INFORMATION VERIFICATION FOR BEGINNERS

How to fact-check online content

#FactCheckingMatters

The Project of
the European Union

Since the dawn of information, there has been disinformation. However, certain characteristics of the information ecosystem in which we are living today make recognition of disinformation and the fight against it spreading particularly challenging – development and accessibility of technologies for designing, changing and sharing content, the increase in popularity of mobile technologies, and social networks are some of them.

Spreading disinformation, be it inaccurate information related to vaccines and baby food or conspiracy theories at a global level, is harmful to society and citizens, and may influence decrease trust in media, even professionally managed media.

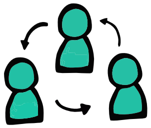
The purpose of this brochure is to teach you how to recognise disinformation and to inform you of tools for verifying suspicious information, as well as to aid you, as an informed citizen, to prevent its further spread.

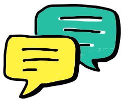
WHAT IS DISINFORMATION?

Disinformation is verifiably false or misleading information created and/or disseminated to intentionally deceive the public.

This brochure will help you to:

1. recognise information and fake news,
2. use tools for verification of photo, video and other type of content on social networks and websites,
3. prevent spreading of disinformation,
4. readily respond to disinformation in you virtual environment.





"This publication is developed with the aid of the European Union. The content of this publication is the exclusive responsibility of the authors and in no way represents the opinions of the European Union."

MEDIA

GLOSSARY

- **PROPAGANDA** – content directed toward emotions of the user intended to spread a certain ideological or commercial message - may or may not be malicious,
- **CONSPIRACY THEORIES** – content created to explain complex events in a simplified manner, often in response to sense of insecurity or fear,
- **PSEUDOSCIENCE** – content representing existing or fabricated scientific studies in a manner contrary to scientific principles - may be published with good intentions, but is among the most harmful forms of information deviation.
- **CLICKBAIT** – a form of media content in which the title and the text are not directly related, created exclusively to get the reader to visit a website and ensure additional "clicks",
- **BOTS** – automated social media accounts created to automatically transfer or publish content of a certain type. Bots may be useful and do not have to be malicious, but are often used to spread propaganda material of a political or commercial type,
- **TROLLS** – a troll is an Internet user who deliberately posts provocative content or comments in order to provoke reactions of other social network users and other online services,
- **DEEPFAKE** – use of digital technologies to manipulate recordings and voices in order to create fake video recordings,
- **SATIRE AND PARODY** – content using misleading content to point to a certain social occurrence and problem, published without intention to harm,
- **MANIPULATED CONTENT** – content that may be true, but presented in misleading, non-original context,
- **MISREPRESENTED CONTENT** – content or a website that is represented as coming from a reliable source, by stating links or taking over designs,
- **FACT-CHECKING** – in explanation, verification of facts. The practice of checking information published by public media. The person in charge of this process is called a fact-checker.

The Project of
the European Union

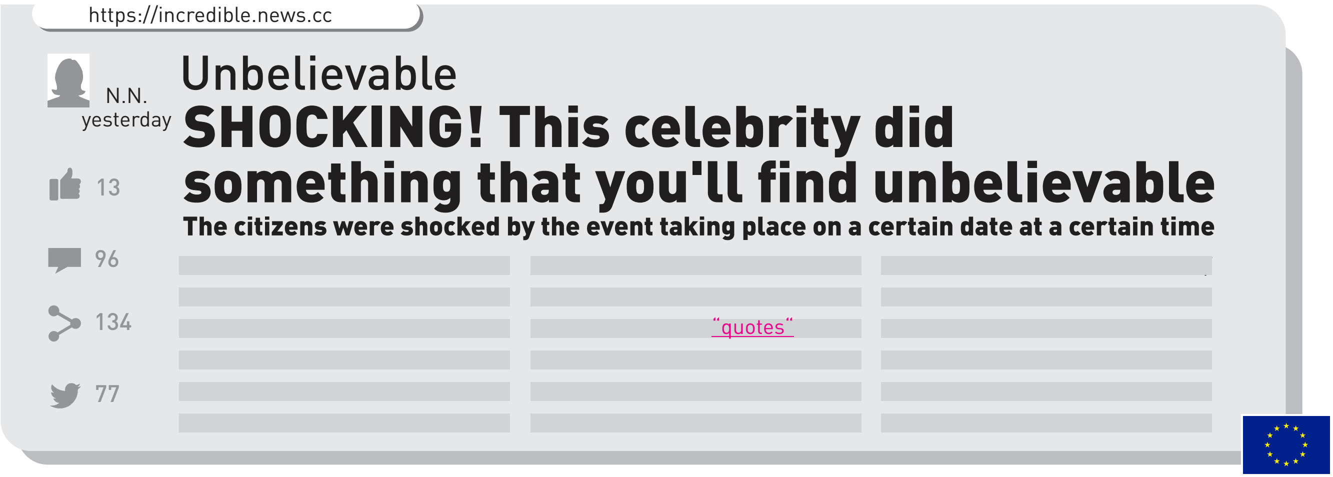
HOW TO VERIFY ACCURACY OF ONLINE CONTENT?

Tools for creating, changing and publishing online content are developing and becoming ncreasingly available. Today there are a number of applications available enabling a creation of fake SMS messages, tweets, Facebook statuses, front page news, manipulated images and video recordings in a matter of minutes. The reasons for publishing such content do not always have to be malicious or a part of the disinformation campaign, but an informed social network and other online service user has to know that digital content can be manipulated, and that even accurate information may be manipulated to cause harm.

If you doubt the accuracy of a certain news, try to trace back the first time it appeared online by searching its title on Google or another search engine. How can you know whether a certain photo was taken where it is said to had been taken? Which kind of website contains warnings that should be shared as relevant to the society? These are the fundamental questions to be asked when encountering suspicious online content:

- Origin: Is it the original content?
- Source: Who uploaded the content?
- Date: When was the content created? When was it published?
- Location: Where was the content created?

Can you provide complete answers to these questions? The fact-checking community is developing different tools on a daily basis to enable media workers, activists and ordinary citizens to verify certain aspects of online news and other content. Let us see how some of them are used:



https://incredible.news.cc

N.N.
yesterday

Unbelievable

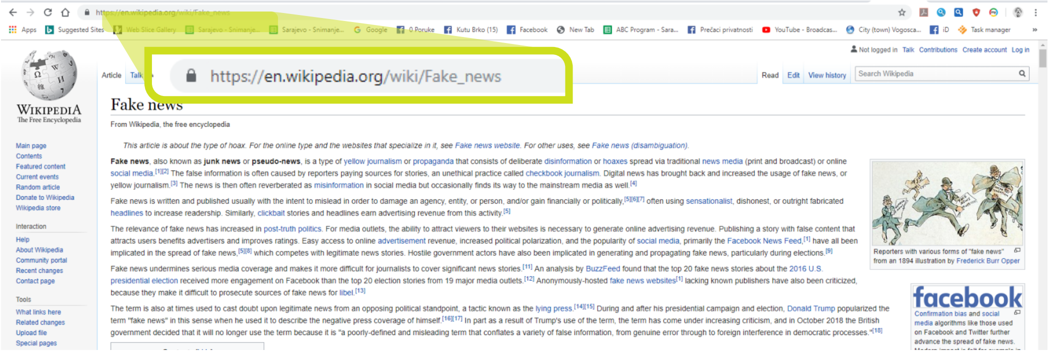
SHOCKING! This celebrity did something that you'll find unbelievable

The citizens were shocked by the event taking place on a certain date at a certain time

The Project of
the European Union

HOW TO VERIFY A WEBSITE?

The simplicity and speed required to register, create and initiate a website or a blog have made the option of creating your own media very simple not only to professional media organisations but also to common citizens. Research shows that so-called "content farms", networks of websites that increase the outreach of certain content, are spreading online and that today's audience of media content has to be careful when trusting media they have not previously encountered.



https://en.wikipedia.org/wiki/Fake_news

Fake news

From Wikipedia, the free encyclopedia

This article is about the type of hoax. For the online type and the websites that specialize in it, see Fake news website. For other uses, see Fake news (disambiguation).

Fake news, also known as **junk news** or **pseudo-news**, is a type of yellow journalism or propaganda that consists of deliberate disinformation or hoaxes spread via traditional news media (print and broadcast) or online social media.[1][2] The false information is often caused by reporters paying sources for stories, an unethical practice called checkbook journalism. Digital news has brought back and increased the usage of fake news, or yellow journalism.[3] The news is then often reverberated as misinformation in social media but occasionally finds its way to the mainstream media as well.[4]

Fake news is written and published usually with the intent to mislead in order to damage an agency, entity, or person, and/or gain financially or politically,[5][6][7] often using sensationalist, dishonest, or outright fabricated headlines to increase readership. Similarly, clickbait stories and headlines earn advertising revenue from this activity.[5]

The relevance of fake news has increased in post-truth politics. For media outlets, the ability to attract viewers to their websites is necessary to generate online advertising revenue. Publishing a story with false content that attracts users benefits advertisers and improves ratings. Easy access to online advertisement revenue, increased political polarization, and the popularity of social media, primarily the Facebook News Feed,[1] have all been implicated in the spread of fake news,[5][8] which competes with legitimate news stories. Hostile government actors have also been implicated in generating and propagating fake news, particularly during elections.[9]

Fake news undermines serious media coverage and makes it more difficult for journalists to cover significant news stories.[11] An analysis by BuzzFeed found that the top 20 fake news stories about the 2016 U.S. presidential election received more engagement on Facebook than the top 20 election stories from 19 major media outlets.[12] Anonymously-hosted fake news websites[1] lacking known publishers have also been criticized, because they make it difficult to prosecute sources of fake news for libel.[13]

The term is also at times used to cast doubt upon legitimate news from an opposing political standpoint, a tactic known as the lying press.[14][15] During and after his presidential campaign and election, Donald Trump popularized the term "fake news" in this sense when he used it to describe the negative press coverage of himself.[16][17] In part as a result of Trump's use of the term, the term has come under increasing criticism, and in October 2018 the British government decided that it will no longer use the term because it is "a poorly-defined and misleading term that conflates a variety of false information, from genuine error through to foreign interference in democratic processes."[18]

Reporters with various forms of "fake news" from an 1894 illustration by Frederick Burr Opper

Confirmation bias and social media algorithms like those used on Facebook and Twitter further advance the spread of fake news.

These are some of the things to be taken into consideration when you encounter news from an unreliable website:

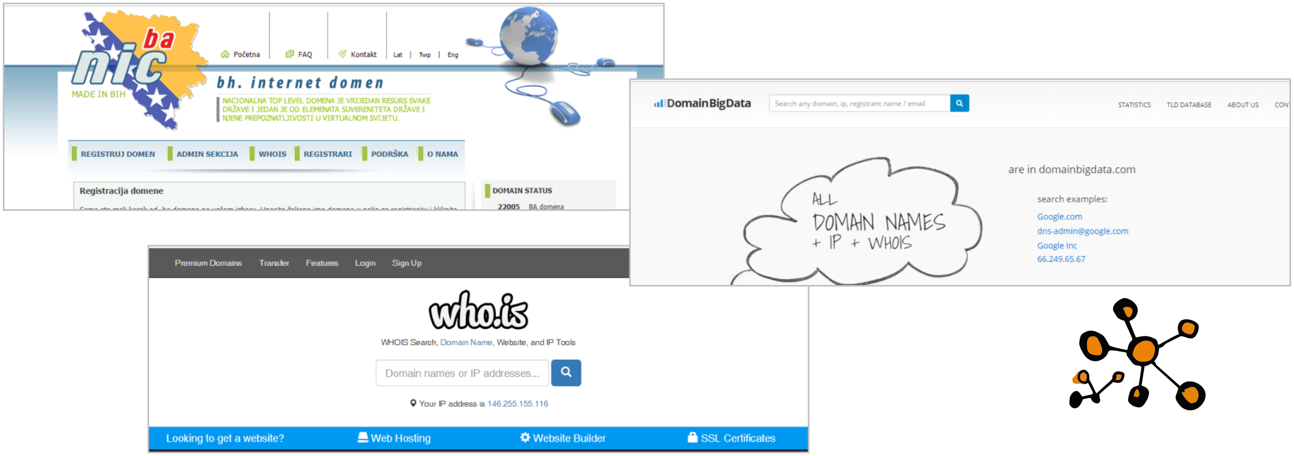
Website verification – check list

- URL – can we recognise the web address of the site? Is the website registered on a known domain (.ba, .com, .net, etc.) or is it a domain that is either unknown or hosted by a blog service?
- Impressum – does a website have a visible impressum? Do you now the creator and editor of the content you are reading? Anonymous websites are often the most effective place in which to false and manipulated content
- Contact information – is there a visible manner through which you can contact the editors?
- Who.is/Domain BigData – check the name and location of who registered the website.
- Backlink analysis – do links in the text take you to designated sources?
- Bias/agenda – is this website related to a political option or commercial campaign?
- Blacklist – is this website included on a public list of sites publishing problematic content?
- Who else is reporting about the event?

DAILY NEWS

Tools: Nic.ba, Who.is, Domain Big Data

Information on name and location of registration of a certain website may be found in some online lookups, such as Nic.ba (www.nic.ba), Who.is (www.who.is) and Domain Big Data (www.domainbigdata.com). In order to check a website, enter the web address in the search field and, unless the data is hidden, these online services will inform you on who registered the website, its links to other websites, the registration location, the location of servers and other data useful for further search.



If you doubt an accuracy of a certain news, trying to trace back the first time it appeared online by search its title in Google or another search engine. Who else is quoting the news, are other sources reliable? Has the news been originally published some time ago, and changed and adapted in the meantime? For news in foreign languages, use online services for translation of text, such as Google Translate. Google advance search options offer different ways to narrow down your inquiry so as to search a specific website, everything except a certain website, titles only, only documents of certain format, etc.

Shortcuts for the advanced Google search

Search within a website: search site:website.com

Everything except a website: search -website.com

Title search: allintitle: title

URL search in url: looking.for.this

Document search search filetype:pdf

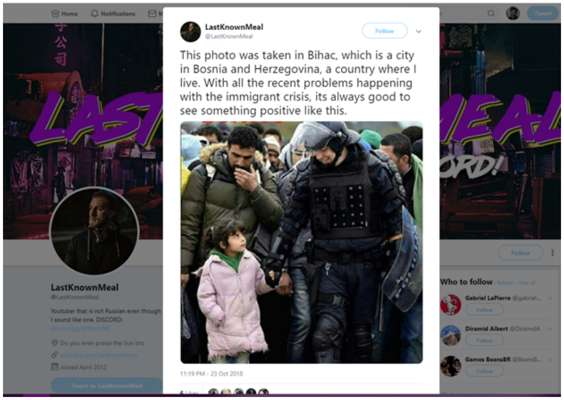
Source search: source

The Project of the European Union

HOW TO VERIFY AN IMAGE?

Tools: Google Reverse Image Search, Yandex, TinEye, Forensically, FotoForensics

Tools for creating and photoshopping visual information elements (images) are today available to the broad public. Images spreading disinformation may be changed, manipulated or placed in a wrong context. In order to verify whether the image you found shows what it claims, search the Internet for other addresses in which the image was presented first and find out when it was originally shown online.


LastKnownMeal
@LastKnownMeal

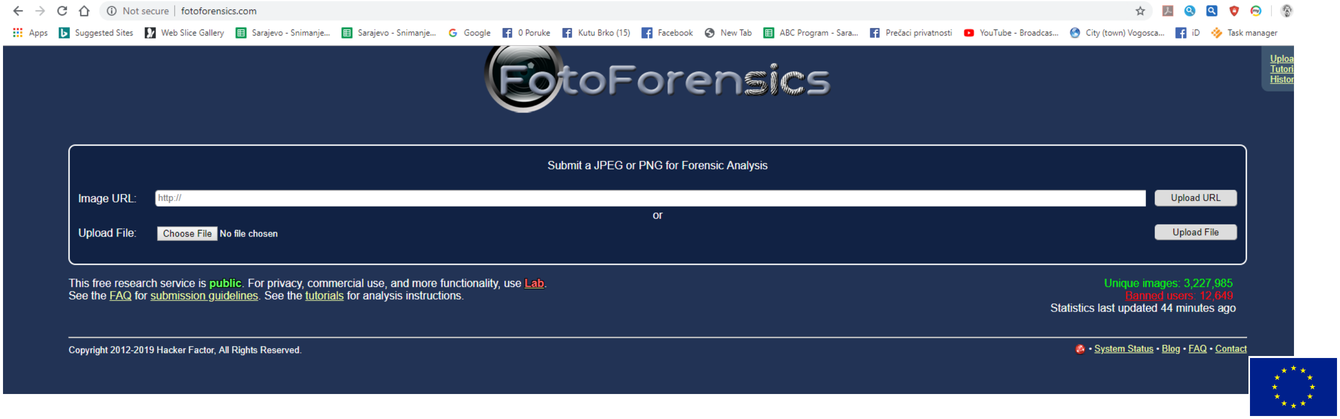
This photo was taken in Bihac, which is a city in Bosnia and Herzegovina, a country where I live. With all the recent problems happening with the immigrant crisis, its always good to see something positive like this.

11:19 PM - 23 Oct 2018

LastKnownMeal
@LastKnownMeal
Youtuber that is not Russian even though I sound like one. DISCORD: discord.gg/6kWpRAW
Do you even praise the Sun bro
youtube.com/lastknownmeal
Joined April 2012

This can be accomplished by using the Google Reverse Image Search (if you're using the Chrome search engine, click right on the image and select the option "Search Google for Image"), which will provide a list of all locations that have used the image. The same function is available on the sites Yandex.com and TinEye.com, and, given the fact that results on these websites may differ sometimes, it is recommended to use them in combination. For finding the original source of an image, pay attention to the date of upload and size of the image (source image is usually in greater resolution).

If you want to verify whether the image has been photoshopped or manipulated, the tool FotoForensics will enable you to examine the elements of the image and see if they have been changed. This tool will also provide you with information on when the examined image was uploaded to the website from which it is examined, which is useful when there is no date of publishing of news.


Not secure | fotoforensics.com

FotoForensics

Submit a JPEG or PNG for Forensic Analysis

Image URL: http://

or

Upload File: Choose File No file chosen

This free research service is public. For privacy, commercial use, and more functionality, use Lab.
See the FAQ for submission guidelines. See the tutorials for analysis instructions.

Unique images: 3,227,985
Banned users: 12,649
Statistics last updated 44 minutes ago

Copyright 2012-2019 Hacker Factor, All Rights Reserved.

The Project of
the European Union

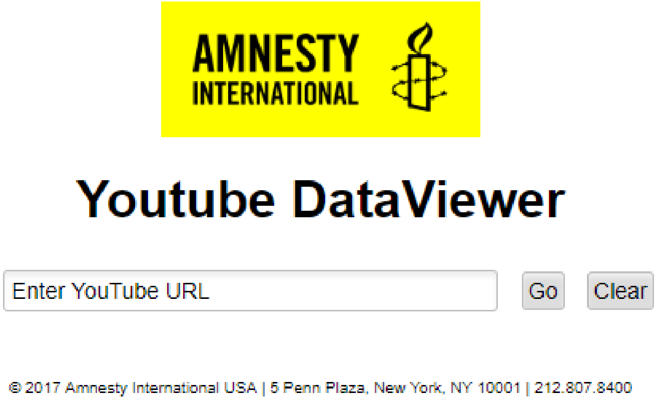
HOW TO VERIFY A VIDEO?

Tools: InVID, YouTube Data Viewer

Although they cannot be as easily manipulated as images, video recordings are also frequent formats of sharing disinformation. A video recording published with the aim of spreading disinformation may be misinterpreted, edited so as to transfer a message that was not stated in the original context, or to allegedly represent the location or situation corresponding to the intentions of the users or website that published it. The development of the artificial intelligence technology in the last few years has enabled massive progress in the field of manipulating video content, and users are recommended to be cautious about sharing suspicious video content.
Let's remind ourselves of the questions relevant to a verification of all online content:

- Origin: Is this the original content?
- Source: Who uploaded the content?
- Date: When was the content created? When was it published?
- Location: Where was the content created?

The popular video service YouTube offers the option of viewing data related to the video and, if the video you wish to verify has been published on this platform, we recommend you start your search there. See when the video was published, and by using the tool YouTube Data Viewer, developed by the organisation Amnesty International, you will get screenshots from the video. Every screenshot can be used in the "reverse image search" option on the side, or you may make your own screenshot of the video recording and use other reverse image search tools to search for all places in which the video occurs online.



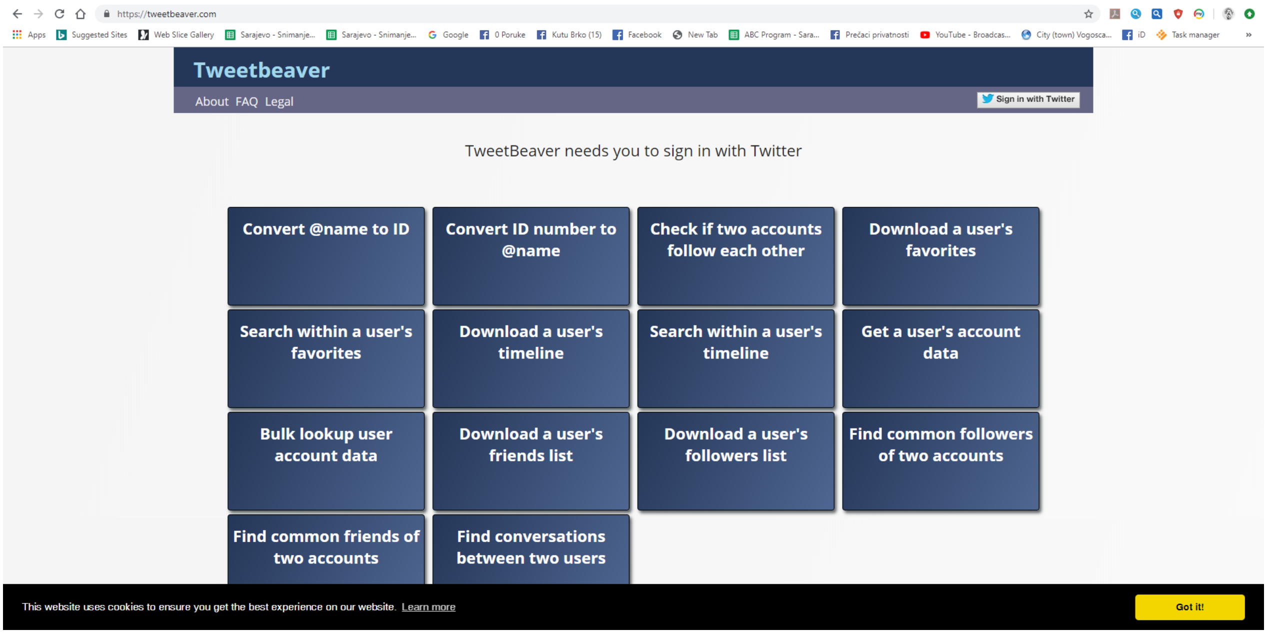
Youtube DataViewer

© 2017 Amnesty International USA | 5 Penn Plaza, New York, NY 10001 | 212.807.8400

HOW TO VERIFY TWEETS AND OTHER SOCIAL NETWORK POSTS?

Tools: Social media ID, Twitonomy, Tweetbeaver, Twitter advanced search

Today's social networks are significant sources of information for all users, but also for media organisations. If you encounter information that has been shared from a certain user account on Twitter, Instagram, YouTube or Facebook, there are certain steps you can take to verify the reliability of the content, and whether you should share it with your friends. Within the community of experts handling information verification, there is a saying: "You don't have to check everything, just the information you're planning on sharing."


https://tweetbeaver.com
Apps
Suggested Sites
Web Slice Gallery
Sarajevo - Snimanje...
Sarajevo - Snimanje...
Google
0 Poruke
Kutu Brko (15)
Facebook
New Tab
ABC Program - Sara...
Prečaci privatnosti
YouTube - Broadcas...
City (town) Vogosca...
iD
Task manager
Tweetbeaver
About FAQ Legal
Sign in with Twitter
Convert @name to ID
Convert ID number to @name
Check if two accounts follow each other
Download a user's favorites
Search within a user's favorites
Download a user's timeline
Search within a user's timeline
Get a user's account data
Bulk lookup user account data
Download a user's friends list
Download a user's followers list
Find common followers of two accounts
Find common friends of two accounts
Find conversations between two users
Learn more
Got it!

TweetBeaver needs you to sign in with Twitter

This website uses cookies to ensure you get the best experience on our website. Learn more

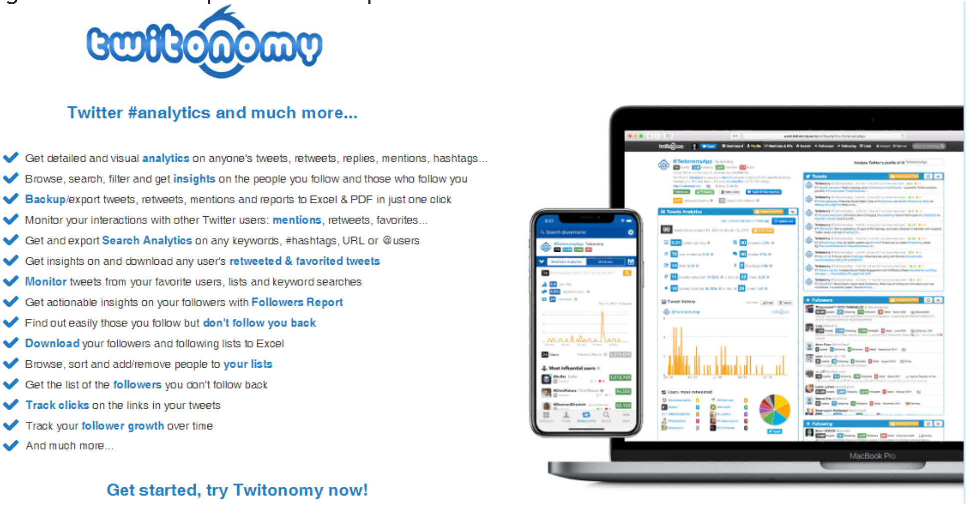
Source verification

- Can you find the same or similar post/content elsewhere?
- When was the first/oldest version uploaded/recorded/created?
- Can you identify the location? Is the content geotagged?
- Does the content take you to certain websites?
- Can you identify the person who shared the content and contact them for more info?

Verifying social network accounts

- Can you verify the identity or contact persons?
- Do you know the account from before? Was its content and reports reliable before?
- Verify the history of the person/account in social networks.
- Verify their connections on social networks.
- Try finding other orders with the same name on other social networks.
- Is the account (actually) verified? – It is not easy to acquire the famous blue check mark next to the account name, which stands for verified users, but it can be photoshopped to the front page photo in the background. Bring your cursor the check mark to see the word "verified" which proves that the social network verified the account.
- Social media ID – Number identifying the respective post in certain social networks (Twitter, YouTube, Instagram) which is unique for that post, and the search of the number enables us to see where the content was transferred and used.
- Is it a bot? ---

Tools like Twitonomy.com and Tweetbeaver enable a detailed overview of certain Twitter posts and determine the relationship between accounts that publish them. You may see whether certain accounts follow each other, whether they publish the same (propaganda) content, therefore increasing the outreach of certain messages. It is recommended that you separately check the multimedia part of the post by using tools from the previous chapters.



twitonomy

Twitter #analytics and much more...

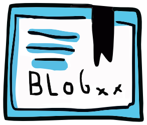
- ✓ Get detailed and visual **analytics** on anyone's tweets, retweets, replies, mentions, hashtags...
- ✓ Browse, search, filter and get **insights** on the people you follow and those who follow you
- ✓ **Backup**/export tweets, retweets, mentions and reports to Excel & PDF in just one click
- ✓ Monitor your interactions with other Twitter users: **mentions**, retweets, favorites...
- ✓ Get and export **Search Analytics** on any keywords, #hashtags, URL or @users
- ✓ Get insights on and download any user's **retweeted & favorited tweets**
- ✓ **Monitor** tweets from your favorite users, lists and keyword searches
- ✓ Get actionable insights on your followers with **Followers Report**
- ✓ Find out easily those you follow but **don't follow you back**
- ✓ **Download** your followers and following lists to Excel
- ✓ Browse, sort and add/remove people to **your lists**
- ✓ Get the list of the **followers** you don't follow back
- ✓ **Track clicks** on the links in your tweets
- ✓ Track your **follower growth** over time
- ✓ And much more...

Get started, try Twitonomy now!

The Project of
the European Union

How to recognise bots and fake profiles on social networks

- Publishing content in regular time periods – does the account publish notices in regular time periods (e.g. every 14 minutes)? It might be a bot.
- Constant activity – automated accounts (bots) are not limited by the human body that conditions the activity of other users. Does the account post equally day and night? It might be a bot.
- Propaganda material – is the account you are verifying publishing content that propagates an idea, political option or commercial campaign?
- Profile picture – fake profiles often keep the automatic user profile picture (the so-called "egg" on Twitter, a silhouette of a person on Facebook) or use photos of other users for the profile picture from online bases (stock photo).
- Birthday – fake profiles often keep the birthday automatically assigned by the social network, e.g. January 1.
- Who are their friends? – fake profiles often add as friends other fake profiles, or automatically send a vast number of friend requests to users all over the world. Do the friends of the suspicious account look unrelated and come from many different countries?



Text author: Maja Ćalović
Publishers: BORAM and Media centar
Printing: Optigraf d.o.o. Sarajevo 11
Sarajevo, July 2019

The Project of
the European Union

RESOURCES – tools, links, publications, games

Tools for verifying multimedia content and other elements of online news are constantly developing. This list is not and should not be final, its purpose is to inspire you to test your information verification skills and discover new ways of regularly implementing the practice.

- Raskrinkavanje.ba – website managing the verification of media content
- Manual for verifying information in state of urgency: www.verificationhandbook.com
- factitious.augamestudio.com – do you know how to recognise fake news?
- www.getbadnews.com – play the role of a fake content creator
- Gapminder Test: forms.gapminder.org/s3/test-2018

Web addresses of tools stated in this brochure:

- Nic.ba: http://nic.ba/
- Who.Is: https://who.is/
- Domain Big Data: https://domainbigdata.com/
- TinEye: https://www.tineye.com/
- Yandex pretraga slika: https://yandex.com/images/
- Forensically: https://29a.ch/photo-forensics/
- FotoForensics: http://fotoforensics.com
- InVID: https://www.invid-project.eu/
- YouTube Data Viewer: https://citizenevidence.amnestyusa.org/

I have discovered other tools:

____

____

____

____

#FactCheckingMatters

The Project of
the European Union