## Essay

Peter Welchering

# The problem with pictures

## Source analysis and fact-checking in a time of war

*Abstract:* In a hybrid war, photos and especially videos become a weapon in themselves – used to secure air supremacy over (digital) discussions and cause people to assume and think the 'right' thing. To achieve this, image material is mercilessly falsified. That is nothing new: Stalin did it, and now Putin is too. Day in, day out, we journalists receive images from combat zones in Ukraine, without knowing whether they are authentic or have been manipulated. It is our job to find out, conducting analysis that takes both time and basic knowledge of image forensics. There are many testing tools and platforms for this. But many of those working in journalism are unsure about what exactly these tools look at and how to interpret the findings they produce. This situation has changed little since the row over the analysis of satellite images from the Russian Defense Ministry by the British platform Bellingcat in summer 2015 (cf. Higgins 2021: 90-141). At a press conference on July 21, 2014, the Russian Defense Ministry showed two satellite photos as evidence that Malaysia Airlines flight MH17 was shot down by Ukrainian rocket launchers on July 17, 2014. Having conducted forensic examination of these photos, the Bellingcat analysts were able to prove that they had been manipulated (cf. Welchering 2015b). This debate arose in part because some journalists had misjudged the significance of the Bellingcat analysis. That is why a basic knowledge of source analysis and image forensics methods is so important. Image forensics and source analysis cannot convict war criminals – but they can be used to research initial indications of when and where a crime was committed. And it is vital that people are warned against the error of relying solely on a reverse image search to detect manipulation of videos and photos. This paper examines these problem areas, as well as the urgent need to incorporate these research methods into journalistic training at all levels.

On April 3, 2022, many editorial offices and image forensics experts, including in Germany, found themselves working on a Sunday. Media in Germany had received a video from Bucha, a small town just outside Kyiv that had been occupied by Russian forces a few weeks earlier. The video showed dead bodies in the streets.

The troops had taken over the town in late February and left again in late March. The video showed people who had been shot, their hands tied behind their backs. Ukrainian forces had filmed the images while on patrol in Bucha.

They accused the Russian soldiers of having committed war crimes there. The Kremlin denied the allegations, claiming first that the images were fake, and later that they were staged.

The video shows dead people. But a video like this cannot tell us who killed them. It is one person's word against another. The Ukrainian government blames Russian troops; the Kremlin blames Ukrainian troops. But first things first: On April 3, the question is, is the video real or fake?

Answering this question usually means checks on three levels. The first is to search for other videos or photos online that show the same scene – in this case, the bodies on the streets of Bucha.

The second stage is a plausibility check. Does the weather seen on the video match the weather conditions in the alleged location at the time the video was filmed (as seen in the metadata)? Weather documentation platforms like https://www.wunderground.com/history and the search engine https://www.wolframalpha.com/ can help here. An analysis of the sun's position and the way the shade falls can help to home in on the time of recording, and can be conducted very easily with tools such as www.suncalc.org, www.Findmyshadow.com and www.shadowcalculator.eu.

The third stage is more detailed. It involves looking at the clothing, including the uniforms, seen in the images. Are there any special features? Do these uniforms match the usual uniforms or work clothes? The vehicles seen in the images are identified. In the case of military vehicles, the vehicle types seen are compared with official information from the Defense Ministry in question.

Talking to military advisors and researching on blogs on military topics are also useful approaches. Where videos have sound, language comparison and analysis are important. Translators are essential here. Simply working with transcription and translation programs is not enough – these services can be useful for a first impression, but no more than that.

Journalists conducting research in this field receive an enormous amount of support from private individuals, who film videos, take photos, and are available to answer questions. This enables German journalists to ask very specific questions on the orientation of satellite images and maps of the area generated from

them, without leaving the comfort of their desks. Often, this even allows the two-source principle to be applied.[1]

In some cases, research inquiries like this on the ground have succeeded in correcting exaggerations or incorrect information from the Ukrainian authorities. In others, additional image material could be obtained directly from people in the combat area (cf. Stahnke 2022). Needless to say, all principles of informant protection need to be adhered to when processing and using this material. Military authorities on both sides try to prevent photos and videos that are unfavorable to them from getting into the hands of independent journalists in the West (cf. Welchering/Kloiber 2017).

## Who betrayed us? Metadata!

Where material from sources like this is to be published, it is a good idea to »grab« the video in question, i.e. effectively to re-record it on your own computer so that security authorities and activist groups can only find the metadata of the media house publishing it, not the original data. Of course, it is important to be transparent about this informant protection measure.

After all, if not, a metadata analysis would lead to incorrect conclusions. A metadata analysis is usually used to determine data such as the time of recording, an approximate time of processing, the camera type used, and sometimes even the aperture chosen. Tools for this are provided by fotoforensics.com, the image verification assistant mever.iti.gr/forensics, metadata2go.com, and Jeffrey's Exif Viewer at exif.regex.info.

Of course, this metadata can only be used for source analysis if it is taken directly from the original file. This is not always the case – a fact that can easily be overlooked by editorial offices who examine files too fleetingly.[2]

If the metadata passes the plausibility tests, this is often enough for the image or video to be approved for use in reporting. When doubts remain, image forensics is the next step. With journalistic fact checkers often out of their depth here, it is a good idea to consult professional image forensics experts, whose role is to check for features such as picture noise and color defects in the material. Other aspects examined include typical interpolation patterns in the colors, block artefacts caused by compression, and image defects, especially in the lighting.

---

1   It is important to include sufficient informant protection measures at the planning stage. For example, I conduct video conferences with informants on the ground in well-secured conference rooms provided by the company Visavid. Confidential information is exchanged in encrypted internet relay chats via the Tor network.
2   Examining image material using a hexadecimal editor can be extremely enlightening, revealing file structures and often even the conditions under which the image was created.

This leads to a specific noise component in the photographic image. This noise component is relatively stable across multiple images from a specific cell phone or DSLR camera, but varies from model to model. Today, there are even reference noise patterns for the various camera models, which can be compared with the noise signal of the photo being examined.

This allows researchers not only to check which camera model was used to take the photo, but also whether there are deviations in the noise component caused by image editing programs like Photoshop. A color examination further underpins the method.

The sensors of a digital camera only measure brightness; it is the color filter field that gives the video its color. The color values are calculated from brightness and temperature values – a process known in the trade as interpolation. The pattern of brightness and color temperature values can provide indications of subsequent processing.

## Additional material as a second source

There were other videos from Bucha, distributed on various channels of the messenger service Telegram. According to information from the Ukrainian Ministry of Defense, the location in which the images were taken was also quickly confirmed through a combination of geolocalization services and consulting and comparing the relevant material from Google Maps.

All cases of video material examined here, from Bucha on April 3, are of Yablunska Street in Bucha. The weather visible in the video taken by the Ukrainian patrol – it is raining – matches that reported by the weather services. The video originated from April 1, as confirmed by the metadata analysis.

The video was uncut, and no pixels had been moved or added. The brightness and color temperature values were consistent. There was therefore no indication that the video was fake.

Image analysis like this cannot uncover who committed the crimes. That is ultimately the job of investigators on the ground. However, matching video images with satellite data can provide evidence of the time of the crime, or at least a possible time corridor.

This was also the approach taken by colleagues from the New York Times (cf. Browne et al. 2022), who viewed images from the satellite company Maxar, taken of Bucha on February 28 and March 19, 2022. On the images from February 28, the streets are clear. On March 19, corpses can be seen. That means that the bodies were already on the street by March 19, but were not yet there on February 28.

This allows the conclusion to be drawn that the bodies arrived on Yablunska Street during the Russian occupation and not, as the Russian Defense Ministry argued, after Russian troops left on March 30, 2022.

The New York Times journalists then compared the satellite images directly with the video images in order to find out whether the bodies seen on Maxar's satellite images are the same ones seen on the video taken by the Ukrainian patrol on April 1.

This is done with two screens or a split screen. In this case, the video images are on the left-hand side of the screen, and the satellite photos on the right. The video is taken from a vehicle moving along the road, with bodies seen to the left and right.

The locations in which these bodies were found were then compared with the bodies seen on the satellite images, based on the positions of buildings, cars and other wreckage. All the bodies on the satellite images could be matched to those on the videos.

However, the videos show more bodies than are seen on the satellite images. And of course, the videos show more gruesome details, such as corpses with their hands tied, burned body parts, and people who have been shot in the head.

Most satellite companies provide images with a resolution of more than ten centimeters. Only military satellites can manage a resolution of less than four centimeters. Video images taken on the ground of course provide many more details for analysis.

## Even satellite images can lie

Needless to say, the satellite images also need to be checked for authenticity. Satellite material provided by governments must always be seen as problematic and subjected to plausibility tests accordingly. Raw material purchased directly from commercial service providers is considered much more trustworthy.

In connection with the events in Bucha, Russian authorities published videos intended to suggest that the patrol was staged with actors and the people seen in the video were not dead at all.

In one video, it was claimed, a body lying at the side of the road stood up once the patrol had passed by. In other words, it was not a dead body, but a living person. Closer inspection showed that the wing mirror of the vehicle had been filmed, i.e. the person at the side of the road was seen in the wing mirror.

In recording these images, the camera scanned from left to right and back again repeatedly. This created the impression that the person's clothing, at least, moved slightly. But this is an optical illusion created by the multiple scanning motions.

A second video, the Russians claim, shows a body lying at the side of the road waving to the vehicle as it passes by. However, examining the video frame by frame, video by video, does not reveal this. What it does reveal is a dot on the windscreen, probably a raindrop.

These manipulated videos are of course not suitable as evidence – yet all sides still continue to use material that has been manipulated like this. When manipulation is uncovered, the reaction is often extremely robust, with source analysts and fact checkers often having to swallow a great deal of abuse and even threats.[3]

Generally speaking, using methods of source analysis and image forensics to examine material from war zones fulfills two purposes. Firstly, it makes it possible to clarify whether or not the video material is fake. If not, a team of investigators must be sent to the location, as something that needs clarification really has happened. Secondly, comparing satellite images with videos filmed on the ground allows rough time corridors to be determined in which the alleged war crimes were committed. However, it is important to remember that these findings are of limited scope.

## Time pressure is the enemy of analysis

Despite this, readers and viewers often expect much more. Journalists need the courage to put their analyses into context and be precise in outlining the range of evidence. Unfortunately, they do not always succeed. In some cases, this may be because methods of source analysis and image forensics for research are not sufficiently taught in journalistic training at any level.

Bild-TV recently delivered a typical example of failure to conduct sufficient analysis in advance. On February 24, at the start of the Russian attack on Ukraine, the broadcaster showed old images, including of a deployment of paratroopers, in its reporting on Russian attacks. The image material was actually of a military exercise from 2014 and did not show any hostile action against Ukraine.

Bild-TV corrected its error. However, its reporting was criticized on social media as »Western fake news,« with the journalists involved accused of deliberately propagating false information.

---

3   I have often been asked in recent weeks whether working on fact checking like this puts a great strain on me, or is perhaps even damaging in the long term. I have always responded with three relevant aspects: It is very important to talk to colleagues about the things with which one is confronted in this work. Just as important is taking time to reflect on what this journalistic work is doing to you at the moment. Thirdly, an occasional supervision is a good idea. Personal protection is also often enough to give a sense of security.

In cases like this, people often do not even make the effort to look at the meta-data available on the video files. Arguments are fired out under enormous time pressure. Yet the fundamental causes of this kind of error often lie somewhere else entirely.

The first step is often a failure to provide sufficient research training to train-ees, with many of those responsible for providing training at media houses no longer seeing research on the ground as important. Even many of the extremely numerous journalism courses at universities pay little heed to methods of source analysis and image forensics. It is easy to get the impression that the majority believes reverse image searching to make these research methods unnecessary.[4]

## More training needed

This discussion has been bubbling away at all levels of journalistic training for more than 20 years now. Initially, it was solely about the training time and costs that would have to be spent on teaching appropriately substantial research expertise. But it soon expanded.

As it became clear that research skills on the ground were increasingly being lost, replaced by the so-called »investigative« units set up in many media houses, speakers at various conferences and events on journalistic training began to argue that methods of source analysis and image forensics should only be used within these departments (cf. Welchering 2021).

These departments, however, were happy with the very one-sided approach to reverse image searching taught by Google Fellows. After all, it was cheaper than a comprehensive analysis, bringing in external image forensics experts, or train-ing your own staff in this field.

When conducting reverse image searching for the current war in Ukraine in particular, it would have been very useful to use not just the search machines usually chosen – such as Google and tineye.com – but also the Russian search engine Yandex.com. Yet since so many editorial offices offer little more training than a brief introduction to Google's search engine, journalists are often simply not aware of the other search engines and the tools they offer.

The war in Ukraine has triggered a level of hype in Germany about analyzing images and videos. Yet this hype should not mask the fact that many people simple do not possess fundamental skills and expertise in source criticism and image forensics.

---

4   Patrik Baab draws attention to this, highlighting the insufficiencies of this kind of Google search: »Another major barrier to research, however, is the hidden and untransparent influence of programmed algorithms on the public communication and journalistic search process. After all, the data is edited by the search algorithms, resulting in a modifiable selection« (Baab 2022: 211).).

It is therefore no wonder that it was journalists from the *New York Times* who conducted and published the revealing comparison of video material with satellite images on the events in Bucha. Only then was this source analysis method also discussed in German media.

## A long tradition of false flag videos

Colleagues from the *Neue Zürcher Zeitung* (NZZ) were also quick to report on ›false flag‹ videos, published by the Russians on various online platforms even before the attack on Ukraine on February 24, 2022. The videos claimed to show attacks by Ukraine on Russia (cf. Jacot-Descombes 2022, Zellweger 2022). History tells us that this kind of narrative about attacks can easily be used to justify a war.

Various videos show Ukrainian soldiers in armored vehicles moving into Russian territory, with claims that this frontier violation took place close to Luhansk.

By comparing the plants, tank barriers, and buildings seen in the video with satellite images, fact checkers from Bellingcat were able to confirm that the images were filmed close to Luhansk – but in the pro-Russian separatist area, not on Russian territory.

In other videos, the armored vehicles can be seen in more detail, making it easy to recognize the precise model – one that cannot be found in the Ukrainian military inventory. There must therefore be significant doubt as to whether the Ukrainian army even owns or has ever driven this kind of vehicle. That would indicate that the images were staged.

The NZZ researchers hold up another video as an example: Shown on a pro-Russian Telegram channel on February 18, 2022, it claims to show how apparently Polish-speaking saboteurs tried to blow up a chlorine tank in the Donbas region on that day.

When investigating the video's metadata, the researchers came across embedded audio files from a YouTube video from 2010, in which the sound of explosions is heard. These audio files with explosions in the background had been copied into the video from February 18, 2022. The metadata also showed that the video was filmed on February 8, 2022 – ten days before the sabotage was alleged to have occurred.

We in Germany often find this kind of research difficult. One of the reasons undoubtedly lies in the way we train journalists.[5] An example: The basic

---

5   As much as I criticize the situation in journalistic training here, there are of course also developments that give cause for optimism. Examples include the regular monthly research meeting held by the Wissenschaftspressekonferenz since summer 2020, and the hybrid seminar series on research at the Journalisten-Akademie in Munich. For transparency, it should be noted that I am involved in both projects.

seminars for trainees and lateral entrants at newspapers offered by the Journalisten-Akademie Stuttgart began teaching methods of image forensics and source analysis in 2010, investing a great deal of time in the topic. Of course, there were repeated calls to reduce this, in order to spend more time on topics like search engine optimization (cf. Welchering 2015a). For eight years, the Managing Director of the Journalisten-Akademie managed to hold firm against this restriction of research training. When she retired, her successor replaced the field with topics like social media production for Instagram, and later TikTok and related platforms.[6]

This undoubtedly has an impact on our journalistic discussions on topic selection. The meeting of Russia's National Security Council on February 21, 2022, for example, was claimed to have been broadcast live on Russian state television at 5 p.m. Moscow time. Colleagues in the UK in particular immediately doubted that the broadcast was live – a look at the often very large faces of the expensive watches of the meeting's participants showed that the allegedly ›live‹ images had been recorded at 12:46 Moscow time. German media were very late to report this.[7]

If we are unable to agree on a basis of methodological expertise and how to teach it in journalistic training, it will become increasingly difficult to counteract this kind of propagandist video with precise clarification of the situation (cf. Schiffer 2021, esp. p. 90ff.).

Over the last few years, collaboration with colleagues from ProRecherche e.V. has shown that journalists are certainly very interested in methods of source analysis and image forensics, but that the media houses they work for are reluctant to pay for training in the field. However, demand for this kind of content in journalistic training is usually driven not by those working in the engine room of journalism, but by managers at media houses and officials at associations. It would be well worth conducting an empirical investigation into the extent to which this distorts the choice of topics.

6   This development led to me resigning as a lecturer at the Journalisten-Akademie Stuttgart at the end of 2018, after 24 years of teaching. Reasons of professional ethics and media policy meant that I could no longer support the neglect of journalistic principles, especially systems of research. As far back as 2001, in seminars I held at the then Axel-Springer-Schule in Berlin, it became clear that those responsible were not particularly interested in teaching source analysis methods. I left that job for that reason. In contrast, this research topic has become an increasing focus of some university-based training programs in Germany and Switzerland in recent years. A quantitative analysis, however, remains but a wish.

7   Discussions with colleagues on the allegedly live report on Russian state television really stick in my mind. At best, the colleagues were flabbergasted that simply zooming in on the image around the watch faces could reveal so quickly that the images were recorded. Others disputed that such a simple method was all it took to back up such a far-reaching assertion with evidence. After all, they said, this accuses Russian state television of having produced a fake. Discussion of the topic was adjourned. A little while later, Kremlin spokesperson Dmitry Peskov confirmed that the program on Russian state television on the meeting of the Security Council had been a recording. This is undoubtedly of little significance in the context of the war, but it does demonstrate the atmosphere that often prevails when source analysis processes and the analysis of image content are discussed in German journalism. The work involved, and the methodological approaches behind it, are often held in little esteem. This makes the work significantly more difficult.

## About the author

**Peter Welchering** has worked as a journalist for radio, television and print since 1983 (incl. Deutschlandradio, ZDF, various ARD broadcasters, *Frankfurter Allgemeine Zeitung*). Having also held various teaching roles at journalism schools in Germany and abroad, he is a certified journalism coach (KfJ). Welchering studied philosophy and believes that the tools he learned there are enormously helpful in his journalism work. He teaches online/offline investigation at the Merz-Akademie, Stuttgart, as well as journalistic practice (including as an introduction to science journalism) at the University of Göttingen. Welchering spent three years as an instructor for trainees at Heise-Verlag (incl. *c't*) and eight years as Chief Editor and Editorial Office Director at Konradin-Verlag (*Computer-Zeitung* and online portals). Since 2001, he has worked in his own media office, focusing on journalistic training at all levels.

*Translation: Sophie Costella*

## References

Baab, Patrik (2022): *Recherchieren. Ein Werkzeugkasten zur Kritik der herrschenden Meinung*. Frankfurt/M.: Westend.

Browne, Malachy; Botti, David; Willis, Haley (2022): War in Ukraine. Satellite images show bodies lay in Bucha for weeks, despite Russian claims, in: *New York Times*, dated 4 April 2022, https://www.nytimes.com/2022/04/04/world/europe/bucha-ukraine-bodies.html (15 April 2022)

Higgins, Eliot (2021): *Digitale Jäger. Ein Insiderbericht aus dem Recherchenetzwerk Bellingcat*. Cologne: Quadriga.

Jacot-Descombes, Jasmine; Zellweger, Conradin (2022): Als Vorbereitung auf die Invasion in der Ukraine flutete Russland das Internet mit gefälschten Videos, *NZZ*, dated 01 March 2022, https://www.nzz.ch/international/false-flag-gefaelschte-videos-russland-ukraine-krieg-ld.1672236 (17 April 2022)

Schiffer, Sabine (2021): *Medienanalyse. Ein kritisches Lehrbuch*. Frankfurt/M.: Westend.

Stahnke, Jochen (2022): Open Source Intelligence. Wie Amateure den Geheimdiensten Konkurrenz machen. In: *Frankfurter Allgemeine Zeitung*, dated 11 April 2022. https://www.faz.net/aktuell/politik/ausland/ukraine-was-open-source-intelligence-ueber-den-krieg-verraet-17949655.html (16 April 2022)

Welchering, Peter (2015a): Nur Google reicht nicht – Die meisten Redaktionen sind mit Online-Recherchen heillos überfordert, in: *Impresso* 1/2015, Stuttgart: Südwestdeutscher Zeitschriftenverlegerverband.

Welchering, Peter (2015b): Fotos lügen. Satellitenfotos zum MH17-Absturz über der Ukraine offenbar gefälscht. In: ZDF, *heute.de*, dated 1. June 2015.

Welchering, Peter (2020): *Journalistische Praxis: Digitale Recherche. Verifikation und Fact Checking*. Wiesbaden: Springer VS.

Welchering, Peter (2021): Wie wir den Journalismus abschaffen. TEDx-presentation 18 September 2021 at Liederhalle, Stuttgart. https://www.youtube.com/watch?v=-QcRg8DOYz0 (16 April 2022)

Welchering, Peter; Kloiber, Manfred (2017): *Informantenschutz. Ethische, rechtliche und technische Praxis in Journalismus und Organisationskommunikation*. Wiesbaden: Springer VS.