnnyhax, was a pioneer of dorking. He first posted his definition of the newly coined term, googleDork, in 2002. Since then, its meaning has evolved to include other usages.

Google dorking (also known as Google hacking) is a technique used by newsrooms, researchers, investigative reporters and others to query search engines in order to find hidden information that might be available on public websites. The technique can strengthen your investigations by expanding your access to information that is of public interest but that is not, whether by design or by accident, readily available. Google dorking is also used by security auditors to identify evidence of digital security vulnerabilities and flaws in online services and publication platforms.

This technique can be used on most search engines, not just Google's, so we typically refer to it simply as "dorking."

Dorking involves using search engines to their full potential to unearth results that are not visible with a regular search. It allows you to refine your searches and dive deeper, and with greater precision, into webpages and documents that are available online. Uncovering hidden files and security flaws by dorking does not require a great deal of technical knowledge. It's really about learning just a few search techniques and using them across a number of search engines.

All you need in order to carry out dorking is a computer, an internet connection and a basic understanding of the appropriate search syntax: keywords and symbols – sometimes called "operators" or "filters" – that you can use to refine your search results. To do so effectively, however, you may also need persistence, creativity, patience and luck.

With great information access comes great ethical responsibility. While you can use these techniques in a responsible manner to extend your investigations, others can use them to obtain personal data or exploit vulnerabilities. As is often the case, intentions matter.

Dork it yourself

In everyday use, search engines like Google, Bing, DuckDuckGo and Yahoo accept a search term (a word), or a string of search terms, and return matching results. But most search engines are programmed to accept more advanced “filters” or “prefix operators” as well. A filter is a keyword or phrase that has particular meaning for the search engine. This includes terms like:

inurl:

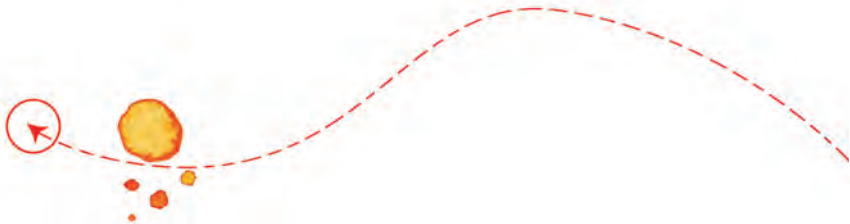
intext:

site:

feed:

language:

On the next page is a list of the relevant dorks - as in search operators - we identified and tested as of March 2019 for Google, DuckDuckGo, Yahoo and Bing. This list might not be exhaustive, but the operators should help you get started.



Dork	Description	Google	DuckDuckGo	Yahoo	Bing
cache:[url]	Shows the version of the web page from the search engine's cache.	✓			
related:[url]	Finds web pages that are similar to the specified web page.	✓			
info:[url]	Presents some information that Google has about a web page, including similar pages, the cached version of the page, and sites linking to the page.	✓			
site:[url]	Finds pages only within a particular domain and all its subdomains.	✓	✓	✓	✓
intitle:[text] or allintitle:[text]	Finds pages that include a specific keyword as part of the indexed title tag. You must include a space between the colon and the query for the operator to work in Bing.	✓	✓	✓	✓
allinurl:[text]	Finds pages that include a specific keyword as part of their indexed URLs.		✓		
meta:[text]	Finds pages that contain the specific keyword in the meta tags.				✓
filetype:[file extension]	Searches for specific file types.	✓	✓	✓	✓
intext:[text], allintext:[text], inbody:[text]	Searches text of page. For Bing and Yahoo the query is inbody:[text]. For DuckDuckGo the query is intext:[text]. For Google either intext:[text] or allintext:[text] can be used.	✓	✓	✓	✓
inanchor:[text]	Search link anchor text	✓			
location:[iso code] or loc:[iso code], region:[region code]	Search for specific region. For Bing use location:[iso code] or loc:[iso code] and for DuckDuckGo use region:[iso code]. An iso location code is a short code for a country for example, Egypt is eg and USA is us. https://en.wikipedia.org/wiki/ISO_3166-1		✓		✓
contains:[text]	Identifies sites that contain links to filetypes specified (i.e. contains:pdf)				✓
altloc:[iso code]	Searches for location in addition to one specified by language of site (i.e. pt-us or en-us)				✓
feed:[feed type, i.e. rss]	Find RSS feed related to search term		✓	✓	✓
hasfeed:[url]	Finds webpages that contain both the term or terms for which you are querying and one or more RSS or Atom feeds.		✓		✓
ip:[ip address]	Find sites hosted by a specific ip address			✓	✓
language:[language code]	Returns websites that match the search term in a specified language		✓	✓	
book:[title]	Searches for book titles related to keywords	✓			
maps:[location]	Searches for maps related to keywords	✓			
linkfromdomain:[url]	Shows websites whose links are mentioned in the specified url (with errors)				✓

Defensive dorking

You can use dorking to protect your own data and to defend websites you are responsible for. We call this “defensive dorking,” and it typically takes one of two forms:

Checking for security vulnerabilities in an online service, such as a website or an FTP server, that you administer; or

Looking for sensitive information about yourself - or about someone else, with their permission - that might be exposed unintentionally on a website, regardless of whether or not you administer that website.

For the first instance, *The Google Hacking Database (GHDB)* (exploit-db.com/google-hacking-database) suggests various keywords and other terms that you can use - along with the “site:yoursite.org” filter in order to identify certain vulnerabilities. While these searches may help attackers locate vulnerable services, they also help administrators protect their own.

For the second instance, we recommend starting with the following simple commands, along with the “site:yoursite.org” filter. You can then remove the “site:” filter to discover which other websites might be exposing information about you or your organisation. Below are a few examples.

You can search for your name in PDF documents with:

<your name> filetype:pdf

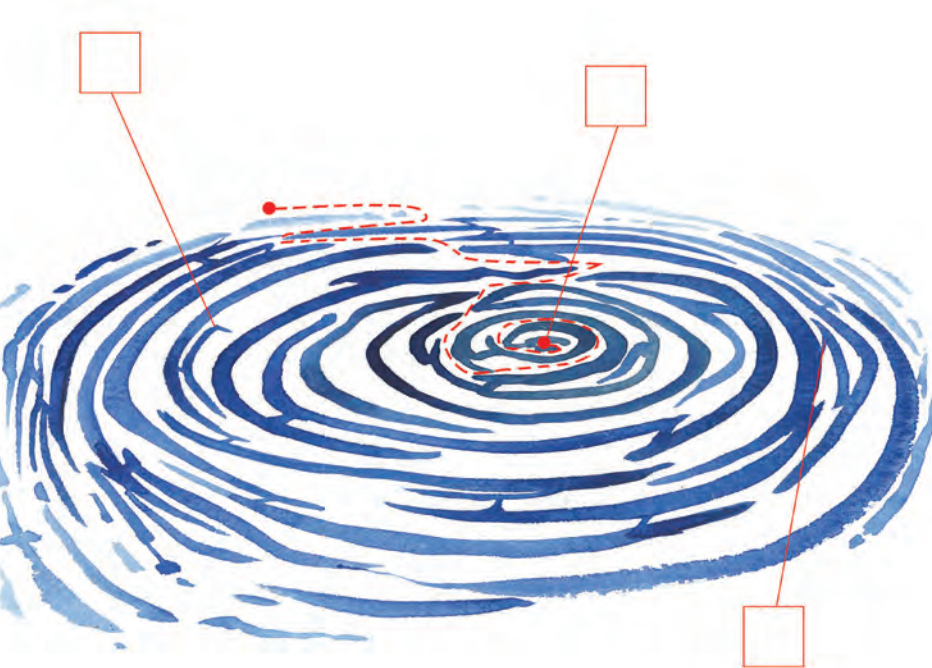
You can repeat this search with other potentially relevant filetypes, such as xls, xlsx, doc, docx, ods or odt. You can even look for several different file types in one search:

<your name> filetype:pdf OR filetype:xlsx OR filetype:docx

Or you can search for your name in regular website content with something like the following:

<your name> intext:“<personal information like a phone number or address>”

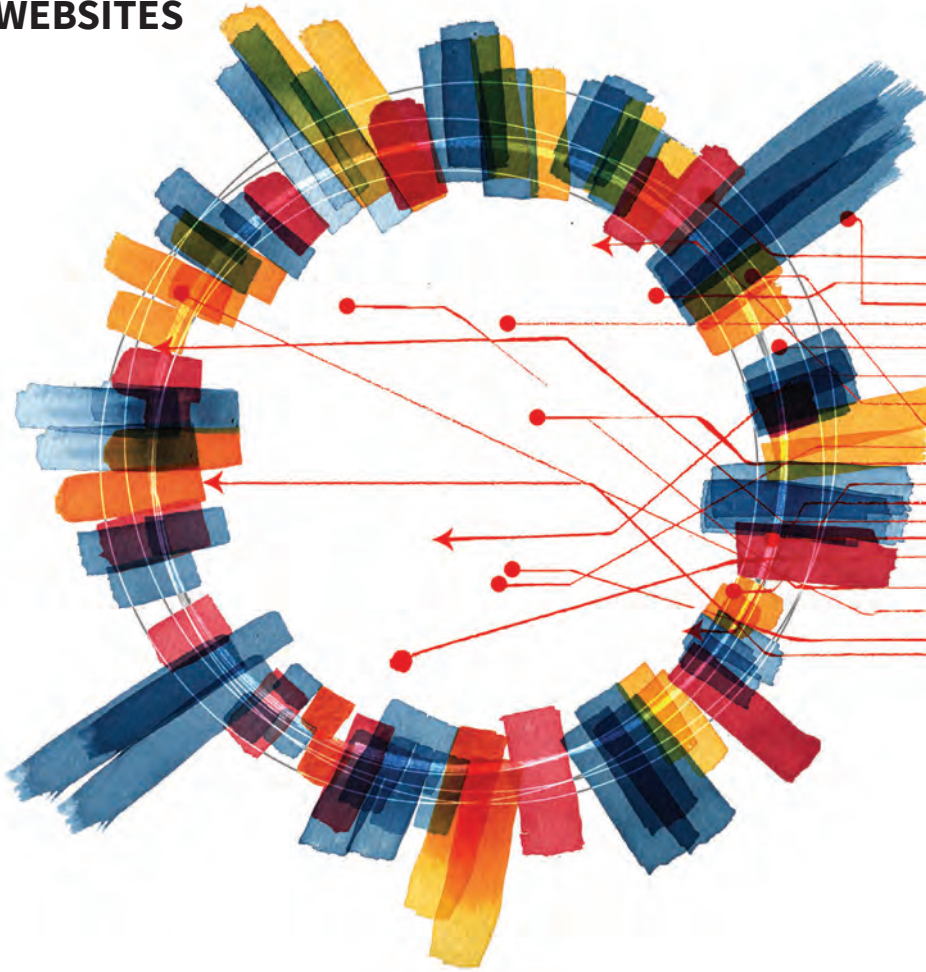
See the table for information about whether your search engine of choice uses intext: or inbody: as the text-searching filter.



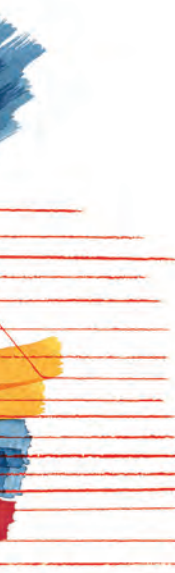
Visit the Kit for the complete guide “Search Smarter by Dorking” by Gabi Sobliye:

kit.exposingtheinvisible.org/how/google-dorking.html

RETRIEVING AND ARCHIVING INFORMATION FROM WEBSITES



You can find and retrieve historical and ‘lost’ information from websites to serve as evidence that something existed online, as well as archive and preserve your own copies of webpages for future reference.



Sometimes, when you want to verify online information, you'll end up following a trail that leads to broken links or to websites that are no longer available. Other times, when you revisit a website, you may find that a specific webpage you remember has been removed or that information you need is no longer accessible and has been replaced with new content.

What if there were some way to travel back in time and get a copy of that webpage, or even a portion of it, before it was altered or taken down?

Luckily, there are some easy techniques and digital archiving tools and services to help retrieve old content and deleted pages so you can still reference them in your investigation. Apart from this, **digital archives** often contain information that can help you identify other important data such as the owner of a website, useful names, contact details, documents and links to other sites.

Some of these tools allow you to contribute to the list of websites they archive by manually saving and preserving webpages at times of your choice. You and others can then retrieve snapshots of those websites later on.

Archiving and retrieving content with the Wayback Machine

The Wayback Machine (archive.org/web) is a project of *Internet Archive* (archive.org), a digital library dedicated to preserving billions of websites since 1996, as part of an effort to archive the internet and provide universal access to all knowledge. The Wayback Machine is an essential tool for researchers, historians, investigators and scholars. It is freely available to the public and can help you access archived snapshots of webpages taken at various points in time.

The Wayback Machine uses automated **crawlers** (also called 'spiders') to access and archive virtually any public website. These crawlers don't have a fixed pattern of deciding which websites they visit and how often they do so. As a result, you may not always find an archived version from a specific day, month or even year. Nevertheless, the Wayback Machine's vast trove of data will likely be indispensable in many of your investigations.

Apart from offering a simple interface for retrieving automatically archived websites, the Wayback Machine also allows you to manually store snapshots of webpages so you can make sure they do not suddenly disappear from the internet.

While it is often a good idea to save HTML or PDF copies of important webpages to your own devices to make sure that you have multiple back-ups, archiving them with the Wayback Machine can add an element of neutrality and trust if you end up sharing those archives with others. It is also far more convenient, for most people, than maintaining an offline library of digital files.

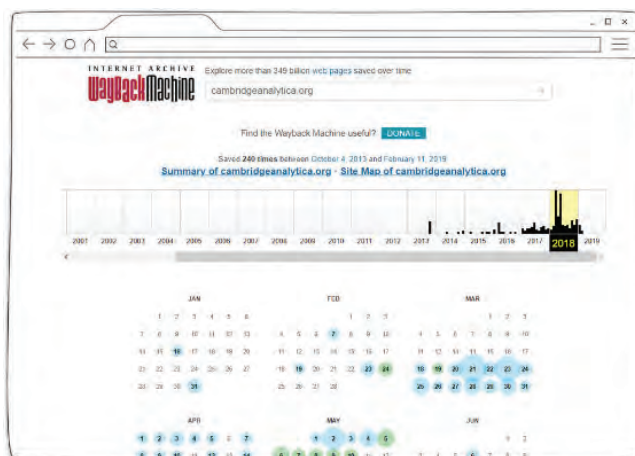
Looking up pages with the Wayback Machine

In order to find a page that is no longer accessible, or to view an older version of a webpage, simply go to web.archive.org and enter the web address that you are searching for.

If the page was previously archived, the dates when it was saved will appear on a calendar of the current year. You can navigate to previous years using the timeline, which also displays a graph of how often the page was archived each year. After clicking on the year you are interested in, archives from that year will be marked on the calendar with colour-coded dots.

Try searching for cambridgeanalytica.org, a website that was taken down in 2018 due to the closure of the company.

Screenshot of the Wayback Machine calendar to access Cambridge Analytica's website



A blue dot indicates that a full webpage capture took place on that date. These are usually the archives you are looking for. A green dot indicates that, when the crawler accessed that web address, it was automatically redirected to another page on the same website. These archives might not contain the content you are searching for. Orange and red dots indicate that an error occurred during the archiving process, so you will not find much information there.

After you select an archived version of the page, the Wayback Machine's navigation bar is displayed at the top of the screen. This allows you to browse between different archives of that page by using the timeline or by clicking on the "next" and "previous" buttons.

Using the Wayback Machine to archive webpages

Another key feature of the Wayback Machine is its ability to archive webpages on demand. Whether you are looking to save and preserve information for an investigation or ensure the accessibility of your own published work, you can navigate to archive.org/web and find the "Save Page Now" form toward the lower, right-hand corner of the page. Simply enter a web address (say "www.yoursite.com/projects") and click the "SAVE PAGE" button.

Unless the website you enter has denied access to the Internet Archive's crawlers, the Wayback Machine will begin archiving it. You will see a progress bar that will let you know when the page has been saved. At that point, you will be able to view the page's archive, and a timeline will display any previous captures from that site.

The SAVE NOW steps will only archive the page you submitted ("www.yoursite.com/projects", in this case) not all of the content on that website. If you want to archive an entire website using this method, you will need to submit each page separately. Furthermore, this feature does not guarantee that regular archives of the page will be captured in the future, so you might want to revisit the Wayback Machine from time to time to request additional snapshots.

Limitations of the Wayback Machine

The Wayback Machine has other limitations as well. Examples include:

Password-protected websites are not archived.

Dynamic websites that rely heavily on JavaScript may not be archived properly.

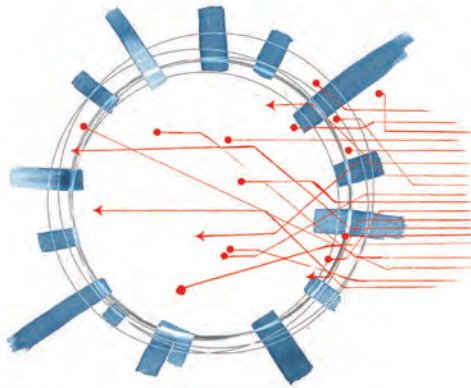
Website administrators can explicitly request that their sites not be archived, either by publishing a restrictive robots.txt file, or by sending a direct request to the Internet Archive.

Website administrators can request that previously archived content be removed from the Wayback Machine.

There is currently no full-text search available on the Internet Archive.

Robots.txt - a file on a website that instructs automated programs (bots/robots/crawlers) how to behave with data on the website.

In the European Union and a few other regions, *The Right To Be Forgotten* legislation provides individuals with the option to request that search engines and digital archives remove indexed content related to them, which they deem harmful or libelous. This right has limitations so not everything can or will be removed upon request but it is worth keeping in mind that some subjects of your investigation (politicians, criminals and other controversial figures) could be using the opportunity to take down internet content related to them that is relevant to your investigation.



Other ways to retrieve and archive webpages

Archive.today

Archive.today (archive.fo; formerly archive.is) archives web pages much like the Wayback Machine. It differs, however, by only storing individual pages, rather than entire websites, and it does so only at the request of its users, not automatically.

Since it doesn't crawl sites, it doesn't have the breadth of information you can find on the Wayback Machine. It does provide three key features, however:

First, unlike the Wayback Machine, it allows you to search the full text of its archives.

Second, it ignores any restrictions that might be specified in the robots.txt files of the websites that it archives. As a result, it can save snapshots of some pages that the Wayback Machine cannot, such as public Facebook profiles and Twitter posts.

Third, it also saves both a text copy and a graphical screenshot of the archived pages. This sometimes provides greater accuracy than saving the page itself, especially when archiving content that changes rapidly (such as rolling images or snapshots of forum messages, etc.).

Like the Wayback Machine, archive.today provides you with direct links to the archived content using web addresses with embedded date stamps.

When you archive a webpage with a service like the Wayback Machine or archive.today - especially if it has a long, complicated web address like an archived copy of a Google Cache entry - be sure to record that archived link somewhere in a file on your computer, in a secure cloud folder or elsewhere. Relying on your browser history to find such things is a recipe for disaster.

Visual site monitors

Another option to retrieve website contents and to stay updated if any changes occur is to use visual site monitors. These are services that can track and monitor visual changes in webpages, whether they happen in code, images, text etc. They can be very useful for researchers and help automate some of the work if you need to monitor many websites that are useful in your investigation.

Visual site monitors archive webpages in a different way than the tools and services we explored above. You give the service a particular section of a webpage to watch, and it takes a snapshot, then monitors the page for visible changes. If there are any changes, big or small, the site monitor will send you an email to let you know.

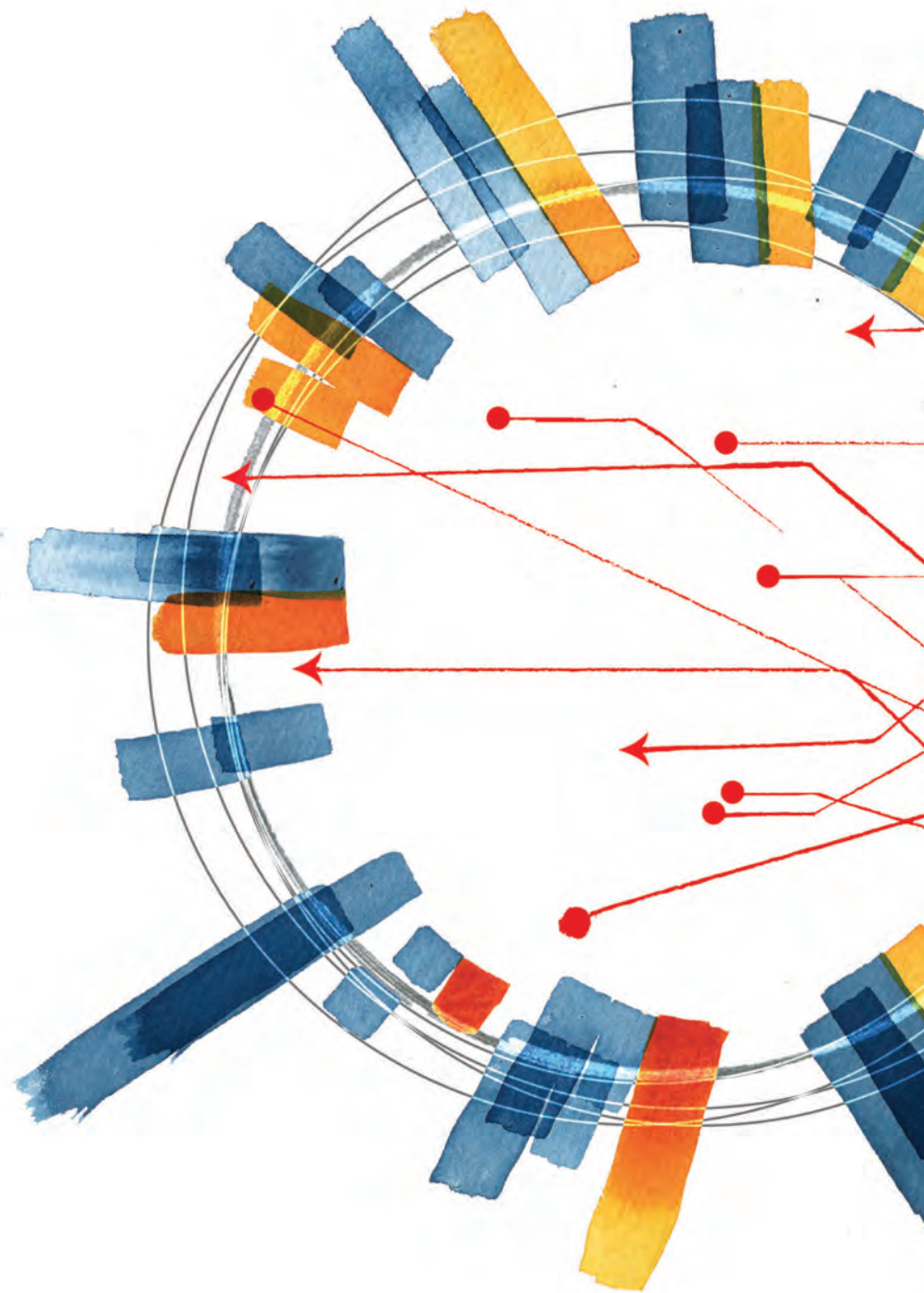
Useful visual site monitors we can recommend are:

Visual Ping (visualping.io) - offers a free plan that allows you to monitor up to 62 webpages a month. The free version can run checks hourly, daily, weekly or monthly to compare a webpage with its previous versions and alert you by email when modifications in text, images, keywords or any selected page areas take place. It also works via the Tor Browser and we recommend using this option for an extra layer of privacy and security.

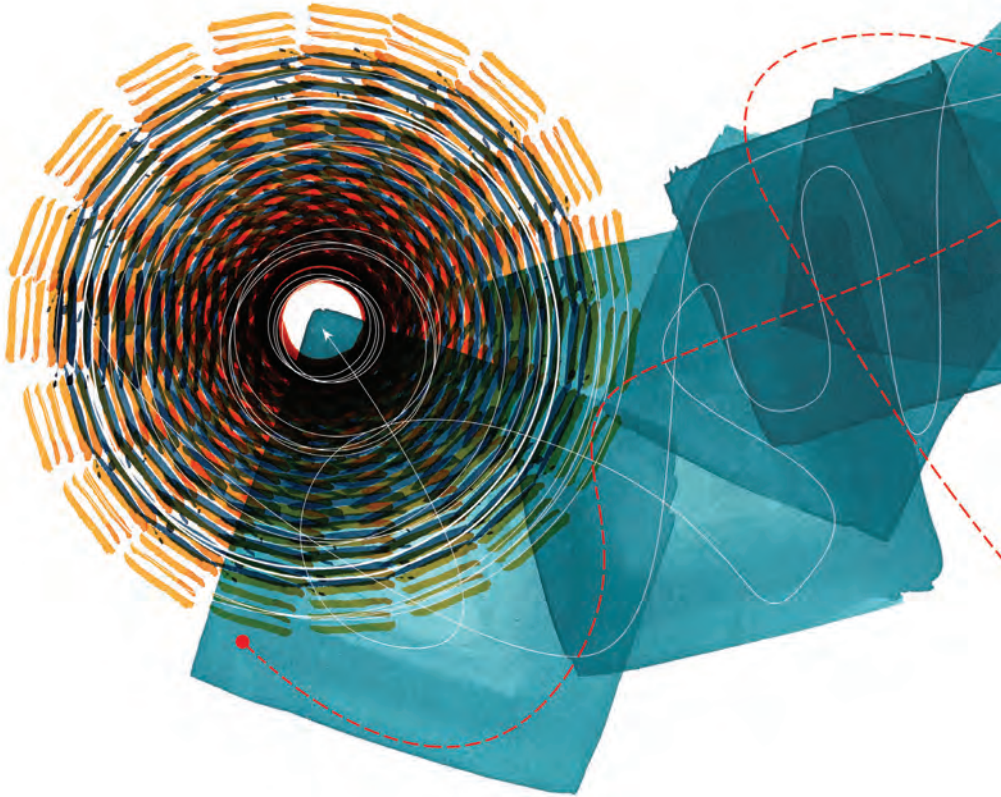
Change Tower (changetower.com) - offers a free plan that monitors up to three websites and conducts up to six checks per day. It can monitor a specific URL (webpage), an entire website or different variations. It can search for changes in content (text), visual content, html, keywords etc. The free plan stores your monitoring results for up to a month. It also works via the Tor Browser.

Visit the Kit for the complete guide “Retrieving and Archiving Information from Websites” by Wael Eskandar and Brad Murray:

kit.exposingtheinvisible.org/how/web-archive.html



HOW TO SEE WHAT'S BEHIND A WEBSITE



Tools and techniques you can use to investigate the ownership of websites and uncover hidden information online.

On the surface, websites look like they're designed to make information available to the public. However, there is plenty of valuable information hiding behind what you are able to see in your web browser.

Sometimes it is important to research hidden data: to identify the individuals or companies that own a domain name or maintain a website, to determine where that site was registered or to dig up content that it once contained but that has since been removed. Doing so is not always straightforward. For example, people who do not want to be associated with a website's content, or with the affiliated business, sometimes try to hide their connection to the site by using intermediaries when they register its domain name.

Finding hidden content and connections is not an exact science but it requires a combination of acquired skills, a set of methods and tools and a good dose of perseverance.

A website and its elements

To investigate a website effectively, you will need to know what goes into one: from elements that are immediately visible to visitors to others that exist beneath the surface.

Websites and webpages

A website is made up of webpages that display information, which anyone with internet access and a web browser can see. That information might include the profile of a company, a description of a product, a collection of photographs, or just about anything else. From another perspective, however, a webpage is really just a digital file that is stored on a disk that is attached to a computer that is plugged into power and connected to a network cable somewhere in the physical world. It helps to keep this in mind when investigating a website.

IP address

To visit a website, your device needs to know the Internet Protocol address, or IP address, of the computer that hosts it. Hosting a website means making it available to the world; the computers responsible for doing so are often called servers.

An IP address is typically written as a series of four numbers, separated by periods, each of which ranges from 0 to 255. For example: 172.217.16.174 is the IP address of one of the servers that hosts the “google.com” website, at which visitors can access Google’s search engine.

At any given time, each device that is directly connected to the internet - be it a webserver, an email service or a home WiFi router - is identified by a particular IP address. This allows other devices to find it, to request access to whatever it is hosting and, in some cases, to send it content like search terms, passwords or email messages.

Domain name

Like most long numbers, IP addresses are difficult to remember, so we tend to use domain names instead. Each domain name points to one or more IP addresses. In the example above, the domain name “google.com” points to 172.217.16.174 and is far easier for most people to remember.

Domain registration, registrar and registrant

Domain names are unique. There can only be one “google.com,” for example. The process of purchasing a domain name is called domain registration. When someone registers a domain name, a record is created to keep track of that domain’s official owner and administrator, or their representatives.

A person who registers a domain is called a domain registrant. That registrant - or someone to whom they give access - can then point their domain to a particular IP address. If a webserver is listening at that IP address, a website is born.

The companies that handle the registration process are called domain registrars, and they almost always charge a fee for their services. These companies are required to keep track of certain information about each of their registrants.

A non-profit organisation called the Internet Corporation for Assigned Names and Numbers (ICANN, icann.org) governs the domain registration process for every website in the world.

Web host

We know that a website has a domain name and that a domain name is translated into an IP address. We also know that every website is actually stored on a computer somewhere in the physical world. The computer that hosts the website is called a web host.

There is an entire industry of companies that store and serve websites. They are called web hosting companies, they have buildings filled with computers that store websites, and they can be located anywhere in the world. While it is most common for websites to be hosted in “data centres” like these, they can actually be hosted from almost any device with an internet connection.

Basic WHOIS look-up

When researching a website, one of the most useful sources of data can be found in its domain registration details.

Over the course of your investigation, it might be relevant to know who registered or who owns a particular domain (whether it is an organisation or an individual registrant), when it was registered and by which registrar, as well as other details. In many cases, this information can be accessed through third-party services that are detailed below.

Sometimes the owner of a domain would not want to appear as linked to the site (whether to conceal something or simply to protect privacy), so it's worth noting that domains can be registered through proxy or intermediary organisations that conceal the full details of the registration.

The information collected from domain registrants is called WHOIS data, and it includes contact details for the technical staff assigned to manage the site, as well as contact details of the actual site owner or their proxy.

There are many services that provide useful WHOIS data for free or for a fee. Here are a few we recommend:

who.is

whois.com/whois

godaddy.com/whois

whois.domaintools.com

iana.org/whois

As different search engines return different results for the same query depending on their indexes and algorithms, it may be that searching with different WHOIS query services returns varying amounts of detail about your domain of interest. Checking with multiple sources whenever possible is therefore a good way to make sure you collect as much information as possible, as is standard in any part of an investigation.

GDPR implications for access to WHOIS data

The European Union's (EU) *General Data Protection Regulation (GDPR)* was adopted in 2018 across the EU to safeguard the privacy of citizens' personal data. This affects the status of public WHOIS registries in the EU because in theory, WHOIS data of owners and administrators of EU-registered domains should not be collected and published by registrars. Under the GDPR, this is considered to be private information. There is still a large grey area around applications of GDPR by EU domain registrars, including some ongoing court cases, but as of 2019 some still provide data while others restrict it. Paid services such as [domaintools.com](https://www.domaintools.com) still provide useful information that is based on historical records.

Historic WHOIS

Historic data can be a useful tool when investigating websites, because it can track the transfer of a domain's ownership. It can also help identify owners of websites who have not consistently chosen to obscure their registration data by using a WHOIS privacy service.

Several services offer access to historic WHOIS records, though these records may often be restricted to non-EU countries due to the GDPR, as mentioned above.

DomainTools (research.domaintools.com/research/whois-history)

- perhaps the best-known of these companies that offer historic hosting and WHOIS data. However, it is a paid service that requires you to register for a membership in order to access it.

Whoisology ([whoisology.com](https://www.whoisology.com)) - a good alternative to Domain Tools that also provides historical WHOIS data. It requires you to create an account for basic free services, as well as advanced fee-based services.

Reverse WHOIS look-up

When you look up the domain names registered to a certain email address, phone number or name, it is called a “reverse WHOIS look-up.” Several tools and services offer these kinds of searches.

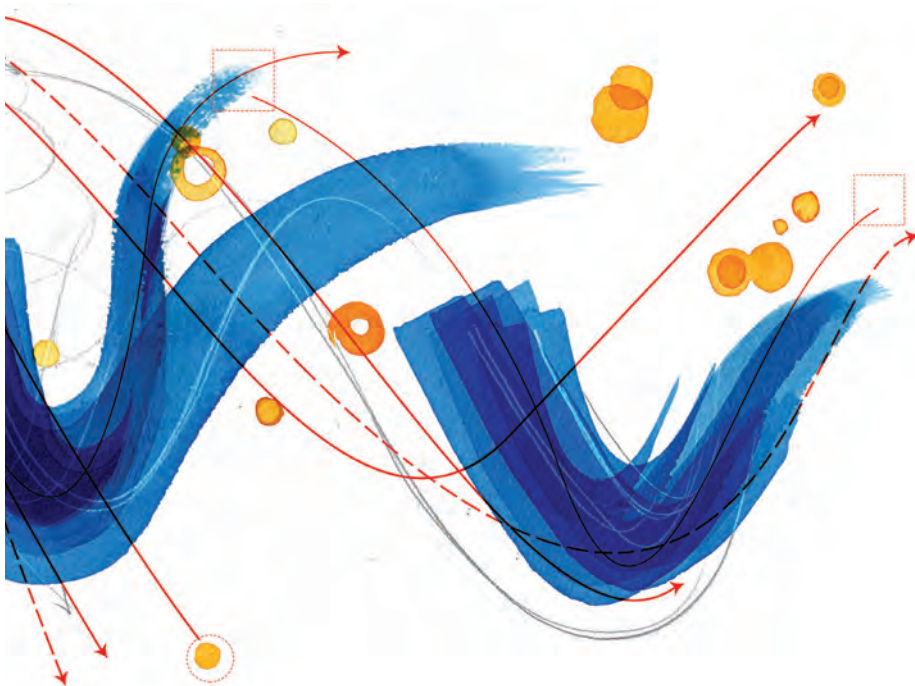
When trying to locate the owner of a domain name, focus on locating information that can help you “reverse search” back to an ultimate owner, such as a phone number, email or location.

Here are some tools you can use for reverse searches:

ViewDNSInfo (viewdns.info/reversewhois) - free and allows searches by email or phone number. It also provides other useful options such as searching by an individual or company, historical IP address search (historical list of IP addresses a given domain name has been hosted on as well as where that IP address is geographically located). Note that IP address owners are sometimes marked as ‘unknown’ so it helps to use several websites for your searches and combine the results for a fuller picture.

Domain Eye (domaineye.com/reverse-whois) - requires creating an account and provides you with 10 free searches per day.

Domain Tools (reversewhois.domaintools.com) - a useful service but it doesn’t provide any free options for reverse WHOIS as of 2019.



Finding information with shared hosting and reverse IP search

Websites are hosted on one or more servers, or computers running server applications that transmit the site's content to visitors.

Because web hosting costs money, related websites will often share hosting. Analysing the other domains sharing the same hosting service can sometimes shine a light on the owner or administrator of the site you are investigating.

You can use the IP address to see which other sites are hosted on the same server, and then further verify whether some of them might be related. Some of the tools you can use to identify shared hosting are:

ViewDNSInfo (viewdns.info/reverseip) - you can search for a domain name or IP address.

Bing IP search (www.bing.com) - add the prefix "IP:" to your IP address query in the Bing search engine and it will reveal websites hosted on the same IP addresses. Try with ip:213.108.108.217.

Netcraft (www.netcraft.com) - displays domain information as well as other information that may be useful in investigating a website such as the web trackers, hosting history and site technology.

Exposing hidden web content

Nearly every site on the internet hides something (and often, many things) from visitors, intentionally or not. For example, the content management systems employed by most sites hide the internal files used to generate posts and maintain the website. Databases that store data for sites and applications are usually hidden from public access.

There are simple tools and techniques that allow you to access such information without raising suspicions. These are just small tricks that let you see what a website is made of and what additional data it might reveal to you about website owners or connections to other sites.

Robots.txt

Websites indicate how scrapers and search engines should interact with their content by using a file called “robots.txt”. This file allows site administrators to request that scrapers, indexers and crawlers limit their activities in certain ways (for instance, some do not want information and files from their websites to be scraped).

Robots.txt files list particular files or subdirectories - or entire websites - that are off-limits to “robots.” As an example, this could be used to prevent the Wayback Machine crawlers from archiving all or part of a website’s content.

Some administrators may add sensitive web addresses to a robots.txt file in an attempt to keep them hidden. This approach can backfire, as the file itself is easy to access, usually by appending “/robots.txt” to the domain name, for instance: `cnn.com/robots.txt`.

Be sure to check the robots.txt file of the websites you investigate, just in case they list files or directories that the sites’ administrators want to hide. If a server is securely configured, the listed web addresses might be blocked. If they are accessible, however, they might contain valuable information.

Sitemap.xml

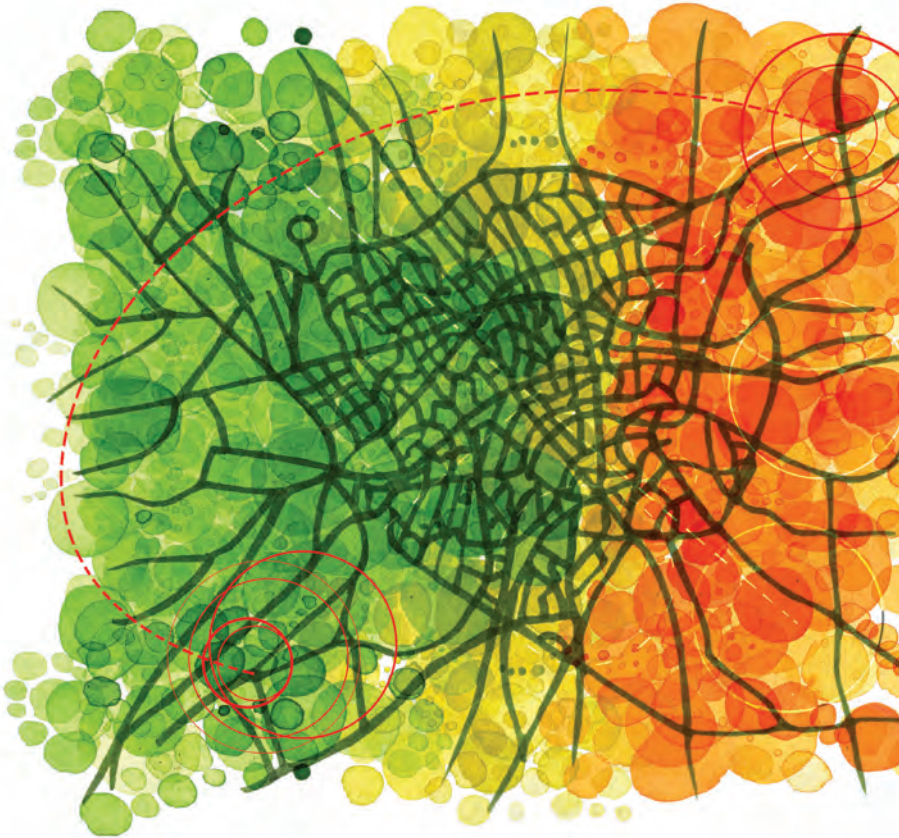
Sitemap files are sort of the opposite of robots.txt files. They are used by site administrators to inform search engines about pages on their site that are available for crawling. Websites often use sitemap files to list all of the parts of the site they want to be indexed, and how often they want search engine indexes to be updated.

To access sitemaps, you need to add “/sitemap.xml” to the domain name. Not all sites will have an accessible sitemap.xml file. The result is sometimes URLs that typically do not show up in searches and you can explore those manually.

Visit the Kit for the complete guide “How to See What’s Behind a Website” by Wael Eskandar and Brad Murray:

kit.exposingtheinvisible.org/how/web.html

USING MAPS TO SEE BEYOND THE OBVIOUS



Explore how to use maps, geographic data and satellite imagery to find and visualise information, and how common mapping tools can help you investigate a physical place and what happens there.



Maps and satellite imagery not only allow you to get an overview of an area but also help you make connections that would otherwise be difficult, if not impossible, to establish from ground level. You can see, for example, how a series of factories are arranged along the same railway or river, notice a pattern of illegal deforestation in a rainforest or assess environmental and infrastructural damage following a disaster.

Adding further information to maps – showing land ownership or the habitat of protected animals, for example – can help you make connections that might be valuable to an investigation. Maps and satellite images can also enable you to see over walls and look at what is happening in places that are difficult to access because they are restricted or unsafe, or far from where you are based.

Maps can be useful for an investigation if the data you use has a geographic or spatial element. Any data that can be referenced to a particular place can be added to a map. This includes natural features, such as rivers, coastlines and elevation; administrative data such as country outlines, county boundaries and city limits; aerial photographs, whether from satellites, drones, balloons or kites; and databases containing location information, such as the addresses of all the hospitals in a region, or a list of countries together with their population size.

Large amounts of such data can be found for free online, often already assembled into maps. An even greater amount of geographic information is available to you if you're able to assemble these different datasets yourself, using accessible data visualisation and geographic information system (GIS) software.

Map - a graphic representation of physical areas or objects and where they are located geographically.

It is also possible to generate your own geographic datasets and imagery, which you can then use to produce maps. You can create your own aerial imagery using drones, balloons or kites, and make or add to an existing map using basic survey techniques with simple tools such as a tape measure, paper and pen.

Geographic information is everywhere

Geodata is digital information that's directly linked to a physical or geographic location. There is plenty of visualised geodata available online and it may be useful when researching certain topics. Weather data, land use data, zoning maps (used for urban planning) and building permits are just some examples. Social media posts and photographs can often be linked to a specific place and time via their location metadata, which can help you verify what happened there and when.

You are probably familiar with a number of common map applications, and have at least one on your phone that you use regularly. Even this basic tool can be helpful in planning and carrying out investigations.

Many such applications have features that allow you to search for photographs of a certain place, or find 360-degree ground-level views. These can be useful when familiarising yourself with a place before you go, finding the address of companies located there, or learning about an event at a certain time. Route planners in map applications can help you plan your trips, and also verify times, means of transportation, route options and costs for specific journeys.

Generally, investigations have at least one geographic component. In most cases, the company you are investigating has physical or registered offices somewhere and probably also operates in a distinct location. The people you are investigating most likely leave physical or digital traces that can be linked back to specific places – images from their trips or social media posts, for example. While places may be more obviously important in some investigations than in others – for instance, deforestation has a clear link to a certain location – creating maps, using geodata and geolocating evidence can often help to verify, or call into question, other sources of information.

Understanding mapping vocabulary

Location coordinates:

The latitude and longitude (also known as lat-long) coordinates system divides the Earth into a grid of horizontal and vertical lines and is used to accurately pinpoint any location. Latitude measures how far a place is north or south of the equator. The equator is 0 degrees latitude, with the north pole at 90 degrees north and the south pole at 90 degrees south. Longitude measures how far a place is east or west of the prime meridian, which is at 0 degrees longitude.

Latitude and longitude coordinates can be written in a number of formats:

Degrees / minutes: 52°31.86797' N, 013°24.03009' W

Degrees / minutes / seconds: 52°31'52.0784" N, 013°24'01.8054" W

Decimal: 52.5311329 lat, -13.4005015 long. North of equator is positive (plus is usually not marked), south negative (marked with a "-"). East of the prime meridian is positive, west is negative.

Main types of maps:

Thematic maps - maps showing information related to a specific subject, such as air pollution, forest cover or election results.

Choropleths - different regions of the map are coloured to show a statistical difference, such as voting percentages or life expectancy.

Symbol maps - symbols or shapes are placed on your map, with different sizes and colours. Symbol maps are useful to illustrate two or more datasets together - for example, the number of earthquakes around the world, together with their intensity.

Heat maps - show variations in intensity, such as how air pollution differs across a city.

Satellite image - images/photographs of the Earth's surface or of other planets' surfaces taken by satellites. These images are often taken in stages and combined to obtain a complete overview of large areas, to create maps, and to observe land and water surface details.

Key features in maps and satellite images

Pattern - on maps, agricultural areas can often be identified by the pattern of farmers' fields, which may be rigidly rectangular, or circular in countries that use rotating booms for irrigation. Natural growth forest has a more irregular pattern of trees than a plantation, which may be laid out in a grid.

Shape - bodies of water, such as lakes and rivers, tend to have distinctive shapes and are often easy to identify on a map. Straight lines in a landscape are likely to be human-made, such as roads, canals and land boundaries.

Texture - refers to how smooth or rough a feature is. Texture can give you clues about what you're looking at, for example a large area of concrete or tarmac, such as a car park, will appear smooth on a map, while vegetation is likely to have a rougher appearance.

Tone and colour - are really important when interpreting images. Satellite images created using visible light (as opposed to infrared light) are fairly intuitive to interpret, as the colours are similar to what you would see with your own eyes. Vegetation tends to be green (though this can change over the course of seasons, it may turn brown/yellow in the fall). Water absorbs light and tends to appear black or dark blue, although sediment in the water will make it look brown; shallow water can be lighter in colour and sunlight reflections can make it seem white or grey. Infrared images are often used to monitor vegetation, which will appear in different shades of red (rather than green, as in visible light images).

Collecting evidence from reference maps and photographs

Reference maps show important physical features such as rivers, hills and coastlines, as well as buildings, roads, paths etc., plus the names of places and streets, and are often useful for way-finding. In many cases, they will contain additional services, such as satellite imagery, street level views of places, detailed route planning and geo-located photographs or videos. Here are some common reference map platforms and apps:

OpenStreetMap (openstreetmap.org) - is a free map platform created through crowdsourcing. This also means that you may need to verify any information you find on it by checking other maps and confirming geodata about the places you need to investigate. It also has a humanitarian layer, which shows details like the location of camps for displaced people, and is used by the humanitarian community for planning and coordinating responses.

OsmAnd (osmand.net) - uses OpenStreetMap's database but is independent from OSM. It provides satellite views from Bing. Its mobile app (for Android and iOS) works completely offline and in addition to route planning and navigation, it also includes foot, hiking and bike paths. It can be particularly useful if you need to map terrains that are off-road.

Open Chart Plotter Navigator ([Open CPN: opencpn.org](http://opencpn.org)) - is free and open source software developed by a team of active sailors with the aim of improving the mapping of waters. It is constantly updated and tested by users and provides navigation and route planning support as well as data about weather conditions and tides, tracking of other vessels, avoidance of possible collisions, and much more.

Google Maps (google.com/maps) - lets you plan routes, look at detailed satellite imagery, track your own route and find photographs linked to a certain place.

Google Earth (google.com/earth) - uses satellite imagery as its background. It offers a number of features that Google Maps doesn't, including historical satellite imagery and 3D models of terrain and buildings.

Bing Maps (bing.com/maps) - is a good alternative to Google Maps. It provides satellite views, bird eye's views and road views, as well as street views (streetside) for some places. It is particularly strong on data about street traffic (use the traffic light icon on top of the map) and distance travel planning.

HERE WeGo (wego.here.com) - free map and navigation platform providing satellite view, terrain view, route planning and traffic updates.

Yandex Maps (yandex.com/maps) - is a Russian web mapping service available worldwide but with limited coverage as compared to Google Maps. It has detailed maps only for Russia, Belarus, Ukraine, Turkey and Kazakhstan but it is worth checking in comparison with other map platforms because it may provide additional details, especially in these regions.

Baidu Maps (map.baidu.com) - is particularly useful when checking locations in China, as it provides far more detailed coverage than Google Maps. It includes satellite imagery, street maps, street view, and route planners for foot, car or public transportation travel.

Mapbox (mapbox.com) - allows you to add your data to a custom designed map tile. It has a free tier that you can use to create many kinds of maps such as symbol maps, heatmaps or choropleth maps.

Using already mapped data and thematic maps

There are many existing datasets that can be visualised using maps. Some information, such as the boundary of a protected ecosystem or the transport routes of cargo ships, can only be properly understood when viewed on a map. Other information, such as a spreadsheet showing infant mortality rates around the world, may be comprehensible in its raw form, but putting it on a map can be a valuable way to analyse patterns it might contain.

Many organisations that compile datasets also offer maps and visualisation tools as part of their data portals. This list is just a starting point to give you an idea of the resources and categories of thematic maps that exist and that may be useful to your investigation:

Shipping traffic

Marine Traffic (marinetraffic.com) - a live map providing near real-time information about vessels' positions, details and voyage-related information, based on automatic identification system (AIS) data.

Global Fishing Watch (globalfishingwatch.org/map) - a map showing the up-to-date positions of approximately 300,000 of the largest commercial fishing vessels, as well as historical data on these ships' whereabouts.

Flight traffic

Flight Radar (flightradar24.com) - a live map showing the positions of commercial aircraft, together with flight numbers and route information. Searching by flight number allows you to track individual planes.

FlightAware (flightaware.com) - a free service allowing you to track the real-time flight status and location of most commercial flights worldwide as well as the whereabouts of charter and private planes in the US and Canada.

Forest cover

Global Forest Watch (globalforestwatch.org/map) - a map of changing tree cover around the world from 2010 to the present.

Air pollution

European Environmental Agency (eea.europa.eu/data-and-maps) - a live map of air quality data across Europe, with options to look at overall air quality, as well as concentrations of particulate matter such as carbon monoxide, ozone, nitrogen dioxide etc.

World's Air Pollution (waqi.info) - a live map of air quality around the world, with links to individual countries' air quality monitoring agencies.

Mining and resources

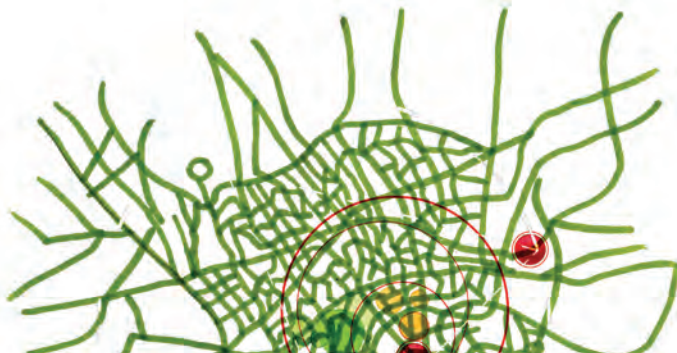
Mineral Resources Data System (mrdata.usgs.gov/mrds) - provides historical data on global mineral resources, including information about mine ownership, all available on a user friendly map. Note that some of the information is outdated.

United Nations data

UN cartographic division (un.org/Depts/Cartographic/english/htmain.htm) - has a collection of maps mostly related to humanitarian and peacekeeping operations.

The United Nations High Commissioner for Refugees - Map portal (maps.unhcr.org) - has a large number of maps available for download related to current refugee situations. It also features a number of maps of areas where large numbers of people have been displaced.

The World Bank (databank.worldbank.org) data portal - has an online visualisation tool, which you can use to view their data as a map.



Do it yourself: Mapping a small area, the low-tech way

Carrying out a detailed survey of a place can be useful for some investigations. It can help you create an accurate record of earthquake damage to one or more buildings, for example, or document the location of bullet holes following a shooting. This approach is low-tech, but that doesn't mean it should be regarded as an inferior or amateur technique: many professionals, including architects and engineers, use it to gain the most accurate measurements.

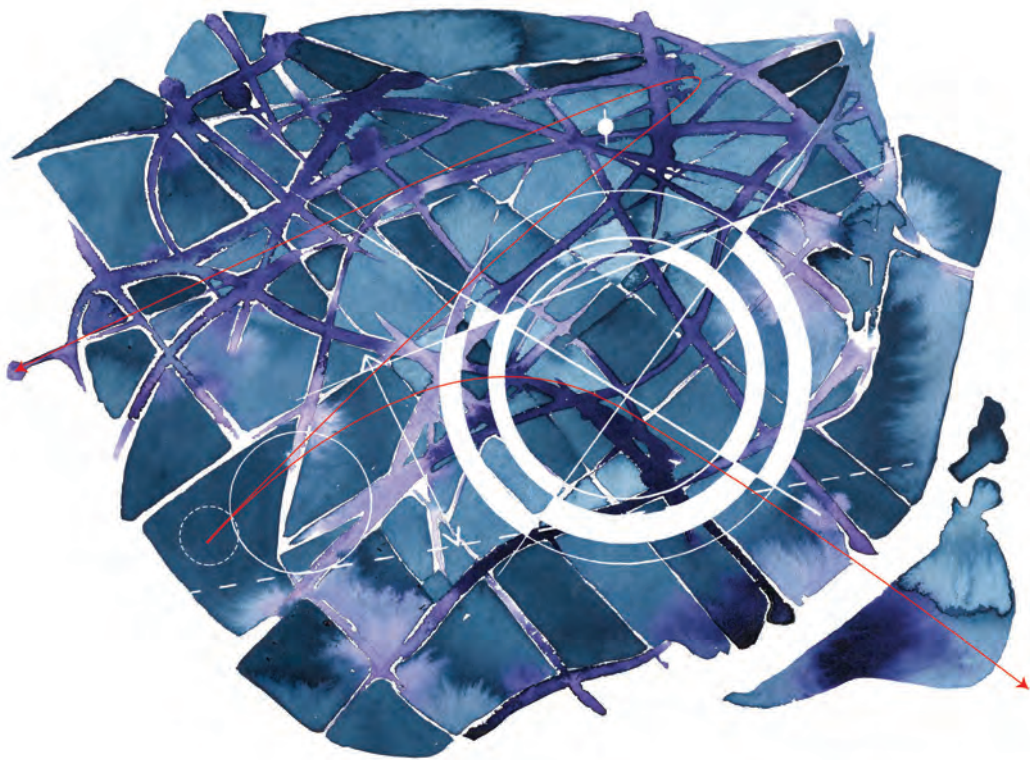
What you need: pen and paper, measuring tape.

To practice, do a survey of a nearby place that you have easy, legal access to. The garden or courtyard of your home or office could work.

Sketch out the area in “plan” (in 2D - viewed as flat, from above). Using your tape measure, take measurements of the elements you have drawn on your plan – for instance, the lengths of walls and staircases, and the distances between them. Remember to measure diagonals in the space, so that you can draw it more accurately later – this will help you ascertain whether a courtyard that looks like a rectangle really does have parallel sides, for example.

Take note of the orientation by marking which way is north. You may be able to look at an existing, less detailed map to work this out. Looking at the position of the sun and time of day can also be a good guide. Or, of course, you could use a compass.

It is also helpful to take photographs of the area you are surveying. These will be useful when it comes to drawing up your survey measurements, as they give a wider sense of what the place is like. To get a full overview, take panoramic shots, ideally from different places on and around the site. To build a bigger picture of the place, try to take photographs that contain as much context as possible – surrounding streets, adjacent buildings, etc. Close-up photographs of key features, such as damage to a window or graffiti on one of the walls, are also useful.



Visit the Kit for the complete guide “Using Maps to See Beyond the Obvious”, by Alison Killing:

kit.exposingtheinvisible.org/how/maps.html.

AWAY FROM YOUR SCREEN, OUT IN THE FIELD



See what it takes to plan, run and evaluate your field investigations safely and effectively.



Field research or field investigation is any kind of information collection and verification process for which you have to leave your house or place of work. This means that going out to talk to a witness, observe a protest, collect environmental samples (such as water, mud or plants) or take photos to support an investigation are part of your field research.

Field research is remarkably effective, since it often yields physical evidence such as film, video or sound recordings, which can make even the most controversial and complex issues easier to understand. This is usually accompanied by other investigative techniques and research strategies. In fact, investigators often exhaust their desktop research before considering going into the field.

While digital or remote research can be carried out relatively quickly, field research requires planning, arranging transportation (anything from a walk to several expensive flights), and doing the investigation itself before returning home to analyse the results. Field investigations can take half a day, weeks or even months to carry out.

Why you need field research

You can conduct field research for various purposes, including to:

Corroborate digital material (such as information on satellite images)

Collect environmental samples (water, soil or air)

Obtain, review or copy documents that are not available remotely

Meet and interview sources and witnesses in their own environment, such as their home or workplace

Identify new sources that might provide information of interest

Expand your understanding of evidence you have already gathered

Corroborate or refute an initial hypothesis, narrative or other existing evidence

Confirm information on products, such as bar codes or names of manufacturers, if you are doing supply chain research or investigating companies (see our Supply Chain section in the Kit)

Gather photographic, video or audio recordings to capture details for documentaries or articles.

Each field investigation will likely require different kinds of preparation, even within the same project. For instance, the way you prepare for and execute a seemingly simple activity such as taking photos of a building to verify a witness' statement can vary depending on the type of building – whether it's a private residence or a government building, the headquarters of a company or an airport. In addition, the country, the city and even the neighbourhood where these buildings are located can make a huge difference to your access, your safety and the quality of your results.

Skills you need

As with all investigative methods, it takes time and practice to obtain good field research skills. Curiosity, adaptability, patience and a good dose of caution are valuable traits that can be of great help in the field. Other attributes you need to develop are:

The ability to adapt to rapidly changing circumstances and to predict when a situation may change, even in highly stressful situations.

The ability to understand risks and to mediate, de-escalate and soften difficult situations. For instance, you may be confronted by a security guard when photographing a building as part of your research. The way you react will determine whether you'll have to abandon the plan or whether you'll manage to turn the situation to your advantage and gather additional information from the guard.

The ability to realistically assess qualities, skills and weaknesses. As an investigator you should be able to admit where you lack skills and be ready to either postpone potentially risky work or to improve your skills and knowledge in order to conduct it.

The ability to "blend in." Whether you are trying to get information from witnesses or obtain video and photographic evidence from difficult-to-access locations, you need to be able to relate to the people and locations you encounter.

The research cycle

Most research, whether field or remote, follows a cycle of four phases:

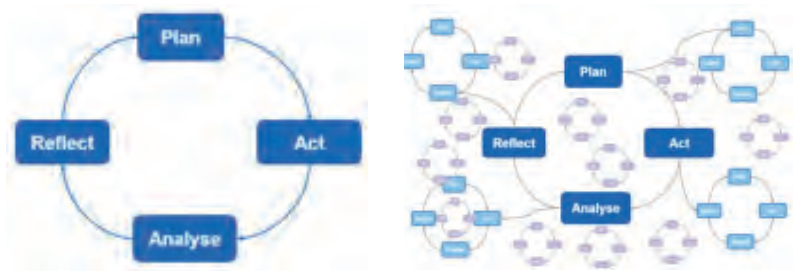
Plan - develop a good understanding of the objectives, logistics and risks of your field research activity

Act - the actual field research activity

Analyse - assess and reflect on research results

Reflect - compare your research results with the objectives of your investigation. More often than not, this leads to a new plan for continued research.

Particularly with desktop and other remote research, the boundaries of these phases are often fluid. In fact, actual research looks much less like the image on the left and more like the image on the right.



Planning for field research

Don't skip on preparation if you're already familiar with the location. Circumstances may change, the issues you are investigating may create new conditions and risks or the people you need to talk to are unpredictable.

With field research, you often have to travel to and work in places you are unfamiliar with. To increase your chances of being successful, you should not only familiarise yourself with the research location, but also manage logistics such as transportation and places to stay.

If you are working in different countries, you need to think about the usual administrative issues that come with travel and accommodation, but also pay special attention to your equipment and the way you carry information on you as you travel across borders. For instance, there are regions where journalists and researchers are not allowed to enter without special visas or passes, so bringing obvious recording equipment or external hard-drives can raise suspicions.

Set your goals and objectives

Your field research will be more efficient if you set clear goals and objectives for yourself beforehand. While each research trip is unique, there is a kind of formula for successfully fulfilling a research objective.

A research objective is usually a concrete purpose that describes what you are trying to achieve. Ideally this purpose is SMART:

Specific **M**easurable **A**ttainable **R**ealistic **T**imebound

For instance, your objective may be to ‘collect photographic evidence of a coal vessel arriving in a seaport in a few days.’ Another objective might be to ‘meet up with and obtain documents from a confidential source helping you to investigate suspicious decisions your local council has made on a tender for a building project.’



Plan your activities

In many cases, your field research will focus on one task, and you won't always need to come up with detailed task lists. In other instances, if you plan on interviewing and recording witnesses, or collecting samples from a place, things may get more complicated. You need to think in more detail about equipment, locations, safety, questions to ask, etc.

For more complicated research projects, it makes sense to write down your strategy, what questions you have to answer, the challenges you may face as well as possible solutions to them. There is no fixed format for this and you can do it in any way that suits you.

On the next page is an example of potential tasks for a hypothetical situation of going out to test water when investigating possible pollution in a community:

Component	Question	Activities
Sampling	Where to test?	Remote desktop and phone research to identify communities relying on ground water for drinking and cooking.
Sampling	Transport & accommodation	Research best options remotely. You need battery-powered refrigerators that are large enough to hold the collected samples. Look at motor homes (large camper vans) where you could stay during the field research.
Testing	What lab to use?	Identify potential labs (get price quotes for 50 samples to be tested)
Testing	Equipment needs & protocols	Talk to labs to learn about sampling protocols and receive advice on required equipment (bottles etc.)
Testing	How to ship samples?	Identify shipping companies that are equipped to ship scientific samples. Ask lab for guidance.
Interviewing experts and affected community	Equipment needed?	Compile equipment list including cameras, SD cards, spare batteries, microphones, car chargers, GPS, etc. Have backups for most important equipment.
Interviewing experts and affected community	Questionnaire for interviewees	Develop a detailed questionnaire so you ask everyone in the affected community the same questions. Prepare by talking to existing sources about what interviewees are likely to say about the impact of herbicides on their health and environment.
Interviewing experts and affected community	Release forms	Prepare release/consent forms for interviewees to sign. Explain what these are for and what happens with the information they provide.

Before you go

There will be situations where you only have one opportunity to engage with a witness or observe an event, so good preparation is vital. To gather the best evidence, consider some of the strategies below.

Practice interviews - if your research is likely to involve interviewing people, you can simulate and practice this with people in similar situations. Consider carrying out the same kind of research at another location in advance, in particular if the activity is low-risk. Ask a friend or trusted collaborator to help you role-play various situations you may encounter.

Practice your research methodology - if you've never taken environmental samples, used drones or a hidden camera, for instance, start by practicing these techniques in places that are unrelated to your actual investigation, and in a low-risk environment.

The best devices can prove useless if you don't know how to operate them. When you consider that in many situations you will only have one chance to obtain the evidence you need, there's no such thing as learning on the job. Before you decide to use specific equipment in the field, it's vital to practice with your devices and simulate investigation scenarios.

Simulate what could go wrong - it's much harder to practice what could go wrong in your research, since you generally want to avoid such situations. The best way to do this is to create a risk assessment and management list and act out potential problem situations together with people you trust. You should never carry out field research without an emergency contact and without someone knowing what you are doing, so try to practice with that person in advance.

Ensure legality - knowing what is legal and what isn't in the places where you go on field research is critical, and should be a priority in your risk management. Things like secretly recording a conversation with a person can be legal in one county and illegal in another. These laws can even vary from state to state within a country.

Sometimes there is a difference between what will likely result in your arrest or detention, and what is actually illegal. Instead of focusing on written legality, look for local guidance on what is most likely to put you on law enforcement's radar, and how you can avoid it. Journalists and staff at NGOs as well as other researchers working in areas you are interested in are likely to have relevant information.

Plan your entry and exit - how you exit your location is even more important than how you get there, especially when things can go wrong. Know the surrounding areas and have a plan to exit quickly. Researching in remote areas, forests and other poorly mapped places will require careful planning, including the use of GPS (Global Positioning System) coordinates and mapping apps or even physical maps. Learn how to use these tools and geographic coordinates before you go.

In the field

Once you are in the field you will start to focus on collecting the evidence needed to meet your objective. To do this you need the right methods and tools:

Technology - having the right technology makes a huge difference in the field. Among other things, it can let you see over long distances, document witness statements, gain access to places that would otherwise be difficult to enter and collect and process evidence in various formats.

Sometimes it matters where exactly you found the documents. For instance, there are countries where material that has been put out as garbage is considered abandoned property, and can be taken. Photographing documents may be a good way forward but this is weaker evidence than having the originals. You should research these legal aspects as part of your planning before going into the field.

Evidence collection - photo, video and audio evidence is very powerful because it counts as objective proof, although it can also be manipulated. There is a wide range of imagery you might have to take during an investigation, including exteriors and interiors of buildings, events, people, animals, documents, your own activities to prove you have done what you claim you have, etc. These situations might determine the kind of cameras and other devices you will need. Your phone camera may be of use at times but will probably have limited potential in some of these scenarios.

Witness statements - as a general rule, keep in mind that when interviewing witnesses in the field, either covertly or overtly, their statements can rarely be seen as completely impartial. Usually, you will need to corroborate their statements with other types of evidence from additional sources while in the field or later on.

Documents - you may sometimes receive or come across important documents in the field. Be careful how you handle them. You can use copies of documents received from libraries and archives and documents released by authorities through Freedom of Information (FOI) requests in any way you want. But removing documents from buildings or other public or private locations could have significant legal ramifications depending on the places you are in.

Environmental samples - if collecting samples (water, soil etc.) your planning has to address relevant sampling protocols. Rules can be complicated and require a good deal of care and attention. If you do not follow protocol, your samples could be of poor quality, or, at worst, become contaminated and provide false results. Sample analysis should always be done in accredited laboratories. Make sure you check with these laboratories what best practices you should adopt while collecting samples in the field.

Visit the Kit for the complete guide “Away From Your Screen, Out in the Field” by Mario Rautner:

kit.exposingtheinvisible.org/how/field-research.html

INTERVIEWS: THE HUMAN ELEMENT OF YOUR INVESTIGATION



The techniques, skills and good practices you need to safely identify, interview and maintain contact with people who can provide you evidence.

On Sources and Interview Subjects

It's important to make a distinction between interview subjects/ interviewees and sources. Interviewees are those that you may meet for a current investigation, and may or may not meet again. Sources are those you will need to invest some effort in building connections with, to create and maintain a network of contacts for current and future work. Some of your interviewees may become your sources and you will have to establish different dynamics with them than you would with a one-time interviewee.

Most of the time when undertaking an investigation, you will need to support it beyond desk and field research. This involves dealing with people, establishing trust, conducting expert conversations, interviewing witnesses and sometimes facing subjective reactions to incidents. This makes it important to learn how to address difficult subjects, how to keep yourself and your interviewees safe, and how to build up connections with sources that might be helpful in future investigations.

Human interactions are all about common sense and may seem fairly intuitive on the surface. But with interviews in particular, because you are dealing with people and people are often unpredictable, preparation is key. Interviewing is a much longer process than just a one-time conversation or a series of questionnaires to collect information. It requires background research, building profiles of people, establishing trust, anticipating risks, taking safety measures and more. Sometimes you will need to meet people more than once, while other subjects will be reluctant to meet at all.

Before the interview: preparation

Finding potential human sources of information and interview subjects is your initial step. This requires research, practice and commitment. Depending on whether you are starting your investigation from scratch, looking to add a face to your story or to collect testimonies, you will most likely have to find and interview different people to meet different needs of your research.

Ways to identify potential interviewees:

Observe their activity on social media - create topic-related lists that you can follow depending on the issue you are investigating. Gather a list of all those working for particular organisations or in similar fields such as activists, civil society members or companies.

Avoid 'liking' or 'following' potential interviewees on social networks if any connections to particular issues or people might get you in trouble, depending on what you are investigating.

Subscribe to newsletters - most organisations have them and you can find potential sources or interviewees among those who appear in their publications or who write for them.

Attend press conferences - people who are not generally accessible over email or phone might be approachable during press conferences, especially officials, their assistants and other institutional staff.

Attend public events - keep track of open meetings, conferences, public lectures, conventions, etc. Such events may host speakers or participants that it would otherwise be difficult or even impossible to access. Collect business cards and give out yours, if you consider it safe.

Follow blogs and webpages - such resources, if maintained by activists or local citizens, can be rich in documentation and open a door to someone who may become a source, provide leads for an investigation, or help you get in touch with the right person.

Visit official websites - these can be helpful when trying to get access to government officials. You can find out which ministries or departments are in charge of your area of interest and then request interviews with relevant officials.

Find closed, specialised groups - NGO workers, journalists and activists sometimes rely on closed (or secret) groups to exchange information and support. As you build more connections, you may want to reach out to someone you trust and ask about some of these groups if your investigation is centered on a specific country or topic.

Types of sources and interviewees will differ depending on several factors such as:

Their role in your investigation and information they can provide - primary sources who can provide direct evidence or witness accounts; or secondary sources who can provide additional background information.

Their position relative to your investigation - vulnerable sources (victims) vs. perpetrators; or willing to collaborate vs. adversarial sources who are likely to interfere in your investigation.

At times, your sources can be both vulnerable and adversarial. In most cases you will have to combine multiple approaches to address a source, while in some cases you will be able to get what you want in fewer steps.

Reaching out to sources and interviewees

Here are some basic planning guidelines:

Prioritise and organise interviews - if possible, start with interviews that provide background information about the investigation or about other potential interviewees. Then, you will be able to approach more evidence-focused interviews. Try to go from the easiest interviews to the most difficult ones so you can prepare better to address adversarial subjects at the end, when you have more knowledge on the topic.

Diversify and gain multiple perspectives - any investigation is multi-layered. The more diverse sources you include, the richer your evidence becomes and the easier it is to avoid bias. Include primary and secondary sources and try to interview people across different ages, genders, castes, classes, beliefs or job statuses.

Conduct a risk assessment - do this especially when contacting people who are close to the problem you investigate. Sometimes you will need to plan the order of the interviews carefully to prevent interferences, conflicting interests or bias in your work. Consider how risky the interaction might be for you, for the investigation, and for your sources and interviewees.

Initiate contact - sometimes you will be able to get in touch with an interview subject immediately. Other times you may need to rely on someone close to them to initiate contact. Activists, organisations, lawyers or journalists may be able to put you in touch with primary or vulnerable sources to whom they already have access. Follow protocols for safe communication in any interaction with your human sources.

Introduce yourself and your purpose - this is the first step in building trust with your sources and interviewees. Explain your work at the outset if you consider it safe to do so. If you run a public project, a website or have work that can be shared, show these to your sources or interviewees to establish your authenticity. Avoid terms that might sound too heavy, like “investigator.” You can use the term “researcher” instead, but never hide the purpose of your work unless safety risks require you to work under cover.

Preparing for interviews

Once you've decided who you will interview and have established contact, you need to prepare for the interview itself. Here is a check-list that can help:

Travel safety and security - if you travel to unknown places, you should do a risk assessment of the country or region you are visiting. To start, gather information from friends and colleagues who share your identity. Risk and identity are closely related. This means that your risk is impacted by your race or ethnicity, gender, sexual orientation or country of citizenship. Sometimes, your passport may carry privilege and protections; other times it may be the opposite.

Do your background checks - gather as much information as possible about a person / organisation / topic. Consider how safe it is to share certain information while doing your research on sensitive topics and dangerous people you plan to interview.

Define your goals.

Write a list of questions, organise it.

Prepare for difficult interviewees - mark questions that you think may raise concern or which may be faced with rejection. Prepare a set of alternative questions that can help you obtain a response.

Use time effectively - try to save time for the really significant questions. Respect your interviewee's time and offer to take breaks if they need them.

Know your terms - be careful with the language you use during your interview, both for the sake of accuracy, and out of respect. For example, make sure that you understand terms like "trans," "nonbinary," "pansexual," before interviewing someone who is LGBTQI+. The same applies to race, social status, religion, etc.

Get the right mindset - leave your own feelings and biases aside, especially if you have to face an adversarial source you may disagree with.

Get legal advice - get in touch with a lawyer if you have doubts about the information that you are handling or if you obtain access to information about a wrongdoing or a crime. Be aware of the laws that protect (or endanger) you and your interviewees and sources, which might vary depending on the country.

Arrange necessary logistics carefully - how you set the time and place of your interviews is as important as the interview itself. Public places may not always be the best option if your source is a victim of abuse, while private spaces and remote areas may be a bad idea if you meet a perpetrator or a potentially dangerous person.

During the Interview

The main difference between **non-attributable** and **off the record** is that with non-attributable you can publish the information but you cannot name the source; with off the record, you cannot publish the information or the source.

Part of preparing for an interview is establishing what medium or channels you will use with your sources and interviewees. The most common ones are: face to face, calls or email. On a scale from best to worst, face to face should be your top option while email should be the last resort.

Explain key terms - not everyone understands interview jargon, and people can get confused by terms like on the record / off the record, non-attributable, anonymous, release forms, etc. Also, these may apply differently in various contexts and cultures so better avoid them and just explain to your interviewee how the information will be used. This process should be a two-way conversation, expect the source to push back at times, until you arrive at an agreement you can both accept.

Obtain consent and permission - even if a person has agreed to talk to you, try to obtain written permission for recording and taking photos/videos and get their explicit agreement on how the information they are providing will be used, or if their name will be mentioned and how. This is especially important when interviewing minors, where an adult should always give consent on their behalf. Note that some of the evidence might not be admissible if you don't have legal consent - especially if information may end up used in courts or as proof by others (journalists, lawyers, campaigners, NGOs etc.).

Anonymous means you can publish information given during an interview, but you must never name the source or any details that may reveal the source. For instance, you cannot even mention that a certain official provided you with the information if that's the case.

Establish boundaries - make sure your interviewees understand that you are getting in touch with them because of your work - even if you already know them - and that the relationship is professional.

Document the interview - the testimonies and evidence that you collect from human sources should ideally be recorded in some form. Ethically and legally, you can only do so after they have granted you consent. Documenting techniques include audio, photo or video recordings, as well as recordings of the video/phone calls.

Use recordings ethically - if you publish your investigation, choose images or sound with utmost care. For example, if you are writing on sexual violence, avoid images that make victims appear powerless or weak. The same applies to minors: mind the sort of images that you take and the legislation that applies.

Interviews Requiring a Special Approach

Every investigation will require different human sources and you will need to vary the type of interviews you conduct to gain a broader perspective. This may mean interviewing people in different locations, but also some who might require special attention because they are vulnerable or because the goal of your investigation might be to build a legal case.

Interviews in foreign countries and other unfamiliar places

If you are planning to meet a subject in another country, consider cultural, religious, gender and other locally relevant particularities. Make sure you have a reliable contact or network there, and try to know the basics of the local language. This may make a huge difference in the results you obtain. Safety is of utmost importance so do your risk assessment in advance and prepare your way in, your stay there, and your way out carefully.

Interviewing vulnerable sources

Some sources might be particularly vulnerable, such as survivors of trauma, coerced victims, victims of trafficking, threatened communities and minorities or minors. Some might not have a good understanding of the work you are doing or what it means to have their story, name and image published online. Perhaps they have unrealistic expectations about whether and how you can help them after an interview. Sometimes, by speaking to you, they might be risking their freedom or physical safety. In such circumstances, it's important to ensure an even higher level of care, responsibility, ethics and legality on your side. It's your responsibility to make sure sources understand exactly what your use of the evidence or testimony that they will provide means for them, how it will be used, how they will be identified, if at all, and what the risks are. Make sure to think through the possible repercussions for your source before making their evidence and testimony public, and decide together whether those risks are worth taking.

Interviewing adversarial sources

Some interviewees may be or become adversarial or combative over the course of your communication and interviews. It might be that they are simply hostile by character or that they are perpetrators refusing to cooperate or trying to deviate from your line of investigation. It's important to do as much research as possible before your interview so you can speak confidently if a confrontation takes place. Most importantly, don't let your bias take over; even if you don't respect a hostile person or a suspected perpetrator, you have to approach the interview with empathy. As your time with the source progresses, you can begin to ask more pointed and tougher questions. Remember that getting verifiable evidence from the interview is your objective.

After the interview

Assessing your interview findings and preparing the next steps is essential to ensuring a useful follow-up to your efforts. Here are some steps and principles to remember:

Checks and balances - avoid your personal biases and consider your interviewees' biases in order to gain a broader perspective from your interviews. The ways in which you display your evidence and the weight that you give to every interview is important. Try to counterbalance statements accurately.

Assessing needs, thinking it over - your investigation is like a jigsaw puzzle. Even if you have fact-checked at every step, you should revisit your evidence when you have all your information and statements. You may pick up details you haven't seen before.

Giving right of reply - if the purpose of your investigation is to publish a story that accuses someone of wrongdoing, they have a right to respond to those allegations.

Honouring the efforts of sources and interviewees - consider the time and effort that they put into answering your questions, especially in conditions of risk and/or limited resources. You can do little things like sending them copies or links to your investigation if you publish it, or reconnecting with them when you are next in their area, if you consider it safe to do so.

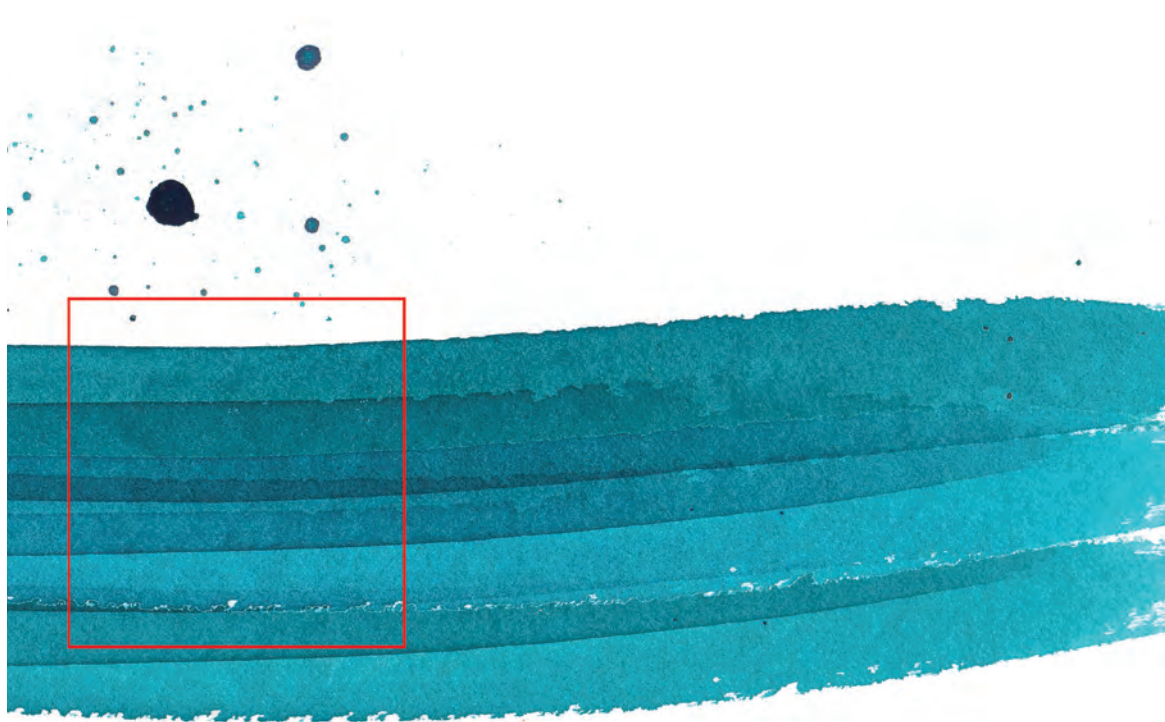
Staying in touch - there are a few considerations to bear in mind if you want to do this. Depending on who the source is, having your card or your contact details may compromise them and/or yourself. Make sure they understand that for their own safety it's important to maintain secure communication, rely on encrypted messaging applications, and only reveal new and sensitive information when you meet or establish safe communication channels.

Know when to let go - there are different reasons why you may have to give up your investigation. Feeling stressed and overwhelmed is natural, and the pressure of your work may be too much at some point. In addition, your research may end up showing that there is no case, or that you won't be able to collect all the evidence you need. Thinking your investigation over will help you decide whether you need to let go.

Visit the Kit for the complete guide "Interviews: the Human Element of Your Investigation" by Nuria Tesón, Ankita Anand, Jess Lempit, Megha Rajagopalan:

kit.exposingtheinvisible.org/how/interviews.html

HOW TO MANAGE YOUR SOURCES



Start building your own contacts, learn how to develop, interact with and maintain sources and how to enrich your investigations with their cooperation.

During the course of your investigation you will be in touch with people you will want to interview but also with others who will provide you information over longer periods of time and whom you may not necessarily interview. These will be your sources.

Creating an agenda and database

If you work (or plan to work) as an investigator, you need to create a network of sources that you can rely on for information over time. You can reach out to potential sources and build connections in various ways: by starting with an informal interaction, having a coffee or meeting them at their workplace. You can also try to turn your interviewees into sources by keeping in contact with them after you are done with a specific interview or investigation.

When creating agendas, organise and gather contacts in a meaningful way while also taking extra care to save and store their details safely to protect the identity of your sources. For instance, your agenda may involve building a topic-specific contact list of environmentalists, lawyers, political activists, human rights researchers, officials, etc.

Don't dismiss lower-ranking people from your network. They might be able to help you with accessing evidence and/or interviews just by being close to those in power, or they might reach a position of responsibility in the future and gain access to more sensitive information.

If you are (or become) known in the field of investigation, people may also start reaching out to you and offering information over a longer period. You should always establish their reliability and biases, ask them about their intentions and lay out the boundaries of your relationship.

Building trust

Your work is your best tool when you are trying to gain a source's trust. If you have done previous investigations and you were able to preserve the privacy and safety of your interviewees and sources, others may feel more inclined to collaborate with you. Build a reputation not only as an investigator but as someone who cares about the people you are interviewing, and remember to be genuine. People might be assuming a huge risk by maintaining a relationship with you and you should always make sure you acknowledge it.

Keeping contact: the law of the three calls

Never take your sources for granted. Once you have established contact and started building a relationship, you need to show interest and maintain contact. Ideally, don't just call your sources when you need something. Rather, try applying the law of the three calls.

Once in a while, send a message showing interest in how they are doing and make sure they feel that you are not looking for information. A second call may follow later on to check on them, ask how things are going with work and in their lives, and let them know that you are up for a coffee. This should be only for the purpose of catching up and not to extract any information. Then, when you really need them for the purpose of an investigation, the third call will happen naturally.

It might happen that they actually get in touch first to inform you of something because you are on their mind and because they don't think of you as a selfish investigator who only appears when they need something.

Is your source compromised?

The fact that someone has been trustworthy or reliable at a certain point doesn't mean they are going to be so forever.

You need to preemptively check your source's credibility and reliability every time you meet them, and not just before the first meeting, depending on who they are, the context they are informing in, and other factors.

For example, you may have been in a country where someone working for an organisation was helping put you in touch with people you wanted to interview. In the meantime, the source or source's family or organisation might have been threatened or pushed to denounce you or your work if you ever come back. Be alert to changes in their behaviour. If they suddenly ask too many questions or want to know too many personal details like where you live, who your partner is, who gave you this or that evidence, their status as a reliable source may have changed.

Protecting sources

In the United States, for instance, civil and criminal courts can issue subpoenas forcing you to disclose the identities of confidential sources, and you will have to decide whether to reveal them, or face fines and even jail time.

Confidentiality is key for your sources. If you disclose their details to others, you compromise your sources and your relationship with them.

Your interaction must be based on mutual trust and sources have to be sure that you will not deceive them under any circumstances. You have the right to protect them even when asked about them by a judge, though this might vary depending on the country you're in. You must be aware of the legislation in your own country and in the country you will be working from.

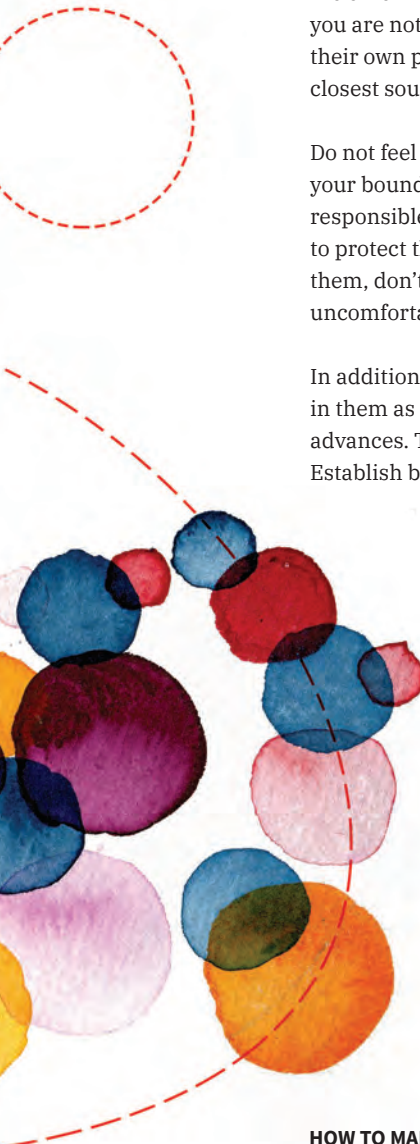
A good way of protecting the privacy of your relationship with sources is to keep your communications encrypted and your contact databases protected with passwords. Follow digital security advice and best practices to make sure that you are doing your best to protect your devices, communication and information from unwanted access.

Maintaining boundaries

When you have been investigating the same issue for some time, or when you are just starting to build a network of reliable sources, you may need to be careful that your relationships remain professional.

This might be tricky, and the line can sometimes become blurred, as the bond you establish with certain sources is all about trust, commitment or joining forces to fight against wrongdoing. You need to consider the fact that if your relationship strengthens to the extent of befriending your sources you may become biased and lose both objectivity and credibility.

Sometimes you may get to know details that are useful for your investigation in a context in which your source talks to you as to a friend rather than an investigator. Establish the necessary boundaries to avoid this if possible, though sometimes it will occur naturally. Try to avoid revealing details about your personal life whenever possible. Be friendly but professional. As an investigator you will need allies, but make sure that you are aware of the difference between someone trusting you because of your shared friendship and someone trusting you because of your work.



If you can avoid the relationship with your source becoming personal, you have to consider how your interactions might change. For instance, if they disclose information in a private, friendly (and not investigative) context, you must ask them straightforwardly whether it can be used, and never use it without their consent. Be aware that they may feel pressured to let you use the information, so consider potential risks and don't abuse your position of power to make them talk to you as an investigator if they were confiding in you as a friend. The same applies the other way around. A source may feel entitled to ask you something you are not comfortable doing if your relationship is too close, or use their own power to mislead or manipulate you. Make sure that even your closest sources are still reliable at different moments in time.

Do not feel forced to maintain a relationship with a source if you think your boundaries are being crossed. Don't let them make you feel responsible for their wellbeing. If you have done everything you can to protect them and you have no regrets about your behaviour toward them, don't feel obliged to go forward with an interaction that makes you uncomfortable or may put you and your work at risk.

In addition, it can happen that sources end up interpreting your interest in them as personal and this may make you vulnerable to unwanted advances. This can ultimately affect anyone, regardless of gender. Establish boundaries from the beginning and stick to them.

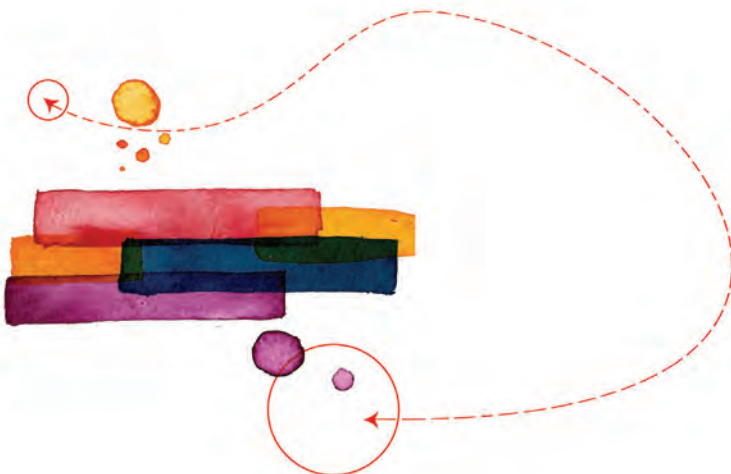
Risk Assessment

There can never be too much warning or awareness about risks to safety. Whenever you are dealing with sources you should repeatedly assess any risk you and your source are assuming. You may consider using pseudonyms to hide their identities when building your databases of sources, and remember to always keep your files encrypted.

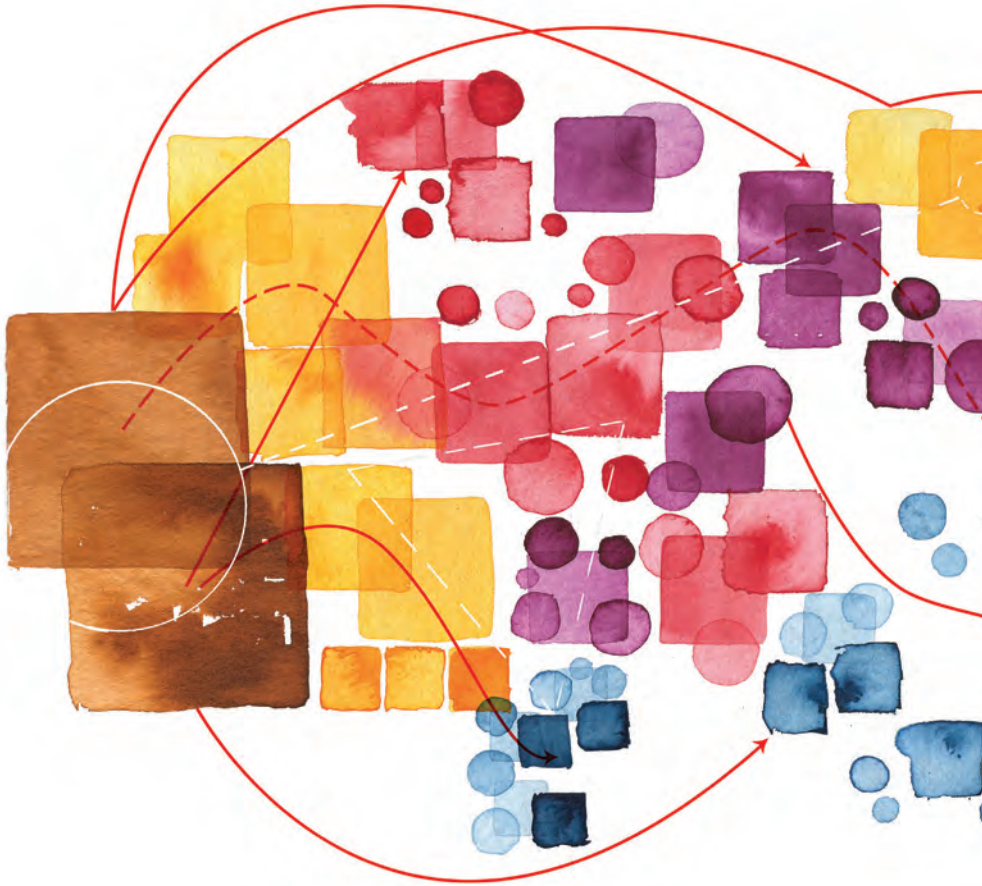
You need to decide carefully when it's secure to get in touch with a source and how you do it. This is especially necessary if these sources are confidential or the information they hold is controversial or dangerous. Whenever possible, stick to encrypted communications. If you need to use mobile or landline phones that are not secure, you may want to establish a code with your source to make them aware that the call might not be private and there is risk of surveillance. Don't disclose any sensitive information, such as your subject matter or where you will meet. When meeting, avoid going to places you visit frequently or where you may run into people either of you know.

Visit the Kit for the complete guide “How to Manage Your Sources” by Nuria Tesón, Ankita Anand, Jess Lempit, Megha Rajagopalan:

kit.exposingtheinvisible.org/how/manage-sources.html



SUPPLY CHAIN AND PRODUCT INVESTIGATIONS



Get an overview of the main actors, stages and processes of a supply chain, as well as the main tools, techniques and data resources for evidence collection.

A supply chain is a set of steps that commodities (goods or raw materials) undergo on their way to becoming products used by consumers or industry. Stages of a supply chain can include places where products are transformed – for instance, an electronics company where circuit boards are made from transistors and copper lines – and where products change hands through transport, such as the loading of circuit boards onto a truck and their shipment to a computer manufacturing company.

Supply chain investigations focus on collecting evidence to link each stage of a product's journey, from the origin of the commodity (for example, the conflict metal Cassiterite used in the solder of laptops) to the final product (the laptop itself), which can contain hundreds of different components.

Supply chain investigations can be particularly impactful because they have the potential to change the behaviours of entire industries when done effectively, with thorough and reliable evidence. Investigation findings can have an impact not only on the reputation but also the financial status of the companies involved, in particular when they reveal illegal or controversial activities taking place along the chain.

In the most successful cases, this impacts the supply chain all the way back to the origin of the product, where it may prevent social injustice, from poor working conditions and human rights abuses to land grabbing and environmental destruction. Most supply chain investigations are carried out by journalists or NGOs, but they can also be carried out by determined independent investigators or people and communities directly affected by an issue.

Shining a light on where our products really come from

Everything around us is part of a supply chain: from the food we eat to the clothes we wear and the devices we use. But the nature of supply chains means we rarely know how commodities are produced or even where they originate.

We might not always consider where our items come from, who harvested their source materials and under what conditions, whether there was exploitation or abuse at any point in the production process, or if illicit acts were carried out along the way. However, these questions might be brought to light when public controversies emerge about certain products or brands.



Even if you are not physically present at a location where commodities are produced or extracted, many supply chain investigations can be carried out remotely. Indeed, in most cases, elements of a supply chain are located far from the source - for example, wood processing and furniture manufacturing can take place continents away from where the forest was originally cleared.

Elements of a supply chain investigation

Supply chains are often complicated networks or webs of actors, processes and movements. While it takes thousands of links in multiple supply chains to manufacture one laptop, investigations usually focus on very specific components of a supply chain, such as the source of one single element used in the manufacture of one part of the laptop, or a single factory where one stage of the production takes place. Maintaining such a focus makes the research more effective.

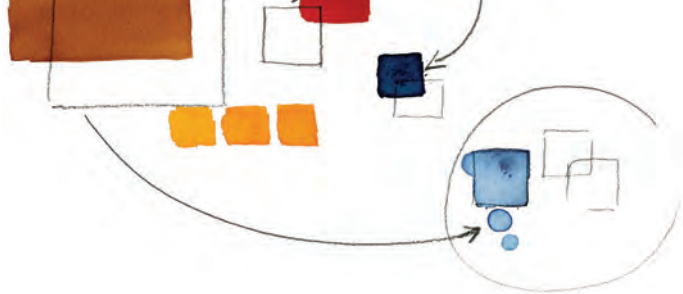
Barcodes on consumer products can be used to identify the manufacturer, as well as additional information about them. The most commonly used barcodes are the European Article Numbers / EAN, which are usually 13 digits and used both within and outside of Europe, and the 12-digit Universal Product Code (UPC), which is very similar to the EAN, but contains a zero at the beginning to signify registration in the USA or Canada. The global standard of barcodes is maintained by the non-profit organisation GS1 that has a searchable database (gepir.gs1.org/index.php/search-by-gtin) of many (but not all) barcodes.

Supply chain research can be instrumental in linking a company to ethical issues that taint their products, even though the physical components of the product itself may not be controversial – for example, the violation of indigenous land rights that often occurs when producing rubber for car tires.

Key concept to remember about supply chains are:

Traceability - the passing of information from one stage in the supply chain to the next. This can relate to the initial source of the ingredients or raw material of a product, the alterations it incurred along the way, or other relevant details that may help trace an entire history of transportation and production. Some companies have systems for this but many supply chains are so long and complicated that it can be difficult even for the companies directly involved to achieve a fully traceable supply chain.

Certification schemes - are often used to ensure that products are manufactured, produced and traded following specific standards. For instance, they can indicate that the human rights and traditional land rights of local and indigenous people are observed or that no tropical forests are cleared to make a specific product. Well known certification schemes include those for organic and fair trade produce or for sustainable timber, palm oil or coffee.



Food hygiene labels:

European Union rules regarding food hygiene cover all stages of the production, processing, distribution and sale of animal products intended for consumption. This includes, for example, fish, meat and dairy products, but also pet food. Every company that puts food products on the market has to have a unique registration code that identifies it. These codes are printed on the product label and consist of a combination of letters and numbers within an oval. Have a look at a product in store to find the label. The EU has an online database of codes and permits (ec.europa.eu/food/safety/biosafety/food_hygiene_en), making it possible to identify the name of the company that put a product on the market. The database covers imported and exported goods and includes details of companies from over 80 EU and non-EU countries.

Company finances and trading and transport processes - are essential aspects to research and understand when tracing supply chains across different countries. This all combines with other data you may need to collect about the product you are trying to track and its production prices.

Verification at every step - as with any investigation, you should always question your initial assumptions and results to make sure that the information you collect is relevant to what you intended to prove. What at first appears likely may in fact have another explanation. For instance, you might have linked a company illegally clearing forests to a timber mill that sells to a furniture company, only to find out that the furniture company does not actually use the timber species harvested from the forest in question. You therefore cannot make a direct connection between the company and the illegal deforestation activity.

Flexibility and unpredictability - are features that best define the nature of supply chain research. This means that it's not always possible to anticipate how long your research will take. Sometimes linking two processes can take a day of online database work; sometimes it can take months and dozens of research strategies and tools, including online and field research.

Fairtrade certificate logos.



Where to start

You can start your investigation at any point along the supply chain where you suspect unethical or illegal behaviour might be taking place.

NGOs like Greenpeace, Rainforest Action Network, Rainforest Alliance, Mining Watch and many others conduct research on various supply chains and their impact on human rights, the environment, and the wellbeing of communities living and working along the chain. Check their work for further inspiration, methods and resources.

In most cases, investigators follow the trail downstream along the supply chain from this entry point. For instance, if an investigation starts at a mobile phone assembly plant suspected of using child labour, it will most likely continue downstream to the brand that sells the mobile phones, rather than upstream to the origin of the plastics and metals used in the phones' manufacturing process. The focus here will be to expose illegal and unethical practices of exploiting children to produce that phone.

In some cases, however, research can occur upstream. An example might be the case of an ill-famed company establishing a manufacturing plant in a town whose residents want to find out if the products and commodities entering the plant are of controversial origin.

Once you identify an entry point, you can follow a sequential path along the supply chain to collect evidence connecting each step, be it along a production process or a product's transport path.

You might need to use anything from maps to identify the source locations of raw materials or interactive transport tracking services to follow commodity shipments, to online customs and product databases or corporate records and stock exchange websites to learn more about the products and companies you are focusing on. You might also sometimes undertake field research and collaborate with others to collect evidence and witness accounts about what happens on the ground.

Companies tend to tightly guard information about their suppliers and customers to avoid exposing their internal mechanisms and advantages to their competitors. Companies also sometimes hire investigators to research the supply chains of competing products and of other companies.

Supply chain investigators look for evidence that links the chain, and this often requires a lot of creativity since no two supply chains are the same and access to information can vary vastly depending on the data sources available or the geographies where research is being conducted.

The ability to 'look sideways' by making previously unseen connections is a critical skill, as is being able to come up with innovative solutions to research problems.

Profiling supply chain actors

When thinking about supply chains, a useful first step is to understand the various actors – the participating companies or individuals – that operate along the way. While the actual chains are usually unique combinations, some of the actors can be categorised into groups, which are often connected by shipping or transport providers.

Most often, along a supply chain you will encounter the following:

Producer: company, person or group of persons that takes, grows, mines or otherwise produces the raw materials (such as the owner of a timber plantation).

Initial processor: company that carries out the first transformation of the product (for instance, a timber mill turning a log into planks).

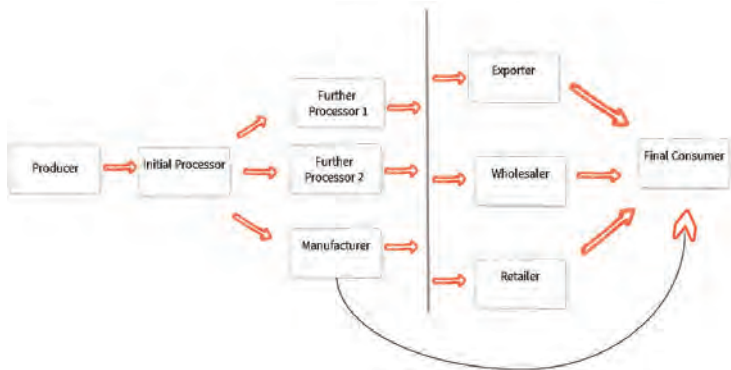
Further processors: companies that carry out additional transformations of the product (wood can ultimately even turn into fiber for textiles). In many supply chains there are multiple further processors, while other supply chains may not have any.

Importers, exporters, distributors: companies responsible for getting the products into different countries, by operating or hiring shipping or trucking services to carry the products (for example, shipping the wood planks to a deposit in country X, from where it can be sold to furniture manufacturers and others).

Manufacturers: companies that carry out the last transformation before the product is sold to consumers or industrial users (such as the company making furniture or toothpicks).

Retailers: companies and individuals responsible for selling the products to consumers or industrial users (like a hardware shop or furniture store).

Simplified example of supply chain actors and their connections



Each product and shipment that exits or enters a country has an **HS code** (Harmonized Commodity Description and Coding System) attached to it. This is a standardised system of names and numbers that helps classify commodities worldwide. HS codes are developed and maintained by the World Customs Organization (wcoomd.org). They are useful when tracking product shipments and trade (import/export) data. The United Nations maintains the Comtrade database (comtrade.un.org/data), which contains such statistics that are useful for chain of custody investigations.

Let's assume you've chosen your entry point in the supply chain: for example, a local fabrics manufacturer where you suspect that workers are mistreated and underpaid, and you want to find out what fashion brands buy these fabrics and where they are sold. You've also mapped the actors you will focus on: the manufacturer and the retailer plus potentially, the final consumers so you can raise public awareness about your investigation findings.

Now you know what and whom you are investigating. The next step is to establish a list of companies and people of interest. Before you move any further, begin by researching their company ownership, business models, networks of collaborators, places where they are registered and/or operate, products they manufacture or sell, and possible controversies surrounding them already.

By doing this background research you create a profile of your main actors and their connections, build your foundation for further investigation, prepare yourself for interviews with relevant people (sources, witnesses, specialists etc.), establish connections and assess your potential risks.

Internet research is a good place to start looking for basic information about businesses and people associated with the companies in the supply chain you're investigating. Try to find out as much as possible from companies' websites and activity reports, supply chain due diligence reports (if available), stock exchanges (if the company is listed), media articles or social media profiles of the company, its board and staff. At the same time, look for official documents that include the companies' registration data, shareholders, subsidiaries, members of the board, directors, annual financial reports and other relevant details. If you already know in which countries to look for official documents, you can start by checking available online corporate registries and other official databases, such as land records, court records, patent registries etc.

Researching companies

The Investigative Dashboard (investigativedashboard.org) is a resource built by the Organized Crime and Corruption Reporting Project (OCCRP), which indexes public company registries, land and courts records from around the world. From this platform you can go to the country and type of records you want, but note that while some corporate records provide free access to basic or more advanced information, others will require registration and charge a fee to provide detailed company records. The Investigative Dashboard also allows you to freely search and use a database (data.occrp.org) of millions of documents and datasets from public sources, leaks and investigations that OCCRP has conducted in the past.

Open Corporates (opencorporates.com) is a platform that lets you search freely for company records and related data it collects from all over the world. In addition, the International Consortium for Investigative Journalism (ICIJ) provides the Offshore Leaks Database (offshoreleaks.icij.org) a massive resource of company records and other useful documents that have been revealed by large leaks and projects the group has been working on, including the Paradise Papers, Panama Papers, Offshore Leaks and Bahamas Leaks.

Visit the Kit for the complete guide "Supply Chain and Product Investigations" by Mario Rautner:

kit.exposingtheinvisible.org/what/supply-chain.html

SAFETY FIRST!



Stay digitally and physically safe and aware of potential risks at all times by adopting some basic good practices and tools to keep yourself, your sources and your evidence protected.

Staying safe is an integral part of any investigation. Your safety, and that of your data, your human sources and your collaborators should always be a priority.

It's therefore vital to think of the risks associated with the type of research or investigation activity you are undertaking in any context, in order to mitigate those risks. This is part of a process called **risk assessment**.

The more complicated and risky your activity, the more comprehensive your risk assessment should be.

Risk assessments are a common exercise in a number of disciplines involving online and offline / field activities including scientific research, journalistic investigations, information collection by NGOs, or law enforcement investigations.

Before starting your work, make sure you also have a **risk mitigation** or **risk reduction** plan. This involves coming up with ways you could prevent, respond to and resolve problems that might arise. This plan can help you navigate the potential issues highlighted in your risk assessment.

Online safety

Searching and collecting evidence online - whether it's about social media data, online company records, domain ownership details, website history, image metadata, etc. - involves navigating a large number of platforms, tools and services. Some of these work with the *Tor Browser* (torproject.org) and that allows you to protect your privacy to a certain extent. Others not only do not work on Tor but they also require you to sign up with an email address, name and other personal details. Depending on your investigation subject, your context and that of the people you work with, leaving digital traces while you investigate online might put you at higher risk.

Consider these suggestions for digital safety techniques and tools that can help protect your digital privacy and enhance the security of your devices and data.

The Tor Browser is a browser that keeps your online activities private. It disguises your identity and protects your web traffic from many forms of internet surveillance. It can also be used to bypass internet filters.

Accounts

Some online services require you to create an account, to choose a username, to provide payment information, to verify an email addresses or to sign up with your social media profile to gain access to their platforms. Try to limit your exposure by considering these options: Create a more secure, compartmentalised email account, which you can do easily with services like *Tutanota* (tutanota.de) or *Protonmail* (protonmail.com).

Establish a separate set of social media accounts to use with services that require your data, in order to compartmentalise (separate) your investigative work from your personal online identity.

Create a single use “identity” for a particular investigation, and dispose of it once research is done. This may be needed especially when doing sensitive work.

Browsers

As someone who is looking to uncover hidden truths, you probably already use the internet for personal communication and for some of your research.

It's a good idea to use different browsers for your research and for casual web browsing. By doing so, you are again practicing “compartmentalisation” - using one browser for research and another for everything else.

We recommend you choose a “privacy aware” browser for your research and avoid logging in to web-based email and social media on that browser. This will prevent a lot of your personal data from being sent to the websites you visit.

Before using any of the online tools we talk about here or in the online Kit, it's a good idea to download and install one of these browsers. Then, add an extra layer of certainty by testing the browser with a tool like *Panoptlick* (panoptlick.eff.org) or *Browser Leaks* (browserleaks.com). The results of what you see when using a privacy aware browser should look different from when you visit Panoptlick or Browser Leaks with a normal browser, which would usually reveal more weaknesses.

These are some examples of tools that can help protect your privacy while researching online, with pros and cons of using them:

Tor Browser (torproject.org)

Some webpages block Tor by default and you will have to decide whether or not to visit them with Tor turned off.

Pros: This is the best privacy aware browser. The code is published openly so anyone can see how it works. It has a built-in way of changing your IP address and encrypting your traffic.

Cons: There are places in the world where Tor Browser usage is blocked or banned. While there are ways around these blocks, such as *Tor Bridges* (torproject.org/docs/bridges), using Tor may also flag your traffic as suspicious in such places.

Firefox ([firefox.com](https://www.firefox.com))

Pros: It blocks trackers and cookies with a setting called “Enhanced Tracking Protection”, which is automatically turned on when you set “Content Blocking” to “strict”.

Cons: You need to turn on this option, it’s off by default. When you use Firefox, it’s important to remember that your IP address is still visible to the sites you visit.

Brave (brave.com)

Pros: It tries to protect privacy without the need for turning options on or adding add-ons or extensions. Brave has a security setting to erase all Private Data when the browser is closed. It has a feature called ‘Shields’ where you can block ads and trackers. It also allows you to create a new “Private Tab with Tor”, which uses the Tor network to protect your IP address (regular use doesn’t protect it).

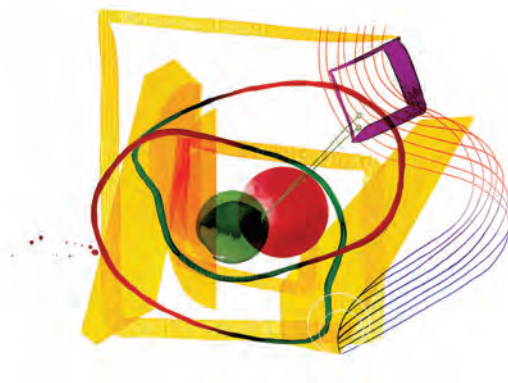
Cons: The “payments” or “Brave payments” feature that allows donations should be kept off as it sends data that could be used to identify you. When using Brave, you should use the ‘Private Tab with Tor’ feature to protect your IP address.

DuckDuckGo (duckduckgo.com)

Pros: This is a privacy-aware search engine (not a browser) that claims not to collect any personal data about its users. You can use DuckDuckGo in combination with the Tor Browser to further preserve your privacy.

Cons: DuckDuckGo does save your search queries but it doesn’t collect data that can identify you personally.

Brave’s “Private Tab with Tor” also allows you to visit Tor hidden service sites - which are sites that end in .onion and are configured to be securely accessed only by Tor-enabled browsers.



VPNs work by disguising your IP address, which can be used by websites you visit to map where you are coming from. When using a VPN, rather than seeing your real IP address, sites you visit will see the IP of the VPN provider.

Virtual Private Networks (VPNs)

If you cannot use Tor, another option, though less effective in preserving your anonymity, is to use a VPN (Virtual Private Network).

Visiting a website is like making a phone call. The website you are visiting can see your “number” - your IP address - which can be used to map where you are coming from. Think of the VPN as a concrete tunnel between you and the site you want to visit. The VPN creates a tunnel around your traffic so it can't be observed from the outside, and routes it through an intermediary server owned by your VPN provider, so your traffic looks to any site you visit like it's coming from a different location than where you actually are. Neither the web browser, your internet service provider nor the site you visit will see your IP or be able to identify you. Sites will only see that your traffic is coming from the IP address of your VPN provider.

If you are researching a corporation and frequently visit its board of directors webpage – a page that typically gets very little traffic - your repeated visits from your specific location might make the company aware of your research.

There are many VPN options and it can be confusing when deciding which one to pick. To add to the confusion, most VPN reviews and listings are not independent, some are really biased. *ThatOnePrivacySite* (thatoneprivacysite.net) is a VPN review site we can endorse.

It is recommended you choose a VPN company that claims that they do not record logs of your traffic. While you should avoid most free VPNs because they are often funding their operation by selling their log data (records of what sites users visit via the VPN), there are some reputable ones we recommend: *Bitmask* (BitMask.net), *Riseup VPN* (riseup.net/en/vpn), *PsIPhon* (Psiphon.ca), *Lantern* (getLantern.com).

Communication

Whenever possible, use encrypted email (PGP - Pretty Good Privacy,) in communication with collaborators, sources and interviewees.

For calls and messaging, there are different applications with enhanced levels of encryption and privacy such as *Signal* (signal.org) or *Wire* (wire.com). These are preferred over WhatsApp, though the latest is of more common use and you may encounter people who are not easily accessible on any other (safer) apps.

Check the Secure Communication guide (securityinabox.org/en/guide/secure-communication) from Tactical Tech's Security in a Box for tips, tools, and methods to keep your digital communication as private as possible.

When you are forced to rely on conventional ways of communication - non-encrypted phone calls, landlines, etc., - make sure that you provide only the minimum information and try to establish in advance what details are less risky to communicate with the person at the other end of the line, and how. When fearing threats and surveillance, use the above encrypted methods to get in touch with someone close to your sources who can help organise a meeting.

Field safety

On occasion, if you think your phone might be monitored, consider using a burner phone - a disposable phone you can use on one or a few occasions and that is not linked to you or that you can discard easily.

Field investigations carry more physical risk than working from behind a computer. Traveling to new places, talking to people, filming, or using certain equipment can make you look suspicious in some contexts. This is why planning, carrying out a risk assessment, and considering the possible consequences of your actions is vital even if you are certain your activity is low-risk. There are no strict rules for a risk assessment but make sure you have a clear plan established in advance, know who your important contacts are and which individuals or organisations could provide assistance in the field.

Here are some essential aspects to consider when assessing your situation:

If your activity includes interviews with confidential or vulnerable sources, address the risks they are exposed to in your assessment. Discuss with them any vulnerabilities they might face while collaborating with you.

Take care when deciding the order in which you collect information, the people that you share it with, when/where you arrange to meet them and where and how you store the information you've gathered. Start with background research and less risky interviews or field work first, advance as you gather more information and always reassess the risks.

Beware of disclosing confidential or sensitive information about your investigation and sources. This might put you and your collaborators at risk depending on the context and issues you are researching.

Image metadata can reveal more than you want it to. It may be possible for someone to use it to locate other photos on the internet that you or someone else took with the same camera, or figure out where you live if any of the photographs were taken in your home. While you may wish to preserve location information as part of your evidence, especially during field research, you should also be cautious about where and how you share images and other location-based data you collect.

Risk is inherited. If you are someone with little to no risk (you may live and work in a safe area) but you are interviewing a person experiencing high risk (living in a dangerous area, being under pressure, working on controversial issues), you inherit that risk. Your risk level will be higher for a period of time before and after the interview. If you interview someone for a report or an article that will be published, be prepared for your risk to increase at the time of publication. When investigating individuals in positions of power and influence, be prepared for a prolonged higher risk if they become aware of your investigation.

Keeping your location safe

A number of common apps, including Google Maps and WhatsApp, allow you to share your real-time location with specific people for a limited period of time. This feature could potentially be helpful when conducting field research because it can allow a trusted colleague to monitor where you are, as a safety measure.

On the other hand, sharing your location in real time can put you at risk if others who are interested in your whereabouts are able to access the data you share. When researching sensitive topics, or if you suspect that you might be under surveillance, you should avoid sharing or storing your location without using encryption.

Instead, consider finding alternative ways of tracking your daily movements while investigating, such as marking places and details manually, or using a printed map. In many cases, it is wiser to disable such location sharing features from your mobile phone and other devices with location tracking functions. Most smartphones allow you to do so under “Location Settings.”

Other factors

You will encounter situations where your perceived gender, race, religion and other personal aspects will have an effect on how you can do your work and how people you meet and interview accept or address you. Be aware of this and make sure you establish clear boundaries from the beginning to avoid unwanted or unexpected reactions. Research the place, culture, beliefs, and social norms of the places, communities, and people you visit or plan to talk to.



Visit the “Safety First!” sections of the online Kit for detailed advice applied to each investigation context:

kit.exposingtheinvisible.org.

GLOSSARY

Aerial imagery - photographs of the Earth's surface taken from manned or unmanned flying objects such as airplanes, balloons, kites, helicopters, drones etc.

API - Application Programming Interface, by which a platform can make its data accessible to external developers for free or under some conditions or fees.

Browser extensions - also called add-ons, they are small pieces of software used to extend the functionalities of a web browser (e.g. extensions for spell-checks, screen-shots etc).

Brute force - a password cracking technique that involves trying every possible combination.

Cache - a temporary, high-speed storage for data that has been used or processed and may be retrieved again quickly rather than visiting the original source or redoing computing associated with the requested data.

CAPTCHA - an automated test used by websites and online services to determine whether a user is human or robot.

Chain of custody - the documented history of the treatment of a piece of evidence. A chronological record of how material (documents, samples, etc.) is handled and by whom during an investigation. The term is used in legal cases when managing evidence but also applies to any other investigations.

Choropleth - a map where the different regions are coloured to show a differences, for example, in voting percentages, or life expectancy etc.

Content Management System (CMS) - software used to manage content that is later rendered into pages on the internet.

Cookie - a small file, saved on your computer by your browser, that can be used to store information for, or identify you to, a particular website.

Commodity - traded goods or raw material.

Corroborating evidence - additional evidence that supports other evidence already obtained. Anything that supports a witness's story or your understanding of information.

Crawler - also called a spider, is a piece of software that systematically browses the internet to collect and index information.

Database - a system used to store and organize collections of data with a particular focus or purpose. For example, a database of land and property ownership in country Z.

Dataset - a collection of data sharing some common attributes and that is usually organized in rows and columns (tables) for easier processing. For example, a dataset of the foreign owners of land and properties in country Z.

Directory - a container used to categorise files or other containers of files and data.

Domain name - a name that is commonly used to access a website (e.g. tacticaltech.org). Domain names are translated into IP addresses.

Dorking - a technique of using search engines to their full potential by employing refined searches.

Filter - in web search context, it is a keyword or phrase that has particular meaning for the search engine.

Full-disc encryption - encryption that happens at a device or hardware level. For example, encrypting an entire computer's disk would also automatically encrypt all the data saved on it.

Geocoding - the process of converting location data, such as a street address, into precise latitude and longitude coordinates.

Geodata - digital information that is directly linked to a physical or geographic location.

Geographic information system (GIS) - a system or software used to collect, store, process, analyse, interpret and represent geographic information.

Geolocation - finding the real world location of an object, such as the place that a photograph was taken.

Global Positioning System (GPS) - a US system of navigational satellites that allow users to determine their position on earth.

Hacker - traditionally, anyone who interacts with technology in unexpected ways in order to learn more about it or to exploit it.

Human source - someone who shares information with you and/or with whom you maintain contact over time, and who may contribute information to your investigations.

Internet Protocol (IP) address - a set of numbers used to identify a computer or data location you are connecting to (example: 213.108.108.217).

Land cover (data, maps) - a way of classifying maps and satellite imagery data based on what covers the Earth's surface: grass, trees, water, buildings, crops etc.

Land use (data, maps) - a way of classifying maps and satellite imagery data based on how people use the land on the Earth's surface: for agriculture, transport, recreation, residential, etc.

Metadata - information about information. E.g.: the content of a sound file is the recording, but the duration of the recording is a property of the file that can be described as metadata.

Off the record - you cannot make information you receive public or attribute it to the person who gave it to you.

On the record - you can use the information provided in an interview or conversation and mention the person that gives it to you.

Proof of life - a document that contains confidential information and sometimes passwords that someone you fully trust will keep in order to determine, based on your online activity (or lack of it), whether you are still alive.

Release/consent form - forms that grant permission for the use of information or media from interviews, or which show that you have done your due diligence in explaining to your subjects the details and possible risks associated with participating in your research.

Risk assessment - a method of measuring the chance that certain threats might happen along your investigation, so you know how to prevent them and/or address them if you can't avoid them.

Robots.txt - a file on a website that instructs automated programs (bots/robots/crawlers) how to behave with data on the website.

Satellite imagery - images of the Earth's surface or of other planets' surface taken by satellites. These images are often taken in stages and combined to obtain a complete overview of large areas, to create maps, and to observe land and water surface details.

Server – a computer that remains on and connected to the internet in order to provide a service, such as hosting a webpage or sending and receiving email, to other computers.

Supply chain - a set of steps that commodities (goods or raw materials) undergo on their way to becoming products used by consumers or industry.

Thematic map - a map showing information related to a specific subject, such as air pollution, forest cover, election results.

Tor browser - a browser that keeps your online activities private. It disguises your identity and protects your web traffic from many forms of internet surveillance. It can also be used to bypass internet filters.

Universal Resource Locator (URL) - a web address used to retrieve a page or data on a network or internet.

Virtual Private Network (VPN) - software that creates an encrypted “tunnel” from your device to a server run by your VPN service provider. Websites and other online services will receive your requests from - and return their responses to - the IP address of that server rather than your actual IP address.

Webpage - a document that is accessible via the internet, displayed in a web browser. A collection of webpages make a website.

Web server - also known as internet server, is a system that hosts websites and delivers their content and services to end users over the internet. It includes hardware (physical server machines that store the information) and software that facilitates users' access to the content.

Web tracker - tool or software used by websites in order to trace their visitors and how they interact with the site.

CREDITS

Contributing Authors: Ankita Anand, Annabel Church, Hang Do Thi Duc, Wael Eskandar, Alison Killing, Jess Lempit, Hanna Liubakova, Offray Luna-Cárdenas, Amber Macintyre, Filip Milosevic, Matt Mitchell, Bianca Mondo, Brad Murray, Megha Rajagopalan, Laura Ranca, Mario Rautner, Gabi Sobliye, Nuria Tesón, Carolyn Thompson, Marek Tuszynski, Jose Felix Farachala Valle, Chris Walker, Johanna Wild

Editors: Natalie Holmes, Christy Lange, Karolle Rabarison, Laura Ranca, Michael Runyan, Sasha Gubskaya

Design: Tactical Tech's design team - Cade Diehm (design lead), Ida Flik, Yiorgos Bagakis, Philipp Dollinger

Developers for the online Kit: Jacopo Anderlini, Laurent Delleré, Wael Eskandar, Zach Green, Danja Vasiliev, Chris Walker

Illustrations: Ann Kiernan

Communications: Daisy Kidd

Project Team Behind The Kit: Wael Eskandar, Christy Lange, Matt Mitchell, Laura Ranca, Gabriela Rodriguez Berón, Marek Tuszynski, Chris Walker, Leil Zahra

Special Thanks: This kit would not have been possible without our collaboration with Share Lab and Share Foundation in co-hosting the 2017 Data Investigation Camp and the 2018 Citizen Investigation Kit Residency.

The Kit would also not have been possible without the hard work of Exposing the Invisible's former project lead Gabi Sobliye.

Special, special thanks to the Perast Group!

**TACTICAL
TECH**

Making sense of
the digital

EXPOSING THE INVISIBLE

Exposing the Invisible (ETI) is a Tactical Tech project that actively experiments with ways to promote investigation as one of the most important forms of public engagement. Through a series of films, interviews, guides and resources, ETI looks at different techniques, tools and methods along with the individual practices of those working at the new frontiers of investigation.

exposingtheinvisible.org

eti@tacticaltech.org

GPG Key fingerprint: BD30 C622 D030 FCF1 38EC C26D DD04 627E 1411 0C02

Tactical Tech

Tactical Tech is a Berlin-based non-profit organisation that investigates the evolving impact of digital technologies on society. Through our work we aim to educate, advocate and create practical solutions that contribute to the wider socio-political debate around digital security, privacy and the ethics of data.

tacticaltech.org

[@info_activism](https://twitter.com/info_activism)

facebook.com/tactical.tech

ttc@tacticaltech.org

GPG Key fingerprint: 0X9B7146F981654FBEE17A0CAAF6B047919EC6096D

This Kit was possible thanks to the support of:



and Tactical Tech's other funders.

Licensing:

CC BY-SA 4.0

The Kit is licensed under a Creative Commons Attribution-ShareAlike 4.0

International license

Tactical Tech 2020



**TACTICAL
TECH**

Making sense of
the digital