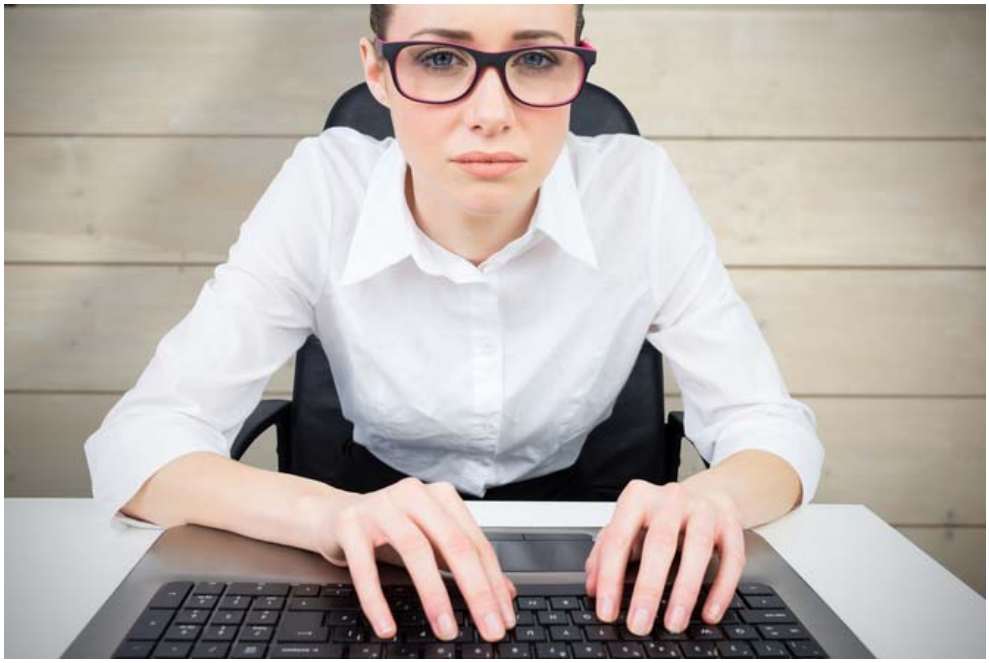
THE CONVERSATION

Six easy ways to tell if that viral story is a hoax

September 18, 2015 9.26am EDT

Pete Brown
Research Fellow, University of Oxford



Pull the other one. from www.shutterstock.com

"And so it begins … ISIS flag among refugees in Germany fighting the police," blared the headline on the Conservative Post; "with this new leaked picture, everything seems confirmed". The image in question purported to show a group of Syrian refugees holding ISIS flags and attacking German police officers.

For those resistant to accepting refugees into Europe, this story was a godsend. The photo quickly spread across social media, propelled by far-right groups such as the English Defence League and Pegida UK. At the time of writing, the page claims to have been shared over 300,000 times.

The problem is, the photo is three years old, and has precious little to do with the refugee crisis. In fact, it seems to be from a confrontation between members of the far-right Pro NRW party and muslim counter-protesters, which took place in Bonn, back in 2012. A number of news outlets tried to highlight the hoax, including Vice, the Independent and the Mirror, as did numerous Twitter users.

The Independent
@Independent

Follow

You've probably seen that picture of a refugee holding an Isis flag. It's a complete lie ind.pn/1ida9Xa

3:17 AM - 15 Sep 2015

480 149

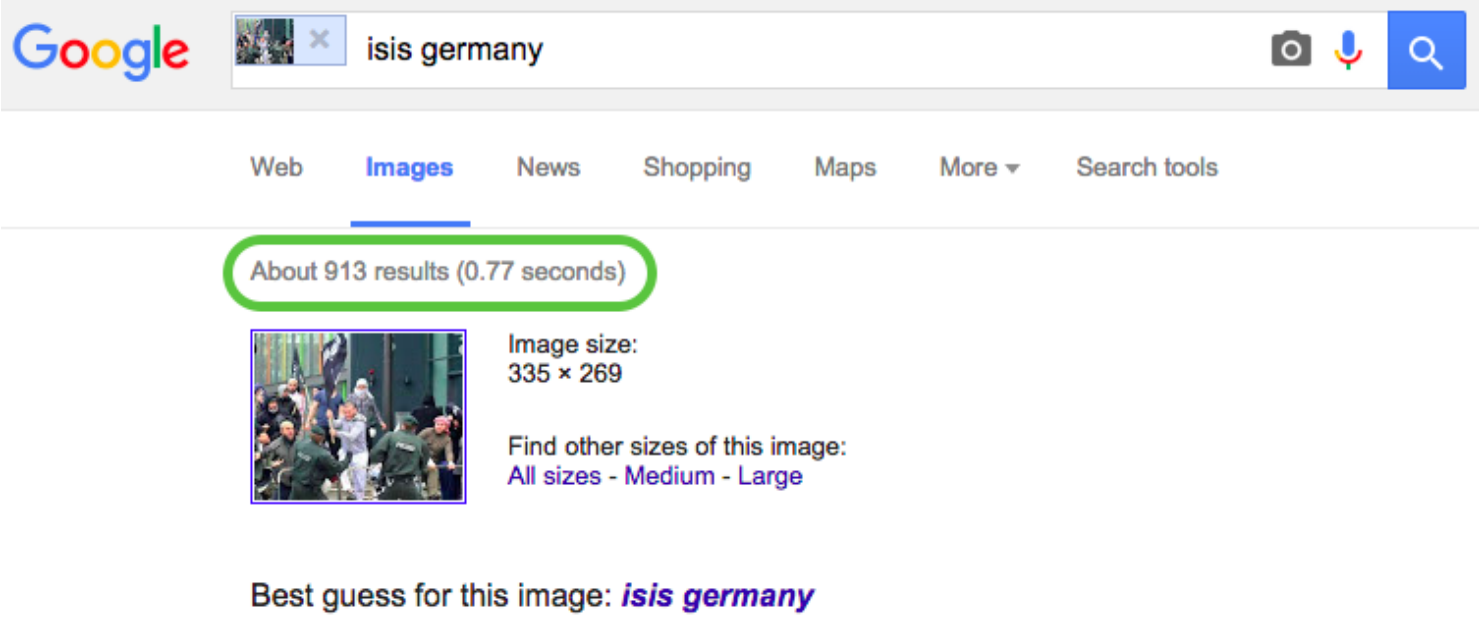
But news in the digital age spreads faster than ever, and so do lies and hoaxes. Just like retractions and corrections in newspapers, online rebuttals often make rather less of a splash than the original misinformation. As I have argued elsewhere, digital verification skills are essential for today's journalists, and academic institutions are starting to provide the necessary training.

But ordinary people are also starting to take a more sophisticated approach to the content they view online. It's no longer enough to read the news – now, we want to understand the processes behind it. Fortunately, there are a few relatively effective verification techniques, which do not require specialist knowledge or costly software. Outlined below are six free, simple tools that any curious news reader can use to verify digital media.

Reverse image search

Not only is a reverse image search one of the simplest verification tools, it's also the one that showed the "leaked" ISIS refugee photo was a fake. Both of the most popular services, Google Images and TinEye, found pages containing this image dating back to mid-2012. As the screenshot below shows, the "ISIS refugee" story could be debunked in less than a second.

When a link to the story was posted to Reddit, sceptical users swiftly took to Google to query it. Soon, one reported back: "Google Image Search says the photo is from 2012".



YouTube DataViewer

When watching the latest viral video on YouTube, it's important to be on the look-out for "scrapes": a scrape is an old video, which has been downloaded from YouTube and re-uploaded by someone who fraudulently claims to be the original eyewitness, or asserts that the video depicts a new event.

Amnesty International has a simple but incredibly useful tool called YouTube DataViewer. Once you've entered the video's URL, this tool will extract the clip's upload time and all associated thumbnail images. This information – which isn't readily accessible via YouTube itself – enables you to launch a two-pronged verification search.

If multiple versions of the same video are hosted on YouTube, the date enables you to identify the earliest upload. This is most likely to be the original. The thumbnails can also be used in a reverse image search to find web pages containing the video, offering a quick and powerful method for identifying older versions or uses of the same video.

Jeffrey's Exif Viewer

Photos, videos and audio taken with digital cameras and smartphones contain Exchangeable Image File (EXIF) information: this is vital metadata about the make of the camera used, and the date, time and location the media was created. This information can be very useful if you're suspicious of the creator's account of the content's origins. In such situations, EXIF readers such as Jeffrey's Exif Viewer allow you upload or enter the URL of an image and view its metadata.

Below is the EXIF data of a photograph I took of a bus crash in Poole in August 2014. It's very comprehensive; had I claimed the photo was taken, say, last week in Swanage, it would be very simple to disprove. It is worth noting that while Facebook, Instagram and Twitter remove EXIF data when content is uploaded to their servers, media shared via platforms such as Flickr and WhatsApp still contain it.

Basic Image Information

Target file: IMG_0150.JPG

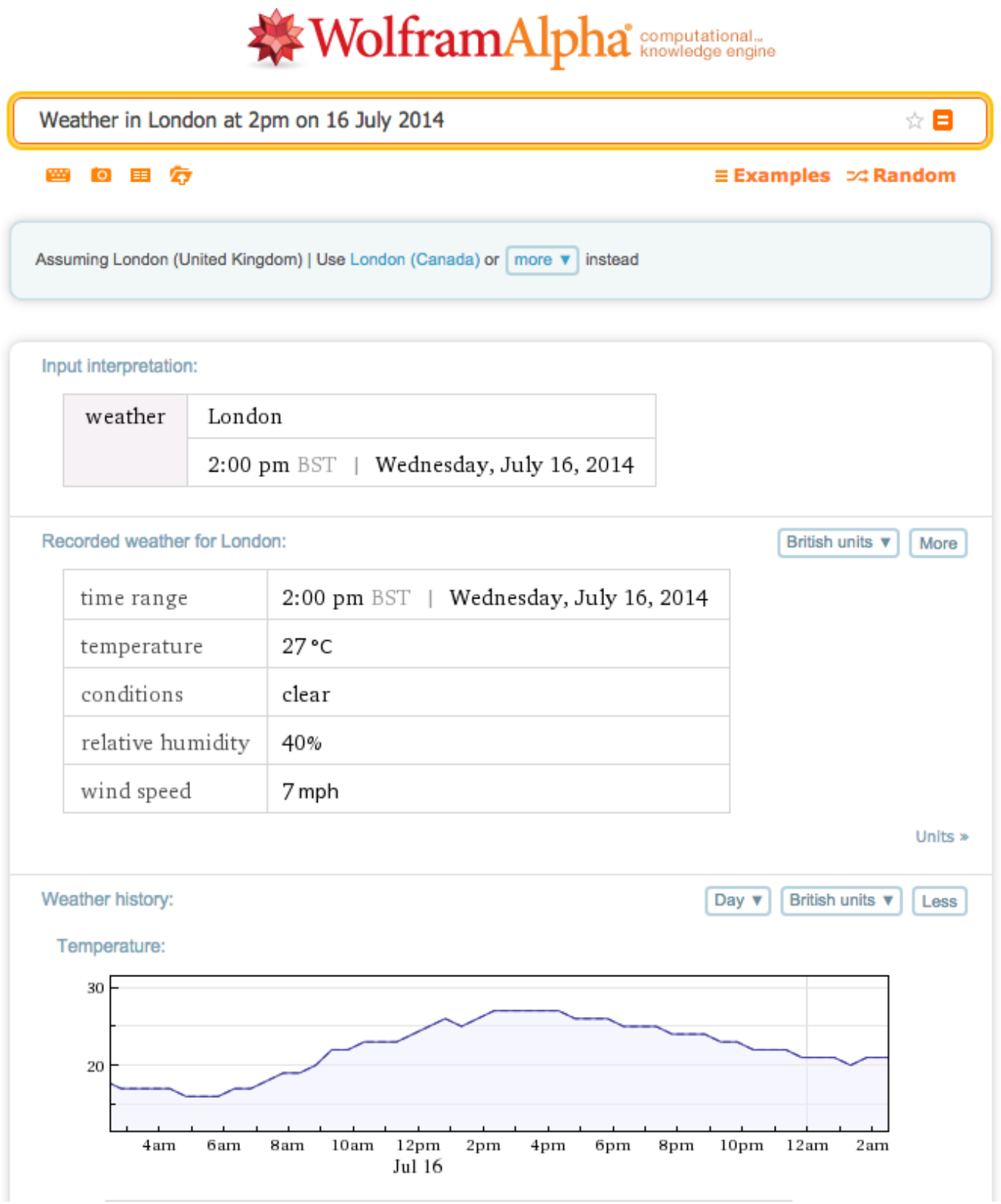
Camera:	Apple iPhone 4S
Lens:	iPhone 4S back camera 4.28mm f/2.4 Shot at 4.3 mm
Exposure:	Auto exposure, Program AE, 1/132 sec, f/2.4, ISO 50
Flash:	Auto, Did not fire
Date:	**August 29, 2014** 12:40:20PM (timezone not specified) (1 year, 18 days, 20 hours, 21 minutes, 27 seconds ago, assuming image timezone of US Pacific)
Location:	Latitude/longitude: **50°** 41' 9.2" North, **1°** 56' 33.8" West (50.685875, -1.942717) Location guessed from coordinates: *40 Banks Rd, Poole, Poole BH13, UK* Map via embedded coordinates at: Google, Yahoo, WikiMapia, OpenStreetMap, Bing (also see the Google Maps pane below) Altitude: 11 meters (36 feet) Camera Pointing: Northeast
File:	**3,264 × 2,448** JPEG (**8.0** megapixels) 2,971,193 bytes (2.8 megabytes)
Color Encoding:	**WARNING:** Color space tagged as sRGB, without an embedded color profile. **Windows and Mac browsers and apps treat the colors randomly.** Images for the web are most widely viewable when in the sRGB color space and with an embedded color profile. See my Introduction to Digital-Image Color Spaces for more information.

FotoForensics

FotoForensics is a tool that uses error level analysis (ELA) to identify parts of an image that may have been modified or “photoshopped”. This tool allows you to either upload, or enter the URL of a suspicious image and will then highlight areas where disparities in quality suggest alterations may have been made. It also provides a number of sharing options, which are useful for challenging the recirculation of inaccurate information, because they allow you to provide a direct link to your FotoForensics analysis page.

WolframAlpha

WolframAlpha is a “computational knowledge engine”, which allows you to check weather conditions in at a specific time and place. You can search it using criteria such as “weather in London at 2pm on 16 July, 2014”. So if, for example, a photo of a freak snowstorm has been shared to your timeline, and WolframAlpha reports that it was 27 degrees and clear when the photo was purportedly taken, then alarm bells ought to be ringing.



Online maps

Identifying the location of a suspicious photo or video is a crucial part of the verification process. Google Street View, Google Earth (a source of historical satellite images) and Wikimapia (a crowd-sourced version of Google Maps, featuring additional information) are all excellent tools for undertaking this kind of detective work.

You should identify whether there are any reference points to compare, check whether distinctive landmarks match up and see if the landscape is the same. These three criteria are

frequently used to cross-reference videos or photos, in order to verify whether or not they were indeed shot in the location the uploader claims.

Google Earth, in particular, has been put to incredible use use by Elliot Higgins AKA Brown Moses, of Bellingcat – a site for investigative citizen journalism.

Internet
Journalism
News
Going viral