# VERIFICATION HANDBOOK

## FOR INVESTIGATIVE REPORTING

A GUIDE TO ONLINE SEARCH AND RESEARCH TECHNIQUES FOR USING UGC AND OPEN SOURCE INFORMATION IN INVESTIGATIONS

European Journalism Centre

EDITED BY CRAIG SILVERMAN

EDITOR OF 'REGRET THE ERROR', THE POYNTER INSTITUTE

# Chapter 1: The opportunity for using open source information and user-generated content in investigative work

**Craig Silverman** is the founder of Emergent, a real-time rumor tracker and debunker. He was a fellow with the Tow Center for Digital Journalism at Columbia University, and is a leading expert on media errors, accuracy and verification. Craig is also the founder and editor of Regret the Error, a blog about media accuracy and the discipline of verification that is now a part of the Poynter Institute. He edited the Verification Handbook, previously served as director of content for Spundge, and helped launch OpenFile, an online local news startup that delivered community-driven reporting in six Canadian cities. Craig is also the former managing editor of PBS MediaShift and has been a columnist for The Globe And Mail, Toronto Star, and Columbia Journalism Review. He tweets at @craigsilverman.

**Rina Tsubaki** leads and manages the "Verification Handbook" and "Emergency Journalism" initiatives at the European Journalism Centre in the Netherlands. Emergency Journalism brings together resources for media professionals reporting in and about volatile situations in the digital age, and Tsubaki has frequently spoken on these topics at events, including a U.N. meeting and the International Journalism Festival. Earlier, she managed several projects focusing on the role of citizens in the changing media landscape, and in 2011 she was the lead contributor of the Internews Europe's report on the role of communication during the March 2011 Japan quake. She has also contributed to Hokkaido Shimbun, a regional daily newspaper in Japan. She tweets at @wildflyingpanda.

With close to 18,000 followers, the Twitter account @ShamiWitness has been a major source of pro-Islamic State propaganda. In their investigation of the account, British broadcaster Channel 4 reported that ShamiWitness' tweets "were seen two million times each month, making him perhaps the most influential Islamic State Twitter account." Channel 4 also reported that two-thirds of Islamic State foreign fighters on Twitter follow the account.

Channel 4 set out to investigate who was behind the account. All it had to go on was the account and its tweets — the person behind ShamiWitness had never shared personal information or anything that might indicate where they were based.

Simon Israel, the Channel 4 correspondent who led the investigation, said in the report that there were no known photos of ShamiWitness.

"But there are moments — and there are always moments — when the hidden trip up," he said.

Israel said an analysis of the ShamiWitness account revealed that it used to go by a different handle on

Twitter: @ElSaltador. At some point, the account owner changed it to @ShamiWitness.

Channel 4 investigators took that previous Twitter handle and searched other social networks to see if they could find anyone using it. That led them to a Google+ account, and then to a Facebook page. There they found photos and other details about a man living in Bangalore who worked as a marketing executive for an Indian company. Soon, they had him on the phone: He confirmed that he was behind the ShamiWitness account.

The result was an investigative story broadcast in December 2014. That report caused the man behind the Twitter account to stop tweeting.

Channel 4 used publicly available data and information to produce journalism that shut down a key source of propaganda and recruitment for the Islamic State.

Journalists, human rights workers and others are constantly making use of open data, user-generated content and other open source information to produce critically important investigations of everything from conflict zones to human rights abuse cases and international corruption.

> "Open source information, which is information freely available to anyone through the Internet — think YouTube, Google Maps, Reddit — has made it possible for ANYONE to gather information and source others, through social media networks," wrote Eliot Higgins on the Kickstarter campaign page for his open source investigations website, Bellingcat. "Think the Syrian Civil War. Think the Arab Spring."

The abundance of open source information available online and in databases means that just about any investigation today should incorporate the search, gathering and verification of open source information. This has become inseparable from the work of cultivating sources, securing confidential information and other investigative tactics that rely on hidden or less-public information. Journalists and other who develop and maintain the ability to properly search, discover, analyze and verify this material will deliver better, more comprehensive investigations.

Higgins, who also goes by the pseudonym Brown Moses, is living proof of the power of open source information when combined with dedication and strong verification practices. He has become an internationally recognized expert in the Syrian conflict and the downing of Flight MH17 in Ukraine, to name but two examples. His website, Bellingcat, is where he and others now use open source materials to produce unique and credible investigate work.

In February 2015, Bellingcat launched a project to track the vehicles being used in the conflict in Ukraine. They invited the public to submit images or footage of military vehicles spotted in the conflict zone, and to help analyze images and footage that had been discovered from social networks and other sources. In its first week of operation, the project added 71 new entries to the vehicles database, almost doubling the amount of information they had previously collected. These were photos, videos and

other pieces of evidence that were gathered from publicly available sources, and they told the story of the conflict in a way no one had before.

It's all thanks to open source information and user-generated content. As chapters and case studies in this Handbook detail, this same material is being used by investigative journalists in Africa and by groups such as Amnesty International and WITNESS to expose fraud, document war crimes and to help the wrongly accused defend themselves in court.

This companion to the original Verification Handbook offers detailed guidance and illustrative case studies to help journalists, human rights workers and others verify and use open source information and user-generated content in service of investigative projects.

With so much information circulating and available on social networks, in public databases and via other open sources, it's essential that journalists and others are equipped with the skills and knowledge to search, research and verify this information in order to use it in accurate and ethical ways.

This Handbook provides the fundamentals of online search and research techniques for investigations; details techniques for UGC investigations; offers best practices for evaluating and verifying open data; provides workflow advice for fact-checking investigative projects; and outlines ethical approaches to incorporating UGC in investigations.

The initial Verification Handbook focused on verification fundamentals and offered step-by-step guidance on how to verify user-generated content for breaking news coverage. This companion Handbook goes deeper into search, research, fact-checking and data journalism techniques and tools that can aid investigative projects. At the core of each chapter is a focus on enabling you to surface credible information from publicly available sources, while at the same time offering tips and techniques to help test and verify what you've found.

As with the verification of user-generated content in breaking news situations, some fundamentals of verification apply in an investigative context. Some of those fundamentals, which were detailed in the original Handbook, are:

- Develop human sources.
- Contact people, and talk to them.
- Be skeptical when something looks, sounds or seems too good to be true.
- Consult multiple, credible sources.
- Familiarize yourself with search and research methods, and new tools.
- Communicate and work together with other professionals — verification is a team sport.

Journalist Steve Buttry, who wrote the Verification Fundamentals chapter in the original Handbook, said that verification is a mix of three elements:

- A person's resourcefulness, persistence, skepticism and skill
- Sources' knowledge, reliability and honesty, and the number, variety and reliability of sources you can find and persuade to talk
- Documentation

This Handbook has a particular focus on the third element: documentation. Whether it is using search engines more effectively to gather documentation, examining videos uploaded to YouTube for critical evidence, or evaluating data gathered from an entity or database, it's essential that investigators have the necessary skills to acquire and verify documentation.

Just as we know that human memory is faulty and that sources lie, we must also remember that documents and data aren't always what they appear. This Handbook offers some fundamental guidance and case studies to help anyone use open source information and user-generated content in investigations — and to verify that information so that it buttresses an investigation and helps achieve the goal of bringing light to hidden truths.

# Chapter 2: Using online research methods to investigate the Who, Where and When of a person

**Henk van Ess** trains media professionals, teaches internet research, social media and multimedia in Europe. Current projects include 'fact-checking the web', Facebook graph search and data journalism. He works for EBU, Schibsted, Axel Springer Akademie and eight European universities. He is @henkvaness on Twitter.

Online research is often a challenge for traditional investigative reporters, journalism lecturers and students. Information from the web can be fake, biased, incomplete or all of the above.

Offline, too, there is no happy hunting ground with unbiased people or completely honest governments. In the end, it all boils down to asking the right questions, digital or not. This chapter gives you some strategic advice and tools for digitizing three of the biggest questions in journalism: who, where and when?

### 1. Who?

Let's do a background profile with Google on Ben van Beurden, CEO of the Shell Oil Co.

a. *Find facts and opinions*

```
"van beurden is" AROUND(15) shell
```

The simple two-letter word "is" reveals opinions and facts about your subject. To avoid clutter, include the company name of the person or any other detail you know, and tell Google that both words should be not that far from each other.

The AROUND() operator MUST BE IN CAPITALS. It sets the maximum distance in words between the two terms.

b. *What do others say?*

```
filetype:pdf "ben van beurden" -site:shell.*
```

This search is asking Google to “Show me PDF documents with the name of the CEO of Shell in it, but exclude documents from Shell.” This will find documents about your subject, but not from the company of the subject itself. This helps you to see what opponents, competitors or opinionated people say about your subject. If you are a perfectionist, go for

inurl:pdf “ben van beurden” –site:shell.*

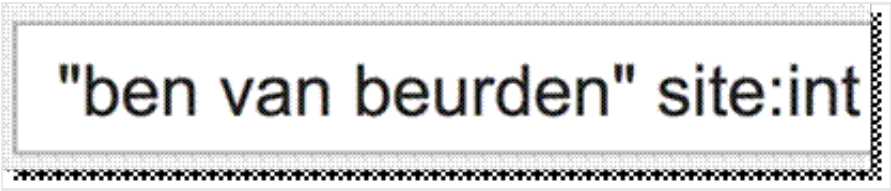
because you will find also PDFs that are not visible with filetype.

c. *Official databases*

Search for worldwide official documents about this person. It searches for gov.uk (United Kingdom) but also .gov.au (Australia), .gov.cn (China), .gov (U.S.) and other governmental websites in the world. If you don’t have a .gov website in your country, use the local word for it with the site: operator. Examples would be site:bund.de (Germany) or site:overheid.nl (The Netherlands).

With this query, we found van Beurden’s planning permission for his house in London, which helped us to find his full address and other details.

d. *United Nations*




You are now searching in any United Nations-related organization. In this example, we find the Shell CEO popping up in a paper about “Strategic Approach to International Chemicals Management.” And we found his full name, the name of his wife, and his passport number at the time when we did this search. Amazing.

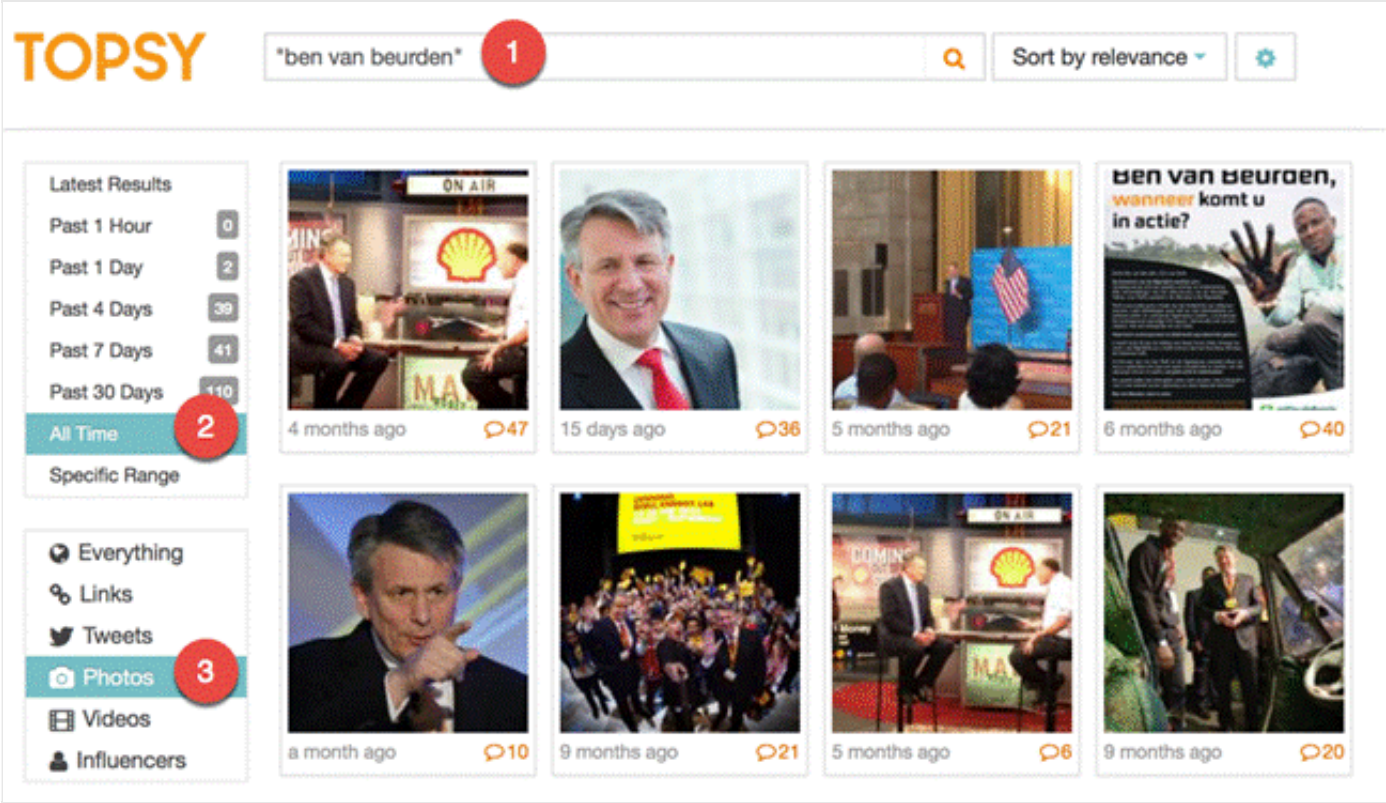
e. *Find the variations*

"mr * van beurden" -ben shell

With this formula you can find result that use different spellings of the name. You will receive documents with the word Shell, but not those that include “Ben” as the first name. With this, you will find out that he is also referred to as Bernardus van Beurden. (You don’t need to enter a dot [.] because Google will ignore points.) Now repeat steps a, b, c and d with this new name.

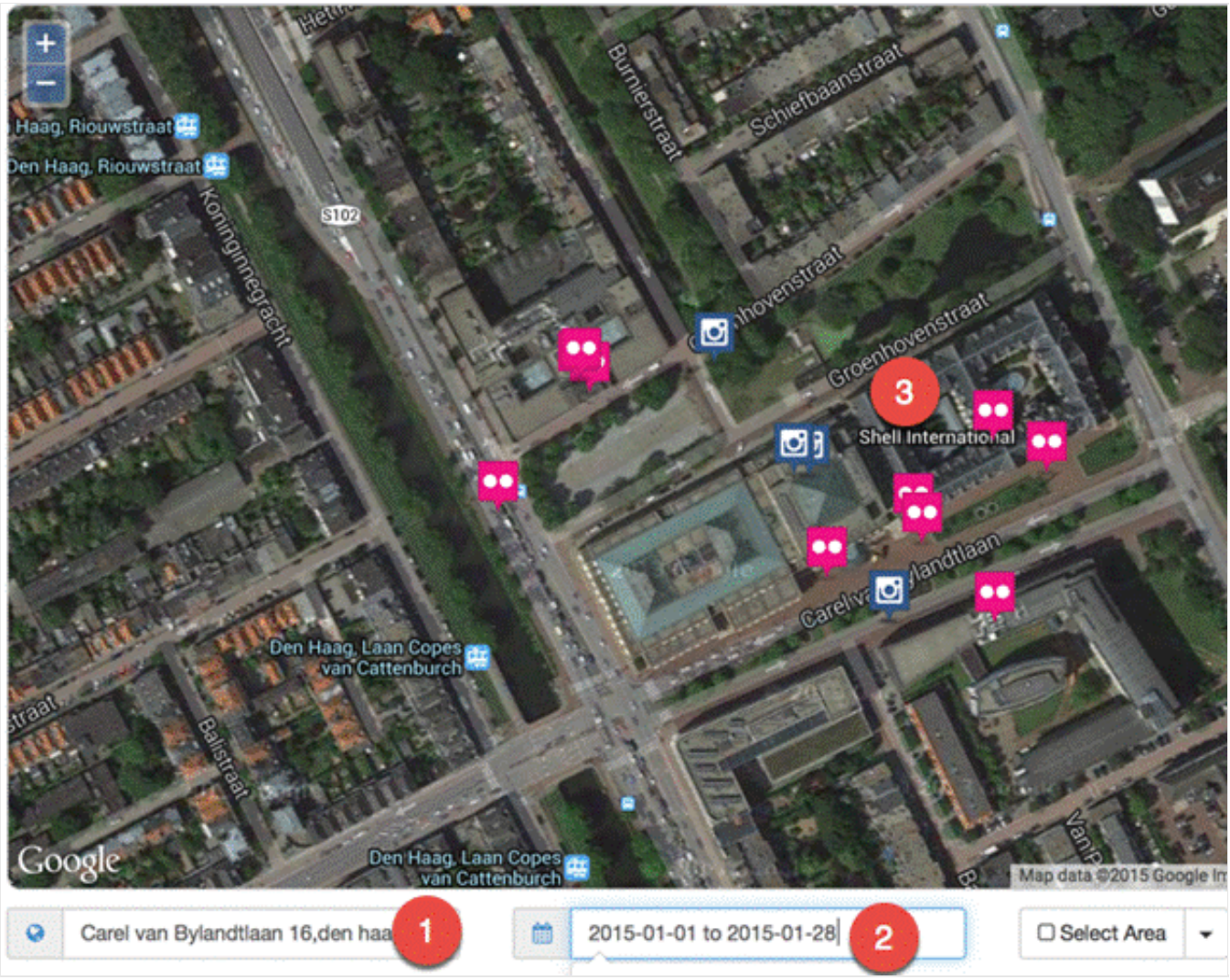
## 2. Where

a. *Use photo search in Topsy*




You can use www.topsy.com to find out where your subject was, by analyzing his mentions (1) over time (2) and by looking at the photos (3) that others posted on Twitter. If you’d rather research a specific period, go for “Specific Range” in the time menu.

b. *Use Echosec*




With Echosec, you can search social media for free. In this example, I entered the address of Shell HQ (1) in hopes of finding recent (2) postings from people who work there (3).

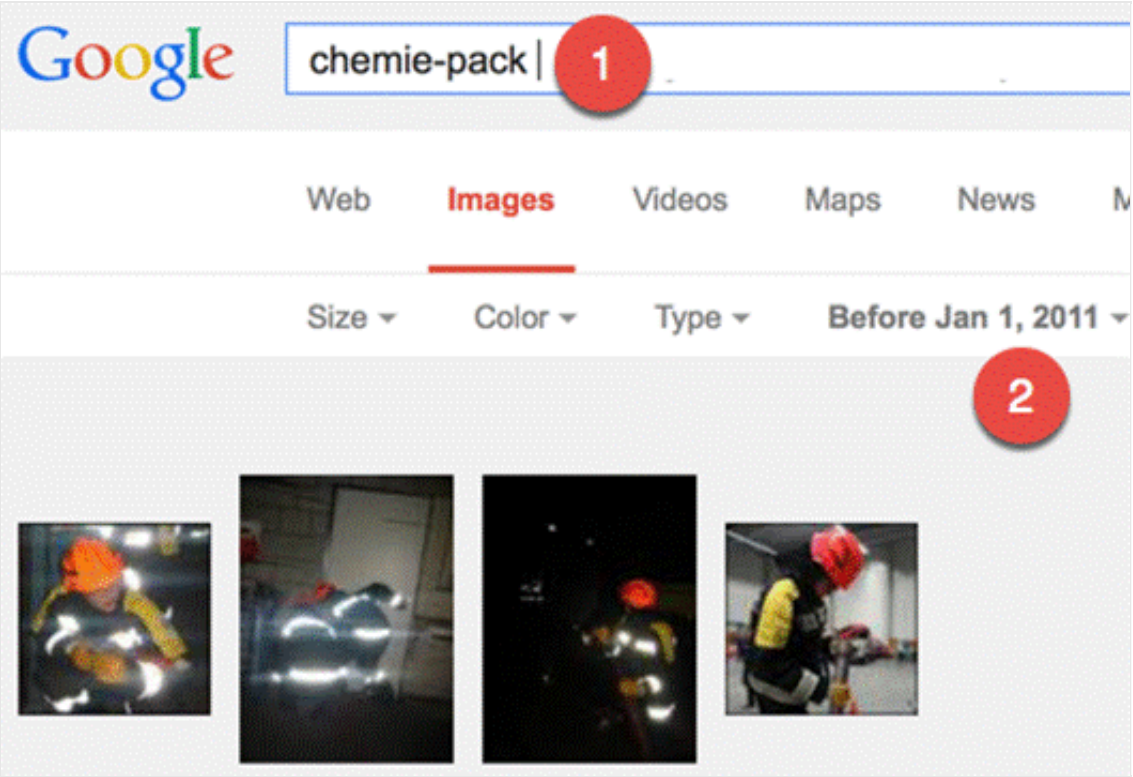
c. *Use photo search in Google Images*

Combine all you know about your subject in one mighty phrase. In the below example, I'm searching for a jihadist called @MuhajiriShaam (1) but not the account @MuhajiriShaam01 (2) on Twitter (3). I just want to see the photos he posted on Twitter between Sept. 25 and Sept. 29, 2014 (4).

## 3. When

a. *Date search*

Most of the research you do is not based on today, but an earlier period. Always tell your search engine this. Go back in time.



Let's investigate a fire in a Dutch chemical plant called Chemie-Pack. The fire happened on Jan. 5, 2011. Perhaps you want to investigate if dangerous chemicals were stored at the plant. Go to images.google.com, type in Chemie-pack (1) and just search before January 2011 (2). The results offer hundreds of photos from a youth fire department that visited the company days before the fire. In some photos, you can see barrels with names of chemicals on them. We used this to establish which chemicals were stored in the plant days before the fire.

b. *Find old data with archive.org*

Websites often cease to exist. There is a chance you can still view them by using archive.org. This tool can do its work only if you know the URL of the webpage you want to see. The problem is that often the link is gone and therefore you don't know it. So how do you find a seemingly disappeared URL?

Let's assume we want to find the home page of a dead actress called Lana Clarkson.

**Step One: Find an index**

Find a source about the missing page. In this case, we can use her Wikipedia page.

**Step Two: Put the index in the time machine**

Go to archive.org and enter the URL of her Wikipedia page, http://en.wikipedia.org/wiki/Lana_Clarkson. Choose the oldest available version, March 10, 2004. There it says the home page was http://www.lanaclarkson.com.

**Step Three: Find the original website**

Now type the link in archive.org, but add a backslash and an asterisk to the URL: https://web.archive.org/web/*/http://www.lanaclarkson.com/*

All filed links are now visible. Unfortunately, in this case, you won't find that much. Clarkson became famous only after her death. She was shot and killed by famed music producer Phil Spector in February 2003.

# Chapter 3: Online research tools and investigation techniques

**Paul Myers** is a BBC internet research specialist. Paul joined the BBC in 1995 as a news information researcher. He also runs The Internet Research Clinic, a website dedicated to directing journalists to the best research links, apps and resources. His role in the BBC Academy sees him organize and deliver training courses related to internet investigation, data journalism, freedom of information, reporting statistics, working with social media, web design and image production. He has worked with leading programmes like Panorama, Watchdog, national news bulletins, BBC Online, local & national radio and the World Service. He is also a regular blogger on the BBC College of Journalism website. Paul has also helped train personnel from The Guardian, the Daily Telegraph, the Times, Channel 4, CNN, the World Bank and the UNDP.

Search engines are an intrinsic part of the array of commonly used "open source" research tools. Together with social media, domain name look-ups and more traditional solutions such as newspapers and telephone directories, effective web searching will help you find vital information to support your investigation.

Many people find that search engines often bring up disappointing results from dubious sources. A few tricks, however, can ensure that you corner the pages you are looking for, from sites you can trust. The same goes for searching social networks and other sources to locate people: A bit of strategy and an understanding of how to extract what you need will improve results.

This chapter focuses on three areas of online investigation:

1. Effective web searching.
2. Finding people online.
3. Identifying domain ownership.

## 1. Effective web searching

Search engines like Google don't actually know what web pages are about. They do, however, know the words that are on the pages. So to get a search engine to behave itself, you need to work out which words are on your target pages.

First off, choose your search terms wisely. Each word you add to the search focuses the results by eliminating results that don't include your chosen keywords.

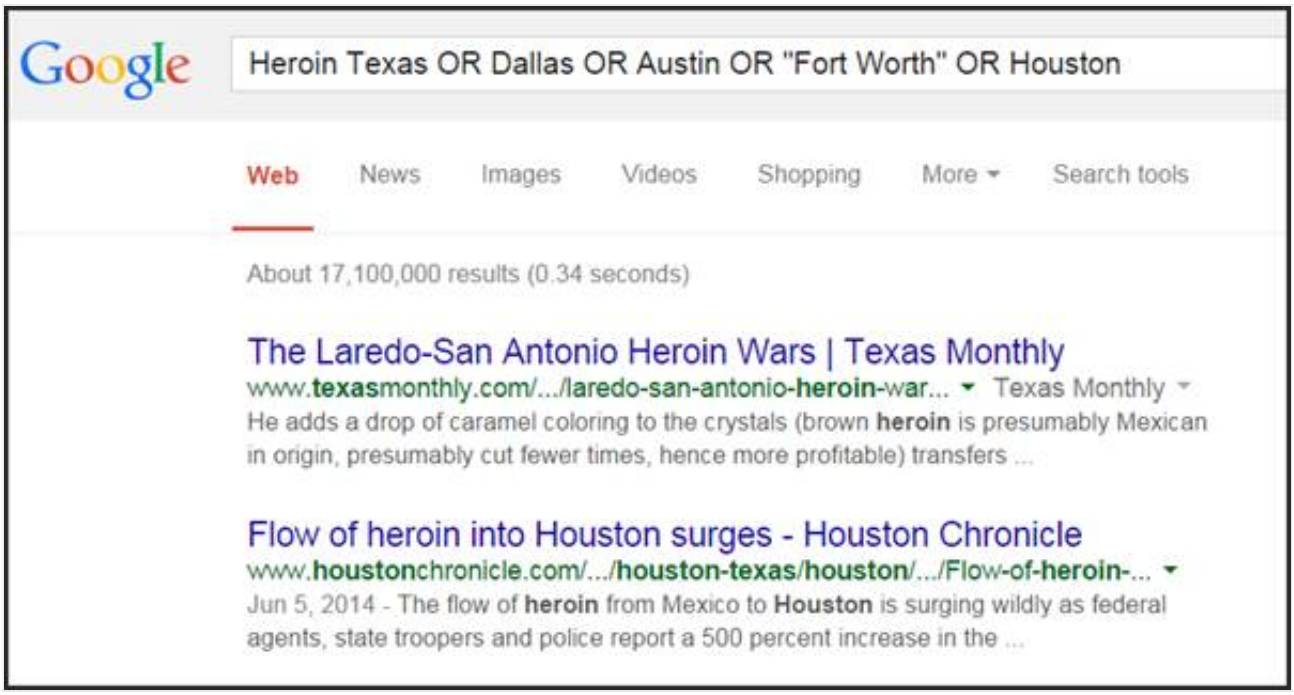
Some words are on every page you are after. Other words might or might not be on the target page. Try to avoid those subjective keywords, as they can eliminate useful pages from the results.

**Use advanced search syntax.**

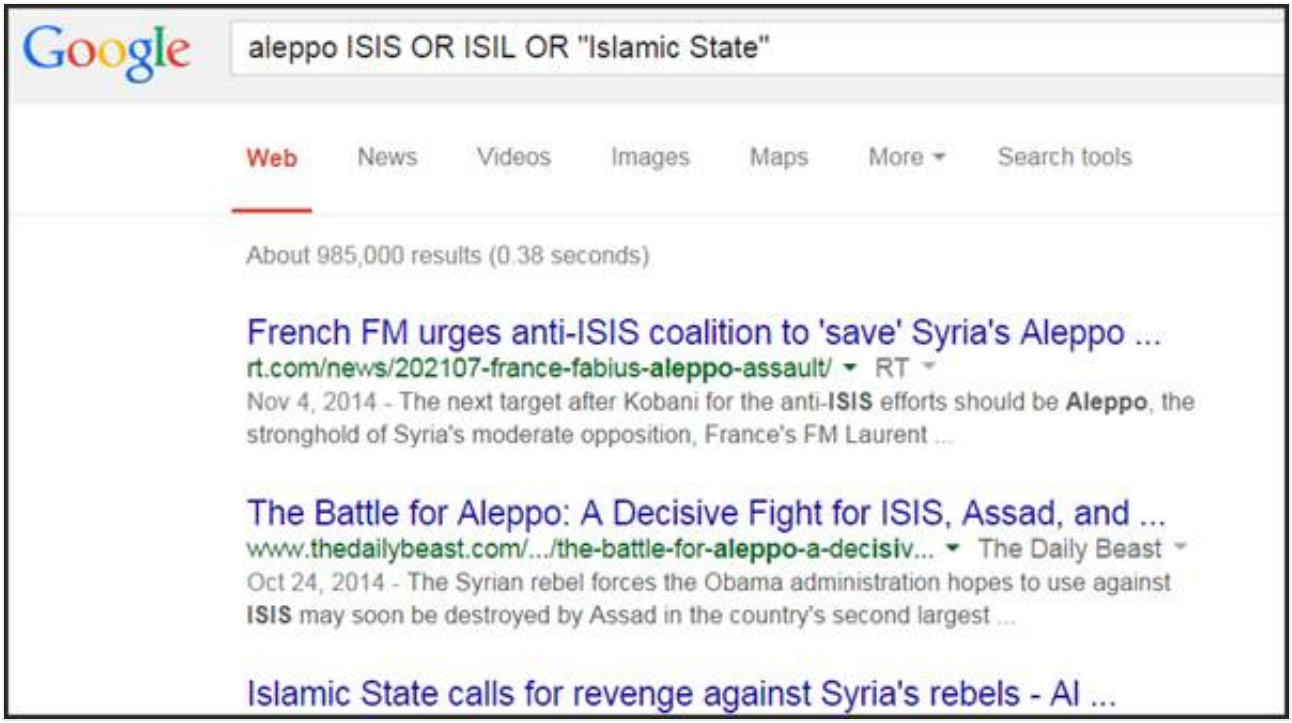
Most search engines have useful so-called hidden features that are essential to helping focus your search and improve results.

*Optional keywords*

If you don't have definite keywords, you can still build in other possible keywords without damaging the results. For example, pages discussing heroin use in Texas might not include the word "Texas"; they may just mention the names of different cities. You can build these into your search as optional keywords by separating them with the word OR (in capital letters).




You can use the same technique to search for different spellings of the name of an individual, company or organization.




*Search by domain*

You can focus your search on a particular site by using the search syntax “site:” followed by the domain name.

For example, to restrict your search to results from Twitter:

To add Facebook to the search, simply use “OR” again:

You can use this technique to focus on a particular company's website, for example. Google will then return results only from that site.

You can also use it to focus your search on municipal and academic sources, too. This is particularly effective when researching countries that use unique domain types for government and university sites.

Note: When searching academic websites, be sure to check whether the page you find is written or maintained by the university, one of its professors or one of the students. As always, the specific source matters.

*Searching for file types*

Some information comes in certain types of file formats. For instance, statistics, figures and data often appear in Excel spreadsheets. Professionally produced reports can often be found in PDF documents. You can specify a format in your search by using "filetype:" followed by the desired data file extension (xls for spreadsheet, docx for Word documents, etc.).

## 2. Finding people

Groups can be easy to find online, but it's often trickier to find an individual person. Start by building a dossier on the person you're trying to locate or learn more about. This can include the following:

- The person's name, bearing in mind:
    - Different variations (does James call himself "James," "Jim," "Jimmy" or "Jamie"?).
    - The spelling of foreign names in Roman letters (is Yusef spelled "Yousef" or "Yusuf"?).
    - Did the names change when a person married?
    - Do you know a middle name or initial?
- The town the person lives in and or was born in.
- The person's job and company.

- Their friends and family members' names, as these may appear in friends and follower lists.
- The person's phone number, which is now searchable in Facebook and may appear on web pages found in Google searches.
- Any of the person's usernames, as these are often constant across various social networks.
- The person's email address, as these may be entered into Facebook to reveal linked accounts. If you don't know an email address, but have an idea of the domain the person uses, sites such as email-format can help you guess it.
- A photograph, as this can help you find the right person, if the name is common.

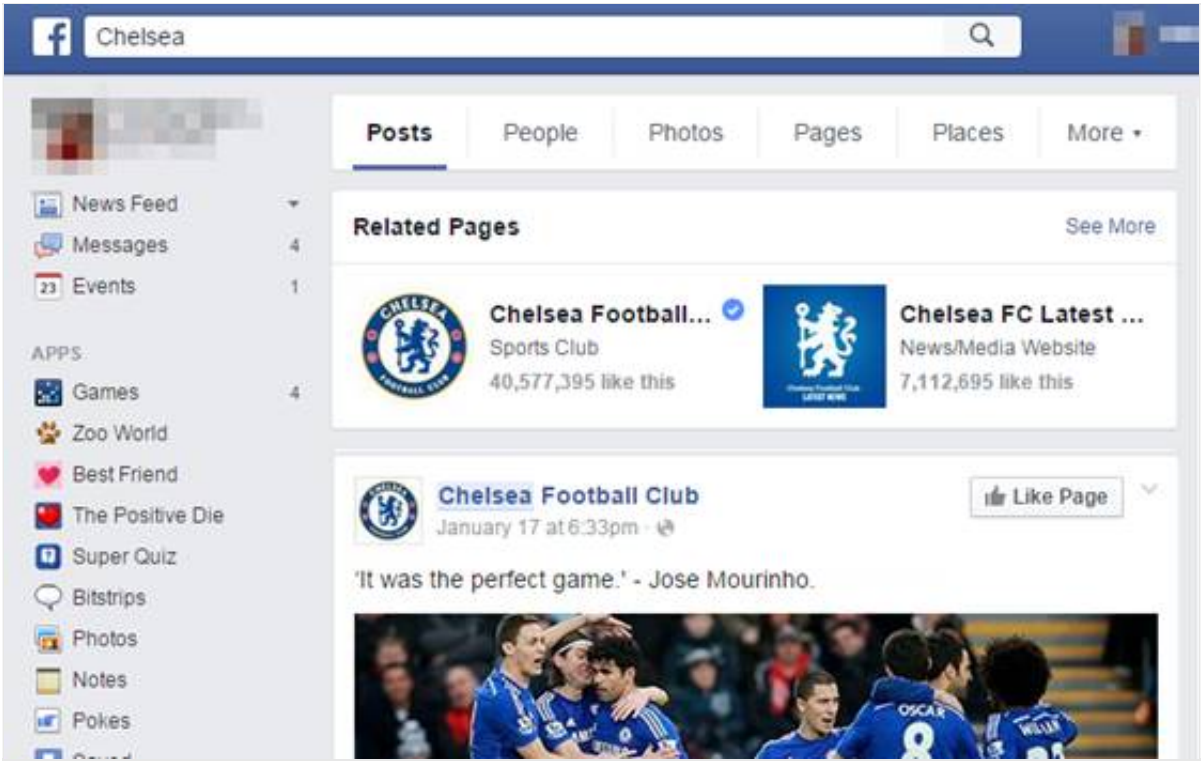
*Advanced social media searches: Facebook*

Facebook's newly launched search tool is amazing. Unlike previous Facebook searches, it will let you find people by different criteria including, for the first time, the pages someone has Liked. It also enables you to perform keyword searches on Facebook pages.

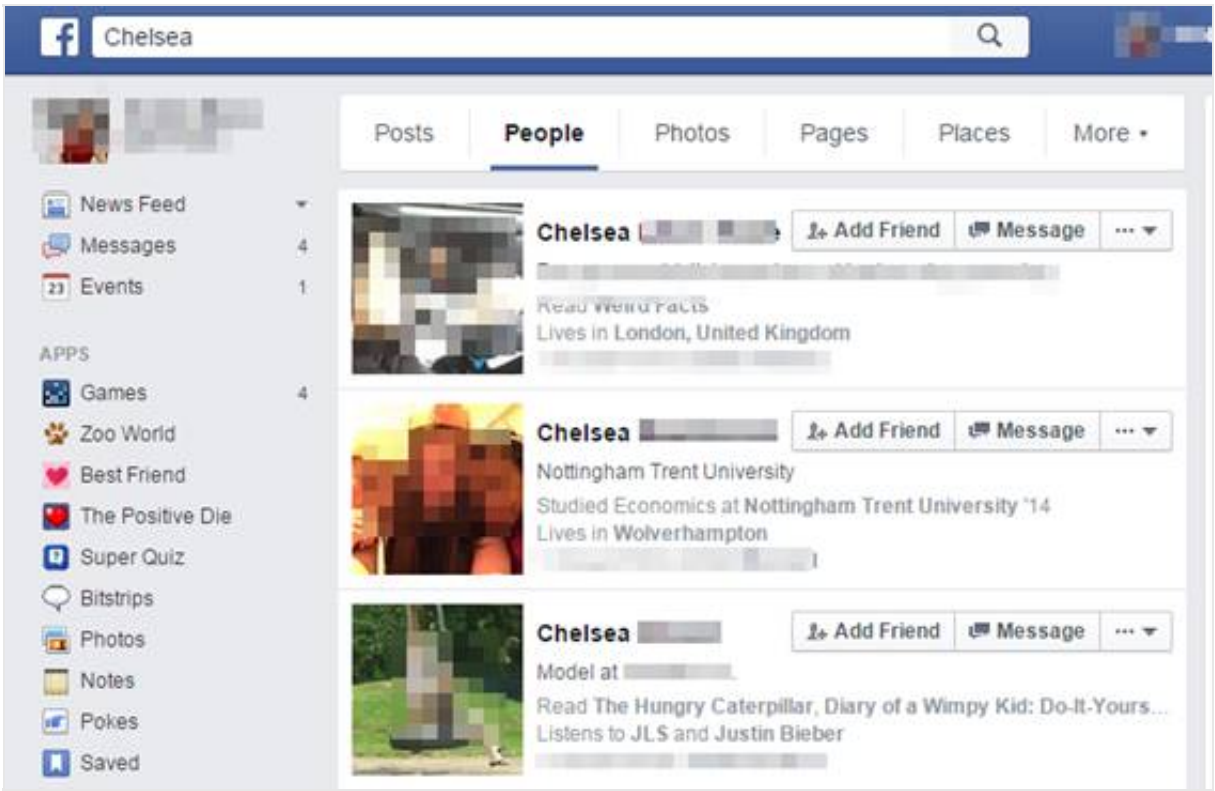
This keyword search, the most recent feature, sadly does not incorporate any advanced search filters (yet). It also seems to restrict its search to posts from your social circle, their favorite pages and from some high-profile accounts.

Aside from keywords in posts, the search can be directed at people, pages, photos, events, places, groups and apps. The search results for each are available in clickable tabs.

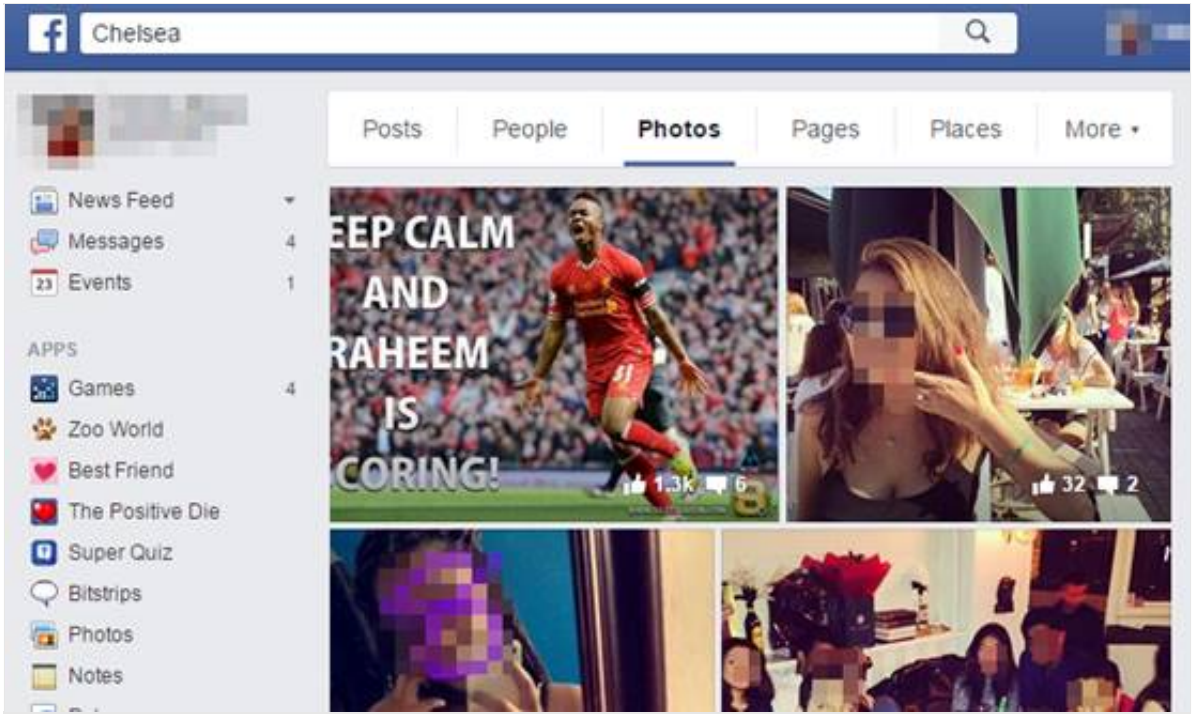
For example, a simple search for Chelsea will find bring up related pages and posts in the Posts tab:




The People tab brings up people named Chelsea. As with the other tabs, the order of results is weighted in favor of connections to your friends and favorite pages.




The Photos tab will bring up photos posted publicly, or posted by friends that are related to the word Chelsea (such as Chelsea Clinton, Chelsea Football Club or your friends on a night out in the Chelsea district of London).




The real investigative value of Facebook's search becomes apparent when you start focusing a search on what you really want.

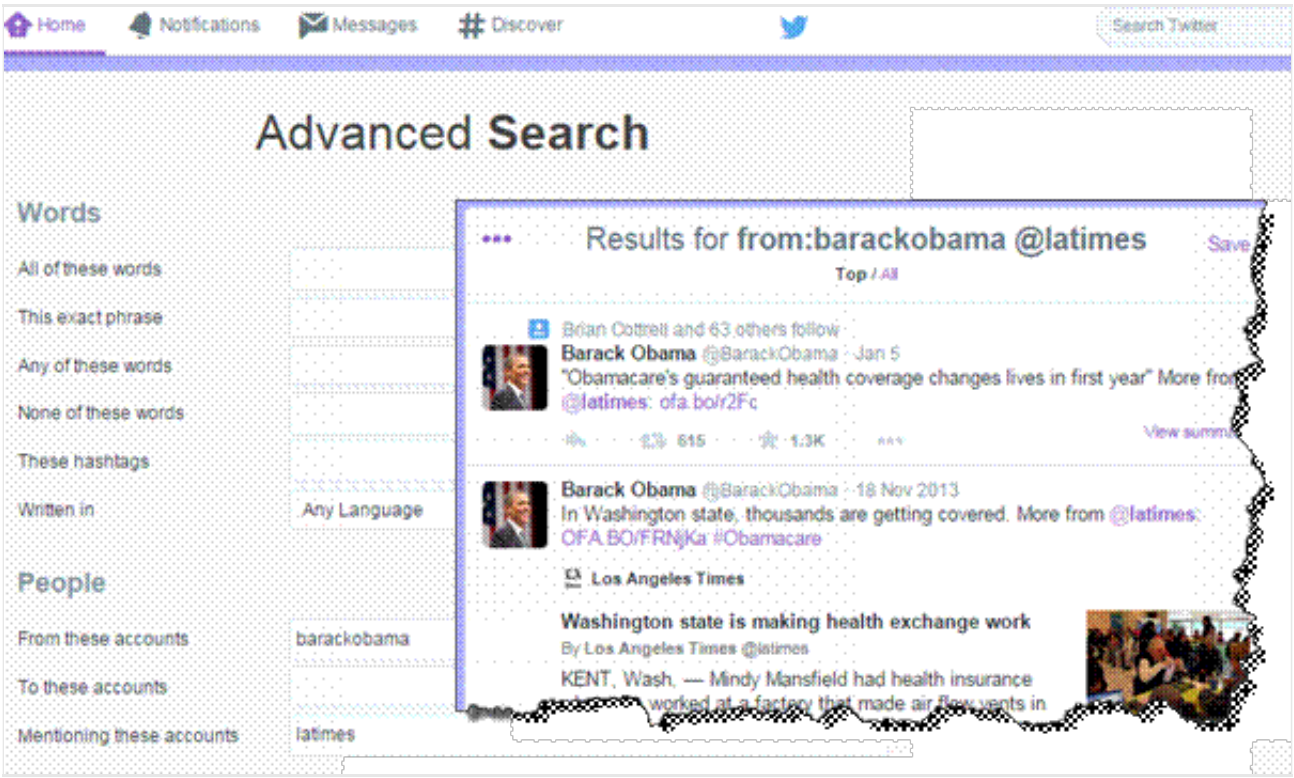
For example, if you are investigating links between extremist groups and football, you might want to search for people who like The English Defence League and Chelsea Football Club. To reveal the results, remember to click on the "People" tab.

This search tool is new and Facebook are still ironing out the creases, so you may need a few attempts at wording your search. That said, it is worth your patience.

Facebook also allows you to add all sorts of modifiers and filters to your search. For example, you can specify marital status, sexuality, religion, political views, pages people like, groups they have joined and areas they live or grew up in. You can specify where they studied, what job they do and which company they work for. You can even find the comments that someone has added to uploaded photos. You can find someone by name or find photos someone has been tagged in. You can list people who have participated in events and visited named locations. Moreover, you can combine all these factors into elaborate, imaginative, sophisticated searches and find results you never knew possible. That said, you may find still better results searching the site via search engines like Google (add "site:facebook.com" to the search box).

*Advanced social media searches: Twitter*

Many of the other social networks allow advanced searches that often go far beyond the simple "keyword on page" search offered by sites such as Google. Twitter's advanced search, for example, allows you to trace conversations between users and add a date range to your search.




Twitter allows third-party sites to use its data and create their own exciting searches. Followerwonk, for example, lets you search Twitter bios and compare different users. Topsy has a great archive of tweets, along with other unique functionality.

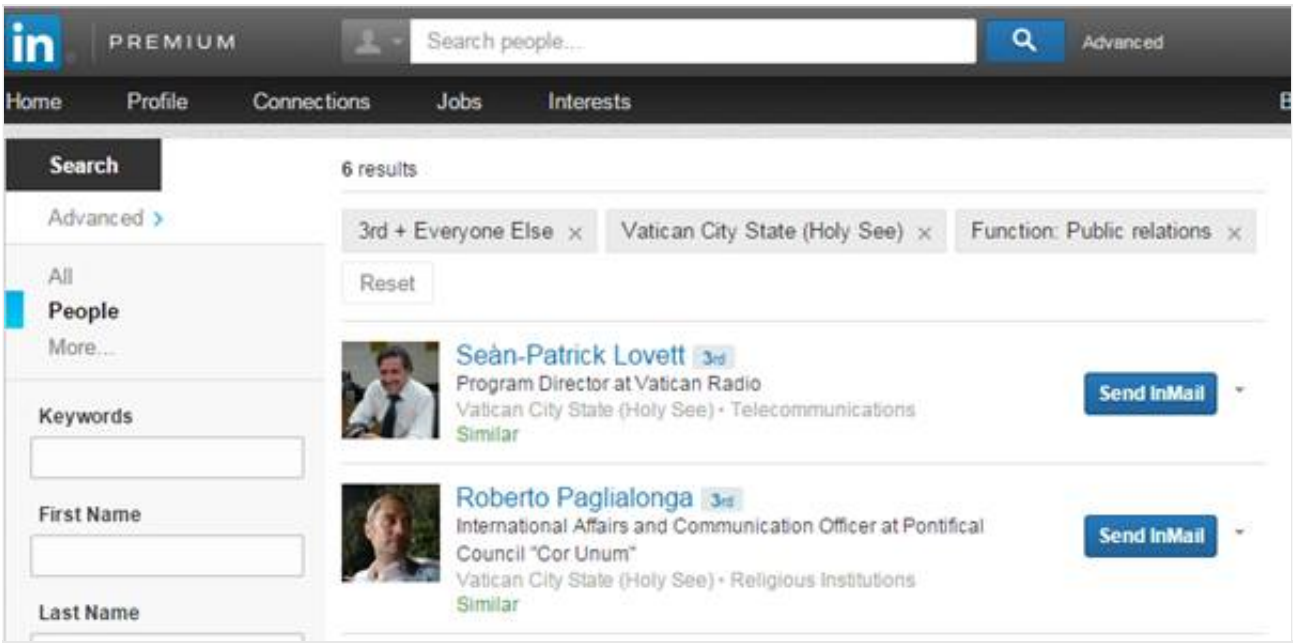
*Advanced social media searches: LinkedIn*

LinkedIn will let you search various fields including location, university attended, current company, past company or seniority.

You have to log in to LinkedIn in order to use the advanced search, so remember to check your privacy settings. You wouldn't want to leave traceable footprints on the profile of someone you are investigating!

You can get into LinkedIn's advanced search by clicking on the link next to the search box. Be sure, also, to select "3rd + Everyone Else" under relationship. Otherwise , your search will include your friends and colleagues and their friends.

LinkedIn was primarily designed for business networking. Its advanced search seems to have been designed primarily for recruiters, but it is still very useful for investigators and journalists. Personal data exists in clearly defined subject fields, so it is easy to specify each element of your search.




You can enter normal keywords, first and last names, locations, current and previous employers, universities and other factors. Subscribers to their premium service can specify company size and job role.

LinkedIn will let you search various fields including location, university attended, current company, past company and seniority.

*Other options*

Sites like Geofeedia and Echosec allow you to find tweets, Facebook posts, YouTube videos, Flickr and Instagram photos that were sent from defined locations. Draw a box over a region or a building and reveal the social media activity. Geosocialfootprint.com will plot a Twitter user's activity onto a map (all assuming the users have enabled location for their accounts).

Additionally, specialist "people research" tools like Pipl and Spokeo can do a lot of the hard legwork for your investigation by searching for the subject on multiple databases, social networks and even dating websites. Just enter a name, email address or username and let the search do the rest. Another option is to use the multisearch tool from Storyful. It's a browser plugin for Chrome that enables you to enter a single search term, such as a username, and get results from Twitter, Instagram, YouTube, Tumblr and Spokeo. Each site opens in a new browser tab with the relevant results.

*Searching by profile pic*

People often use the same photo as a profile picture for different social networks. This being the case, a reverse image search on sites like TinEye and Google Images, will help you identify linked accounts.

## 3. Identifying domain ownership

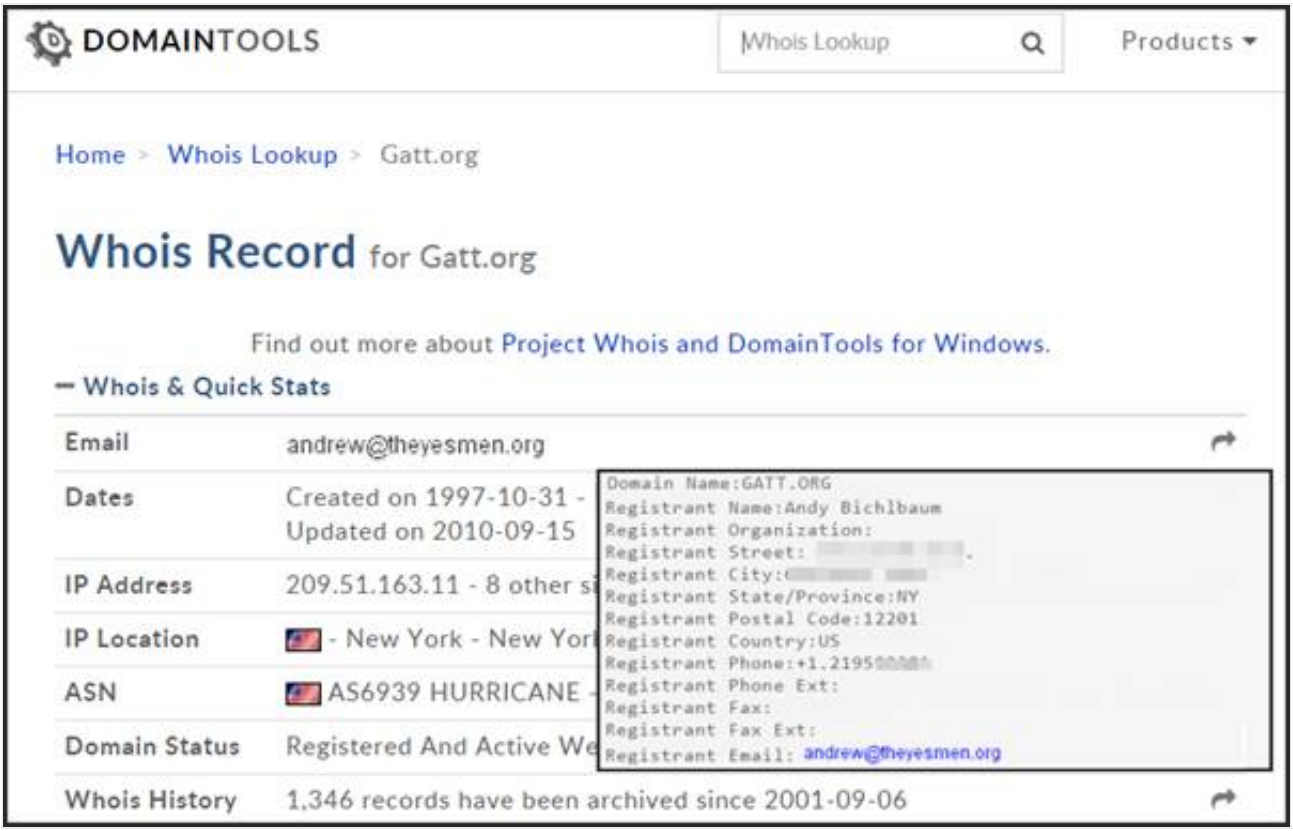
Many journalists have been fooled by malicious websites. Since it's easy for anyone to buy an unclaimed .com, .net or .org site, we should not go on face value. A site that looks well produced and has authentic-sounding domain name may still be a political hoax, false company or satirical prank.

Some degree of quality control can be achieved by examining the domain name itself. Google it and see

what other people are saying about the site. A “whois” search is also essential. DomainTools.com is one of many sites that offers the ability to perform a whois search. It will bring up the registration details given by the site owner the domain name was purchased.

For example, the World Trade Organization was preceded by the General Agreement on Tariffs and Trades (GATT). There are, apparently, two sites representing the WTO. There’s wto.org (genuine) and gatt.org (a hoax). A mere look at the site hosted at gatt.org should tell most researchers that something is wrong, but journalists have been fooled before.

A whois search dispels any doubt by revealing the domain name registration information. Wto.org is registered to the International Computing Centre of the United Nations. Gatt.org, however, is registered to “Andy Bichlbaum” from the notorious pranksters the Yes Men.




Whois is not a panacea for verification. People can often get away with lying on a domain registration form. Some people will use an anonymizing service like Domains by Proxy, but combining a whois search with other domain name and IP address tools forms a valuable weapon in the battle to provide useful material from authentic sources

# Chapter 4: Corporate Veils, Unveiled: Using databases, domain records and other publicly available material to investigate companies

**Khadija Sharife** an investigative researcher and writer, coordinates Africa forensics research at Investigative Dashboard (ID) and is a senior researcher for the African Network of Centers for Investigative Reporting (ANCIR). She is the author and co-author of several books including, "Tax Us If You Can: Africa." Her articles have been published in mainstream and academic journals. She is based in South Africa.

Everything has a paper trail, a lead that exposes the systemic underwire of a network, company, or person's illicit or illegal activities. The trick is to find it.

Recently, the African Network of Centers for Investigative Reporting (ANCIR) investigated a global Ponzi scheme controlled by a U.K.-based director, Renwick Haddow. He was the man at the top of an entity called Capital Organisation, which used a network of more than 30 shell companies to sell more than $180 million in fraudulent investments over five years.

It was a global network of interconnected entities, and our organization had a total budget of $500 to investigate and expose it. That budget was entirely invested in our Sierra Leone journalist who was needed to visit a farm related to the scam, meet the locals, and to extract documents from the relevant ministries. That left us with zero budget for other aspects of the story, including the financial trail.

How did we unravel the scam? By finding and following the paper trail, which in this case involved accessing a range of information from databases, corporate brochures, court records and other publicly available sources. All of the evidence we gathered is accessible here, and you can read our full investigation, "Catch and Release", in the Spring 2015 issue of World Policy Journal.

### Anatomy of a scam

The scam used the shell companies to peddle fabricated investments in far-off locations to investors, particularly U.K. pensioners. The purported investments ranged from agricultural (farms producing palm oil, rice, cocoa and wheat) to minerals (gold, platinum, diamonds) as well as properties, water bonds, Voice Over Internet Protocol, and more. High returns were promised, often with guaranteed exit strategies, which assured investors they could recoup their money with a profit.

Shell entities with names such as Agri Firma, Capital Carbon Credits and Voiptel International had no staff, bank accounts, offices or other components of real business. Instead, Haddow and his crew channeled money to financial receiving agents who then deposited it into tax havens such as Cyprus. Then final remittance was made to British Virgin Islands holding companies such as Rusalka and

Glenburnie Investment.

The shell entities promoted investment schemes that were unregulated or lightly regulated by the U.K.'s Financial Conduct Authority (FCA). The investments were then promoted through fictitious brokers carrying names such as Capital Alternatives, Velvet Assets, Premier Alternatives, Able Alternatives and others. These entities were based in the U.K. and eventually spread around the world from Gibraltar to Dubai. They often consisted of nothing more than short-term or mailbox offices. Many even shared the same telephone number or address.

On the front line of the scam were often unscrupulous sales agents who were incentivized with commissions of between 25 and 40 percent of what they sold as new investments. The rest would be transferred as "investment arrangement fees" to the private offshore accounts of architects such as Renwick Haddow, Robert McKendrick and other key players.

## Following the trail

The most important aspects of any investigation are to dig, listen and ask pertinent questions. But asking questions requires context, and listening to the right sources means finding the core of the story. Data, free or otherwise, can never replace good investigative research. In order to do good investigative research, these days, one must become familiar with how and where knowledge can be found, and how best to access and develop it.

Court documents showed us that this was not the first time that some of the people and entities in this scam had been investigated. Though the court document in question only looked at a seemingly minor question — whether it was a collective or individual scheme — the process often yields evidence and leads that may otherwise not be available.

We gathered corporate brochures that listed financial receiving agents, brokers, auditors, physical offices and other details that detailed connections between seemingly independent companies.

Our work made use of free public databases such as Duedil that allow for individual and corporate director searches. These enable users to identify the number of companies — current, dissolved, etc. — that a director is involved in. It can also provide other important information: Shareholders, registered offices and a timeline of retired and current individuals involved. We also used LinkedIn to probe prior personal and corporate connections.

Some free resources such as Duedil worked well for the U.K.-connected companies in this investigation. We followed up specific aspects with Companies House, Orbis and other corporate data sites, all of which are accessible for free to journalists via the Investigative Dashboard. The Dashboard "links to more than 400 online databases in 120 jurisdictions where you can search for information on persons and businesses of interest."

The African Network of Centers for Investigative Reporting plays a role in coordinating the Dashboard's Africa department. Unlike other jurisdictions, African countries often do not have digitized or electronically accessible data. To this end, we train and deploy in-country researchers to physically obtain not just the updated and accurate corporate, land, court and other data, but also to visit critical locations, conduct basic interviews and take relevant photos, among other things.

Along with databases, we used Whois Internet searches where possible to determine the date of creation and ownership information of websites that were connected to the network. We then cross-referenced the contact details of the websites with the information listed in corporate databases for the brokers and shell entities. Using specific search phrases, we were able to draw out mentions of certain names, companies, products etc. from various files on the Internet. We also searched for news articles about the people and companies identified in the network. We soon discovered that their ranks included murderers, money launderers and the like.

As part of the investigation, we also created dummy profiles on social media to enable us to connect with relevant companies and individuals, and to engage in email communication. We posed as potential investors to gain firsthand access to the push and pull of the scam.

A critical aspect of reporting was done in person. Once it was clear that Sierra Leone was a focal point of the story, we invested the $500 allocated from Open Society West Africa (OSIWA) to secure an in-country researcher, Silas Gbandia. He physically double-checked whether land leases were correctly entered, and if not, which sections or aspects were excluded.

Most investors in our story presumed the land leases were legitimate. Yet in all cases, the right to sublease by investors was not legal. Some land leases were not entered into the Sierra Leone official registry and therefore were not legitimate (such as those involving palm oil). At least one land lease was totally fraudulent; others were only partially legitimate. The use of in-country researchers to pull the registered land leases could not have more invaluable.

We used sourceAfrica, a free service by ANCIR, to annotate, redact and publish critical documents, including those sent to us by carefully cultivated and trusted sources.

Finally, with all of our information collected, we connected with Heinrich Böhmke, a South African prosecutor and an in-house expert at ANCIR, to "cross-examine" our evidence. This is a process Böhmke took from the legal world and adapted for investigative journalism. We looked for bias, contradictions, consistency and probability within evidence, resources, interviews and sources. A detailed guide to cross-examination for journalists is available here. (Along with Böhmke, we relied on Giovanni Pellerano, ANCIR's in-house tech specialist, to help extract metadata from multiple electronic sources and documents.)

In the end, by identifying the broad relations within, and between, people, companies, jurisdictions,

receiving agents and products, and by studying the corporate data from Duedil, Companies House and others, we were able to visualize the network's structure. This told us how the scheme functioned and who was involved.

Much of this work was enabled by the analysis and investigation of publicly accessible information and documents. This data helped map the activity, people and entities in question and gave us the information we needed to further this investigation.

## Key Questions

The bottom line is that it doesn't take a genius to develop a good investigation or to lift the corporate veil — it simply takes curiosity, technique and a commitment to read as much and as far into the issue as possible. Scour as many data sources as possible: Corporate, media, NGO, shipping, sanctions, land… Look for what is not obvious, seems illogical, or that just plain sticks out to you. Follow your instinct. Ask as many questions as possible. For example, when investigating a corporate entity pursue questions such as:

- What does the company do?
- How many employees does it have? Who are they?
- In which countries does it operate?
- In which countries is it incorporated?
- What are the names of linked companies in each country of operation?
- Where does it pay taxes?
- Where does it report its profits?
- What is the extent of transfer pricing among its subsidiaries?
- Which companies use this practice and why? (And where?)

Remember, everything has a paper trail.

# Chapter 5: Investigating with databases: Verifying data quality

**Giannina Segnini** is currently visiting professor at the Journalism School at Columbia University in New York. Until February 2014, Segnini headed a team of journalists and engineers at La Nacion, in Costa Rica. The team was fully dedicated to delivering investigative stories by gathering, analyzing and visualizing public databases. Since 2000, Segnini has trained hundreds of journalists on investigative journalism, Computer Assisted Reporting (CAR) and data journalism in Latin America, the United States, Europe and Asia.

Segnini earned the Jorge Vargas Gene National Journalism Award three times, the National Award on Journalism Pio Víquez, the Excellence Award in Journalism Gabriel García Márquez, the Ortega y Gasset Prize from daily El País, in Spain, the award to the Best Journalistic Investigation of a Corruption Case by Transparency International for Latin America and the Caribbean (TILAC), and a the Maria Moors Cabot award by the Columbia University. Segnini was previously a Nieman Fellow (2001-2002) at Harvard University.

Never before have journalists had so much access to information. More than three exabytes of data — equivalent to 750 million DVDs — are created every day, and that number duplicates every 40 months. Global data production is today being measured in yottabytes. (One yottabye is equivalent to 250 trillion DVDs of data.) There are already discussions underway about the new measurement needed once we surpass the yottabyte.

The rise in the volume and speed of data production might be overwhelming for many journalists, many of whom are not used to using large amounts of data for research and storytelling. But the urgency and eagerness to make use of data, and the technology available to process it, should not distract us from our underlying quest for accuracy. To fully capture the value of data, we must be able to distinguish between questionable and quality information, and be able to find real stories amid all of the noise.

One important lesson I've learned from two decades of using data for investigations is that data lies — just as much as people, or even more so. Data, after all, is often created and maintained by people.

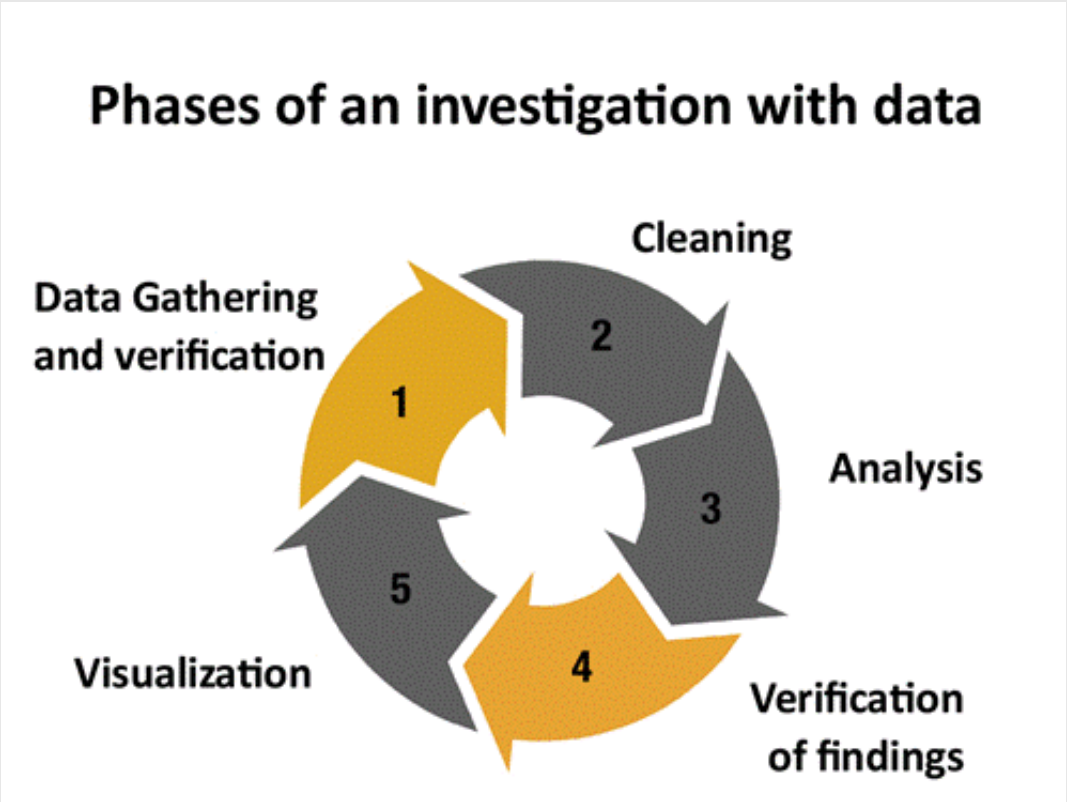
Data is meant to be a representation of the reality of a particular moment of time. So, how do we verify if a data set corresponds to reality?

Two key verification tasks need to be performed during a data-driven investigation: An initial evaluation must occur immediately after getting the data; and findings must be verified at the end of the investigation or analysis phase.

### A. Initial verification

The first rule is to question everything and everyone. There is no such thing as a completely reliable source when it comes to using data to make meticulous journalism.

For example, would you completely trust a database published by the World Bank? Most of the journalists I've asked this question say they would; they consider the World Bank a reliable source. Let's test that assumption with two World Bank datasets to demonstrate how to verify data, and to reinforce that even so-called trustworthy sources can provide mistaken data. I'll follow the process outlined in the below graphic.




1. *Is the data complete?*

One first practice I recommend is to explore the extreme values (highest or lowest) for each variable in a dataset, and to then count how many records (rows) are listed within each of the possible values.

For example, the World Bank publishes a database with more than 10,000 independent evaluations performed on more than 8,600 projects developed worldwide by the organization since 1964.

Just by sorting the Lending Cost column in ascending order in a spreadsheet, we can quickly see how multiple records have a zero in the cost column.

J1 | Lending Project Cost

| | Project Name | Region | Country Code | Country Name | Approval Date | Approval FY | Sector Board | Agreement Type | Lending Project Cost | Deactivation Date | Exit FY |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | ROAD | AFR | 3A | Africa | 01-Feb-90 | 1990 | Financial Sector | IBRD | 0 | 31-Dec-97 | 1998 |
| 3 | EDUCATION | AFR | GA | Gabon | 07-Jun-68 | 1968 | Education | IBRD | 0 | 30-Jun-75 | 1975 |
| 4 | ROADS II | AFR | GA | Gabon | 07-Jan-69 | 1969 | Transport | IBRD | 0 | 30-Jun-75 | 1975 |
| 5 | BATHURST PORT REHAB | AFR | GM | Gambia, The | 07-Apr-70 | 1970 | Transport | IDA | 0 | 30-Jun-79 | 1979 |
| 6 | RICE DEVELOPMENT I | AFR | GM | Gambia, The | 12-Sep-72 | 1973 | Agriculture and Rural Development | IDA | 0 | 30-Jun-78 | 1978 |
| 7 | RURAL DEVT. | AFR | GM | Gambia, The | 15-Jun-76 | 1976 | Agriculture and Rural Development | IDA | 0 | 31-Mar-82 | 1982 |
| 8 | TOURISM I | AFR | GM | Gambia, The | 30-Dec-75 | 1976 | Urban Development | IDA | 0 | 30-Jun-82 | 1982 |
| 9 | DFC (GCDB) | AFR | GM | Gambia, The | 25-May-78 | 1978 | Financial Sector | IDA | 0 | 30-Jun-83 | 1983 |
| 10 | EDUCATION | AFR | GM | Gambia, The | 18-Apr-78 | 1978 | Education | IDA | 0 | 30-Jun-83 | 1983 |
| 11 | HIGHWAYS | AFR | GM | Gambia, The | 24-Apr-79 | 1979 | Transport | IDA | 0 | 30-Jun-86 | 1986 |
| 12 | ENERGY | AFR | GM | Gambia, The | 03-Nov-83 | 1982 | Energy and Mining | IDA | 0 | 31-Mar-88 | 1988 |
| 13 | SAL II | AFR | GM | Gambia, The | 08-Jun-89 | 1989 | Economic Policy | IDA | 0 | | 1992 |
| 14 | ENTERPRISE REF & DEV | AFR | GM | Gambia, The | 22-Dec-88 | 1989 | Energy and Mining | IDA | 0 | | 1997 |
| 15 | WOMEN IN DEVELOPMENT | AFR | GM | Gambia, The | 24-May-90 | 1990 | Social Protection | IDA | 0 | 31-Dec-97 | 1998 |
| 16 | WOMEN IN DEVELOPMENT | AFR | GM | Gambia, The | 24-May-90 | 1990 | Social Protection | IDA | 0 | 31-Dec-97 | 1998 |
| 17 | KIRUMIRO R/D | AFR | BI | Burundi | 16-Jun-81 | 1981 | Agriculture and Rural Development | IDA | 0 | 30-Jun-88 | 1988 |
| 18 | HINVI AGRIC DEVELOPM | AFR | BJ | Benin | 18-Feb-69 | 1969 | Agriculture and Rural Development | IDA | 0 | 30-Jun-78 | 1978 |
| 19 | DFC/SME | AFR | BJ | Benin | 20-Mar-80 | 1980 | Financial Sector | IDA | 0 | 30-Jun-89 | 1989 |
| 20 | RURAL DEVT./COTTON I | AFR | BJ | Benin | 07-Apr-81 | 1981 | Agriculture and Rural Development | IDA | 0 | 31-Dec-88 | 1989 |
| 21 | RURAL DEVT./COTTON I | AFR | BJ | Benin | 07-Apr-81 | 1981 | Agriculture and Rural Development | IDA | 0 | 31-Dec-88 | 1989 |

Qry_final_IEG_World_Bank_Projec

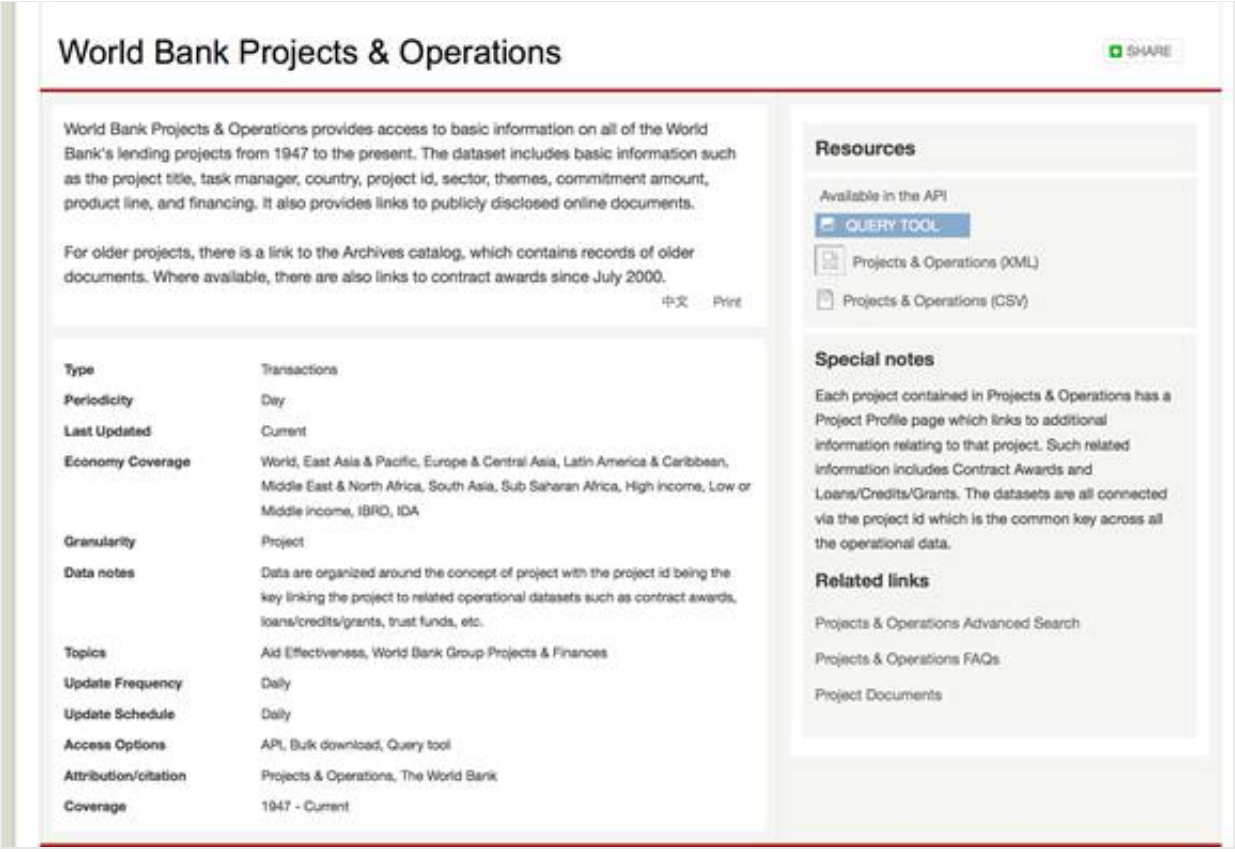
If we create a pivot table to count how many projects have a zero cost, in relation to the total records, we can see how more than half of those (53 percent) cost zero.

B19

| | A | B |
|---|---|---|
| 3 | Count of Lending Project Cost | |
| 4 | Row Labels | Total |
| 5 | ▼0 | |
| 6 | 0 | 5496 |
| 7 | ▶400000 to 8910000 | 4911 |
| 8 | Grand Total | 10407 |
| 9 | | |

This means that anyone who performs a calculation or analysis per country, region or year involving the cost of the projects would be wrong if they failed to account for all of the entries with no stated cost. The dataset as it's provided will lead to an inaccurate conclusion.

The Bank publishes another database that supposedly contains the individual data for each project funded (not only evaluated) by the organization since 1947.



# World Bank Projects & Operations

SHARE

World Bank Projects & Operations provides access to basic information on all of the World Bank's lending projects from 1947 to the present. The dataset includes basic information such as the project title, task manager, country, project id, sector, themes, commitment amount, product line, and financing. It also provides links to publicly disclosed online documents.

For older projects, there is a link to the Archives catalog, which contains records of older documents. Where available, there are also links to contract awards since July 2000.

中文 Print

| | |
|---|---|
| **Type** | Transactions |
| **Periodicity** | Day |
| **Last Updated** | Current |
| **Economy Coverage** | World, East Asia & Pacific, Europe & Central Asia, Latin America & Caribbean, Middle East & North Africa, South Asia, Sub Saharan Africa, High income, Low or Middle income, IBRD, IDA |
| **Granularity** | Project |
| **Data notes** | Data are organized around the concept of project with the project id being the key linking the project to related operational datasets such as contract awards, loans/credits/grants, trust funds, etc. |
| **Topics** | Aid Effectiveness, World Bank Group Projects & Finances |
| **Update Frequency** | Daily |
| **Update Schedule** | Daily |
| **Access Options** | API, Bulk download, Query tool |
| **Attribution/citation** | Projects & Operations, The World Bank |
| **Coverage** | 1947 - Current |

## Resources

Available in the API

QUERY TOOL

Projects & Operations (XML)

Projects & Operations (CSV)

## Special notes

Each project contained in Projects & Operations has a Project Profile page which links to additional information relating to that project. Such related information includes Contract Awards and Loans/Credits/Grants. The datasets are all connected via the project id which is the common key across all the operational data.

## Related links

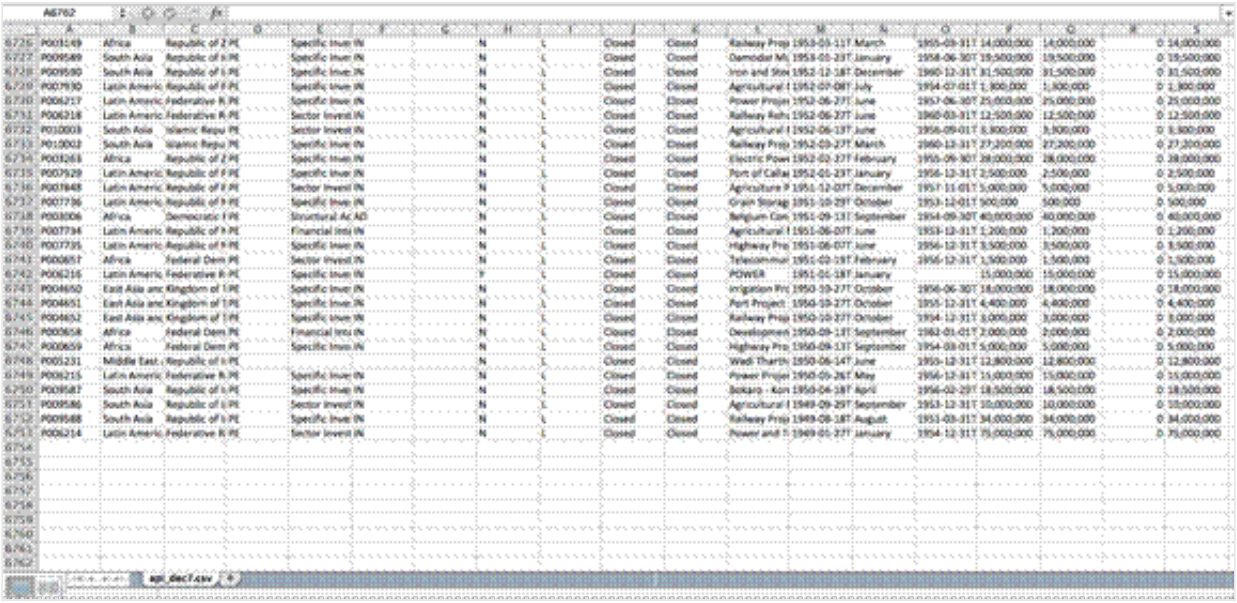
Projects & Operations Advanced Search

Projects & Operations FAQs

Project Documents

Just by opening the api.csv file in Excel (version as of Dec. 7, 2014), it's clear that the data is dirty and contains many variables combined into one cell (such as sector names or country names). But even more notable is the fact that this file does not contain all of the funded projects since 1947.

The database in fact only includes 6,352 out of the more than 15,000 projects funded by the World Bank since 1947. (Note: The Bank eventually corrected this error. By Feb. 12, 2015, the same file included 16,215 records.)



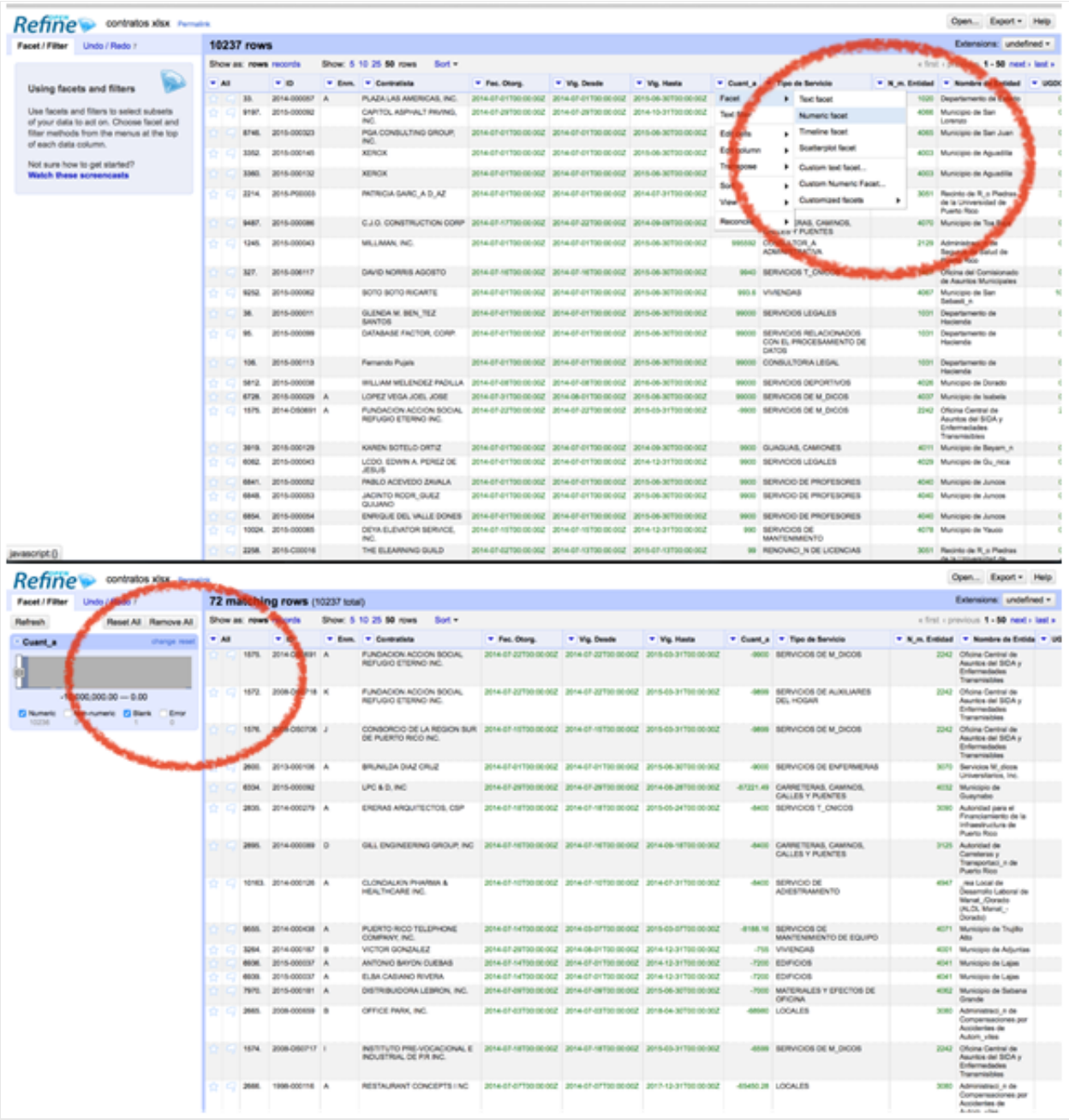
After just a little bit of time spent examining the data, we see that the World Bank does not include the

cost of all projects in its databases, it publishes dirty data, and it failed to include all of its projects in at least one version of the data. Given all of that, what would you now expect about the quality of data published by seemingly less reliable institutions?

Another recent example of database inconsistency I found came during a workshop I was giving in Puerto Rico for which we used the public contracts database from the Comptroller's Office. Some 72 public contracts, out of all last year's contracts, had negative values ($–10,000,000) in their cost fields.

Open Refine is an excellent tool to quickly explore and evaluate the quality of databases.
In the first image below, you can see how Open Refine can be used to run a numeric "facet" in the Cuantía (Amount) field. A numeric facet groups numbers into numeric range bins. This enables you to select any range that spans a consecutive number of bins.

The second image below shows that you can generate a histogram with the values range included in the database. Records can then be filtered by values by moving the arrows inside the graph. The same can be done for dates and text values.




2. *Are there duplicate records?*

One common mistake made when working with data is to fail to identify the existence of duplicate records.

Whenever processing disaggregated data or information about people, companies, events or transactions, the first step is to search for a unique identification variable for each item. In the case of the World Bank's projects evaluation database, each project is identified through a unique code or "Project ID." Other entities' databases might include a unique identification number or, in the case of public contracts, a contract number.

If we count how many records there are in the database for each project, we see that some of them are duplicated up to three times. Therefore, any calculation on a per country, region or date basis using the

data, without eliminating duplicates, would be wrong.

| | A | B |
|---|---|---|
| 1 | Count of Project ID | |
| 2 | PROJECT ID | Total |
| 3 | P010162 | 3 |
| 4 | P010410 | 3 |
| 5 | P070371 | 3 |
| 6 | P078994 | 3 |
| 7 | P000075 | 2 |
| 8 | P000082 | 2 |
| 9 | P000090 | 2 |
| 10 | P000099 | 2 |
| 11 | P000101 | 2 |
| 12 | P000105 | 2 |
| 13 | P000106 | 2 |
| 14 | P000120 | 2 |
| 15 | P000133 | 2 |
| 16 | P000138 | 2 |
| 17 | P000139 | 2 |
| 18 | P000142 | 2 |
| 19 | P000145 | 2 |
| 20 | P000147 | 2 |
| 21 | P000173 | 2 |
| 22 | P000178 | 2 |
| 23 | P000183 | 2 |
| 24 | P000186 | 2 |
| 25 | P000188 | 2 |
| 26 | P000258 | 2 |
| 27 | P000261 | 2 |
| 28 | P000263 | 2 |
| 29 | P000267 | 2 |
| 30 | P000270 | 2 |
| 31 | P000274 | 2 |
| 32 | P000276 | 2 |
| 33 | P000282 | 2 |
| 34 | P000285 | 2 |
| 35 | P000290 | 2 |
| 36 | P000293 | 2 |
| 37 | P000304 | 2 |

In this case, records are duplicated because multiple evaluation types were performed for each one. To eliminate duplicates, we have to choose which of all the evaluations made is the most reliable. (In this case, the records known as Performance Assessment Reports [PARs] seem to be the most reliable because they offer a much stronger picture of the evaluation. These are developed by the Independent Evaluation Group, which independently and randomly samples 25 percent of World Bank projects per year. IEG sends its experts to the field to evaluate the results of these projects and create independent evaluations.)

3. *Are the data accurate?*

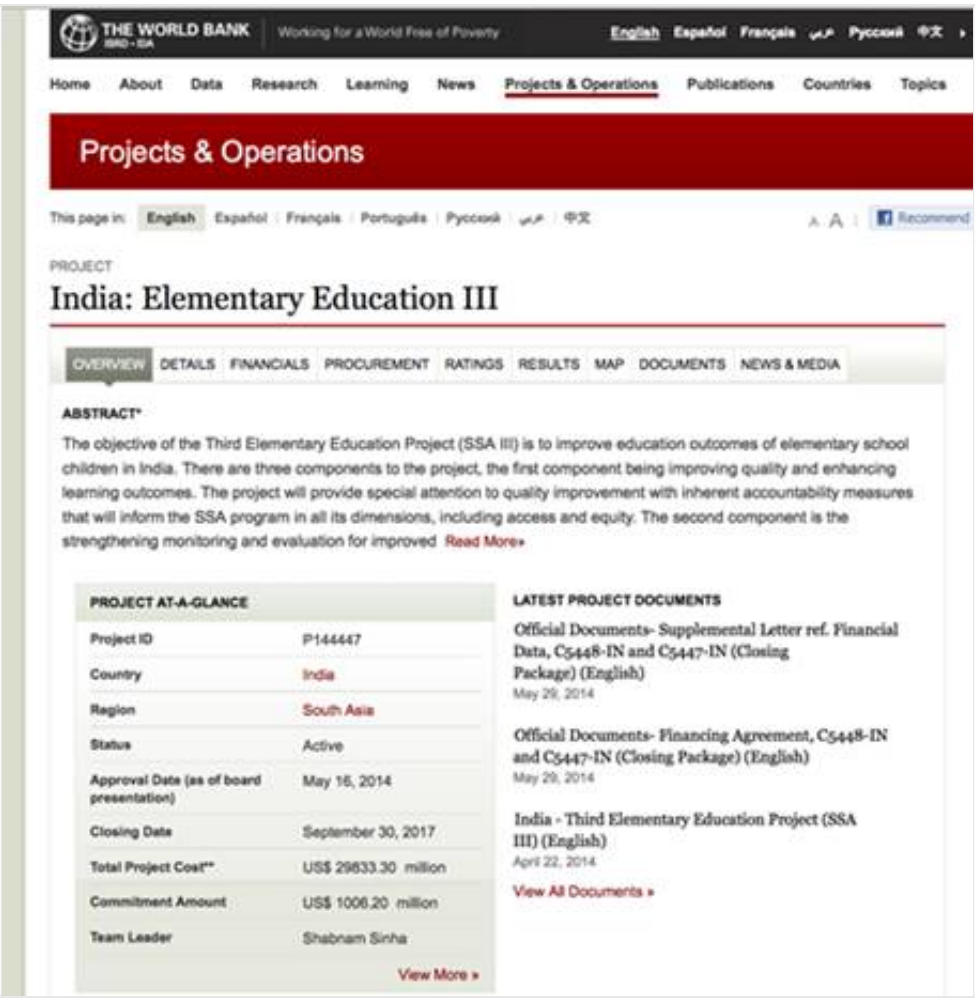
One of the best ways to assess a dataset's credibility is to choose a sample record and compare it against reality.

If we sort the World Bank's database — which supposedly contained all the projects developed by the institution — in descending order per cost, we find a project in India was the most costly. It is listed

with a total amount of US$29,833,300,000.

If we search the project's number on Google (P144447), we can access the original approval documentation for both the project and its credit, which effectively features a cost of US$29,833 million. This means the figure is accurate.

It's always recommended to repeat this validation exercise on a significant sample of the records.




4. *Assessing data integrity*

From the moment it's first entered in a computer to the time when we access it, data goes through several input, storage, transmission and registry processes. At any stage, it may be manipulated by people and information systems.

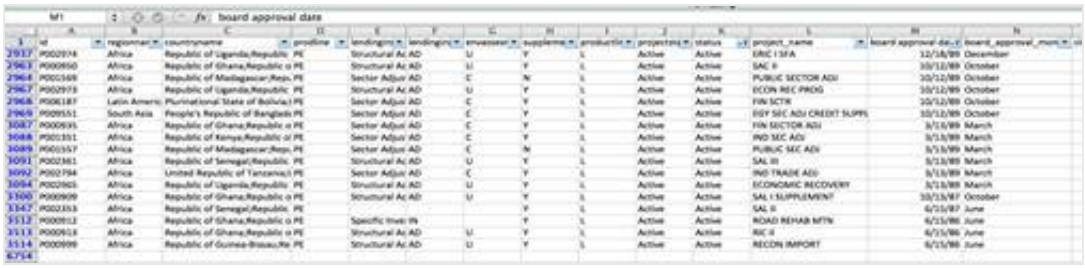
It's therefore very common that relations between tables or fields get lost or mixed up, or that some variables fail to get updated. This is why it's essential to perform integrity tests.

For example, it would not be unusual to find projects listed as "active" in the World Bank's database many years after the date of approval, even if it's likely that many of these are no longer active.

To check, I created a pivot table and grouped projects per year of approval. Then I filtered the data to

show only those marked as “active” in the “status” column. We now see that 17 projects approved in 1986, 1987 and 1989 are still listed as active in the database. Almost all of them are in Africa.

| | A | B | C |
|---|---|---|---|
| 1 | status | Active | |
| 2 | | | |
| 3 | | Values | |
| 4 | Row Labels | Count of board approval date | Count of status |
| 5 | 1986 | 3 | 3 |
| 6 | 1987 | 2 | 2 |
| 7 | 1989 | 12 | 12 |
| 8 | 1990 | 6 | 6 |
| 9 | 1991 | 5 | 5 |
| 10 | 1992 | 4 | 4 |
| 11 | 1997 | 1 | 1 |
| 12 | 2002 | 3 | 3 |
| 13 | 2008 | 1 | 1 |
| 14 | 2009 | 7 | 7 |
| 15 | 2010 | 47 | 47 |
| 16 | 2011 | 199 | 199 |
| 17 | 2012 | 271 | 271 |
| 18 | 2013 | 387 | 387 |
| 19 | 2014 | 466 | 466 |
| 20 | **Grand Total** | **1414** | **1414** |
| 21 | | | |



In this case, it’s necessary to clarify directly with the World Bank if these projects are still active after almost 30 years.

We could, of course, perform other tests to evaluate the World Bank’s data consistency. For example, it would be a good idea to examine whether all loan recipients (identified as “borrowers” in the database) correspond to organizations and/or to the actual governments from the countries listed in the “Countryname” field, or whether the countries are classified within the correct regions (“regionname”).

5. *Deciphering codes and acronyms*

One of the best ways to scare a journalist away is to show him or her complex information that’s riddled with special codes and terminology. This is a preferred trick by bureaucrats and organizations who offer little transparency. They expect that we won’t know how to make sense of what they give us. But codes and acronyms can also be used to reduce characters and leverage storage capacities. Almost every database system, either public or private, uses codes or acronyms to classify information.

In fact, many of the people, entities and things in this world have one or several codes assigned. People have identification numbers, Social Security numbers, bank client numbers, taxpayer numbers, frequent flyer numbers, student numbers, employee numbers, etc.

A metal chair, for example, is classified under the code 940179 in the world of international commerce. Every ship in the world has a unique IMO number. Many things have a single, unique number: Properties, vehicles, airplanes, companies, computers, smartphone, guns, tanks, pill, divorces, marriages…

It is therefore mandatory to learn how to decrypt codes and to understand how they are used to be able to understand the logic behind databases and, more importantly, their relations.

Each one of the 17 million cargo containers in the world has a unique identifier, and we can track them if we understand that the first four letters of the identifier are related to the identity of its owner. You can query the owner in this database. Now those four letters of a mysterious code become a means to gain more information.

The World Bank database of evaluated projects is loaded with codes and acronyms and, surprisingly, the institution does not publish a unified glossary describing the meaning of all these codes. Some of the acronyms are even obsolete and cited only in old documents.

The "Lending Instrument" column, for example, classifies all projects depending on 16 types of credit instruments used by the World Bank to fund projects: APL, DPL, DRL, ERL, FIL, LIL, NA, PRC, PSL, RIL, SAD, SAL, SIL, SIM, SSL and TAL. To make sense of the data, it's essential to research the meaning of these acronyms. Otherwise you won't know that ERL corresponds to emergency loans given to countries that have just undergone an armed conflict or natural disaster.

The codes SAD, SAL, SSL and PSL refer to the disputed Structural Adjustment Program the World Bank applied during the '80s and '90s. It provided loans to countries in economic crises in exchange for those countries' implementation of changes in their economic policies to reduce their fiscal deficits. (The program was questioned because of the social impact it had in several countries.)

According to the Bank, since the late '90s it has been more focused on loans for "development," rather than on loans for adjustments. But, according to the database, between the years 2001 and 2006, more than 150 credits were approved under the Structural Adjustment code regime.

Are those database errors, or has the Structural Adjustment Program been extended into this century?

This example shows how decoding acronyms is not only a best practice for evaluating the quality of the data, but, more important, to finding stories of public interest.

### B. Verifying data after the analysis

The final verification step is focused on your findings and analysis. It is perhaps the most important verification piece, and the acid test to know if your story or initial hypothesis is sound.

In 2012, I was working as an editor for a multidisciplinary team at La Nación in Costa Rica. We decided to investigate one of the most important public subsidies from the government, known as "Avancemos." The subsidy paid a monthly stipend to poor students in public schools to keep them from leaving school.

After obtaining the database of all beneficiary students, we added the names of their parents. Then we queried other databases related to properties, vehicles, salaries and companies in the country. This enabled us to create an exhaustive inventory of the families' assets. (This is public data in Costa Rica, and is made available by the Supreme Electoral Court.)

Our hypothesis was that some of the 167,000 beneficiary students did not live in poverty conditions, and so should not have been receiving the monthly payment.

Before the analysis, we made sure to evaluate and clean all of the records, and to verify the relationships between each person and their assets.

The analysis revealed, among other findings, that the fathers of roughly 75 students had monthly wages of more than US$2,000 (the minimum wage for a nonskilled worker in Costa Rica is $500), and that over 10,000 of them owned expensive properties or vehicles.

But it was not until we went to visit their homes that we could prove what the data alone could have never told us: These kids lived in real poverty with their mothers because they had been abandoned by their fathers.

No one ever asked about their fathers before granting the benefit. As a result, the state financed, over many years and with public funds, the education of many children who had been abandoned by an army of irresponsible fathers .

This story summarizes the best lesson I have learned in my years of data investigations: Not even the best data analysis can replace on-the-ground journalism and field verification.

# Chapter 6: Building expertise through UGC verification

**Eliot Higgins** is an investigative journalist and researcher, specialising in open source investigations. He has achieved worldwide recognition for his work, that has included investigating the use of cluster munitions in Syria, the smuggling of weapons to the Syrian opposition, the August 21st Sarin attacks in Damascus, and the downing of MH17 in Ukraine. His recently launched website Bellingcat aims to spread the use of open source investigation techniques to NGOs, media organisations, and other groups. He is @EliotHiggins on on Twitter.

During the later stages of the Libyan civil war in 2011, rebel groups pushed out from the Nafusa Mountain region and began to capture towns. There were many contradictory reports of the capture of towns along the base of the mountain range. One such claim was made about the small town of Tiji, just north of the mountains. A video was posted online that showed a tank driving through what was claimed to be the center of the town.

At the time, I was examining user-generated content coming from the Libyan conflict zone. My interest was in understanding the situation on the ground, beyond what was being reported in the press. There were constant claims and counterclaims about what was happening on the ground. There was really only one question I was interested in answering: How do we know if a report is accurate?

This is why and how I first learned to use geolocation to verify the location where videos were filmed. This work helped me sharpen the open source investigation techniques that are now used by myself and others to investigate everything from international corruption to war zones and plane crashes.

The video in Tiji showed a tank driving down a wide road, right next to a mosque. Tiji was a small town; I thought it might be easy to find that road and the mosque.

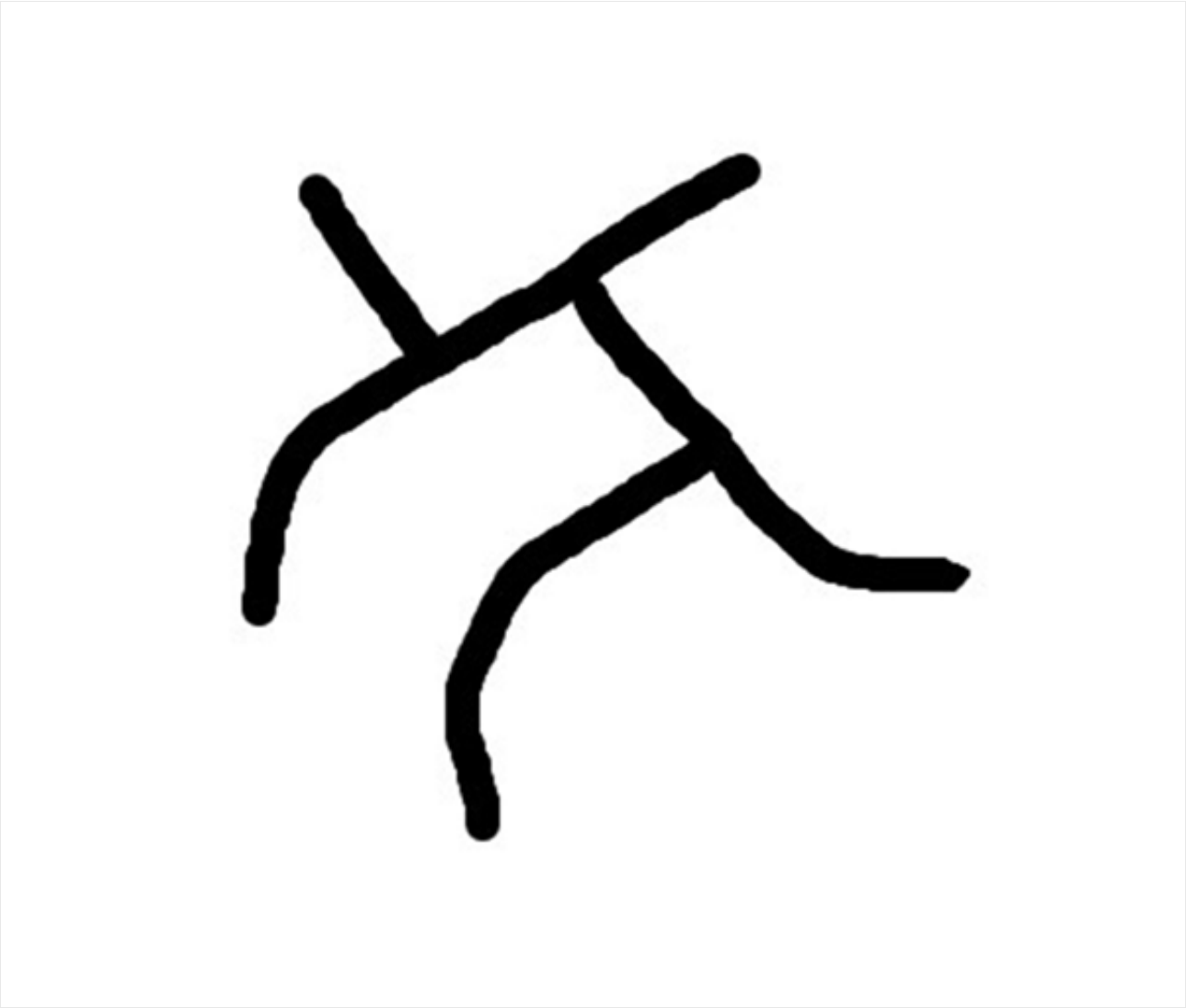
Until that point, I hadn’t even considered that you could use satellite maps to look for landmarks visible in videos to confirm where they had been filmed. The satellite map imagery below clearly showed only one major road running through the town, and on that road there was one mosque. I compared the position of the minaret, the dome and a nearby wall on the satellite map imagery to that in the video, and it was clear it was a perfect match.

Now that the likely position of the camera in the town was established, I could watch the whole video, comparing other details to what was visible on satellite map imagery. This further confirmed the positions matched.

Building expertise in satellite map based geolocation was something I did over time, using new tricks and techniques as I moved onto new videos.

### Matching roads

After the Tiji video, I examined a video purportedly filmed in another Libyan town, Brega, which featured rebel fighters taking a tour of the streets. At first, it appeared there were no large features, such as mosques, on a satellite map imagery. But I realized there was one very large feature visible in the video. As they walked through the streets, it was possible to map out the roads along the route they took, and then match that pattern to what was visible in satellite map imagery. Below is a hand-drawn map of the roads, as I saw them represented on the video.

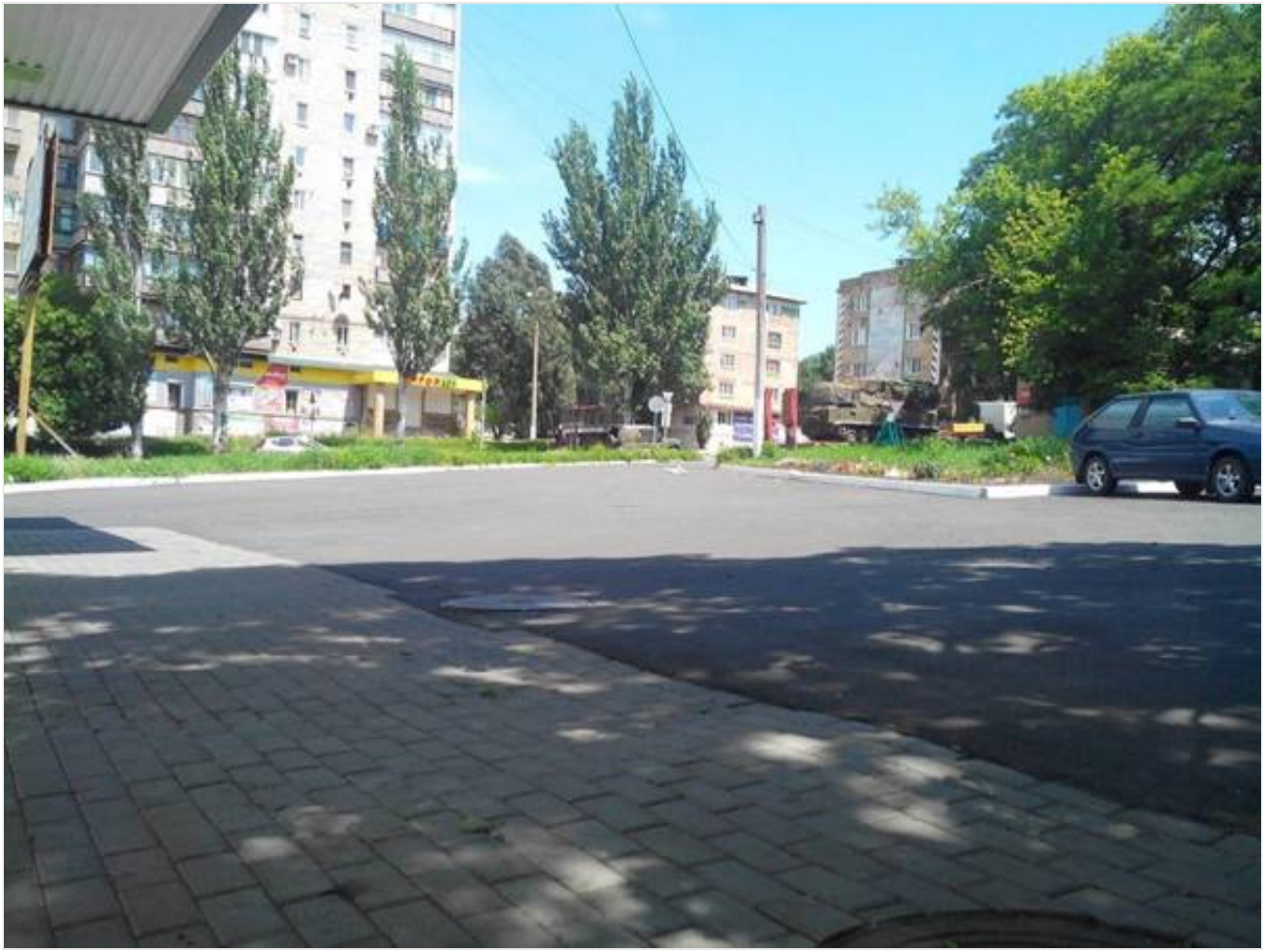


I scanned the satellite imagery of the town, looking for a similar road pattern. I soon found a match:

## Hunting shadows

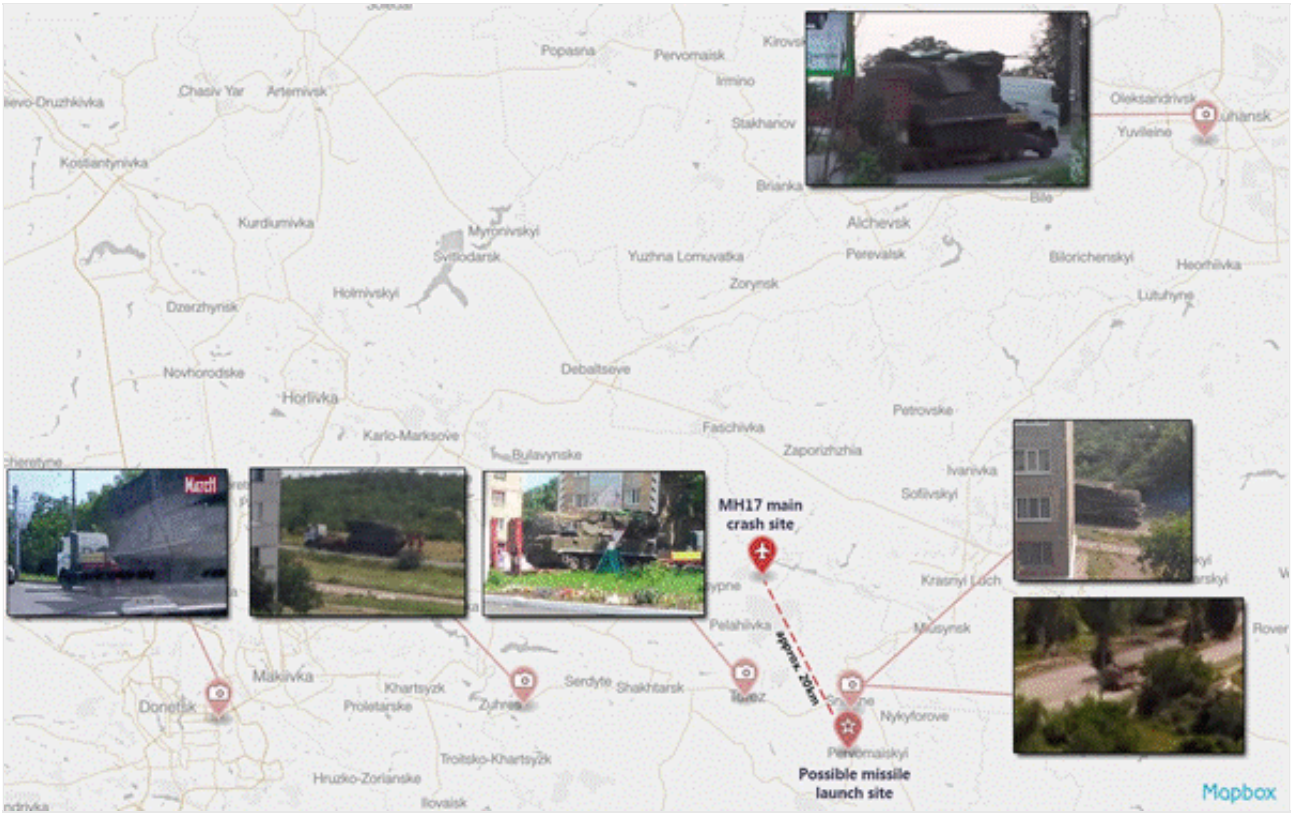
As you become more familiar with geolocating based on satellite map imagery, you'll learn how to spot smaller objects as well. For example, while things like billboards and streetlights are small objects, the shadows they cast can actually indicate their presence. Shadows can also be used to reveal information about the comparative height of buildings, and the shape of those buildings:

Shadows can also be used to tell the time of day an image was recorded. After the downing of Flight MH17 in Ukraine, the following image was shared showing a Buk missile launcher in the town of Torez:



It was possible to establish the exact position of the camera, and from that, it was possible to establish the direction of the shadows. I used the website Sun Calc, which allows users to calculate the position of the sun throughout the day using a Google Maps based interface. It was then possible to establish the time of day as approximately 12:30 p.m. local time, which was later supported by interviews with civilians on the ground, and with social media sightings of the missile launcher traveling through the town.

In the case of July 17, 2014, and the downing of MH17, it was possible to do this by analyzing several videos and photographs of the Buk missile launcher. I and others were able to create a map of the missile launcher's movements on the day, as well as a timeline of sightings.




By bringing together different sources, tools and techniques, it was possible to connect these individual pieces of information and establish critical facts about this incident.

A key element of working with user-generated content in investigations is understanding how that content is shared. With Syria, a handful of opposition social media pages are the main sources of information from certain areas. This obviously limits the perspective on the conflict from different regions, but also means it's possible to collect, organize and systematically review those accounts for the latest information.

In the case of Ukraine, there's few limits on Internet access, so information is shared everywhere. This creates new challenges for collecting information, but it also means there's more unfiltered content that may contain hidden gems.

During Bellingcat's research on the Buk missile launcher linked to the downing of MH17, it was possible to find multiple videos of a convoy traveling through Russia to the Ukrainian border that had the same missile launcher filmed and photographed on July 17 inside Ukraine.

These videos were on social media accounts and several different websites, all of which belonged to different individuals. They were uncovered by first geolocating the initial videos we found, then using that to predict the likely route those vehicles would have taken to get from each geolocated site. Then we could keyword search on various social media sites for the names of locations that were along the route the vehicle would have to had to travel. We also searched for keywords such as "convoy," "missile," etc. that could be associated with sightings.

Although this was very time consuming, it allowed us to build a collection of sightings from multiple sources that would have otherwise been overlooked, and certainly not pieced together.

If there's one final piece of advice, it would be to give this work and approach a try in any investigation. It's remarkable what you can turn up when you approach UGC and open source information in a systematic way. You tend to learn quickly by just doing it. Even something as simple as double-checking the geolocation someone else has done can teach you a lot about comparing videos and photographs to satellite map imagery.

# Chapter 7: Using UGC in human rights and war crimes investigations

**Christoph Koettl** is an adviser on technology and human rights for Amnesty International. He is the founder and editor of the Citizen Evidence Lab, the first dedicated social media authentication resource for human rights researchers. He tweets at @ckoettl. The views expressed are those of the author, and do not necessarily reflect the positions of Amnesty International.

In the early summer of 2014, Amnesty International received a video depicting Nigerian soldiers slitting the throats of suspected Boko Haram supporters, and then dumping them into a mass grave. The video, which circulated widely in the region and on YouTube, implicated Nigerian soldiers in a war crime. However, in order to draw that conclusion, we undertook an extensive investigation involving video analysis and field research. This resulted in the publication of Amnesty International's (AI) findings of this incident.

This incident is a powerful example of how user-generated content can contribute to in-depth investigations. It also demonstrates the importance of digging deeper and going beyond the basic facts gathered from standard UGC verification. This is particularly important for human rights investigations. UGC not only aids in determining the place and time of a violation; it can also help with identifying responsible individuals or units (linkage evidence) that can establish command responsibility, or with providing crucial crime base evidence that proves the commission of a crime.

While there are differences between human rights and war crimes investigations and journalistic reporting, there is also immense overlap, both in regards to the verification tools used and in terms of the benefits of relying on UGC. In fact, the British media outlet Channel 4 conducted an investigation into the conflict in northeastern Nigeria that was largely built on the same UGC footage.

## Principles of human rights investigations

While a lot of UGC might have immense news value, human rights groups are of course primarily interested in its probative value. In a human rights investigation, we compare all facts gathered with relevant human rights norms and laws (such as human rights and humanitarian, refugee and criminal law) to make determinations of violations or abuses. Consequently, a single analyst who looks at UGC, such as myself, must be part of a team comprising relevant country, policy and legal experts.

Our ultimate goal is to achieve a positive human rights impact, such as when our work contributes to establishing an international inquiry, or the indictment of a suspected perpetrator. Today we are achieving the best results when combining a variety of evidence, such as testimony, official documents,

satellite imagery and UGC.

This requires the close collaboration of researchers who possess country expertise, trusted contacts on the ground, and highly specialized analysts who do not focus on a specific region or country, but are able to provide analysis based on satellite imagery or UGC.

In some instances, one piece of evidence does not corroborate some of the information gathered during the investigation, such as when satellite imagery does not support eyewitness claims of a large mass grave. We then exercise caution and hold back on making statements of fact or determinations of violations.

This close collaboration among a range of experts becomes even more relevant when going beyond war crime investigations, which can be based on a single incident caught on camera. Crimes against humanity, for example, are characterized by a systematic and widespread nature that is part of a state or organizational policy. Research solely based on UGC will hardly be able to make such a complex (legal) determination. It usually provides only a snapshot of a specific incident. However, it can still play a crucial role in the investigation, as the following example will show.

### War crimes on camera

In 2014, AI reviewed dozens of videos and images stemming from the escalating conflict in northeastern Nigeria. Human rights groups and news organizations have extensively documented abuses by Boko Haram in the country. But this content proved especially interesting, as the majority of it depicts violations by Nigerian armed forces and the state-sponsored militia Civilian Joint Task Force (CJTF).

The most relevant content related to events March 14, 2014, when Boko Haram attacked the Giwa military barracks in Maiduguri, the state capital of Borno state. The attack was captured on camera and shared on YouTube by Boko Haram for propaganda purposes. It resulted in the escape of several hundred detainees. The response by authorities can only be described as shocking: Within hours, Nigerian armed forces and the CJTF extra-judicially executed more than 600 people, mostly recaptured detainees, often in plain sight, and often on camera.

Thorough research over several months allowed us to connect different video and photographs to paint a disturbing picture of the behavior of Nigerian armed forces. For example, one grainy cellphone video showed a soldier dragging an unarmed man into the middle of a street and executing him, next to a pile of corpses.

We first performed standard content analysis. This involved extracting the specifications of the road and street lamps, buildings and vegetation, as well as details related to the people seen in the video, such as clothes and military equipment. Reviewing the video frame by frame greatly aided with this process. The geographic features were then compared to satellite images of the area on Google Earth.

Based on this work, it was possible to pinpoint the likely location within Maiduguri, a large city of around a million people.

Several months later, additional photographs, both open source and directly collected from local sources, were used to paint a more comprehensive and even more worrisome picture of the incident. For example, at least two of the victims had their hands tied behind their backs. It is noteworthy that several photographs in our possession were actually geotagged. We discovered this by using a EXIf reader to examine the metadata in the photo. This location data proved a perfect match to the street corner we identified as part of the content analysis of the initial video.

Other videos from the same day documented an even more gruesome scene, which suggested another war crime. They show the killing of several unarmed men, as detailed earlier in this chapter. The videos were a textbook example of how UGC can be a powerful tool in longterm investigations when combined with traditional investigative methods.

We slowed the video to perform a content analysis in order to identify distinctive markings on the soldiers and victims, or anything that could indicate location, time or date. This revealed two important details: a soldier wearing a black flak jacket stating “Borno State. Operation Flush,” the name of the military operation in northeastern Nigeria; and, for a split second, an ID number on a rifle (“81BN/SP/407”) became visible. No distinctive geographic features were visible that could be used to identify the exact location.

*Extracted details from video. Note that frames have been cropped and edited for visualization purposes. Colors were inverted on right frame in order to highlight ID number on rifle.*

AI subsequently interviewed several military sources who independently confirmed the incident, including the date and general location outside of Maiduguri. An AI researcher was also able to secure the actual video files while on a field mission to the area. This allowed us to conduct metadata analysis

that is often not possible with online content, since social media sites regularly modify or remove metadata during the upload process.

The data corroborated that the footage had been created March 14, 2014. Obtaining the original files is often possible only through well-established local contacts and networks, who might share content in person or via email (ideally encrypted). Savvy news desk researchers and journalists who might be inclined to contact local sources via Twitter or other public platform should consider the risk implications for asking for such sensitive footage from contacts in insecure environments.

In this case, two sources stated that the perpetrators may be part of the 81 Battalion, which operates in Borno state, and that the rifle ID number refers to a "Support Company" of that battalion. Most important, several sources, who had to remain anonymous, separately stated that this specific rifle had not been reported stolen, disqualifying the predictable response by Nigerian authorities that the soldiers were actually impostors using stolen equipment.

After an initial public statement about the most dramatic footage, AI continued its investigation for several months, bringing together traditional research, such as testimony, with satellite imagery and the video footage and photographs detailed above. This UGC supported the overall conclusion of the investigation that both Boko Haram and Nigerian armed forces were also implicated in crimes against humanity. These findings can have serious implications, as the violations detailed are crimes under international law, and are therefore subject to universal jurisdiction and fall under the jurisdiction of the International Criminal Court.

# Chapter 8: Applying ethical principles to digital age investigation

**Fergus Bell** is head of newsroom partnerships and innovation at SAM, a social media search, curation and storytelling platform designed for the news industry. He joined SAM from The Associated Press, where, as international social media and UGC editor, he led the global operation to source and verify user-generated content for the AP's platforms. In 2013, Bell co-founded a committee for the Online News Association that has brought together leaders in the journalism community to explore the ethics and standards of UGC and digital newsgathering. Bell is a graduate of the University of Leeds and has also worked at ITN, CNN and radio stations across the U.K.

User-generated content (UGC) is taking an increasingly prominent role in daily news coverage, with audiences choosing to share their stories and experiences through the content they create themselves. Our treatment of the people who share this compelling content has a direct impact on the way that we, and other organizations, can work with them in the future.

It is essential to determine what ethical standards will work for you and your audience, and what actions will allow you to establish and preserve a relationship with them. Our approach must be ethical so that it can be sustainable.

Individuals contribute to news coverage in two typical ways. In one, journalists can invite and encourage people to participate in programming and reporting. This type of contributor will often be loyal, create content in line with the organization's style, and will be conscientious with any contributions.

The second type of contributor is the "accidental journalist." This could be an eyewitness to an event, or someone sharing details that will aid your investigation, even if that person may not be doing so with the idea of assisting journalists. These types of contributor often have little or no idea that what they have to offer, or are inadvertently already offering, may be of value or interest to journalists. This is especially true in the context of investigative reporting.

This chapter highlights some key questions and approaches when applying ethics and standards to newsgathering from social media, and when working with user-generated content.

## Entering private communities

Private communities can be extremely fruitful for generating investigative leads. Obvious examples of private communities are blogs, subreddits and Facebook groups. A less-obvious private community might be when an individual uses a YouTube page to share videos with friends and family. It's a public account, but the user assumes a level of privacy because the material is being shared with specific people. The key takeaway here is to consider how the content creator sees their activity, rather than

how you see it. This will help you apply the most sensitive and the most ethical approach.

The main issue is likely to be how you identify yourself to and within that community. Within your organization, you need to consider two questions about how transparent you should be.

1. *When is anonymity acceptable?* — Users on platforms such as Reddit and 4Chan are mostly anonymous, and it might be acceptable to start interactions without first identifying yourself as a journalist. However, if you are more than just conversation-watching, there will likely be a time when it's appropriate to identify yourself and your profession. Reddit recently issued guidance on how to approach its community when working on stories. These should be consulted when utilizing that platform.

2. *When is anonymity unlikely to be an option?* — Networks such as Facebook and Twitter are often more useful for breaking news because people are more likely to use real names and identities. In this kind of environment, anonymity as a journalist is less of an option. Again, if you are just watching rather than engaging with individuals, then being open and honest about who you are is often going to be the best way forward.

There are always going to be exceptions to the rule. This is also the case when it comes to deciding when it's acceptable for journalists to go undercover in the real world. Working out your policy before you need it is always going to yield the best results. You can then act with the confidence that your approach has been properly thought through.

## Securing Permission

Seeking permission to use content from creators of UGC helps establish and maintain the reputation of your organization as one that gives fair treatment. Securing permission will also help you ensure you are using content from an original source. This may save you legal headaches in the long run. All of the principal social platforms have simple methods for communicating quickly and directly with users.

Communication with individuals is, of course, an important part of any verification process. This means the act of asking for permission also opens up a potential source of additional information or even content that you otherwise wouldn't have had.

The question of payment for content is a separate issue that your organization needs to determine for itself. But it's clear that securing permission and then crediting is the new currency for user-generated content. Claire Wardle covers this in the next chapter.

## Contributor management and safety

*Audience contributions/assignments*

If you are gathering content from your audience through requests or assignments, then there are

several ethical issues to take into account. At the top of the list is your responsibility to keep them safe. When devising standards in this area, you should discuss the following issues:

- Does an assignment put someone at risk?
- Could an individual get too close to a dangerous event or to people who may cause them harm?
- What is your responsibility to a person who is harmed while carrying out an assignment set by you?
- How will you identify this person in the publication or broadcast?
- What impact does an assignment have on the honesty/authenticity of the content being produced versus something that was created unprompted?

*Discovered content*

The above issues also apply to those people whose contributions you've discovered, as opposed to having them sent to you. However, in the case of accidental journalists, there are additional questions you need to ask within your organization. These help establish your policy for communicating with them and for using their content:

- Does the person realize how they might be affected by sharing this content with the media?
- Do you think the owner/uploader knew that their content was discoverable by organizations like yours? Do you think they intended it for their personal network of friends and family?
- For something that is particularly newsworthy, how can you seek permission or contact with them without bombarding them as an industry?
- How can you sensitively communicate with individuals who have something newsworthy but are perhaps in a situation which has caused them distress, or loss?
- Does the publication or broadcast of their content identify their location or any personal information that might cause them to be harmed or otherwise affected?

## Charting an ethical course for the future

The Online News Association has several initiatives to address many of the issues raised in this chapter. The aim is to create resources that will allow journalists at all types of news organizations to chart an ethical course for the future.

The ONA's DIY ethics code project allows newsrooms to devise a personalized code of ethics. The ONA's UGC working group was established to bring leaders together from across the journalism community to freely discuss challenges and possible solutions to the ethical issues raised by the increased use of social newsgathering and UGC.

The group is focusing on three specific areas:

- Can the industry agree on an ethical charter for UGC?
- Can we work with the audience to understand their needs, frustrations and fears?
- How can we further protect our own journalists working with UGC?

Those interested in becoming a member of this working group can join our Google+ community.

# Chapter 9: Presenting UGC in investigative reporting

**Claire Wardle** is the research director at the Tow Center for Digital Journalism at Columbia University. She led a research project into UGC and broadcast news at the center, and later, with her fellow researchers, launched the Eyewitness Media Hub. She designed the social media training for BBC News, and went on to train at organizations around the world. Wardle has also worked at Storyful and UNHCR. Wardle has a Ph.D. in communication from the Annenberg School for Communication at the University of Pennsylvania. She is @cward1e on Twitter.

Ten years ago, a huge earthquake in the Indian Ocean unleashed a devastating tsunami across the region. At first, there were no pictures of the wave; it took a couple of days for the first images to surface. And when they did appear, most were shaky footage, captured mostly by tourists pressing record on their camcorders as they ran to safety. None of them expected their home videos of a family holiday to become eyewitness footage of a terrible tragedy.

Today, it's a completely different situation. During almost every news event, bystanders use their mobile phones to share text updates in real-time on social media, as well as to capture and post pictures and videos straight to Twitter, Facebook, Instagram or YouTube.

But just because we now take this behavior for granted doesn't mean we've worked out the rules for how to use this material legally, ethically or even logistically. Organizations are still working through the most appropriate ways to use this type of content. This is true whether it's news outlets, brands, human rights groups or educators.

There are important differences between footage that has been sent directly to a particular organization versus material that has been uploaded publicly on a social network. The most important point to remember is that when someone uploads a photograph or video to a social network, the copyright remains with them. So if you want to download the picture or video to use elsewhere, you must first seek permission. If you simply want to embed the material, using the embed code provided by all of the social networks, legally you don't need to seek permission. Ethically, however, it might be appropriate to contact the person who created the content to let them know how and where you intend to use it.

## Seeking permission

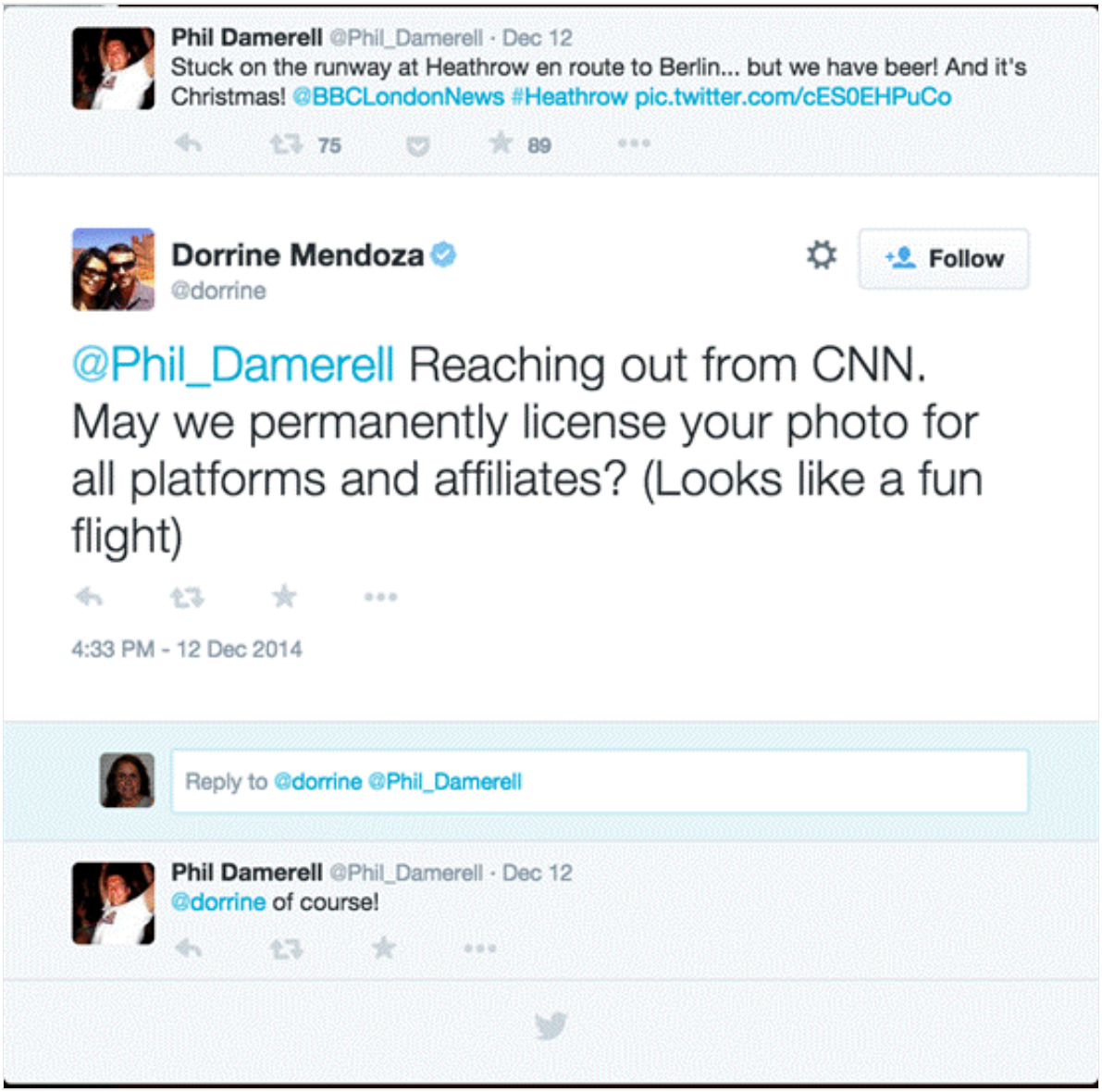
A lawyer would always prefer an agreement to be conducted formally via a signed contract; however, in the heat of a breaking news event, seeking permission on the social network itself has become the norm. This has many benefits, not the least of which is that it provides an opportunity for immediate dialogue with the user who has shared the material.

Asking the right questions at the point of contact will help with your verification processes. The most important question to ask is whether the person actually captured the material him or herself. It is amazing how many people upload other people's content on their own channels. They will often "give permission" for use even though they have no right to do so. You also want to ask basic questions about their location, and what else they could see, to help you authenticate what they claim to have witnessed.

If the person has just experienced a traumatic or shocking event, they could possibly still be in a dangerous situation. Establishing that they are safe and able to respond is also a crucial step. When seeking permission, it's also important to be as transparent as possible about how you intend to use the footage. If you intend to license the video globally, this should be explained in a way that ensures that the uploader understands what that means.

Here's

one example of how to do it:



However, if you want a watertight legal agreement, you would need to arrange something more substantial over email. If you do seek permission on the social network itself, make sure that you take a screenshot of the exchange. People will sometimes provide permission for use, and then, after negotiating an exclusive deal with another organization, they will delete any exchanges on social media that show them giving permission to others.

### Payment

There isn't an industry standard for payment. Some people want payment for their material, and others don't. Some people are happy for organizations to use their photo or video, as long as they are credited. Other people don't want to be credited.

This is why you should ask these questions when you are seeking permission. You should also think about the implications of using the material. For example, a person might have captured a piece of content and in their mind, they've only shared it with their smallish network of friends and family. But they didn't expect a journalist to find it. They captured it when they were perhaps somewhere they shouldn't have been, or they captured something illegal and they don't want to be involved. Or they simply don't want a picture, quickly uploaded for their friends to see, to end up embedded on an online news site with millions of readers.

Here's an example of a response from a person who uploaded a picture to Instagram during the shooting at the Canadian parliament in October 2014.

> @cnnjustin @demotix @newzuluca I did take the photo myself. I suppose since I put this online to share it's intended to share. I would rather not have my name included in any further publication. You can credit it to a Concerned Canadian

As part of ongoing monitoring and research, Eyewitness Media Hub has analyzed hundreds of exchanges between journalists and uploaders over 18 months in 2013, 2014 and 2015, and the responses of the people who created the material are not always what you would expect. This piece by Eyewitness Media Hub, of which I'm a co-founder, reflects on the content that emerged during the Paris shootings in early 2015, and the people who found themselves and their material unexpectedly at the center of the news coverage.

### Crediting

Our experience and analysis show that the vast majority of people don't want payment; they simply want a credit. This isn't just a case of what's right: It's also a question of being transparent with the

audience. There isn't an industry standard when it comes to crediting, as every uploader wants to be credited in a different way. Especially if you're not paying to use their material, you have a legal right to follow their instructions.

With television news, without the opportunity to embed content, a credit should be added onscreen. The most appropriate form of credit is to include two pieces of information. First, the social network where the footage was originally shared, and, second, the person's name, in the way they asked to be credited. That might be their real name or their username, e.g., Twitter / C. Wardle or Instagram / cward1e or YouTube / Claire Wardle.

Online, the content should be embedded from the platform that it was originally posted, whether that's Twitter, Instagram or YouTube. That means the credit is there as part of the embed. If a screen grab is taken of a picture or a video sourced from a social network, the same approach should be used. In the caption, it would be appropriate to hyperlink to the original post.

Be aware that embedded content will disappear from your site if it is removed from the social network by the original uploader. So you should ultimately try to procure the original file, especially if you are planning to run the content for a long time.

In certain situations, it's necessary to use your judgment. If a situation is ongoing, then sharing the information of the person who created the content might not be the most sensible thing to do, as shown by this BBC News journalist:

## Labeling

It is best practice to "label" who has captured the content. If we take this picture of a woman in the snowstorm in the Bekaa Valley in Lebanon, it's important that the audience knows who took this. Was it a UNHCR staff member? Was it a freelance journalist? Was it a citizen journalist? Was it a refugee?

In this case a refugee took the photograph, but it was distributed by UNHCR to news organizations via a Flickr account. When someone unrelated to the newsroom takes a picture that is used by the newsroom, for reasons of transparency, any affiliation should be explained to the audience. Simply labeling this type of material as “Amateur Footage” or something similar doesn’t provide the necessary context.

## Verification

There is no industry standard when it comes to labeling something as verified or not. The AP will not distribute a photograph or video unless it passes its verification procedures. While other news outlets try not to run unverified footage, it is difficult to be 100 percent sure about a photo or video that has been captured by someone unrelated to the newsroom.

As a result, many news organizations will run pictures or videos with the caveat that “this cannot be independently verified.” This is problematic, as the truth is that the newsroom may have run many verification checks, or relied on agencies to do these checks, before broadcasting or publishing a photo or video. So this phrase is being used as an insurance policy.

While research needs to explore the impact of this phrase on the audience, repeating it undermines the verification processes that are being carried out. Best practice is to label any content with the information you can confirm, whether that’s source, date or location. If you can confirm only two out of the three, add this information over the photo or video. We live in an age where audiences can often access the same material as the journalist; the audience is being exposed to the same breaking news photos and images in their social feeds. So the most important role for journalists is to provide the necessary context about the content that is being shared: debunk what is false, and provide crucial information about time, date or location, as well as showing how this content relates to other material

that is circulating.

## Being ethical

Overall, remember that when you work with material captured by others, you have to treat the content owner with respect, you need to work hard to verify what is being claimed, and you need to be as transparent as possible with your audience.

The people uploading this phone-taken footage are mostly eyewitnesses to a news event. They are not freelancers. The majority wouldn't identify themselves as citizen journalists. They often have little knowledge of how the news industry works. They don't understand words like exclusively, syndication or distribution.

Journalists have a responsibility to use the content ethically. Just because someone posted a piece of content publicly on a social network does not mean that they have considered the implications of its appearing on a national or international news outlet.

You must seek informed consent, not just consent, meaning: Does the uploader understand what they're giving permission for? And when it comes to crediting, you must talk to them about whether and how they would like credit. The responses are constantly surprising.

# Chapter 10: Organizing the newsroom for better and accurate investigative reporting

**Dr. Hauke Janssen** is the head of documentation at Der Spiegel. He has a Ph.D. in economics and is a former assistant lecturer. He joined Spiegel in 1991 as a fact-checker and researcher and became head of the department in 1998. Janssen is the author of scientific works on the history of economic thought and writes a fact-checking-column for Spiegel online.

It began with a cardboard box full of newspaper clippings. In 1947, Rudolf Augstein, the founder and publisher of Der Spiegel, mandated that his publication should gather and maintain an archive of previously published work.

That box soon grew to become an archive spanning hundreds, then thousands of meters of shelves. Newspapers, magazines and other news media were catalogued, along with original documents from government departments and other sources. Augstein praised his archive, which he said "can conjure up the most extravagant information." He died in 2002.

More than any other republisher in Germany, Augstein believed in the power and value of maintaining an archive, and in the importance of applying it to a fact-checking process.

Up to the late 1980s, Spiegel's archive was purely paper based. Beginning in the 1990s, the classic archives expanded into the virtual space. Today, the archive adds 60,000 new articles each week in its custom Digital Archive System (Digas). This information is collected from over 300 sources reviewed on a regular basis, which includes the entire national German press as well as several international publications. Digas currently stores more than 100 million text files and 10 million illustrations.

## From an archive to a documentation department

A mistake led Der Spiegel to the realization that fact-checking is necessary. When an archivist pointed out a serious error in an article that had already been printed, Augstein answered gruffly, "Well, check that in the future earlier, then."

From that point forward, fact-checking became a part of the duties of archive employees. In June 1949, Spiegel issued guidelines to all its journal

ists that outlined the necessity that every fact be checked. The guidelines read in part:

> Spiegel must contain more personal, more intimate and more background information than the daily press does ... All news, information and facts that Spiegel uses and publishes must be

> correct without fail. Each piece of news and each fact must be checked thoroughly before it is passed on to the news staff. All sources must be identified. When in doubt, it is better not to use a piece of information rather than to run the risk of an incorrect report.

Hans D. Becker, the magazine's managing editor in the 1950s, described the change from a traditional archive to a documentation department.

"Originally, the news library was only supposed to collect information (mostly in the form of press clippings)," he said. "What started as collecting on the dragnet principle imperceptibly became information-gathering through research. Amidst the 'chaos of the battlefield' of a newsroom, collecting and researching information for use in reporting imperceptibly became the exploitation of what was collected and gathered to prove what was claimed ..."

### How Spiegel does fact-checking today

The Dok, as we call it, is today organized into sections, called "referats," that correspond to the various desks in the news departments, such as politics, economy, culture, science, etc. It employs roughly 70 "documentation journalists." These are specialists who often possess a doctorate in their respective fields, and include biologists, physicists, lawyers, economists, MBAs, historians, scholars of Islam, military experts and more.

They are charged with checking facts and with supporting our journalists by providing relevant research. As soon as the author's manuscript is edited, the page proof is transferred to the relevant Dok-Referat. Then the fact-checking starts.

Spiegel has very specific and detailed guidelines for fact-checking. This process ensures we apply the same standard to all work, and helps ensure we do not overlook key facts or aspects of a story. Dok-Referats use the same markings on manuscripts, creating a level of consistency that ensures adherence to our standards.

This approach can be applied to any story, and is particularly useful in investigative work, which must meet the highest standards.

Some of the key elements of our guidelines:

- Any fact that is to be published will be checked to see if it is correct on its own and in context, employing the resources at hand and dependent on the time available.
- Every verifiable piece of information will be underlined.
- Standardized marks will be used to denote statements as correct, incorrect, not verifiable, etc.
- Correct facts and figures will be checked off. If corrections are necessary, they will be noted in

red ink in the margin, using standard proofreading marks.

- The source of factual corrections and quotations must be given.
- Corrections accepted by the author(s) will be checked off, the others will be marked n.ü. (not accepted).
- When fact-checking a manuscript, other and if possible more accurate sources than the author‘s sources should be used.
- A statement is considered verified only if confirmed by reliable sources or experts.
- If a piece of research contradicts an author’s statement, the author must be notified of the contradiction during the discussion of the manuscript. If a fact is unverifiable, the author must also be notified.
- A journalist’s source who is the object of an article may be contacted only with permission from the author. (In practice, we often speak with sources to check facts.)
- Complex passages will be double-checked by the documentation department specialized in the subject matter.
- Sometimes the limited time available means that priorities must be set. In such cases, facts that are the clear responsibility of the fact-checker must be checked first, particularly:
    - Are the times and dates correct?
    - Does the text contradict itself?
    - Are the names and offices/jobs correct?
    - Are the quotations correct (in wording and in context)?
    - How current and trustworthy are the sources used?

The above list represents the most critical elements to be verified in an article when there is limited time for fact-checking. Newsrooms that do not have a similar documentation department should emphasize that reporters and editors double-check all of these items in any story prior to publication.

### Evaluating Sources

Fact-checking starts with comparing a story draft with the research materials provided by the author. The fact-checker then seeks to verify the facts and assertions by gathering additional sources that are independent of each other. For crucial passages, the checker examines a wide variety of sources in order to examine what is commonly accepted and believed and what is a more subjective or biased point of view. They determine what is a matter of fact and what is controversial or, in some cases, a myth.

We use our Digas database to surface relevant and authoritative sources. It's also the responsibility of every Spiegel fact-checker to study the relevant papers, journals, studies, blogs, etc. in their field, daily. This ensures that they have current knowledge on relevant topics, and that they know the trustworthiness of different sources.

This form of domain expertise is essential when evaluating the credibility of sources. However, there are some general guidelines that can be followed when evaluating sources:

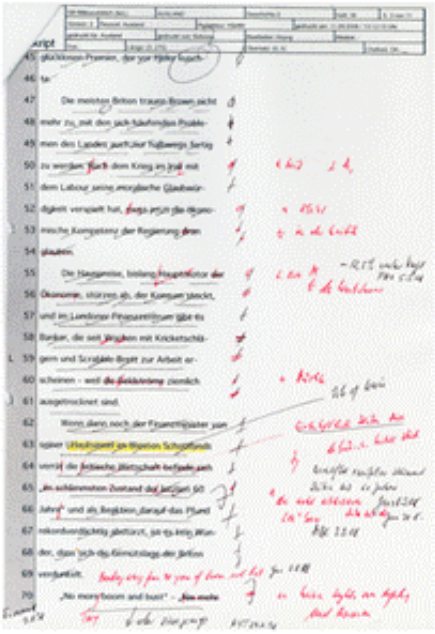
- Prefer original documents. If an academic study is quoted, obtain the original, full text. If company earnings are cited, obtain their financials. Do not reply on press summaries and press releases when the original document can be obtained.
- Prefer sources that delineate between facts and opinion, and that supply facts in their work.
- Prefer sources that clearly indicate the source of their information, as this enables you to verify their work. (Media outlets or other entities that overly rely on anonymous sources should be treated with caution.)
- Beware of sources that make factual errors about basic facts, or that confuse basic concepts about a subject matter.

### Examples of checked manuscripts

After an article has been checked at Spiegel, the documentarist and the author discuss possible corrections until they agree on the final version. The author makes the corrections to the manuscript. The fact-checker checks the corrections a second time and also any other changes that may have been made in the meantime.

DER SPIEGEL

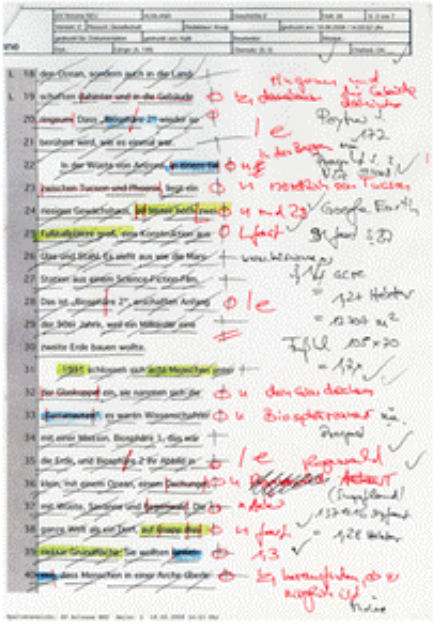
## Examples of Checked Manuscripts



- Notes easily legible
- Sources indicated
- Each line has been marked proved/probable/not verifiable/author's research
- corrections in red ink

DER SPIEGEL

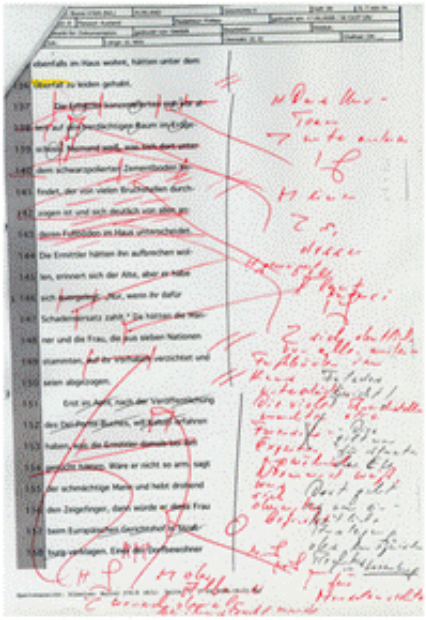
## Examples of Checked Manuscripts



- Somewaht less legible
- More confusing
- Source: Google Earth
- check example: calculation: 3,14 acres = "the size of two football pitches" ?

DER SPIEGEL

## Examples of Checked Manuscripts



- Hard to read
- What goes where?

Accuracy is the basic prerequisite for good journalism and objective reportage. Journalists make mistakes, intended or not. Mistakes damage the most valuable asset of journalism: credibility. That is, after all, the quality to which journalists refer most frequently to distinguish their journalism.

One method to reduce the probability of mistakes is verification; that is, checking facts before publication.

A 2008 thesis produced at the University of Hamburg counted all the corrections made by the documentation department in a single issue of Der Spiegel. The final count was 1,153. Even if we exclude corrections related to spelling and style, there were still 449 mistakes and 400 imprecise passages, of which more than 85 percent were considered to be relevant or very relevant.

# Case Study 1: Combing through 324,000 frames of cellphone video to help prove the innocence of an activist in Rio

**Victor Ribeiro** is a filmmaker, activist, and musician based in Rio de Janeiro. He's worked on educational and human rights projects since 2002 and has extensive experience in the use of multimedia tools for activism, as well as on leading workshops and strengthening community networks. Victor has been collaborating with WITNESS.org in Rio since 2013. Previously, he contributed to projects such as Rádio Madame Satã, Rio Distópico, Laboratório de Direitos Humanos de Manguinhos and Rio+Tóxico. Links to his work are available on the following links: http://rio40caos.tk, http://riotoxico.hotglue.me and http://labdhm.blogspot.com.br/.

(Photo credit: Midia Informal)

On Oct 15, 2013, a 37-year-old activist named Jair Seixas (aka Baiano) was arrested as a protest supporting striking teachers was winding down in Rio de Janeiro. Seixas had been marching peacefully with eight human rights lawyers when police officers approached and accused him of setting fire to a police vehicle and minibus.

As he was being taken away, police refused to tell the lawyers which precinct he was being taken to, or what evidence they had of his alleged crimes.

Seixas was held in prison for 60 days and released. He continues to fight the charges brought against him. When his lawyers began to plan their defense strategy, they looked for videos that might help prove Seixas' innocence. Their search involved looking on social networks, asking those who were at the event, and obtaining footage from the prosecution and courts.

They found five pieces of footage they felt had evidentiary value to their case. Two videos were official court records of the police officers' testimonies under oath; two were videos submitted by the prosecution that were confirmed to have been filmed by undercover police officers who had infiltrated protesters; and the final clip was filmed by a media activist who was covering the protest and was present at the time of Seixas' arrest. This activist used a cellphone to livestream the event, which provided a huge amount of critical first-hand footage of the event.

By putting these videos together, the lawyers found critical evidence of Seixas' innocence. The filmed testimonies of the officers were full of contradictions and helped prove that the officers didn't actually see Seixas set fire to the bus, contrary to what they had claimed earlier. The prosecution's videos captured audio of undercover officers inciting protesters to violence. This helped demonstrate that, in some instances, the violence the protesters were being accused of had originated with undercover officers.

The final clip, filmed by a media activist, was the smoking gun: In a frame-by-frame analysis of roughly three hours of an archived livestream of the protest (324,000 frames!) the defense team uncovered a single frame of video that showed that the police vehicle Seixas was being accused of having set ablaze was the exact same vehicle that drove him away after he was detained. This was proven by comparing the identifying characteristics of the vehicle in the video with the one that Seixas was transported in.

We at WITNESS helped the defense identify and prepare this evidence, both by assembling screenshots of these videos into a storyboard as well as by editing a 10-minute evidentiary submission of video that was delivered to the judge, along with the accompanying documentation.

Though the case is still continuing, the evidence is clear and undeniable. This is an inspiring example of how video from both official and citizen sources can serve justice and protect the innocent from false accusations.

# Case Study 2: Tracking back the origin of a critical piece of evidence from the #OttawaShooting

**Micah Clark** is Mission Manager for SecDev, a private open intelligence agency and cyber-security provider. In that capacity, Micah led SecDev's efforts to understand, orient and analyze events as they unfolded in Ottawa on 22 October 2014. On more routine days, Micah manages a team of analysts, developers and data visualizers delivering analytical products to government and corporate clients in Canada, the US and UK.

“Fear has big eyes,” goes an old Russian folk saying. “What it sees is what is not there.”

This is a story about fear’s big eyes and the things that were not there.

At approximately 9:50 a.m. on Oct. 22, 2014, Michael Zehaf-Bibeau shot and killed a soldier guarding the Canadian War Memorial in Ottawa. In a scene reminiscent of a Hollywood thriller, Zehaf-Bibeau then charged into the halls of parliament, where he was eventually shot and killed.

Two days earlier, a Canadian soldier was killed when he was deliberately hit by a car driven by a man who had previously drawn the attention of Canadian security agencies. The ensuing shootout on Parliament Hill had Canadians on edge. Was this a terrorist attack? What motivated the attacker? Was ISIS involved?

The speculation reached fever pitch when a photo of the assailant, taken at the very moment of his attack, was posted by a Twitter account claiming affiliation with ISIS. Other Twitter accounts, and eventually Canadian journalists and the Canadian public, rapidly used the photo and the ISIS account that posted it to draw a completely imaginary connection between the assailant and ISIS.

All of this speculation, however, was based on fundamentally incorrect source attribution. The story of the photo’s actual provenance is a remarkable example of the new normal for modern journalism.

The photo was first posted by an unknown user to an Ottawa Police tweet, which asked for any information about the assailant. This occurred sometime before 2 p.m., when Montreal journalist William Reymond located the photo and took a screen capture (Reymond, who has reported extensively on his scoop, has not provided a link to the tweet from Ottawa Police. The time and content he describes suggest it was this tweet). The photo and the account that posted it were deleted almost instantly.

With this exceptional photo in his hands, and to his considerable credit, Reymond took a full two hours to verify its authenticity before posting it to his Twitter account, @Breaking3zero, at 4:16 p.m.

Reymond’s process of verification, which he describes here in detail, included comparing the facial

features, clothes and weapon of the man in the photo with surveillance footage, as well as comparing it with details that emerged as witnesses and officials shared details of the attack.

Along with the rifle, two other key pieces of evidence were the fact that the man in the photo was wearing a keffieh, which witness had described, and the fact that he was carrying an umbrella. The shooter used an umbrella to conceal his weapon as he approached the War Memorial, according to reports.

Here is what Reymond tweeted:

It translates to, “After two hours of verification, a source confirmed to me that ‘it looks like the shooter.’ Proceed with caution.”

It was only after Reymond's tweet that an ISIS-related Twitter account, “Islamic Media” (@V_IMS), posted the photo, at approximately 4:45 p.m. This account too has since been suspended and deleted.

“Just twenty minutes after I published it, a French-language feed supporting the Islamic State picks up the photo and posts it,” wrote Reymond. “And that is how some media start to spread the wrong idea that ISIS is at the origin of the photo.”

Within minutes, another Twitter account, @ArmedResearch, posted the photo stating that, “#ISIS Media account posts picture claiming to be Michael Zehaf-Bibeau, dead #OttawaShooting suspect. #Canada.”

In spite of its failure to substantiate this claim or provide appropriate credit to @Breaking3zero, Canadian journalists seized upon @ArmedResearch’s claim, reporting the photo was “tweeted from an ISIS account,” with all the implications that accompany such an assertion.

But as the saying goes, facts are stubborn things. Technical data from @V_IMS’s Twitter page, captured before the account was suspended, show that @V_IMS sourced the photo from @Breaking3zero. The text in grey below shows the original source URL, from twitter.com/Breaking3zero:

```
▼<div class="js-tweet-details-fixer tweet-details-fixer">
  ▼<div class="TwitterPhoto js-media-container">
    ▼<div class="TwitterPhoto-container" data-card-url="//twitter.com/
    Breaking3zero/status/525017889334898688/photo/1" data-card-type="photo"
    data-element-context="platform_photo_card">
      ▼<div class="TwitterPhoto-media">
        ▼<a class="TwitterPhoto-link media-thumbnail twitter-timeline-link"
        href="https://twitter.com/Breaking3zero/status/525017889334898688/
        photo/1" data-url="https://pbs.twimg.com/media/B0k8_N5CcAE61SJ.jpg:
        large" data-resolved-url-large="https://pbs.twimg.com/media/
        B0k8_N5CcAE61SJ.jpg:large">
            ::before
            <img class="TwitterPhoto-mediaSource" src="./Islamic Media
            (@V_IMS)_Twitter_files/B0k8_N5CcAE61SJ.jpg-large" alt="Embedded
            image permalink" style="margin-top: -6.0px" lazyload="1">
          </a>
        </div>
      </div>
    </div>
    <div class="js-machine-translated-tweet-container"></div>
  </div>
```

The claim that the photo of Zehaf-Bibeau originated with an ISIS account is categorically false. The ISIS account that circulated the photo acquired it hours after it was originally posted to Twitter.

SecDev’s independent monitoring of ISIS’ social media shows that prominent ISIS accounts were

reacting to events in Ottawa in much the same way that Ottawans and others were — posting contradictory and often incorrect information about the attack. There is no indication in social media that ISIS had prior knowledge of the attack, or that they were in any way directly affiliated with Zehaf-Bibeau.

Indeed, there is still no evidence to indicate ISIS involvement in the October attack in Ottawa. There is, however, a remarkable photo taken at an incredible moment, a testament to the game-changing power of mobile technology and social media.

The temptation to draw a connection between vivid photos like this one and our worst fears is enormous. Avoiding this temptation is one of the chief responsibilities of 21st century journalists.

# Case Study 3: Navigating multiple languages (and spellings) to search for companies in the Middle East

**Hamoud Almahmoud** is the Senior Researcher and Trainer for a leading ARIJ's Mena Research & Data Desk at the Arab Reporters for Investigative Journalism (ARIJ). He is also regional researcher at the Organized Crime and Corruption Reporting Project (OCCRP). He has worked as an investigative reporter for print and TV then as an editor in chief of Aliqtisadi business magazine and online for several years. He is @HamoudSy on Twitter.

Searching for names of companies or people in the Middle East presents some special challenges. Let us start with a real example I have worked on recently:

I recently received a request from a European reporter who was investigating a company, Josons, which had won a bid to supply weapons in Eastern Europe.

This company was registered in Lebanon. The reporter had come up empty when searching for information in online Lebanese business registries.

I immediately started to think about how this company would be spelled in Arabic, and especially with the Lebanese accent. Of course, I knew beforehand that this company name must be mentioned in English inside the online company records in Lebanon. But the search engine of the Lebanese commercial registry shows results only in Arabic. This was why the reporter had come up empty.

For example, a search for "Josons" in the official Commercial Register gives us this result:

As you can see, the results are (0), however, we should not give up and quit. The first step is to guess how Josons is written in Arabic. There could be a number of potential spellings. To start, I put did a Google search with the word

“Lebanon” in Arabic next to the English company name: josons لبنان. The first page of search results shows that the company’s Arabic name is جوسانز as in this official directory:

Josons (@JOSONS_Lebanon) | Twitter
https://twitter.com/josons_lebanon
The latest Tweets from **Josons** (@JOSONS_Lebanon): "Let's Re-build our **Lebanon** together... http://t.co/0VJarwkbm4"

Josons :: Beirut.com :: Beirut City Guide
www.beirut.com/l/29834
**Josons**, Tools & Hardware, Zouk Mosbeh, Beirut: Founded in 1975, Joseph Abi ... can be called a a safe retreat for all hunters in **Lebanon** and the Middle East.

أسلحة وذخائر، أجزاؤها ولوازمها - دليل الصادرات والصناعة في لبنان
www.**lebanon**-industry.com/ar/Sections.aspx?Id1... Translate this page
الشركة الصناعية لابناء جوزيف ابي سمعان-جو سانز فا, جبل **لبنان**, اهمج, الخريطة, 09/504540-644444-
**josons@josons**.com ,03/444429 ...

Josons - Kesserwen, كسروان, Lebanon News and Events
www.kesserwen.org/n/single-dalil.php?id=1384 Translate this page
موقع الكتروني اخباري ينشر أخبار **لبنان** بشكل عام ومنطقة كسروان الفتوح بشكل خاص بغض النظر عن الانتماءات الفنوية
أو السياسية! كسروان للجميع! Mob: 71062040 ...

Bayt.com - لبنان - Josons وظائف في
www.bayt.com/ar/company/**josons**-1470342/jobs/ Translate this page
**Josons**. القطاع: دعم الأعمال; الموقع: **لبنان**; النوع: صاحب عمل (القطاع الخاص); الموظفين: 10-49 موظف; الموقع
الالكتروني: http://www.**josons**.com ...

That was also confirmed by searching in an online Lebanese business directory.

Now we have the company name in Arabic. A search with the name جوسانز in the Commercial Register shows that the company was registered twice — once onshore and another offshore.

## Cultures of writing

That was one example of how to deal with language challenges when gathering information about companies in the MENA region. Doing this work often requires working with Arabic, French, English and Kurdish, in addition to many different Arabic accents.

The first step is to determine which language to search for the information you need, and then to figure out the spelling in Arabic. However, keep in mind that the pronunciation of a single word can differ widely among Arabic- speaking countries.

For example, in order to search for a holding company, it's useful to know how to write the word

“group” in the Arabic database of business registries. However, there are three different ways of writing this word based on how the English word “group” is transliterated into Arabic. (Arabic has no letter for the “p” sound.).

1. In the Jordanian business registry, for example, it is written as: جروب

دائرة مراقبة الشركات
Companies Control Department

العودة الى موقع الدائرة

المملكة الاردنية الهاشمية
وزارة الصناعة والتجارة
دائرة مراقبة الشركات

***تنبيه هام ... سوف يتم عرض اول 500 سجل فقط ***

الشركات المسجلة

| مسلسل | اسم الشركة | النوع | الرقم | تاريخ التسجيل | راس المال | الحالة | المحافظة | التلفون |
|---|---|---|---|---|---|---|---|---|
| | امكان انترناشونال جروب ش.م.ح | أجنبية-فرع غير عامل | 2614 | 2013/12/08 | | | عمان | |
| | غلوبال نومادز جروب / الاردن | لا تهدف إلى ربح | 410 | 2013/03/17 | 50,000 | | عمان | 0797418883 |
| | ألفا فلايت جروب ليمتد | أجنبية-فرع غير عامل | 2515 | 2012/07/17 | | | عمان | |
| | أي . م . و . جروب . أيه . جي | أجنبية-فرع غير عامل | 2204 | 2008/06/17 | | | عمان | 0795432111 |
| | ادجو منجمنت جروب (اي. ام. جي) اس. ايه | أجنبية-فرع غير عامل | 1877 | 2006/07/11 | | | عمان | |
| | انتلاف بيلفنجر + بيرجروباساقانت فيركه | أجنبية - فرع عامل | 608 | 1998/06/21 | | | عمان | |
| | (ادجومانجمنت جروب (اى ام.جى | أجنبية-فرع غير عامل | 546 | 1992/11/19 | | | عمان | 065820005 |
| | ار بي اس جي ريموت بروجكتس سيرفيسيز جروب جي ام بي اتش | أجنبية-فرع غير عامل | 1749 | 2006/02/13 | | | عمان | 5921447 |
| | امكان انترناشونال جروب انك | أجنبية-فرع غير عامل | 2387 | 2010/11/02 | | | عمان | 5666360 |
| | | | | 2013/06/24 | 100,000 | | | |

دائرة مراقبة الشركات
Companies Control Department

العودة الى موقع الدائرة

المملكة الاردنية الهاشمية
وزارة الصناعة والتجارة
دائرة مراقبة الشركات

***تنبيه هام ... سوف يتم عرض اول 500 سجل فقط ***

الشركات المسجلة

| مسلسل | اسم الشركة | النوع | الرقم | تاريخ التسجيل | راس المال | الحالة | المحافظة | التلفون |
|---|---|---|---|---|---|---|---|---|
| | امكان انترناشونال جروب ش.م.ح | أجنبية-فرع غير عامل | 2614 | 2013/12/08 | | | عمان | |
| | غلوبال نومادز جروب / الاردن | لا تهدف إلى ربح | 410 | 2013/03/17 | 50,000 | | عمان | 0797418883 |
| | ألفا فلايت جروب ليمتد | أجنبية-فرع غير عامل | 2515 | 2012/07/17 | | | عمان | |
| | أي . م . و . جروب . أيه . جي | أجنبية-فرع غير عامل | 2204 | 2008/06/17 | | | عمان | 0795432111 |
| | ادجو منجمنت جروب (اي. ام. جي) اس. ايه | أجنبية-فرع غير عامل | 1877 | 2006/07/11 | | | عمان | |
| | انتلاف بيلفنجر + بيرجروباساقانت فيركه | أجنبية - فرع عامل | 608 | 1998/06/21 | | | عمان | |
| | (ادجومانجمنت جروب (اى ام.جى | أجنبية-فرع غير عامل | 546 | 1992/11/19 | | | عمان | 065820005 |
| | ار بي اس جي ريموت بروجكتس سيرفيسيز جروب جي ام بي اتش | أجنبية-فرع غير عامل | 1749 | 2006/02/13 | | | عمان | 5921447 |
| | امكان انترناشونال جروب انك | أجنبية-فرع غير عامل | 2387 | 2010/11/02 | | | عمان | 5666360 |
| | | | | 2013/06/24 | 100,000 | | | |

2. In Lebanon, its: غروب

Republic of Lebanon
Ministry of Justice
COMMERCIAL REGISTER

الجمهورية اللبنانية
وزارة العـــدل
السجل التجاري

رقم التسجيل أو الإسم التجاري: غروب
بحث
طريقة البحث: أدخل أي جزء من رقم السجل أو الإسم التجاري واضغط على زر البحث

نتائج البحث

عدد النتائج = 840

1900001 - انترناشونال ترايدنغ غروب (هولدنغ ) ش.م.ل.
بيروت (ب) - الشكل التجاري: هولدينغ، تاريخ التسجيل: 5/21/2002 12:00:00 AM

1900004 - فرنسيس كتانة غروب ش.م.ل.(شركة قابضة)
بيروت (ب) - الشكل التجاري: هولدينغ، تاريخ التسجيل: 5/23/2002 12:00:00 AM

1800008 - شركة أم.أن.جي.بي. غروب ش.م.ل.(اوف شور ).
بيروت (ب) - الشكل التجاري: اوف شور، تاريخ التسجيل: 6/6/2002 12:00:00 AM

70376 - شركة ميدل ايست كابيتال غروب ش.م.ل. ( ام.اي.سي.جي)
بيروت (ب) - الشكل التجاري: ش.م.ل، تاريخ التسجيل: 7/1/1996 12:00:00 AM

1900012 - شركة غروب فور هولدنغ ش.م.ل.
بيروت (ب) - الشكل التجاري: هولدينغ، تاريخ التسجيل: 6/13/2002 12:00:00 AM

77115 - شركة حب الله غروب ش.م.ل.

تعريف السجل التجاري
تسجيل التجار
المؤسسة التجارية
الشركات التجارية
الدفاتر التجارية
أحكام عامة
نماذج
أخبار
إتصل بنا
عودة الى الصفحة الرئيسية

©2012 وزارة العدل اللبنانية،
جميع الحقوق محفوظة.
إتفاقية رفع مسؤولية

3. The third spelling is shown in the Tunisian registry of commence: قروب

Personnne Morale | Personnne Physique | S'inscrire

Sociétés : 163009 Personnes : 243152

Vos Critères de Recherche

Recherche Avancée : Personne morale

الاسم الجماعي : قروب

Résultat 1 à 10 sur un total de 450 registres

1 2 3 4 5 6 7 8 9 10

| Dénomination Sociale | Nom Commercial | الاسم التجاري | الاسم الجماعي | Visualiser |
|---|---|---|---|---|
| ZIRICON GROUP ET COMPAGNIE | | | زيركون قروب شركاتهم | |
| STE RIHEM GROUP SARL | | | شركة ريهام قروب | |
| ABI CONSULTING GROUPE | | | أ.ب.إي كونسيلتينغ قروب ش م م | |
| STE PITO GROUPE | | | شركة بيتو قروب | |
| STE DON-ARE GROUP | | | شركة دون أ قروب | |
| SOCIETE OHF GROUP | OHF GROUP | او هاش اف قروب | شركة او هاش اف قروب | |
| STE JEMAL VENDING GROUP | | JEMAL VENDING GROUP | شركة الجمل فنديق قروب | |
| THE JUST GROUB | THE JUST GROUB | ذي جاست قروب | ذي جاست قروب | |
| STE LILY GROUP | STE LILY GROUP | شركة ليلي قروب | شركة ليلي قروب | |
| STE LGI-GROUP | STE LGI-GROUP | "شركة "ل.ج.اي.قروب | "شركة "ل.ج.اي.قروب | |

ser au moins un critère de recherche');

Also be aware that even within the same registry you should search using multiple spellings of the same word. For example, the word “global” might be written like غلوبال or like غلوبل. You can find both spellings in the Bahraini business registry:

## بحث السجل التجاري لوزارة الصناعة والتجارة

### تفاصيل السجل التجاري

### نتيجة البحث

الاسم التجاري (بالعربية) مثال' غلوبل'

إعداد تقرير | تحميل النتيجة

| رقم التسجيل التجاري | إسم الشركة (إنجليزي) | إسم الشركة (عربي) | نوع الشركة | تاريخ التسجيل | تاريخ الاستحقاق | الحالة |
|---|---|---|---|---|---|---|
| 6263-5 | GLOBAL GATE WELDING AND FABRICATION | غلوبل جيت للحداده والتجاره | مؤسسة فردية | 21/06/2007 | 21/06/2015 | نشطة |
| 28568-1 | GHLOUBAL PUBLISHING | غلوبل للتوزيع | مؤسسة فردية | 02/12/1992 | 02/12/1993 | ملغي مع عدم استيفاء شروط الإلغاء |
| 78407-1 | GLOBAL BAHRAIN GARAGE | كراج غلوبل بحرين | مؤسسة فردية | 13/07/2011 | 13/07/2016 | نشطة |

مجموع السجلات المماثلة : 3 سجلات

اختر رقم السجل التجاري المعروض أعلاه للحصول على مزيد من التفاصيل.

رجوع

## بحث السجل التجاري لوزارة الصناعة والتجارة

### تفاصيل السجل التجاري

### نتيجة البحث

الاسم التجاري (بالعربية) مثال' غلوبال'

إعداد تقرير | تحميل النتيجة

| رقم التسجيل التجاري | إسم الشركة (إنجليزي) | إسم الشركة (عربي) | نوع الشركة | تاريخ التسجيل | تاريخ الاستحقاق | الحالة |
|---|---|---|---|---|---|---|
| 42430-1 | GLOBAL INVESTOR RELATIONS LEMTAD | غلوبال انفستور ريليشنز ليمتد | فرع لشركة أجنبية | 07/02/1999 | 07/02/2000 | تحت التصفية |
| 65469-1 | PIONEER GLOBAL INVESTMENTS LIMITED FOREI | بايونير غلوبال انفستمنتس ليمتد فرع لشركة | فرع لشركة أجنبية | 06/06/2007 | 03/05/2011 | تم تصفية المنشأة |
| 73236-1 | ABJAD GLOBAL ADVISORS BAHRAIN S.P.C | أبجد غلوبال أدفايسرز البحرين ش.ش.و | شركة الشخص الواحد | 05/11/2009 | 05/11/2011 | غير مجدد |
| 89561-1 | EXCELSIS GLOBAL W.L.L | إكسلسيس غلوبال ذ.م.م | شركة ذات مسئولية محدودة | 14/05/2014 | 14/05/2015 | نشطة |

مجموع السجلات المماثلة : 4 سجلات

اختر رقم السجل التجاري المعروض أعلاه للحصول على مزيد من التفاصيل.

رجوع

These examples demonstrate how an understanding of cultures, languages and other factors can play a role in ensuring how effectively you can make use of public data and information during an investigation.