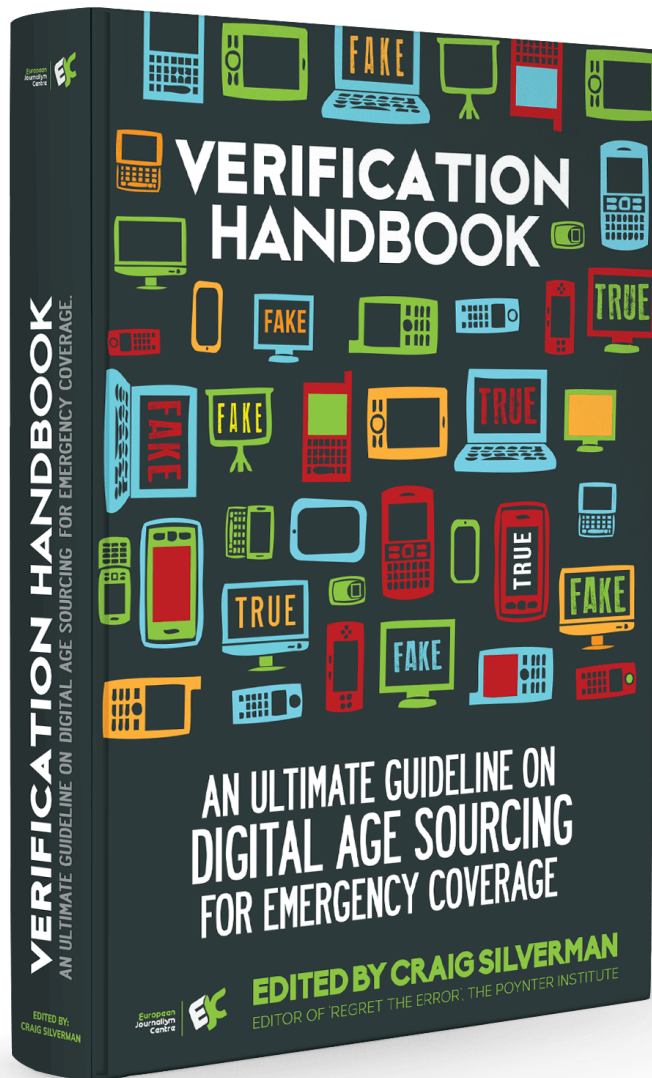


Verification Handbook





INVESTIGADOR_Z

INVESTIGADOR_Z

Chapters

01. [Foreword](#)
02. [1. When Emergency News Breaks](#)
03. [1.1. Separating Rumor From Fact in a Nigerian Conflict Zone](#)
04. [2. Verification Fundamentals: Rules to Live By](#)
05. [2.1. Using Social Media as a Police Scanner](#)
06. [3. Verifying User-Generated Content](#)
07. [3.1. Monitoring and Verifying During the Ukrainian Parliamentary Election](#)
08. [4. Verifying Images](#)
09. [4.1. Verifying a Bizarre Beach Ball During a Storm](#)
10. [4.2. Verifying Two Suspicious “Street Sharks” During Hurricane Sandy](#)
11. [5. Verifying Video](#)
12. [5.1. Verifying a Key Boston Bombing Video](#)
13. [5.2. Investigating a Reported ‘Massacre’ in Ivory Coast](#)
14. [5.3. Confirming the Location and Content of a Video](#)
15. [6. Putting the Human Crowd to Work](#)
16. [6.1. Tripped Up by Arabic Grammar](#)
17. [7. Adding the Computer Crowd to the Human Crowd](#)
18. [7.1. How OpenStreetMap Used Humans and Machines to Map Affected Areas After Typhoon Haiyan](#)
19. [8. Preparing for Disaster Coverage](#)
20. [8.1. How NHK News Covered, and Learned From, the 2011 Japan Earthquake](#)
21. [9. Creating a Verification Process and Checklist\(s\)](#)
22. [9.1. Assessing and Minimizing Risks When Using UGC](#)
23. [9.2. Tips for Coping With Traumatic Imagery](#)
24. [10. Verification Tools](#)
25. [“VISUALIZE JUSTICE: A Field Guide to Enhancing the Evidentiary Value of Video for Human Rights”](#)
26. [Verification and Fact Checking](#)
27. [Creating a Verification Workflow](#)
28. [Tracking Back a Text Message: Collaborative Verification with Checkdesk](#)
29. [The Fake Football Reporter](#)
30. [The Story of Jasmine Tridevil: Getting around Roadblocks to Verification](#)
31. [Stolen Batmobile: How to Evaluate the Veracity of a Rumor](#)
32. [Russian Bear Attack: Tracking Back the Suspect Origin of a Viral Story](#)
33. [Educator’s Guide: Types of Online Fakes](#)

Foreword

"In today's digital environment, where rumors and false contents circulate, journalists need to be able to actively sort out true, authentic materials from the fakes. This groundbreaking handbook is a must-read for journalists dealing with all types of user generated contents."

- Wilfried Ruetten, Director, The European Journalism Centre (EJC)

"Accurate information can be a life-saving resource during a humanitarian crisis, but the circumstances from which these crises emerge are typically the most difficult in which to gather reliable information. This book will help not only journalists but anyone working in humanitarian situations in the field to verify facts on the ground."

- William Spindler, Spokesman, The United Nations High Commissioner for Refugees (UNHCR)

"This handbook will be essential for journalists covering interreligious and interethnic conflicts to report in a more balanced, transparent and accurate way, and ultimately help defuse tensions across and within communities."

- Matthew Hodes, Director, The United Nations Alliance of Civilizations (UNAOC)

"In these times, knowing what is real and how to verify news and other information is essential. This handbook provides essential tools for everyone, journalism and consumer."

- Howard Finberg, Director of Training Partnerships and Alliances, The Poynter Institute

"Getting the facts right is a cardinal principle of journalism but media struggle to be ethical when a big story is breaking. This handbook helps news makers keep faith with truth-telling - even when online speculation is rampant."

- Aidan White, Director, The Ethical Journalism Network (EJN)

"It's all about the right information at the right time in the right place. When there is limited access to the disaster-affected areas, it's crucial for aid workers to gather information via social networks effectively. This handbook would be useful for aid workers working on the ground, as well as online volunteers."

- Christoph Dennenmoser, Team Lead Urgent Needs, Humanity Road Inc.

1. When Emergency News Breaks

Written by **Craig Silverman** and **Rina Tsubaki**

"... There is a need on the part of all journalists to never assume anything and to always cross-check and verify in order to remain trusted sources of news and information."

- Santiago Lyon, vice president and director of photography, The Associated Press

After an 8.1 magnitude earthquake struck northern India, it wasn't long before word circulated that 4,000 buildings had collapsed in one city, causing "innumerable deaths." Other reports said a college's main building, and that of the region's High Court, had also collapsed.

It was a similar situation when a 9.0 magnitude earthquake hit northeastern Japan. People heard that toxic rain would fall because of an explosion at an oil company's facilities, and that it was not possible for aid agencies to air drop supplies within the country.

They were false rumors, every single one of them.

It's a fundamental truth that rumors and misinformation accompany emergency situations. That earthquake in India? It occurred in 1934, long before the Internet and social media. The earthquake in Japan came in 2011.

Both quakes resulted in rumors because uncertainty and anxiety - two core elements of crises and emergency situations - cause people invent and repeat questionable information.

"In short, rumors arise and spread when people are uncertain and anxious about a topic of personal relevance and when the rumor seems credible given the sensibilities of the people involved in the spread," write the authors of "Rumor Mills: The Social Impact of Rumor and Legend."

An article in Psychology Today put it another way: "Fear breeds rumor. The more collective anxiety a group has, the more inclined it will be to start up the rumor mill."

In today's networked world, people also intentionally spread fake information and rumors as a joke, to drive "likes" and followers, or simply to cause panic.

As a result, the work of verification is perhaps most difficult in the very situations when providing accurate information is of utmost importance. In a disaster, whether its cause is natural or human, the risks of inaccuracy are amplified. It can literally be a matter of life and death.



Jānis Krūms

@jkrums



Follow

<http://twitpic.com/135xa> - There's a plane in the Hudson. I'm on the ferry going to pick up the people. Crazy.

Reply Retweet Favorite Buffer More

122

RETWEETS

699

FAVORITES



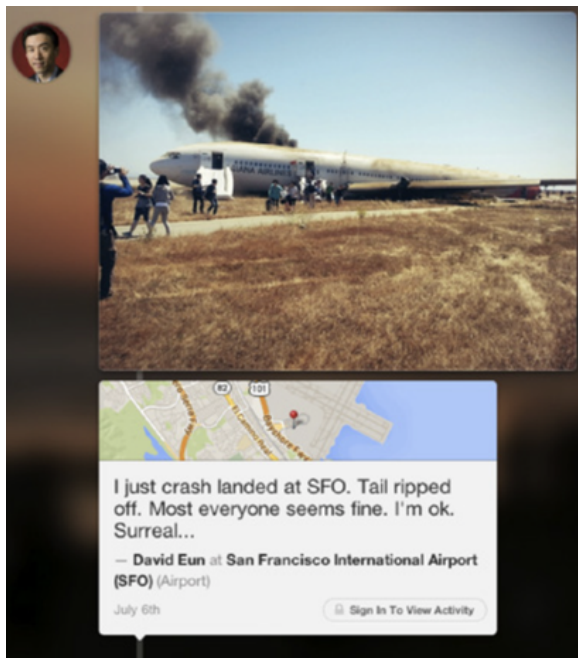
3:36 PM - 15 Jan 09

Yet amid the noise and hoaxes there is always a strong signal, bringing valuable, important information to light. When a US Airways flight was forced to land on the Hudson River, a man on a ferry was the source of an urgent, eye-opening image that only a bystander could have captured at that moment:



People on the ground are even more valuable in places where journalists have little or no access, and aid agencies have not been able to operate. Today, these witnesses and participants often reach for a phone to document and share what they see. It could be a bystander on a boat in a river - or a man who just walked away from a plane crash, as with this example from 2013:

INVESTIGADOR_Z



The public relies on official sources such as news organizations, emergency services and government agencies to provide credible, timely information.

But, at the same time, these organizations and institutions increasingly look to the public, the crowd, to help source new information and bring important perspective and context. When it works, this creates a virtuous cycle: Official and established sources of information - government agencies, NGOs, news organizations - provide critical information in times of need, and work closely with the people on the ground who are first to see and document an emergency.

To achieve this, journalists and humanitarian and emergency workers must become adept at using social media and other sources to gather, triangulate and verify the often conflicting information emerging during a disaster. They require proven processes, trustworthy tools, and tried and true techniques. Most of all, they need to gain all of the aforementioned before a disaster occurs.

A disaster is no time to try to verify on the fly. It's not the moment to figure out what your standards and practices are for handling crowdsourced information. Yet it's what many - too many - newsrooms and other organizations do.

Fortunately, an abundance of tools, technologies and best practices have emerged in recent years that enable anyone to master the new art of verification, and more are being developed all the time.

It is, in the end, about achieving a harmony of two core elements: Preparing, training and coordinating people in advance and during an emergency; and providing them with access and resources to enable them to take full advantage of the ever-evolving tools that can help with verification.

The combination of the human and the technological with a sense of direction and diligence is ultimately what helps speed and perfect verification. Admittedly, however, this is a new combination, and the landscape of tools and technologies can change quickly.

This book synthesizes the best advice and experience by drawing upon the expertise of leading practitioners from some of the world's top news organizations, NGOs, volunteer and technical communities, and even the United Nations. It offers essential guidance, tools and processes to help organizations and professionals serve the public with reliable, timely information when it matters most.

The truth is that good professionals often fall for bad information, and that technology can lead us astray just as much as it can help. This can be even more true when so much information is moving at such a fast pace, and when so many newsrooms and organizations lack formal verification training programs and processes.

“The business of verifying and debunking content from the public relies far more on journalistic hunches than snazzy technology,” wrote David Turner in a [Nieman Reports article](#) about the BBC’s User Generated Content Hub. “While some call this new specialization in journalism ‘information forensics,’ one does not need to be an IT expert or have special equipment to ask and answer the fundamental questions used to judge whether a scene is staged or not.”

This realization that there is no silver bullet, no perfect test, is the starting point for any examination of verification, and for the work of providing reliable information in a disaster. This requires journalists and others to first look to the fundamentals of verification that have existed for decades and that won’t become obsolete.

Steve Buttry focuses on a core question at the heart of verification in his chapter. Joining that is this list of fundamentals:

- Put a plan and procedures in place before disasters and breaking news occurs.
- Develop human sources.
- Contact people, talk to them.
- Be skeptical when something looks, sounds or seems too good to be true.
- Consult credible sources.
- Familiarize yourself with search and research methods, and new tools.
- Communicate and work together with other professionals - verification is a team sport.

One other maxim that has been added to the above list in recent years is that when trying to evaluate information - be it an image, tweet, video or other type of content - you must verify the source and the content.

When The Associated Press promoted Fergus Bell to take the lead in creating and practicing its process for confirming user-generated video, he first looked to the organization’s long- standing guidance on verification, rather than to new tools and technology.

“AP has always had its standards and those really haven’t changed, and it was working with those standards that we were able to specifically set up workflows and best practices for dealing with social media,” Bell said. “So AP has always strived to find the original source so that we can do the reporting around it. And that’s always the way that we go about verifying UGC. We can’t verify something unless we speak to the person that created it, in most cases.”

By starting with these fundamentals, organizations can begin to build a reliable, repeatable process for verifying information during emergency situations. Verifying information on social networks, be it claims of fact, photos or video, becomes easier once you know your standards, and know how to apply them.

That’s when it’s possible to make the best use of tools such as EXIF readers, photo analysis plug-ins, advanced Twitter search, whois domain lookups and the other tools outlined in this book.

Along with that toolkit, and the standards and processes that inform how we use the tools, there is also the critical element of crowdsourcing: bringing the public into the process and working with them to ensure we all have better information when it matters most.

Andy Carvin, who recently left the job of senior social strategist at NPR, is perhaps the most celebrated and experienced practitioner of crowdsourced verification. He said the key is to work with the crowd to, as the NPR motto goes, “create a more informed public.”

“When a big story breaks, we shouldn’t just be using social media to send out the latest headlines or ask people for their feedback after the fact,” he said in a keynote address at the International Journalism Festival.

He continued:

We shouldn’t even stop at asking for their help when trying to cover a big story. We should be more transparent about what we know and don’t know. We should actively address rumors being circulated online. Rather than pretending they’re not circulating, or that they’re not our concern, we should tackle them head-on, challenging the public to question them, scrutinize them, understand where they might have come from, and why.

This book is a guide to help all of us - journalists, emergency responders, citizen reporters and everyone else - gain the skills and knowledge necessary to work together during critical events to separate news from noise, and ultimately to improve the quality of information available in our society, when it matters most.

1.1. Separating Rumor From Fact in a Nigerian Conflict Zone

Written by **Stéphanie Durand**

The region of Jos in Central Nigeria is traditionally known as the “Home of Peace and Tourism.” Today, and for some time now, it is home to an ongoing war along religious and sectarian lines.

Jos straddles the north-south border of Nigeria. The northern part of the country is predominantly Muslim; the south is predominantly Christian.

The crisis in Jos has led to alarming headlines such as “Islamic Assailants Kill Hundreds of Christians near Jos” and “Muslims Slaughter Christians in Central Nigeria.” Those headlines and others like it prompted some religious leaders to blame the media for inciting religious violence because of the provocative nature of the reports.

But there is deadly violence in Jos and the press must accurately tell that story. To do so, they must sift through an increasing number of rumors that spread via text messages, social media and blogs - and be careful to avoid publishing false information that further enflames the situation.

Local journalists are also exposed to intimidation, self-censorship and fear of retribution from state authorities or militants. International media face challenges from decreasing resources that result in foreign reporters' working alone to cover an entire region

This can affect their knowledge of the local context and sensitivity to it. It also increases their reliance on content gathered and distributed by (often unknown) witnesses on the ground.

Journalists must be careful to verify what they discover, or risk increasing tensions and generating reprisal attacks based on nothing more than rumors.

In January 2010, when news outlets started reporting another major conflict in Jos, rumors began to spread about mobs armed with knives and machetes around houses, mosques and churches. Witnesses reported different causes of the conflict: Some said it was because of the rebuilding of houses destroyed by riots in 2008, others a fight during a football match, or the burning of a church.

Text messages also played a significant role in directly inciting violence with messages such as “slaughter them before they slaughter you. Kill them before they kill you.”

At the same time, blogs regularly displayed photos of the victims of violence.

The verification process is more crucial than ever in a situation where misperception and fear pervade all sides. It is essential for journalists to remove themselves from the passions of those involved, and verify the accuracy of accounts that narrate or visually feature ethnic or religious violence. Debunking a false rumor about a murderous rampage, or impending crisis, can literally save lives.

As is the case elsewhere, in Jos social media perpetuate misinformation, while at the same time enabling journalists to connect and interact with members of the public as part of their work. Social media also provide a platform to respond to rumors, and verify information that ultimately creates the type of trust and transparency necessary to avoid an escalation of conflict.

In Jos, the application of verification, in collaboration with the public, helps the media play a role in diffusing tension and containing conflict. It results in, and encourages, fair and accurate reporting that is sorely needed.

While this is certainly not the only response needed to alleviate tensions, such reporting goes a long way towards dissipating the fear, suspicion and anger that is at the heart of ethnic and religious conflicts.

2. Verification Fundamentals: Rules to Live By

Written by **Steve Buttry**

In 1996, I did a project on an American high school [girls basketball team that had won the Iowa state championship 25 years earlier](#). I interviewed all 12 members of the Farragut team, as well as the star and coach of Mediapolis, the team Farragut beat for the championship.

I asked them all how Farragut won the game. They gave different, often vivid, accounts of the same story: Mediapolis star Barb Wischmeier, who was 6 feet tall, scored easily on the shorter Farragut girls early in the game, and Mediapolis took the lead.

The Farragut coach sent Tanya Bopp, who was barely 5 feet, into the game to guard Wischmeier. Bopp drew several charging fouls (some remembered specifically that it was three or four fouls) on the larger girl, who became flustered and less aggressive. Farragut came back to win the game.

I didn't question these consistent memories in my reporting, but learned almost by accident that they were exaggerated. One of the girls loaned me a video of the game. I watched the whole game, looking for details that would help my story. I wasn't challenging anyone's memory, but when I finished the tape, I thought I must have missed something. So I watched it again.

Tiny Tanya Bopp drew only one foul on the larger girl. It did fluster the Mediapolis star and was the turning point of the game, but it happened only once. All those firsthand accounts I had heard were inaccurate, fueled by the emotions (joy or anguish) of an important moment in their lives, and shaped by a legend that grew from the game.

The legend - and the opportunity to honor it by debunking it - gave me a great narrative thread for [my article](#) but also taught me a lesson in verification: Don't trust even honest witnesses. Seek documentation.

Legends are fine, and even fun, for athletes and fans reliving the glory days of a legendary sports team. But journalists, activists or human rights workers must deal with the truth and must be committed to finding and telling the truth, especially in an emergency situation.

Whether we're assembling the tale of a natural disaster, a breaking news story or a bit of popular lore, storytellers must remember that we hear the product of faulty memory or limited perspective. If telling the truth is our goal, verification must be our standard.

We need to look and listen earnestly to the stories of our sources, watching for opportunities to verify. Does the source have a (new or old) video, photograph, letter or document that can offer verification or detail, or perhaps correct a foggy memory? And when we're supplied with this material, especially in emergency situations where time is tight, we need to investigate it and apply the fundamentals of verification.

Regardless of the moment and your role in it, the principles of verification are timeless and can be applied to any situation, be it breaking news, a natural disaster or the retelling of an apocryphal tale from a quarter century earlier.

The Essence of Verification

One of journalism's most treasured clichés, spouted by seasoned editors who ruthlessly slash other clichés from stories, is: "If your mother says she loves you, check it out."

But the cliché doesn't tell the journalist, or humanitarian professional, how to check it out. Verification is the essence of journalism, but it also illustrates the difficulty of journalism and the need for high standards: The path to verification can vary with each fact.

So this handbook won't present journalists, human rights workers and other emergency responders with one-size-fits-all simple steps to verification, but with strategies to check it out - whatever "it" is, and whatever motivation or role you have.

The question at the heart of verification is: "How do you know that?"

Reporters need to ask this question of their sources; editors need to ask it of reporters. Reporters, editors, producers and human rights workers need to ask the question in the third person about sources they can't ask directly: How do they know that?

Newsroom coach Rosalie Stemer adds a second question that illustrates the multilayered process of verification and the ethic of persistence and resourcefulness that verification demands: How else do you know that?

As we question sources and material, and as colleagues question us, we need to seek multiple sources of verification, multiple paths to the truth. (Or, to finding holes in the data or story before we act on it.)

Verification employs a mix of three factors:

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

Technology has changed how we apply all three factors: The 24/7 news cycle and rise of social media and user-generated content require us to gather and report as events unfold, making swift decisions about whether information has been sufficiently verified; digital tools give us new ways to find and reach sources; databases and ubiquitous cellphones with cameras give us massive amounts of documentation to seek and assess. Successful verification results from effective use of technology, as well as from commitment to timeless standards of accuracy.

The need for verification starts with the simple fact that many of our information sources are wrong. They may be lying maliciously or innocently passing along misinformation. They may have faulty memories or lack context or understanding. They may be in harm's way and unable to provide everything they know, or unable to see the full picture of events as they unfold.

Our job is not to parrot sources and the material they provide, but to challenge them, triangulate what they provide with other credible sources and verify what is true, weeding from our work (before we publish, map or broadcast) what is false or not adequately verified.

Each of the many verification paths that we might take has its flaws: In many cases, and especially in emergency situations, we are increasingly presented with an abundance of official sources and can find firsthand sources, the people who actually saw - or even participated - in the events in question. But those accounts can be flawed.

West Virginia Gov. Joe Manchin told reporters in 2006 that 12 of 13 miners trapped underground had been [rescued from the Sago mine](#). What reporter wouldn't run with that story?

But the governor was wrong. Twelve of the miners died; only one was rescued. The governor relied on second- and thirdhand accounts, and was not challenged on how he knew the miners were alive. We need to question seemingly authoritative sources as aggressively as we challenge any source.

New Tools

Documentation has changed with technology. The video that helped me debunk the legend in 1996 wouldn't have been available from one of the team members if I'd tried doing that story 15 years earlier (though I still could have watched it by going to the archives of the TV station). And in the years since I used that video for verification, the availability of cellphones and security cameras has increased the amount and importance of video documentation. But the ease of digital video editing raises the importance of skepticism. And, of course, any video catches only part of the story.

Technology has also changed how we find and deal with sources and information. As participants and witnesses to news events share their accounts in words, photos and videos on social media and blogs, journalists can more quickly find and connect with people who saw news unfold both by using digital search tools and other technologies, and by crowdsourcing.

We can use new tools most effectively by employing them with those old questions: How do they know that? How else do they know that?

That old cliché about checking out Mom's love? I verified the source (the old Chicago City News Bureau) from multiple online sources: the [Chicago Tribune](#), [AJR](#) and [The New York Times](#). Even there, though, legend complicates verification. A 1999 [Baltimore Sun](#) article by Michael Pakenham said legend attributes the admonition to the bureau's longtime night city editor, [Arnold Dornfeld](#) (as three of the articles linked above do), but "Dornie said it was another longtime editor there, [Ed Eulenberg](#), who actually said it first."

2.1. Using Social Media as a Police Scanner

Written by **Anthony de Rosa**

The medium by which we're gathering information may change, but the principles of verification always apply. Challenging what you see and hear, seeking out and verifying the source, and talking to official and primary sources remain the best methods for accurate reporting.

At Circa, we track breaking news from all over the world - but we publish only what we can confirm. That requires that we use social media to monitor breaking news as it happens so we can apply verification

Remember that the information on social media should be treated the same as any other source: with extreme skepticism.

For the most part, I view the information the same way I would something I heard over a police scanner. I take in a lot and I put back out very little. I use the information as a lead to follow in a more traditional way. I make phone calls, send emails and contact primary sources who can confirm what I'm hearing and seeing (or not).

In the case of the 2013 shooting at the Los Angeles airport, for example, we observed reports from the airport coming from eyewitnesses and contacted LAPD, the LA FBI field office and the LA county coroner. If we couldn't independently verify what we saw and heard, we held it until we could.

Even in cases where major news organizations were reporting information, we held back until we could confirm with primary sources. Often these organizations cite unnamed law enforcement sources, and as we've seen with the Boston Marathon bombing, the Navy Yard shooting, the Newtown shooting and other situations, anonymous law enforcement sourcing is often unreliable.

Using TweetDeck to monitor updates

If social media is a police scanner, TweetDeck is your radio. There are a few ways you can create a dashboard for yourself to monitor the flow of updates.

I build Twitter lists ahead of time for specific uses. My list topics include law enforcement for major cities, reliable local reporters and news organizations for major cities, and specialized reporters. I can plug these lists into columns on TweetDeck and run searches against them, or simply leave them up as a monitoring feed.

Small plane lands in the Bronx

Here's how I used searches on TweetDeck during the January 2014 emergency landing of a small plane on a Bronx expressway to unearth breaking news reports and to triangulate and verify what I saw.

I noticed several tweets appear in my main timeline mentioning a plane landing on the Major Deegan Expressway in the Bronx section of New York, which is not a normal occurrence.



NYC Fire Wire
@NYCFireWire

Follow

Bronx *Plane Down* Major Deegan Expy. E-81 confirming a small plane down, no fire, appears to be an emergency landing.

Reply Retweet Favorite More

49
RETWEETS

6
FAVORITES



12:28 PM - 4 Jan 14

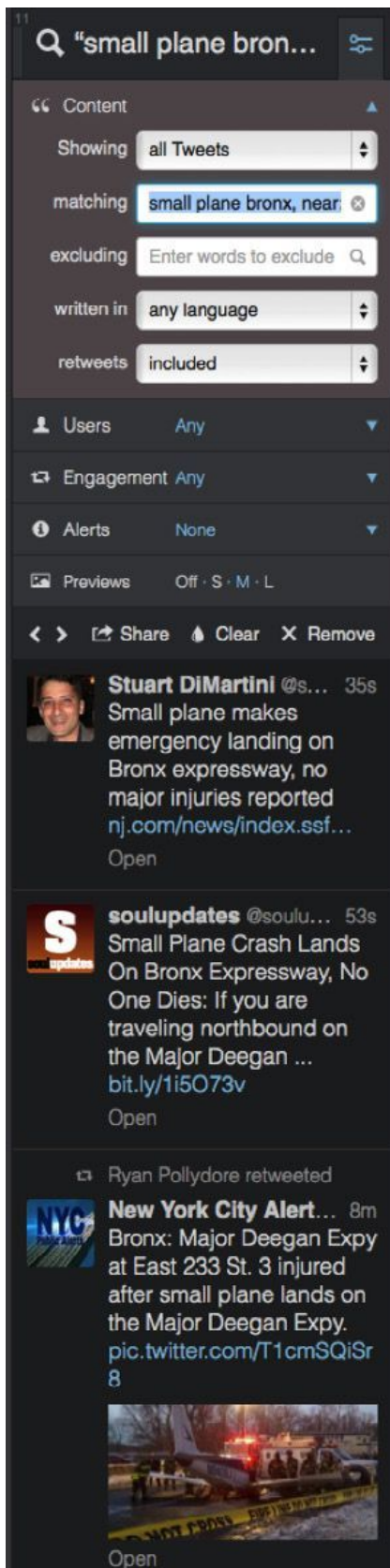
The plane landed around 3:30 p.m. local time in New York. (The tweet is dated in Pacific Standard Time.) This was one of the first tweets to report the landing. I follow a couple of NYC area accounts like, which act as a sort of police scanner for what's going on in the area. I won't report it until I can back it up, but it's useful to have as a potential alert to dig deeper.

After seeing the initial reports, I proceeded to run a search on TweetDeck using its ability to show tweets that only have images or video. I used the search terms "small plane" and "Bronx."

INVESTIGADOR_Z



The above results showed that credible local news sources were reporting the plane landing, and they had images. I also found additional information and images from a wider search of all tweets that used a location filter (within 5 miles of New York City) and the keywords "small plane" and "bronx":



I also searched within my specialized list of verified accounts belonging to New York State and City agencies, and used the location filter again. These credible sources (below) helped confirm the event.

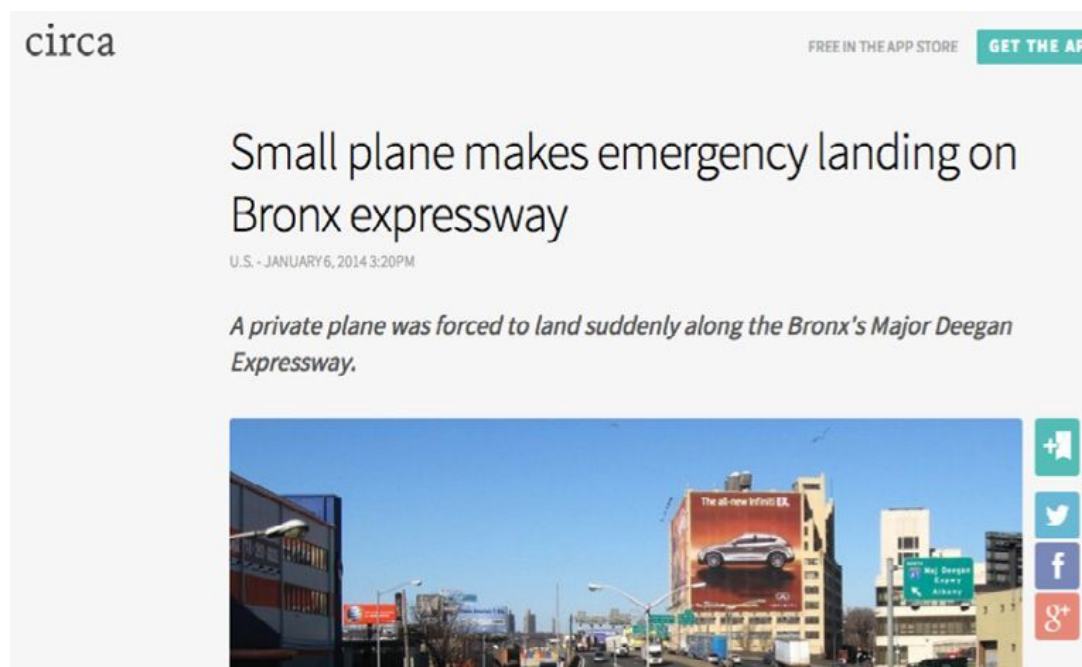
INVESTIGADOR_Z



At this point I contacted the public information office for the FDNY to confirm what I saw and ask for any other details they might have. I was told there were three people on board, two passengers and a pilot. We were later told the make/model of the plane, the name of the person the plane was registered to, and the hospital the pilot and passengers were taken to. Social media led us to the event - but we had to track the details down the old-fashioned way.

Feeling we had properly run down enough credible information to get started, we filed our story (see below). The Circa app offers readers an option to “follow” a story and receive push updates as more information is added. Our process is to get a story up as soon as possible with verified reports and continue to push out updates. TweetDeck

allows us to get a jump on a developing story and seek out reliable people (law enforcement, primary sources) we can contact to confirm the validity of social media updates. In some cases we contact the person who sent the information to Twitter and try to determine if they're reliable.



Building a body of evidence

The information you're seeing on social media should be the first step toward trying to verify what actually occurred, rather than the final word.

The key is to observe as much as you can, take in information and compare it to other content and information to build up a body of evidence. Find ways to corroborate what you find by directly contacting and verifying the people who are connected to the content you find.

As I said, treat social media as a police scanner.

INVESTIGADOR_Z

3. Verifying User-Generated Content

Written by: Claire Wardle

In less than a decade, newsgathering has been transformed by two significant developments.

The first is mobile technology. In the summer of 2013 an important tipping point was reached. For the first time, more than half (55 percent) of all new mobile phone handsets sold were smartphones.

By definition a smartphone has a high-quality camera with video capability, and it allows the user to easily connect to the Web to disseminate the pictures. As a result, more and more people have the technology in their pockets to very quickly film events they see around them, and share them directly with people who might be interested, as well as more widely via social networks.

The second, connected development is the social Web. When the BBC's User Generated Content Hub started its work in early 2005, they were reliant on people sending content to one central email address. At that point Facebook had just over 5 million users, rather than the more than one billion today. YouTube and Twitter hadn't launched. Now, every minute of the day, [100 hours of content is uploaded to YouTube](#), [250,000 tweets are sent](#) and [2.4 million pieces of content are shared on Facebook](#). Audience behavior has shifted substantially.

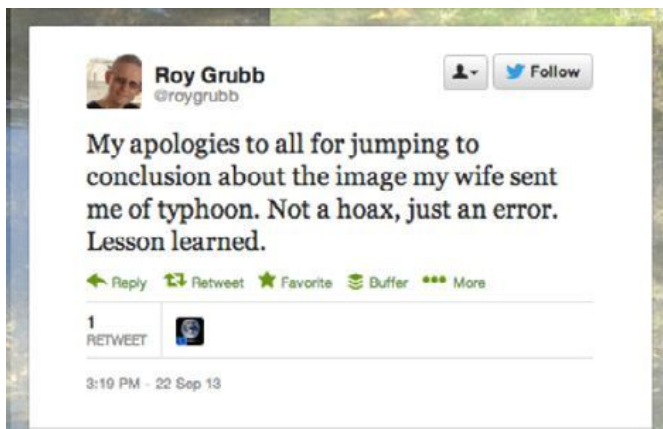
Rather than film something and, when prompted, send it to a news organization, people shoot what they see and upload it to Facebook, YouTube or Twitter. Research has shown very few audience members have enough understanding of the news process to think of their footage as valuable enough to send it, unprompted, to a news organization or [other entity](#). Essentially, they're uploading the content to share the experience with their friends and family.

Increasingly, at any news event around the world there are "accidental journalists": people standing in the right place at the right time with a smartphone in their hands. As Anthony De Rosa, the former social media editor for Reuters and current editor-in-chief of Circa, [writes](#): "The first thought of the shooter is usually not: 'I need to share this with a major TV news network' because they don't care about traditional television news networks or more likely they've never heard of them. They have, however, heard of the Internet and that's where they decide to share it with the world."

Similarly, during breaking news events, the audience is often more likely to turn to social networks for information, meaning first responders and emergency organizations are using social networks themselves. Unfortunately, these news events invite false information to circulate, either deliberately or by accident. Therefore, journalists and humanitarian professionals should always start from a position that the content is incorrect. During emergencies, when information can literally affect lives, verification is a critical part of the newsgathering and information dissemination process.

The importance of verification

The ability for anyone to upload content, and to label or describe it as being from a certain event, leaves many journalists, and particularly editors, terrified about being hoaxed or running with false content.



Some people go out of their way to deliberately hoax news organizations and the public by creating fake websites, inventing Twitter accounts, Photoshopping images or editing videos. More often, the mistakes that happen aren't deliberate. People, trying to be helpful, often find mislabeled content from previous news events and share it. Below is an example of a man apologizing after [tweeting a photo](#) emailed to him by his wife. She had told him it showed Typhoon Usagi as it headed toward Hong Kong; in fact it was an old image of an- other event.

People downloading content from YouTube and uploading it to their own accounts, claiming it as their own, cause other problems. This isn't a hoax - it's what is known as a "scrape" - but it means we have to work harder to find the original uploader of the content.

The difficulty of finding original footage was demonstrated when the U.S. Senate Intelligence Committee [released a playlist of 13 videos](#) that had originally appeared on YouTube, which they had used to look for evidence related to the 2013 chemical weapons attack on East Gouta in Syria. A number of these videos were taken from a well-known Syrian aggregator YouTube channel which regularly republishes videos from other people's channels. This suggested the videos within the playlist were not the original videos and were in fact "scrapes." Using a range of different verification techniques, Félim McMahon from Storyful was able to discover the original versions of these videos. He wrote up the process [here](#). What this example shows is that these issues are no longer just a concern for the journalism community.

Verification checks

Verification is a key skill, made possible through free online tools and old-fashioned journalism techniques. No technology can automatically verify a piece of UGC with 100 percent certainty. However, the human eye or traditional investigations aren't enough either. It's the combination of the two.

When a journalist or humanitarian professional finds a piece of information or content via social media, or has it sent to her, there are four elements to check and confirm:

1. Provenance: Is this the original piece of content?
2. Source: Who uploaded the content?
3. Date: When was the content created?
4. Location: Where was the content created?

1. Provenance: Confirming the authenticity of the piece of content

If you find content on a social media profile, you have to run a number of checks on that profile to make sure it is real.

In the case of a tweet, be aware that the site lemmetweetthatforyou.com makes it shockingly easy to fake a tweet, which can be then shared as a picture.

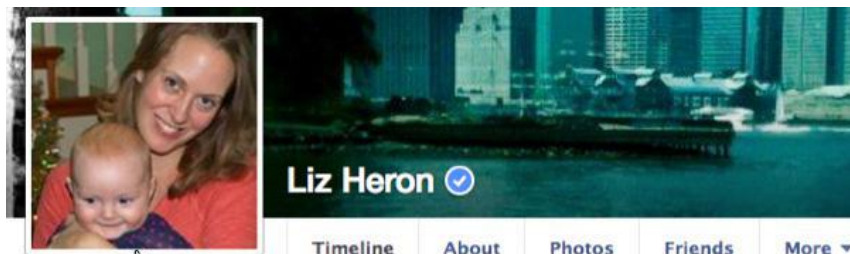
Another way people spread fake information on Twitter is by presenting the fake information as a retweet. For example: “Really? RT@JoeBiden I’m announcing my retirement from politics.” That makes it appear as if you’re simply retweeting an original tweet.

Fakers also often add a Twitter blue verification check mark to the cover photo on a faked account to make it appear legitimate. To check whether an account is actually verified, hover over the blue tick, and you will see the text “verified account” pop up. If it’s not there, it is not a verified account.

Facebook introduced a similar verification program, using the same blue tick system, for celebrities, journalists and government officials. Verified ticks can appear on Facebook pages as well as personal profiles. (As with Twitter, Facebook manages the verification program, and decides which verification requests to accept.) On Facebook pages, such as Usain Bolt’s below, the tick appears underneath the cover photo, next to the person’s name.



On personal profiles, the tick appears on the cover photo. Here’s the profile of Liz Heron, editor of emerging media at The Wall Street Journal:



It’s worth noting that, as with Twitter, people have been known to Photoshop blue ticks onto cover photos. So, as with Twitter, if you hover your mouse over the blue tick, the phrase “verified profile” will appear.

But as with Twitter, remember the verification process is far from transparent, so with less famous people, it can be unclear whether an unverified account is a fake, or whether they’re just not famous enough to be verified!



But even with these official verification programs in place, there is no quick way of checking whether an account is real, other than painstaking checks on all of the details available on the profile. Items to review include linked websites, location, previous pictures and videos, previous status updates or tweets. Who are their friends or followers? Who are they following? Do they feature on anyone else's lists?

If you're looking at a piece of rich content, such as a photo or video, one of the first questions is whether this is the original piece of footage or picture. Using reverse image search tools such as TinEye or Google Images³ you can find out whether it has been posted online previously. (For more detail on using these tools, see Chapter 4 of this book.)

While deliberate hoaxes are rare, they do happen. In recent years there have been relatively harmless hoax videos produced by [PR companies looking for publicity](#), and by [students completing an end-of-term assignment](#). There have also been deliberate attempts to create false content, particularly in Syria and Egypt, where discrediting the "enemy" can be achieved via reputable-looking content shared on social media channels.

Techniques include creating a false, but identical-looking website and [claiming responsibility for a bomb attack](#), or staging a gruesome incident and blaming the other side. Manipulation is relatively easy to do today, and whether you're Nancy Pelosi trying to create a photograph of all female Congresswomen even when some of them are late, or a Syrian activist group sharing video of a man appearing to be buried alive, any journalist or humanitarian professional has to start off by assuming a piece of UGC is false. (See Chapter 5 of this book for more detail about verifying video.)

2. Confirming the source

The ultimate goal when attempting to verify UGC is to identify the original uploader and get in touch with them.

In that conversation, the key questions involve discovering where someone was standing when they took the footage, what they could see, and the type of camera used to record the footage. (These questions provide the essential data to answer Steve Buttry's essential "How do you know that?" test outlined in the previous chapter.)

If someone is attempting to pass along false information, either deliberately or not, asking direct questions will often result in the person's admission that they did not actually film the footage themselves. Additionally, it is possible to cross-reference answers to some of these questions with available information by examining the EXIF data in a photo, or comparing video of a specific location to Google Street View, which we detail in subsequent chapters.

But first you have to find the person responsible for the content. Researching the history of an uploader can mimic the characteristics of an old-fashioned police investigation, and perhaps also make you feel more like a stalker rather than a journalist or researcher.

Some people list a great deal of information on their social profiles, and a real name (especially one that is not too common) can provide a wealth of information. As people live more of their lives on different social networks, they are often unaware how clues can be combined to build up a substantial dossier of information. A YouTube profile with little personal information listed but that includes a website URL can lead a journalist to a person's address, email and personal telephone number, via the website who.is.

3. Confirming the date of the event

Verifying the date of a piece of video can be one of the most difficult elements of verification. Some activists are aware of this fact and will show a newspaper from that day, with the date clearly visible when they share their footage. This obviously isn't foolproof, but if an uploader becomes known and trusted by organizations, be they

news or humanitarian, this is a helpful additional piece of information.

Be aware that YouTube date stamps its video using Pacific Standard Time. This can sometimes mean that video appears to have been uploaded before an event took place.

Another way to help ascertain date is by using weather information. [Wolfram Alpha](#) is a computational knowledge engine that, among other things, allows you to check weather from a particular date. (Simply type in a phrase such as “What was the weather in Caracas on September 24, 2013” to get a result.) This can be combined with tweets and data from local weather forecasters, as well as other uploads from the same location on the same day, to cross-reference weather.

4. Confirming the location

Only a small percentage of content is automatically geolocated, but mapping platforms - Google Maps, Google Earth, Wikimapia - of the first checks that need to be performed for video and photos, and it is quite incredible what can be located. Geolocation is always more difficult, however, when the imaging is out of date, for example in Syria, subject to damage from bombs or shelling, or on Long Island after Hurricane Sandy.

Activists who are aware of the challenges of verification often pan upward before or after filming some footage to identify a building that could be located on a map, whether that's a tall tower, a minaret or cathedral, or signpost. This is partly a result of news organizations' asking activist groups to do this, as well as [activists themselves sharing advice about best practice](#) when uploading UGC.

Verification as process

Unfortunately, people often see verification as a simple yes/no action: Something has been verified or not.

In practice, as described above and in subsequent chapters, verification is a process. It is relatively rare that all of these checks provide clear answers. It is therefore an editorial decision about whether to use a piece of content that originates from a witness.

Two recent academic studies performed content analysis of output on the BBC and Al Jazeera Arabic. They found that while these verification checks are undertaken by editorial staff, and considered absolutely necessary, the results of the checks are rarely shared with the audience.

As Juliette Harkin concluded in [her 2012 study](#), “[n]either BBC Arabic nor Al Jazeera Arabic explicitly mentioned in any of the programs or video packages that were evaluated whether the sources were verified or were reliable. The common on air explanation of ‘this footage cannot be verified,’ was absent in all the content evaluated for this study.”^f

There are recent moves to increase transparency with the audience about the verification checks made by journalists when a piece of UGC is used by a news organization. The AP and BBC are both working toward making their verification processes clearer; in August 2013, the BBC [said](#) that since a [comprehensive study into the use of UGC during the Arab Spring](#), “the BBC has adopted new wording for all user-generated footage where independent verification has not been possible,” letting its audience know what it knows.

It is likely that within the next few years, a new grammar of verification will emerge, with the audience expecting to be told what is known and what isn't known about a piece of UGC sourced from social media. With the audience able to see the same footage as the news organizations and others that gather material from the crowd, this level of transparency and accountability is required.

3.1. Monitoring and Verifying During the Ukrainian Parliamentary Election

Written by **Anahi Ayala Iacucci**

During the Ukrainian parliamentary elections of fall 2012, Internews Ukraine, a local NGO supported by the global nonprofit media organization [Internews](#), ran an election monitoring project called Elect.UA. It used a mix of crowdsourcing, mobile phones, social media, professional electoral monitoring and media monitoring to oversee the electoral campaign, and possible violations of or tampering with the results.

The project was built upon a fairly complex structure: 36 journalists around the country reported stories during the electoral campaign and on election day. At the same time, three different electoral monitoring organizations had workers reporting to the same platform using SMS, online forms and emails. Elect.UA also invited Ukrainians to report about their election experience using social media (Twitter and Facebook), mobile technology (SMS and a hotline number), a smartphone app, an online form or email.

All information coming from Internews-trained journalists and electoral monitors was automatically tagged as verified, while messages from the crowd were vetted by a team of 16 administrators in Kiev.

For the messages coming from the crowd, the admin team set up a verification protocol based on the source of the information: mobile technology, social media, online form or email.

For each source, the team would try to verify the sender of the information (when possible), the content of the information and the context. For each of those components the team would also try to establish if something could be 100 percent verified, or only partly verified.

For information coming via social media, [this image](#) shows the decision tree model used by administrators in the verification process.

The first step was to perform an online search of the information and its source to identify all possible digital traces of that person, and the piece of content. (For example, we examined other social media accounts, mentions by media articles, information about university, affiliations, etc.). The search was aimed at determining if the person was a reliable source, and if there was a trace of the information they provided elsewhere online.

The second step was to use the information collected to build a profile of the person, as well as a profile of the content they provided. For each of the 5Ws - who, what, when, where and why - administrators had to carefully determine what they could prove, and what they could not.

For multimedia content, the source verification protocol was the same, but we had a different path for the content. Photos and video were verified by looking for any identifiable landmarks, and by performing an analysis of the audio (to listen for language, dialects, slang words, background noise, etc.), clothes and of light (artificial or natural), among other elements in the content.

When a piece of information could not be verified with a sufficient degree of certainty, the report was sent back to an electoral monitor or a reporter on the ground for real-time, inperson verification.

For example, on September 28, 2012, Elect.UA received an anonymous message via its website that parliamentary candidate Leonid Datsenko had been invited for a discussion by a stranger, and then was intimidated in order to force him to withdraw from the elections.

INVESTIGADOR_Z

The next day, the administrators of the platform found [an article](#) in a reliable media source that included a record of the exchange. We still held the report for verification, and then, on October 1, local journalists [reported on a press conference about the incident](#). Elect. UA's local journalists also conducted interviews with local law enforcement services, who acknowledged this case to be true.

Overall, the Elect.UA team managed to verify an incredible amount of information using these protocols, and also noticed that the more the administrators became familiar with the verification process, the faster they were able to work. This proves that the verification of user generated content is a skill that can be systematized and learned, resulting in efficient, reliable results.

The decision tree model:



4. Verifying Images

Written by **Trushar Barot**

One powerful image can define a story.

That was certainly the case for BBC News' User Generated Content hub in the beginning of July 2005. It had been one week since the initial pilot team was set up to help collate the content being sent to BBC News by its audiences, and help get the best of it shown across TV, radio and online.

Then the July 7 bombings in London happened.

That morning, as the BBC and other news organizations reported a power surge on the London Underground, the UGC team started seeing a very different story emerging via content sent to BBC News directly from its audience.



Photo: Alexander Chadwick

This was one of the first images the team received. Before it was broadcast, the image was examined closely and the originator was contacted to verify his story and the details of what he saw. The photo inadvertently became one of the first examples of the UGC image verification process that has since moved toward standard practice across the industry.

That image, and others like it, showed the terror and chaos in London during the moments immediately after the attacks. As a result, it ensured that the reporting of the story quickly changed. It was the first significant example of UGC's proving critical to helping BBC News tell a major story more accurately, better and faster.

Today, the UGC team is embedded within the heart of the BBC newsroom. Its 20 journalists work across TV, radio, online and social media platforms to produce content sourced either directly from the BBC's audiences or from the wider Web.

Verification is critical to the success of what the UGC team produces. Technology has moved on considerably since 2005, bringing an exponential rise in the use of social networks and the power of mobile phones. These changes offer great benefits in our newsgathering processes, particularly on breaking news; they also bring great challenges.

Whether a trusted global news organization like the BBC or a humanitarian professional on the ground, the need to be fast at collecting and disseminating key images on a breaking news story has to be balanced with the need to be sure the images are credible and genuine. We also have to ensure copyright is protected and appropriate

INVESTIGADOR_Z

permissions are sought.

Since that day in 2005, the UGC team has developed a number of approaches to help in this process. While the technology will continue to change - as will the tools we use - the basic principles of image verification remain the same:

1. Establish the author/originator of the image.
2. Corroborate the location, date and approximate time the image was taken.
3. Confirm the image is what it is labeled/suggested to be showing.
4. Obtain permission from the author/originator to use the image.

Let's look at these points in more detail.

1. Establish the author/originator of the image

The obvious - and usually most effective - way of doing this is to contact the uploader and ask him directly if he is indeed the person who took the image.

Reaching out to the uploader via the social network account or email address the image was shared from is a first step, but it's also important to try to ascertain as much about the uploader's identity as possible. These details can help in determining whether he is in fact the original source of the image.

As outlined in the previous chapter, in many instances, people may try to be helpful by repost- ing images they have seen elsewhere. This happens frequently to news organizations - images are sent in by well-meaning members of the public to help report a story. Just by asking the sender to confirm if it's his image or not can save a lot of time in the verification process.

While tracking down the source of an image begins with the person who uploaded it, it often ends with a different person - the one who actually captured the image.

As referenced in an earlier chapter, an important step is to use a service like [Google Reverse Image Search](#) or [TinEye](#). Paste the image URL or a copy of the image into either and they will scan the web to see if there are any matches. If several links to the same image pop up, click on "view other sizes" to investigate further.

Usually, the image with the highest resolution/size should take you to the original source. (On Google Images, the resolution for each image result is listed just next to the image itself.) You can then check it against the image you have and see if the source appears authentic.

Quite often on a breaking news event, there will be no images of specific people that you want to illustrate the story with (particularly if they involve ordinary members of the public). Alternatively, you might want to confirm that an image you have of someone is actually them and not someone else with the same name.

I've found Pipl.com to be particularly helpful here as it allows you to cross-reference names, usernames, email address and phone numbers against online profiles of people. For interna- tional searches, WebMii is an additional resource that can help. LinkedIn is also proving to be a great way of verifying individuals and often provides additional leads for being able to track them down (through companies/organizations they are currently or previously associated with).

2. Corroborate the location, date and approximate time the image was taken

There are some useful journalistic and technical ways of establishing information such as date, location and other important details. One core way of gathering this information is when you speak to the creator/uploader of the image. These five questions continue to stand the test of time:

- Who are they?
- Where are they?
- When did they get there?
- What can they see (and what does their photo show)?
- Why are they there?

One important aspect to note here: If the image is from a dangerous location, always check that the person you are talking to is safe to speak to you. Also be aware of any issues about identifying the source through any details you broadcast about him or his images.

From our experience at the BBC, people who were really there will give visual answers, often describing the details in the present tense. ("I'm in the middle of X Street; I can see and hear Y.") The more vague the answer, the more caution you should exercise about what the source is telling you.

Another useful technique is to ask the person to send any additional images shot at the same time. It's rare that someone takes only one picture in a newsworthy situation. Having more than one image helps you learn more about how the events in question unfolded.

Once you've gathered the source's account of how the image was taken, work to corroborate the information further. Two primary methods can be used to investigate the contents of the photo itself and triangulate that with what you were told by the source.

First, check if the image has any metadata. Metadata, also referred to as "EXIF" data when it comes to digital images, refers to information embedded in an image. If the image is an original, there's a good chance you will see information about the make and model of the camera, the timestamp of the image (be careful though - if there is one, it could still be set to the manufacturer's factory setting or another time zone), and the dimensions of the original image, among other details. You can use software like Photoshop (look at the file information) or look for free online tools like [Fotoforensics.com](https://www.fotoforensics.com) or [Findexif.com](https://findexif.com) to generate an EXIF report.

Upload the image and the EXIF reader will return out whatever information is contained on the image. Some of the information is useful to those who have a more technical understanding of digital photography. But for the average person, data such as the date the photo was originally taken or the type of camera that took the image can sometimes help expose a lying source.

One note of caution here: The majority of social media image sites such as Twitter, Facebook and Instagram strip out most of the original metadata from images when they are uploaded onto their platforms, if not all. (Flickr seems to be an exception to this.)

Second, cross-reference the image with other sources. Awaken your inner investigator by examining the image closely. Quite often there will be clues that can help you verify the location and time it was taken:

- License/number plates on vehicles
- Weather conditions
- Landmarks
- Type of clothing
- Signage/lettering

INVESTIGADOR_Z

- Is there an identifiable shop or building?
- What is the type of terrain/environment in the shot?

3. Confirm the image is what it is labeled/suggested to be showing

An image may be authentic, but it could be inaccurately labeled. For example, during Hurricane Sandy, this image spread widely on Twitter and was described as being a shot of three soldiers standing guard at the Tomb of the Unknown Soldier during the storm:



The image was accurate in that it did show soldiers at the Tomb. **But it had been taken a month earlier, not during Sandy.** The picture had been posted on the Facebook page of the First Army Division East.

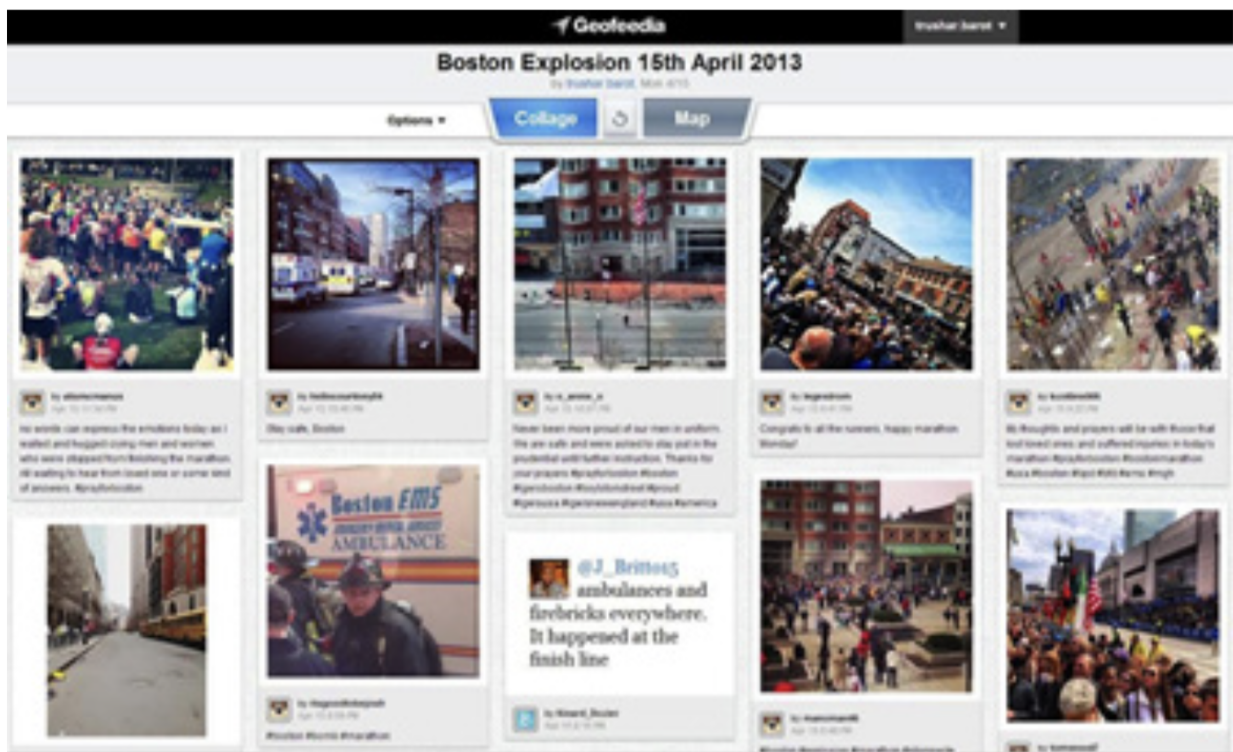
As part of verifying the date, time and approximate location of an image, it's also important you confirm that the image is what it purports to be. An authentic image can still be placed in a false context.

Use [Google Maps](#), [Bing Maps](#) or [Wikimapia](#) to help you verify locations. UGC images are increasingly being tagged on these services now, and they can also provide useful leads to follow up on, as well as different angles to locations you are investigating. (Learn more about using these mapping services for verification in Chapter 5: Verifying Video.)

Use weather sites that can give you accurate reports of conditions at that location on that date to confirm if the weather in the image matched. As noted in the previous chapter, [Wolfram Alpha](#) is very good at searching for weather reports at specific times and places.

If there is lettering (e.g. on a sign) in a different language within the image, use [Google Translate](#) to see if it can give you another clue to the location. The optical character reading tool [free-ocr.com](#) can also be helpful if you want to extract text from an image -which you can then run through an online translation.

Social media location services like Geofeedia and [Banjo](#) can also help establish the location from which an image was uploaded. These services use the GPS data from the mobile device that uploaded the image. While they currently capture only a small percentage of the social media content uploaded from a given location, they do provide a useful initial filter. The image below is an example of some of the photos captured by Geofeedia in the immediate aftermath of the Boston marathon bombings:



Along with those tools and techniques, for images it's also useful to check to see if similar images are being distributed by official news organizations or agencies. Are there any images from that location being uploaded on social media by others? If they show a similar scene from a different angle, that will also help establish credibility of the image.

Finally, on a big story, it's always worth double checking if a particularly strong image you come across appears on [Snopes](#), which specializes in debunking urban legends and misinformation on the Internet.

4. Obtain permission from the author/originator for use of the image

It is always best practice to seek permission from the copyright holder of images. Adding to this, copyright laws in many countries are increasingly clear that damages can be sought by the originator if permission isn't asked for or granted.

The terms and conditions with regards to the copyright of content uploaded on social media sites vary from service to service. Some, like Flickr, show clearly alongside the image if the photographer has retained all copyright, or if he allows Creative Commons usage. (It's a good idea to read up on [Creative Commons licenses](#) so you are familiar with how they differ.)

When seeking permission, it's important to keep a few details in mind:

- Be clear about the image(s) you wish to use.
- Explain how the image(s) will be used.
- Clarify how the photographer wishes to be credited (name, username, etc., keeping in mind that in some cases they may wish to remain anonymous).

Most importantly, remember that if you've gone through the above checks and processes and you're still in doubt - don't use the image!

4.1. Verifying a Bizarre Beach Ball During a Storm

Written by **Philippa Law** and **Caroline Bannock**

Storm force winds and rain brought flooding and power outages to the south of the U.K. in October 2013. This event affected a lot of people, so to widen and enrich the Guardian's coverage, we asked our readers to share their photos, videos and stories of the disruption via our user-generated content platform, GuardianWitness.

Among the contributions we received was a bizarre photo of what appeared to be a giant multicolored beach ball, at least twice the height of a double decker bus, on the loose at Old Street roundabout in London. This was one of those images that immediately evokes the question, "Is this too good to be true?" We were very aware that it could be a hoax.



We started verifying the user's photo by running it through Google reverse image search and TinEye to verify that the image hadn't been borrowed from another website. Users often try to show us a news event by sending pictures that have been published on other news sites, or shared on Twitter and Facebook. So a reverse image search is always the first check we make.

In the case of the rampant inflatable, Google returned no hits - which suggested the photo was either original or very recent and hadn't been picked up by any other news organizations - yet. Good content gets published very fast!

The most important verification tool we have is a direct conversation with the user. Every contributor to GuardianWitness has to share an email address, though there's no guarantee it's a correct one. So we emailed the user in question to try to make contact. In the meantime we continued with our verification checks.

Usually we would verify where a photo had been taken by comparing it with images on Google Street View, but as our team is familiar with the Old Street area, we recognized the view in the photo and felt reasonably confident the picture had been taken there. Although we knew the area, we didn't recall seeing a giant beach ball - so we searched online for earlier evidence. We found it had previously been tethered to the top of a building nearby. This finding meant the image was looking less like a hoax than it had first appeared.

We checked Twitter for mentions of the beach ball that morning and were able to confirm that there had been other sightings around the time the user claimed to have taken the photo. Our Twitter search also revealed a later photo, taken by another user, after the ball had deflated.

Finally, the user got in contact with us and, by speaking to him on the phone, we were able to confirm that he had taken the photo himself.

Having taken all these steps to verify the image, we were happy that the story held up to scrutiny. The compelling image of a runaway beach ball in the driving rain was published on the Guardian's live-blog and was shared widely on social media.

INVESTIGADOR_Z

4.2. Verifying Two Suspicious “Street Sharks” During Hurricane Sandy

Written by **Tom Phillips**

When Hurricane Sandy hit New York and New Jersey, I was running a blog called “Is Twitter Wrong?” an experiment at fact-checking viral images.

When a major natural disaster hits an area densely populated with heavy social media users - and media companies - one result is a huge number of images to sift through. Telling the good from the bad suddenly shot up the editorial agenda.

One particularly viral pair of images showed a shark supposedly swimming up a flooded New Jersey street. I teamed up with Alexis Madrigal from The Atlantic to try to verify these images.

One aspect of the images, shown below, is that they were strange enough to make you suspicious, yet they weren't implausible enough to dismiss out of hand. In the end, and they proved very hard to definitively debunk.



Pre-existing images that have been misattributed (perhaps the most common form of “fake”) can often be debunked in a few seconds through a reverse image search. And pictures of major events can often be at least partly verified by finding mutually confirmatory images from multiple sources.

But neither of those work for a one-off chance sighting that’s either an original picture or an original hoax. (My experience is that verification of images that can’t be debunked/verified within a few minutes tends to take a lot longer.)

In the end, sometimes there’s no substitute for the time-consuming brute force approach of image verification: tracing an image’s spread back through social media to uncover the original; walking the streets of Google Street View to pinpoint a rough location; and/or scrolling through pages of Google Image results for a particular keyword, looking for possible source images.

In this case, the Google Image search approach paid off - we were able to find the exact image of a shark’s fin that had been Photoshopped into one of the pictures.

But even then, we were unable to say that the other image was definitively fake. It used a different shark.

Our attempts to find the origin of both shark images kept hitting the barrier of people saying, vaguely, that it was “from Facebook.” We eventually found the originating Facebook poster via [a tweet directing us](#) to a news site that credited the source. (Both the news report and Facebook posts have since vanished from the Web.) But even that didn’t entirely help, as the page owner’s other photos showed genuine flooding in the same Brigantine, New Jersey, location. He also insisted in replies to friends that the shark pictures were real. (In retrospect, he seemed to be intent mostly on pranking his social circle, rather than hoaxing the entire Internet.)

The fact that he was claiming one undoubted fake as real was enough for us to move the other shark image into the “almost certainly fake” category. But we still didn’t know for sure. It wasn’t until the next day, when the fact-checking site [Snopes managed to identify the source image](#), that we were able to make that call with 100 percent certainty. This was the shark image that was used to create the fake:



INVESTIGADOR_Z

That may be the main lesson from Sandy: Especially in rapidly developing situations, verification is often less about absolute certainty, and more about judging the level of acceptable plausibility. Be open about your uncertainties, show your work, and make it clear to the reader your estimate of error when you make a call on an image.

5. Verifying Video

Written by **Malachy Browne**

The convergence of affordable smartphone and camera technology, ubiquitous Internet access and social media is largely responsible for the explosion in citizen-powered news coverage. One byproduct of this is an enormous amount of video being uploaded and shared every minute, every hour.

The revolution in information technology is not over and the volume of newsworthy user-generated content will only grow. Journalists have a new responsibility - to quickly gather, verify and ascertain the usage rights of UGC. Traditional values of investigation apply, but a new skillset is required for media such as video.

Verifying video from an unknown source on social media may initially appear daunting. But it's not rocket science.

Here's what you need to get the job done: A determination to investigate the backstory of the content, coupled with a healthy level of skepticism and a familiarity with the multitude of free tools that can help establish facts about a video. This chapter will help to equip you with all three.

A first point to understand about verifying user-generated video is that it spreads across social media in a way that makes the version you first see unlikely to be the original. Videos may be spliced, diced and reposted with different context. Important traces from the original video may disappear. Your job is to root out the facts that support or deny what this video purports to show.

As with any story, start with the basic questions: who, what, when, where and why. In this context, the metadata associated with a video can help answer some of these questions by providing you with details about the original source, date and location.

One rule, however, is that one piece of evidence alone is insufficient to verify a video -usually a body of evidence needs to be collected to form a complete picture. Get ready for that adrenaline rush when the puzzle comes together.

Here's a step-by-step-guide to verifying video from social media.

Provenance

Identifying a video's provenance is the first step. Sometimes it is obvious that the video belongs to the Facebook or YouTube account where you discovered it. But as detailed in Chapter 3, you always start from the assumption that a video has been "scraped" or duplicated.

Most videos come with a description, tag, comment or some piece of identifying text. Extract useful keywords from this information to begin your search. Acronyms, place names and other pronouns make good keywords. If the description is in a foreign language, paste the text into Google Translate to highlight these keywords.


Search for the earliest videos matching these keywords using the date filter to order results. On YouTube, look directly below the search bar for the Filters menu and select Upload Date, as in the below image. Vimeo, YouKu and other video platforms have similar filters. Scroll through the results and compare video thumbnails to find the earliest version (the thumbnails of original and "scraped" videos usually match).

YouTube ^{BE}

nino AND belfry

Filters ▾ About 668 results

Upload Date	Result Type	Duration	Features	Sort by
Last hour	Video	Short (~4 minutes)	HD (high definition)	Relevance
Today	Channel	Long (20~ minutes)	CC (closed caption)	Upload date
This week	Playlist		Creative commons	View count
This month	Film		3D	Rating
This year	Show		Live	
			Purchased	



Actual collapse of church belfry
 by **ABSCBN News** • 3 months ago • 759,880 views
 Watch the **belfry** of the Sto. **Nino** Church in Cebu City collapse when the magnitude 7.2 earthquake struck on Tuesday. Shot by ...

Another method to find the earliest version of a video is to perform an image search of the video thumbnail using Google Image Search or TinEye (as explained in the previous chapter). This can identify the first instance of video thumbnails and images. The helpfulness of these tools depends on the image quality; a strong contrast in the video and a distinctive color scheme help.

Once you've found the source behind the video, contact the source to begin the next step.

Verify the source

It's time to examine the source the same way we would look at any more-traditional source of information. Indeed, often much more information is available about an online source than a traditional source telephoning a tip line, for example.

Online profiles leave a digital footprint that allows us to examine history and activity. Most platforms enable us to contact uploaders, which is an essential step. Ultimately we seek to engage with the uploader, ask questions and satisfy ourselves that the uploader filmed the footage.

These questions are useful when examining an uploader's digital footprint:

- Are we familiar with this account? Has the account holder's content and report age been reliable in the past?
- Where is this account registered?
- Where is the uploader based, judging by the account history?
- Are video descriptions consistent and mostly from a specific location? Are videos dated?
- If videos on the account use a logo, is this logo consistent across the videos? Does it match the avatar on the YouTube or Vimeo account?
- Does the uploader "scrape" videos from news organizations and other YouTube accounts, or does he upload solely user-generated content?
- Does the uploader write in slang or dialect that is identifiable in the video's narration?
- Are the videos on this account of a consistent quality? (On YouTube, go to Settings and then Quality to determine the best quality available.)
- Do video descriptions have file extensions such as .AVI or .MP4 in the video title? This can indicate the video was uploaded directly from a device.
- Does the description of a YouTube video read: "Uploaded via YouTube Capture"? This may indicate the video was filmed on a smartphone.

Gathering the answers to these questions helps paint a picture of the source, the source's online history and the kind of content he shares. From there, it's important to try to connect that account's activity to any other online accounts the source maintains. Below are some practices/questions to guide this process.

- Search Twitter or Facebook for the unique video code - are there affiliated accounts? (Every piece of UGC is identified by a unique code that appears in the URL. On YouTube and Facebook, for instance, the code is placed between "v=" and the next "&" in the URL.)
- Are there other accounts - Google Plus, a blog or website - listed on the video profile or otherwise affiliated with this uploader?
- What information do affiliated accounts contain that indicate recent location, activity, reliability, bias or agenda of the account holder?
- How long have these accounts been active? How active are they?
- Who are the social media accounts connected with, and what does this tell us about the uploader?
- Can we find whois information for an affiliated website?
- Is the person listed in local phone directories, on Spokeo, Pipl.com or WebMii or on LinkedIn?
- Do the source's online social circles indicate proximity to this story/location?

Asking these questions, and answering them, gives us an impression as to the reliability of a source of content. And, importantly, it provides a means to contact the uploader to seek further questions and guidance on the how the video may be used by news organizations.

When speaking to the source, be sure to ask about some of the information you came across. Do the answers match up? If the source isn't honest with you about information, then you should be extra suspicious of the content.

Locate the video

With the source identified and examined, it's time to try to verify the content of the video itself. This begins with confirming, or establishing, the location of the video.

Verifying where a video was filmed very much depends on the clues the video presents. A distinctive streetscape, a building, church, line of trees, mountain range, minaret or bridge are all good reference points to compare with satellite imagery and geolocated photographs. Should the camera pan across a business name, this might be listed in online classifieds or a local directory. A street sign might give clues to the precise location. Car registration plates or advertising billboards might indicate provincial details. Sunlight, shadows and the approximate time of day of the event can also be helpful. And if the video contains dialogue, do the accents or dialects fit the circumstances it purports to represent?

The starting point, again, is to examine any text accompanying the video and clues within the video. Home in on the location using Google Maps and try to map the video location. If possible, zoom into Street View to get the camera angle. If Street View is not available, turn on "Photos" in Google Maps' options and check if geolocated photographs match the video location. Geolocated photos may also be searched using the advanced search features on Flickr, Picasa and Twitter.

If the video is in a foreign language, enter the text into Google Translate and identify the place name. Be aware that Google Translate often mistranslates: for instance, the Arabic for Lattakia in Syria mistranslates as "Protoplasm," Daraa as "Shield." Also be aware that various English transliterations of Arabic render names differently: Jidda or Jiddah, for example. By taking the Arabic text for these places and entering it into Google Maps, we'll find our way to the city. The below image shows searches in Google Translate and Google Maps.

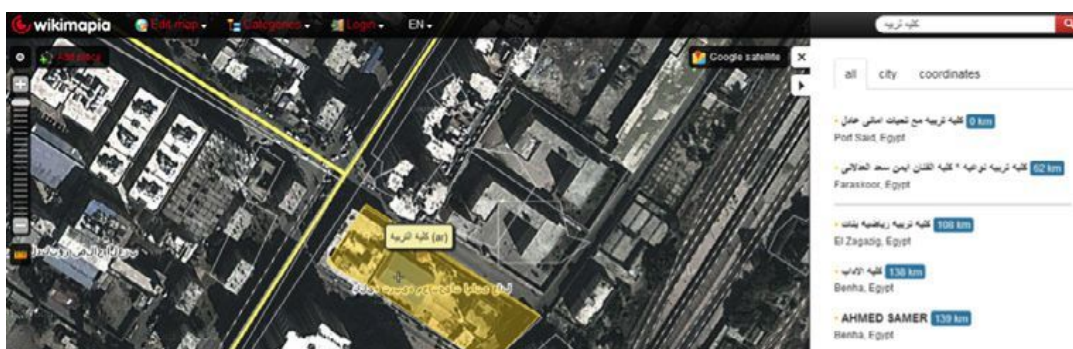


When translating, use the language skills available among your colleagues and contacts. Translating Japanese characters to Korean or Mandarin yields a more accurate translation than Japanese to English. So if you have a Korean or Mandarin speaker in your midst, or can find one quickly, ask her to investigate the translations for you.

Wikimapia is a crowdsourced version of Google Maps in which buildings, suburbs, military sites and other points of interest are outlined and described. This is useful to get context for an area and identify locations, though this information should be corroborated by other information, as it is possible to encounter errors, or deliberately misleading information.

One example of how Wikimapia can be useful came when a day of “civil disobedience” was held in Port Said, Egypt, in February 2013. Demonstrators were [filmed marching](#) by the Port Said University’s Faculty of Education, according to one YouTube uploader. The streetscape was difficult to identify on Google Maps amid the densely packed streets of Port Said. However, the Faculty of Education (فريق تلافك) is tagged on Wikimapia; finding and examining this reference point confirmed the location of the demonstration, as shown on the next page.

Google Earth is another useful tool, in that it provides a history of satellite images. This is useful when examining older videos where the terrain may have changed.



Google Earth's terrain view is also valuable when examining terrain and the relative dimensions of buildings. Recently when the team at Storyful was considering a video as evidence supporting a reported Israeli strike on Syria, Google Earth Terrain's view of mountains north of Damascus verified the location of a YouTube uploader, as you can see in the below comparison.



Verify the date

Confirming the date of videos uploaded from a planned event like a demonstration or political rally is generally straightforward. Other videos of the same event are likely to exist via news reports, and corroborating pictures are usually shared on Twitter, Facebook, Instagram and other social media sites. Searching these platforms with relevant keywords and hashtags is usually sufficient to discover supporting evidence such as distinctive buildings or street furniture, placards or weather conditions.

However, for more obscure videos, date is generally the most difficult piece of metadata to verify. YouTube videos are time-stamped in Pacific Standard Time (PST) from the moment the upload begins. This led Russia's Foreign Ministry to [cast doubt](#) on videos depicting a chemical weapons attack on Ghouta near Damascus: The videos were uploaded in the early hours of August 21, and therefore were dated on YouTube as August 20. The Foreign Ministry's ignorance of this prompted it and others to claim the videos were staged and uploaded ahead of the reported time of the attack.

Weather reports alone are insufficient to verify dates, but they help. As previously detailed, Wolfram Alpha provides weather information about a place on a particular date. After Rita Krill uploaded what purported to be [amazing video](#) of a lightning strike in her Florida backyard on October 5, 2012, Wolfram Alpha showed that thunderstorms were active in the area.

And searching Twitter for Naples, Florida, on that date showed a local weatherman asking his followers for pictures of storm clouds in Naples. Below is an image of the Wolfram Alpha search and the tweet.



WolframAlpha computational...
knowledge engine

Enter what you want to calculate or know about:

Weather, Naples Florida on October 5



Examples Random

Input interpretation:

weather

Naples, United States

Friday, October 5, 2012

Recorded weather for Naples, United States:

Show metric

More

time range	day of Friday, October 5, 2012
temperature	(72 to 89) °F (average: 79 °F)
conditions	rain, thunderstorm, fog, overcast, cloudy, partly cloudy
relative humidity	(65 to 100)% (average: 91%)

Final checks: What does the video show?

Now it's time to bring all of your data together and ask the obvious questions: Does the video make sense given the context in which it was filmed? Does anything jar my journalistic instinct? Does anything look out of place? Do clues suggest it is not legitimate? Do any of the source's details or answers to my questions not add up? Remember, your assumption is that the video is false. Does the evidence confirm or refute that assumption?

When it comes to video, bear in mind that elaborate hoaxes have been, and continue to be, played. Canadian students infamously [faked a video of an eagle swooping down in a park in Montreal and picking up a baby](#). This was debunked by splitting the video into single frames and spotting that the eagle's shadow was missing in some frames. (More technical people can use video editing software like the free [VLC media player](#) or the free [Avidemux video editor](#), or the licensed [Vegas Pro](#) editor to split a video into its constituent frames if you have doubts over its construction.)

5.1. Verifying a Key Boston Bombing Video

Written by Malachy Browne



One of the [iconic videos of the tragic 2013 Boston bombings](#) was filmed by an athlete running her final mile of the marathon. As she approached the finish line on Boylston Street, the second bomb detonated meters ahead. It was a compelling video, but we needed to verify it.

One photo showing the moment of the blast was posted by Boston journalist Dan Lampariello (below), a member of one of our pre-curated Twitter lists, and someone familiar to Storyful. Lampariello's tweet was geolocated to Boylston Street; this information, which came from a reliable source, helped to confirm the location of the explosion. It also gave us a reference point to use with what was shown in the runner's video.



Google Street View of Boylston street (below) confirmed both Dan Lampariello's photo and the athlete's point of view as she approached the finish line. Indeed, some of the athletes filmed in the video are seen in Lampariello's photo, upon close inspection.

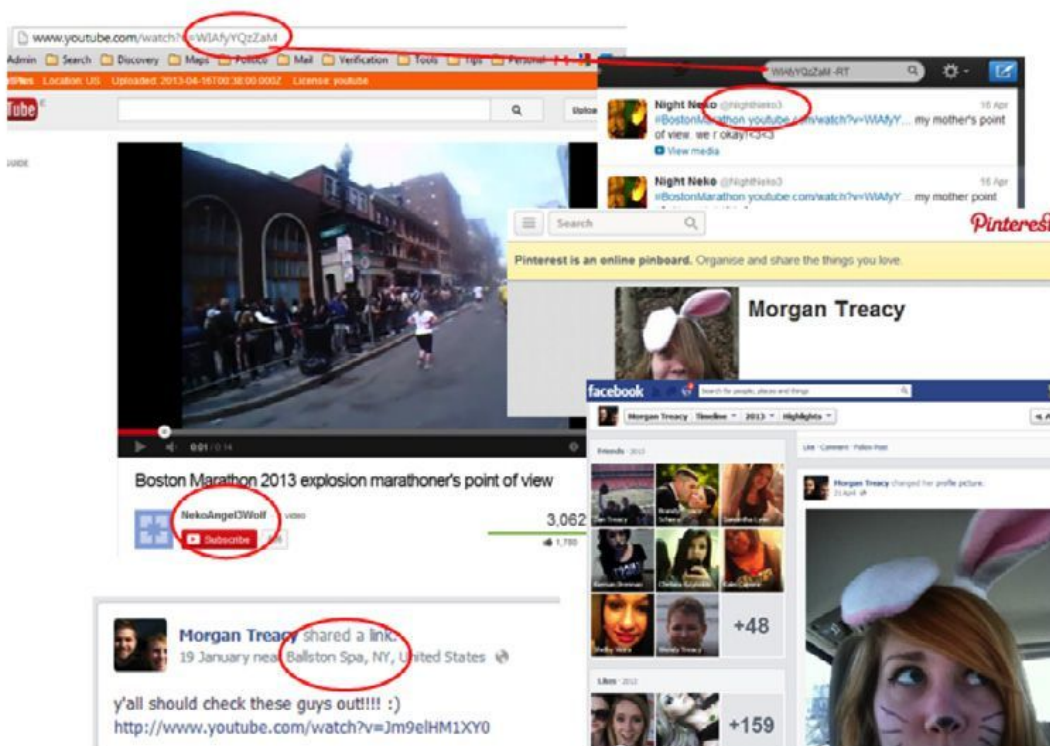
INVESTIGADOR_Z



That process confirmed the content of the video. Finding the original source of this video was less straightforward.

The video itself was uploaded to a YouTube account with no giveaway details and an obscure username, NekoAngel3Wolf. Searching Twitter for the unique video code led us to someone sharing it under the handle NightNeko3, again with no personal details. The “Neko” reference in both profiles suggested they were affiliated.

Searching for similar social profiles, we found a Pinterest account also registered as NightNeko3, giving the real name Morgan Treacy. Our team at Storyful quickly located a Facebook account for Morgan Treacy, a teenager whose posts were geolocated to Ballston Spa in New York State.



Morgan described the video on Twitter as her mother’s perspective of the explosion. Knowing that a prestigious marathon like Boston’s would likely track athlete times, we checked the surname “Treacy” on Boston Athletic Association’s registrant page. A single result was returned - Jennifer Treacy, age 45-49, from New York State.

Jennifer Treacy's time split shows her passing the 40 kilometer mark at 2:38 p.m. but failing to cross the finish line 2 kilometers later. Jennifer was averaging 10 minutes per mile, placing her in the vicinity of the blast at 2:50 p.m., when the bombs exploded.

The social people search website Spokeo.com gave us an entry for Jennifer L. Treacy, 47, with an address at Ballston Spa, New York. LinkedIn also gave us a profile for Jennifer Treacy from Ballston Spa, who is employed by the New York State Department of Health.

One final piece of evidence confirmed our investigation. A man named Gerard Quinn is a Facebook friend of Morgan Treacy, who we were now almost 100 percent sure was Jennifer's daughter. Quinn previously commented on family videos posted by Morgan. So there was a link between him and the family. We saw on Quinn's Facebook profile (below) that he had expressed pride that his niece, Jennifer, was running the Boston marathon. He'd linked to her marathon map and time splits. He also later commented on Facebook that Jennifer was OK after the blast and on her way home.



person details

participant

Name	Treacy, Jennifer (USA)
age group	Female 45-49
bib number	19367
Age	46
State	NY

totals

place (M/W)	
place (ag)	
place (total)	
time total (net)	
time total (gun)	

splits

Split	time of day	time	diff	min/mile	miles/h
5K	11:08:40AM	00:27:52	27:52	08:58	6.69
10K	11:37:43AM	00:56:56	29:04	09:22	6.42
15K	12:05:56PM	01:25:09	28:13	09:05	6.61
20K	12:34:49PM	01:54:02	28:53	09:18	6.46
HALF	12:41:09PM	02:00:22	06:20	09:18	6.46
25K	01:03:56PM	02:23:08	22:46	09:24	6.39
30K	01:34:48PM	02:54:00	30:52	09:56	6.04
35K	02:06:18PM	03:25:31	31:31	10:09	5.92
40K	02:37:55PM	03:57:08	31:37	10:11	5.90
Finish Net	-	-	-	-	-



Gerard Quinn

15 hours ago

So extremely proud of my niece Jennifer, who is running the Boston Marathon today!



A public telephone directory produced a phone number that allowed us to speak directly to Jennifer Treacy. She confirmed the video was hers and that news organizations were permitted to use it. She had also informed law enforcement agencies of the video, she said.

In summary, all of the information supporting the veracity of this video was available online via free tools - location information, corroborating accounts of the event, the uploader's digital history and the owner's contact details. Familiarity with these tools allowed us to verify the video in around 10 minutes.

5.2. Investigating a Reported ‘Massacre’ in Ivory Coast

Written by **Malachy Browne**



In March 2011 a [graphic video surfaced on YouTube](#) that depicted what was claimed to be the killing of at least six [women](#) by Ivorian security forces (FDS) during a protest in Abobo. The demonstration occurred during a period of unrest when President Laurent Gbagbo clung to power after his defeat in presidential elections the previous November.

At the behest of a client, Storyful set about verifying the video two years after it happened. The video shows a large group of women chanting “ADO” (a reference to Alassane Dramane Ouattara, Gbagbo’s rival). Then, at the 3:32 mark, armored personnel carriers come into view and large-caliber rounds are fired. Several people appear to be fatally wounded. At the time, some Ivorians claimed the injuries were staged. The country’s then defense minister cast doubt over the video and Gbagbo supporters claimed the video was a “fake” in YouTube reconstructions ([here](#) and [here](#)).

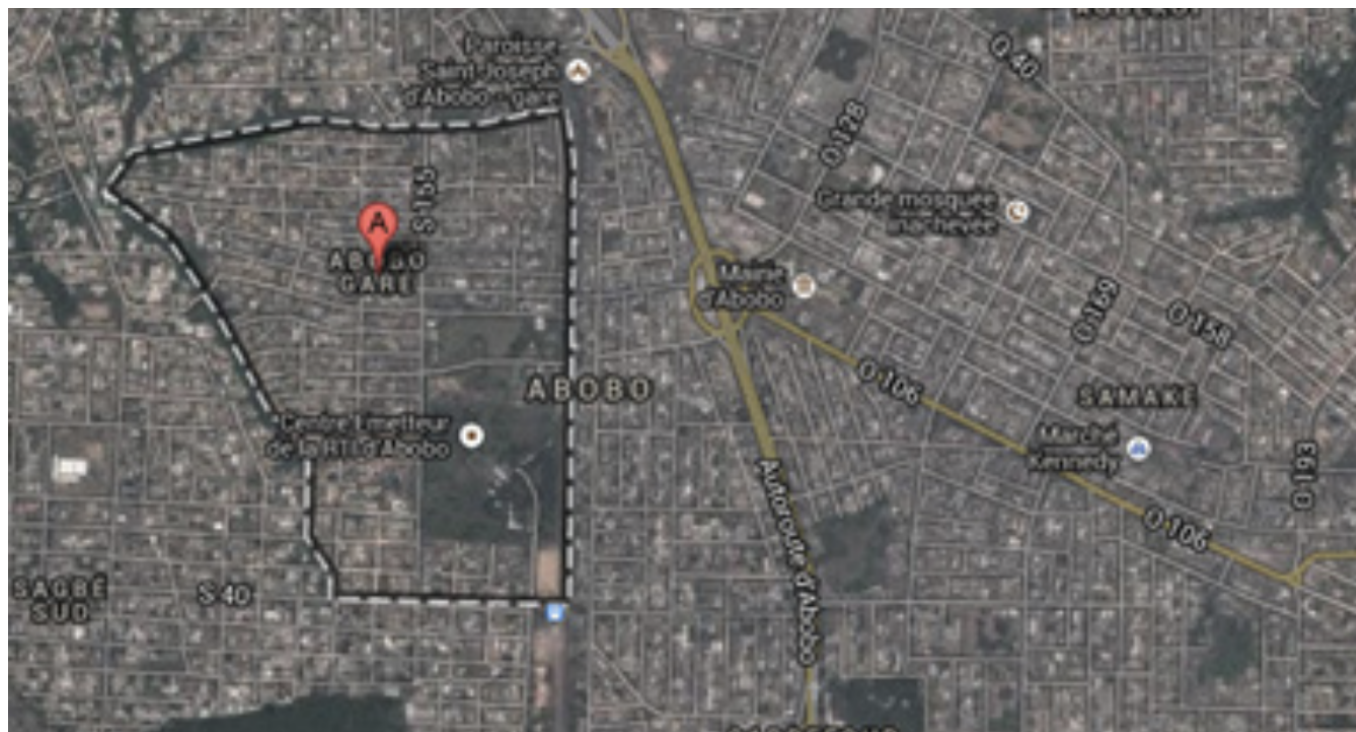
Verifying video in a breaking news scenario is in some respects easier than this form of retrospective investigation. Information that corroborates or debunks a video is more accessible in the recent timeframe; information related to an older event is often hidden deep within social networks. Archival search is either challenging or not possible.

With those limitations in mind, here’s how I worked to try to verify the video.

Gather context on the event

Unfamiliar with the details of the reported massacre, I searched Google for “Women killed Gbagbo March 3 2011.” This returned several reports ([here](#) and [here](#)) describing the approximate location and the sequence of events. This search also returned a statement about the event made by the country’s then defense minister, who claimed the scenes were staged.

Importantly, these reports also provided keywords I could use to run a more focused search. Using these terms for historical search on Twitter and YouTube, I unearthed eyewitness accounts and UGC. (Always try to put yourself in the shoes of the uploader and imagine how she would tag and describe video and other information.)



Location

According to reports, the demonstration and shooting happened at a roundabout in the vicinity of Abobo, a northern district of Abidjan. Specifically, [one report](#) located it at a major junction/roundabout on Autoroute d'Abobo, adjacent to the area known as Abobo Gare. A witness in the report described the security forces passing by a roundabout, doubling back and opening fire on the women “before heading back to Adjamé.” Adjamé lies south of Abobo, giving us a lead on the direction of traffic.

According to a contemporaneous report published in *Le Patriote* on March 8, demonstrators gathered “at the roundabout intersection of Banco” (mapped below). Searching a local forum shows that the roundabout was the site of previous such demonstrations.

Google Maps shows two major roundabouts. One of them, Carrefour Banco, lies at the southern end of Abobo, toward Adjamé. This fit with the previous report, so I used it as my starting point.





The position of street lights and traffic lights, the alignment of palm trees and deciduous trees filmed in the video from 4:00 onward line up with the satellite view of Banco Carrefour's north-western corner, as shown in the above white circles. The large building with two prominent protrusions atop the roof (circled in red) also aligns with a building we see in the distance as the convoy of security vehicles disappears from view. This matches the direction of traffic evident in the satellite image above, and the account given by an eyewitness of the vehicles driving south toward Adjamé.



One piece of video evidence (above), however, did not match the satellite imagery. We counted three large deciduous trees as the convoy entered the roundabout; Google Maps shows just two such trees. The video was filmed in 2011 and the satellite images were dated 2013, so perhaps a tree was cut down. So we looked through historic satellite images on Google Earth. Images from 2009 show three large deciduous trees stood at this corner of the roundabout.

The third, missing tree from the 2013 satellite imagery is outlined in the above image. (It has been flipped 180 degrees from north to south). Judging by this view, we can see that the camera position was directly across the road. I later spoke with a reputable source known to Storyful who is familiar with the video, and who had visited Abobo to report on the "massacre." The source confirmed this was the camera angle.

Date

INVESTIGADOR_Z

The date of the shooting is corroborated by several independent reports and videos shared on social media. These are found retrospectively through a variety of searches: on Twitter, on Topsy or Topsy Pro (which allows a date range to be set), and on YouTube with results ordered by upload date.

Some of the steps I followed:

- I used [historical Twitter search](#) to generate leads by scrolling back to results from March 3, 2011, onwards.
- I examined Tweets and questions about the event and found [this](#) and [this reply](#). These sources are potential witnesses, or people who could identify witnesses. The first source lists her location as Cocody, Abidjan, and the second one as Abidjan.
- I also located [this person](#), who uploaded video from Abobo and previous RHDP rallies. Checking other Twitvids on his account leads to a video uploaded on the day of the protest.
- I looked further at his Twitter timeline and found other [references to RHDP on that day](#). That led me to other links, such as this [news report of the event](#). It included a photo credited to Reuters that showed victims matching those in our video.
- Running a [Google Image Search](#) on the photo confirmed it wasn't used prior to March 3. However, the results also show that a [Guardian article](#) credited AFP/Getty Images and not Reuters. This meant a credible photographer was on the ground at the event.

I dug further into the photo, shown below.



The image is consistent with the picture of the victim at 5:30 in the lead video. The victim is covered by garments and green leaves used by many of the demonstrators. Note the tight, dark blue T-shirt worn by the victim and the distinctive garment with a square pattern of red, orange, white and dark lines, shown over the page in a close-up.

France 24 Observateurs was also [provided with photos](#) from the event by sources in Abid- jan. We at Storyful confirmed this with France 24.

Other searches uncovered a photo-diary published [here](#) by an Agence France-Presse journalist, Issouf Sanogo. Sanogo interviewed a woman named Sirah Drane, who says she helped organize the demonstration on March 3. Drane says she was holding a megaphone to address the large crowd that had gathered at a traffic circle in Abobo. A woman matching this description is seen in the video.



The video correlates with three other videos of the event. These videos were documented by Storyful at the time, and could be found by searching YouTube using search terms identified earlier.

The [first video](#) was uploaded on the day of the shooting to an Ivory Coast-registered YouTube account which was created specifically to upload the video. There is no further activity on the account to provide information regarding the source. The same wounded women are filmed in the video, as is the distinctive square building in the background.

A [second video](#) was uploaded to another Ivory Coast-registered YouTube account on the morning of March 4 at 09:06:37 GMT. The uploader describes it as “several women killed” at the “RHDP demonstration yesterday,” meaning March 3.

None of these videos or corroborating photos exist before March 3, suggesting to a high degree of certainty this was the date of the event.

Original uploader

The video itself was uploaded to YouTube on March 4, 2011. It's the earliest such video found on YouTube. However, it's highly likely the video originated from a Facebook account or elsewhere and was scraped onto this YouTube account.

The YouTube account is registered in the United States and is linked to a defunct website, onemendo.com. The account appeared to be operated by someone with connections to Jamaican emigrants living in New York or New Jersey because the account contained promotional material for a local club, DanceHallReggae.com.

Videos from around that time on an affiliated Vimeo account indicate they are based in Rochester, New York. An affiliated Facebook account also posts links to music by Jamaican DJs. It gives no further clues as to the origins of the video and did not post a link to it on March 3, 2011. Videos of a Senegalese soap opera were also posted to the YouTube account.

Is the video authentic?

The evidence above confirms the location and establishes the date of the video as highly likely to be March 3. However, to the central point: Does the video show women protesters being shot dead by the FDS on that day?

Claims [have been made](#) that the killing is staged and bodies were placed on the street after the security forces drive past. These serious questions warrant investigation.

In this statement, Gbagbo's defense minister, Alain Dogou, referred to the emergence of this amateur video on March 4. He said a woman was instructed to “lay down, lay down,” (and we do hear this said in the video). Dogou said it is “difficult to say” that the video is from the location reported by journalists. (Of course, we have confirmed

the location.) He also said international journalists were not covering the protest because they were attending a news conference by UNOCI, or another event related to the Council of Ministers. Finally, he acknowledged that a Women's March did take place in Abobo on this date.

Serious questions that arise:

- Why did the camera point away from the wounded for so long as the convoy entered the roundabout?
- Would all the victims be shot within meters of one another?
- Would they all fall face down as they have in the video?
- Their faces are quickly obscured by garments - why is this?
- A bloodied woman is told to "lay down, lay down" in the video, as described by Defense Minister Dogou. Why is this? Is this out of concern for her poor condition, or to stage an injury?
- The "massacre" creates a frenzy of emotion in the video; is this real?
Or were other protesters duped by or complicit in a staged "massacre"?

Several witnesses give convincing accounts that injuries did result from the reported massacre. A doctor from South Abobo Hospital is quoted on page 63/64 in this [Human Rights Watch report](#). The doctor reported seeing victims from the shooting:

A doctor who has treated many women who did not survive said their injuries were clearly caused by heavy weapons, and not by bullets. The doctor and two witnesses at the scene told Human Rights Watch that the head of one of the victims had been completely separated from her body. Other victims, two of whom did not survive due to serious injuries, were injured by machine gun bullets.

(The video does appear to show a victim whose head was blown apart.)

A New York Times report quoted two named witnesses as follows:

"The forward tank started firing," said one Abobo resident, Idrissa Diarrassouba. "Right away six women were killed. I was right there, beside them. They just fell."

"There was a burst of machine-gun fire," [the witness, Idrissa Sissoko] said. He also spoke of seeing six women being shot. "I saw six bodies lying there, suddenly," he said.

According to [this report](#), a military source told a Reuters journalist that the shooting was an accident resulting from the nervousness of the security forces following previous clashes.

Conclusion

We can say that the date and location are verified to a high degree. The original source is not, and we therefore did not get the opportunity to speak to the person who filmed the footage.

Ultimately, though, does the video show what it claims?

This we cannot determine to 100 percent satisfaction from a distance, and with the material that's been gathered. Along with being able to contact and interview the uploader, it would be important to gather additional firsthand testimony from witnesses, doctors who treated victims, and the families of the reported victims. To identify those victims we could attempt a more detailed investigation of the first video, splitting it frame by frame at the key moments of the shooting to try and find ways to the identify victims, and then to track down their survivors.

Even with all of the corroborating facts and information I was able to marshal, the verdict is still out on this video.

INVESTIGADOR_Z

5.3. Confirming the Location and Content of a Video

Written by Christoph Koettl

During the violent clashes in Cairo in August 2013 there was one particular YouTube video that received a lot of media attention. (The original video was subsequently removed from YouTube, but can be also viewed [here](#)). The widely used description for this video, which for example appeared in the headline on a [Washington Post](#) blog post, was that protesters had pushed a police car off a bridge in Cairo.



Violent behavior displayed by protesters is, of course, relevant when investigating disproportionate use of force by the police, as we at Amnesty International do. We also work to verify video as part of determining whether human rights abuses have occurred. As a result, this video represented important footage that needed careful review.

What stood out from this video, in contrast to the description and resulting headline, was that at no time could the protesters be seen actually pushing the car off the bridge. It clearly required a closer look. Here's what I did to assess the content of the video and determine the exact location of the incident:

One of the first steps when validating citizen video is to search for other content that shows the same incident. I normally search YouTube as well as in the Storyful dashboard (a paid service) and Storyful's Open News Room to find additional video content. (As noted in the chapter, I filter my YouTube searches by upload date to narrow down the number of results.) Using these tools, I found a [second video](#) that was shot from a different angle. It appears to be filmed from a nearby high-rise, and thus provides a great view of the whole scene. The additional

footage shows that no one actually pushed the police car off the bridge. Rather, the car appears to have collided with another vehicle, causing it to roll back and fall off the bridge. This second video confirmed the incident was real, but also revealed that the description (and headline) were inaccurate.

With the new vantage point provided by the second video, it became easier to find the exact location of the incident. The Washington Post article provided the “6th of October Bridge” as the setting of the video. This is sufficient to get started, as the bridge is easy to find on online maps. However, the bridge is actually a very long elevated road that runs through large parts of the city. This made it more challenging to find the exact location.

When carefully reviewing the second video, one landmark stood out: a sports stadium. By tracing the 6th of October Bridge on Google Earth, I was able to identify two stadiums that are in close proximity to the bridge. After rotating the view on Google Earth to find the potential location and line of sight of the person filming, I found a location that matches up with the [second stadium](#). Having confirmed the general location, it was then easy to pinpoint the high-rise buildings overlooking the incident. Using the mapping tool in Google Earth Pro, I produced a simple overview map, depicting the location of the two videos, the area of sights, and relevant landmarks:

Finally, two more features further confirmed the location: A broadcasting tower is visible in the background of the video, which is also visible in [satellite images](#). Additionally, I turned on the Panoramio photo layer in Google Earth to check for user-generated photos. The Panoramio layer contains georeferenced, user-generated photos that provide an on-the-ground view, and thus a high level of detail. There are also [several photos from underneath the bridge](#) where the car landed, and the pillars of the bridge as seen in the video match up perfectly.

Thanks to a combination of video searches, Google Earth and Google Maps, I was quickly able to verify where the video was shot, and to also debunk an erroneous description that could have had serious implications for the protesters in Cairo.



Coordinates of lead video: 30.058807, 31.303089

INVESTIGADOR_Z

In the end, after the real story of why the police car fell off the bridge was clear, The Washington Post followed up with a [second post](#) and a [correction](#).

6. Putting the Human Crowd to Work

Written by **Mathew Ingram**

The idea of crowdsourcing verification of news events and emergencies isn't really that all new - the crowd, broadly speaking, has always been a crucial part of how the news is formed and understood. It's just that social technologies like Twitter, Facebook, YouTube and others allow us to engage in this kind of shared decision-making process on a much larger and broader scale, and they allow us to do it faster as well. That's not to say there aren't flaws in this process, because there are - but on balance, we are probably better off than we were before.

Just think about how facts and news events were established in the not-so-distant past: When a war broke out, a hurricane struck or a bomb exploded somewhere, there were often few journalists around, unless they just happened to be there. Sources on the ground would relay the information to a news outlet and then the painstaking process of verifying those events would begin, based on interviews with witnesses, phone calls and so on.

Now, we are just as likely to find out about news - particularly sudden, unpredictable events like earthquakes or mass shootings - on Twitter, within minutes or even seconds of their happening. And instead of just one or two observations from bystanders and witnesses, we can get hundreds or even thousands of them. Some of them are likely to be erroneous, as we saw with the bombings in Boston and other similar emergency situations, but overall a fairly accurate picture can be gradually assembled of what occurred and how - and it happens faster than ever.

Here's a look at some of the best practices for the emerging practice of crowdsourced verification, as practiced by innovators like Andy Carvin, a former senior strategist at NPR, and others.

Identify, verify and connect with sources

In most cases, the starting point is to identify sources that are reliable and then curate, aggregate and verify the information that comes from them. Andy Carvin of NPR built what he called a "Twitter newsroom" of sources in the Middle East during the Arab Spring by starting with people he knew personally and using them as a means to discover other sources.

"What I find really important is paying attention to who these folks on Twitter, and occasionally on Facebook, are talking to," Carvin told Craig Silverman in a 2011 interview. "For both Tunisia and Egypt I already had about half a dozen sources in each country that I had known."

Carvin also asked people he knew to recommend or verify other sources he was finding through Twitter searches and by following specific hashtags. Over time, he generated lists of hundreds of valuable sources.

Those lists in turn became the engine that allowed Carvin to effectively live-tweet a series of wars - receiving information, republishing it, asking his followers and sources for help verifying it, then posting the results. In many ways it was a chaotic process, but ultimately successful.

To manage these many contacts, he built Twitter Lists to organize them into logical groups based on topics or geographical location. Today, this kind of thing could also be accomplished with Facebook Interest Lists, Google Plus circles and other tools, or by subscribing to YouTube accounts and building playlists, among other options.

Carvin also took another critical step, which was to contact many of his sources directly or meet them in person to develop a relationship. Many people saw only what he was doing with his Twitter account, but he also spent a lot of time communicating with people via Skype, email and other means to confirm their identities.

INVESTIGADOR_Z

As detailed in previous chapters, these kinds of sources and the information they provide must be verified. After using Twitter advanced search, YouTube search and other means to find people and organizations on the ground or with access to relevant information, you need to work to contact them and verify where their information is coming from.

The more you interact with your sources, and learn about them, the more you'll see their strengths, weaknesses, biases and other factors that need to be weighed when considering the information they share. As your list of sources grows, you also begin to see patterns in what they see and share and report, and this provides the raw material needed to triangulate and determine exactly what is and isn't happening.

"Some of these folks are working to actively overthrow their local regimes," Carvin said of the sources he connected with during the [Arab Spring](#). "I just have to be aware of that at all times. Perhaps the answer is transparency, so a certain person might be giving me good information but I should never forget that they are part of the opposition."

Engaging your sources

It all began on March 12, 2011 when I was at the SXSW Festival in Austin, Texas, participating in a session about social media and the Middle East, organized by the New York Times.

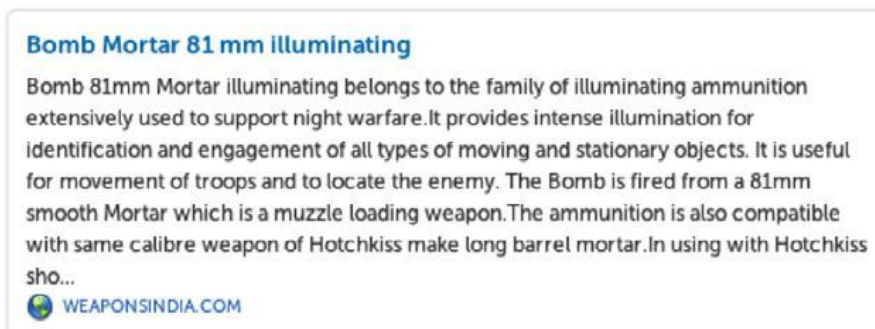
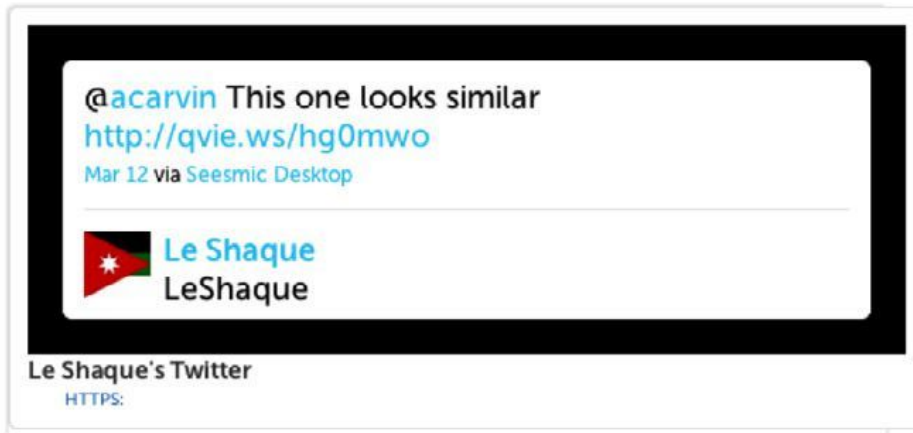


While sitting in the session, I received a tweet from [@jan15egy](#) asking me to look into something.



At one point during the violence in Libya in 2011, Carvin was contacted by someone on Twitter who asked him - and by extension his Twitter newsroom - to help verify if Israeli weapons were being used in Libya. He detailed how it played out in a Storify:

A Syrian living in Beirut named [@LeShaque](#) began to dig up a lot of intriguing leads from weapons manufacturers in India:



From that tip, Carvin enlisted his followers by asking them to help confirm whether the mortar in question was Israeli. They responded with a mix of useful tips and views, along with some dead ends. He eventually received specific information that helped answer the question:

In the end, the weapon wasn't Israeli; it was Indian. And it wasn't a mortar at all. Carvin said one way he knew he was onto the correct information was that he heard it from multiple sources whom he knew were unconnected to each other.

"In the case of what we did for the so-called Israeli weapons, I had a lot of people that were giving me essentially the same information and they didn't really know what they were talking about some of that in my Storify," he said.

INVESTIGADOR_Z

It's important to remember that one thing that helped Andy Carvin do what he did was his reaching out to others for help in a very human and approachable way. He also treated those he came into contact with as colleagues, rather than as just sources he could command to do his bidding. Journalists and others who simply hand out orders get very little in response, but treating people like human beings makes all the difference.

New York Times war reporter C.J. Chivers has taken advantage of a similar approach as Carvin's to verify bombs used in various conflicts, and [says](#) the process arrives at the truth far quicker than would have been possible in the past.

With any given piece of information, there are likely to be knowledgeable people in your social circle (or in their broader web of connections) who know the truth about that incident or event. You just have to find them.

Said Chivers: "The proof in this case was made possible with the help of the standard tools of covering war from the field: the willingness to work in the field, a digital camera, a satellite Internet connection, a laptop, an e-mail account and a body of sources with specialized knowledge. But there was a twist that is a reflection of new ways that war can be examined in real time - by using social media tools to form brief crowds of experts on a social media site."

Chivers has also celebrated the achievements of a British "citizen journalist" by the name of Brown Moses. He's a blogger whose real name is Eliot Higgins, and who has developed an expertise in chemical weapons by watching and verifying thousands of YouTube videos of the conflict in Syria.

Higgins had no training in either journalism or military hardware, but has become a key link in the chain of verification, to the point where professional journalists like Chivers and even aid agencies have come to rely on him. New, critical sources like Moses can emerge in certain situations, either because they work at an issue over time or because they are in the right (or wrong) place at the right time.

Responsible crowdsourcing

One thing that anyone, journalist or not, trying to collect and verify information during a crisis has to remember is that you are also a source of information for others, when using social media like Twitter or Facebook or Google Plus. That means any unsubstantiated information you post while you are doing your verification work could contribute to the confusion around the event.

Keep that in mind while tweeting or posting details and looking for corroboration. The best approach is to be as open as possible about what is happening, and to repeatedly remind your followers or social connections that you are looking for help, not just circulating unconfirmed information.

In order to prevent confusion, be as clear as possible about what you know and what you don't know, and which pieces of information you need help confirming. With some kinds of sensitive or inflammatory details, you are better off trying to confirm through offline methods first before taking to social media or online methods. You may be careful to flag the information as "unconfirmed" or a rumor, but these flags can often disappear once they start to spread. We all have a responsibility to consider that reality, and to not add to confusion or misinformation in a crisis situation.

The power of the crowd

Algorithms and automated searches can generate a huge amount of content when it comes to breaking news events, as detailed in the next chapter. But arguably only human beings can sift through and make sense of that amount of content in an efficient way, in real time. As examples like Andy Carvin and Brown Moses have shown,

by far the best tool for doing this is a network of trusted sources who are focused either on a specific topic area, or in a specific physical location - a network that you can use as your own crowdsourced newsroom.

Entering into this kind of relationship with sources shouldn't be taken lightly, however. It's not just a tool or a process that allows you to do your job or complete a task faster and more efficiently - it's a collaborative effort, and you should be prepared to give as much as you receive

INVESTIGADOR_Z

6.1. Tripped Up by Arabic Grammar

Written by **Tom Trewinnard** and **M.SH.**

Shabab Souria (Syria Youth) is a network of Syrians inside and outside Syria who collaborate using online tools to verify and publish on-the-ground updates from across Syria. Working as a closely administered open Facebook group, members crowdsource verification of the hundreds of reports that emerge daily from official media and social networks. They then publish the verified content in Arabic and English using Checkdesk.

[Checkdesk](#) is an open source platform for newsrooms and media collectives to verify and publish digital media reports on breaking news events. Checkdesk was launched by Meedan in July 2013 with six leading Middle East media partners, all of whom have conducted a series of workshops within their communities to train citizens in media literacy, source awareness and digital verification techniques.

A good example of how Shabab Souria works to debunk and verify reports occurred [on December 5, 2013](#). A person going by the name Sham al-Orouba posted a YouTube video to the Shabab Souria Facebook group. In the video, a bearded man was identified as a member of the Seyoof al Islam Jihadist group claimed the group had carried out attacks against the Christian community of Saydna and the Deir Cherubim monastery.

His narrative of the alleged attacks was interspersed with unclear clips apparently showing damage to a hilltop building and a statue of Jesus Christ. In submitting the video to the Shabab Souria network, Al-Orouba asked a simple question: "Confirmed or denied?"

Member Mohammad Fakhr Eddin (all members of the group use pseudonyms to protect themselves) responded quickly, noting that subtle grammatical inaccuracies in the presenter's Arabic are atypical of a Jihadist. Based on their experience reviewing hundreds of videos and other content from Jihadists, the group often finds these people to be eloquent in their use of language.

Another user, Abu Nabil, agreed that the presenter's weak Arabic betrayed him, signaling he is not who he says he is. Nabil added that Islam prohibits attacks on churches, and another user agreed that Jihadist groups generally don't target churches in Syria unless there is a strong military reason to do so.

Shamya Sy and Mohammad Fakhr Eddin added another important piece of information about the source: they said the person who uploaded the video to YouTube - Nizar Nayouf - is notoriously unreliable. Their evidence was that Nayouf has in the past been responsible for pro-Assad regime propaganda aimed at defaming anti-Assad groups.

"This couldn't be confirmed from any other sources," wrote Abu Karam al-Faraty in a post to the group.

No one could locate other reports, images or footage of Seyoof al Islam, or other Jihadist groups, attacking Deir Cherubim or the Christian community in Saydna.

Over time, members of a group such as Shabab Souria develop their own areas of expertise, as well as a reputation for their work. Sy and al-Faraty are known sleuths: Through their record of diligently checking media, they have established themselves as credible experts on matters of verification. The fact that they were the ones to identify the source of the video as being unreliable added extra weight to the information.

In the end, it took less than three hours for the group to determine the video was fake. By bringing together the expertise of various group members, they were able to check to see if other, corroborating footage or reports existed; examine and question the credibility of the source; and analyze the content of the video and identify

aspects that questioned its authenticity.

Seven different users collaborated to debunk the video. If taken at face value, the fake Jihadist report could have contributed to a continuing propaganda war that influences not only civilians inside Syria, but also policymakers abroad.

As one user in the thread wrote, “The problem is we know that this is false, but the Western media will pick this up as real.”

This all took place at a time when an international military intervention seemed a real possibility. It was therefore essential that the video be debunked - and also publicly noted as such via the social media that have become so crucial in the flow of information in the Syria conflict.

7. Adding the Computer Crowd to the Human Crowd

Written by **Patrick Meier**

Investigative journalists and human rights practitioners have for decades used a mix of strategies to verify information in emergency and breaking news situations. This expertise is even more in demand with the growth of user-generated content.

But many are increasingly looking to “advanced computing” to accelerate and possibly automate the process of verification. As with any other technique, using advanced computing to verify social media content in near real time has promises and pitfalls.

Advanced computing consists of two elements: machine computing and human computing. The former uses techniques from natural language processing (NLP) and machine learning (ML), while the latter draws on crowdsourcing and microtasking methods.

The application of advanced computing to verify user-generated content is limited right now because the field of research is still new; the verification platforms and techniques described below are still being developed and tested. As a result, exactly how much value they will add to the verification process remains to be seen, but advancements in technology are likely to continue to bring new ways to help automate elements of the verification process.

This is an important moment in the application of advanced computing to verify user-generated content: Three new projects in this field are being developed. This chapter provides an overview of them, along with background on how human and machine computing are being used (and combined) in the verification process. As we dive in, let me add a disclaimer: I spearheaded the digital humanitarian response efforts described below - for Haiti, the Philippines and Pakistan. In addition, I'm also engaged in the Verily project and with the creation of the Twitter Credibility Plugin, both of which are also mentioned.

Human computing

In human computing, also referred to as crowd computing, a machine outsources certain tasks to a human or crowd. The machine then collects and analyzes the processed tasks.

An early use of human computing in an emergency was after the Haiti earthquake in 2010. [Ushahidi Inc. set up a Web-based human computing platform](#) to microtask the translation of urgent text messages from Haitian Creole into English. These messages came from disaster-affected communities in and around Port-au-Prince. The translated texts were subsequently triaged and mapped to the Ushahidi Haiti Crisis Map. While the translation of the texts was the first and only time that Ushahidi used a human computing platform to microtask crisis information, the success of this computer science technique highlighted the value it added in disaster response.

Human computing was next used in 2012 in response to Typhoon Pablo in the Philippines. At the request of the United Nations, the Digital Humanitarian Network (DHN) [collected and analyzed all tweets posted during the first 48 hours of the typhoon's making landfall](#). More specifically, DHN volunteers were asked to identify all the pictures and videos posted on Twitter that revealed damage caused by the strong winds and rain. To carry out this operation, the DHN used the free and open-source microtasking platform CrowdCrafting to tag individual tweets and images. The processed data was then used to create a crisis map of disaster damage.

The successful human computing response to Typhoon Pablo prompted the launch of a new, streamlined microtasking platform called MicroMappers. Developed using CrowdCrafting software, MicroMappers [was first used in September 2013 to tag tweets and images posted online following the Baluchistan earthquake](#). This operation was carried out by the DHN in response to a request by the U.N. in Pakistan.

In sum, human computing is just starting to gain traction in the humanitarian community. But human computing has thus far not been used to verify social media content.

Verily platform

The Verily platform that I am helping to develop uses human computing to rapidly crowdsource evidence that corroborates or discredits information posted on social media. [We expect Verily to be used to help sort out conflicting reports of disaster damage, which often emerge during and after a major disaster](#). Of course, the platform could be used to verify images and video footage as well.

Verily was inspired by the Red Balloon Challenge, which was launched in 2009 by the Defense Advanced Research Projects Agency (DARPA). The challenge required participants to correctly identify the location of 10 red weather balloons planted across the United States.

The winning team, from MIT, found all 10 balloons in less than nine hours without ever leaving their computers. Indeed, they turned to social media, and Twitter in particular, to mobilize the public. At the beginning of the competition, the team announced that rather than keeping the \$40,000 cash prize if they won, they would share the winnings with members of the public who assisted in the search for the balloons. Notably, they incentivized people to invite members of their social network to join the hunt, [writing](#): “We’re giving \$2000 per balloon to the first person to send us the correct coordinates, but that’s not all - we’re also giving \$1000 to the person who invited them. Then we’re giving \$500 whoever invited the inviter, and \$250 to whoever invited them, and so on.”

The Verily platform uses the same incentive mechanism in the form of points. Instead of looking for balloons across an entire country, however, the platform facilitates the verification of social media reports posted during disasters in order to cover a far smaller geo- graphical area - typically a city.

Think of Verily as a Pinterest board with pinned items that consist of yes or no questions. For example: “Is the Brooklyn Bridge shut down because of Hurricane Sandy?” Users of Verily can share this verification request on Twitter or Facebook and also email people they know who live nearby.

Those who have evidence to answer the question post to the Verily board, which has two sections: One is for evidence that answers the verification question affirmatively; the other is for evidence that provides a negative answer.

The type of evidence that can be posted includes text, pictures and videos. Each piece of evidence posted to the Verily board must be accompanied by an explanation from the person posting as to why that evidence is relevant and credible.

As such, a parallel goal of the Verily project is to crowdsource critical thinking. The Verily platform is expected to launch at www.Veri.ly in early 2014.

Machine computing

The 8.8 magnitude earthquake that struck Chile in 2010 was widely reported on Twitter. As is almost always the case, along with this surge of crisis tweets came a swell of rumors and false information.

One such rumor was of a tsunami warning in Valparaiso. Another was the reporting of looting in some districts of Santiago. Though these types of rumors do spread, recent empirical research has demonstrated that Twitter has a self-correcting mechanism. A [study of tweets posted in the aftermath of the Chilean earthquake](#) found that Twitter users typically push back against noncredible tweets by questioning their credibility.

By analyzing this pushback, researchers have shown that the credibility of tweets could be predicted. Related data-driven analysis has [also revealed that tweets with certain features are often false](#). For example, the length of tweets, the sentiment of words used and the number of hashtags and emoticons used provide indicators of the likely credibility of the tweet's messages. The same goes for [tweets that include links to images and videos](#) - the language contained in tweets that link to multimedia content can be used to determine whether that multimedia content is credible or not.

Taken together, these data provide machines with the parameters and intelligence they need to begin predicting the accuracy of tweets and other social media content. This opens the door to a bigger role for automation in the verification process during disasters and other breaking news and emergency situations.

In terms of practical applications, these findings are being used to [develop a "Credibility Plugin" for Twitter](#). This involves my team at the Qatar Computing Research Institute working in partnership with the Indraprastha Institute of Information Technology in Delhi, India.

This plugin would rate individual tweets on a scale from 0 to 100 based on the probability that the content of a given tweet is considered credible. The plugin is expected to launch in early 2014. The main advantage of this machine computing solution is that it is fully automated, and thus more scalable than the human computing platform Verily.

Hybrid computing

The Artificial Intelligence for Disaster Response (AIDR) platform is a hybrid of the human and machine computing models.

The platform combines human computing (microtasking) with machine computing (machine learning). Microtasking is taking a large task and splitting it into a series of smaller tasks. Machine learning involves teaching a computer to perform a specified task.

AIDR enables users to teach an algorithm to find information of interest on Twitter. The teaching process is done using microtasking. For example, if the Red Cross were interested in monitoring Twitter for references to infrastructure damage following a disaster, then Red Cross staff would use AIDR's microtasking interface to tag (select) individual tweets that refer to damage. The algorithm then would learn from this process and automatically find additional tweets that refer to damage.

This hybrid computing approach can be used to automatically identify rumors based on an initial set of tweets referring to those rumors. Rapidly identifying rumors and their source is an important component of verifying user-generated content. It enables journalists and humanitarian professionals to track information back to its source, and to know whom to contact to take the next essential step in verifying the information.

To be sure, the goal should not only be to identify false or misleading information on social media but to counter and correct this information in near real time. A first version of AIDR was released in November 2013.

Accelerating the verification process

As noted earlier, the nascent stages of verification platforms powered by advanced computing mean that their ultimate value to the verification of user-generated content remains to be seen. Even if these platforms bear fruit, their early iterations will face important constraints. But this early work is essential to moving toward meaningful applications of advanced computing in the verification process.

One current limitation is that AIDR and the upcoming Credibility Plugin described above are wholly dependent on just one source: Twitter. Cross-media verification platforms are needed to triangulate reports across sources, media and language. While Veri.ly comes close to fulfilling this need, it relies entirely on human input, which does not scale easily.

In any event, these solutions are far from being the silver bullet of verification that many seek. Like other information platforms, they too can be gamed and sabotaged with sufficient time and effort. Still, these tools hold the possibility of accelerating the verification process and are likely to only advance as more effort and investment are made in the field.

7.1. How OpenStreetMap Used Humans and Machines to Map Affected Areas After Typhoon Haiyan

Written by **Dan Stowell**

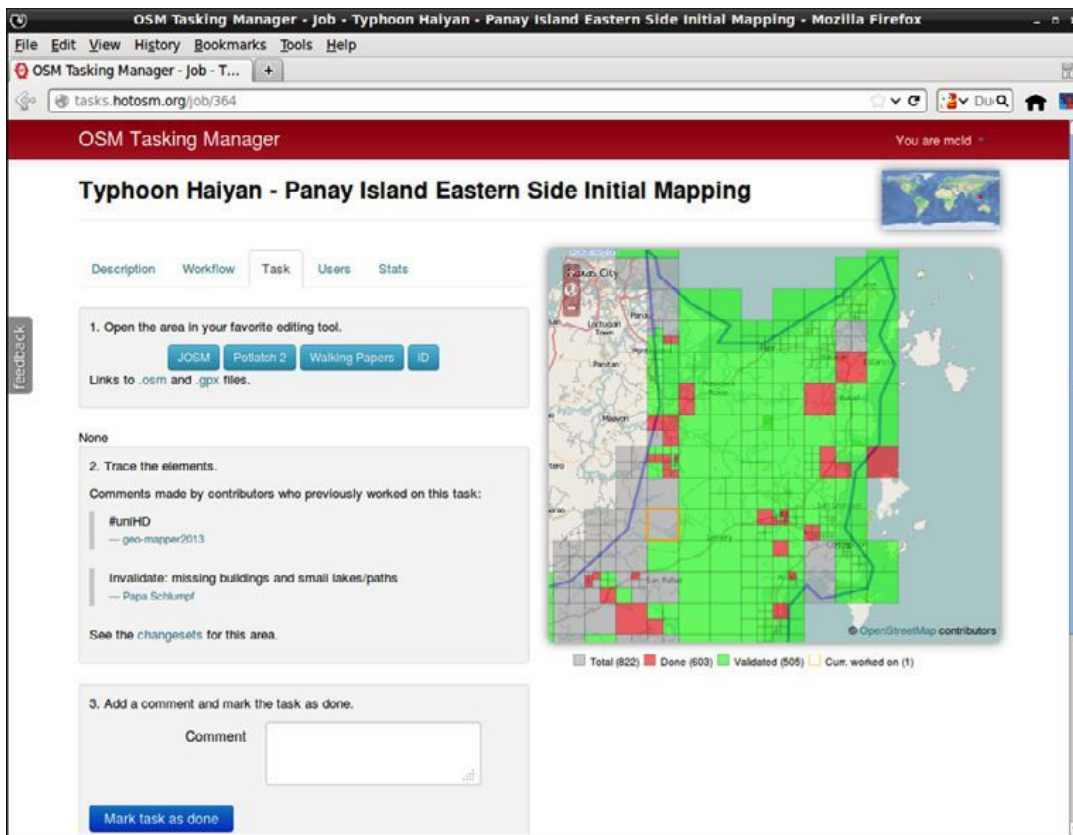
OpenStreetMap is a map database, built on the crowd-edited and copyleft model that many will recognize from Wikipedia. It provides some of the most detailed maps publicly available - particularly for many developing countries.

When Typhoon Haiyan struck the Philippines in 2013, a group of volunteer mappers came together to map and validate the damage experienced in the area. This was coordinated by the Humanitarian OpenStreetMap Team (HOT), which responds to humanitarian incidents by “activating” volunteers to map affected areas with fast turnaround. The work combines human validation with automated analysis to get results that are relied on by the Red Cross, Médecins Sans Frontières and others to guide their teams on the ground.

The HOT maintains a network of volunteers coordinated via a mailing list and other routes. Twenty-four hours before the typhoon struck, members discussed the areas likely to be hit and assessed the quality of existing data, preparing for a rapid response.

Once the typhoon reached the Philippines and was confirmed as a humanitarian incident, the HOT team called for the network of volunteers to contribute to mapping the area, including specific mapping priorities requested by aid agencies. There were two main goals. The first was to provide a detailed general basemap of populated areas and roads. The second was to provide a picture of what things looked like on the ground, postdisaster. Where had buildings been damaged or destroyed? Which bridges were down?

Work was coordinated and prioritized through the HOT Tasking Manager website (pictured below), which is a microtasking platform for map-making. It allows HOT administrators to specify a number of “jobs” to be done - such as mapping the roads and buildings within a defined area - and divides each job into small square “tasks,” each manageable by one volunteer mapper by tracing from aerial imagery.



During the Haiyan response, more than 1,500 mappers contributed, with up to 100 using the Tasking Manager at the same time. Dividing each job was crucial in order to make the best use of this surge of effort.

After claiming a task, a user edits their area of OpenStreetMap and can then mark their task square as “Done” (the red squares in the picture). However, the Tasking Manager requires that a second, more experienced person survey the work done before the task can be marked as “Validated” (green). (If the task was not completed properly, the “Done” status is removed by the second person.) Mappers can leave comments on the task’s page, explaining reasons for unvalidating or highlighting any issues encountered in mapping.

Aerial imagery is crucial to enable “armchair mappers” to contribute remotely by tracing roads, buildings and other infrastructure. Microsoft provides global Bing imagery for the use of OpenStreetMap editors, and this was used during Haiyan.

Representatives of HOT also liaised with the State Department Humanitarian Information Unit through the Imagery to the Crowd program and other agencies and companies, to obtain high-resolution aerial imagery. Once that became available, the HOT team created new jobs in the Tasking Manager, asking volunteers to further validate and improve the basemap of the Philippines.

The Tasking Manager is the most visible validation step, but the OpenStreetMap ecosystem also crucially features a lot of automatic (machine-driven) validation. Map editing software (“JOSM”) automatically validates a user’s edits before upload, warning about improbable data, such as buildings overlapping, or rivers crossing without meeting.

Other automated tools regularly scan the OpenStreetMap database and highlight potential problems. Experienced mappers often use these for post-moderation: They can fix or revert problematic edits, or contact the user directly.

This workflow (combined with ongoing coordination and communication via email lists, blogs and wikis) provides a validation structure on top of OpenStreetMap’s human-driven community model.

The model remains highly open, with no pre-moderation and a semiformal hierarchy of validators; yet it rapidly produces highly detailed maps that informed humanitarian response agencies for a very variable.

INVESTIGADOR_Z

Since the data are open, agencies responding to needs in the aftermath of Typhoon Haiyan have been able to use it in many different ways: They printed it out as maps; downloaded it to response teams' SatNav units; used it to locate population centers such as villages; and analyzed it to understand patterns of disease outbreak.

This rapidly updated map data can also be used by journalists with a bit of geodata know-how; for example, to provide geolocated contextual information for data coming in from other sources such as tweets, to help validate claims about the relative impacts on different areas, or to produce infographics of the impact and spread of a disaster.

8. Preparing for Disaster Coverage

Written by **Sarah Knight**

News organizations traditionally have had two information-driven roles during an emergency. The first is to provide people the information they need to respond to an event. This information must be clear, timely and unambiguous. Often this information comes directly from government agencies, the army, fire service, police or another official source.

The second role is the one newsrooms practice (or should practice) every day: to share critical information fairly and without favor or prejudice.

These days, there is also a third role. People today often first learn about an emergency threat through social media. Rather than being the first to inform people about an emergency event, newsrooms and other organizations often find themselves acting as a critical second source of verification, a filter that separates signal from noise, and rumor.

Preparedness is key to getting accurate information to the people who need it - and to ensuring you don't accidentally spread false information.

What can you do to make sure that you get the information you need to keep people safe, and to be the trusted source during a time of chaos and confusion? In this chapter we'll look at some simple ways to prepare yourself and your colleagues to deliver quality, timely information during an emergency.

Elements of preparedness

The first thing to decide is what informational role your organization is going to play. Are you reporting and/or are you assisting the community by issuing warnings and timely advice?

The Australian Broadcasting Corporation separates the two. Our newsroom reports and our programs on Local Radio and to an extent our 24-hour news channel News24 issue official warnings and advice, and report later.

The ABC policy says emergency broadcasting consists of transmitting formal and official warnings related to an emergency event, and transmitting information provided by other sources, including listener calls and social media and recovery broadcasting. Our policy does not apply to "Staff and contractors of the ABC News Division, whose reporting of emergency events is excluded."

Local information

With your role(s) defined, the next thing is to arm your people with the local information they need to respond quickly, and to understand the implications of a potential threat. This means analyzing what kind of emergency situations are likely to occur in your area, and to prepare for them.

Some questions to consider:

- What are the most common and likely natural disasters that strike in our area?
- What kinds of crimes or emergencies tend to occur?
- What are the critical structures in the area (highways, bridges, etc.)?
- Are there sensitive government agencies or military installations that could be targets?
- What are the risky roadways or other infrastructure elements that often are the scene of emergency incidents?

- What neighborhoods/regions are home to gangs, rebel groups, etc.?

Now that you've identified some of the more likely situations, begin to build a list of the authoritative sources - both official and unofficial - that will have useful, critical information.

This includes first responders (are they on Twitter? Facebook? Can you build a list of them to have ready?), as well as local experts at universities, NGOs and government offices, and the communications leads for important agencies, companies and other organizations.

Gather phone numbers, Twitter accounts, Facebook pages and put everything into a central, accessible format, be it a shared database, spreadsheet or other means. Organize your contacts by the kind of situation where they might be most helpful.

Building relationships

Every journalist or humanitarian worker needs contacts. But it's not just about the phone numbers and other details - it's about the relationships. Trusted sources you know you can call for quality information. Sources that trust you.

That trust is not going to instantly develop during an emergency.

You need to be proactive. If possible, meet your sources face to face. Invite them to look around your newsroom, office or facilities. Show them what you do with the information they provide. Explain how you will be helping them get their message to the people who need it. Take time to visit them and see how they work during an emergency. Understand their processes and the pressures on them. Knowing you personally will help you get priority when they are busy dealing with multiple requests.

As well as relationships with key personnel in emergency management services and other organizations/agencies, consider the relationship with your audience.

Do they know that you will provide them with timely information? Do they know when they are likely to hear or see it? Do they know what services you provide - and don't provide - during an emergency?

For newsrooms, preparedness stories are one way to communicate the message that you will be a source of information that can help them. For example, at the ABC we publish reports offering [a view of what the upcoming fire season looks like](#), as well as [guides to packing emergency kits](#). This sort of content can be offered by newsrooms, aid agencies and other organizations, and helps set the stage for how you can be of help to the public.

It's also important to get the information flowing the other way, too. Your audience and community will be a valuable important source of information for you in an emergency. Encourage your audience to call, email or text you with information. This can start with traffic snarls, weather photos and other information.

Training staff

At the ABC we start with an Emergency Broadcast Plan. In it are clear instructions for how to treat official warnings on air, as well as information such as transmission coverage maps to make sure the warnings get to the people affected.

We also have in our plan information that anchors can use on air to help people. The information comes from the various emergency management agencies. For example: "Fill up your bath with water so you can use that water to put out spot fires if the water pressure falls," or "Fasten all cyclone screens. Board up or heavily tape exposed

windows.”

Part of your preparation should also include gathering advice that can be provided to the public when disaster strikes. This can be collected as you reach out to your sources ahead of time.

Be sure to create internal processes that require you to reconnect with your sources to ensure this information is current. This updating can be scheduled if your area is prone to weather-related emergencies.

In northern Australia, for example, cyclones are a big concern. They are also somewhat predictable in that there is a season when they’re most likely to occur. Prior to the season, our local plans are updated, and emergency agencies are called to check that the information and contacts are still correct. Staff are brought together to go through the procedures in small groups.

This not only ensures that the information in the plan is current but also helps to re-establish relationships that may have been neglected in the quiet period.

A tool we’ve found handy when training staff are hypotheticals based on previous experience. The hypothetical forces the staff to think through what they would do in that scenario and can sometimes lead to vigorous discussion about best practices. Technology and tools change quickly, so this can be a great way to ensure you’re up to date.

We pitch these hypotheticals at different levels, for example:

- What to do when a catastrophic weather event is forecast?
- What do you do when you’re asked to evacuate the studio?
- What if you’re doing your normal shift and a warning comes in?

Work health and safety is a key concern. Ensure your people have adequate training in being in hazardous zones. In Australia, for example, fire and emergency authorities hold training sessions for the media in reporting from fire zones; staff are not sent to the fire ground without having completing that training.

Emergency management agencies often run media training sessions to train journalists – in the hazards of visiting fire grounds, for example. This can be especially important to participate in if only journalists accredited with such training are able to pass through roadblocks to report the story. (The training in itself is another way for the journalist to make contacts within the emergency organization and to begin building trust.) At aid organizations, training people is especially important, as they can remain on the ground for long periods of time.

Finally, don’t neglect new hires and new members of your team. We have a policy of inducting staff in emergency broadcast procedures within two weeks of their starting. Emergencies unfortunately don’t wait for an annual training session!

Internal communication

It’s not enough to have fast communication pathways with external stakeholders. You need to devise the workflow and communication plan for you and your colleagues to work together.

Some key questions to consider and answer include:

- How you will communicate what you’re doing with the rest of your organization?
- Who is in charge of making the final call on what gets shared/published/broadcast?
- Is there a paywall that needs to come down in an emergency?
- Will you have a dedicated section of your website

- What does your technical support team need to know/do?
What about your website producers? Those handling social media?
- Are your transmitters and other critical infrastructure safe?

At the ABC we've developed a Situation Report that is distributed widely through our email system when there is a significant emergency. This ensures that everyone has an idea of the threat and the ABC's response and who is managing the emergency internally.

The "Sitrep" is a useful tool not just to communicate internally but also as a checklist for managers when there is a danger of paralysis from information overload.

Email distribution groups of key personnel in each state have been set up and are regularly maintained for ease of distribution. You can also consider SMS distribution lists and other ways to pushing information to your people. (We use Whispir, an internal email/text tool that can deliver emergency alerts for breaking news.)

During a major emergency, such as the recent New South Wales bushfires, we ask the rest of the network to not call the team dealing with the emergency for interviews about the emergency. We also ask that teams outside of the affected area not call emergency authorities so that they are not overloaded. Sometimes we allocate someone to deal with outside requests specifically so that our team can get on with delivering emergency information to the people under threat.

When it comes to verification, the key piece to communicate is the workflow for how content and information will be gathered, checked and then approved or denied for publication. Who does the checking and who reviews that work? How do you ensure that each piece of content an benefit from many eyes, while still enabling you to move quickly and get important information out?

Recovery broadcasting

Organizations always want to cover and respond to an emergency during the height of the disaster, but the communities affected can take many months, or years, to recover. Newsrooms should plan to be there in the aftermath to support those communities with information they can use. (This is less of an issue with aid and humanitarian organizations, who put a priority on this aspect.)

Being there at this time can build trust with your organization. One of the common complaints post-emergency is a feeling of abandonment.

You need to aid your staff's recovery as well. A debrief after the emergency is essential to allow people to vent and to make sure you understand what happened in order to improve your service next time. There will be a next time.

Staff members should also be checked on individually. Often these events can be traumatic, and not just for those who physically go to the disaster zone. Staff members may have been affected personally, with family members at risk.

After the 2009 Black Saturday bushfires in Victoria, Australia, many staffers reported feeling helpless after receiving phone call after phone call from desperate people caught in the fire zones.

Years after the Queensland floods of 2011, staff who "soldiered on" reported post-traumatic stress symptoms.

It's important that staff and managers recognize the symptoms of stress in the workplace and have the tools or resources to help at hand.

You can cover an emergency without preparation, but your coverage will be more effective and less stressful on your staff if you create a plan, develop external relationships with stakeholders, set up communication pathways within your organization and ensure staff welfare through training, offering support during an event and conducting effective debriefs.

Tip for Aid Organizations

Aid organizations need to consider the target audience for information. Are you aiming to source information and provide it to your people on the ground to direct their efforts? Are you feeding information to the media or government? Are you communicating directly with the public using social media platforms?

Remember if you aren't telling people what your organization is doing... who is? Someone will be and it may not be accurate. Make sure there isn't an information vacuum.

8.1. How NHK News Covered, and Learned From, the 2011 Japan Earthquake

Written by Takashi Ōtsuki

When a massive earthquake struck Japan the afternoon of March 11, 2011, NHK, Japan's only public broadcaster, was broadcasting a live debate on its main channel.

The Japan Meteorological Agency (JMA) issued an alert 30 seconds after the quake was detected, and NHK reacted by immediately inserting a ticker with a map (seen below). It displayed the quake's epicenter and indicated areas that could expect to experience tremors; the graphic was also accompanied by an audio warning. (The JMA issues alerts and warnings based on data from seismometers placed all over Japan.)

A minute after JMA's alert, all of NHK's TV and radio programs switched to live studio coverage about the earthquake, and the related tsunami warning.



NHK works closely with the JMA to ensure a high standard of disaster preparedness and the rapid communication of events. NHK set up a system that allows us to quickly create graphics and automatically produce news scripts for on-air personnel. NHK also carries out training every day after midnight when no programs are aired. (This is because we are constantly monitoring and reporting on earthquakes). These commitments to disaster preparedness meant we were able to quickly move to live coverage immediately after the quake was detected.

Disaster preparedness at NHK doesn't solely rely on the JMA alerts. We also operate and monitor footage from 500 robot cameras set up in major cities, in coastal areas and around nuclear power plants. This provides us with an amazing amount of live footage when a disaster strikes. For example, during the earthquake, a camera captured a tsunami wave 30 minutes after the quake was detected (shown below).



Along with cameras, NHK used aerial images captured from helicopters to show the effects of the quake and tsunami. It meant we were able to broadcast live, unforgettable footage of a tsunami wiping out houses in Sendai - a mere hour after the quake (as shown in the following page).

By 2014, we will have 15 helicopters stationed in 12 locations around Japan. This will enable us to reach, and broadcast from, any location in the country within an hour.

NHK also made an effort to spread its earthquake coverage to different platforms. Live television and radio broadcasts were livestreamed on platforms such as Ustream and Niconico Live. We were swamped with requests from people seeking information about the safety of loved ones. To do this at scale, NHK placed whatever information we had on [Google Person Finder](#), which “helps people reconnect with friends and loved ones in the aftermath of natural and humanitarian disasters.”



Adapting and improving

Following the earthquake, NHK adapted our disaster coverage approach to improve areas of weakness and improve upon what we already do. Here are five new initiatives we launched:

INVESTIGADOR_Z

1. We improved disaster reporting to ensure it can be understood both visually and auditorily. Our previous disaster broadcasting emphasized a detached, factual approach focused primarily on communicating the details of a quake (such as its epicenter, the expected height of any tsunami, etc.). Today, a newscaster will, in case of a major emergency, immediately call upon viewers to evacuate, when necessary. Newscasters also emphasize the need to evacuate calmly, so as not to cause panic. In addition, we use a visual ticker that can appear whenever there is a call for immediate evacuation (see below). This ensures that people with hearing disabilities receive the essential information.



2. In the wake of the 2011 earthquake, many media outlets relied on press releases from the government and power company to report the situation at nuclear power plants. This was in part a result of limited access to the plants, and it meant we were unable to independently verify the information. To better prepare and ensure that we can present official information in a more accurate context, we now train journalists in scientific and specialized topics. We also seek out and present the opinions of multiple experts, and deliver forecasts of the impact of a quake and any nuclear power plant accidents.

3. People in disaster-affected areas used social media to connect with local print and radio outlets, and with one another. In order to ensure that our reporters use social media effectively when covering a disaster, NHK developed new guidelines that provide protocols to deal with user-generated content, such as including caveats related to the level of verification we were able to apply to a given piece of information. The guidelines also include advice on how to identify fake information.

In addition, we established a "Social Listening" team that focuses on social media monitoring and verification. The team (seen below) makes heavy use of Twitter Lists to pre-establish a network of reliable sources for better monitoring and fact-checking when an event occurs.



4. NHK developed its own user-generated content platform, NHK ScoopBox. The platform gathers an uploader's personal details and location, making it easier to directly contact and confirm their content. When a tornado struck Kanto region in September 2013, ScoopBox enabled us to source and verify 14 items of user-generated content that was used in national and local broadcasts.

5. In the aftermath of the quake, we lost the pictures from several of our robot cameras after power outages hit areas affected by the tsunami. Due to the scope of damage, as well as safety restrictions in Fukushima, NHK crews were unable to recharge the cameras. To avoid this in the future, NHK developed a system to generate power through wind and solar energy and store it more securely in robot cameras. (Below are images showing an NHK camera, and the solar panels that help keep it running.)





9. Creating a Verification Process and Checklist(s)

Written by **Craig Silverman** and **Rina Tsubaki**

Verification Fundamentals

- Put a plan and procedures in place for verification before disasters and breaking news occur.
- Verification is a process. The path to verification can vary with each fact.
- Verify the source and the content they provide.
- Never parrot or trust sources whether they are witnesses, victims or authorities. Firsthand accounts can be inaccurate or manipulative, fueled by emotion or shaped by faulty memory or limited perspective.
- Challenge the sources by asking “How do you know that?” and “How else do you know that?” Triangulate what they provide with other credible sources including documentations such as photos and audio/video recordings.
- Ask yourself, “Do I know enough to verify?” Are you knowledgeable enough about the topics that require understanding of cultural, ethnical, religious complexities?
- Collaborate with team members and experts; don’t go it alone.

Verifying user-generated content

- Start from the assumption that the content is inaccurate or been scraped, sliced, diced, duplicated and/or reposted with different context.
- Follow these steps when verifying UGC:
 - Identify and verify the original source and the content (including location, date and approximate time).
 - Triangulate and challenge the source.
 - Obtain permission from the author/originator to use the content (photos, videos, audio).
- Always gather information about the uploaders, and verify as much as possible before contacting and asking them directly whether they are indeed victims, witnesses or the creator of the content.

1. Identify and verify the original source and the content (including location, date and approximate time).

Provenance

The first step of UGC verification is to identify the original content, be it a tweet, image, video, text message, etc. Some questions to start with:

- Can you find the same or similar posts/content elsewhere online?
- When was the first version of it uploaded/filmed/shared?
- Can you identify the location? Was the UGC geotagged?
- Are any websites linked from the content?
- Can you identify the person who shared/uploaded the UGC, and contact them for more information? (See the “Source” section below.)

When dealing with images and videos, use Google Image Search or TinEye to perform a reverse image/video thumbnail search. If several links to the same image pop up, click on “view other sizes” to find the highest resolution/size, which usually is the original image.

INVESTIGADOR_Z

For verifying provenance of images:

- Use Google Image Search or TinEye to perform a reverse image search. If several links to the same image pop up, click on “view other sizes” to find the highest resolution/size which usually is the original image.
- Check to see if the image has any EXIF data (metadata). Use software like Photoshop or free tools such as FotoForensics.com or Findexif.com to see information about the model of the camera, the timestamp of the image (caution: the data could default to the manufacturer’s settings), and the dimensions of the original image.
- Social networks like Twitter, Facebook and Instagram strip out most metadata. Flickr is an exception. Instead, try Geofeedia and Ban.jo to identify the GPS data from the mobile device that uploaded the image.

For verifying provenance of video:

- Use acronyms, place names and other pronouns for good keyword search on video sharing platforms such as YouTube, Vimeo and Youku.
- Use Google Translate when dealing with contents in a foreign language.
- Use the date filter to find the earliest videos matching the keywords.
- Use Google Image Search or TinEye to perform a reverse video thumbnail search.

Source

With the original content identified, gather information about the author/originator of the content. The goal is to confirm whether the person behind the account is a reliable source. Examine an uploader’s digital footprint by asking these questions:

- Can you confirm the identity of, and contact, the person?
- Are you familiar with this account? Has their content and reportage been reliable in the past?
- Check the history of the uploader on the social network:
 - How active are they on the account?
 - What do they talk about/share?
 - What biographical information is evident on the account? Does it link anywhere else? What kind of content have they previously uploaded?
 - Where is the uploader based, judging by the account history?
- Check who they are connected on the social network:
 - Who are their friends and followers?
 - Who are they following?
 - Who do they interact with?
 - Are they on anyone else’s lists?
- Try to find other accounts associated with the same name/username on other social networks in order to find more information:

- If you find a real name, use people search tools (Spokeo, White Pages, Pipl.com, WebMii) to find the person's address, email and telephone number.
- Check other social networks, such as LinkedIn, to find out about the person's professional background.
- Check if a Twitter or Facebook Verified account is actually verified by hovering over the blue check. If the account is verified by Twitter or Facebook, a popup will say "Verified Account" or "Verified Page."

When dealing with images and videos, adopt the shooter's perspective. (These questions also work when trying to verify textual information.) Ask yourself these questions about the source to check their credibility:

- Who are they?
- Where are they?
- When did they get there?
- What could they see (and what does their photo/video show)?
- Where do they stand?
- Why are they there?

Connect their activity to any other online accounts they maintain by asking these questions:

- Search Twitter or Facebook for the unique video code - are there affiliated accounts?
- Are there other accounts - Google Plus, a blog or website - listed on the video profile or otherwise affiliated with this uploader?
- What information do affiliated accounts give that indicate recent location, activity, reliability, bias or agenda?
- How long have these accounts been active? How active are they? (The longer and more active, the more reliable they probably are.)
- Who are the social media accounts connected with, and what does this tell us about the up- loader?
- Can we find whois information for an affiliated website?
- Is the person listed in local phone directories, on Spokeo, Pipl.com or WebMii or on LinkedIn?
- Do their online social circles indicate they are close to this story/location?

Content

Date

Verify the date and approximate time, particularly when dealing with photos/videos:

- Check the weather information on the day and the location where the event happened. Is the weather condition the same from the (local) weather forecasts and other uploads from the same event? Use Wolfram Alpha to perform a search (e.g., "What was the weather in London, England, on January 20, 2014?").
- Search news sources for reports about events on that day.
- Using video and image search (YouTube, Google, TinEye, etc.), see if any earlier pieces of content from the same event predate your example. (Be aware that YouTube date stamps using Pacific Standard Time from the moment the upload begins.)
- For images and video, look (and listen) for any identifying elements that indicate date/time, such as clocks, television screens, newspaper pages, etc.

Location

Another crucial aspect of verification is to identify the location of the content:

INVESTIGADOR_Z

- Does the content include automated geolocation information? (Services such as Flickr, Picasa and Twitter offer the option of including location, though it is not foolproof.)
- Find reference points to compare with satellite imagery and geolocated photographs, such as:
 - Signs/lettering on buildings, street signs, car registration plates, billboards, etc. Use Google Translate or free.orc.com for online translation.
 - Distinctive streetscape/landscape such as mountain range, line of trees, cliffs, rivers, etc.
 - Landmarks and buildings such as churches, minarets, stadiums, bridges, etc.
 - Use Google Street View or Google Maps' "Photos" function to check if geolocated photographs match the image/video location.
 - Use Google Earth to examine older images/videos, as it provides a history of satellite images. Use Google Earth's terrain view.
 - Use Wikimapia, the crowdsourced version of Google Maps, to identify landmarks.
 - Weather conditions such as sunlight or shadows to find approximate time of day. Use Wolfram Alpha to search weather reports at specific time and place.
 - License/number plates on vehicles
 - Clothing

For Videos:

- Examine the language(s) spoken in the video. Check if accents and dialects match up with the geographical location. Beware that Google Translate does not give correct translation for some languages. Ask those who speak the language for support.
- Are video descriptions consistent and mostly from a specific location?
- Are videos dated?
- If videos on the account use a logo, is this logo consistent across the videos? Does it match the avatar on the YouTube or Vimeo account?
- Does the uploader "scrape" videos from news organizations and other YouTube accounts, or do they upload solely user-generated content?
- Does the uploader write in slang or dialect that is identifiable in the video's narration?
- Are the videos on this account of a consistent quality? (On YouTube go to Settings and then Quality to determine the best quality available.)
- Do video descriptions have file extensions such as .AVI or .MP4 in the video title? This can indicate the video was uploaded directly from a device.
- Does the description of a YouTube video read: "Uploaded via YouTube Capture"? This may indicate the video was filmed on a smartphone.

2. Triangulate and challenge the source

Once you go through the above steps ask yourself:

- Do the images/videos/content make sense given the context in which it was shot/filmed?
- Does anything look out of place?
- Do any of the source's details or answers to my questions not add up?
- Did media outlets or organizations distribute similar images/videos?
- Is there anything on Snopes related to this?

- Does anything feel off, or too good to be true?

When getting in touch with the source, ask direct questions and cross-reference answers to information you get through your own research. Make sure that their answers match up with your findings.

For images:

- When questioning, reflect what you know from the EXIF data and/or geolocation information from tools like Google Street View and Google Maps.
- Ask them to send in other additional images that were shot before and after the image in question.
- If the image is from a dangerous location, always check if the person is safe to speak to you.

For videos:

- If you have doubts over construction of the video, use editing software such as VLC media player (free), Avidemux (free) or Vegas Pro (licensed) to split a video into its constituent frames.

3. Obtain permission from the author/originator to use the content

Copyright laws vary from country to country, and the terms of conditions differ from service to service. Obtaining permission to use images, video and other content is essential.

When seeking permission:

1. Be clear about which image/video you wish to use.
2. Explain how it will be used.
3. Clarify how the person wishes to be credited. Do they want to be credited with a real name, a username or anonymously?
4. Consider any consequences of using the content and/or name of the person. Is it necessary to blur the faces for privacy and security reasons? Will the creator/uploader be put in danger if you credit them by real name?

Preparing for verification success in disaster and breaking news situations

Here are a few tips for creating a better verification process:

1. Build and maintain a network of trusted sources
 - Build a list of reliable sources that include both official and unofficial such as first responders, academic experts, NGOs, government offices, etc. Gather not only social media accounts but also phone numbers and emails in a shared database/spreadsheet.
 - Create Twitter Lists that are organized in logical groups based on topics or geographical location. Find the reliable sources through Twitter advanced searches and by following specific hashtags. You can also use Facebook Interest Lists and Google Plus circles, sub- scribe to YouTube channels and build playlists.
 - Never treat those you come across on social networks as just sources. Treat them like human beings and engage. They are your colleagues.
 - In the crowd, there are reliable sources who developed, either professionally or non-professionally, expertise in a specific topic area. There are also sources in a specific physical location.
 - Build trust by engaging on social networks and meeting people in person. Ask them to recommend and/or help you verify sources. By interacting with them, you will learn their strengths, weaknesses, biases and other

INVESTIGADOR_Z

factors.

2. Identify the role you/your organization will play in the moment, and any possible disaster scenarios

- Identify your role in disaster communications.
- Determine how you should communicate effectively when an emergency occurs.
- Think about with whom you want to communicate, what are the useful information for these target group, what sort of language you should use to advise them.
- Structure your internal communication as fully as you structure your external one.

3. Train, debrief and support staff and colleagues

- Establish the toolset, workflow, approvals and communication procedures to use in disaster situations.
- Provide situational/scenario training, especially for those living in the area where certain types of disasters are expected to happen.
- Give staff the ability to participate in disaster training programs offered by emergency services.
- Prepare scripts/messages that will be used in specific disaster situations.
- Plan regular check-ins with key sources to ensure their contact information is up-to-date.
- Debrief staff after coverage, and adjust your emergency plans and training to adapt to new learnings.
- Do not underestimate “trauma” and “stress” that results from reporting crises. Provide support where needed.

9.1. Assessing and Minimizing Risks When Using UGC

Written by **Madeleine Bair**

Photos and videos that emanate from areas of the world rife with repression and political violence, or that document vulnerable populations, come with risks beyond the possibility that the content has been manufactured or manipulated. In these situations, individuals behind and in front of the camera may face the risk of arrest, harassment, torture or death. That danger can increase if international media picks up the footage.

We saw this during Iran's Green Revolution of 2009, when the [Islamic Revolutionary Guard](#) used photos and video stills they found online to target protesters and crowdsource their identification, actions that sent a chill through the activist community.

Identity exposure [puts individuals at risk of retribution by repressive authorities](#), and can lead to social stigma as well, with its own potentially severe consequences. Just as news organizations adhere to standards for protecting the privacy of rape victims, journalists should consider these same standards when using video that exposes vulnerable people, particularly if it appears to have been taken without their informed consent.

For example, in 2013 U.S. online media and advocacy organizations reported on an alarming pattern of abuse targeting LGBT youth in Russia. Many of their articles embedded photographs and videos shot by perpetrators abusing their victims — exposure which [could perpetuate the harm and stigma](#) to those victims.

Journalists and others should not censor video taken by activists who knowingly take risks to speak out or document their community. But journalists should take basic steps to identify and minimize harm to those who may be unaware of those risks, or who lack the capacity to give informed consent to the recording. In the case of the Russian abuse video, it's clear that the victims did not consent to being a part of such footage.

Assess the potential for future harm

First, you must assess whether an image or video could cause harm to those involved. Are they in a dangerous part of the world? Do they risk reprisals for sharing this information, or for being shown? Can you safely assume that the people shown in the image/video consented to being filmed?

If there is a real risk of harm, you have two options:

1. Don't use the image/footage. Just because it exists does not mean it needs to be shared/broadcast/published. We can report on it in other ways, and use it to inform our work.
2. Blur the identities. Television newsrooms often blur faces of vulnerable individuals when they broadcast their image. Photographs can easily be edited to blur faces. For online videos, you can re-upload the video to YouTube and use its face blurring function. [Explained here](#), the tool was created to protect the identity of vulnerable subjects in videos, and can be found as an "Additional Feature" when you click on the Video Enhancements tool to edit a video.

One credo encompassed in the standard codes of ethics for journalists, crisis responders and human rights workers is to minimize harm. Taking the time to assess and minimize harm to individuals when using citizen media is one way to put that credo into practice in 21st century reporting.

9.2. Tips for Coping With Traumatic Imagery

Written by **Gavin Rees**

Images from war zones, crimes scenes and natural disasters are often gruesome and distressing. When the imagery is traumatic, events that are happening far away can feel like they are seeping into one's personal headspace. Negative reactions, such as disgust, anxiety and helplessness, are not unusual for journalists and forensic analysts working with such material.

We know from research that media workers are a highly resilient group: Exposure to limited amounts of traumatic imagery is unlikely to cause more than passing distress in most cases. Nevertheless, the dangers of what psychologists call secondary or vicarious traumatization become significant in situations where the exposure is repeated, the so-called slow drip effect. The same is true when there is a personal connection to the events - if, for example, it involves injury to someone you know.

Here are six practical things media and humanitarian workers can do to reduce the trauma load:

- 1. Understand what you're dealing with.** The first line of any defense is to know the enemy: Think of traumatic imagery as akin to radiation, a toxic substance that has a dose-dependent effect. Journalists and humanitarian workers, like nuclear workers, have a job to do; at the same time, they should take sensible steps to minimize unnecessary exposure.
- 2. Eliminate needless repeat exposure.** Review your sorting and tagging procedures, and how you organize digital files and folders, among other procedures, to reduce unnecessary viewing. When verifying footage by cross-referencing images from different sources, taking written notes of distinctive features may help to minimize how often you need to recheck against an original image.
- 3. Try adjusting the viewing environment.** Reducing the size of the window, and adjusting the screen's brightness and resolution, can lessen the perceived impact. And try turning the sound off when you can — it is often the most affecting part.
- 4. Experiment with different ways of building distance into how you view images.** Some people find concentrating on certain details, for instance clothes, and avoiding others, such as faces, helps. Consider applying a temporary matte/mask to distressing areas of the image. Film editors should avoid using the loop play function when trimming point of death imagery, or use it very sparingly.
- 5. Take frequent screen breaks.** Look at something pleasing, walk around, stretch or seek out contact with nature (such as greenery and fresh air, etc.). All of these can help dampen the body's distress responses. In particular, avoid working with distressing images just before going to sleep. It is more likely to populate your mental space.
- 6. Develop a deliberate self-care plan.** It can be tempting to work twice, three times, four times as hard on an urgent story or project. But it's important to preserve a breathing space for yourself outside of work. People who are highly resistant to trauma are more likely to exercise regularly, maintain outside interests in activities they love, and to invest time in their social connections, when challenged by trauma-related stress.

Some additional tips for editors and other managers:

- 1. Every member of a team should be briefed on normal responses to trauma.** Team members should understand that different people cope differently, how the impact can accumulate over time, and how to recognize when they or their colleagues need to practice more active self-care.

2. **Have clear guidelines on how graphic material is stored and distributed.** Feeds, files and internal communications related to traumatic imagery should be clearly signposted and distributed only to those who need the material. Nobody should be forced to watch video images that will never be broadcast.

3. **The environment matters.** If possible, workplaces that deal with violent imagery should have windows with a view of the outside; bringing in plants and other natural elements can also help.

10. Verification Tools

Verifying Identity:

Use these online verification tools to find contact details and profiles of users who are active on social media

- [AnyWho](#): a free white pages directory with a reverse look-up function.
- [AllAreaCodes](#): allows users to look up any name and address listed against a phone number. The service is free if the number is listed in the White Pages, and they provide details about unlisted numbers for a small price.
- [Facebook Graph Search](#): provides a streamlined method to locate individuals for the verification of information. Journalists do not need to know the name of the person they are searching for; instead, they can search based on other known criteria such as location, occupation and age.
- [GeoSocial Footprint](#): a website where one can track the users' location "footprint" created from GPS enabled tweets, social check ins, natural language location searching (geocoding) and profile harvesting.
- [Hoverme](#): this plug-in for Google Chrome reveals social media users' profiles on other networks from their Facebook news feed.
- [Linkedin](#): through work history and connections LinkedIn can provide additional means to track an individual down and verify the person's identity or story.
- [Muck Rack](#): lists thousands of journalists on Twitter, Facebook, Tumblr, Quora, Google+, LinkedIn who are vetted by a team of Muck Rack editors.
- [Numberway](#): a directory of international phone books.
- [Person Finder](#): one of the most well-known open source databanks for individuals to post and search for the status of people affected by a disaster. Whenever a large scale disaster happens, the Google Crisis Team sets up a person finder.
- [Pipl.com](#): searches for an individual's Internet footprint and can help identify through multiple social media accounts, public records and contact details.
- [Rapportive](#): this Gmail plugin gives users a profile on their contacts, including social media accounts, location, employment.
- [Spokeo](#): a people search engine that can find individuals by name, email, phone or username. Results are merged into a profile showing gender and age, contact details, occupation, education, marital status, family background, economic profile and photos.

- [WebMii](#): searches for weblinks that match an individual's name, or can identify unspecified individuals by keyword. It gives a web visibility score which can be used to identify fake profiles.
- [WHOIS](#): finds the registered users of a domain name and details the date of registration, location and contact details of the registrant or assignee.

Verifying places:

Did something actually happen where the crowd said it happened?

- [Flickr](#): search for geolocated photos.
- [free-ocr.com](#): extracts text from images which can then be put into Google translate or searched on other mapping resources.
- [Google Maps](#): an online map providing high-resolution aerial or satellite imagery covering much of the Earth, except for areas around the poles. Includes a number of viewing options such as terrain, weather information and a 360-degree street level view.
- [Google Translate](#): can be used to uncover location clues (e.g. signs) written in other languages.
- [Météo-France](#): France's meteorological agency makes freely available Europe focused radar and satellite images, maps and climate modelling data.
- [NASA Earth Observatory](#): the Earth Observatory was created to share satellite images and information with the public. It acts as a repository of global data imagery, with freely available maps, images and datasets.
- [United States ZIP Codes](#): an online map of the United States categorized according to ZIP code. Users are able to search for a specific ZIP code, or can explore the map for information about different ZIP codes.
- [Wolfram Alpha](#): a computational answer engine that responds to questions using structured and curated data from its knowledge base. Unlike search engines, which provide a list of relevant sites, Wolfram Alpha provides direct, factual answers and relevant visualizations.

Verifying images:

Is a particular image a real depiction of what's happening?

- [Foto Forensics](#): this website uses error level analysis (ELA) to indicate parts of an image that may have been altered. ELA looks for differences in quality levels in the image, highlighting where alterations may have been made.
- [Google Search by Image](#): by uploading or entering an image's URL, users can find content such as related or similar images, websites and other pages using the specific image.

INVESTIGADOR_Z

- [Jeffrey's Exif Viewer](#): an online tool that reveals the Exchangeable Image File (EXIF) information of a digital photo, which includes date and time, camera settings and, in some cases GPS location.
- [JPEGsnoop](#): a free Windows-only application that can detect whether an image has been edited. Despite its name it can open AVI, DNG, PDF, THM and embedded JPEG files. It also retrieves metadata including: date, camera type, lens settings, etc.
- [TinEye](#): a reverse image search engine that connects images to their creators by allowing users to find out where an image originated, how it is used, whether modified versions exist and if there are higher resolution copies.

Other Useful Tools

- [AIDR platform](#): uses human and computer monitoring to weed out rumors on Twitter.
- [Ban.jo](#): aggregates all social media into one platform allowing images and events to be cross-checked against each other.
- [HuriSearch](#): enables you to search content from over 5,000 human rights related Web pages and easily filter these to find verifiable sources.
- [InformaCam](#): The app addresses the verification challenge by harnessing metadata to reveal the time, date and location of photos or videos. Users can send their media files, and their metadata, to third parties by using digital signatures, encryption (PGP) and TOR secure servers.
- [PeopleBrowsr](#): a platform and tool on which the crowd can monitor and synthesize social media and news into location and time sequence, which can then also be filtered down. The platform also features a credibility score measuring users' influence and outreach on social networks.
- [SearchSystems.net](#): an international directory of free public records.
- [Snopes.com](#): a site dedicated to debunking Internet hoaxes, which can be used to crosscheck UGC.
- [YouTube Face Blur](#): Developed out of concern for the anonymity of individuals who appear in videos in high-risk situations, this tool allows users to blur faces of people who appear in videos they upload. To use, when you upload a video on YouTube, go to Enhancements, and then Special Effects. There you can choose to blur all faces in the video.

“VISUALIZE JUSTICE: A Field Guide to Enhancing the Evidentiary Value of Video for Human Rights”

As we have seen from the case studies and stories in this invaluable handbook, user-generated content can be instrumental in drawing attention to human rights abuse, if it is verifiable. But many filmmakers and activists want their videos to do more. They have the underlying expectation that footage exposing abuse can help bring about justice. Unfortunately, the quality of citizen video and other content rarely passes the higher bar needed to function as evidence in a court of law.

With slight enhancements, the footage citizens and activists often risk their lives to capture can do more than expose injustice - it can also serve as evidence in the criminal and civil justice processes. The forthcoming free field guide, “Visualize Justice: A Field Guide to Enhancing the Evidentiary Value of Video for Human Rights,” is intended to serve as a reference manual for citizen witnesses and human rights activists seeking to use video not only to document abuses, but also for the ambitious end goal of bringing perpetrators to justice.

Why a field guide?

When image manipulation is simple and false context is easy to provide, it is no longer enough to simply film and share and thereby expose injustice. Activists producing footage they hope to be used not only by journalists but also by investigators and courtrooms must consider the fundamental questions raised in the “Verification Handbook”: Can this video be verified? Is it clear where and when the video was filmed? Has it been tampered with or edited? They must also consider other questions more pertinent to the justice system: Is the footage relevant to a human rights crime? Can provenance be proved? Would its helpfulness in securing justice outweigh its potential to undermine justice?

Who’s it for?

The guide’s primary audience is people working in the field who do or will potentially film human rights abuses. These may be citizen journalists, activists, community reporters or human rights investigators. Some may already be filming such abuses in their work and could use guidance to enhance the evidentiary value of the videos they create. Others may already be investigating human rights abuse by traditional means, but want to incorporate video into their human rights reporting in a way that can enhance their evidence collection.

The comprehensive guide “Visualize Justice,” produced by WITNESS together with human rights colleagues, will cover:

- Video’s role in the criminal justice process
- Techniques for capturing video with enhanced evidentiary value
- How to prioritize which content to capture
- Managing media to preserve the chain-of-custody
- Case studies illustrating how video has been used in judicial settings

Journalism and justice

While this “Verification Handbook” provides innovative ways for journalists and crisis responders to analyze citizen video, WITNESS’s “Field Guide to Enhancing the Evidentiary Value of Video for Human Rights” will address the same issue from the other side of the coin by providing reasons for filmmakers to use so that the videos they capture

INVESTIGADOR_Z

can be as valuable as possible in exposing abuse and bringing about justice. Collectively, these two resources help ensure that more cameras in more hands can lead to better journalism and greater justice.

For more information

To keep abreast of the handbook, bookmark WITNESS's website, www.witness.org

Verification and Fact Checking

Written by: Craig Silverman

Are verification and fact checking the same thing?

The two terms are often used interchangeably, sometimes causing confusion, but there are key differences.

“Verification is the editorial technique used by journalists — including fact-checkers — to verify the accuracy of a statement,” says Bill Adair, the founder of PolitiFact and currently the Knight Professor of the Practice of Journalism and Public Policy at Duke University.

- **Verification** is a discipline that lies at the heart of journalism, and that is increasingly being practiced and applied by other professions.
- **Fact checking** is a specific application of verification in the world of journalism. In this respect, as Adair notes, verification is a fundamental practice that enables fact checking.

They share DNA in the sense that each is about confirming or debunking information. As these two terms and practices enter more of the conversation around journalism, user-generated content, online investigations, and humanitarian work, it's useful to know where they overlap, and where they diverge.

Fact Checking

Fact checking as a concept and job title took hold in journalism in New York in the 1920s. TIME magazine was at the time a young publication, and its two founders decided they needed a group of staffers to ensure everything gathered by the reporters was accurate.

TIME co-founder Edward Kennedy explained that the job of the fact checker was to identify and then confirm or refute every verifiable fact in a magazine article:

The most important point to remember in checking is that the writer is your natural enemy. He is trying to see how much he can get away with. Remember that when people write letters about mistakes, it is you who will be screeched at. So protect yourself.

Soon The New Yorker had fact checkers, as did Fortune and other magazines. Fact checkers have occasionally been hired by book publishers or authors to vet their material, but it remained largely a job at large American magazines.

The ranks of magazine checkers has thinned since layoffs began in the 1990s. Today, some digital operations including Upworthy and Medium employ staff or freelance fact checkers. But there are fewer working today than in decades past.

In fact, the work of fact-checking has largely moved away from traditional publishing and into the realm of political journalism.

Fact checking took on a new, but related, meaning with the launch of FactCheck.org in 1993. That site's goal is to “monitor the factual accuracy of what is said by major U.S. political players in the form of TV ads, debates, speeches, interviews and news releases.”

INVESTIGADOR_Z

In 2007, it was joined in that mission by PolitiFact. Today, according to a study by the Duke Reporters Lab, there are more than 40 active so-called “fact checking” organizations around the world. They primarily focus on checking the statements of politicians and other public figures.

This is increasingly what people mean today when they talk about fact checking.

Here's how PolitiFact describes its process:

- PolitiFact writers and editors spend considerable time researching and deliberating on our rulings. We always try to get the original statement in its full context rather than an edited form that appeared in news stories. We then divide the statement into individual claims that we check separately.
- When possible, we go to original sources to verify the claims. We look for original government reports rather than news stories. We interview impartial experts.

The above notes that in order for PolitiFact staffers to do their fact checking, they must engage in the work of verification.

Once again, it is the application of verification that enables the act of fact checking.

Verification

In their book, “The Elements of Journalism” Tom Rosenstiel and Bill Kovach write that “The essence of journalism is a discipline of verification.”

That discipline is [described](#) as “a scientific-like approach to getting the facts and also the right facts.”

This is a useful definition of verification. It also helps describe the process applied by fact checkers to do their work. You can't be a fact checker without practicing verification. But verification is practiced by many people who are not fact checkers — or journalists, for that matter.

Verification has come back to the fore of journalism, and taken on new urgency for people such as human rights workers and law enforcement, thanks to the rise of social media and user-generated content.

"Not too long ago, reporters were the guardians of scarce facts delivered at an appointed time to a passive audience," wrote Storyful CEO [Mark Little](#) in an essay for Nieman Reports. "Today we are the managers of an overabundance of information and content, discovered, verified and delivered in partnership with active communities."

That abundance of content, from disparate sources spread all over the world, makes the application of verification more essential than ever before. Social media content is also increasingly important in humanitarian, legal, public safety and human rights work.

Regardless of their goals and role, more and more people are working to verify a tweet, video, photograph, or online claim. Knowing whether something is true or false, or is what it claims to be, enables a range of work and actions.

Creating a Verification Workflow

Written by: Craig Silverman

The Associated Press puts a priority on being first and right. It's part of the culture of the news service.

That dual priority was one of the things that Fergus Bell had to keep in mind when creating AP's workflow for verifying user-generated video.

Bell is the AP's Social Media & UGC Editor, International. He leads efforts to gather and verify UGC video from around the world. Part of that role involves ensuring that AP's existing verification standards are applied to content that doesn't come from its own journalists.

Bell had to create a verification workflow that supported rapid, reliable verification — while also upholding the standards and culture of the AP.

The goals and values of an organization are key to creating a workflow, according to Bell. As are existing processes and resources.

"The most essential thing to consider when working out workflows for verification is to come up with a process that is clear, easily understood in times of pressure and fits the editorial standards of your organization," Bell said. "That way, when something breaks and there is a rush to source content you know that you can trust your process if something isn't right without feeling the pressure from the competition. Part of that process is the communication line and knowing who, in a variety of scenarios, will be the person that gives the final sign off."

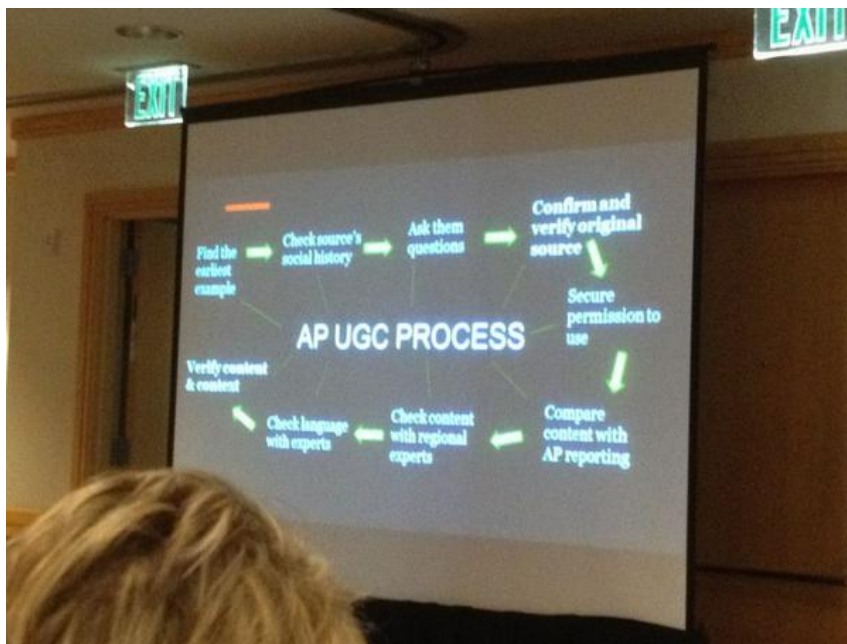
Bell's advice highlights four key elements of a verification workflow:

- Standards and values.
- Tools and people.
- Communication flows/platforms.
- Approval process.

At the core of the AP's process is a "two track" approach, Bell said. "When content is discovered we take the two track approach, verifying and seeking permission from the original source AND separately verifying the content."

This was visualized in [an image shared](#) at a recent Online News association conference:

INVESTIGADOR_Z



"It's a kind of two-line process where they are each done independently of the other," Bell previously said. "... [W]hen I say we confirm a source, that means that we find the original source and we get permission to use it. By content it means that we understand what we're seeing. So I may have verified the source, but I want to confirm myself that what they are telling me is true."

As part of its process, AP makes use of the organization's global resources. Bell and others collaborate to bring as much knowledge and expertise to bear when a piece of content needs to be verified.

"At the AP, the content verification is done by the AP staffer closest to the story in terms of location or expertise — whatever is most relevant," he said. "Once that verification is completed we then submit it to a wider group to check that there are no other issues."

Bell continued:

For example the reason we never ran the purported video of a helicopter going down in Ukraine was because I saw it as part of the screening process and flagged up that I had seen it before somewhere. It wasn't too hard to work out the original was from Syria and the video we were looking at had been edited. Other reasons for this screening could be standards issues, or just generally checking it fits in with our other formats.

AP's social media team possesses deep knowledge of verification tools and procedures. They are a central point of approval before any content is distributed by the organization.

Similarly, the BBC set up a [User-Generated Content Hub](#), which is a team of specialists who are adept at sourcing and verifying UGC. They are the in-house experts. But in neither case does that absolve other journalists from caring about verification, or from taking part in the process.

Larger news organizations, such as the AP and BBC, have the resources to create dedicated, specialized teams. For most other organizations, that's not an option. They must therefore put an emphasis on creating a workflow that is easy enough for everyone to follow, and that is supported by an approvals process that ensures appropriate sign off before publication.

Bell said that in the end what's most important is creating a process that people have confidence in, and that they can easily follow. Otherwise, they will take shortcuts or ignore it. "Even if something is incredibly compelling and it doesn't pass one of our steps, then it doesn't go out," Bell said. "That's how we stop from being wrong, which is

tough sometimes, especially when it's something that's really great. But we just don't put it out, because the [verification] system has grown organically and it hasn't failed us yet, and so we trust it."

INVESTIGADOR_Z

Tracking Back a Text Message: Collaborative Verification with Checkdesk

Written by: [Craig Silverman](#)

During the days of heavy fighting and bombardment in Gaza and Israel in the summer of 2014, this image began to circulate on Twitter and Facebook:



It purported to show a text message that the Israeli Army sent to residents of an area in Gaza, warning them of an imminent attack. Tom Trewinnard, who works for the non-profit Meedan, which is active in the Middle East, saw the image being shared by his contacts.

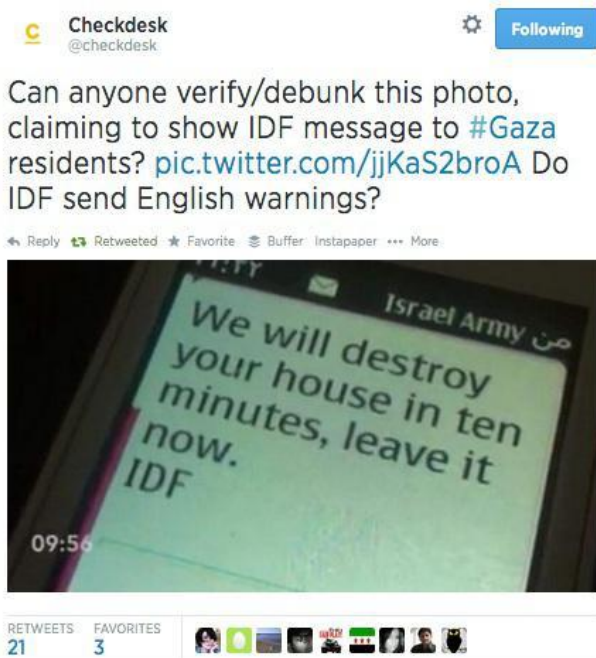
“This was one image that I saw quite a lot of people sharing,” he says. “These were people who I would expect not to share things that they hadn’t checked, or that looked kind of suspicious.”

It seemed suspicious to Trewinnard. A few things raised questions in his mind:

- The message was in English. Would the IDF send an English message to residents of Gaza?
- Language such as “We will destroy your house” seemed too stark, even though Trewinnard said he finds the IDF’s English Twitter account is often very blunt.
- He wondered if someone in Gaza would have “Israel Army” saved as a contact in their phone. That is apparently the case with this person, as evidenced by the contact name in the upper right hand corner.
- The image has a timestamp of 9:56 in the bottom left hand corner. What’s that from?

Trewinnard’s organization is developing Checkdesk, a platform that people and organizations can use to perform collaborative verification. He decided to open a Checkdesk thread to verify the image, and use it to track the verification process for the image in question.

He kicked off the process by sending a tweet from the Checkdesk Twitter account that invited people to help him verify whether this was a real text message:



“The Checkdesk account has less than 300 followers,” Trewinnard said. He didn't expect an onslaught of replies. But a few retweets from people with a lot of followers, including @BrownMoses, inspired others to take action.

The Checkdesk tweet included two specific questions for people to help answer, as well as an invitation for collaboration. Soon, Trewinnard was fielding replies from people who offered their opinion, and, in some cases, useful links.

He was also pointed to an [Instagram account](#) that had shared what appeared to be a real message sent by the IDF to someone in Gaza close to two years earlier:

Trewinnard was able to verify that the Instagram user in question was in Gaza at the time, and that Israel was carrying out an operation in Gaza in that timeframe. He also saw that the same image had been used by the credible 972mag blog.

The above image provided a valuable bit of evidence to compare to the image he was working to verify. It differed in that the above message came in Arabic, and showed that the sender was identified by “IDF,” not “Israel Army.” Trewinnard also said the tone of the message, which warned people to stay away from “ Hamas elements,” was different than the language used in the message they were trying to verify.



INVESTIGADOR_Z



Fanar Haddad
@fanarhaddad



@checkdesk @Brown_Moses Porky pies!
Why would they text in English??? Why
would it b from 'Israel Army' not 'IDF'.
Sounds like BS to me!

Reply Retweet Favorite Buffer More

RETWEET
1

FAVORITE
1



1:39 PM - 21 Jul 2014

This all suggested the image he was working on was not real. But there was still the question of where it came from, and why it had a time stamp in the bottom corner.

Trewinnard said he tried doing a reverse image search on the picture to see where else it had appeared online. But he didn't immediately click through to all of the links that showed where it had appeared on Facebook. Another Twitter user did, and he found a post that showed conclusively where the image had come from:

The Facebook [post](#) includes a video that clearly shows where the text message came from. It was shown in a short film clip that is critical of Israel. The numbers in the bottom left hand corner correspond to a countdown that takes place during the video:

"So there had been these flags ... but this guy found the actual source of the image," Trewinnard said.

He said that the entire process took roughly an hour from his first tweet to the link to the video that confirmed the source of the image.

With an answer in hand, Trewinnard changed the verification status of the image to "False."





Ameer

@7_r



Follow

@checkdesk @Brown_Moses this is the source of this pic:
facebook.com/photo.php?v=85...

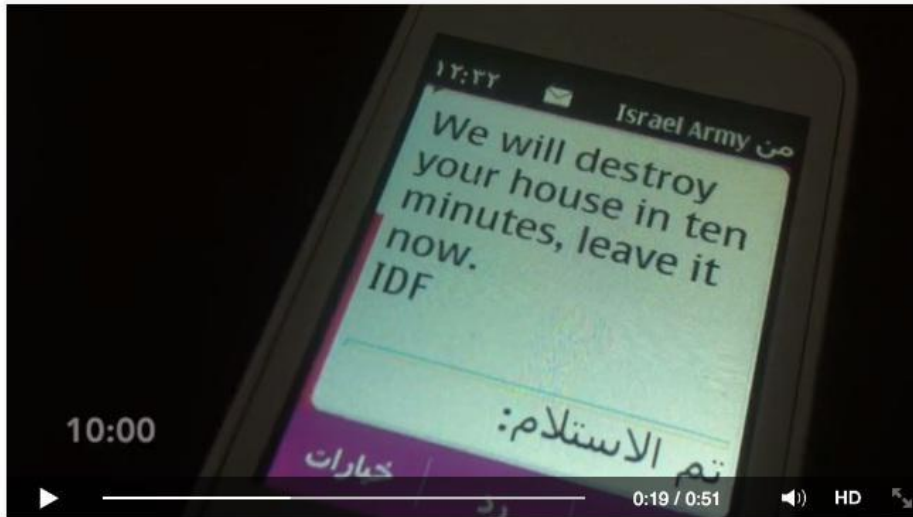
Reply Retweet Favorite Buffer Instapaper More

RETWEETS

3



2:15 PM - 21 Jul 2014



Raya FM

فقط في غزة

See Translation

— with Mina Narmar.

Like · Comment · Share · July 20

Shared with: Public

Embed Post

Report Video

5,829 people like this. Top Comments -

17,572 shares



Write a comment...



Nouha Meftah

لا أحد يمكنه تصور شعور انسان يتلقى رسالة لمعادرة منزله خلال 10 دقائق ليتم تدميره... في تلك اللحظة ستنطق على رناج الذاكرة أجمل اللحظات التي عاشها في بيته ويحمله الحنين الى الضحك الصادقة التي تعالت في أرجائها.. إلى السهرات العائلية التي جمعتهم قبل أن
يف See More...

Like · Reply · 180 · July 20 at 12:09pm · Edited

5 Replies

INVESTIGADOR_Z

The Fake Football Reporter

Written by: Craig Silverman

Samuel Rhodes was a blonde, square-jawed football insider who lit up Twitter with rumors of player transfers and other scoops.

Rhodes tweeted rumors and predictions about what players and managers were up to, and was right often enough to attract over 20,000 followers. His bio described him as a freelance writer for The Daily Telegraph and the Financial Times. His tweets kept the rumors and scoops coming:



One of Rhodes' biggest coups came when he tweeted that Chelsea was going to fire its manager, Roberto Di Matteo, the next day.

He was right.

But things unraveled a few months later. A social media editor at The Daily Telegraph spoke out to say there was no one by the name of Samuel Rhodes writing for them, not now or ever. The FT disclaimed any knowledge or relationship with Rhodes.

Soon, the Twitter account was suspended. Then, in January 2014, the Financial Times revealed that Samuel Rhodes was Sam Gardiner, a teenaged British schoolboy.

"He devised a target of 50,000 Twitter followers and a strategy of propagating rumour," reported the FT.

Gardiner said he created the account, and a previous fake, because he wanted people to listen to his views about football. No one had paid much attention to him when he tweeted as himself.

"My motive wasn't to deliberately mislead people, my motive was to air my opinions on the biggest possible platform, and to flood them around the world," he told BBC Trending radio.

Gardiner's efforts reveal some of the tactics used by Twitter hoax accounts to draw in real people, and to push out rumors and fake information.

Rumor Strategy

One key to the success of the account was that Gardiner played on the insatiable desire for transfer rumors, and for exclusives about which players and managers were being signed or released.

“It was the only way to get big,” Gardiner told the FT. “Everyone has opinions, not everyone has access to the transfer market.”

Offering information that was exclusive and that fed into the desires of people is a common strategy for social media hoaxsters. It's a fast way to gain attention.

He also followed real football journalists on Twitter, and copied them.

“He studied how journalists who are successful on Twitter tweet - a mix of wit, opinion, rumor and statistics, he says - and emulated this. He would tweet at peak times, send out teasers 30 minutes ahead of time and engage with his most high-profile followers,” the BBC reported. xw The FT also noted that “Gardiner interspersed his rumors with genuine tidbits from newspapers to lend his Twitter account more authority.”

This is a common deception tactic. In the world of espionage double agents would intersperse misinformation and deceptions with verifiable (and even mundane) information. Hoax propagators also try to give their falsehoods the trappings of veracity by combining real images and information with fakes.

If Gardiner had only tweeted rumors and scoops, he would have stood out from the other, credible football journalists due to his strange behavior, and the fact that he didn't have any real exclusive information to share. By not only tweeting rumors, he was able to build up credibility, and therefore make his rumors all the more believable.

The Story of Jasmine Tridevil: Getting around Roadblocks to Verification

Written by: Craig Silverman

She went by the name Jasmine Tridevil and claimed to have had a third breast added to her chest as a way to make herself unattractive to men.



That sentence alone includes enough questionable elements to cause journalists and others to treat her claims with great skepticism. But after Tridevil gave a radio interview about her alleged surgery, her story soon went viral, [with some news websites reporting her augmentation as a matter of fact.](#)

As the story spread rapidly on social media, the red flags became even more prominent:

- The only images of her and her new addition came from her own social media accounts and website. She wasn't allowing other people to photograph her.
- She refused to provide the contact information of the doctor who performed the surgery, saying he required that she sign a non-disclosure agreement.
- Plastic surgeons in the United States are bound by an ethical code which holds that "the principal objective of the medical profession is to render services to humanity with full respect for human dignity." Any physician that agreed to add a third breast would likely be in violation of this code.
- The idea of a three-breasted woman was made famous in the film "Total Recall," giving her claim a fictional aspect.
- She claimed to be filming a reality show, with the goal of having it picked up by MTV. If fame was her goal, could she be trusted?
- She was using a pseudonym.

[Snopes](#), the website dedicated to investigating hoaxes and urban legends, pointed out the problems with her story, and the fact that many news sites were parroting it without performing basic checks:

In the initial frenzy of interest in Jasmine Tridevil and her purported third breast, lots of linking and re-posting of the same information and images occurred. However, few looked very deeply at the claims made by the woman shown in the images or her agents, or whether such a modification was even feasible. Instead, multiple media outlets took her claims at face value and ran it as a straight news story with no corroboration (other than self-provided images that could easily have been faked): they contacted no one who knew or had seen Ms. Tridevil, they sought no third-party photographs of her, they didn't verify the story with the doctor who supposedly performed her unusual enhancement surgery, nor did they probe her obvious pseudonym to determine her real name and background.

The lack of independent photos and access to her physician cut off obvious and important avenues for independent verification. When a source throws up so many roadblocks, that alone is reason to question their claims.

In the end, it was Snopes that did the necessary investigation into Tridevil. Along with noting her unwillingness to provide any corroborating evidence, they performed a [Whois](#) search on the domain jasminetridevil.com and discovered it had been registered by Alisha Hessler. Searching for online information about that woman turned up evidence that she looked very much like Tridevil and had worked as a massage therapist in the same city. They also discovered that she had achieved a level of notoriety years earlier:

In December 2013 Hessler made headlines for an incident in which she claimed she was beaten while on the way home from a club, then offered her attacker the choice of standing on a street corner wearing a dunce cap and holding a sign that read "I beat women" rather than being reported to police and charged with a crime. (Hessler also said "she wanted to have the man who beat her sign a waiver allowing her to beat him for 10 minutes.") According to local police, Hessler withdrew her complaint and "stopped returning [their] calls" after she was pressed for details of the alleged attack.

Based on the lack of supporting evidence, Tridevil/Hessler's unwillingness to provide any avenues for verification, and her history as someone who made possible false claims for publicity, Snopes soon declared her claims to be fake. That caused some in the press to begin to question Tridevil's story.

Tridevil, meanwhile, continued to offer ample reason to question her claims. She agreed to an interview with a Tampa TV station but refused to discuss her claim in detail, or to offer proof:

She agreed to the interview on the condition we only discuss her self-produced show she hopes will be picked up by a cable network, and when we asked to see her third breast, she obliged, but with only a quick flash. When asked her why we couldn't have a longer look Tridevil responded, "I'm not ready to do that right now because it's in episode six of my show."

But the smoking gun that proved her to be a fake came a day later. That same Tampa TV station obtained a document from the local airport that had been filled out when Hessler's luggage was stolen weeks before. Among the items listed in the bag was a "3 breast prosthesis":

		<input type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input type="checkbox"/> NO
ITY	13	DESCRIPTION	
	ONE BLACK NYLON ROLLER BAG w/ misc FEMALE CLOTHING, 3 PAIR OF STILETTO HEELS, misc PAPERWORK w/ OWNERS NAME, HAIR BRUSH, 3 BREAST PROSTHESIS		

Though the above document provided the final, irrefutable proof of this hoax, there were many clues and red flags from the very start.

Stolen Batmobile: How to Evaluate the Veracity of a Rumor

On September 12, 2014 [the website BleedingCool.com reported](#) that the Batmobile had been stolen from a film set in Detroit.

At the time of the report, the new Batman v Superman movie was filming in Detroit. So the Batmobile was indeed in town. But had it been stolen? The site's story largely consisted of two paragraphs:

The scuttlebutt from sources in Detroit is that one of the Batmobile models being used in the filming of Batman Vs. Superman has gone missing, believed stolen.

It would not be the first time a Batmobile has been nicked in Detroit. Though that was just a \$200 replica of the TV Series version back in 2010[sic].

The report was based on unnamed "sources," and offered no other evidence to support the claim. The sources were also only identified as being in Detroit.

That didn't stop the claim from spreading to other comics websites, including [CosmicbookNews](#) and [theouthousers.com](#).

The story might have remained an unsourced rumor on a comics websites, but it was soon [picked up by the website of the local CBS station](#):

A [website](#) is reporting that the Batmobile, from the upcoming Batman v. Superman flick, has gone missing in Detroit... and is presumed stolen. If this is true I could only imagine seeing it driving down 696 in rush hour. ...Does this person — if the rumor is true (we don't know how credible the source is) — think that he or she can just go cruising around in this car no one will notice?

Two other local news organizations were aware of the report — but they took a very different approach.

Rather than repeat the unsourced report, The Detroit Free Press assigned reporters to contact people on-set for confirmation, and they also reached out to the police.

At the Detroit News, they also received word about a stolen Batmobile, and they too reached out to the police and the production.

"We wanted to do our own reporting," said Dawn Needham, a digital news editor at The Detroit News. "We saw reports that it had been stolen, but also saw a Tweet that seemed to indicate it might not be true. We called police, tried to contact the production company, followed the string on social media." Within a few hours of the initial report going live at BleedingCool.com, the Free Press published a story about the supposedly stolen Batmobile. Headlined, "Batmobile stolen in Detroit? Good one, joker!" [it debunked the rumor](#).

"Holy Motor City gossip! The rumored theft of the Batmobile in Detroit appears to be a false alarm," it reported.

The story quoted Detroit police spokesman Sgt. Michael Woody saying, "The Batmobile is safe in the Batcave where it belongs."

At the same time other sites had chosen to re-report the claim from BleedingCool.com, the Free Press and News both elected to wait and make calls to sources that could offer a definitive answer. In this case, it was the local police and the film's on-set publicity representatives.

INVESTIGADOR_Z

In cases where information has already been published or is circulating on social media, journalists and others have to decide if they will repeat the rumor, or choose to hold back. In cases where the rumor could cause panic or harm, it's essential to wait and work for confirmation. But what about when the information is of a light-hearted nature, as with a supposedly stolen Batmobile?

The decision making process at the Free Press and Detroit News both involved examining the original source of the rumor in order to judge whether the rumor itself was credible, and therefore worth sharing in the early stages.

It was easy to see why the BleedingCool.com article didn't meet the standard for dissemination:

- The author of the post is based in London, England and did not have a track record for delivering scoops about this film shoot in Detroit.
- The report cited "scuttlebutt from sources in Detroit," but gave no other details of the source of the information.
- There was no evidence to support the claim.
- The site bears this small disclaimer text at the bottom of every page: "Disclaimer: This site is full of news, gossip and rumour. You are invited to use your discretion and intelligence when discerning which is which. BleedingCool.com cannot be held responsible for falling educational standards. Bleeding Cool is neither fair nor balanced, but it is quite fun."

Two newspapers decided to wait and reach out to credible sources. CBS Detroit and others, however, ran with the rumor right away. The CBS story did note that an effort had been made to secure information from the police:

Our brother station WWJ put a call into the Detroit Police Department to see if there is any truth to this. (Update! As of 4 p.m., police were saying they hadn't heard about this, but were looking into it).

That was the last update made on the story. As of today, it still reports the rumor as being possibly true, even though the Free Press story debunking the rumor went online just a few hours later the same day.

"Holy crap, Batman -- look what happened to a a once-distinguished news organization," [noted a post from Detroit news site Deadline Detroit](#).

Russian Bear Attack: Tracking Back the Suspect Origin of a Viral Story

Written by: Craig Silverman

Igor Vorozhbitsyn was on a fishing trip in Northern Russia when he was attacked by a large bear.

Vorozhbitsyn was being mauled and feared for life until the bear was suddenly startled by a noise, causing it to run away. As was later reported by news organizations around the world, the bear ran off when Vorozhbitsyn's phone began to play its ringtone: the song "Baby" by Justin Bieber.

In a line that was echoed by the many websites that ran with the story, MailOnline's [story](#) led with the headline, "Finally, proof that Justin Bieber IS unbearable."

After seeing the story tweeted out by someone on my Twitter timeline, I decided to see if it stood up to scrutiny.

Here's how I eventually discovered that the Justin Bieber ringtone story wasn't what it first appeared.

Step One: Close Reading

The first step was to gather all of the articles I could find in order to examine the facts they reported, and the sources they used. It soon became clear that all the stories about the bear-meets-Bieber tale included the same facts, and these facts were often stated without attribution. Most of the articles pointed to other articles that simply rewrote the story.

Some stories included the same quote from an unnamed "wildlife expert": "Sometimes a sharp shock can stop an angry bear in its tracks and that ringtone would be a very unexpected sound for a bear."

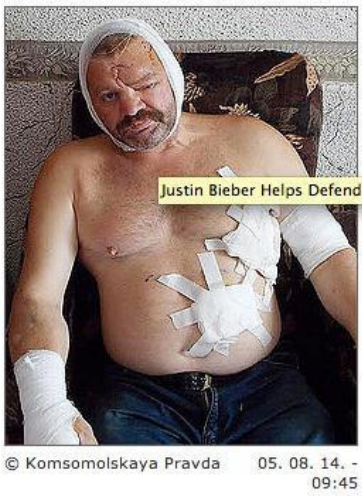
Many articles included the same pictures of the man in bandages. They were often attributed to CEN, the Central European News agency, or to EuroPics, another agency. It was clear that all of the stories were simply rewrites of the same facts, with them all pointing either to MailOnline or a site called the Austrian Times as the source. The photo agency, CEN, was also a potential source, as MailOnline credited it with the images.

Step Two: Identifying and Investigating the Original Source

The Austrian Times' story was published prior to MailOnline's. That meant it appeared to be the first English-language media outlet to carry the story.

The Austrian Times's story repeated all of the same facts as the other stories, but the image it used was different in one important way:

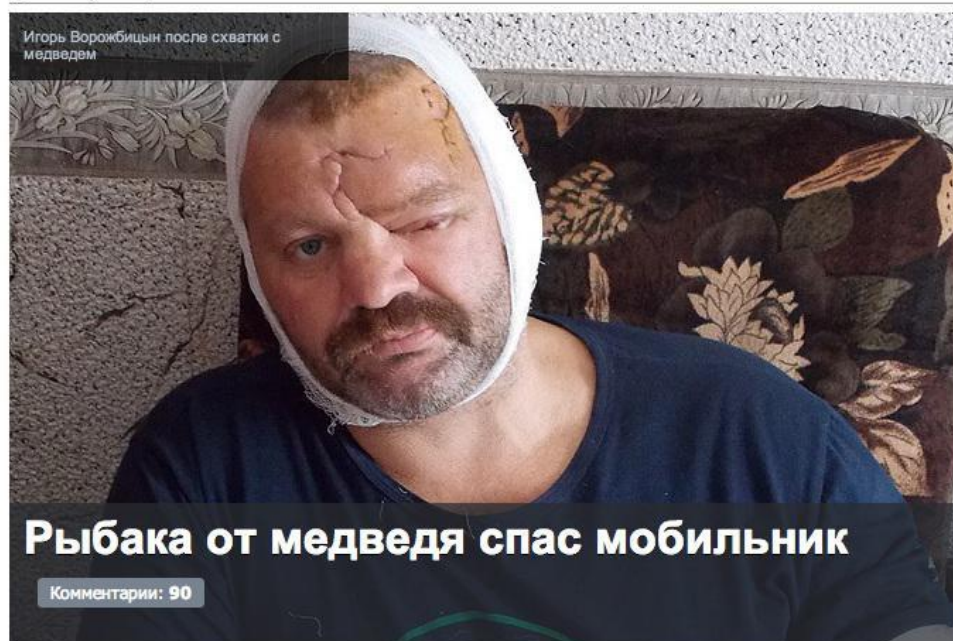
Rather than credit the image to CEN or EuroPics, it cited a Russian publication, Komosomolskaya Pravda. This was the first indication that the story may have originated in a Russian news outlet.



By going to Pravda's website and searching for the fisherman's name, [I discovered the original article about the bear attack](#), which predated the Austrian Times story by over a week:

It featured the photos that had spread everywhere, and a translation of the story also confirmed many of the key facts: the man's name, the location where he was fishing, the bear attack... everything except one key detail. It made no mention of Justin Bieber. Instead, the story reported that the bear was scared off when the man's phone began to recite the current time.

Происшествия | **ЧП**
(31 Июля, 13:30)



Рыбака от медведя спас мобильник

Комментарии: 90

Зверь-людоед, испугавшись сигнала телефона, бросил растерзанную жертву в тайге

Сообщения об участившихся в Якутии нападениях медведей на людей 53-летний житель Нерюнгри Игорь Ворожбицын проигнорировал, мол, за свою жизнь не раз встречался нос к носу с когослапыми и все обходилось. Поэтому как обычно без опаски отправился на рыбалку в соседний Алданский район. От дороги мужчина пошел по ручью, к зимовью, где обычно останавливался на рыбалку. Из оружия только нож на поясе, в руках – удочки, за спиной – рюкзак.

Временами накрапывающий дождь заставил набросить плотный длинный плащ. Через несколько километров вышел на старую автомобильную дорогу. Переобулся, привязал болотники к рюкзаку и пошел в сторону ключа Эвота, к зимовью.

Пройдя в какой-то жутковатой полной тишине метров триста, ясно почувствовал, что

That meant at some point the Justin Bieber reference was inserted. Since it appeared to be the story that set off all the others, The Austrian Times was the place to focus more attention.

Step Three: Digging into The AustrianTimes/CEN/EuroPics

It was time to learn more about the Austrian Times and also about CEN/EuroPics, and where they got the story and the photos.

I called the phone number listed for the Times and asked to speak to the main person listed on their website, but was told he wasn't available. The woman I spoke with said she didn't know the specifics of the Bieber story, but that she would check with their people in Russia. As for their reporting process, she told me:

A lot of stories are found on the wire or in local media but also from local interviews on the ground, or we speak to the reporters who wrote them; we speak to police to get things confirmed.

INVESTIGADOR_Z

That was the last real conversation I had with anyone at the Austrian Times, or at CEN/EuroPics. I soon found that the Times and the two agencies were all owned by the same man, Michael Leidig. The connection between the Times and CEN and its sister agency, EuroPics was found by performing [Whois](#) searches on all of the domains. They all came back to the same parent company and the same man, Leidig.

I called and asked to speak with him, but was told he was away on vacation and out of the country. He also didn't respond to any of my emailed questions.

In the end, there remains no proof of the Justin Bieber connection, and the people who were responsible for spreading it refused to speak or answer questions.

With a bit of work to examine the content of the story, and track it back to the original source, news organizations around the world could have avoided giving exposure to a story that included fabricated material.

Educator's Guide: Types of Online Fakes

Written by **Craig Silverman** and **Rina Tsubaki**

The misinformation and hoaxes that flow over the Internet often fall into specific categories. Understanding what to expect can help you make the right call in a fast moving situation, and avoid giving a hoax new life.

The types of fakes fit into the following categories:

1. Real photos from unrelated events.
2. Art, ads, film and staged scenes.
3. Photoshopped images.
4. Fake accounts.
5. Altered manual retweets.
6. Fake tweets.
7. Fake websites.

1. Real photos from unrelated events

As seen during Hurricane Sandy and the Syrian conflict, images and video from past events are frequently reuploaded and reused on social networks.



JAMIE
@jamster83



Follow

Amazing picture of hurricane #Sandy
decending in New York

Reply Retweet Favorite More



RETWEETS
2,593

FAVORITES
558



11:51 AM - 29 Oct 2012

[Flag media](#)

During Hurricane Sandy, this photo went viral on Twitter. The original photo was published by the Wall Street Journal over a year earlier, on April 28, 2011. But this resharing of the image with a Sandy hashtag quickly attracted retweets and favorites.

Tip: Run a reverse image search to see whether there is an earlier version of the same image online.

Source: <http://verificationhandbook.com/additionalmaterial/types-of-online-fakes.php>



Football Centre
@FootballCentre



Follow

Riots have already started in Brazil. #BRA

Reply Retweet Favorite More



RETWEETS
10,051

FAVORITES
2,109



11:14 PM - 8 Jul 2014

This photo was shared on social networks after the game between Brazil and Germany during the World Cup in 2014. The incident in the photo actually dates back to June 2013, when a number of protests took place ahead of the World Cup. This Reuters photo capturing the scene near the Mineirao Stadium in Belo Horizonte, Brazil that June was reused by @FootballCentre and was retweeted more than 10,000 times.

Tip: Professional photos may be misused in order to report new events. As with the earlier example, a fake can easily be spotted by running a reverse image search.

Source: <http://www.bustle.com/articles/30930-fake-brazil-riot-photos-on-twitter-arent-from-tuesdays-world-cup-loss-to-germany>

Another example is a photo that claimed to show Darren Wilson, the police officer who killed Michael Brown in Ferguson, Mo. in 2014. The photo went viral on Facebook and was shared tens of thousands times. The individual in the photo is not Wilson. It's Jim McNeil, a motocross rider who died in 2011. The photo itself is from 2006, when McNeil was injured after a crash.



INVESTIGADOR_Z

Tip: Identify who and what are captured in the photo and triangulate by comparing different sources, while of course performing a reverse image search.

Source: <http://antiviral.gawker.com/supposed-photo-of-injured-darren-wilson-is-just-some-wh-1630576562>



This photo appeared on Venezuelan state- owned broadcaster VTV's programme "Con El Mazo Dando." It claimed to be proof of weapons being used by General Angel Vivas during the Venezuelan uprising in early 2014.

Interestingly, the same photo was found on the website of a gun store.

Tip: Fakes may be used by the governments and state-owned media outlets to spread their political message and misinform the public.

Source : <http://elpaisperfecto.blogspot.nl/2014/02/montaje-de-diosdado-cabello-24-02-20114.html>



The Daily Mirror used this photo when the Russian Olympic hockey team was defeated by the Finnish team at the Sochi Winter Games in 2014. The photo was originally taken a **few days earlier** during the game between Russia and Slovakia — a game the Russians won.

Tip: It's common practice for some media outlets to use a photo that best describes the story, rather than one from the actual event. It's crucial to question whether images are from the actual event being described, especially on social media.

Source: <https://www.politifact.com/factchecks/2014/feb/19/tweets/photo-showing-sad-/>

When a ferry sank in South Korea, a FOX News report used old footage of the mother of a Mount Everest avalanche victim and portrayed it as being related to the ferry tragedy. The Korean Cultural Centre complained, as did other organizations.



Tip: Images being used to represent an event may reflect older footage, as well as poor sensitivity about races or ethnic groups. Don't assume that the footage has been properly vetted.

Source: <http://www.smh.com.au/world/fox-news-used-images-of-random-sad-asians-in-south-korea-ferry-report-20140507-zr63g.html>

This is another example where a photo from an unrelated event was used in a news story. On 27 May, 2012, the BBC reported about a massacre in Syria and used the above image. It included this description: "This image - which cannot be independently verified - is believed to show the bodies of children in Houla awaiting burial." It was later identified as a photo from Iraq in 2003.

Tip: Pay close attention to photo descriptions that flag it as not having been fully verified.

Source: <http://www.telegraph.co.uk/culture/tvandradio/bbc/9293620/BBC-News-uses-Iraq-photo-to-illustrate-Syrian-massacre.html>

2. Art, ads, movies and staged scenes

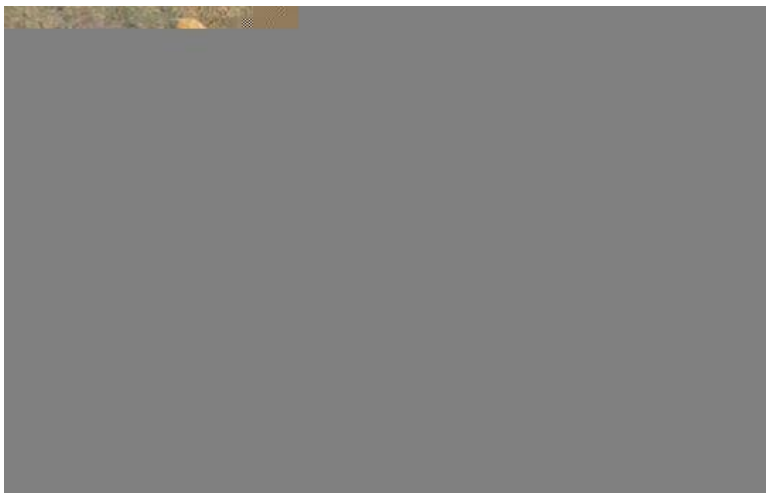
Users on social networks often circulate images taken from art, ads and films during real news events.



This tweet, sent during Hurricane Sandy, is actually a screen capture from an film art project entitled “Flooded McDonald’s,” which can be watched on [Vimeo](#).

Tip: Be cautious of the images that are too good to be true, and seek out reliable sources to aid with confirmation. In this case, contacting local authorities to ask about the flooding situation in Virginia Beach could have provided some necessary context.

Source: <http://www.snopes.com/photos/natural/sandy.asp>



In January 2014, The Daily Bhaskar, a daily newspaper in India, used this photo in an article entitled “Heartbreaking pic: Syrian child sleeps between graves of his parents.” The photo, however, was part of art project by a Saudi Arabia-based photographer, and had been uploaded to Instagram weeks before this happened.

Tip: Media outlets do not necessarily practice verification before sharing an image or other piece of content. It's essential to perform your own verification before republishing.

Source: <http://imediaethics.org/hoax-photo-of-syrian-boy-sleeping-between-parents-graves- was-staged/?new>



This photo was posted across social networks with the hashtag #SaveDonbassPeople. However, it's actually a still from the Russian war film, "The Brest Fortress."

Tip: Check who's spreading the photo. Are they politically active on one side or another, and have they shared other questionable images?

Source: <http://www.stopfake.org/en/snapshot- of-movie-the-brest-fortress-is-being- presented-as-a-photo-of- donbass/>

3. Photoshopped Images



INVESTIGADOR_Z

This photo was released by North Korea's state-owned Korean Central News Agency in March 2013. When The Atlantic examined the hovercrafts, they saw that they were identical to each other. The KCNA had cloned one hovercraft to make the image more threatening.

Tip: Handout images from governments, companies and other sources should be checked and verified.

Source: <http://www.theatlantic.com/photo/2013/03/is-this-north-korean-hovercraft-landing-photo-faked/100480/>



Prior to the Sochi Games in 2014, Quebec's Minister of Higher Education, Research, Science and Technology came under attack after sharing a digitally manipulated photo of two athletes. The original photo did not include Quebec-branded gloves. After sending it, the minister deleted the tweet, adding "The perils of " photoshop " ... I am myself a victim. :)" His press attache also told the media that "He didn't know before he tweeted it that the picture had been photoshopped."

Tip: When influential people share images, they add a layer of credibility and virality to the content. But they too can be victims of fakes.

Source: <http://globalnews.ca/news/1145676/quebec-minister-tweets-photoshopped-olympic-photo/>



The Verification Handbook's [Case 4.2: Verifying Suspicious Sharks](#) During Hurricane Sandy explained how photoshopped shark images circulated during Hurricane Sandy. In fact, street sharks made an appearance even before Sandy. When Hurricane Irene struck in 2011, this tweet went viral, introducing many to the street shark phenomenon. The original photo of the shark is found in an issue of Africa Geographic in 2005.

Tip: Be very wary of shark images shared during hurricanes!

Source: <https://www.imediaethics.org/7-fake-weather-photos-to-watch-out-for-in-the-2014-hurricane-season/>



This example shows how traditional media outlets sometimes publish digitally manipulated photos. The Daily Mail published the image of Tottenham footballer Emmanuel Adebayor saluting the manager after his goal during the match between Tottenham and Sunderland. The print edition included a photo that erased Chris Ramsey, standing next to the manager

INVESTIGADOR_Z

Tip: Professional photos published by media outlets are sometimes (though rarely) altered or manipulated. This is one of the recurring type of fakes that have existed throughout our history. Verification also needs to be applied to non-social media content.

Source: <http://www.theguardian.com/media/greenslade/2014/apr/08/daily-mail-tottenham-hotspur-emmanuel-adebayor>

4. Fake account



Fake accounts are a constant presence on social networks. They are usually set up using the names of celebrities, politicians or other famous people. This unverified account claimed to belong to the son of football player David Beckham and his popstar wife, Victoria Beckham. It was created in 2011 and gathered more than 27,000 followers, in spite of having many characteristics of fake accounts.

Tip: Twitter and Facebook verify accounts of famous/prominent people and organizations. You can spot these because they have a blue tick mark on the profile page. Second guess if there is no blue check mark, and ask them to share the evidence to authenticate the individual.

Source: <https://alexirob.wordpress.com/2013/07/25/the-suspicious-account-of-brooklyn-beckham-brookbecks/>



When Pope Francis I was appointed in 2013, a fake account, @JMBergoglio, tweeted "Immensely happy to be the new Pope, Francis I." Many people, including journalists, were fooled by this account, helping propel it to 100,000 followers within a few hours. However, a quick look at the account's previous tweets reveals many questionable messages. This includes the above message which translates to, "If I'm the new pope, children will love me more than Santa Claus".

Tip: Check previous tweets to see if they are consistent with the person.

Source: <http://mashable.com/2013/03/13/new-pope-fake-twitter/>



This Morrissey Twitter account is a unique example because it's a case where Twitter itself wrongly verified a fake account.

Tip: While this is a rare case, this example shows that even a verified check cannot be treated as 100 percent reliable. Also remember that Twitter accounts can be hacked. In those cases, it's not the real person tweeting.

Source: <http://www.theverge.com/2014/5/19/5730542/morrissey-impersonated-on-twitter>

5. Manual retweets



In 2009 Twitter introduced a retweet button that allows people to retweet the original tweet on their feed. However, many users still manually retweet by copy- pasting the original tweet with RT at the beginning. This opens up the possibility that people will alter the original message and attribute it to other users. It also means that previously deleted messages can live on as manual retweets, thereby spreading misinformation.

Tip: Check if you can find the original tweet.

6. Fake tweet, facebook wall posts and iPhone conversations

There are a number of tools and apps that allow people to easily create a fake tweets, Facebook wall posts and iPhone conversations. Here's a look at some of the ones to watch out for.

- The Wall Machine (<http://thewallmachine.com/>):

INVESTIGADOR_Z

This tool can be used to create fake Facebook wall posts. After signing in with your Facebook account, you can create a profile photo, account name and comments on your imaginary post. A similar tool is from Simulator.com, where you can create a fake Facebook post and download the JPG file from the site. See an example below.



- Lemme Tweet That For You (<http://lemmetweetthatforyou.com>):

This tool is used to fabricate an embeddable and sharable fake tweet with a customizable username, body text, and number of RTs and favorites. Simulator.com also has a tool to create a fake tweet and download it as a JPG image file.



- FakePhoneText (<http://www.fakephonetext.com/>):

This tool is used to create and download a image of fake iPhone message conversation. You can set the name and content of the messages, as well also the cell network, time, type of connection (i.e. 3G, WIFI) and battery status. There is also another text message generator called [iOS7 Text](http://iOS7Text.com).

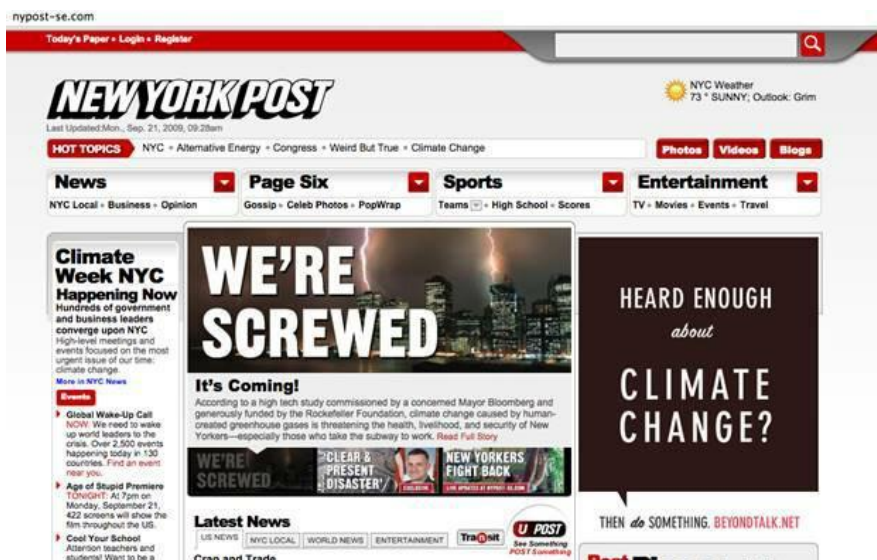


7. Fake websites

It may look real, but this wasn't the authentic New York Post website. It was created to raise awareness about climate change. It's relatively easy to copy a website and set it up on a different web address — and to fool people in the process. That was what Wikileaks did when it set up a fake copy of The New York Times' website in order to promote an equally fake op-ed by columnist Bill Keller:

The differences were subtle, and even some New York Times journalists were fooled.

Tip: Check the URL, and search on different search engines to see if the URL matches with the top hits for that property. If unsure about a URL, perform a Whois search to see who owns the domain, and when it was first registered.



INVESTIGADOR_Z

The New York Times

The Opinion Pages

Search Opinion

THE NEW YORK TIMES

WORLD U.S. N.Y. REGION BUSINESS TECHNOLOGY SCIENCE HEALTH SPORTS OPINION ARTS STYLE TRAVEL JOBS REAL ESTATE AUTOS

Open & use a Webster checking account and get up to \$100.

Learn More

WebsterBank

Advertise on NYTimes.com

OP-ED COLUMNIST

WikiLeaks, A Post Postscript

By BILL KELLER

Published: July 29, 2012

Twitter

AS rumors build about the potential financial blockade against the New York Times by Visa, Mastercard, and American Express for hosting U.S. government cables published by WikiLeaks, I find myself in the awkward position of having to defend WikiLeaks. During the [House Judiciary Subcommittee hearing](#) on July 11th, several Republicans made it clear they also want New York Times journalists charged under the Espionage Act for their recent stories on President Obama's 'Kill List' and secret US cyber attacks against Iran.

FACEBOOK

TWITTER

GOOGLE+

E-MAIL

SHARE

PRINT

SINGLE PAGE

REPRINTS

SESSIONS



Tony Danza/The New York Times

As those of you who have followed my turbulent relationship with WikiLeaks and its Ono-In-Chief Julian Assange know, I am first in line when it comes to distancing myself from his brand of transparency without government checks and balances. You don't have to embrace Assange as a kindred spirit to believe that what he did in publishing those cables falls under the protection of the First Amendment. The backroom pressures by the Obama Administration's State Department to expand its financial blockade targeting WikiLeaks to include news organizations that host information from their trove of pilfered documents goes too far.

Ads by Google

1.65% APY Interest Rate
With a Rockwell Direct Money Market Account. Open an Account Online.
www.rockwelldirect.com

Get A Visa Credit Card
No Annual Fee. Use Visa & Cash Back. Compare Credit Cards & Apply Now.
www.CreditCardGuide.com

Consultant IT Consulting
Small Business Network Consultants. Reliable Service. Request a Quote.
www.kyb-ent.com

Advertise on NYTimes.com

MOST E-MAILED **RECOMMENDED FOR YOU**

We don't have any personalized recommendations for you at this time. Please try again later.

Log in to discover more stories based on what you've read.

Log In Register Now Log In

PRINT This | MAIL | Share

