

SKOPENOW

THE DEFINITIVE GUIDE:

Gab for OSINT
Investigations

INTRODUCTION

3

Profile Discovery

4

Content Extraction

8

Dissenter

21

Expanding the Investigation

27

TABLE OF CONTENTS

INTRODUCTION

Gab is a social media platform launched in 2016 commonly associated with a far-right user base. After the recent removal of Parler from the Apple App Store, Google Play Store, and Amazon Web Services, many free speech advocates are flocking to Gab instead of back to more mainstream platforms. In light of riots at the US Capitol on January 6, 2021, it's essential to understand the importance of expanding an OSINT investigation to alternative social media platforms. This guide will cover how to discover users and groups on Gab and Dissenter, extract relevant content from pages of interest, and analyze the data collected. Additionally, it'll cover Dissenter, a Brave-based custom browser created by Gab, and how it can be useful in an investigation.

Disclaimer

In 2018, Rob Gregory Bowers, the suspected shooter in the attack against a Pittsburgh synagogue on October 27, 2018, maintained an active, verified Gab account. Just before the shooting, he used his Gab account to announce his intent to commit the shooting. Following the event, Gab was taken down temporarily while under investigation by the FBI. Like Parler, Gab is susceptible to unannounced outages and takedowns that could impact an OSINT investigation's continuity.

1

PROFILE DISCOVERY

This chapter will teach techniques to find user profiles using a search engine and how to access the information needed for an OSINT investigation.

Personal Profiles

Search Engines

`site:gab.com intitle:"@" -inurl:trends -inurl:help`

Unlike Parler, Gab doesn't have a specific designation for profile pages. Their URL structure is just `gab.com/{username}`, making it difficult to find results in a search index. Although, after analyzing a few Google search results, it is possible to specify profiles by adding a few filters to the Google query.

Entering `site:gab.com` instructs Google to only view results from gab.com. Adding `intitle:"@"` tells Google to look for pages with that text in the title. In the case of Gab profiles, they always list the username next to the title's name using this format.

`gab.com > drgpradhan` ▼

Gaurav Pradhan (@DrGPradhan) • gab.com - Gab Social

The latest Gabs from Gaurav Pradhan (@DrGPradhan). © Comments w/o Prejudice

#DataScience, #DigitalTransformation, #SMAC, Cyber Warfare, Global Top ...

Finally, to remove subdomains like `trends.gab.com` or `help.gab.com`, simply add the `-inurl:trends` and `-inurl:help` commands to remove those types of results from the search. What remains are only profile pages for individuals. At the time of this writing, there are about 44,700 results indexed. Adding in unique identifiers, like name and username, to this query will begin the search.

`site:gab.com intitle:"@" -inurl:trends -inurl:help "{display name}" OR "{username}"`

After removing potential false positives by excluding subdomains, it's time to enter the information available in conjunction with the Google query we've already built. Using the above search structure, looking for a name or display name OR a username is easier.

It is possible to broaden or narrow this search by adding `OR"{emailaddress}"OR"{phone number}"`, etc. However, because all profiles contain a display name AND a username, there is a high degree of certainty that the results we're looking at are what has been specified.

Here is a specific example:

```
site:gab.com intitle:"@" -inurl:trends "Andrew Anglin" OR "@andrewanglin"
```

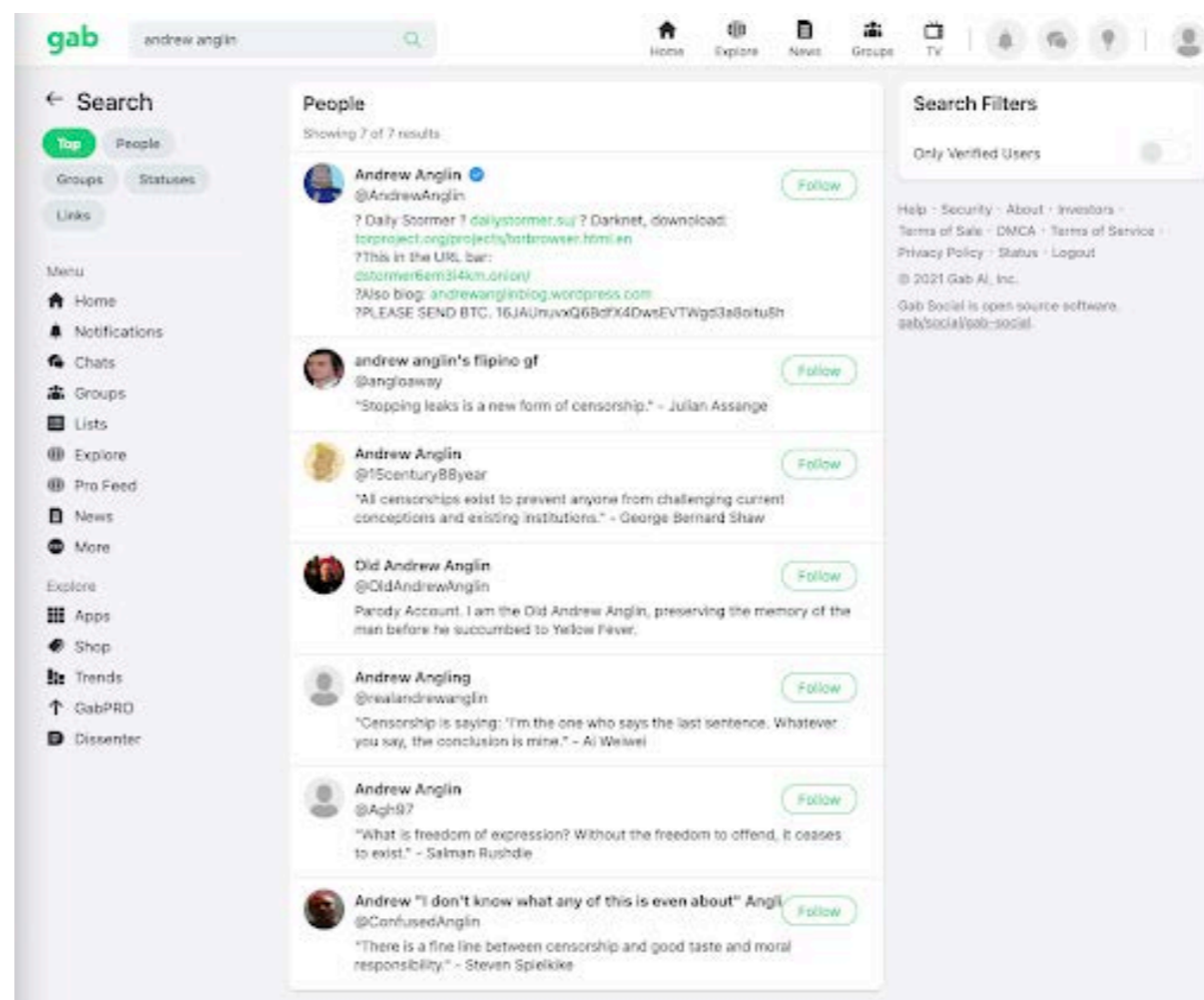
Andrew Anglin is a known white supremacist, neo-nazi, and provocateur. He's the founder of The Daily Stormer, an alt-right blog containing racist and antisemitic content. Because of the no censorship whatsoever' policies of Gab, Andrew Anglin maintains a Gab account. Using the command above finds Andrew Anglin's profile quickly. Now, the reason to start with Google's index rather than just searching for Andrew Anglin using Gab's search engine is that Google will automatically provide additional results, including people who've mentioned Andrew Anglin on their profile or in posts they've shared or written. These additional users can be valuable for link analysis later on. At the time of this writing, there are 810 results for the Andrew Anglin query linked above.

Gab's Search Engine

After exploring the options in Google's search index, it's time to look at Gab's internal search engine. By entering the same query, Andrew Anglin, only seven results are displayed (A).

There's an important item to note here. When examining the URL after searching, it will render like <https://gab.com/search?q=andrew20anglin>; however, expanding "See more" provides the full list, and the URL will revert to <https://gab.com/search/people>. Additionally, once the link is clicked, the <https://gab.com/search?q=andrew20anglin> URL reverts to a generic search page asking for a query to be performed. This is likely an anti-scraping mechanism implemented by Gab to avoid mass collection. It is important to keep tactics like this in mind when using scripts to collect information.

Looking at the results themselves, notice that Gab has a few filtering options: top, people, groups, statuses, and links. Clicking through them will show or hide results for each category of content. Like the URL structure for searching, clicking on each filter will change the URL to the associated filter (</groups/>, </statuses/>, </links/>). Still, it won't include the query itself, which is likely caused by another anti-scraping mechanism.



Gab's internal search engine (A)

Finally, there's an "Only Verified Users" filter. This appears to be non-functional at the time of this writing. It should filter out all results except Andrew Anglin's "blue checkmark" account; hopefully it will be functional again soon.

URL Input

The final and quickest way of checking if a Gab profile exists is to enter the usernames already known directly into Gab's URL to find profiles. By simply adding "andrewanglin" to "gab.com/", the search engine should instantly redirect to his profile: <https://gab.com/andrewanglin>.

CONTENT EXTRACTION

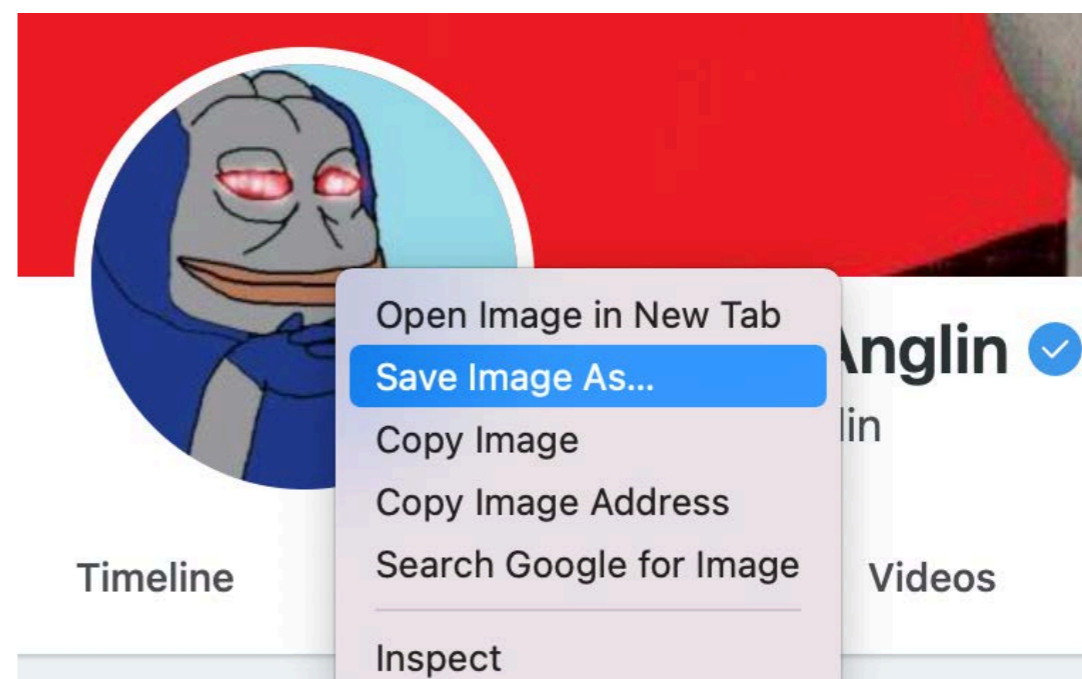
This chapter will show methods to extract the content from profiles for easy analysis once data collection is complete.

Now that we've identified a profile of interest, it's time to begin the extraction process. Because of the potential for Gab to be removed by authorities or service providers in reaction to events, it's essential to archive any relevant information as soon as possible. Once it is understood where to find specific content types, using a scraping or screen capture tool to extract and archive this information for an investigation is easy. Let's look at what types of content are available on Gab and how to extract them.

Profile Pictures

Similar to Parler, Gab allows users to upload a profile image. Unlike Facebook though, a user only gets one, and there isn't a history of previous profile images. For this reason, it's important to extract that profile image and archive it in the event it's changed. Pulling the profile image is easy; however, it takes a small adjustment to get it right.

If you right-click and save the profile image (A), it saves in a .bin format. This is odd because the cover photo, which we'll cover in a moment, is in a .png format. Depending on the operating system used, it might not be possible to view a .bin file without a special utility. Fortunately, simply renaming the file extension from .bin to .png will allow the file to be viewed normally. You can use this image to conduct reverse image searches on Google, Bing, Yandex, or other reverse image search tools to expand an investigation beyond Gab.



Right-click to save image to storage (A)

10- z

At first glance, the display name doesn't seem like a valuable data point. However, it's important to note that not only can a user choose an alias there; instead, they can also change their display name at any moment. Archiving this information with a screen capture is important. Additionally, an HTML download of this page will allow the reference page's source code to be captured if the evidence collected is ever called into question.

Andrew Anglin ✓

Another thing to note is the blue checkmark next to the display name. Blue checks indicate a verified account. Like Parler, Gab requires users to upload a government-issued ID to prove verification. Gab states the information is 'immediately deleted once verified'; although, 'once verified' could include a significant delay.

Username

If the profile in question was found via searching by username, this data point may not be of value; however, if an alternate username was discovered while searching by display name or any other identifier, this can be a very valuable data point. It's important to note a few things here about usernames on Gab.

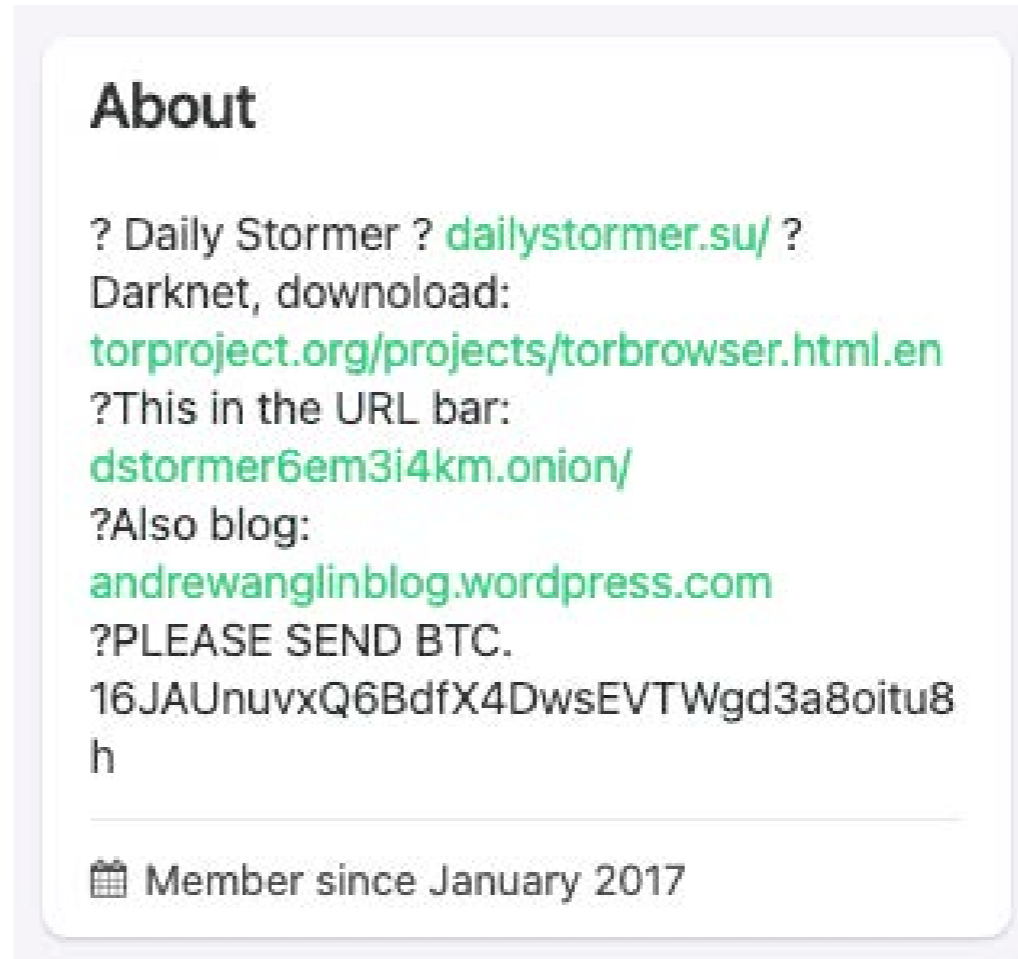
@AndrewAnglin

Username cannot be changed on Gab. Once registered, one's username cannot be altered. Typically, many users will simply abandon accounts to create new ones under alternate usernames. Keep this in mind if abandoned accounts are discovered. The user may still be active but using a different username. Unlike Parler, Gab doesn't automatically generate a username based on an email address if available. During the signup process, Gab asks users to select their username before account creation and checks availability. This means that a username is not indicative of an email address; likewise, an email address isn't indicative of a username. That said, make sure to conduct a reverse username search across multiple social media platforms to expand an investigation beyond Gab.

Biographical Information

In addition to a display name and username, Gab users can also add a biography listed in the “About” section of the page. Often, this is a section where the user describes who or what they are; they may also post URLs, email addresses, and phone numbers in some cases. In the case of Andrew Anglin, there are four URLs (A). The profile also tells us that Anglin’s profile was created in January of 2017.

Finding information such as an email address or phone number can be a significant lead for an investigation. Additionally, finding previously unknown domain names, as seen with Daily Stormer’s URL, can help find additional information doing a reverse WHOIS search or pivoting to that website for further information.



About

? Daily Stormer ? dailystormer.su/ ?
Darknet, download:
torproject.org/projects/torbrowser.html.en
?This in the URL bar:
dstormer6em3i4km.onion/
?Also blog:
andrewanglinblog.wordpress.com
?PLEASE SEND BTC.
16JAUnuvxQ6BdfX4DwsEVTWgd3a8oitu8
h

📅 Member since January 2017

Gab allows links within their biography (A)

Header Photo

The header photo on Gab is similar to cover art on Twitter. This image can be easily downloaded by right-clicking on it and clicking 'save to desktop.' Unlike the profile image, there is no need to convert from .bin to .png on this one. However, the same logic applies. At any given moment, the user can change their header photo, and if it hasn't been archived, it could be lost forever. Like profile pictures, make sure to reverse image search any unique header photo to expand the investigation beyond Gab. If the profile has stock imagery or a common meme/photo, this reverse search will likely produce false positives.

Followers

A user's follower list on Gab might be the most valuable data one can extract from a page beyond the content they've posted to their timeline. Pulling the follower list gives the basic building blocks for social network analysis. Gab uses an infinite scroll to display its users' followers list. Using a scraping or screen capture tool is the best way to extract all followers from a user's profile. This list will include the display name, username, profile image (icon), and link to their profile. Of course, this list is subject to change. A user may gain or lose followers at any time. For this reason, it's important to archive a follower list to avoid missing a follower if the latter scenario occurs.

Once a Follower list has been extracted, reverse search those followers' usernames to find profiles on other social media platforms. If an investigation's subject uses an alias, analyzing the followers of their followers on other social media platforms might lead to an alternate account. Make sure to keep a lookout for identical or similar display names as well as matching profile pictures.

Following

As we've explored, the follower list can be very valuable. Extracting a following list requires the same process. However, it's important to note the difference of value for followers and followings depending on the account type before extraction.

In the case of influencers, they typically have disproportionately more followers than people/accounts they follow; alternatively, regular users often follow far more than follow them. Using this logic, we can quickly identify which accounts are influencers, followers, or spectators. For influencers, a following list can show you other influencers in the same niche without having the noise of thousands of regular users in the mix.

The following list can show other regular users who follow influencers in the same niche (often connected through discourse) or previously unknown influencers. Finally, finding an account with a small number of followers and following is possibly indicative of a spectator or someone who consumes content without the desire to interact with others online.

Timeline

The timeline on Gab is where all content the user has posted is found. It will show a date stamp, whether it's public or not (globe icon), whether it was posted into a group or not, the content itself, and finally, the list of engagements. The timeline also contains content the user has reposted from another user's timeline. Let's break these down a bit further.

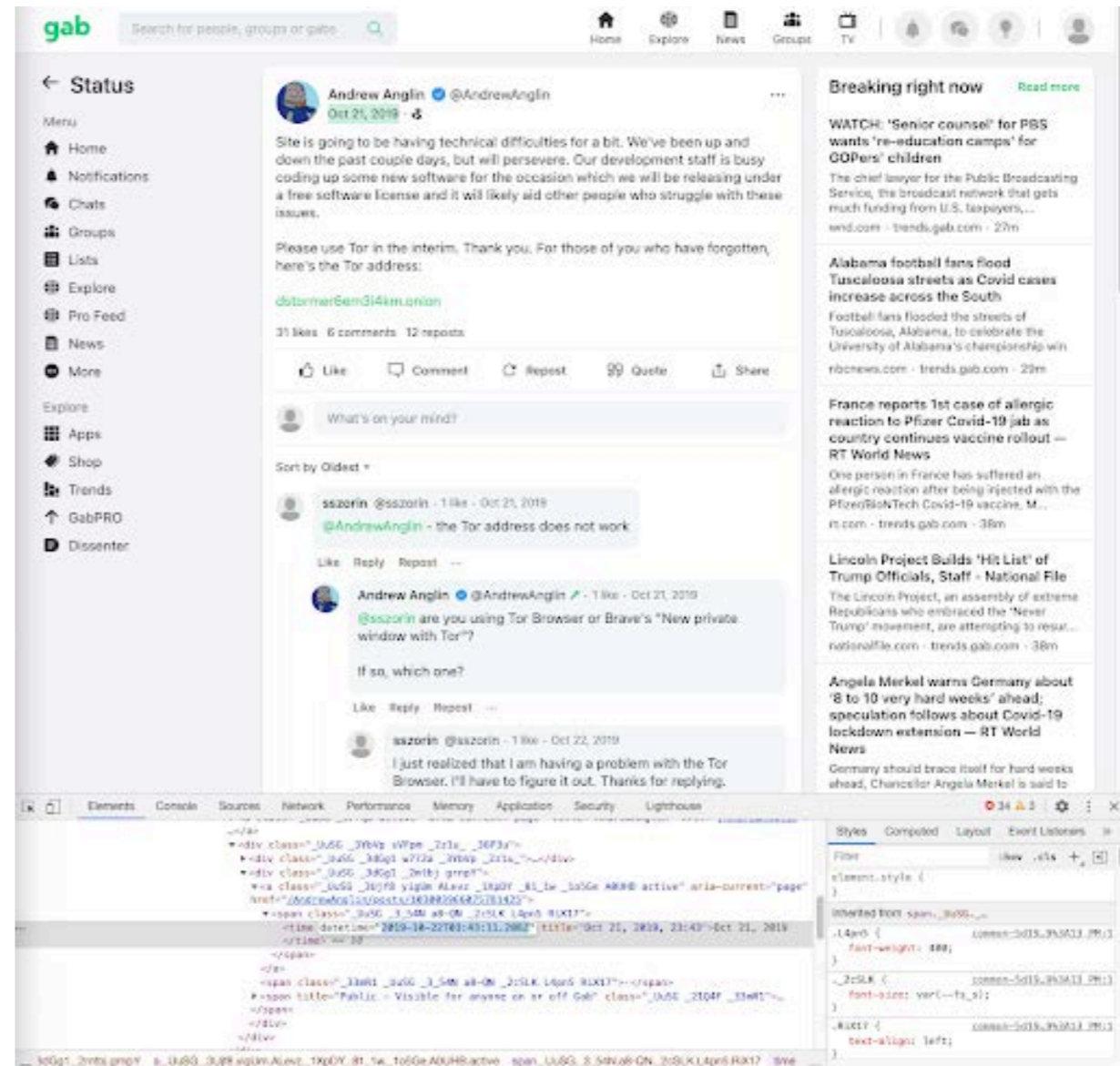
Date / Timestamp

When looking at any post on Gab, there should be a date posted underneath the display name.



While this information is valuable, more information is better. Right-clicking the date stamp and using the "inspect" or "inspect element" tool gives the full date/timestamp (A).

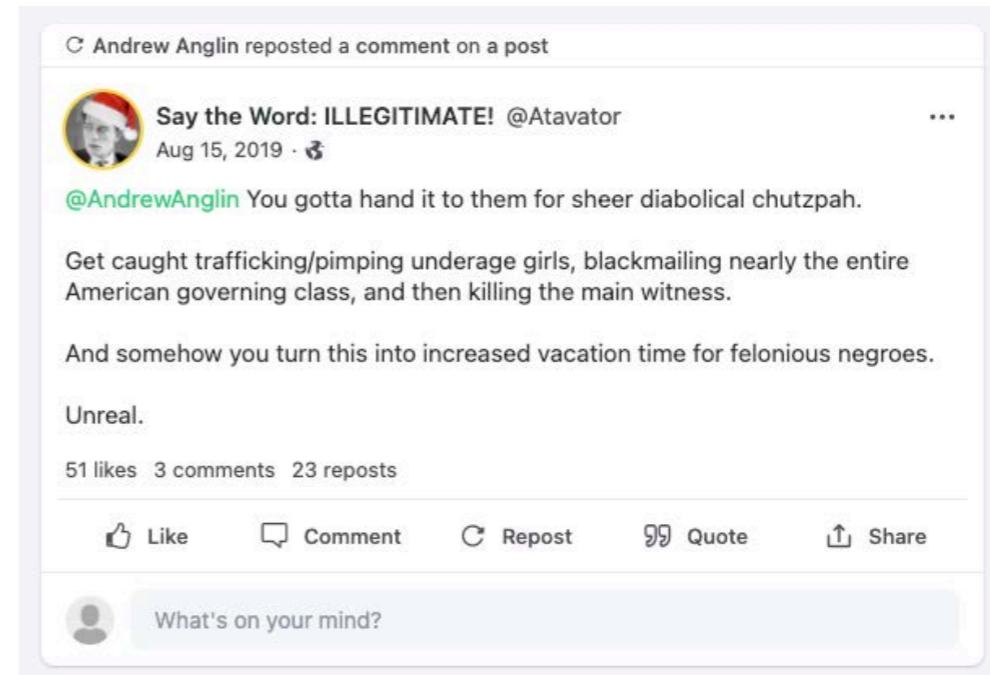
This will give you the time it was posted in UTC: 2019-10-22T03:43:11.208. When building out a timeline of a user's activity on Gab, it's much more valuable to know exactly what time it was posted rather than simply the date. Additionally, when analyzing activity across social networks, comparing timestamps of identical or similar posts from the same or alias accounts can be very useful for verification purposes.



Details available in the source code (A)

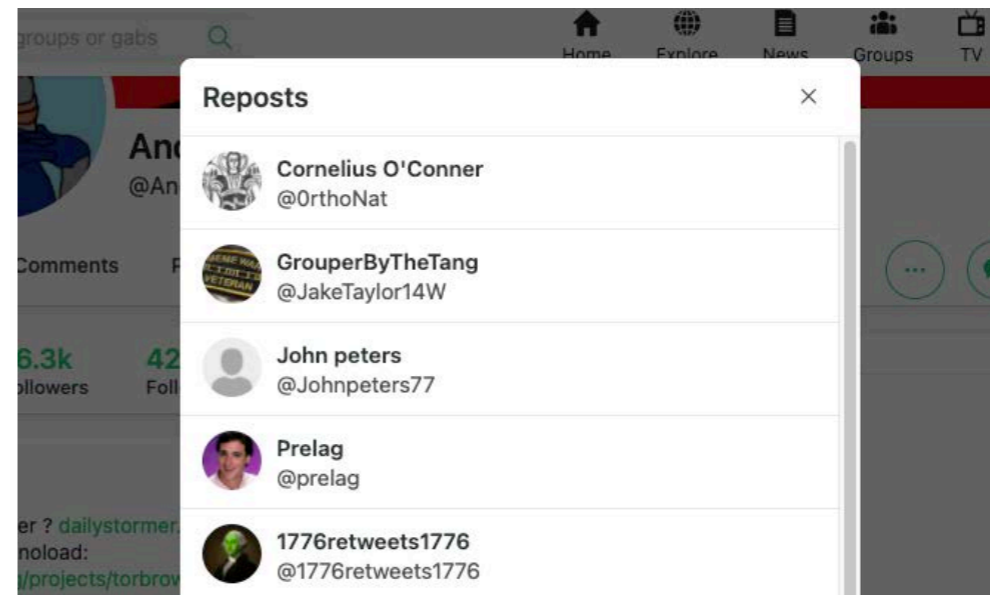
Reposts

A user on Gab can repost anything from anyone with a public profile to their own. This concept is similar to a retweet on Twitter (A). When extracting a user's timeline, which this document covers later, make sure to note the reposts in the extracted list. Compare these against the following/followers list to validate the user's social network. Likewise, reverse searching usernames of content reposted by the subject can reveal profiles on other social media platforms where the investigation can be expanded.



Reposts show the original post and comments (A)

Also viewable here is who has reposted content of interest. When clicking the "reposts" button at the bottom of the post, Gab will display a pop up showing all of the users that reposted that post (B). This is another handy list of information for network analysis.



Pop-up will tell you everyone who reposted (B)

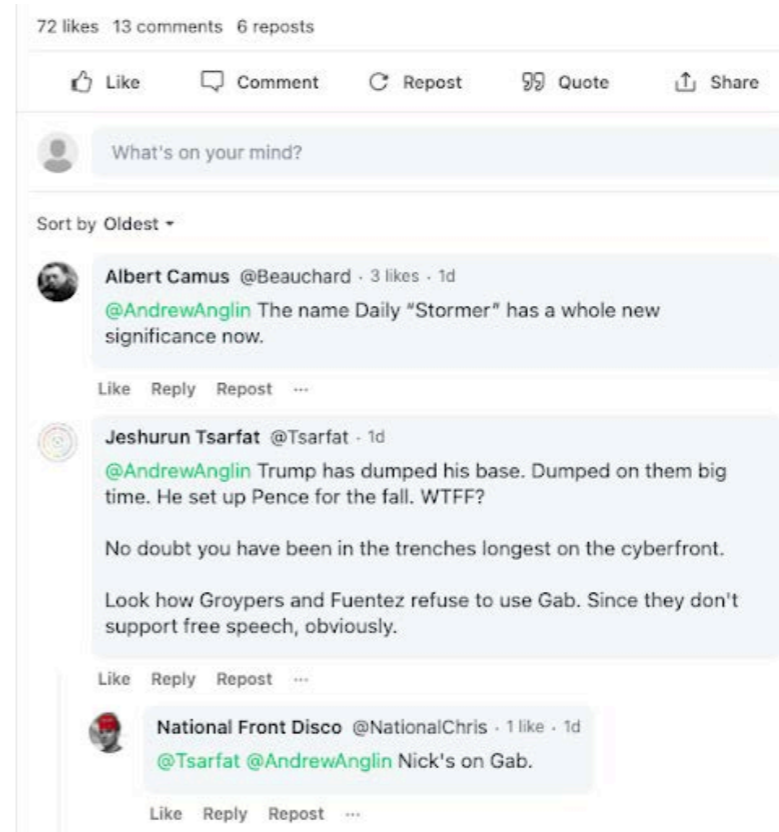
Comments

Gab users can leave comments on any public post they want. When clicking on the “comments” section of a Gab post it’ll show a new page specifically for that post. From there it provides the list of all comments by users. Here’s an example from one of Andrew Anglin’s posts (A).

Using comments in conjunction with reposts, followers, and following lists is a good start when building a frequency analysis based social network. Comparable to other data points, those usernames can also be used to expand an investigation beyond Gab.

Profile Comments

Now that the list of who has commented on the profile of interest is available, checking to see who the profile of interest has commented on comes next. Adjacent to “Timeline,” there is a tab for “Comments” at the top of the profile. Clicking will open a new page showing all of the comments a user has made and who they are directed at. It doesn’t show which post the profile commented on. Alternatively, adding /comments/ to the end of the URL of a profile page (i.e. gab.com/andrewanglin/comments) will go straight to that page (B). Using the list of profiles a subject has commented at to, once again, will add to the quality of the network analysis.



Comment are listed under the post (A)

Comments



Clicking on links opens comments in a new page (B)

Media

Gab allows isolating the photos and videos a profile has submitted. Either by clicking on the “Photos” or “Videos” tab at the top of the profile or by adding /photos or /videos to the profile URL’s end will get you there. Here it is possible to download all media relevant to the investigation and see which posts they’re associated with.

Posts to Groups

A user can also post directly into groups. Fortunately, when a user posts into groups, that post will appear on their timeline as well. This is a great way to identify what groups a user is a member of. Here’s an example from a user on the QAnon Gab group (A).

Once it is known that a user is a member of a group, it’s possible to continue to do network analysis from inside that group.



Posts tell you what groups it's posted to (A)

Hashtags

Gab's search engine specifies people, groups, or gabs (posts), but not hashtags. If searching for a hashtag using Gab's search engine, it will only show people or groups affiliated with that tag. Fortunately, their hashtag URL structure is universal, allowing one to search for any hashtag possible.

<https://gab.com/tags/{hashtag}>

By replacing "{hashtag}" with any hashtag, it is possible to view the most recent content to use it. Here's a sample post from #StoptheSteal, in relation to the riots at the United States Capitol on January 6, 2021 (A).

Using trendy hashtags in a search is likely to create a lot of noise to sift through; however, catching the tag early on can help identify virality points, early influencers, and potential misinformation campaigns. It can also serve as a means of actively monitoring an event or movement. Be sure to compare hashtags across social media platforms. For example, when a hashtag trends on Twitter, make sure to check it on Gab as well.



Multiple hashtags can be added to each post (A)

Group Pages

In addition to individual pages, Gab also allows users to create and participate in groups. Many of the same methods used to search for profiles can be used to search for Groups. For example, it works to use a search engine's index to create an advanced search, use Gab's search engine, or manipulate the URL of group pages to find more or quickly determine a group's age. Let's look at each of them individually.

Search Engines

site:gab.com/groups

Gab designates groups throughout their site by simply adding /groups/ to the URL; however, unlike profiles, groups don't have a username associated with the URL. Instead, they use a number system. While this makes it challenging to test usernames to check for groups, it is very easy to enumerate across different groups and determine which groups are older than others. Let's dive into an example.

QAnon

<https://gab.com/groups/393>

On Gab, the group from QAnon, a conspiracy theory followed by many involved in the US capitol riot, isn't designated as /groups/qanon. Instead, they use /393. If that were to be changed to /394, a different group would show up. Considering there are thousands of groups on Gab, 393 is a relatively older group. According to the group page, it was created on May 15, 2018 and has 123,700 members. It also links to 8kun.top and qanon.pub, two websites associated with the conspiracy.

site:gab.com/groups intitle:QAnon

When trying to find this group using Google's search index, adding the intitle:QAnon command after the site: operator will specify to look for groups titled QAnon. In addition to the QAnon post referenced above, the search will return /1383 and /1046 (QAnon 8chan, and QAnon Patriots respectively) among other groups listed.

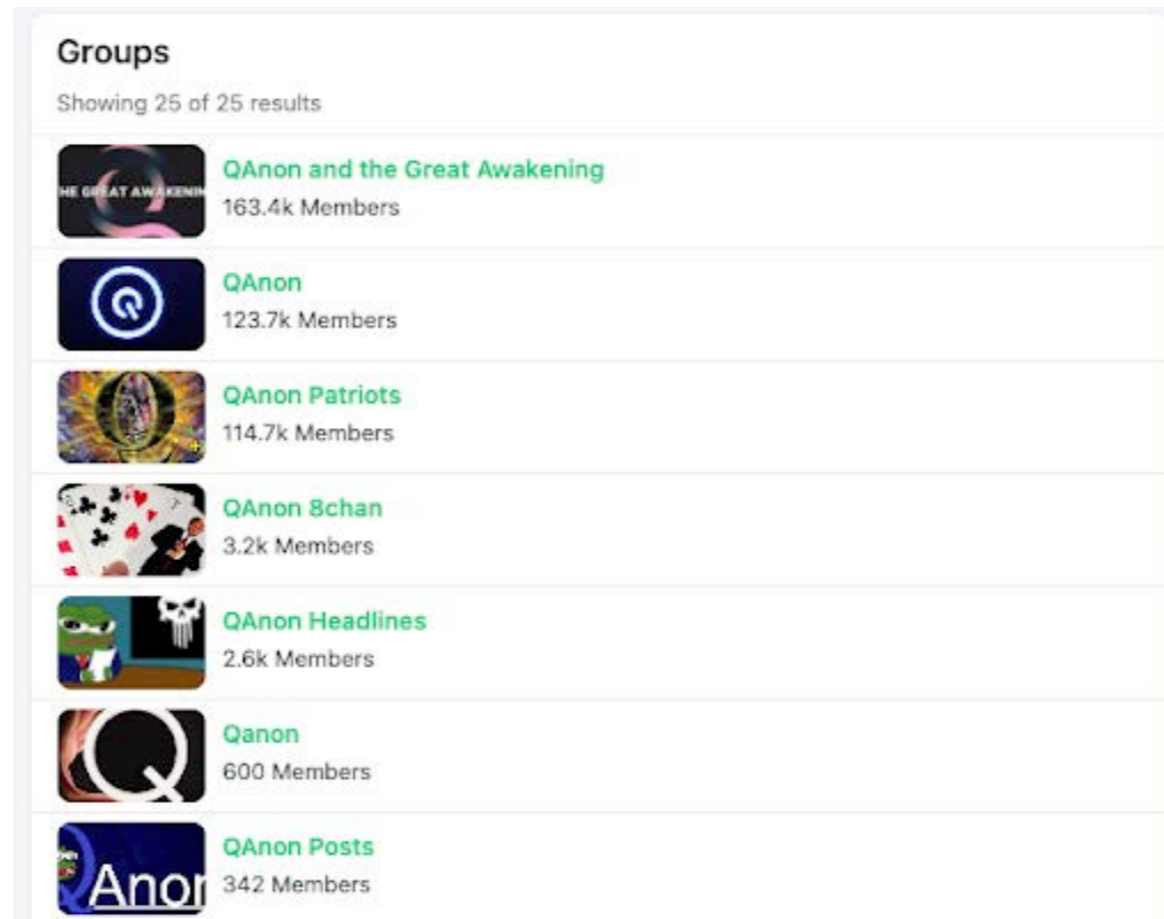
Gab's Search Engine

Similar to Google, Gab's search can be used to find specific groups that match keywords. Although Gab doesn't have an advanced search and has limited boolean logic available, the results shown will be the most up to date and won't rely on a search engine crawling that page as with Google. It will also show how many members are in each group.

The limitations of using Gab's search engine is the inability to do an advanced search or create filters to remove specific content. QAnon is not an ambiguous group name, but using Gab's search may show other groups that use more normal naming conventions.

Group URLs

While the URL of a group doesn't specify the group name, much can be learned about the group using them. As mentioned previously, it is possible to determine the group age by comparing it to other groups in question. Looking for groups created within a certain time range can be used to determine associations. Finally, using that group URL as a filter when querying a search engine like Google can help to find other associated groups. Here's you can see an example (A).



Search results for groups (A)

`site:gab.com/groups intitle:QAnon -inurl:393`

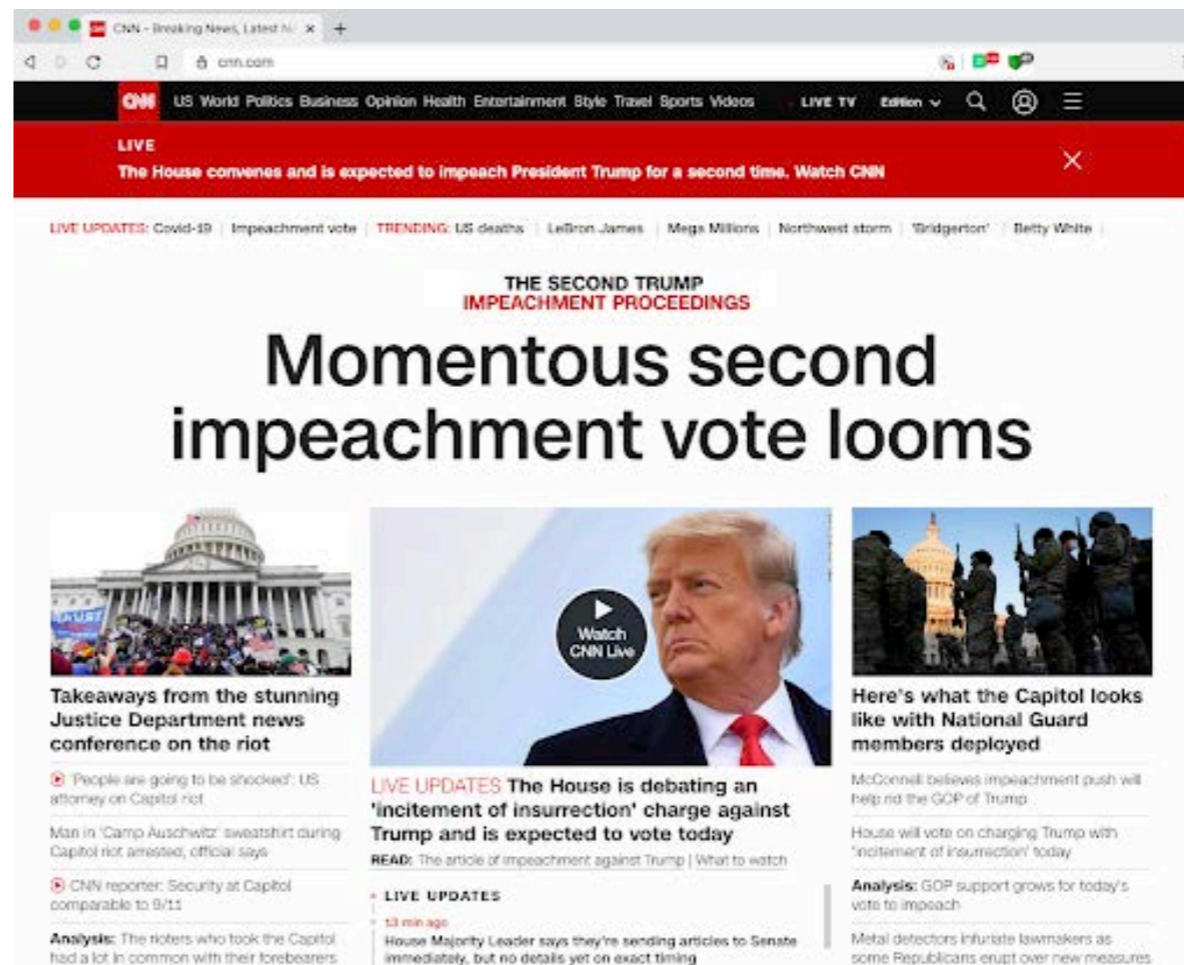
By adding that `-inurl:393` operator, it has removed the QAnon main group from the search results, leaving all other QAnon groups in the remainder.

DISSENTER

Uncover what can be discovered using Gab's tool, called Dissenter, which gives the ability to cross-post on mainstream social media.

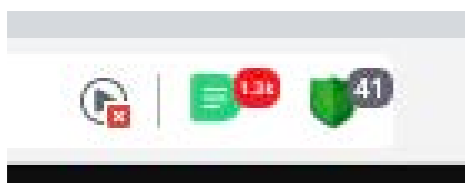
Early on in Gab's history, the platform received a lot of criticism about hosting extreme content. Users of the platform could not interact in comment boxes and on mainstream sites using the same language without removal. In response to this, Gab created Dissenter.

Dissenter gives Gab users the ability to comment on and discuss any content on the web without regular viewers being able to view it. It started off as a browser extension that would generate a pop up when users clicked on the extension allowing users to see comments from other Gab users on the page. Shortly after, Dissenter was removed from web browsers. In response to this action, Gab created its own web browser for Dissenter based on an open source framework (A). Operating similar to the Brave web browser, Dissenter maintains the functionality of "invisible comments" with their browser extension enabled by default on the Dissenter browser. Let's take a closer look.

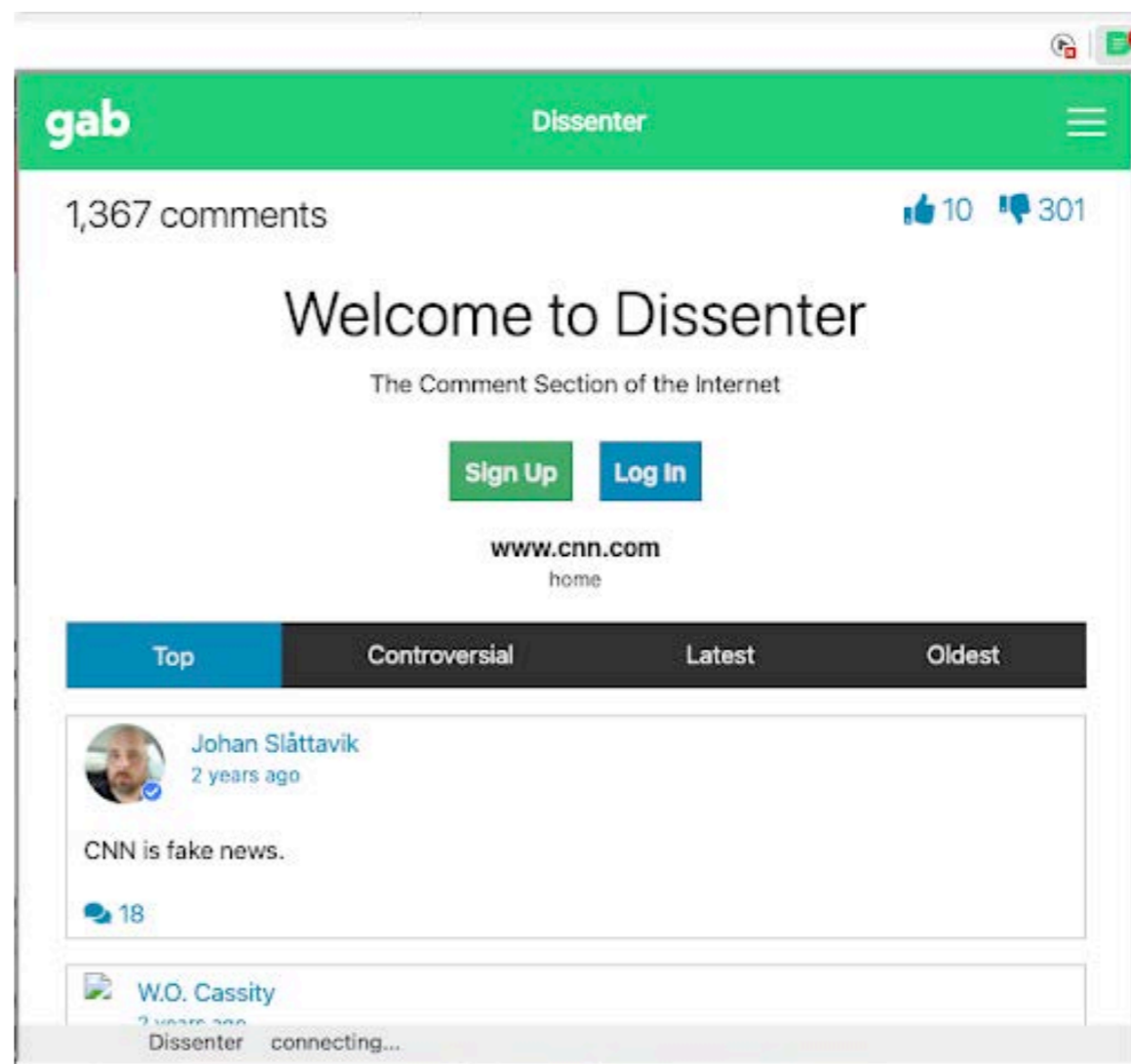


Dissenter is a web browser created by Gab (A)

At first glance, the browser looks very similar to the majority of mainstream browsers. The main difference is the default Dissenter browser extension. We suggest going into the extension settings to make sure it's enabled on all sites and shows when comments are visible on the page.



When the Dissenter extension is clicked on, a pop-up that looks like this is shown. Within the pop-up (A), all 1367 comments on the CNN homepage can be viewed. Within each comment, there is the functionality for conversation among Gab users.



All comments are available to view in the pop-up (A)

Some Dissenter profiles have hundreds of profiles and comments within them. Typically you'd have to expand all of them in order to do a full page screen capture to archive all evidence. Fortunately, Skopenow created a free tool you can use to expand an entire page with one click. Using this short javascript snippet, you can create a bookmarklet that will fully expand a Dissenter profile. Here's how to set it up.

Copy the following javascript code:

```
javascript:(function(){function openReplies(){var e=!1;$("div.comment-footer a").each(function(o,n){$(n).closest("div.comment-card").find(".comment-replies").first().hasClass("d-none")&&(n.click(),e=!0)});var o=$("div.comment-page-list button.text-secondary");o.length&&(o[0].click(),e=!0),e?setTimeout(openReplies,1e3):console.log("done")}openReplies();})();
```

Create a new bookmark on your browser.

Add bookmark

Name

URL

Cancel

Save

In the "Name" field, type in something like "Dissenter Expander". In the URL field, paste that javascript snippet. Save the bookmark and navigate to a Dissenter page.

Now, with one click, the entire profile will expand (A).

Because Dissenter operates from its own domain, it is nearly impossible to see these profiles and content indexed in search engines using gab.com. Instead, it is necessary to use dissenter.com. Let's break this down a bit further.

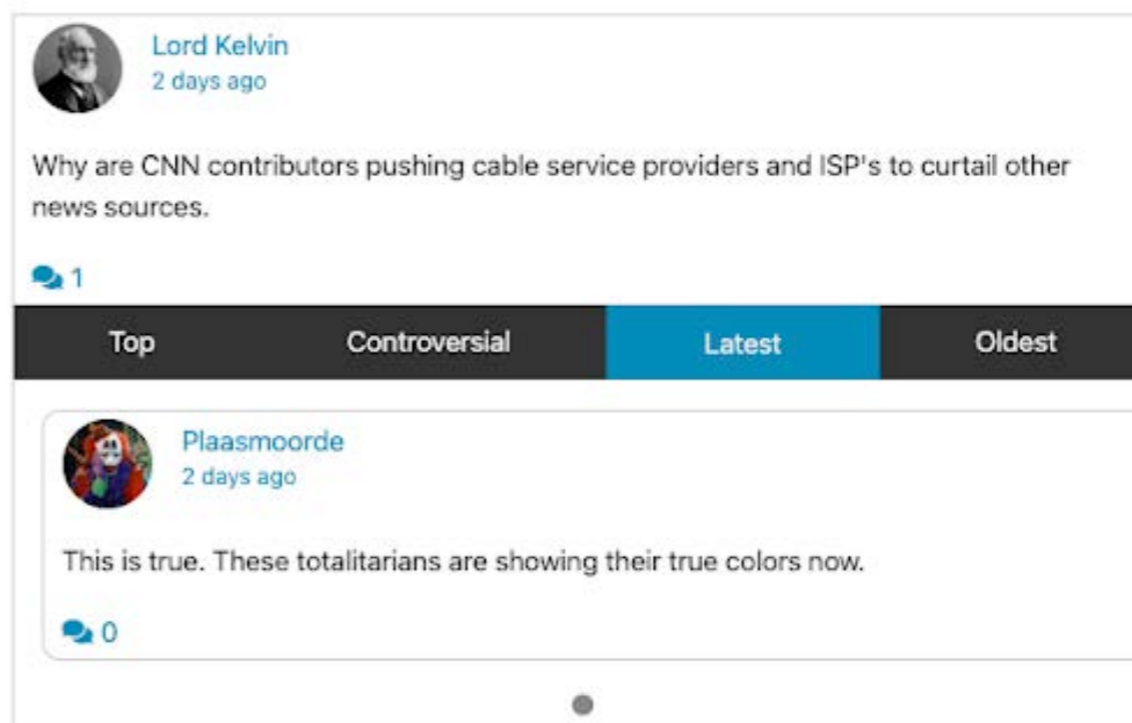
Search Engines

`site:dissenter.com/user`

All profiles on Dissenter have the uniform `dissenter.com/user` URL structure. This makes it easy to isolate on search engines. Applying additional filters to narrow down a search to look for specific users commenting on specific topics. Then, we can analyze those results to see what they're commenting on to establish a narrative. Here's an example:

`site:dissenter.com/user "{name}" OR "{display name}"`

When looking for a specific individual on Dissenter, appending the name or display name to the `site:dissenter.com/user` command will show all users that mention that name on their profile.



Using the java script allows the entire profile to expand (A)

site:dissenter.com/user intext:"qanon"

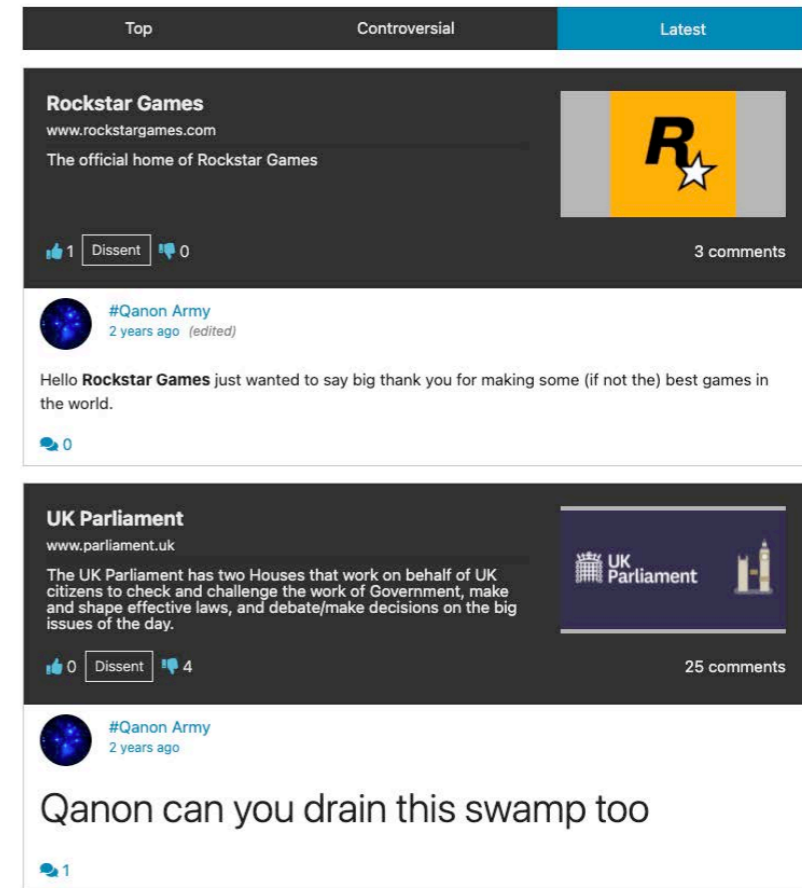
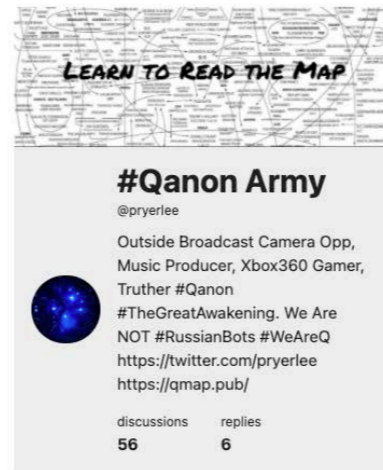
By using the intext:"qanon" operator, all results are filtered to only show Dissenter users that have used the word QAnon or mentioned it some other way in the body of the page. Replacing QAnon with any other query of interest is possible. Alternatively, it is possible to remove QAnon from the query by simply changing intext:"qanon" to -intext:"qanon". This allows removal of qanon results if they're not of interest. Let's look at an example to understand the search better.

<https://dissenter.com/user/pryerlee>

Using the query that specified qanon users on Dissenter, we've found this profile. Here we can see that they commented "Qanon can you drain this swamp too" on the UK Parliament page (A). If a comment is shown that includes other comments on it, you can quickly expand the network of, in this case, Qanon on Gab.

<https://dissenter.com/user/{username}>

Unlike Groups on Gab, Dissenter has alphanumeric usernames. This makes it easy to check if a Dissenter profile exists for a username in question. If one does, it is easy to find what content they consume, what they're saying about it, and others that share the same opinion or are possibly affiliated with the subject.



Dissenter allows cross posting from Gab to other platforms (A)

BROADENING THE INVESTIGATION

Understand how Skopenow can help your investigation go beyond social media and automate the processes outlined in this document.

Using a tool like Skopenow helps by automating each of these processes. Skopenow will conduct reverse username searches across all social media platforms and expand the search beyond social media using tens of thousands of publicly available sources.

Using the Association Search tool, Skopenow can identify connections between two individuals. Skopenow automates the collection of accounts and archives the followers and following lists for further use in your investigation. Lastly, Skopenow's automatic report builder will save hours per investigation, organizing the hundreds of data points collected in a clean and organized manner.

Contact us for a demo to see how Skopenow can streamline your OSINT workflow.