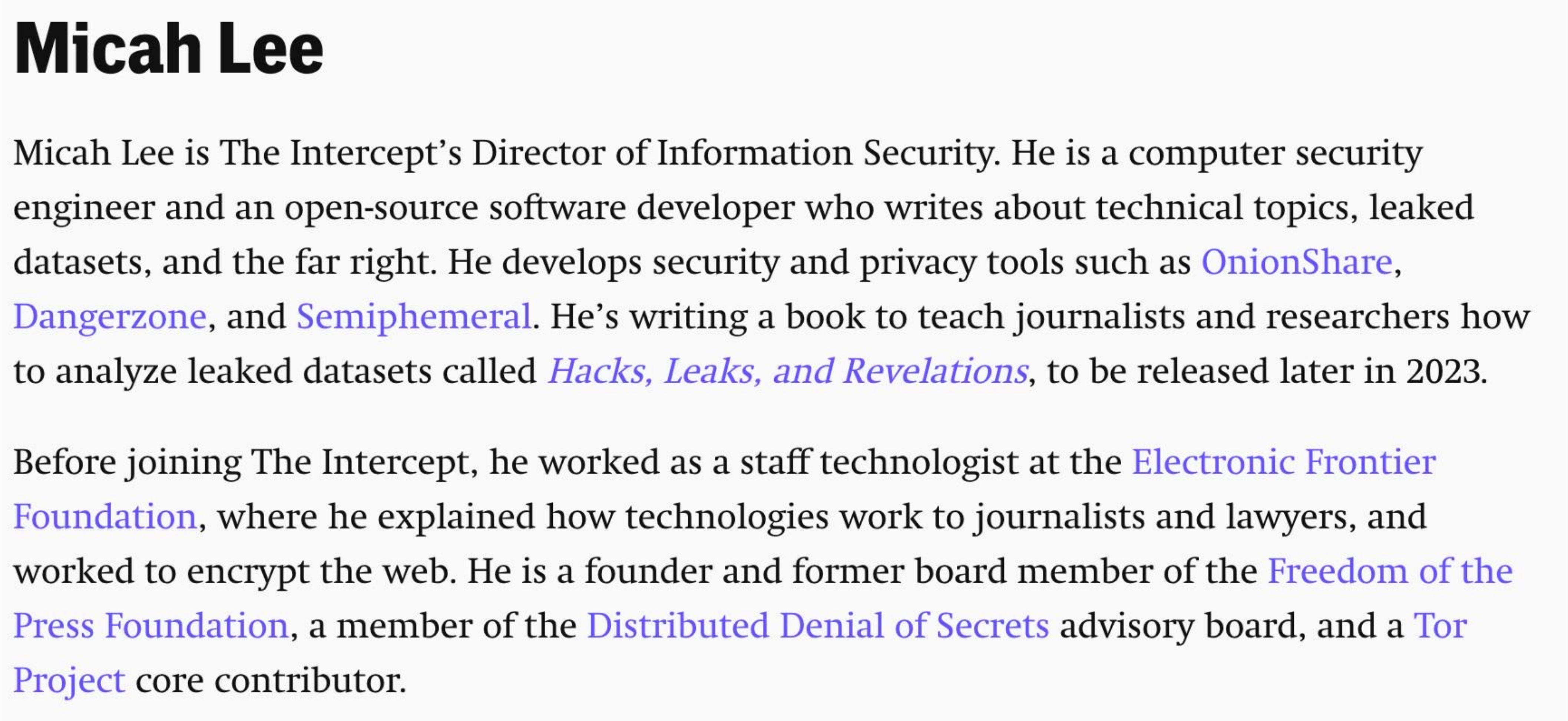
Hacks, Leaks, and Revelations█

A hands-on guide to analyzing hacked and leaked data

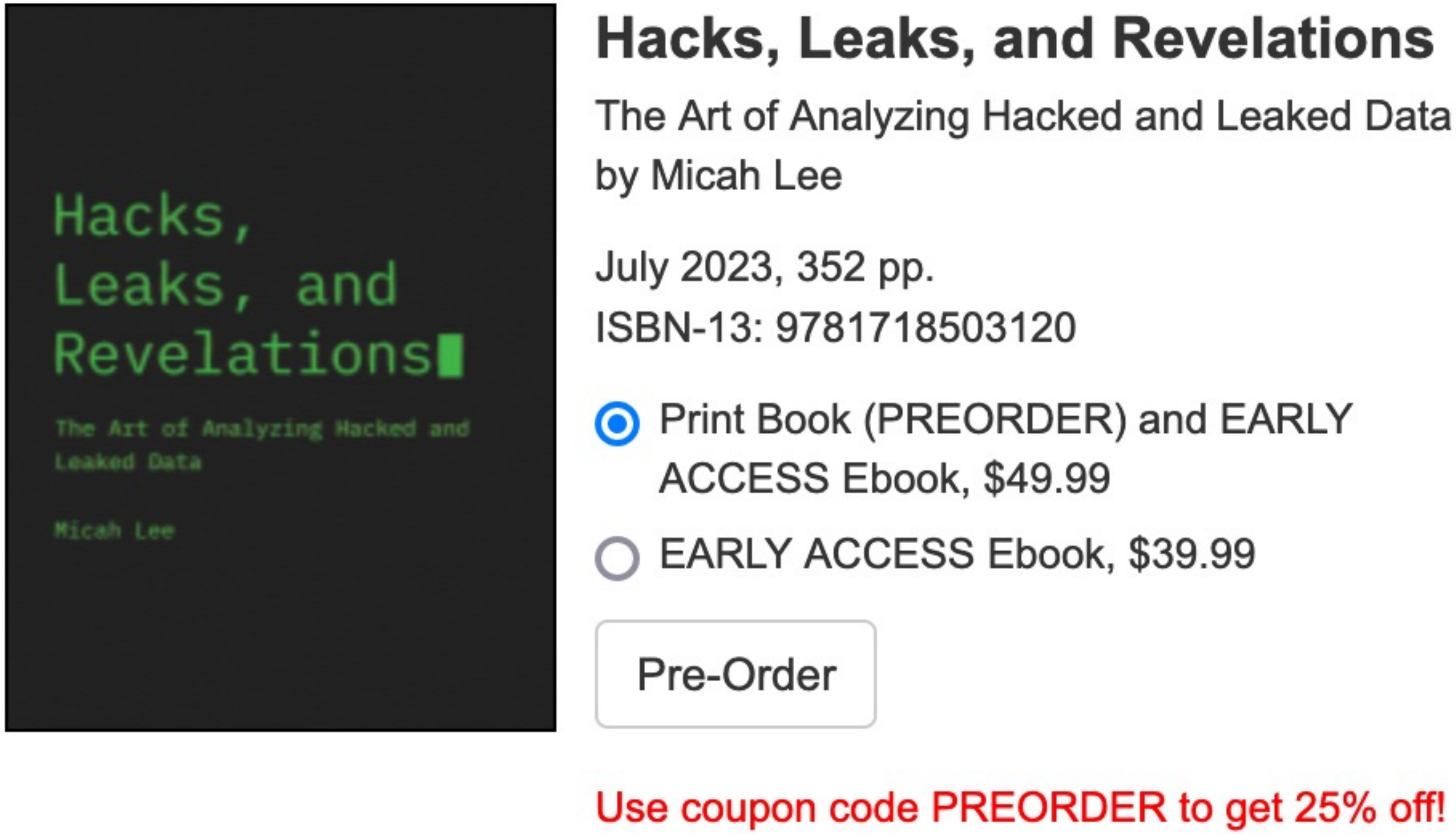


Micah Lee

Micah Lee is The Intercept's Director of Information Security. He is a computer security engineer and an open-source software developer who writes about technical topics, leaked datasets, and the far right. He develops security and privacy tools such as OnionShare, Dangerzone, and Semiphemeral. He's writing a book to teach journalists and researchers how to analyze leaked datasets called *Hacks, Leaks, and Revelations*, to be released later in 2023.

Before joining The Intercept, he worked as a staff technologist at the Electronic Frontier Foundation, where he explained how technologies work to journalists and lawyers, and worked to encrypt the web. He is a founder and former board member of the Freedom of the Press Foundation, a member of the Distributed Denial of Secrets advisory board, and a Tor Project core contributor.

Mastodon: @micahflee@infosec.social | micah@micahflee.com



Hacks, Leaks, and Revelations

The Art of Analyzing Hacked and Leaked Data
by Micah Lee

July 2023, 352 pp.
ISBN-13: 9781718503120

● Print Book (PREORDER) and EARLY ACCESS Ebook, $49.99

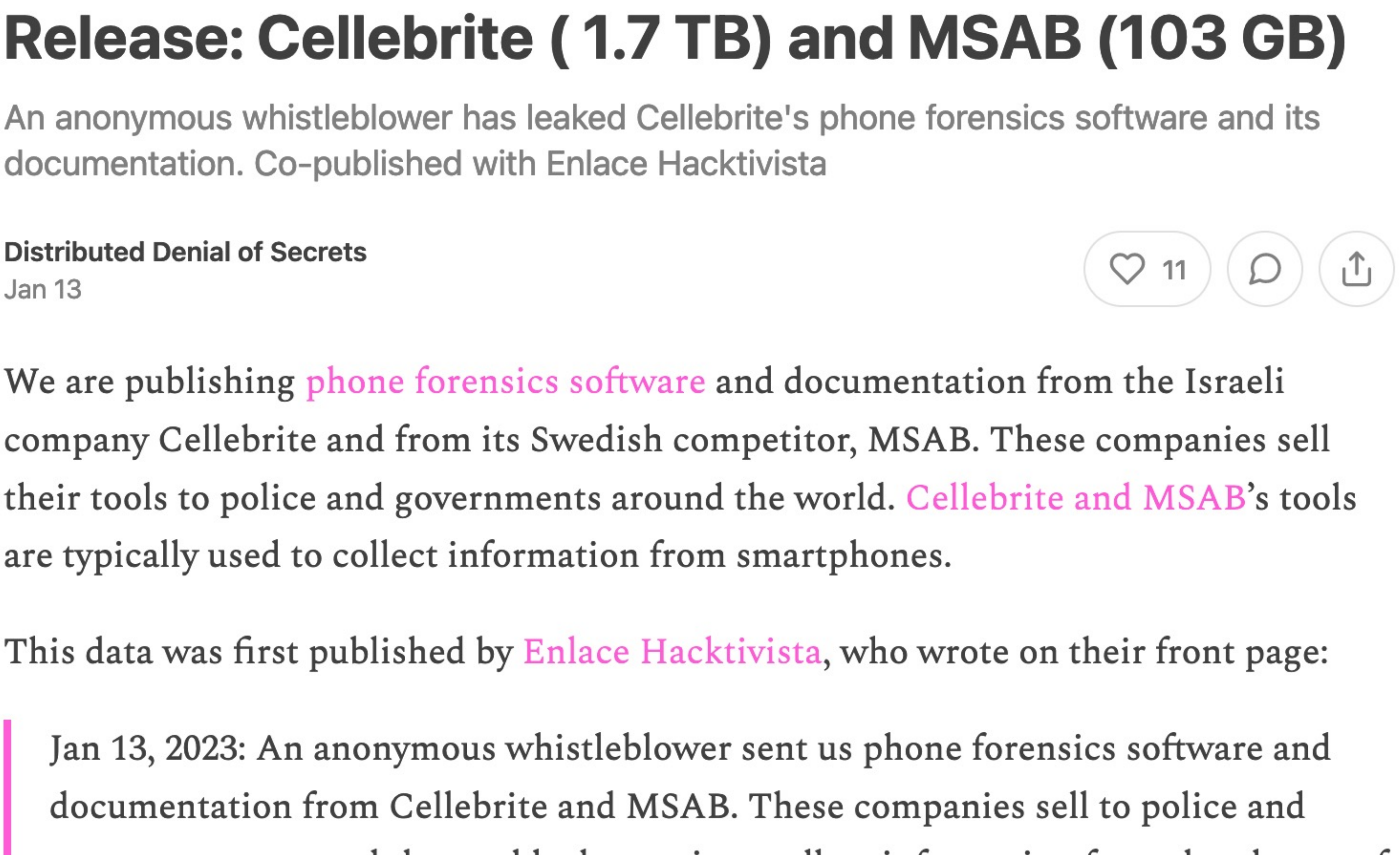
○ EARLY ACCESS Ebook, $39.99

Use coupon code PREORDER to get 25% off!

https://nostarch.com/hacks-leaks-and-revelations

The Internet is Overflowing in Hacked and Leaked Datasets

Just in the first two and a half months of 2023…



Release: Cellebrite (1.7 TB) and MSAB (103 GB)

An anonymous whistleblower has leaked Cellebrite's phone forensics software and its documentation. Co-published with Enlace Hacktivista

Distributed Denial of Secrets
Jan 13

We are publishing phone forensics software and documentation from the Israeli company Cellebrite and from its Swedish competitor, MSAB. These companies sell their tools to police and governments around the world. Cellebrite and MSAB's tools are typically used to collect information from smartphones.

This data was first published by Enlace Hacktivista, who wrote on their front page:

> Jan 13, 2023: An anonymous whistleblower sent us phone forensics software and documentation from Cellebrite and MSAB. These companies sell to police and

Limited distribution: Fundação Nacional de Artes (302 GB)

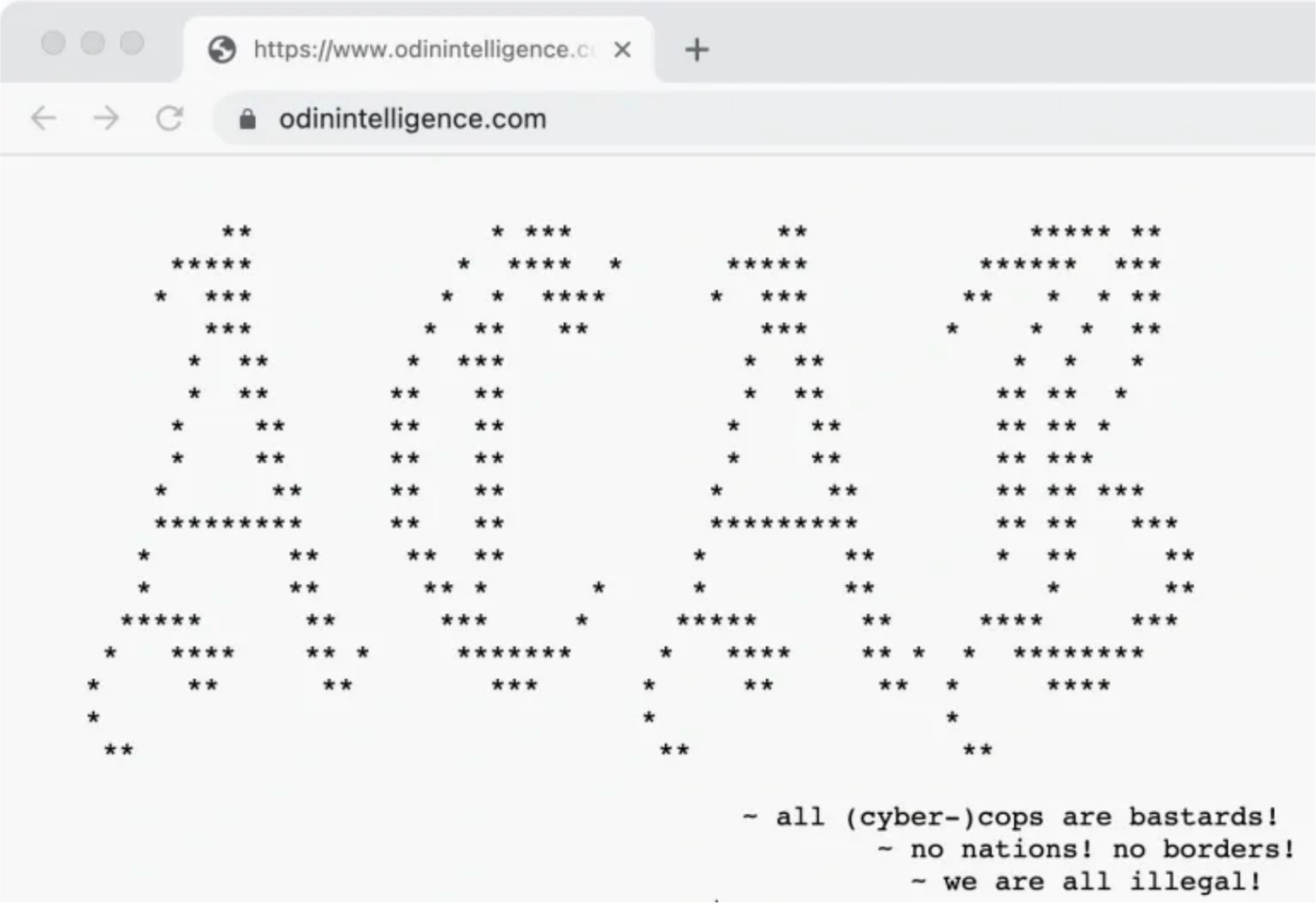
Emails from 2011 to 2022 of Brazil's national arts foundation, including the tumultuous Bolsonaro years. Funarte develops policies to promote the arts.

Distributed Denial of Secrets
Jan 14

Limited distribution: ODIN Intelligence (19 GB)

A contractor that works for police agencies had its website defaced as reported by Techcrunch

Distributed Denial of Secrets
Jan 21



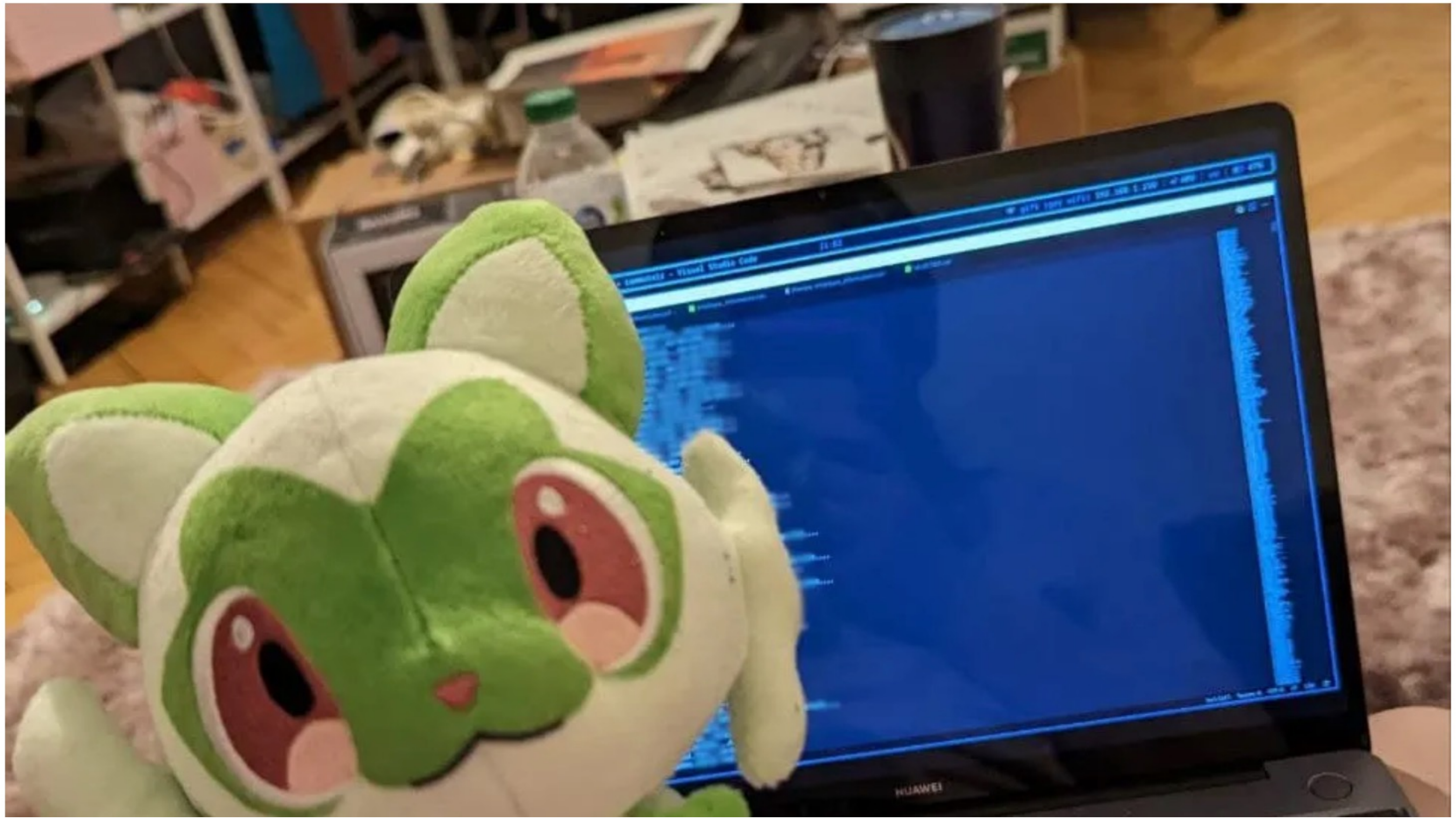
```
~ all (cyber-)cops are bastards!
    ~ no nations! no borders!
     ~ we are all illegal!
```

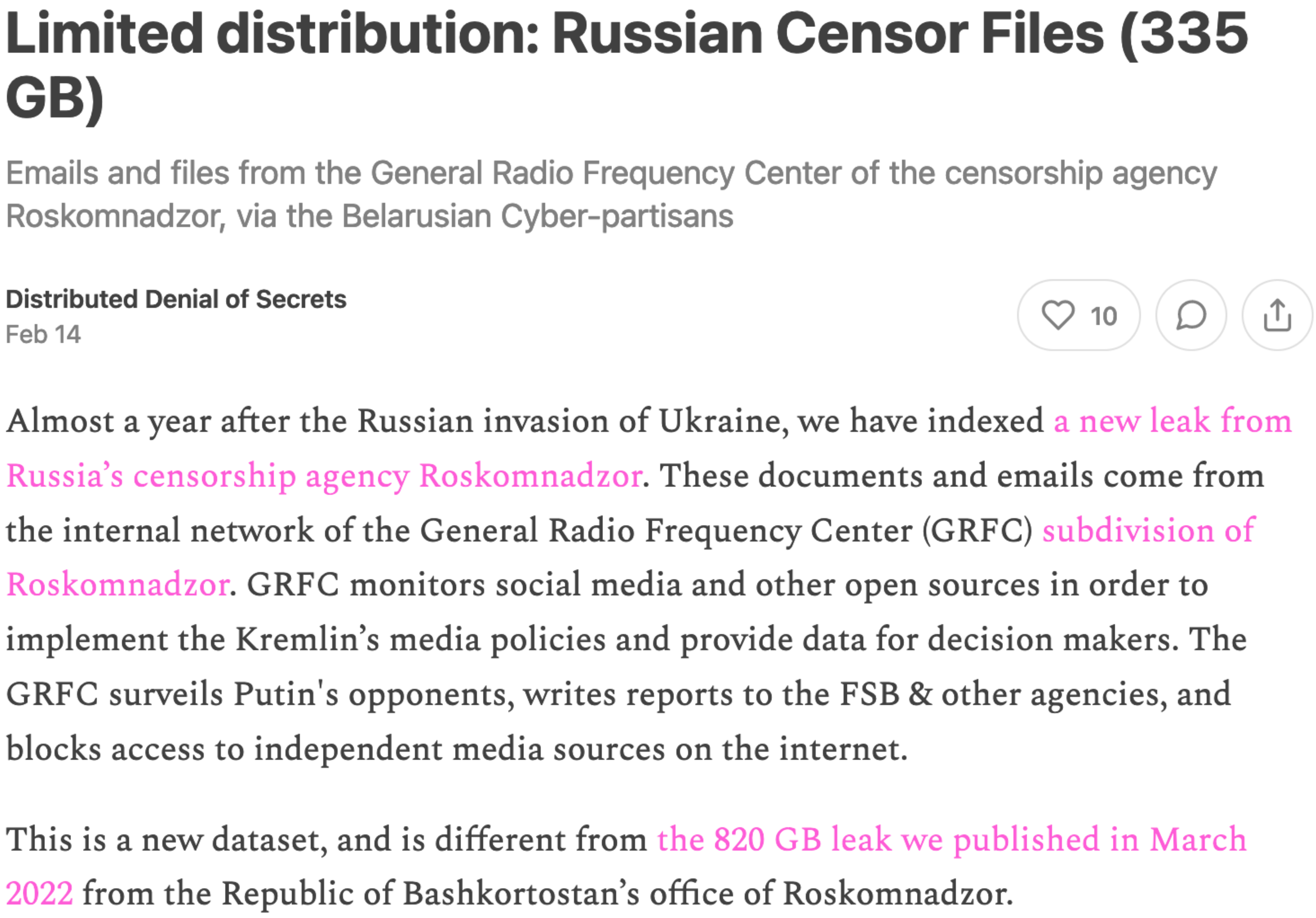
Limited distribution: No Fly list (90 MB)

A 2019 version of the United States' No Fly List. The TSA's terrorist screening list has more than 1.5 million names including 3000 minors

Distributed Denial of Secrets
Jan 27

♡ 9





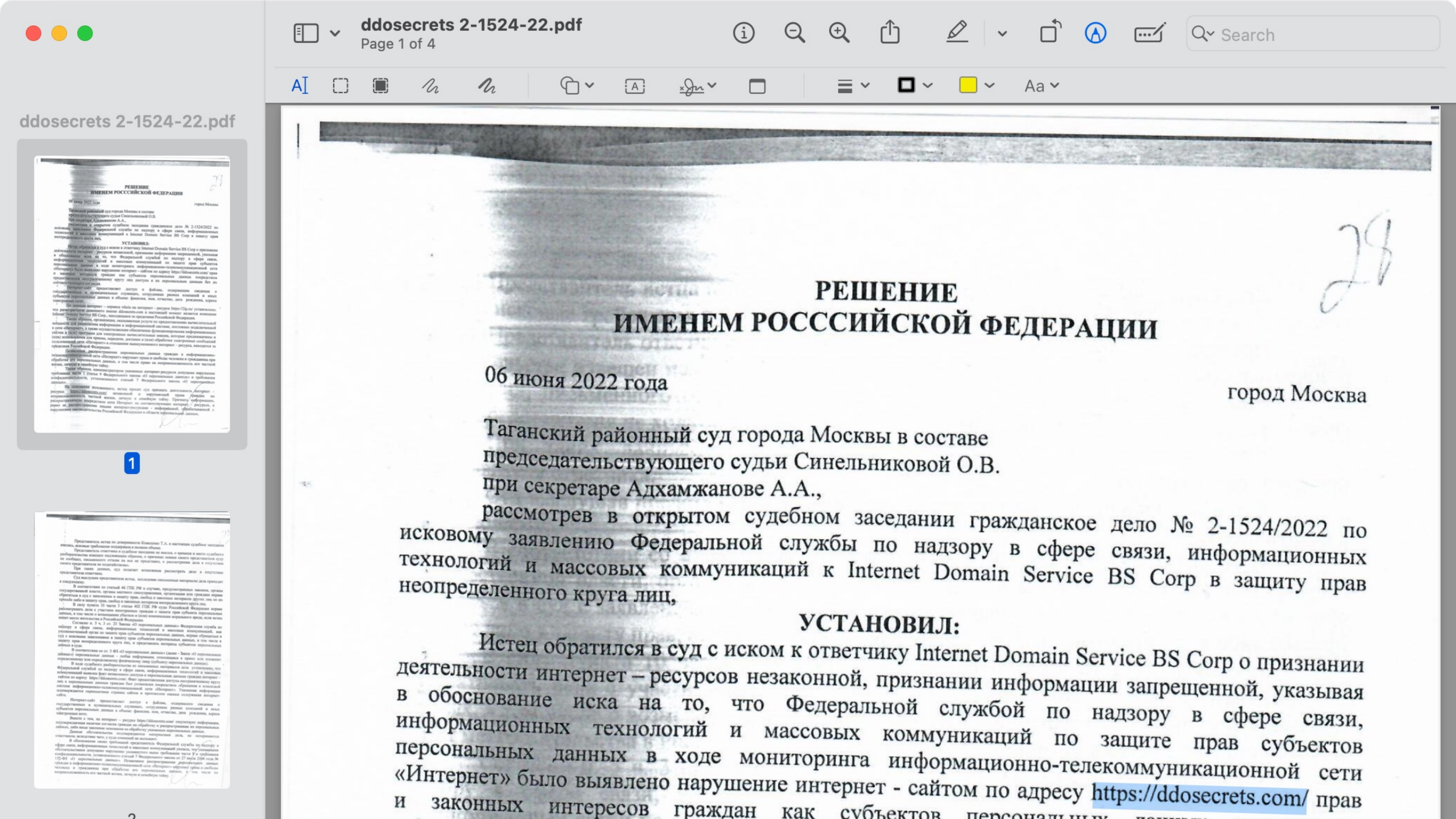
Limited distribution: Russian Censor Files (335 GB)

Emails and files from the General Radio Frequency Center of the censorship agency Roskomnadzor, via the Belarusian Cyber-partisans

Distributed Denial of Secrets
Feb 14

Almost a year after the Russian invasion of Ukraine, we have indexed a new leak from Russia’s censorship agency Roskomnadzor. These documents and emails come from the internal network of the General Radio Frequency Center (GRFC) subdivision of Roskomnadzor. GRFC monitors social media and other open sources in order to implement the Kremlin’s media policies and provide data for decision makers. The GRFC surveils Putin's opponents, writes reports to the FSB & other agencies, and blocks access to independent media sources on the internet.

This is a new dataset, and is different from the 820 GB leak we published in March 2022 from the Republic of Bashkortostan’s office of Roskomnadzor.



28

РЕШЕНИЕ
ИМЕНЕМ РОСССИЙСКОЙ ФЕДЕРАЦИИ

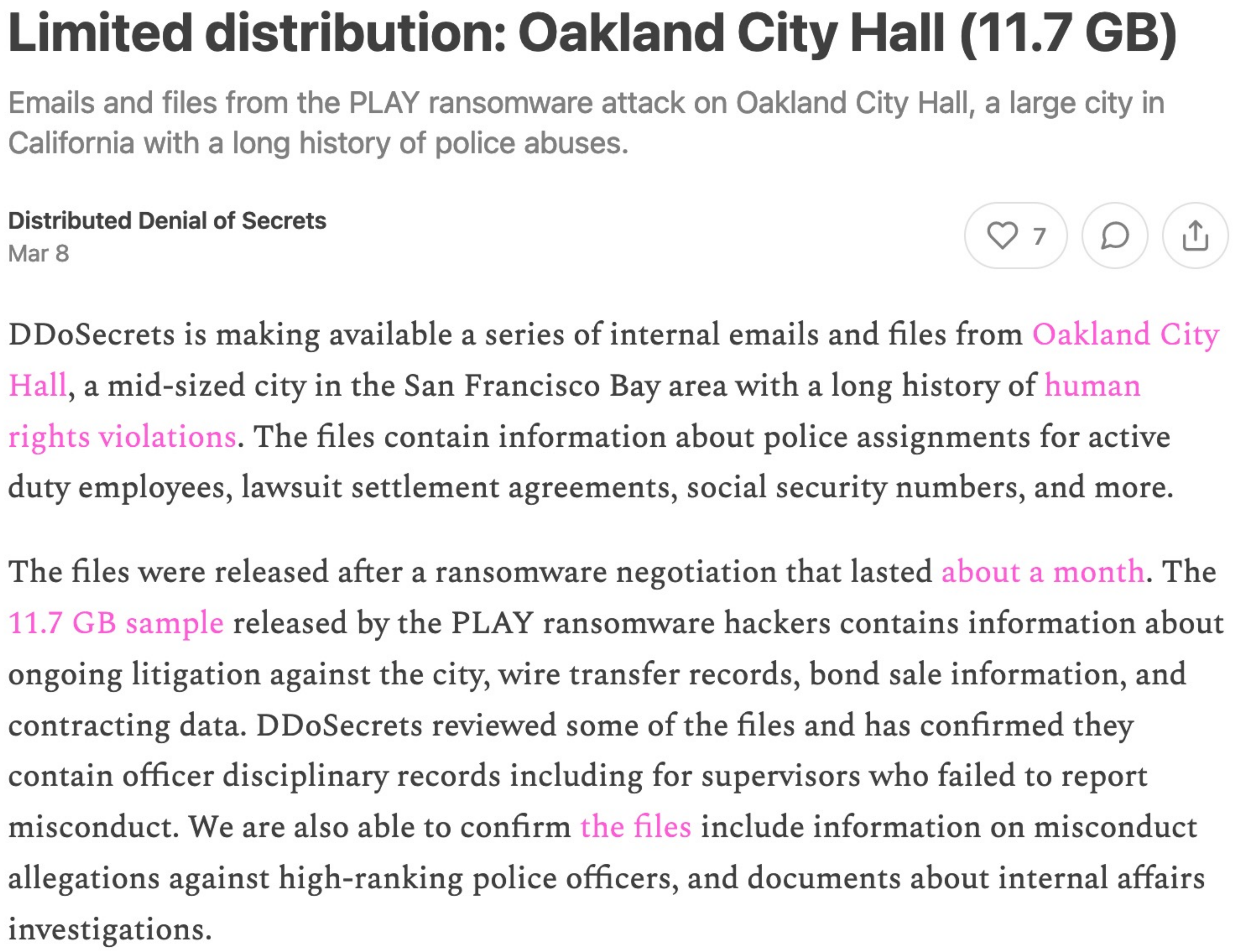
06 июня 2022 года город Москва

Таганский районный суд города Москвы в составе
председательствующего судьи Синельниковой О.В.
при секретаре Адхамжанове А.А.,

рассмотрев в открытом судебном заседании гражданское дело № 2-1524/2022 по исковому заявлению Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций к Internet Domain Service BS Corp в защиту прав неопределенного круга лиц,

УСТАНОВИЛ:

Истец обратился в суд с иском к ответчику Internet Domain Service BS Corp о признании деятельности интернет – ресурсов незаконной, признании информации запрещенной, указывая в обоснование иска на то, что Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций по защите прав субъектов персональных данных в ходе мониторинга информационно-телекоммуникационной сети «Интернет» было выявлено нарушение интернет - сайтом по адресу https://ddosecrets.com/ прав и законных интересов граждан как субъектов персональных данных



Limited distribution: Oakland City Hall (11.7 GB)

Emails and files from the PLAY ransomware attack on Oakland City Hall, a large city in California with a long history of police abuses.

Distributed Denial of Secrets
Mar 8

DDoSecrets is making available a series of internal emails and files from Oakland City Hall, a mid-sized city in the San Francisco Bay area with a long history of human rights violations. The files contain information about police assignments for active duty employees, lawsuit settlement agreements, social security numbers, and more.

The files were released after a ransomware negotiation that lasted about a month. The 11.7 GB sample released by the PLAY ransomware hackers contains information about ongoing litigation against the city, wire transfer records, bond sale information, and contracting data. DDoSecrets reviewed some of the files and has confirmed they contain officer disciplinary records including for supervisors who failed to report misconduct. We are also able to confirm the files include information on misconduct allegations against high-ranking police officers, and documents about internal affairs investigations.

Source Protection, Digital Security, and Acquiring Datasets

Protecting Your Sources and Yourself

- Protecting sources by minimizing the data trail
- Securely storing datasets
- **Verifying that data is authentic using OSINT**
- Deciding what to redact
- Using a password manager, using disk encryption, and opening sketchy documents using Dangerzone
- Talking to sources using Signal

Acquiring Datasets

- Public datasets from DDoSecrets
- Downloading public datasets using BitTorrent
- Various ways to securely get datasets directly from sources

The Command Line Interface

Filtering for Documents Mentioning Antifa

You’ll start by grepping our list of filenames for files that include *antifa* in their names. (Later on you’ll search the content of files, but searching filenames is quicker and provides a good starting point.) From the *BlueLeaks-extracted* folder, search the *BlueLeaks-filenames.txt* file that you created in Homework 4-2 by running:

```
cat ../BlueLeaks-filenames.txt | grep antifa
```

This command pipes the output of `cat ../BlueLeaks-filenames.txt` (which is a list of a million filenames) as input into `grep antifa`. Essentially, it filters that huge list of filenames to only show you ones that include the word *antifa*.

That command returns no results. Since the `grep` command is case-sensitive, try again using the `-i`, or `--ignore-case`, argument:

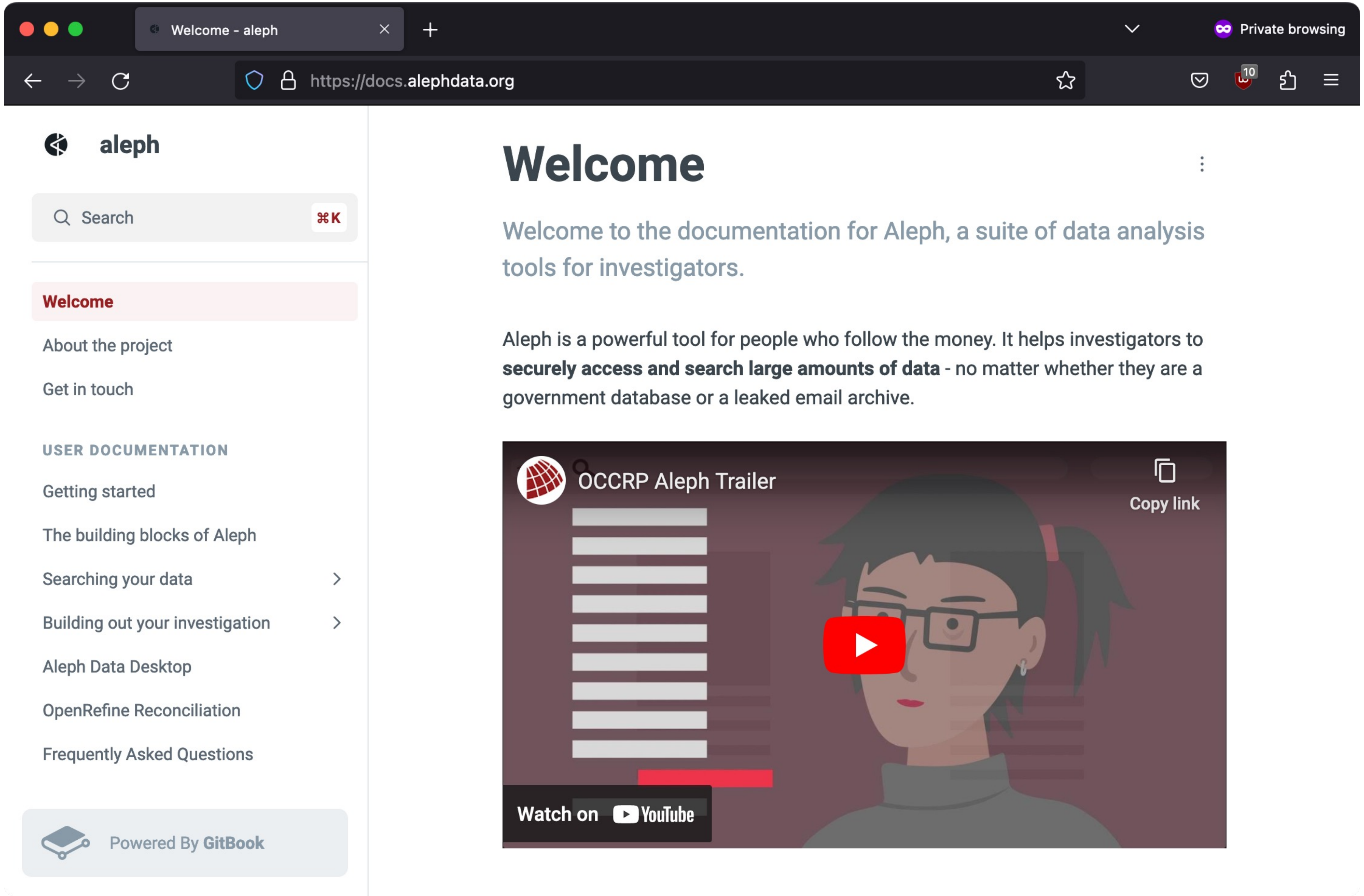
```
cat ../BlueLeaks-filenames.txt | grep -i antifa
```

When I run this command on my macOS computer, this is the output:

```
./ociac/files/EBAT1/U-FOUO_CFIX__OCIAC_JRA_DVE Use of Social Media_ANTIFA_ANTI-ANTIFA
MOVEMENTS.pdf
./arictexas/files/DDF/ARIC-LES - Situational Awareness - Antifa Activity.pdf
./arictexas/files/DDF/SWTFC-LES - Situational Awareness - ANTIFA Event Notification.pdf
./arictexas/files/DPI/ARIC-LES - Situational Awareness - Antifa Activity.png
./arictexas/files/DPI/SWTFC-LES - Situational Awareness - ANTIFA Event Notification.png
./dediac/files/DDF/ANTIFA - Fighting in the Streets.pdf
./dediac/files/DDF/ANTIFA Sub Groups and Indicators - LES.pdf
./dediac/files/DDF/
FBI_PH_SIR_Tactics_and_Targets_Identified_for_4_November_2017_ANTIFA_Rally_in_Philadelphia_PA-
2.pdf
./dediac/files/EBAT1/ANTIFA - Fighting in the Streets.pdf
./dediac/files/EBAT1/ANTIFA Sub Groups and Indicators - LES.pdf
./dediac/files/DPI/ANTIFA - Fighting in the Streets.png
./dediac/files/DPI/
FBI_PH_SIR_Tactics_and_Targets_Identified_for_4_November_2017_ANTIFA_Rally_in_Philadelphia_PA-
2.png
```

This command returns 12 results, all files that have the term *antifa* in their filenames. The `grep` command might highlight your search terms in each line of output by coloring them differently; I've highlighted them in this output by boldfacing them. Try reading some of the documents in this list.

Making Datasets Searchable with Aleph

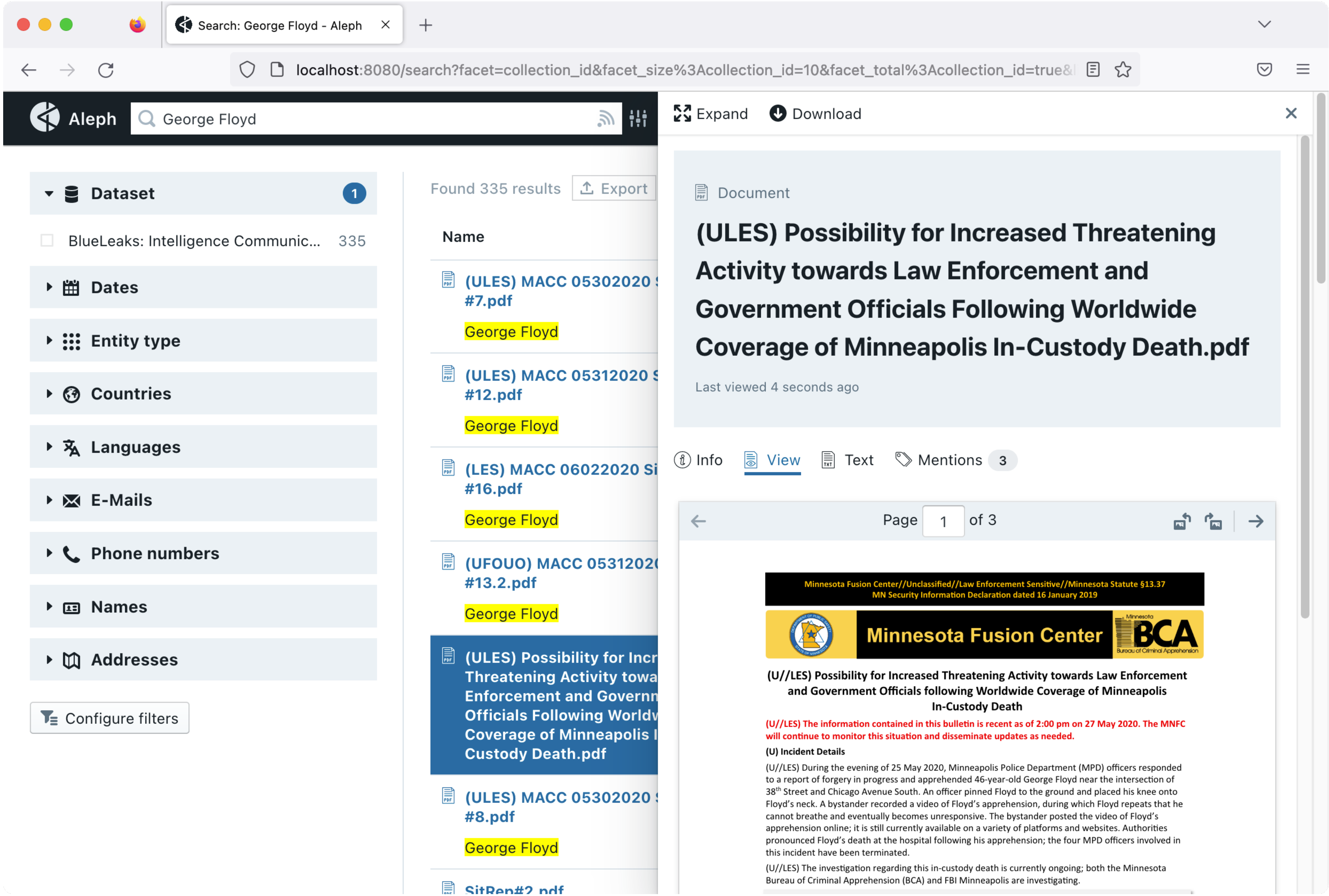


Welcome

Welcome to the documentation for Aleph, a suite of data analysis tools for investigators.

Aleph is a powerful tool for people who follow the money. It helps investigators to **securely access and search large amounts of data** - no matter whether they are a government database or a leaked email archive.

https://docs.alephdata.org/ | https://data.occrp.org/



BlueLeaks: Intelligence Communic... 335

Found 335 results

(ULES) MACC 05302020 S
#7.pdf
George Floyd

(ULES) MACC 05312020 S
#12.pdf
George Floyd

(LES) MACC 06022020 Si
#16.pdf
George Floyd

(UFOUO) MACC 0531202
#13.2.pdf
George Floyd

(ULES) Possibility for Incr
Threatening Activity towa
Enforcement and Govern
Officials Following Worldv
Coverage of Minneapolis I
Custody Death.pdf

(ULES) MACC 05302020 S
#8.pdf
George Floyd

SitRep#2.pdf

Document

(ULES) Possibility for Increased Threatening Activity towards Law Enforcement and Government Officials Following Worldwide Coverage of Minneapolis In-Custody Death.pdf

Last viewed 4 seconds ago

Minnesota Fusion Center//Unclassified//Law Enforcement Sensitive//Minnesota Statute §13.37
MN Security Information Declaration dated 16 January 2019

Minnesota Fusion Center

Minnesota BCA Bureau of Criminal Apprehension

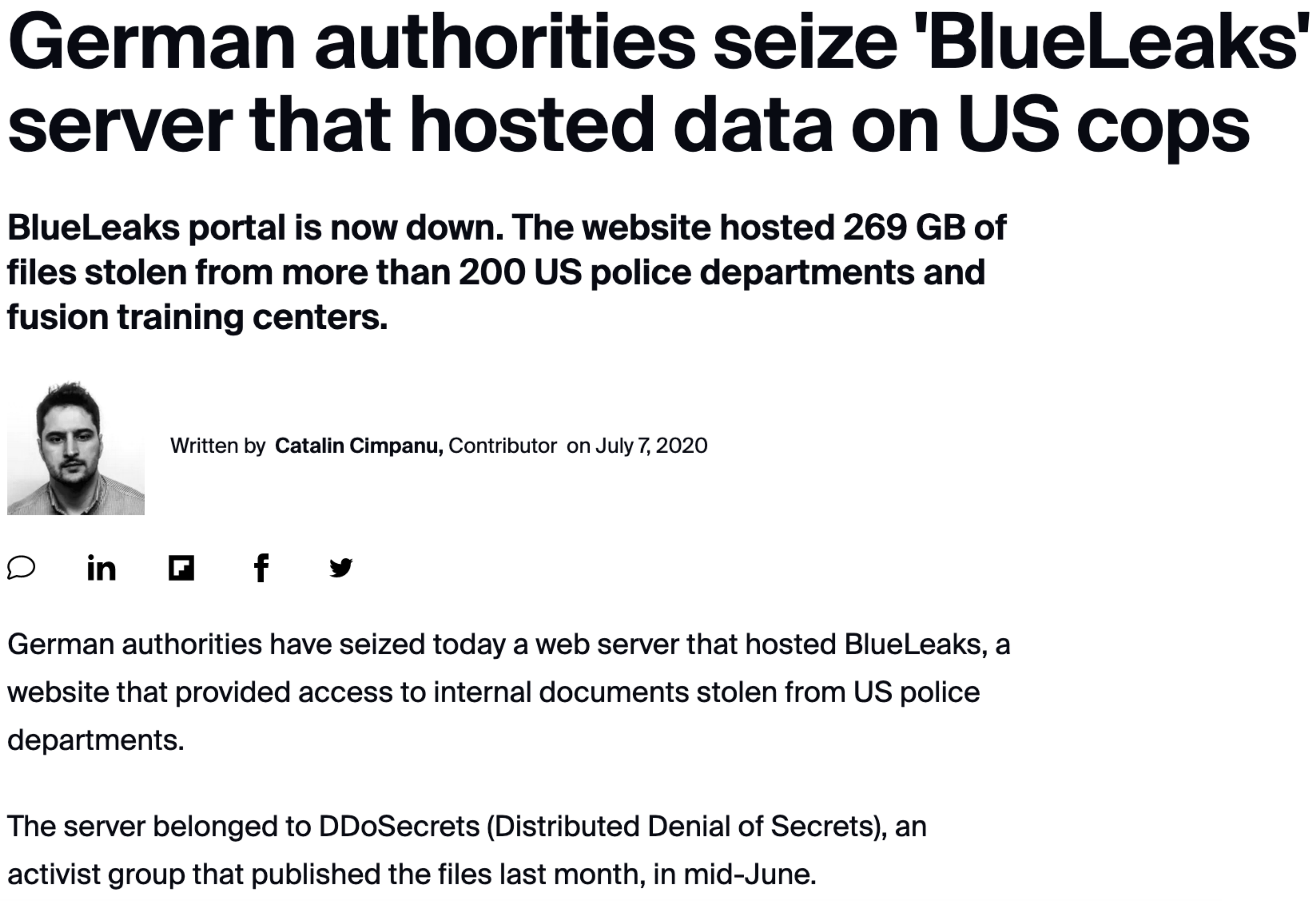
(U//LES) Possibility for Increased Threatening Activity towards Law Enforcement and Government Officials following Worldwide Coverage of Minneapolis In-Custody Death

(U//LES) The information contained in this bulletin is recent as of 2:00 pm on 27 May 2020. The MNFC will continue to monitor this situation and disseminate updates as needed.

(U) Incident Details

(U//LES) During the evening of 25 May 2020, Minneapolis Police Department (MPD) officers responded to a report of forgery in progress and apprehended 46-year-old George Floyd near the intersection of 38th Street and Chicago Avenue South. An officer pinned Floyd to the ground and placed his knee onto Floyd's neck. A bystander recorded a video of Floyd's apprehension, during which Floyd repeats that he cannot breathe and eventually becomes unresponsive. The bystander posted the video of Floyd's apprehension online; it is still currently available on a variety of platforms and websites. Authorities pronounced Floyd's death at the hospital following his apprehension; the four MPD officers involved in this incident have been terminated.

(U//LES) The investigation regarding this in-custody death is currently ongoing; both the Minnesota Bureau of Criminal Apprehension (BCA) and FBI Minneapolis are investigating.



German authorities seize 'BlueLeaks' server that hosted data on US cops

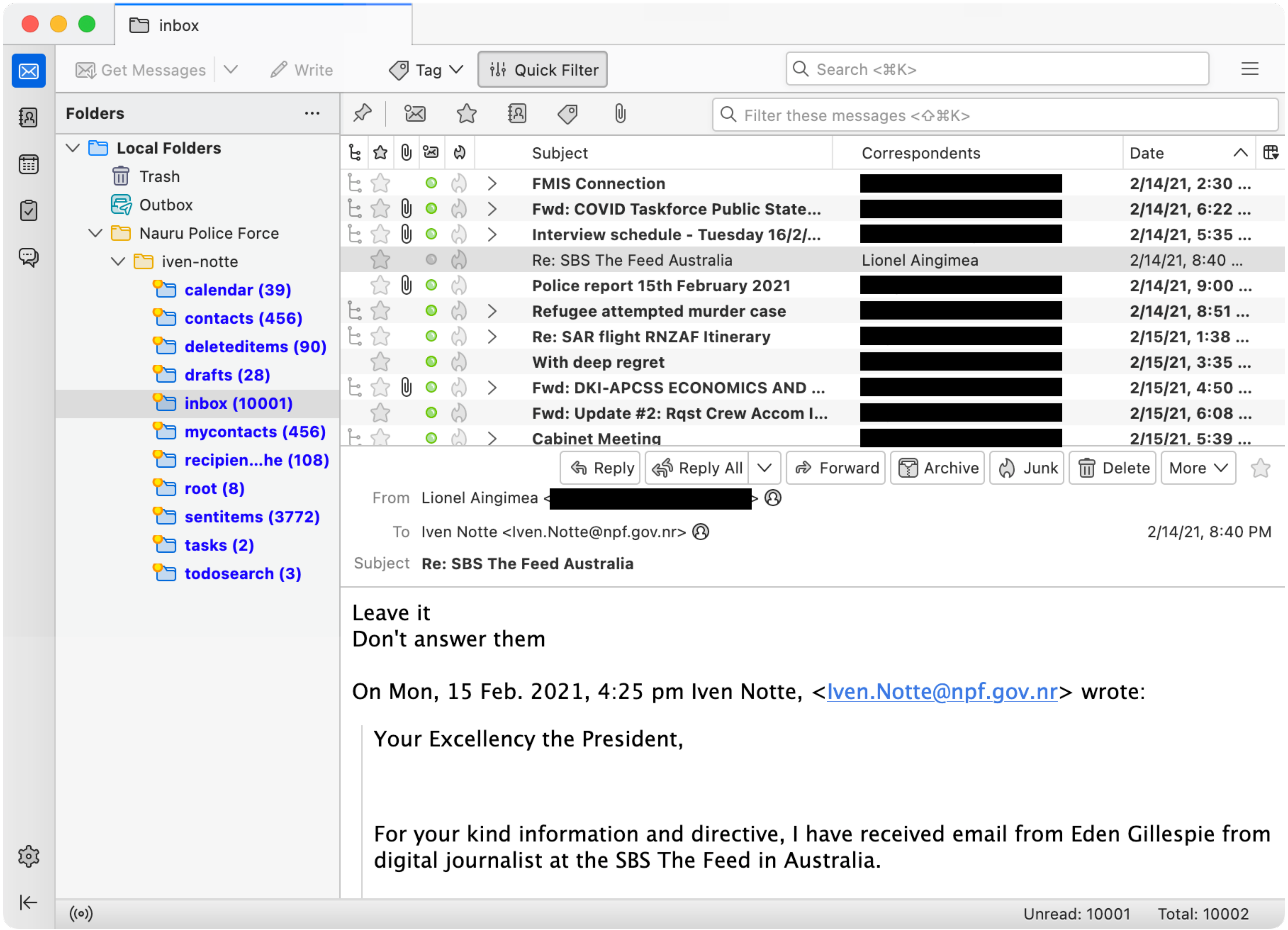
BlueLeaks portal is now down. The website hosted 269 GB of files stolen from more than 200 US police departments and fusion training centers.

Written by **Catalin Cimpanu,** Contributor on July 7, 2020

German authorities have seized today a web server that hosted BlueLeaks, a website that provided access to internal documents stolen from US police departments.

The server belonged to DDoSecrets (Distributed Denial of Secrets), an activist group that published the files last month, in mid-June.

Reading Other People’s Email



Subject	Correspondents	Date
FMIS Connection	[redacted]	2/14/21, 2:30 ...
Fwd: COVID Taskforce Public State...	[redacted]	2/14/21, 6:22 ...
Interview schedule - Tuesday 16/2/...	[redacted]	2/14/21, 5:35 ...
Re: SBS The Feed Australia	Lionel Aingimea	2/14/21, 8:40 ...
Police report 15th February 2021	[redacted]	2/14/21, 9:00 ...
Refugee attempted murder case	[redacted]	2/14/21, 8:51 ...
Re: SAR flight RNZAF Itinerary	[redacted]	2/15/21, 1:38 ...
With deep regret	[redacted]	2/15/21, 3:35 ...
Fwd: DKI-APCSS ECONOMICS AND ...	[redacted]	2/15/21, 4:50 ...
Fwd: Update #2: Rqst Crew Accom I...	[redacted]	2/15/21, 6:08 ...
Cabinet Meeting	[redacted]	2/15/21, 5:39 ...

From Lionel Aingimea <[redacted]>

To Iven Notte <Iven.Notte@npf.gov.nr> 2/14/21, 8:40 PM

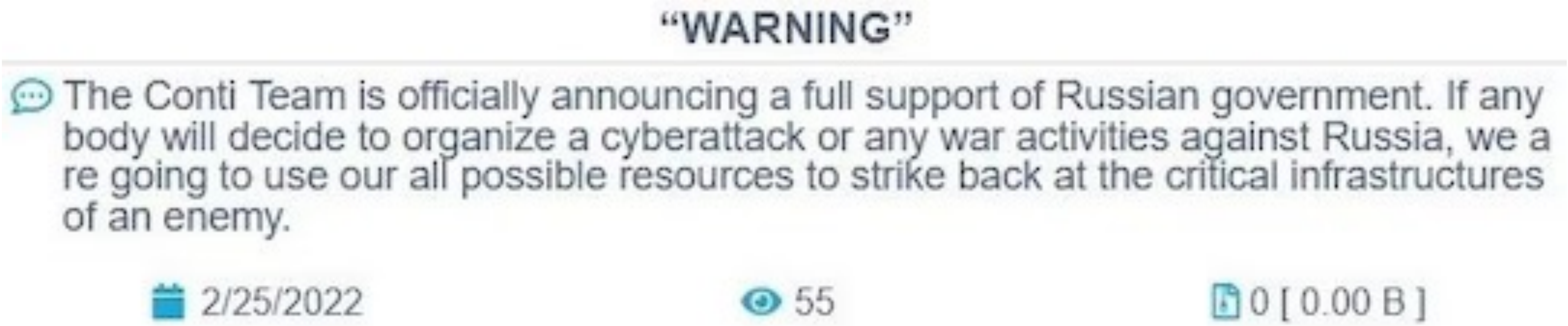
Subject **Re: SBS The Feed Australia**

Leave it
Don't answer them

On Mon, 15 Feb. 2021, 4:25 pm Iven Notte, <Iven.Notte@npf.gov.nr> wrote:

> Your Excellency the President,
>
> For your kind information and directive, I have received email from Eden Gillespie from digital journalist at the SBS The Feed in Australia.

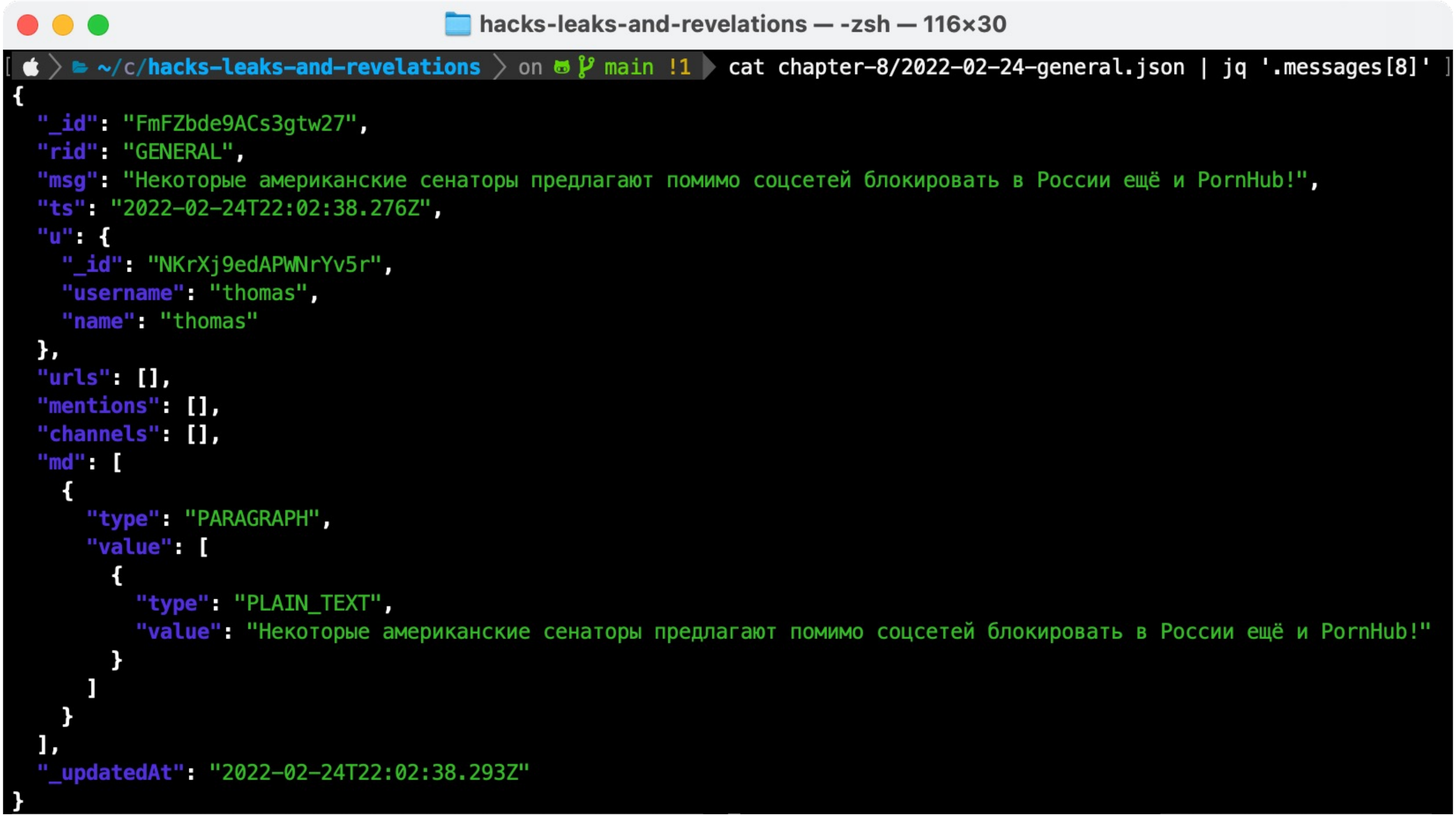
Data Analysis with Python



“WARNING”

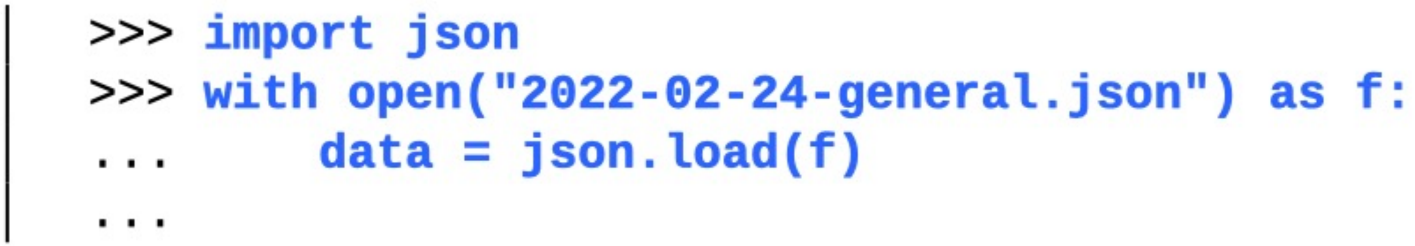
The Conti Team is officially announcing a full support of Russian government. If any body will decide to organize a cyberattack or any war activities against Russia, we a re going to use our all possible resources to strike back at the critical infrastructures of an enemy.

2/25/2022 55 0 [0.00 B]

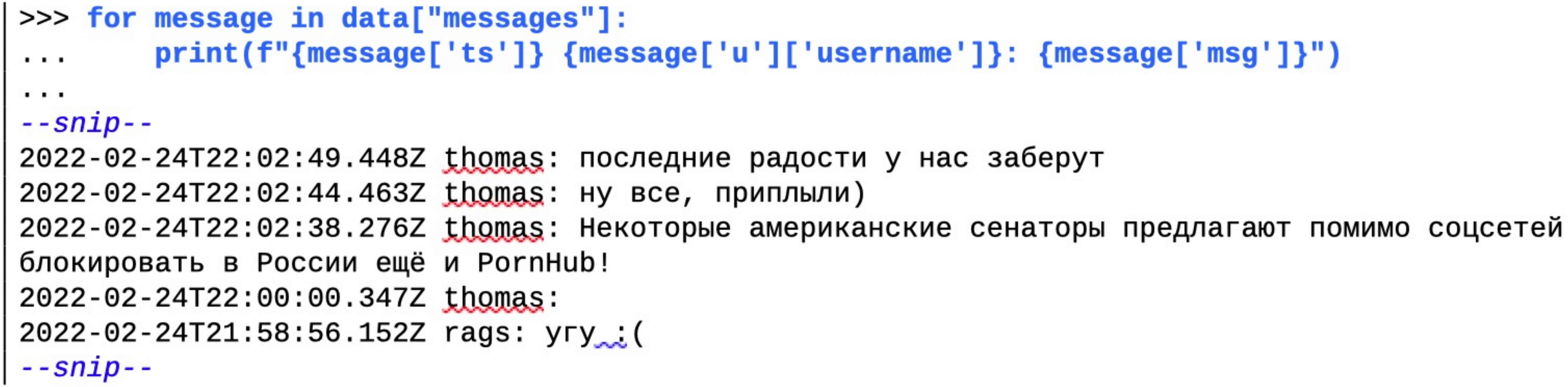


```
~/c/hacks-leaks-and-revelations  on  main !1  cat chapter-8/2022-02-24-general.json | jq '.messages[8]'
```

```
{
  "_id": "FmFZbde9ACs3gtw27",
  "rid": "GENERAL",
  "msg": "Некоторые американские сенаторы предлагают помимо соцсетей блокировать в России ещё и PornHub!",
  "ts": "2022-02-24T22:02:38.276Z",
  "u": {
    "_id": "NKrXj9edAPWNrYv5r",
    "username": "thomas",
    "name": "thomas"
  },
  "urls": [],
  "mentions": [],
  "channels": [],
  "md": [
    {
      "type": "PARAGRAPH",
      "value": [
        {
          "type": "PLAIN_TEXT",
          "value": "Некоторые американские сенаторы предлагают помимо соцсетей блокировать в России ещё и PornHub!"
        }
      ]
    }
  ],
  "_updatedAt": "2022-02-24T22:02:38.293Z"
}
```

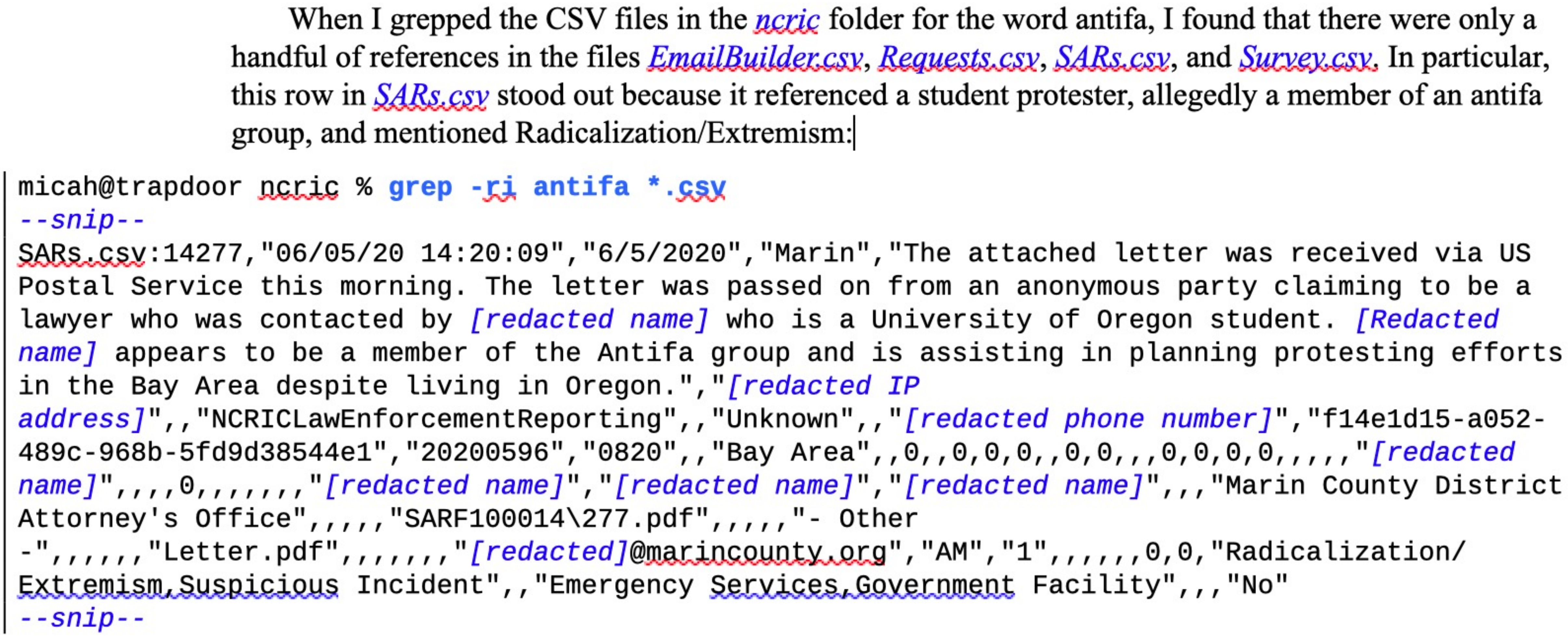


```
>>> import json
>>> with open("2022-02-24-general.json") as f:
...     data = json.load(f)
...
```



```
>>> for message in data["messages"]:
...     print(f"{message['ts']} {message['u']['username']}: {message['msg']}")
...
--snip--
2022-02-24T22:02:49.448Z thomas: последние радости у нас заберут
2022-02-24T22:02:44.463Z thomas: ну все, приплыли)
2022-02-24T22:02:38.276Z thomas: Некоторые американские сенаторы предлагают помимо соцсетей
блокировать в России ещё и PornHub!
2022-02-24T22:00:00.347Z thomas:
2022-02-24T21:58:56.152Z rags: угу :(
--snip--
```

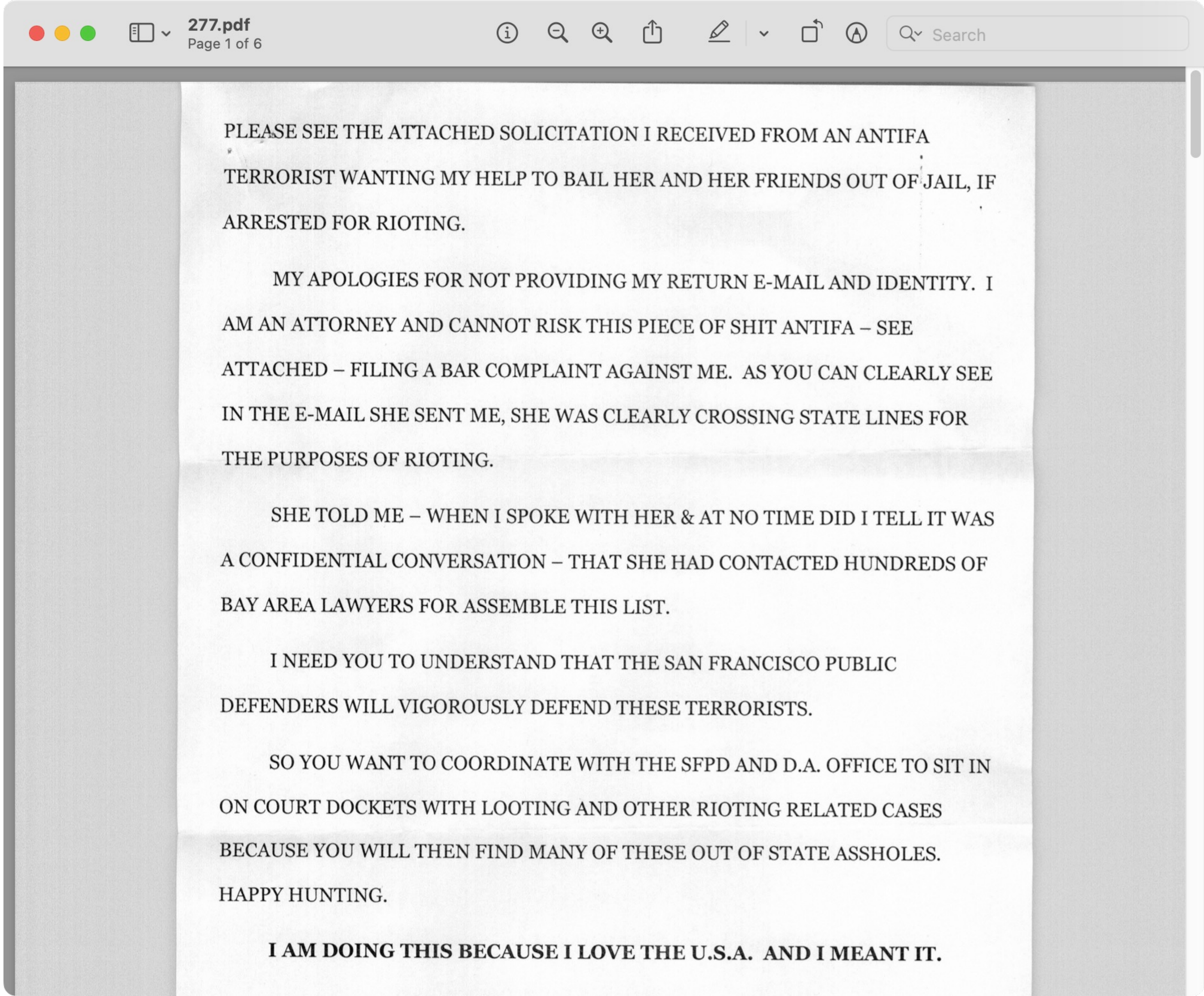
BlueLeaks and the CSV File Format



When I grepped the CSV files in the *ncric* folder for the word antifa, I found that there were only a handful of references in the files *EmailBuilder.csv*, *Requests.csv*, *SARs.csv*, and *Survey.csv*. In particular, this row in *SARs.csv* stood out because it referenced a student protester, allegedly a member of an antifa group, and mentioned Radicalization/Extremism:

```
micah@trapdoor ncric % grep -ri antifa *.csv
--snip--
SARs.csv:14277,"06/05/20 14:20:09","6/5/2020","Marin","The attached letter was received via US
Postal Service this morning. The letter was passed on from an anonymous party claiming to be a
lawyer who was contacted by [redacted name] who is a University of Oregon student. [Redacted
name] appears to be a member of the Antifa group and is assisting in planning protesting efforts
in the Bay Area despite living in Oregon.","[redacted IP
address]",,"NCRICLawEnforcementReporting",,"Unknown",,"[redacted phone number]","f14e1d15-a052-
489c-968b-5fd9d38544e1","20200596","0820",,"Bay Area",,0,,0,0,0,,0,0,,,0,0,0,0,,,,,"[redacted
name]",,,,0,,,,,,,,"[redacted name]","[redacted name]","[redacted name]",,,"Marin County District
Attorney's Office",,,,,"SARF100014\277.pdf",,,,,"- Other
-",,,,,,"Letter.pdf",,,,,,,"[redacted]@marincounty.org","AM","1",,,,,,0,0,"Radicalization/
Extremism,Suspicious Incident",,"Emergency Services,Government Facility",,,"No"
--snip--
```

Column Header	Content
SARSid	14277
FormTimeStamp	06/05/20 14:20:09
IncidentDate	6/5/2020
ThreatActivity	Radicalization/Extremism,Suspicious Incident
BriefSummary	The attached letter was received via US Postal Service this morning. The letter was passed on from an anonymous party claiming to be a lawyer who was contacted by *[redacted name]* who is a University of Oregon student. *[Redacted name]* appears to be a member of the Antifa group and is assisting in planning protesting efforts in the Bay Area despite living in Oregon.
Subjects	*[redacted name]*
AgencyOrganizationNameOther	*Marin County District Attorney's Office*
File1	*SARF100014\277.pdf*
File1Name	*Letter.pdf*
EmailAddress	*[redacted]*@marincounty.org



PLEASE SEE THE ATTACHED SOLICITATION I RECEIVED FROM AN ANTIFA TERRORIST WANTING MY HELP TO BAIL HER AND HER FRIENDS OUT OF JAIL, IF ARRESTED FOR RIOTING.

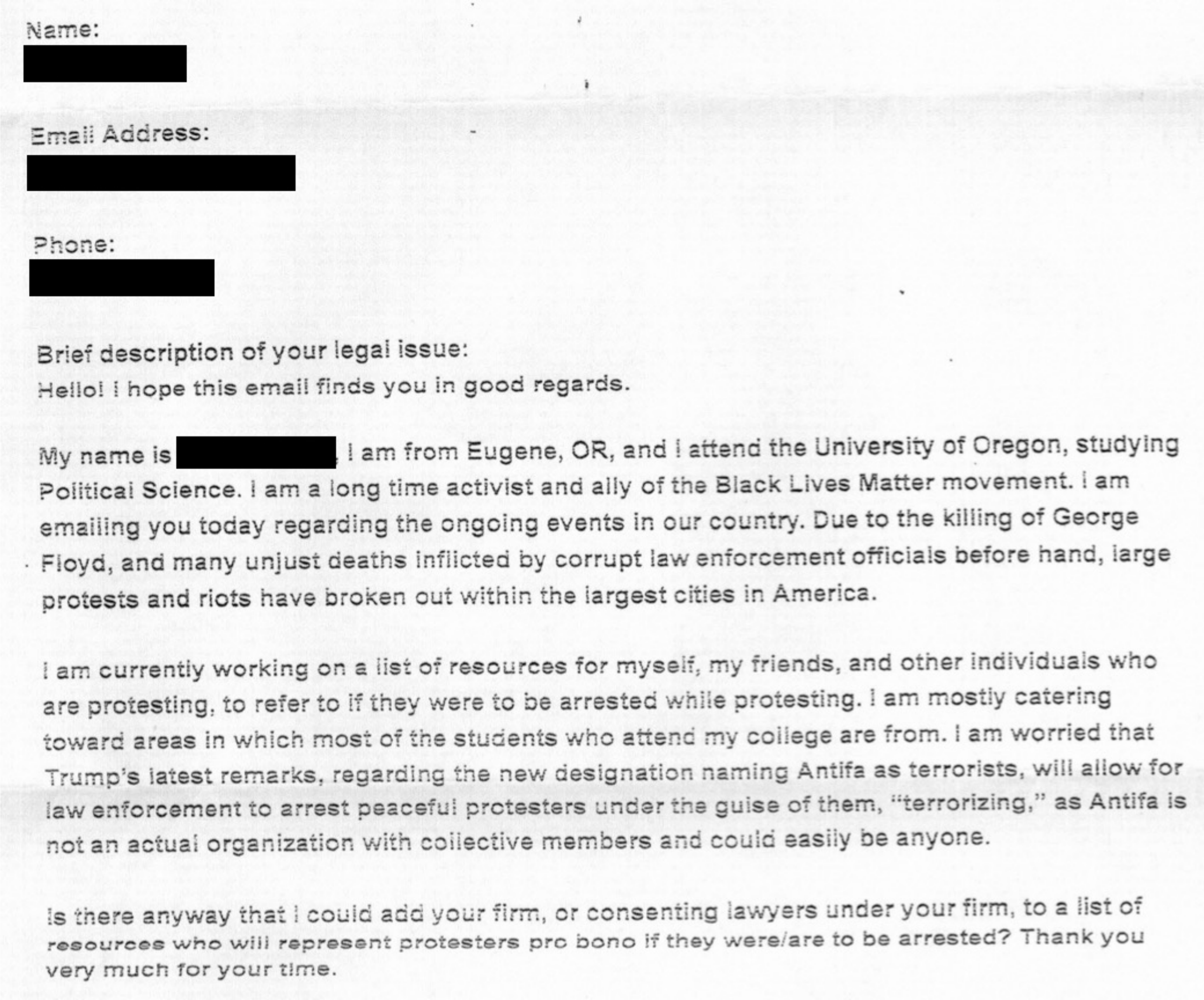
MY APOLOGIES FOR NOT PROVIDING MY RETURN E-MAIL AND IDENTITY. I AM AN ATTORNEY AND CANNOT RISK THIS PIECE OF SHIT ANTIFA – SEE ATTACHED – FILING A BAR COMPLAINT AGAINST ME. AS YOU CAN CLEARLY SEE IN THE E-MAIL SHE SENT ME, SHE WAS CLEARLY CROSSING STATE LINES FOR THE PURPOSES OF RIOTING.

SHE TOLD ME – WHEN I SPOKE WITH HER & AT NO TIME DID I TELL IT WAS A CONFIDENTIAL CONVERSATION – THAT SHE HAD CONTACTED HUNDREDS OF BAY AREA LAWYERS FOR ASSEMBLE THIS LIST.

I NEED YOU TO UNDERSTAND THAT THE SAN FRANCISCO PUBLIC DEFENDERS WILL VIGOROUSLY DEFEND THESE TERRORISTS.

SO YOU WANT TO COORDINATE WITH THE SFPD AND D.A. OFFICE TO SIT IN ON COURT DOCKETS WITH LOOTING AND OTHER RIOTING RELATED CASES BECAUSE YOU WILL THEN FIND MANY OF THESE OUT OF STATE ASSHOLES. HAPPY HUNTING.

I AM DOING THIS BECAUSE I LOVE THE U.S.A. AND I MEANT IT.



Name:

[redacted]

Email Address:

[redacted]

Phone:

[redacted]

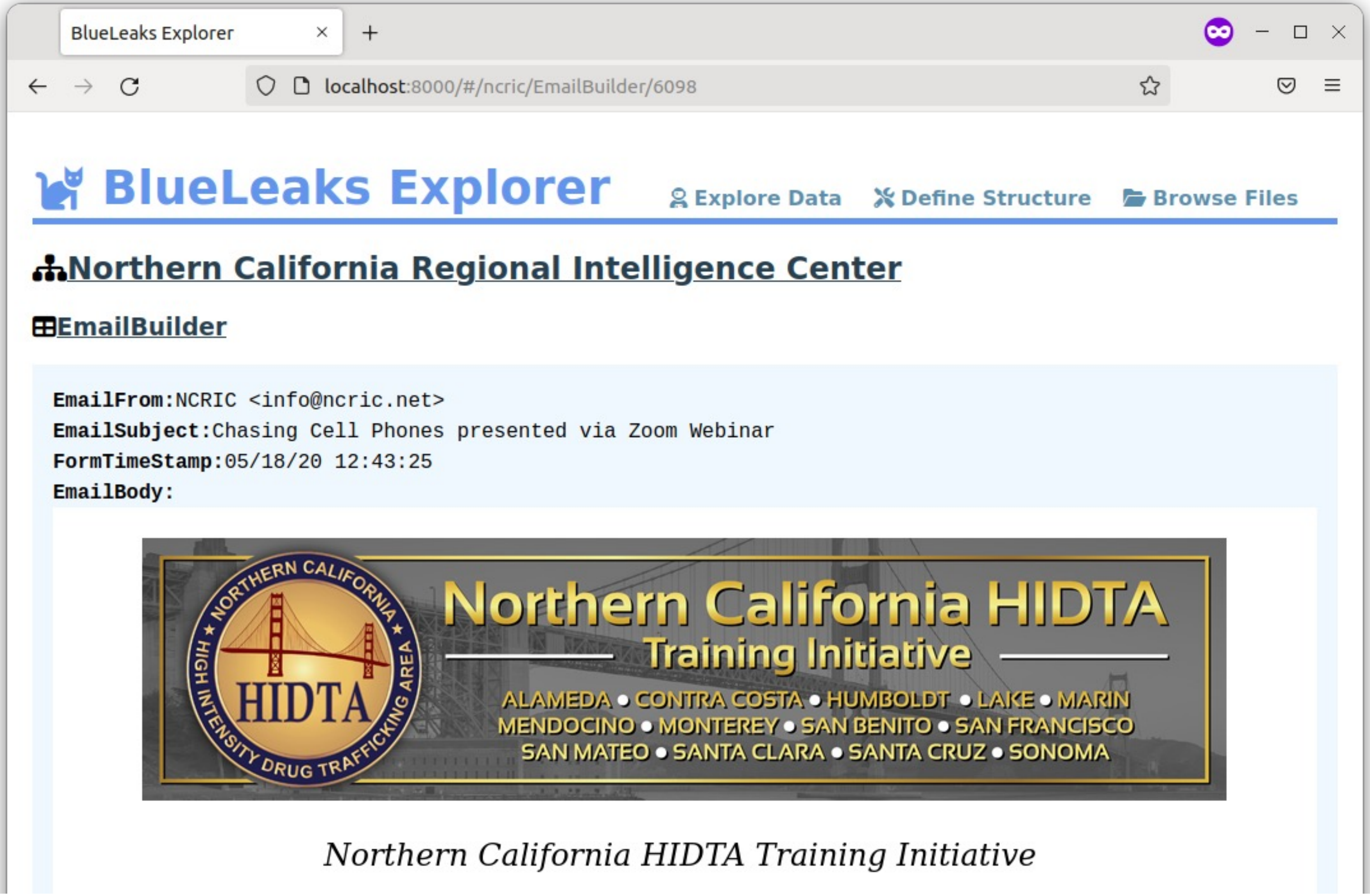
Brief description of your legal issue:

Hello! I hope this email finds you in good regards.

My name is [redacted], I am from Eugene, OR, and I attend the University of Oregon, studying Political Science. I am a long time activist and ally of the Black Lives Matter movement. I am emailing you today regarding the ongoing events in our country. Due to the killing of George Floyd, and many unjust deaths inflicted by corrupt law enforcement officials before hand, large protests and riots have broken out within the largest cities in America.

I am currently working on a list of resources for myself, my friends, and other individuals who are protesting, to refer to if they were to be arrested while protesting. I am mostly catering toward areas in which most of the students who attend my college are from. I am worried that Trump's latest remarks, regarding the new designation naming Antifa as terrorists, will allow for law enforcement to arrest peaceful protesters under the guise of them, "terrorizing," as Antifa is not an actual organization with collective members and could easily be anyone.

Is there anyway that I could add your firm, or consenting lawyers under your firm, to a list of resources who will represent protesters pro bono if they were/are to be arrested? Thank you very much for your time.


BlueLeaks Explorer
localhost:8000/#/ncric/EmailBuilder/6098
BlueLeaks Explorer
Explore Data
Define Structure
Browse Files
NORTHERN CALIFORNIA
HIGH INTENSITY DRUG TRAFFICKING AREA
HIDTA
Northern California HIDTA
Training Initiative
ALAMEDA • CONTRA COSTA • HUMBOLDT • LAKE • MARIN
MENDOCINO • MONTEREY • SAN BENITO • SAN FRANCISCO
SAN MATEO • SANTA CLARA • SANTA CRUZ • SONOMA

Northern California Regional Intelligence Center

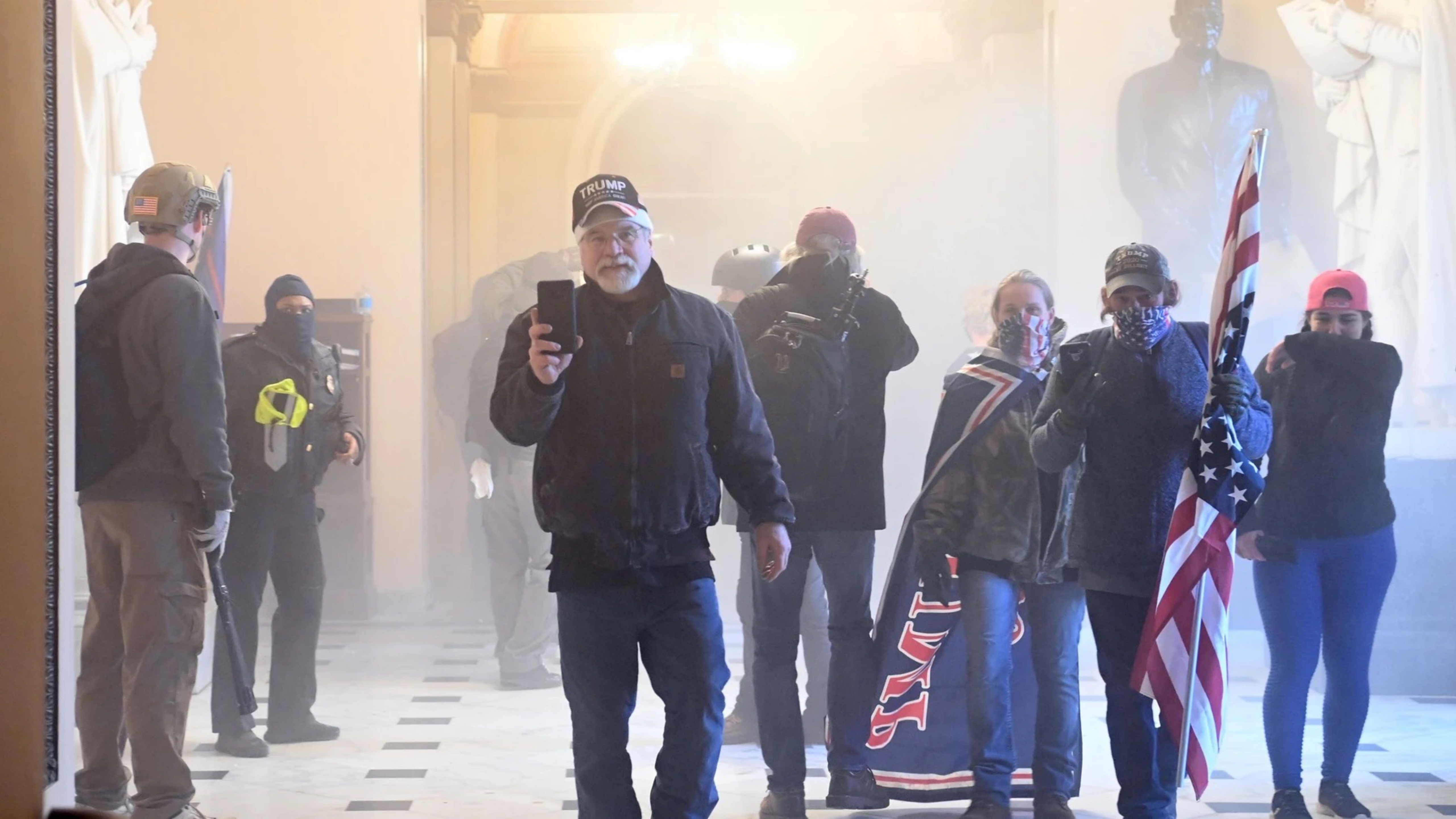
EmailBuilder

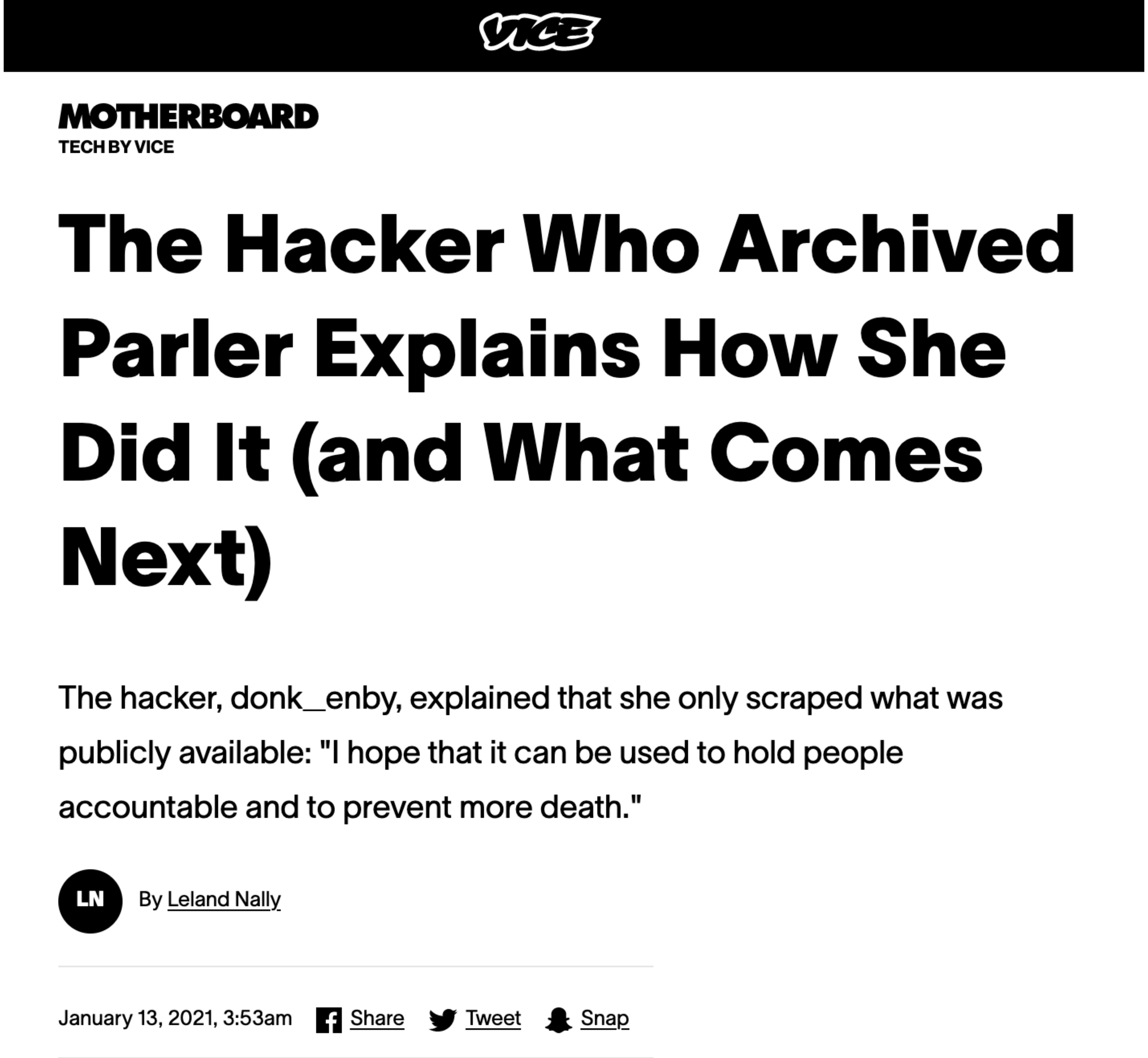
EmailFrom:NCRIC <info@ncric.net>
EmailSubject: Chasing Cell Phones presented via Zoom Webinar
FormTimeStamp:05/18/20 12:43:25
EmailBody:

Northern California HIDTA Training Initiative

https://github.com/micahflee/blueleaks-explorer

JSON, January 6, and Mapping GPS Coordinates


TRUMP
TRUMP



VICE

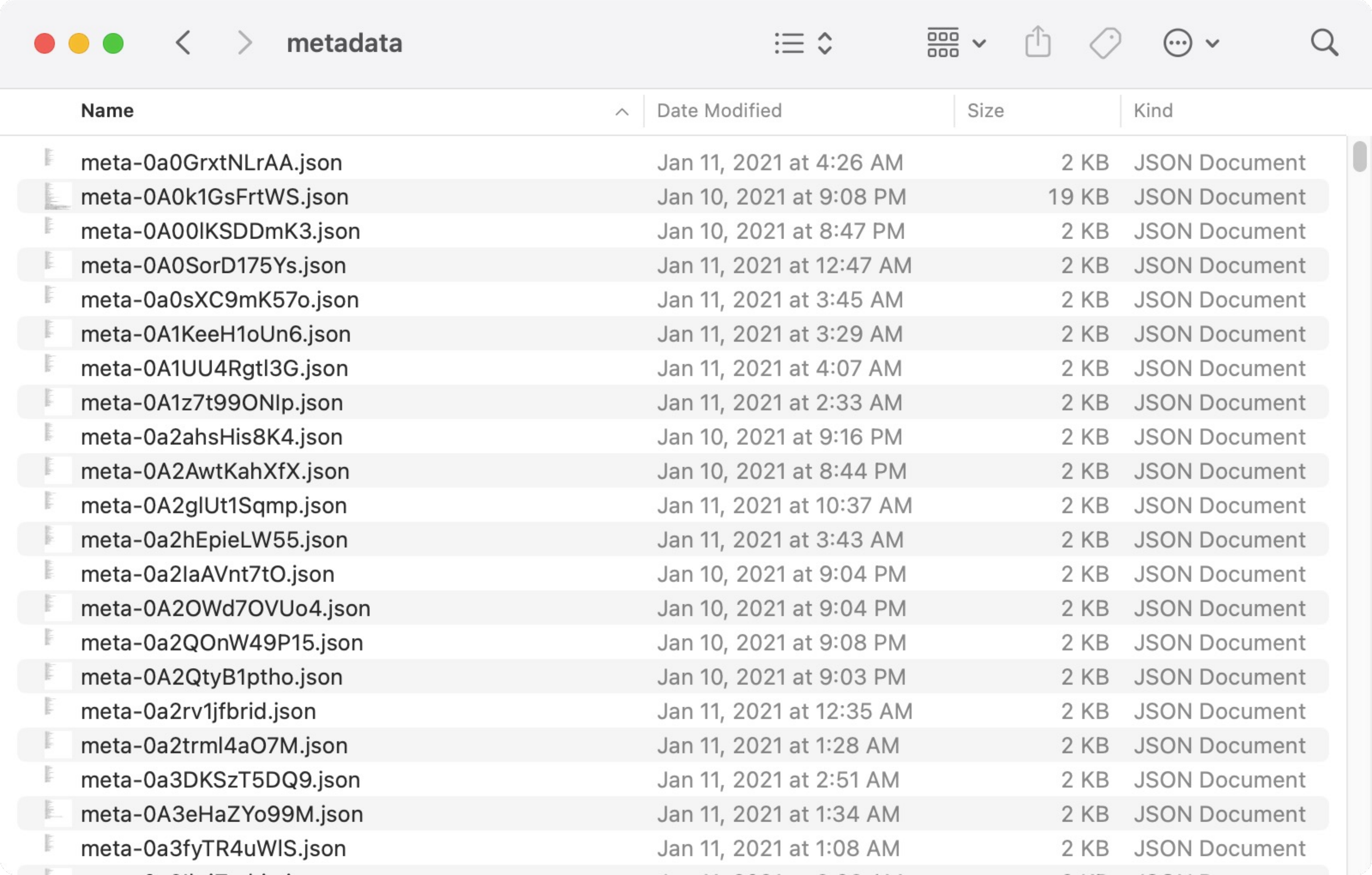
MOTHERBOARD
TECH BY VICE

The Hacker Who Archived Parler Explains How She Did It (and What Comes Next)

The hacker, donk_enby, explained that she only scraped what was publicly available: "I hope that it can be used to hold people accountable and to prevent more death."

LN By Leland Nally

January 13, 2021, 3:53am



Name	Date Modified	Size	Kind
meta-0a0GrxtNLrAA.json	Jan 11, 2021 at 4:26 AM	2 KB	JSON Document
meta-0A0k1GsFrtWS.json	Jan 10, 2021 at 9:08 PM	19 KB	JSON Document
meta-0A00lKSDDmK3.json	Jan 10, 2021 at 8:47 PM	2 KB	JSON Document
meta-0A0SorD175Ys.json	Jan 11, 2021 at 12:47 AM	2 KB	JSON Document
meta-0a0sXC9mK57o.json	Jan 11, 2021 at 3:45 AM	2 KB	JSON Document
meta-0A1KeeH1oUn6.json	Jan 11, 2021 at 3:29 AM	2 KB	JSON Document
meta-0A1UU4Rgtl3G.json	Jan 11, 2021 at 4:07 AM	2 KB	JSON Document
meta-0A1z7t99ONlp.json	Jan 11, 2021 at 2:33 AM	2 KB	JSON Document
meta-0a2ahsHis8K4.json	Jan 10, 2021 at 9:16 PM	2 KB	JSON Document
meta-0A2AwtKahXfX.json	Jan 10, 2021 at 8:44 PM	2 KB	JSON Document
meta-0A2glUt1Sqmp.json	Jan 11, 2021 at 10:37 AM	2 KB	JSON Document
meta-0a2hEpieLW55.json	Jan 11, 2021 at 3:43 AM	2 KB	JSON Document
meta-0a2laAVnt7tO.json	Jan 10, 2021 at 9:04 PM	2 KB	JSON Document
meta-0A2OWd7OVUo4.json	Jan 10, 2021 at 9:04 PM	2 KB	JSON Document
meta-0a2QOnW49P15.json	Jan 10, 2021 at 9:08 PM	2 KB	JSON Document
meta-0A2QtyB1ptho.json	Jan 10, 2021 at 9:03 PM	2 KB	JSON Document
meta-0a2rv1jfbrid.json	Jan 11, 2021 at 12:35 AM	2 KB	JSON Document
meta-0a2trml4aO7M.json	Jan 11, 2021 at 1:28 AM	2 KB	JSON Document
meta-0a3DKSzT5DQ9.json	Jan 11, 2021 at 2:51 AM	2 KB	JSON Document
meta-0A3eHaZYo99M.json	Jan 11, 2021 at 1:34 AM	2 KB	JSON Document
meta-0a3fyTR4uWlS.json	Jan 11, 2021 at 1:08 AM	2 KB	JSON Document

You can pipe JSON data into the `jq` command to indent it and show syntax highlighting in your terminal. For example, try running this command:

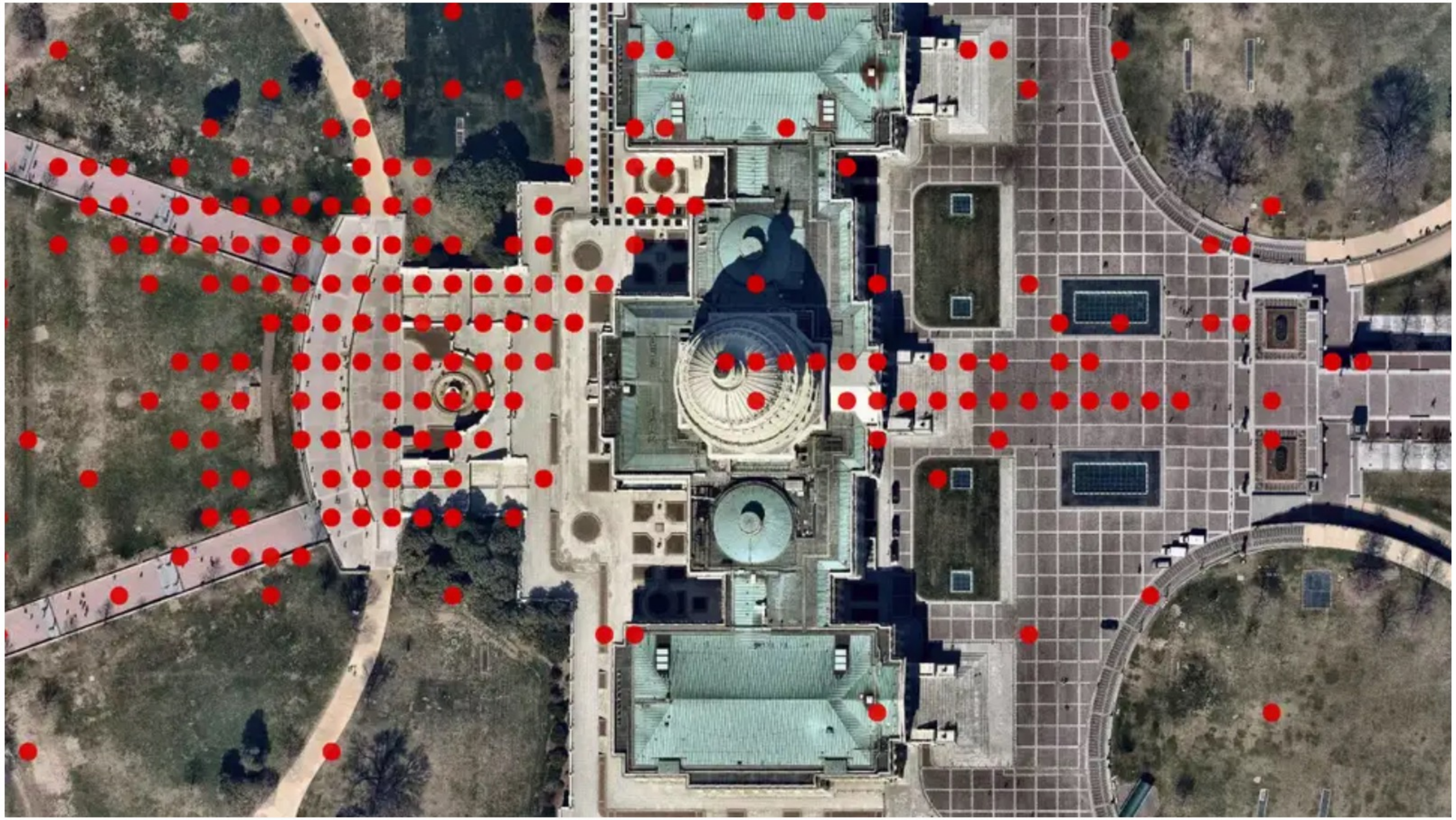
```
cat metadata/meta-HS34fpbzqg2b.json | jq
```

The first part of the command, `cat metadata/meta-HS34fpbzqg2b.json`, outputs the content of that JSON file, which contains the metadata for a single Parler video. The second part, `| jq`, pipes that output as input into `jq`. The output of this command in your terminal should look like this:

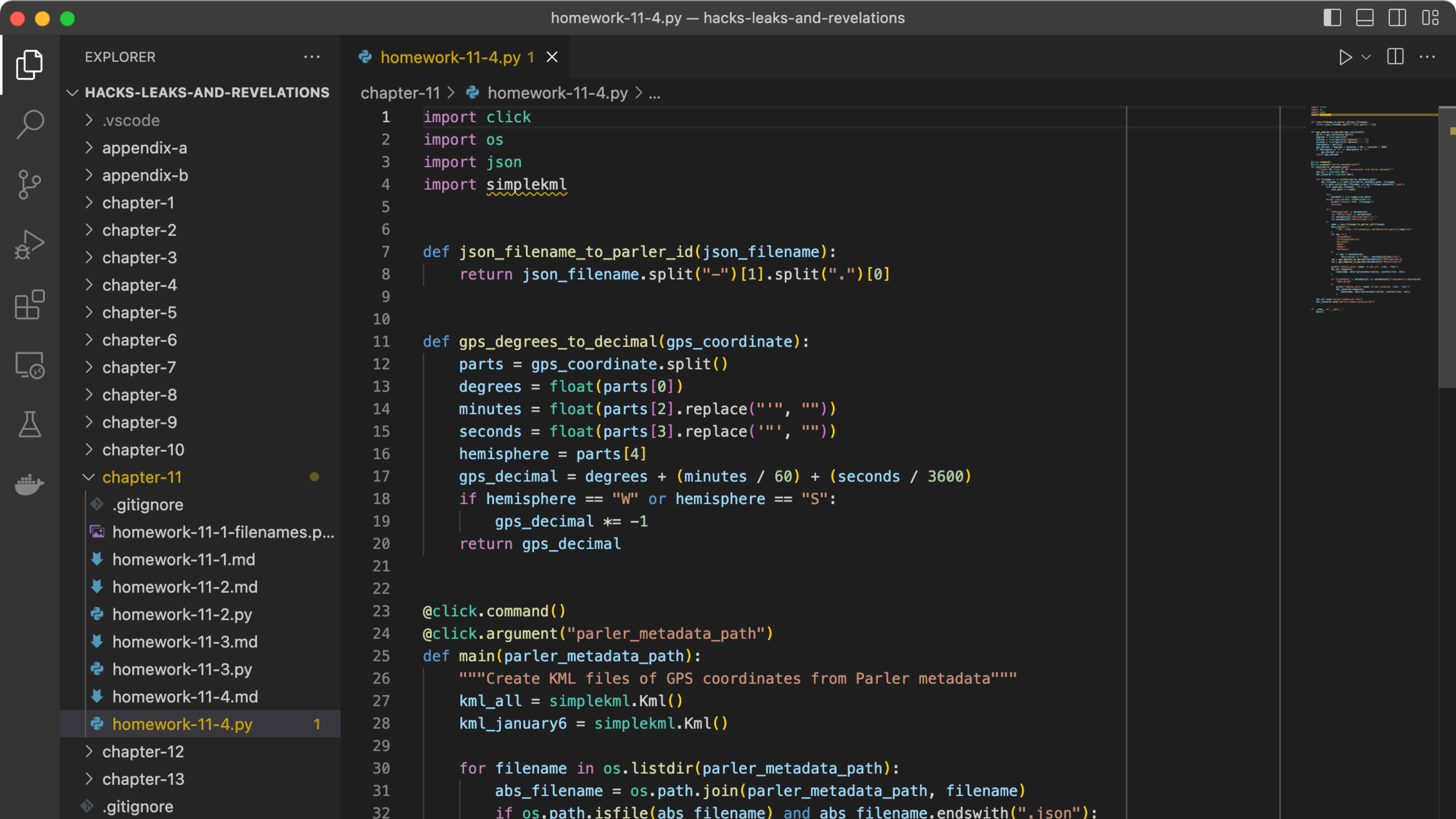
```
[
  {
    "SourceFile": "-",
    "ExifToolVersion": 12,
    "FileType": "MOV",
    "FileTypeExtension": "mov",
    "MIMEType": "video/quicktime",
    "MajorBrand": "Apple QuickTime (.MOV/QT)",
    "MinorVersion": "0.0.0",
    "CompatibleBrands": [
      "qt  "
    ],
--snip--
    "GPSLatitude": "38 deg 53' 26.52\" N",
    "GPSLongitude": "77 deg 0' 28.44\" W",
    "Rotation": 180,
  1 "GPSPosition": "38 deg 53' 26.52\" N, 77 deg 0' 28.44\" W"
  }
]
```

Parler Users Breached Deep Inside U.S. Capitol Building, GPS Data Shows

By **Dell Cameron and Dhruv Mehrotra** | Published January 12, 2021 | Comments (193)



Graphic: Dhruv Mehrota / Gizmodo



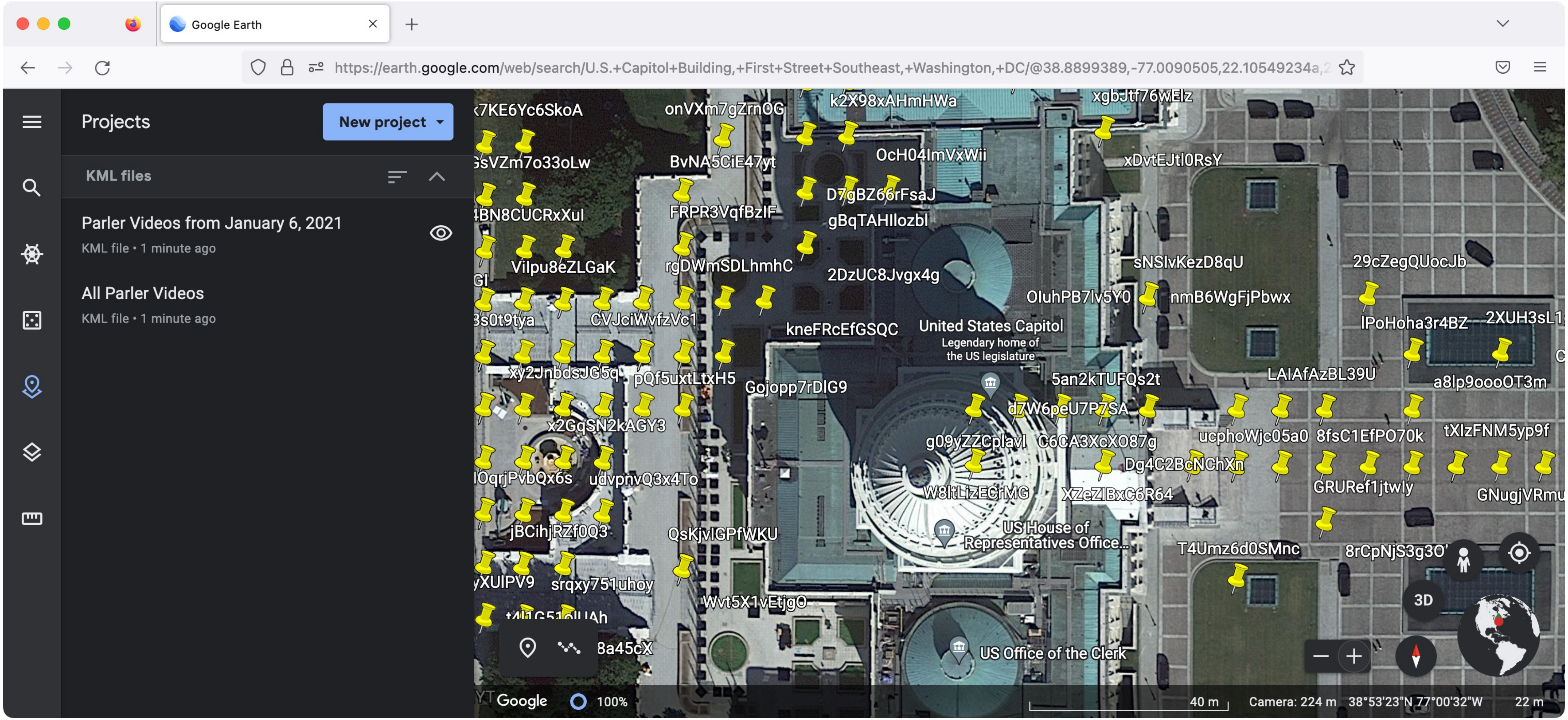
```python
import click
import os
import json
import simplekml


def json_filename_to_parler_id(json_filename):
    return json_filename.split("-")[1].split(".")[0]


def gps_degrees_to_decimal(gps_coordinate):
    parts = gps_coordinate.split()
    degrees = float(parts[0])
    minutes = float(parts[2].replace("'", ""))
    seconds = float(parts[3].replace('"', ""))
    hemisphere = parts[4]
    gps_decimal = degrees + (minutes / 60) + (seconds / 3600)
    if hemisphere == "W" or hemisphere == "S":
        gps_decimal *= -1
    return gps_decimal


@click.command()
@click.argument("parler_metadata_path")
def main(parler_metadata_path):
    """Create KML files of GPS coordinates from Parler metadata"""
    kml_all = simplekml.Kml()
    kml_january6 = simplekml.Kml()

    for filename in os.listdir(parler_metadata_path):
        abs_filename = os.path.join(parler_metadata_path, filename)
        if os.path.isfile(abs_filename) and abs_filename.endswith(".json"):
```



Google Earth

https://earth.google.com/web/search/U.S.+Capitol+Building,+First+Street+Southeast,+Washington,+DC/@38.8899389,-77.0090505,22.10549234a,2

Projects

New project

KML files

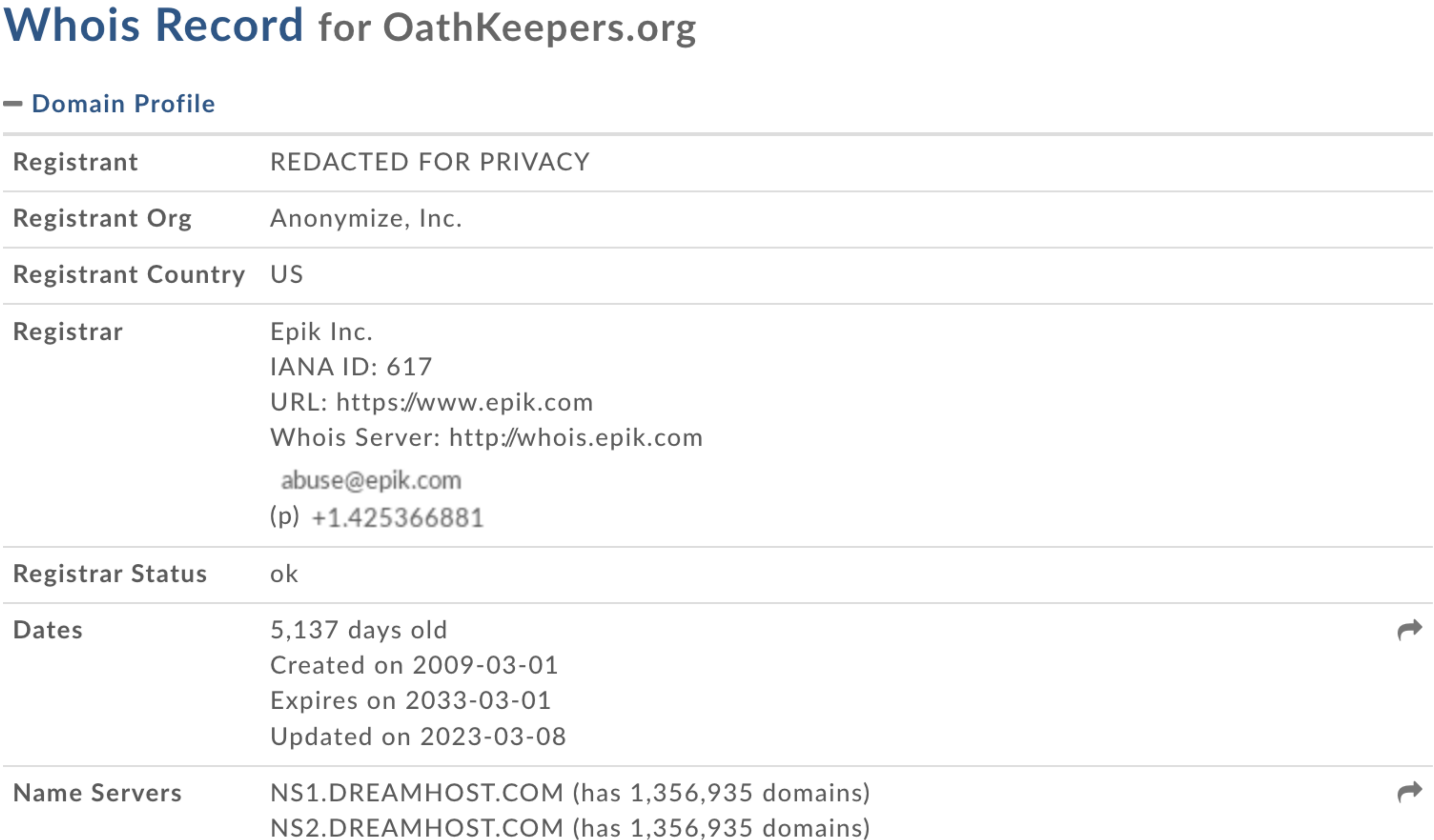
Parler Videos from January 6, 2021

KML file • 1 minute ago

All Parler Videos

KML file • 1 minute ago

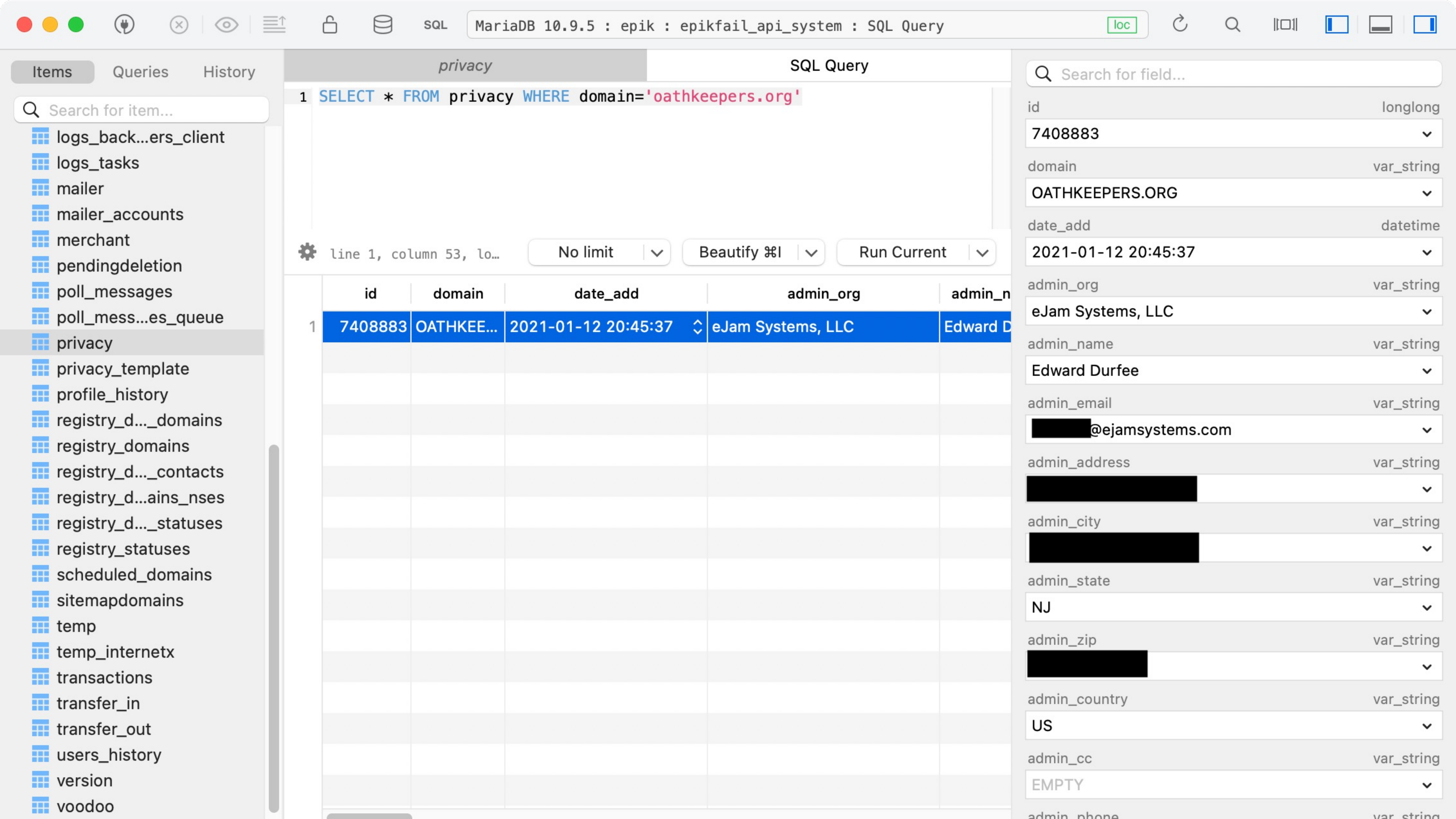
SQL, Epik Fail, and Extremism Research



Whois Record for OathKeepers.org

— Domain Profile

Registrant	REDACTED FOR PRIVACY
Registrant Org	Anonymize, Inc.
Registrant Country	US
Registrar	Epik Inc. IANA ID: 617 URL: https://www.epik.com Whois Server: http://whois.epik.com abuse@epik.com (p) +1.425366881
Registrar Status	ok
Dates	5,137 days old Created on 2009-03-01 Expires on 2033-03-01 Updated on 2023-03-08
Name Servers	NS1.DREAMHOST.COM (has 1,356,935 domains) NS2.DREAMHOST.COM (has 1,356,935 domains)



MariaDB 10.9.5 : epik : epikfail_api_system : SQL Query

```
SELECT * FROM privacy WHERE domain='oathkeepers.org'
```

logs_back...ers_client
logs_tasks
mailer
mailer_accounts
merchant
pendingdeletion
poll_messages
poll_mess...es_queue
privacy
privacy_template
profile_history
registry_d..._domains
registry_domains
registry_d..._contacts
registry_d...ains_nses
registry_d..._statuses
registry_statuses
scheduled_domains
sitemapdomains
temp
temp_internetx
transactions
transfer_in
transfer_out
users_history
version
voodoo

	id	domain	date_add	admin_org	admin_n
1	7408883	OATHKEE...	2021-01-12 20:45:37	eJam Systems, LLC	Edward D

id longlong
7408883

domain var_string
OATHKEEPERS.ORG

date_add datetime
2021-01-12 20:45:37

admin_org var_string
eJam Systems, LLC

admin_name var_string
Edward Durfee

admin_email var_string
[redacted]@ejamsystems.com

admin_address var_string
[redacted]

admin_city var_string
[redacted]

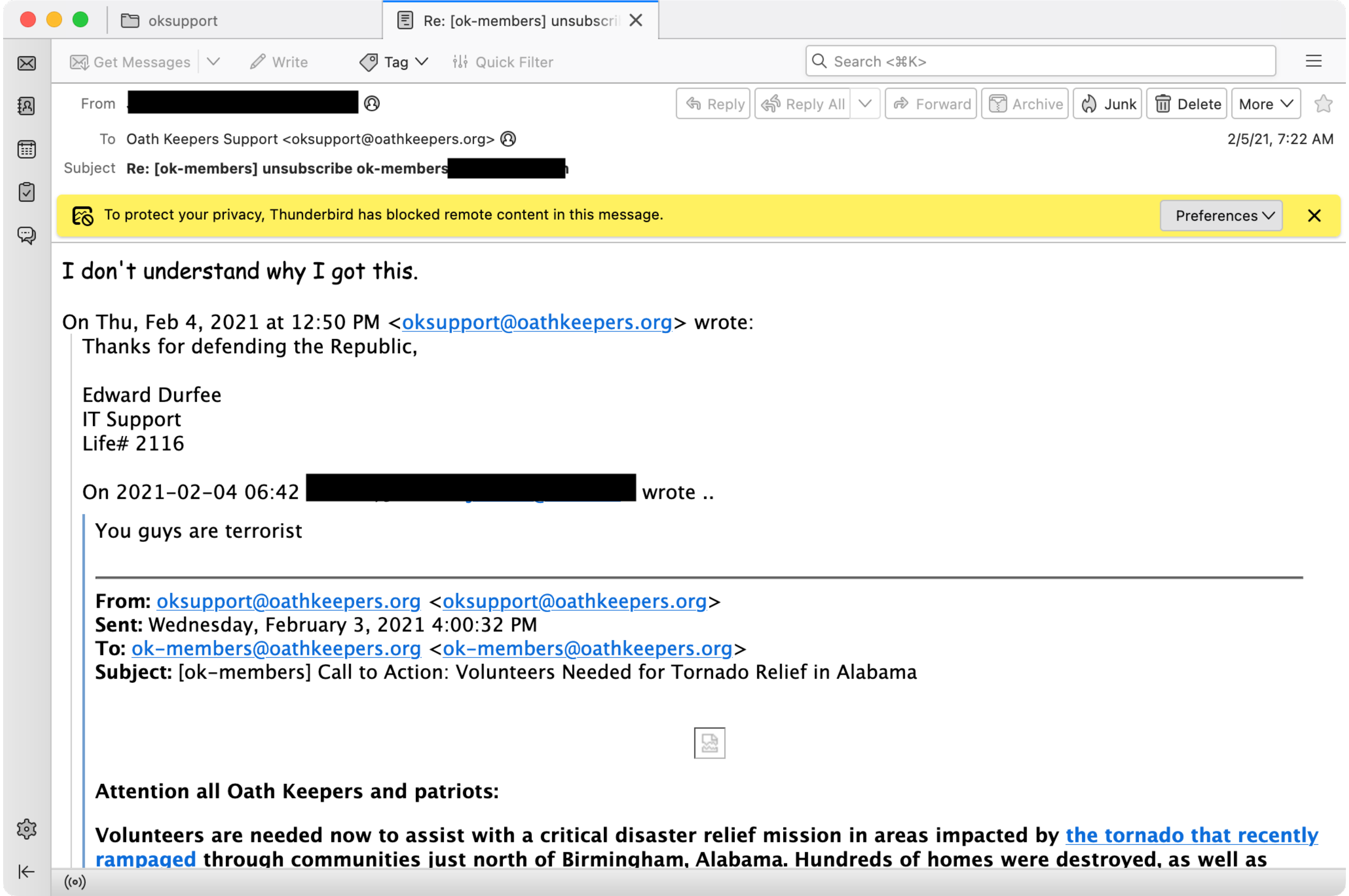
admin_state var_string
NJ

admin_zip var_string
[redacted]

admin_country var_string
US

admin_cc var_string
EMPTY

admin_phone var_string



From [redacted]

To Oath Keepers Support <oksupport@oathkeepers.org>

2/5/21, 7:22 AM

Subject **Re: [ok-members] unsubscribe ok-members[redacted]**

To protect your privacy, Thunderbird has blocked remote content in this message.

I don't understand why I got this.

On Thu, Feb 4, 2021 at 12:50 PM <oksupport@oathkeepers.org> wrote:

> Thanks for defending the Republic,
>
> Edward Durfee
> IT Support
> Life# 2116
>
> On 2021-02-04 06:42 [redacted] wrote ..
>
> > You guys are terrorist
> >
> > ---
> >
> > **From:** oksupport@oathkeepers.org <oksupport@oathkeepers.org>
> > **Sent:** Wednesday, February 3, 2021 4:00:32 PM
> > **To:** ok-members@oathkeepers.org <ok-members@oathkeepers.org>
> > **Subject:** [ok-members] Call to Action: Volunteers Needed for Tornado Relief in Alabama
> >
> > **Attention all Oath Keepers and patriots:**
> >
> > **Volunteers are needed now to assist with a critical disaster relief mission in areas impacted by the tornado that recently rampaged through communities just north of Birmingham, Alabama. Hundreds of homes were destroyed, as well as**

Pandemic Profiteers and COVID-19 Disinformation

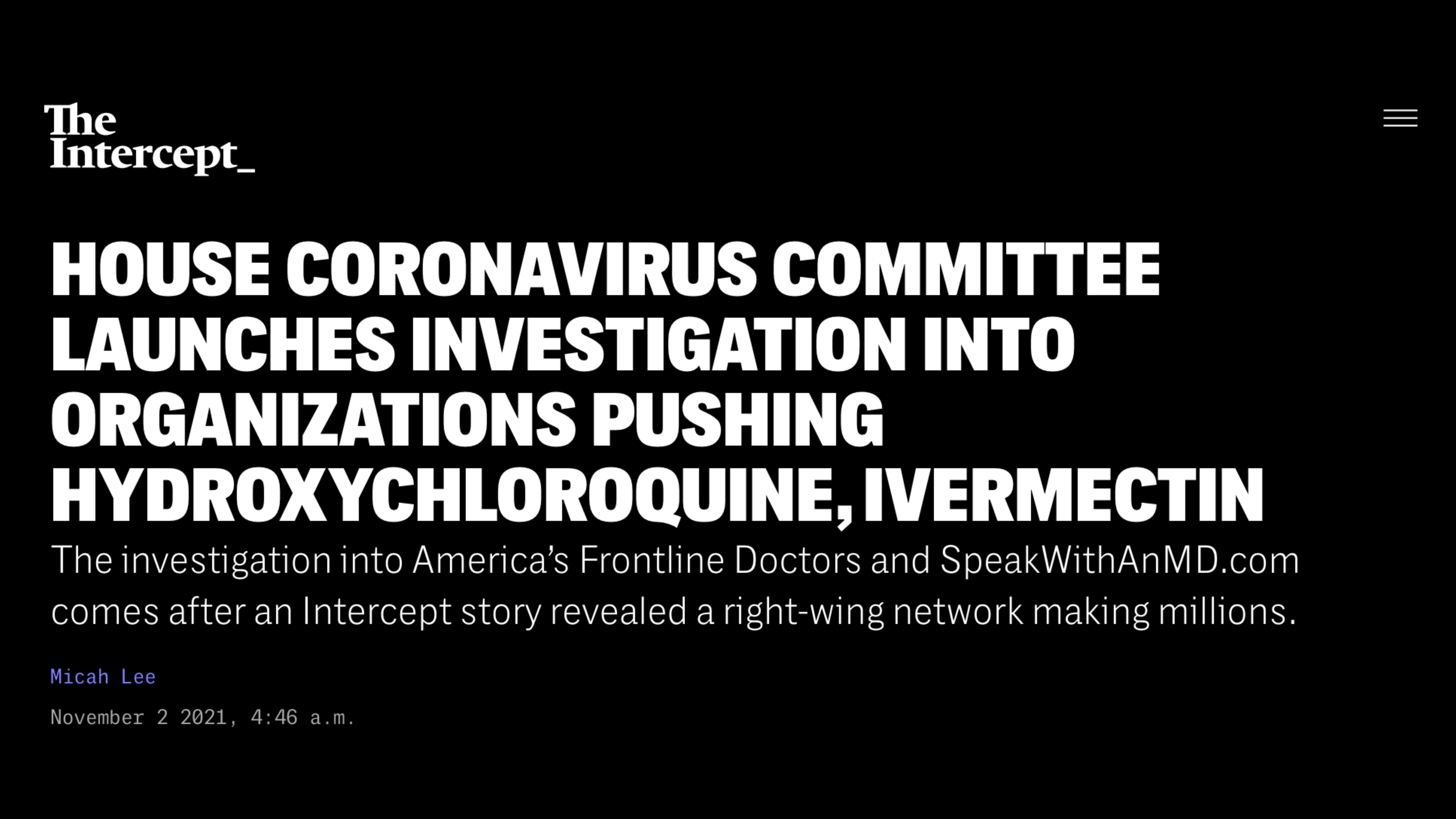
The Intercept_

NETWORK OF RIGHT-WING HEALTH CARE PROVIDERS IS MAKING MILLIONS OFF HYDROXYCHLOROQUINE AND IVERMECTIN, HACKED DATA REVEALS

The data also reveals that 72,000 people paid at least $6.7 million for Covid-19 consultations promoted by America’s Frontline Doctors and vaccine conspiracist Simone Gold.

Micah Lee

September 29 2021, 6:37 a.m.



The Intercept_

HOUSE CORONAVIRUS COMMITTEE LAUNCHES INVESTIGATION INTO ORGANIZATIONS PUSHING HYDROXYCHLOROQUINE, IVERMECTIN

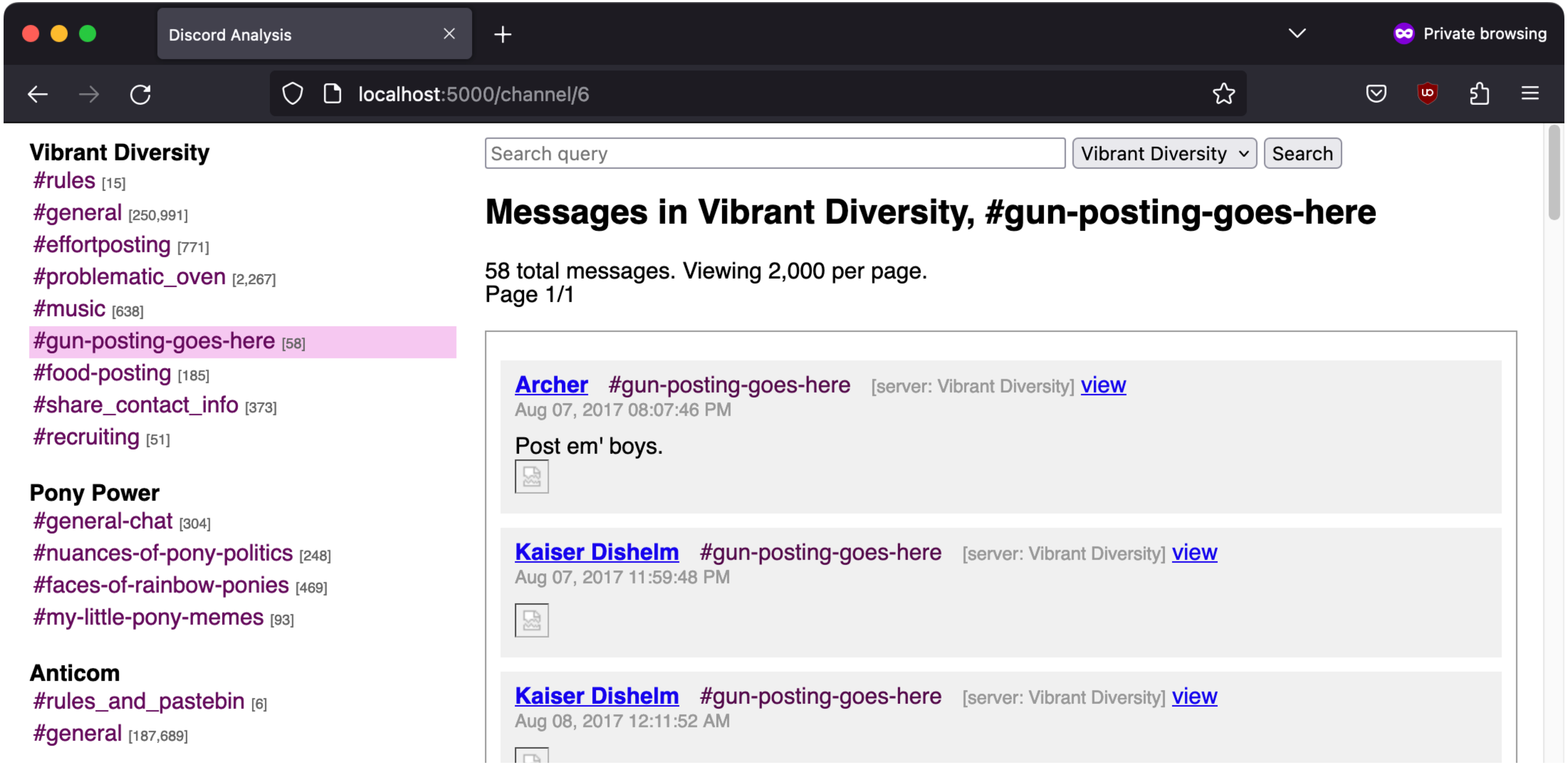
The investigation into America's Frontline Doctors and SpeakWithAnMD.com comes after an Intercept story revealed a right-wing network making millions.

Micah Lee

November 2 2021, 4:46 a.m.

Neo-Nazis and Their Chat Rooms

DONT TREAD
NO PARKING ANYTIME
RESERVED PARKING
8
adidas



Vibrant Diversity
#rules [15]
#general [250,991]
#effortposting [771]
#problematic_oven [2,267]
#music [638]
#gun-posting-goes-here [58]
#food-posting [185]
#share_contact_info [373]
#recruiting [51]

Pony Power
#general-chat [304]
#nuances-of-pony-politics [248]
#faces-of-rainbow-ponies [469]
#my-little-pony-memes [93]

Anticom
#rules_and_pastebin [6]
#general [187,689]

Messages in Vibrant Diversity, #gun-posting-goes-here

58 total messages. Viewing 2,000 per page.
Page 1/1

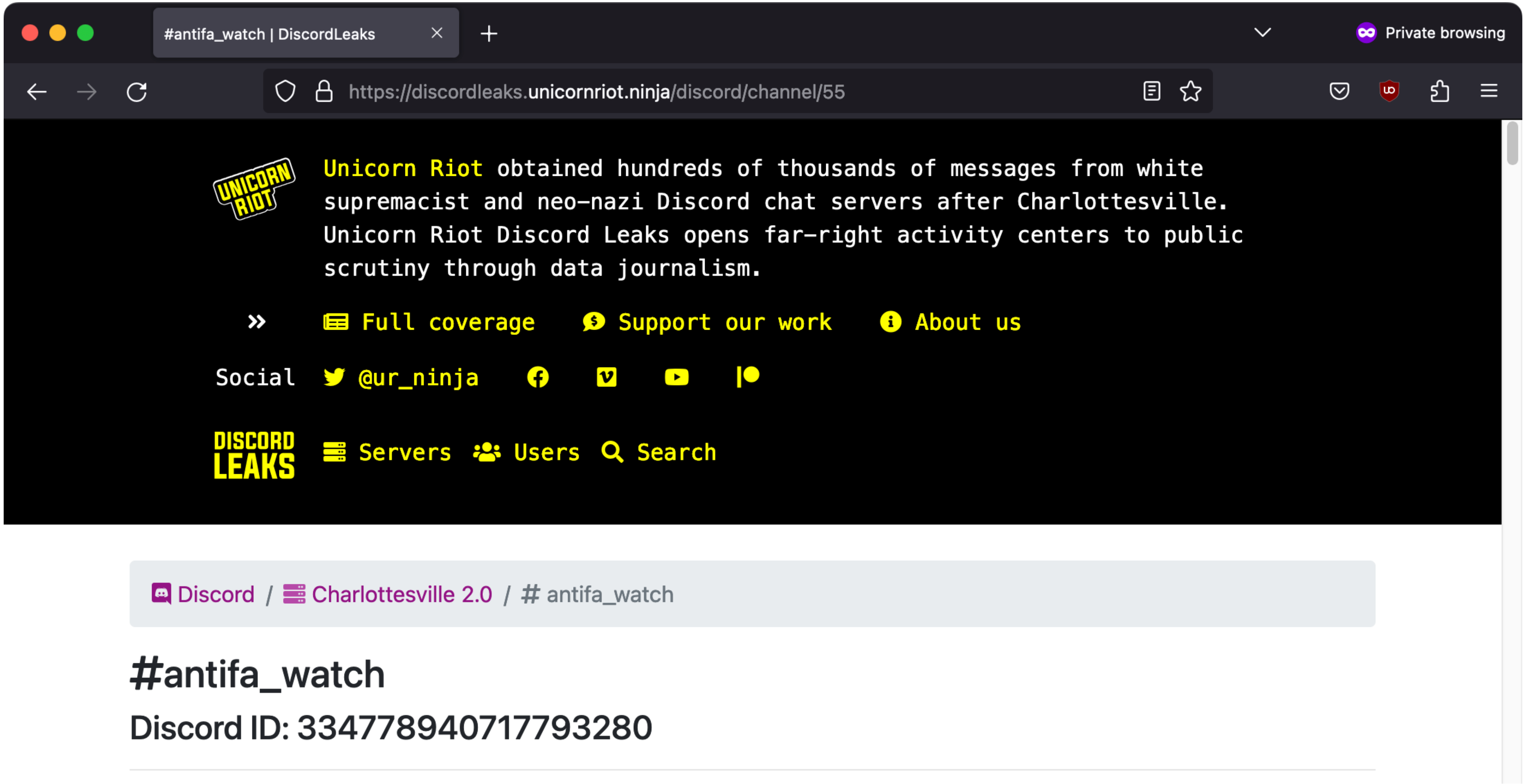
Archer #gun-posting-goes-here [server: Vibrant Diversity] view
Aug 07, 2017 08:07:46 PM

Post em' boys.

Kaiser Dishelm #gun-posting-goes-here [server: Vibrant Diversity] view
Aug 07, 2017 11:59:48 PM

Kaiser Dishelm #gun-posting-goes-here [server: Vibrant Diversity] view
Aug 08, 2017 12:11:52 AM

https://github.com/micahflee/discord-analysis


#antifa_watch | DiscordLeaks
Private browsing
https://discordleaks.unicornriot.ninja/discord/channel/55
UNICORN RIOT

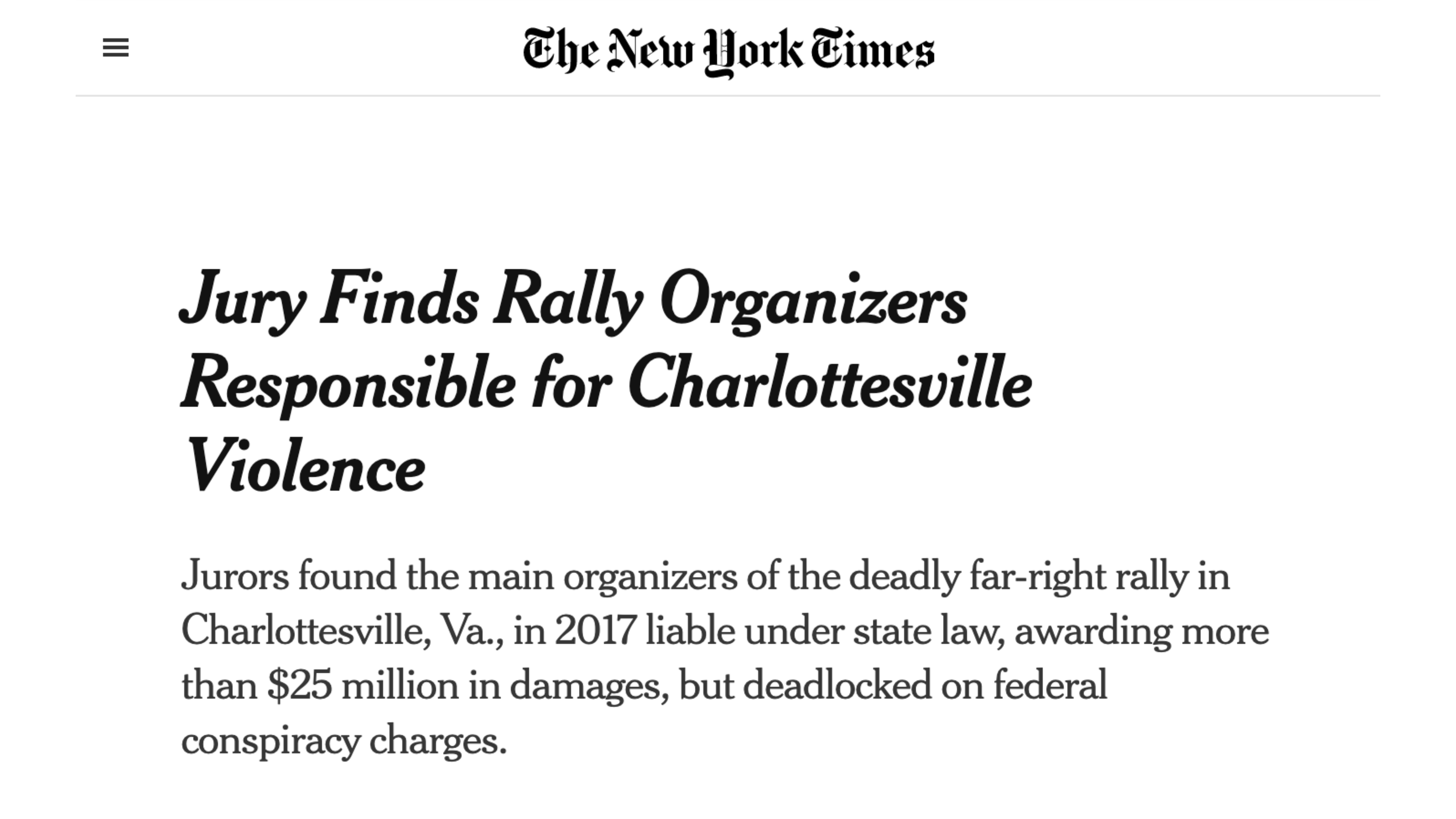
Unicorn Riot obtained hundreds of thousands of messages from white supremacist and neo-nazi Discord chat servers after Charlottesville. Unicorn Riot Discord Leaks opens far-right activity centers to public scrutiny through data journalism.

Discord / Charlottesville 2.0 / # antifa_watch

#antifa_watch

Discord ID: 334778940717793280

https://discordleaks.unicornriot.ninja/



The New York Times

Jury Finds Rally Organizers Responsible for Charlottesville Violence

Jurors found the main organizers of the deadly far-right rally in Charlottesville, Va., in 2017 liable under state law, awarding more than $25 million in damages, but deadlocked on federal conspiracy charges.

ありがとうございます!

I’m Micah Lee, micah@micahflee.com

Hacks, Leaks, and Revelations

to be released ~September 2023

pre-order from No Starch Press:

https://nostarch.com/hacks-leaks-and-revelations