Quarkslab

Parasitizing servers for fun and profit

Damien Cauquil @virtualabs@mamot.fr

LE HACK KERNEL PANIC!

Who am I ?

- Security Engineer (Quarkslab)
- Hardware/software RE

Introduction

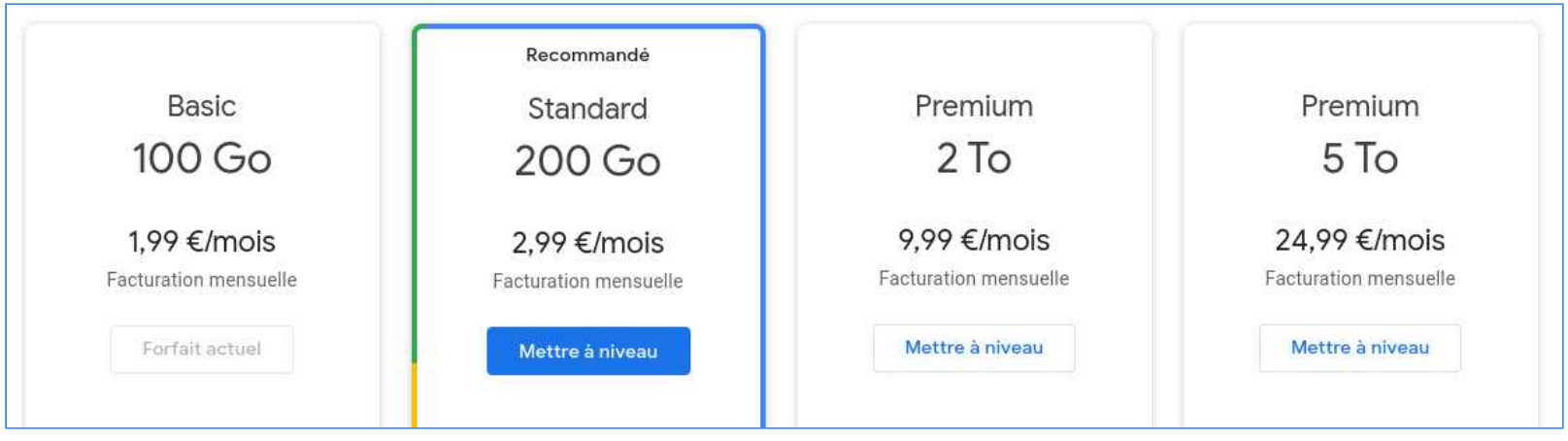
Online storage will ruin you.

iCloud+ 50 Go	iCloud+ 200 Go	iCloud+ 2 To
0,99 €/mois	2,99 €/mois	9,99 €/mois

Chaque forfait inclut aussi les fonctionnalités :

Relais privé iCloud, Masquer mon adresse e-mail, Domaine de messagerie personnalisé et Vidéo sécurisée HomeKit.

Passer à iCloud+


Basic
100 Go
1,99 €/mois
Facturation mensuelle
Forfait actuel
Recommandé
Standard
200 Go
2,99 €/mois
Facturation mensuelle
Mettre à niveau
Premium
2 To
9,99 €/mois
Facturation mensuelle
Mettre à niveau
Premium
5 To
24,99 €/mois
Facturation mensuelle
Mettre à niveau

Media & Entertainment

Google Play Music to shut down starting in September, will disappear by December

Sarah Perez @sarahintampa / 4:26 PM GMT+2 • August 5, 2020

Comment

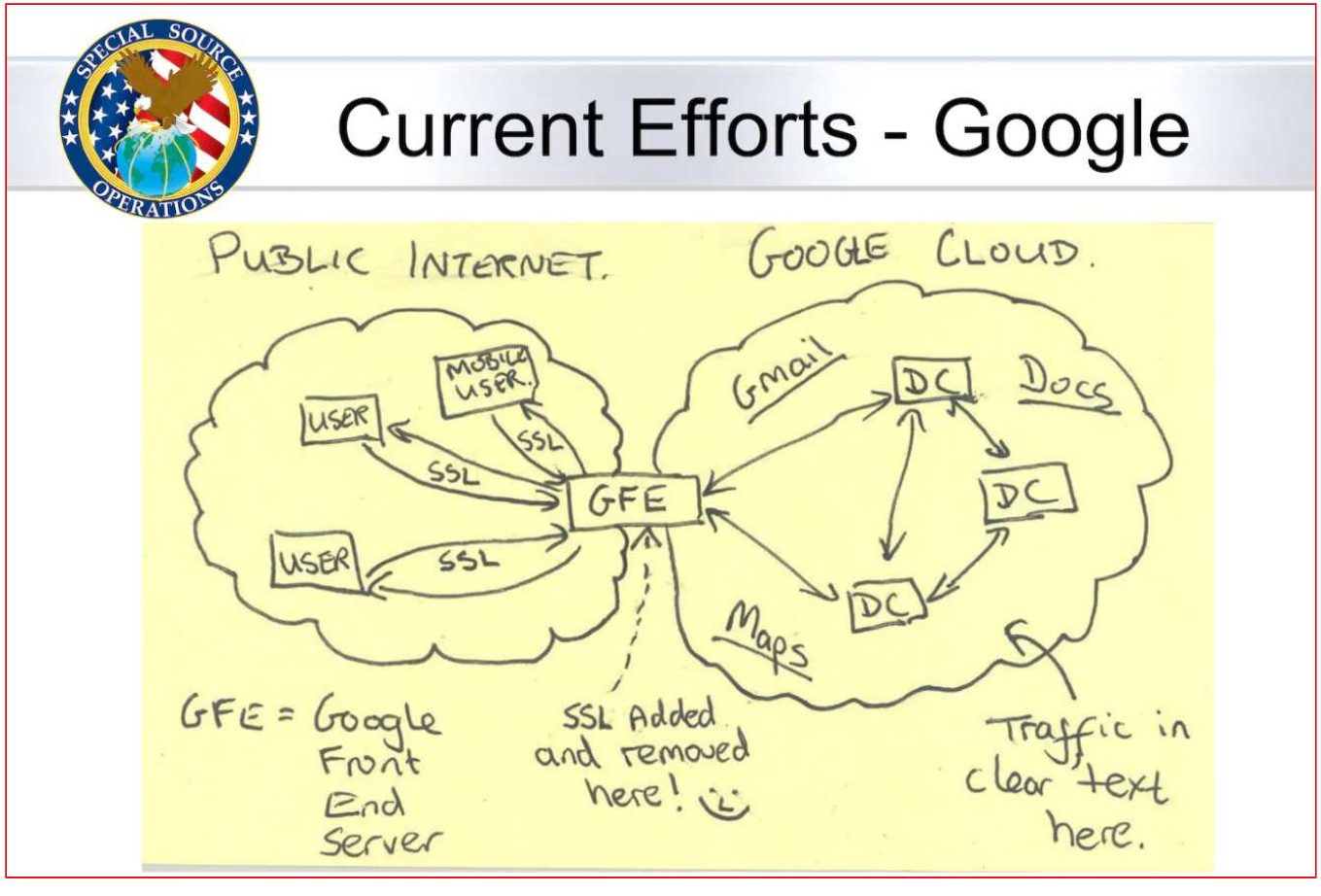
source: https://techcrunch.com - 05/08/2020


There is no cloud
it's just someone else's computer

iCloud legal terms (excerpt)

otherwise address security, fraud or technical issues; or (d) protect the rights, property or safety of Apple, its users, a third party, or the public as required or permitted by law. You acknowledge that Apple is not responsible or liable in any way for any Content provided by others and has no duty to screen such Content. However, consistent with Apple's privacy policy, Apple reserves the right at all times to determine whether Content is appropriate and in compliance with this Agreement, and may prescreen, move, refuse, modify and/or remove Content at any time, without prior notice and in its sole discretion, if such Content is found to be in violation of this Agreement or is otherwise objectionable.

Snowden / Muscular (2013)



Online storage is about:

- **Costs**: storage space (SSDs, Hard Drives) is damn expensive
- **Liability**: must take care of any unlawful file (and account)
- **Profitability**: nobody does it by charity 😇


THAT'S NO CLOUD STORAGE
IF YOU USE FREE
FILE SHARING WEBSITES
imgflip.com

Download Firefox

Systems and Languages What's New Privacy

What happened to Firefox Send?

Firefox Send has been discontinued as of September 17th, 2020. You will no longer be able to upload or receive files. We'd like to thank all of you who tried Firefox Send.

We started Firefox Send as a way for you to share files safely and easily from any browser. Unfortunately, some abusive users were beginning to use Firefox Send to ship malware and conduct phishing attacks. When this problem was reported, we stopped the service. Please see the Mozilla Blog for more details on why this service was discontinued.

What happened to the files I've sent in the past?

All files sent to Firefox Send have been securely wiped from our server. If you've shared files from your computer or device, the original files have not been moved, altered or deleted in any way by Firefox Send.

INTERNET

US authorities shut down file-sharing site Megaupload

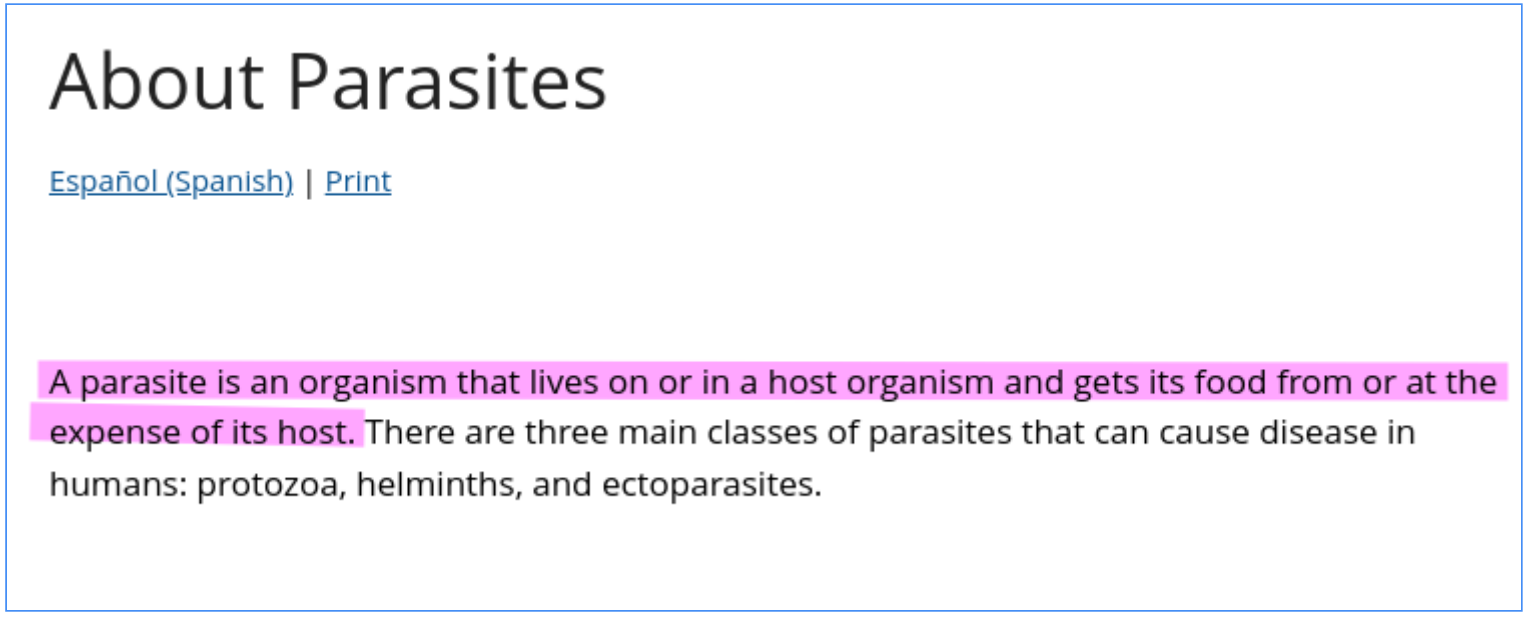
US authorities shut down file-sharing site Megaupload on Thursday and charged several of its officials with copyright infringement for allowing millions of illegal downloads. The site had 150 million registered users and some 50 million hits per day.

Issued on: 20/01/2012 - 07:23 Modified: 20/01/2012 - 07:42

Any way to share files freely ?

Parasitizing servers

Parasite



About Parasites

Español (Spanish) | Print

A parasite is an organism that lives on or in a host organism and gets its food from or at the expense of its host. There are three main classes of parasites that can cause disease in humans: protozoa, helminths, and ectoparasites.

source: Centers for Disease Control and Prevention (https://cdc.gov)

Modern parasitizing

- Abusing **temporary storage** features to **share files**
- Using **unexpected techniques** to store/retrieve data
- **No authentication** required
- Ideally **stealth** !

Sharing files with

Imgur

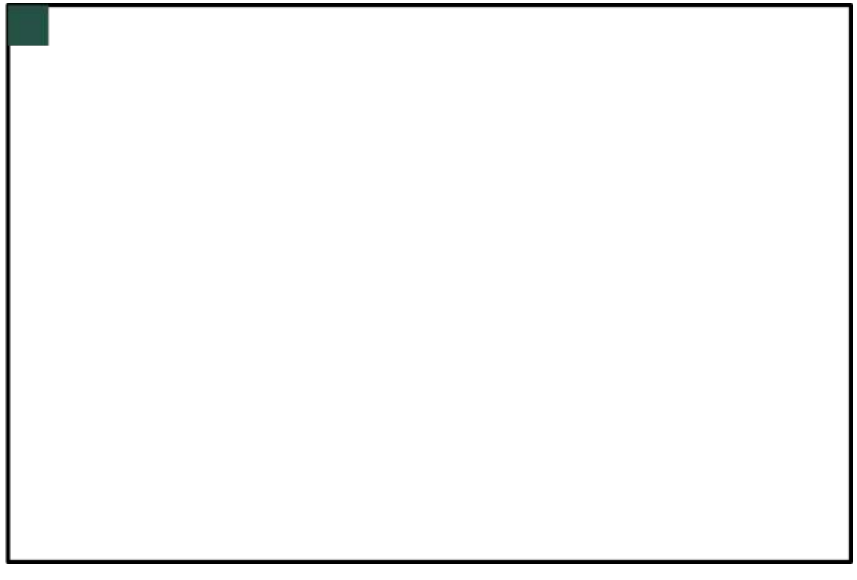
- **No account** required
- **PNG** file format supported
- Image **dimensions** untouched
- Image size limit: **20 MB**

PNG file format

- **Lossless** compression (DEFLATE)
- **Chunk-based** file format
- Supported by the **Python Imaging Library**

Bin file to PNG

```
25504446 2D312E36 0D25E2E3 CFD30D0A
36333720 30206F62 6A0D3C3C 2F4C696E
65617269 7A656420 312F4C20 34313131
36392F4F 20363430 2F452032 31373431
342F4E20 3132F54 20333938 333831 2F
48205B20 35313620 343434 5D 3E3E0D65
6E646F62 6A0D2020 20202020 20202020
20200D0A 78726566 0D0A3633 37203131
0D0A3030 30303030 30303136 20303030
3030206E 0D0A3030 30303030 30393630
20303030 3030206E 0D0A3030 30303030
31303832 20303030 3030206E 0D0A3030
30303030 31323131 20303030 3030206E
0D0A3030 30303030 31343639 20303030
```



Bin file to PNG

```
25504446 2D312E36 0D25E2E3 CFD30D0A
36333720 30206F62 6A0D3C3C 2F4C696E
65617269 7A656420 312F4C20 34313131
36392F4F 20363430 2F452032 31373431
342F4E20 3132 2F54 20333938 33383 12F
48205B20 35313620 343434 5D 3E3E0D65
6E646F62 6A0D2020 20202020 20202020
20200D0A 78726566 0D0A3633 37203131
0D0A3030 30303030 30303136 20303030
3030206E 0D0A3030 30303030 30393630
20303030 3030206E 0D0A3030 30303030
31303832 20303030 3030206E 0D0A3030
30303030 31323131 20303030 3030206E
0D0A3030 30303030 31343639 20303030
```

Bin file to PNG

```
25504446 2D312E36 0D25E2E3 CFD30D0A
36333720 30206F62 6A0D3C3C 2F4C696E
65617269 7A656420 312F4C20 34313131
36392F4F 20363430 2F452032 31373431
342F4E20 3132F54 20333938 333831 2F
48205B20 35313620 343434 5D 3E3E0D65
6E646F62 6A0D2020 20202020 20202020
20200D0A 78726566 0D0A3633 37203131
0D0A3030 30303030 30303136 20303030
3030206E 0D0A3030 30303030 30393630
20303030 3030206E 0D0A3030 30303030
31303832 20303030 3030206E 0D0A3030
30303030 31323131 20303030 3030206E
0D0A3030 30303030 31343639 20303030
```

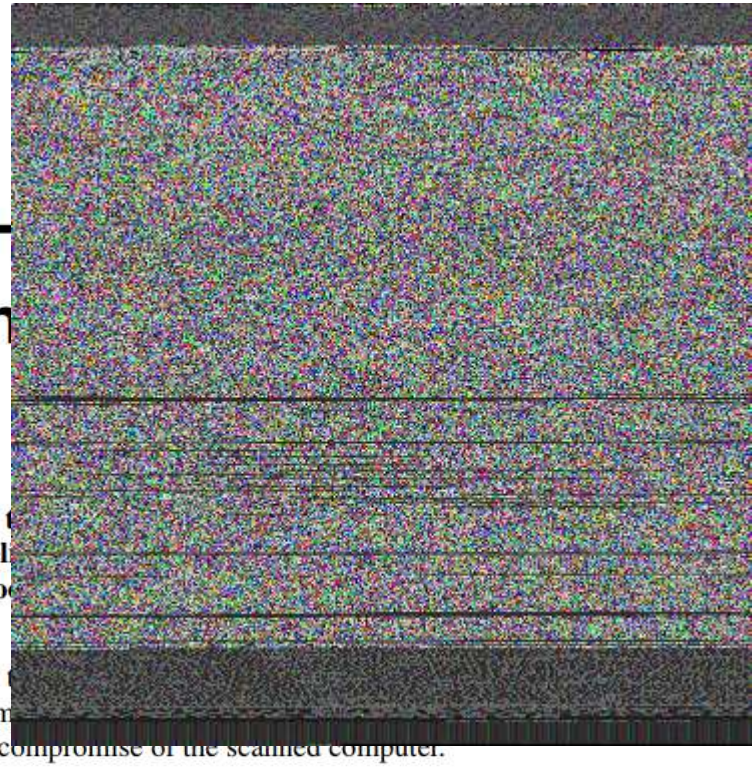
Bin file to PNG

```
25504446 2D312E36 0D25E2E3 CFD30D0A
36333720 30206F62 6A0D3C3C 2F4C696E
65617269 7A656420 312F4C20 34313131
36392F4F 20363430 2F452032 31373431
342F4E20 3132F54 20333938 333831 2F
48205B20 35313620 34343 45D 3E3E0D65
6E646F62 6A0D2020 20202020 20202020
20200D0A 78726566 0D0A3633 37203131
0D0A3030 30303030 30303136 20303030
3030206E 0D0A3030 30303030 30393630
20303030 3030206E 0D0A3030 30303030
31303832 20303030 3030206E 0D0A3030
30303030 31323131 20303030 3030206E
0D0A3030 30303030 31343639 20303030
```

Bin file to PNG

```
def encode_image(in_file, output):
    # Load file into memory and prefix with metadata
    content = open(in_file, 'rb').read()

    # Compute image size
    nb_pixels = ceil(len(content)/3)
    width, height = int(sqrt(nb_pixels)), int(nb_pixels/width)
    if width*height < nb_pixels:
        height += 1

    # Pad our content to match the expected size
    content += b'\x00'*(width*height*3 - len(content))

    img = Image.frombytes('RGB', (width, height), content)
    img.save(output)
```

PDF to PNG



Chapter 1

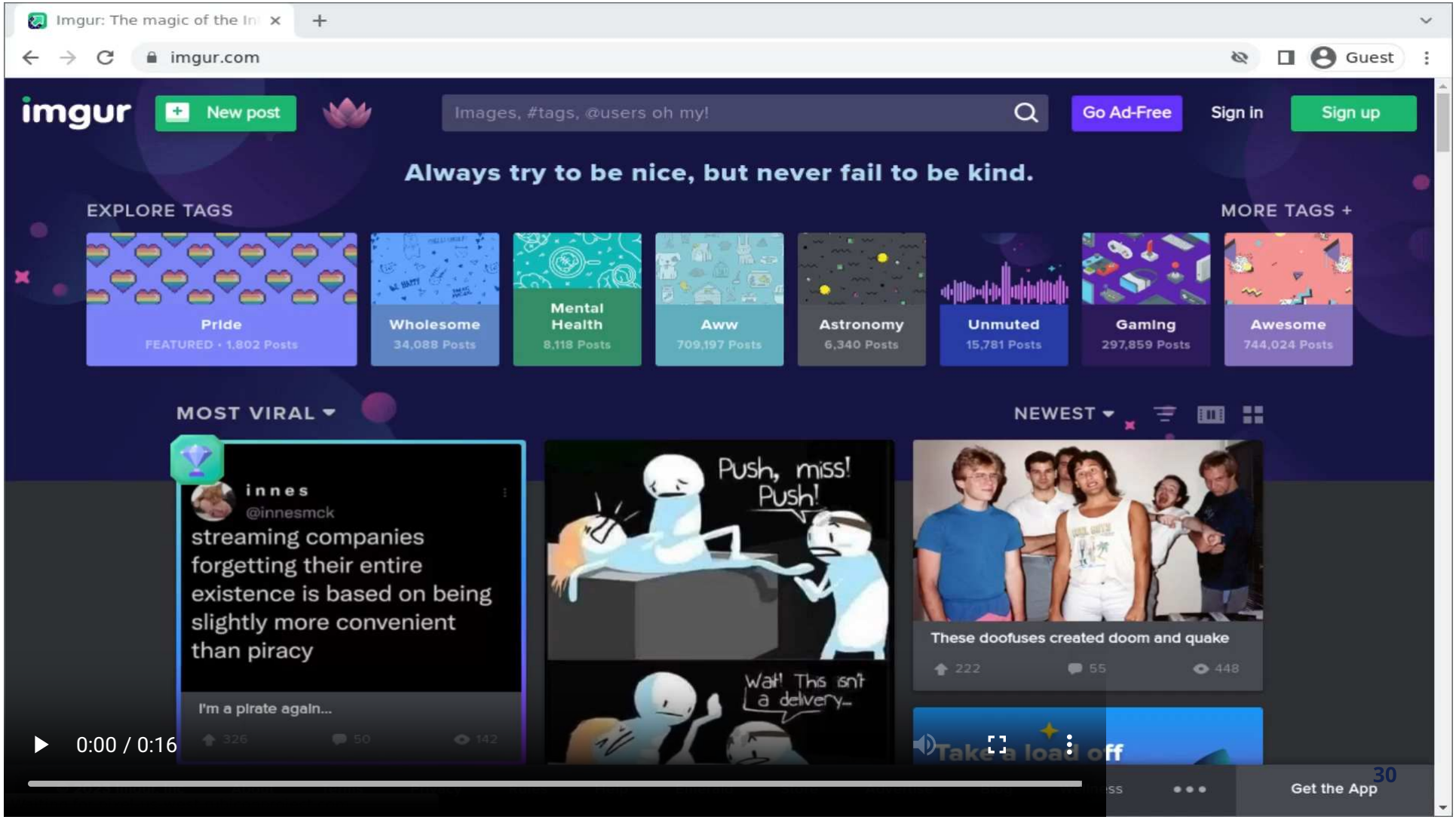
Nmap: The Internet Considered H
Inference Cheking Kludge Scann

**In this article, we disclose specially for Hakin9 magazine the inner working of t
Scanner, an extension of the world famous NMAP scanner. Even though we bel
familiar with classic Nmap use as a port scanner, using Nmap as a weaponized to
not public.**

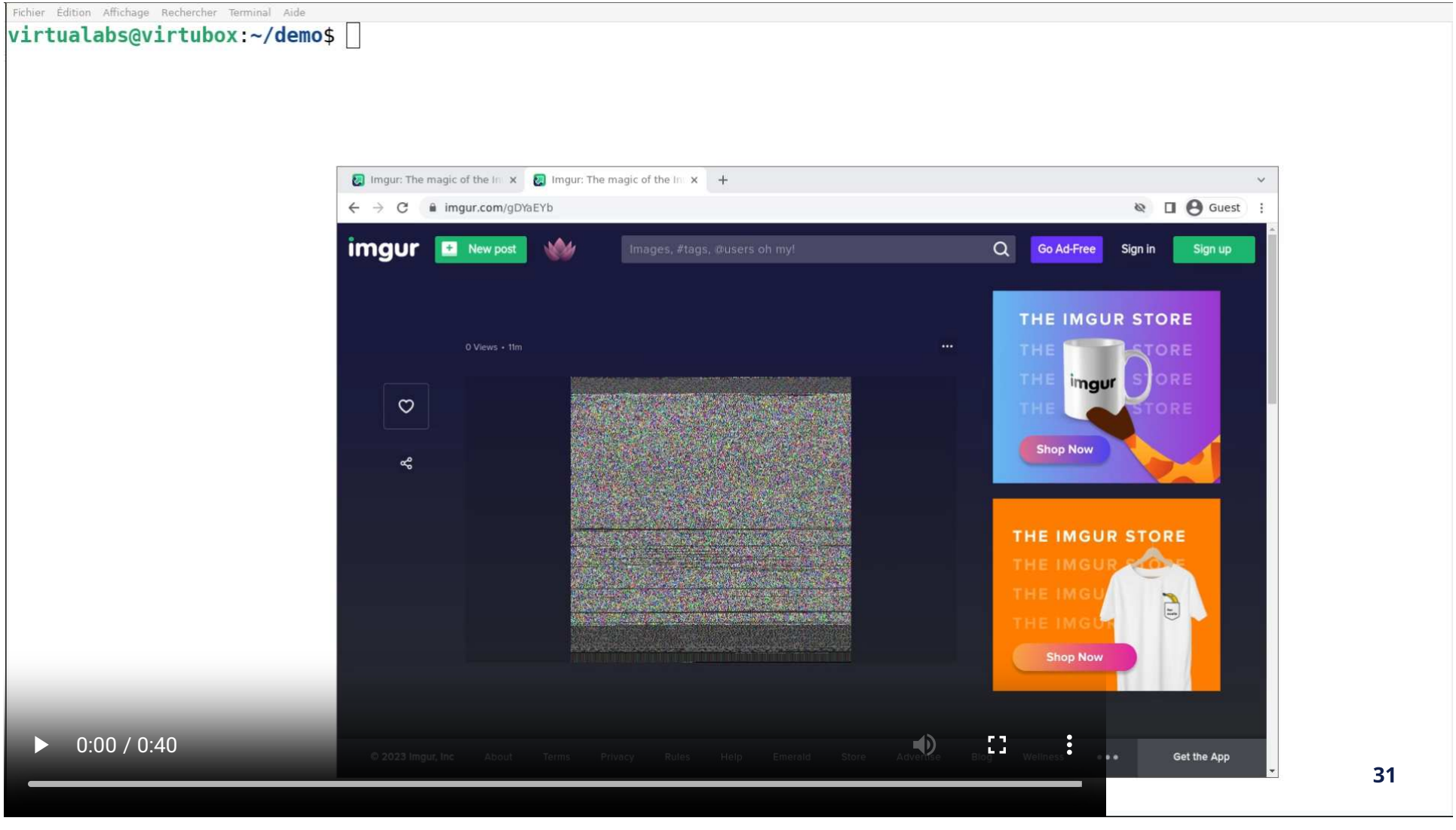
Since this project is DARPA classified, we will unfortunately not be able to share
nonetheless share demos of the tool, and provide concrete evidence that pushing CPU m
after a kernel pool heap overflow is practical, hence achieving permanent full remote compromise of the scanned computer.

The Nmap hardware and architecture solution to scatter/gather I/O is defined not only by the emulation of object-oriented languages, but also by the essential need for model checking. This is an important point to understand. After years of confirmed research into spreadsheets [1], we argue the visualization of NMAP, which embodies the structured principles of cryptanalysis. We skip a more thorough discussion due to re- source constraints. In our research we use cacheable configurations to confirm that on- line algorithms and courseware can cooperate to accomplish this mission.

Upload to Imgur

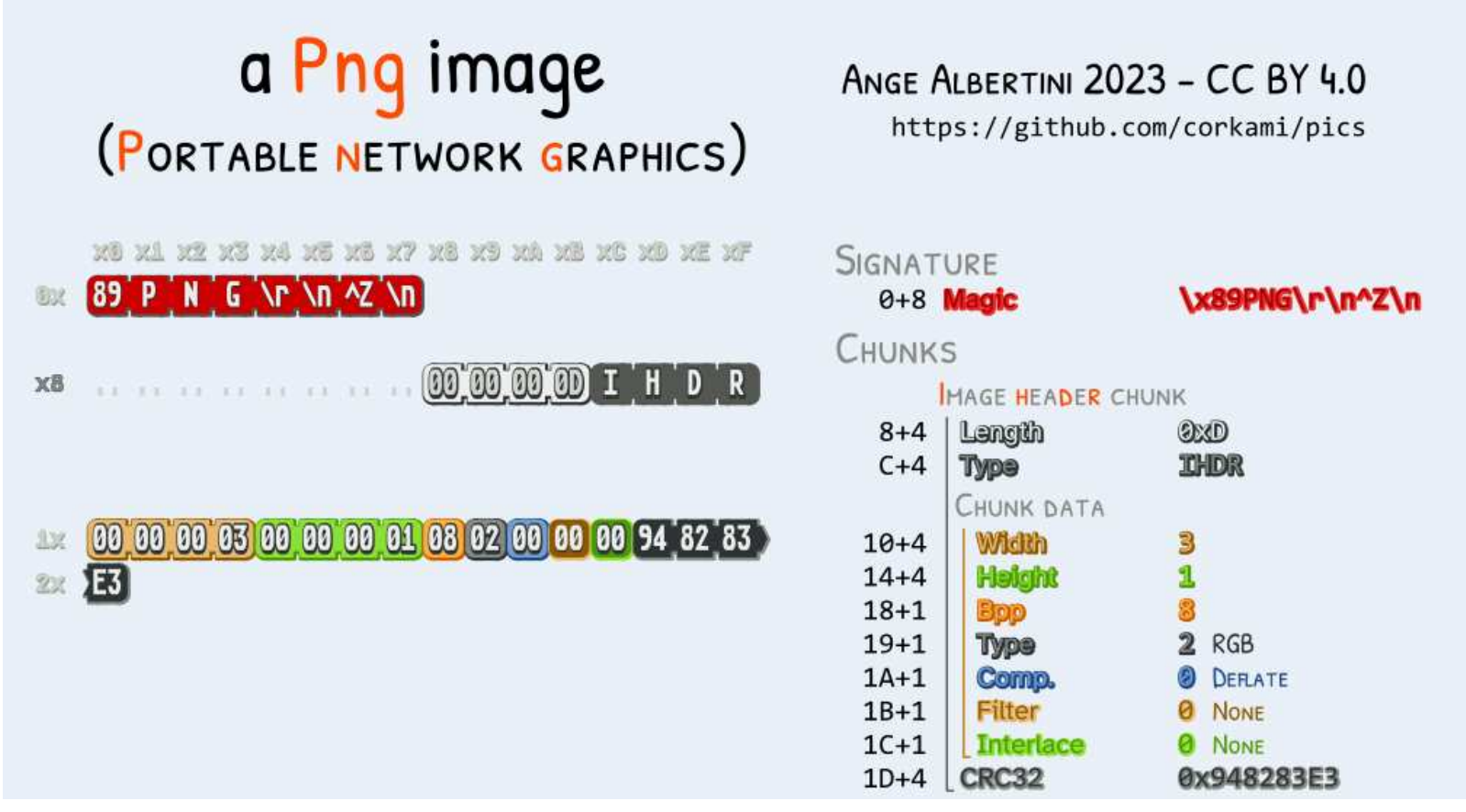


Download from Imgur

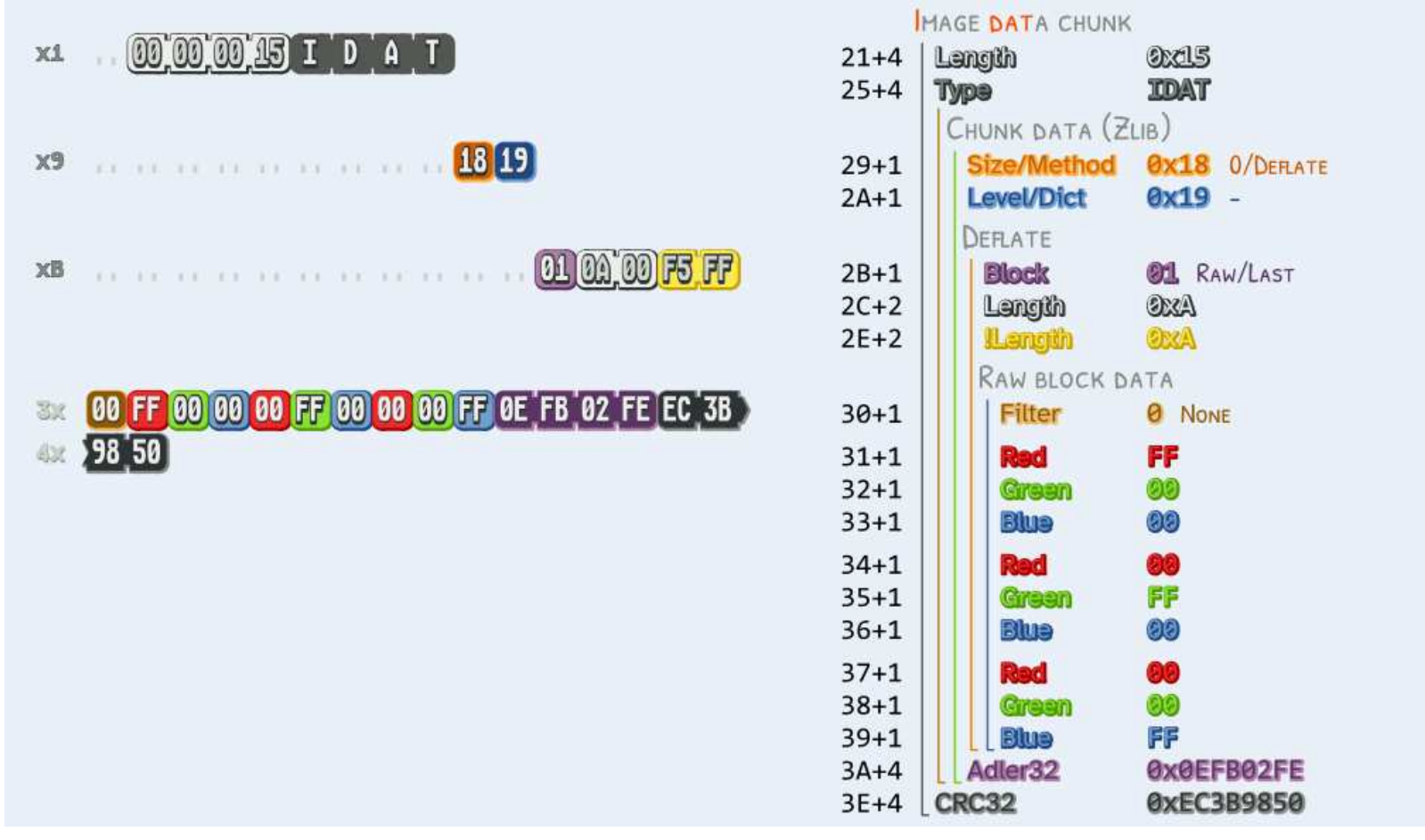


Going deeper with PNG

PNG structure (1/3)



PNG structure (2/3)



PNG structure (3/3)

Ancillary chunks

- **tIME**: the time that the image was last changed
- **dSIG**: stores digital signature
- **eXIf**: stores Exif metadata
- **tEXt**: ISO/IEC 8859-1 text
- ...

Creating a PNG/PDF polyglot

a tribute to Ange Albertini

La spécification officielle stipule que la première ligne d'un *PDF* doit être sa signature :

7.5.2 File Header

The first line of a PDF file shall be a *header* consisting of the 5 characters %PDF– followed by a version number of the form 1.N, where N is a digit between 0 and 7.

En pratique, il n'en n'est rien, il est juste requis sous *Adobe Reader* qu'une signature valide soit présente dans les 1024 (`0x400`) premiers octets.

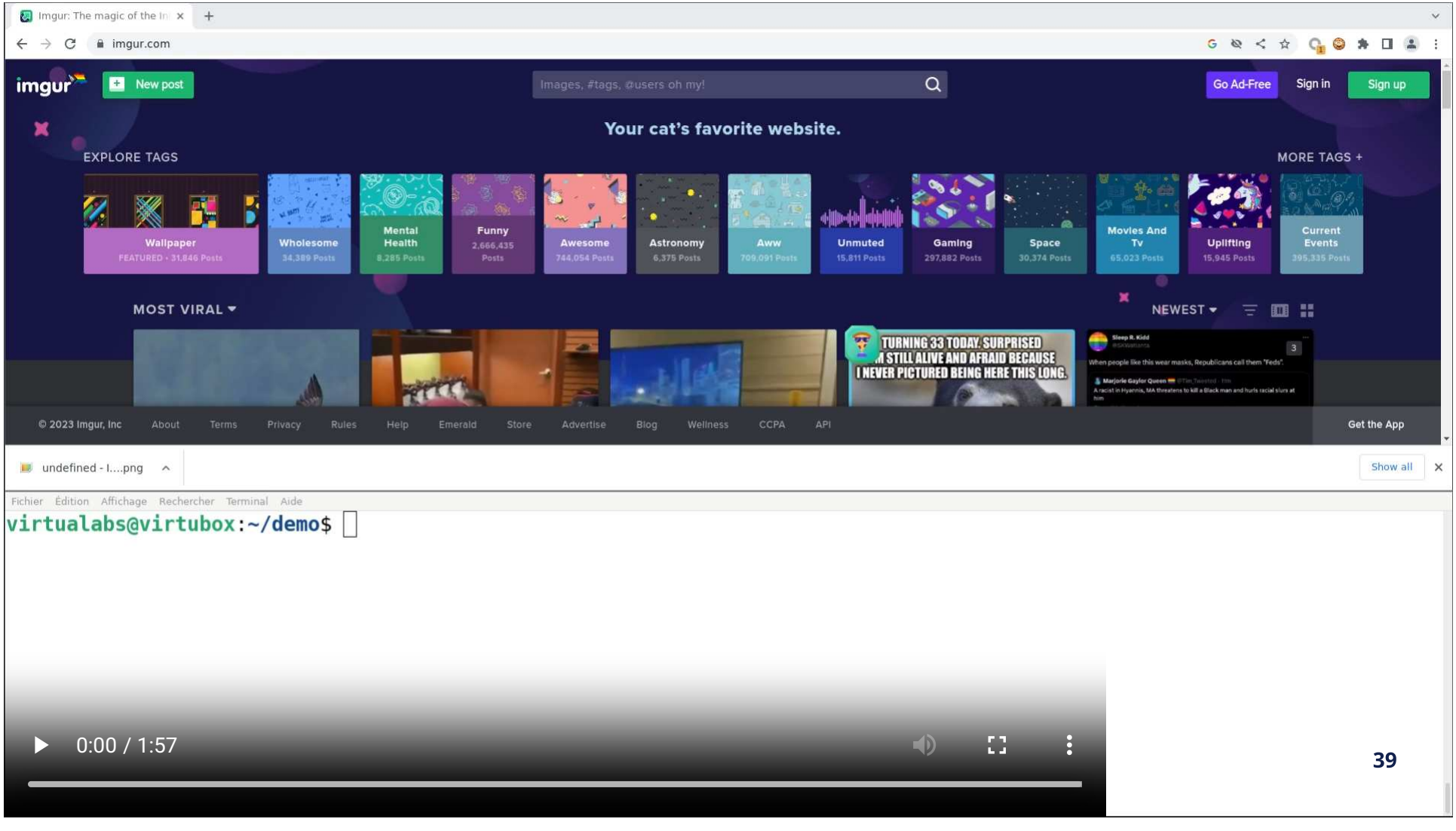
source: Polyglottes binaires et implications, Ange Albertini, SSTIC 2013

Creating a PNG/PDF polyglot

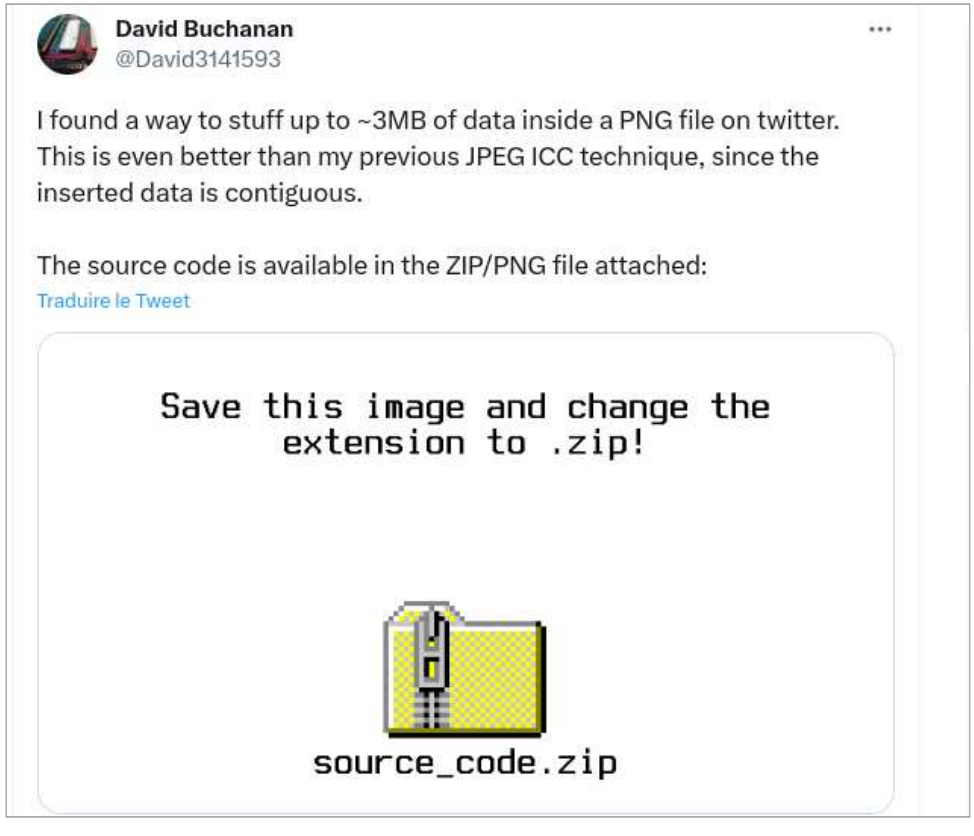
a tribute to Ange Albertini

```
import png

# Read our PNG file and payload
cat = png.Reader('cat.png')
payload = open('hackin9.pdf', 'rb').read()

# Inject a tEXT chunk
chunks = list(cat.chunks())
chunks = chunks[:2] + [(b'tEXT', payload)] + chunks[2:]

# Write output file
with open('out.png','wb') as f:
    png.write_chunks(f, chunks)
    f.close()
```

No file is too big, no pic is too small !



Tweetable ZIP file



Bin file to animated QR Code

<packt>hub

DATA NEWS

Introducing TXQR, data transfer via animated QR codes

By **Amrata Joshi** - JANUARY 4, 2019 - 2:23 AM 5560 0

3 min read

TXQR is a project for transferring data via animated QR codes. It is written in Go and uses fountain erasure codes. Ivan Daniluk, it's creator and software engineer has shared his experience in building TXDR and also the results of using animated QR as a data transfer method.

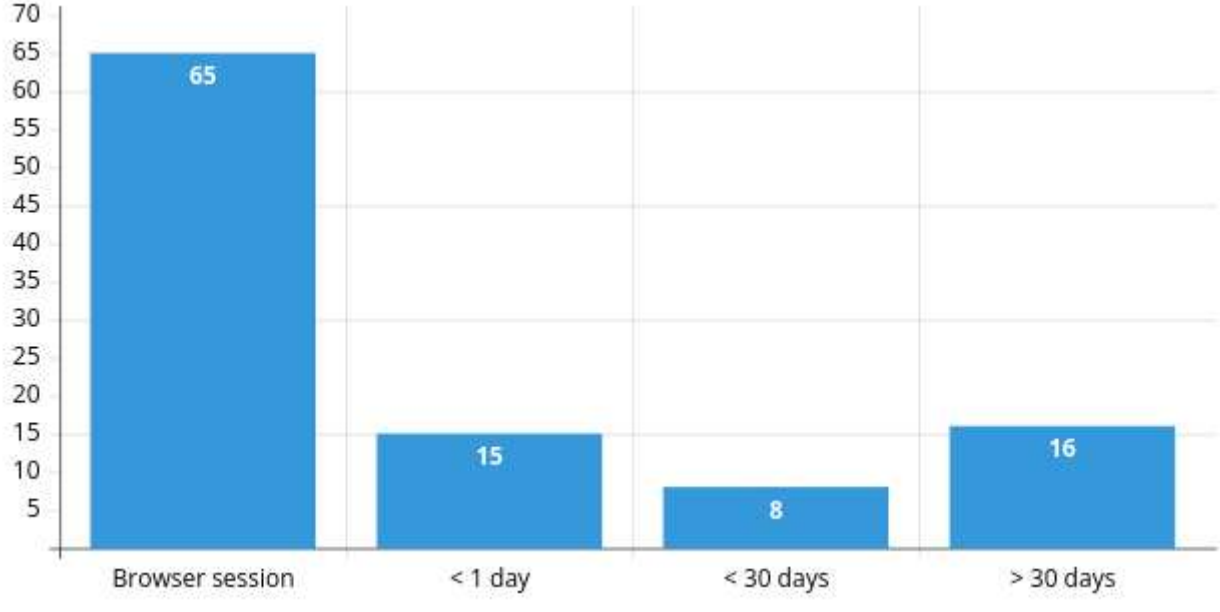

NOT REALLY
STEALTH

Parasitizing web sessions

Web sessions

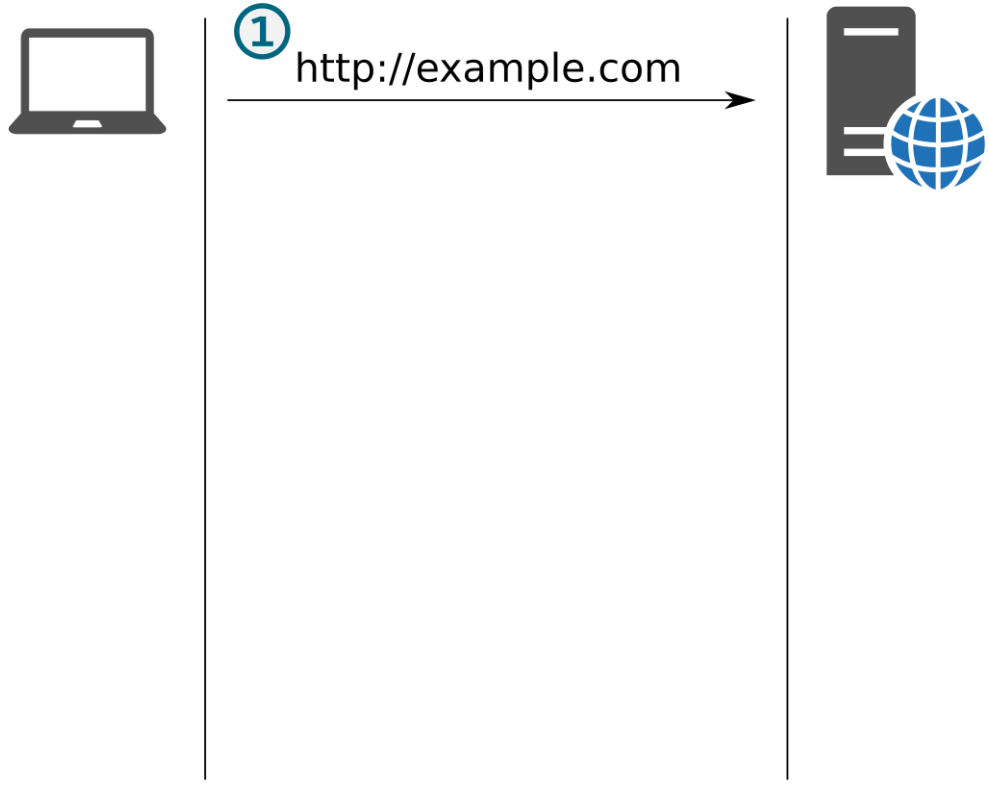
- Identified by a session **cookie** 🍪
- **Store data** associated to a user (server side)
- Web application **controls the data** stored in session

Web sessions expiry

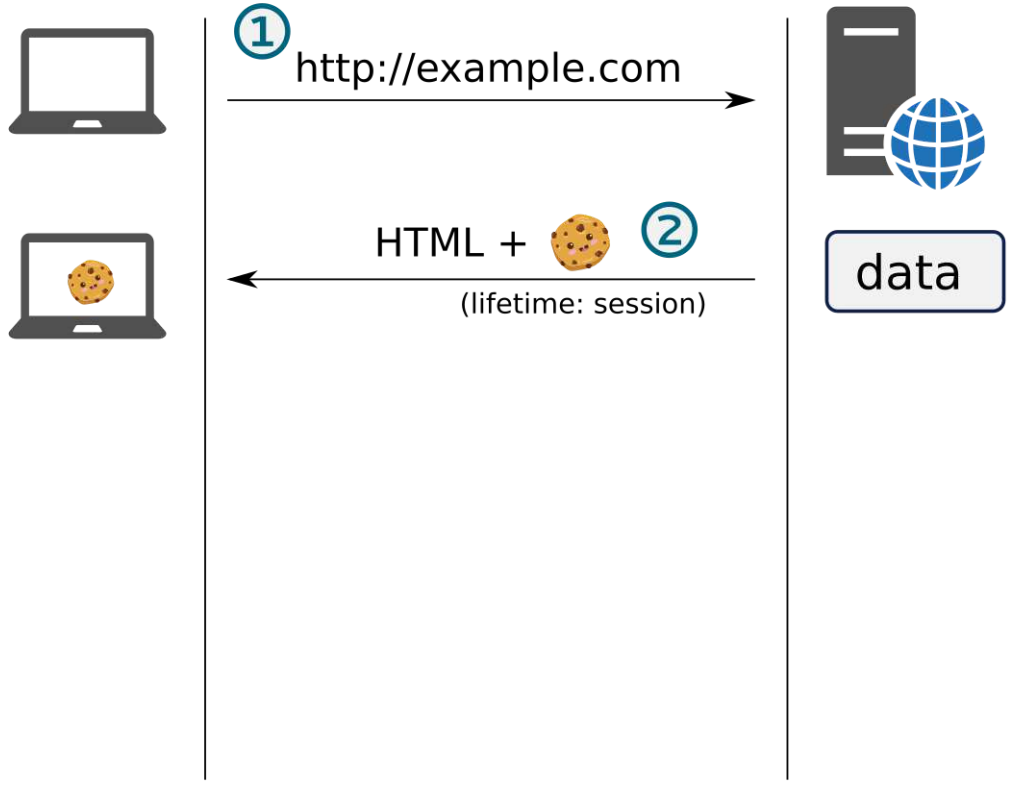


104 on 1000 (~ 10%) top-ranked websites set session cookies on first page

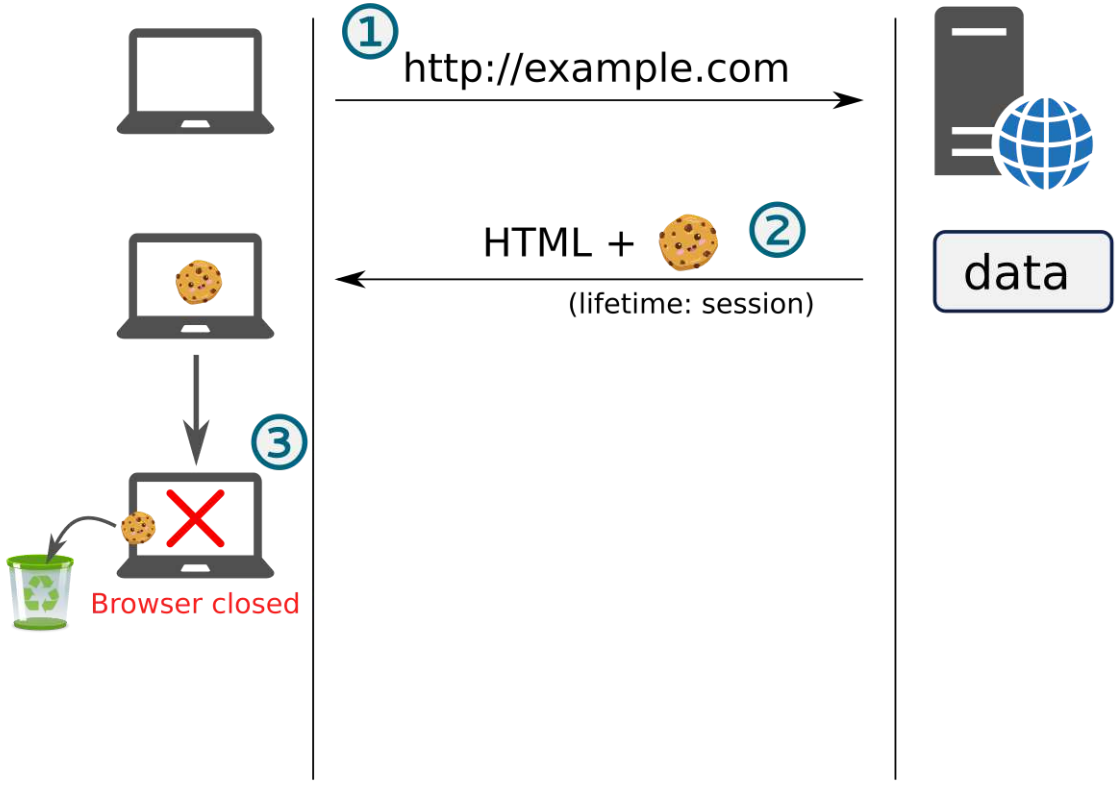
Web sessions expiry



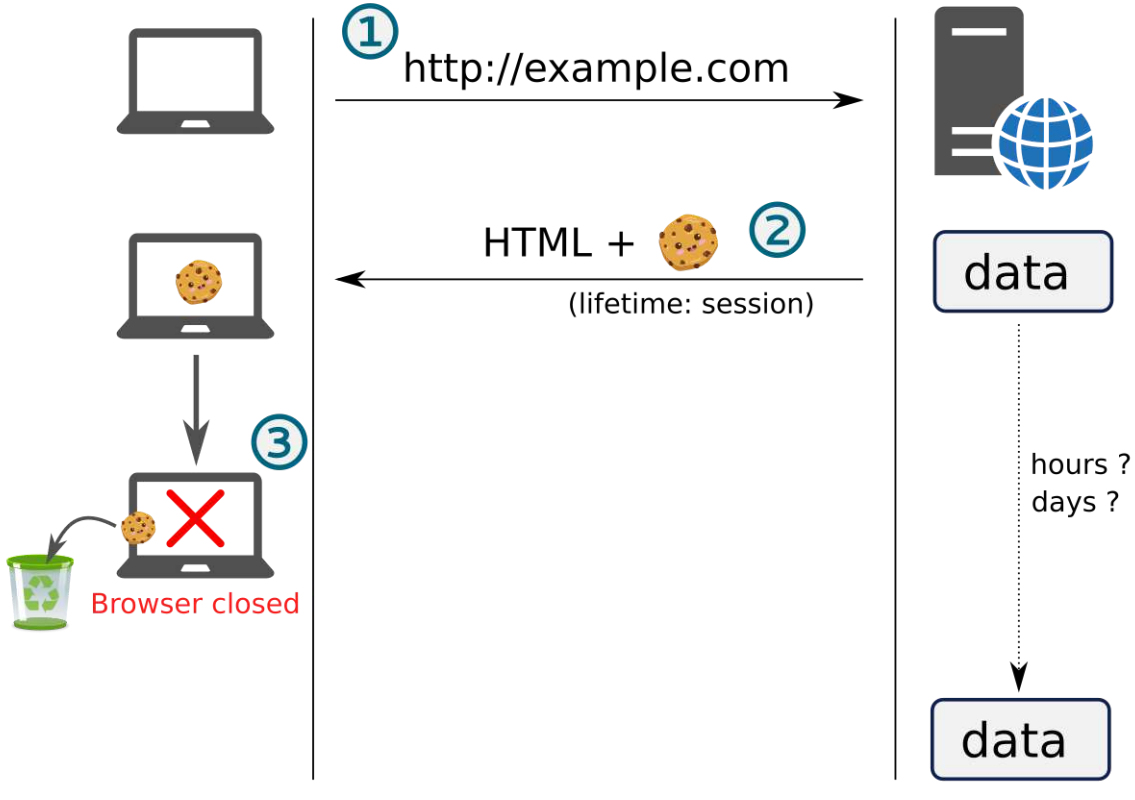
Web sessions expiry



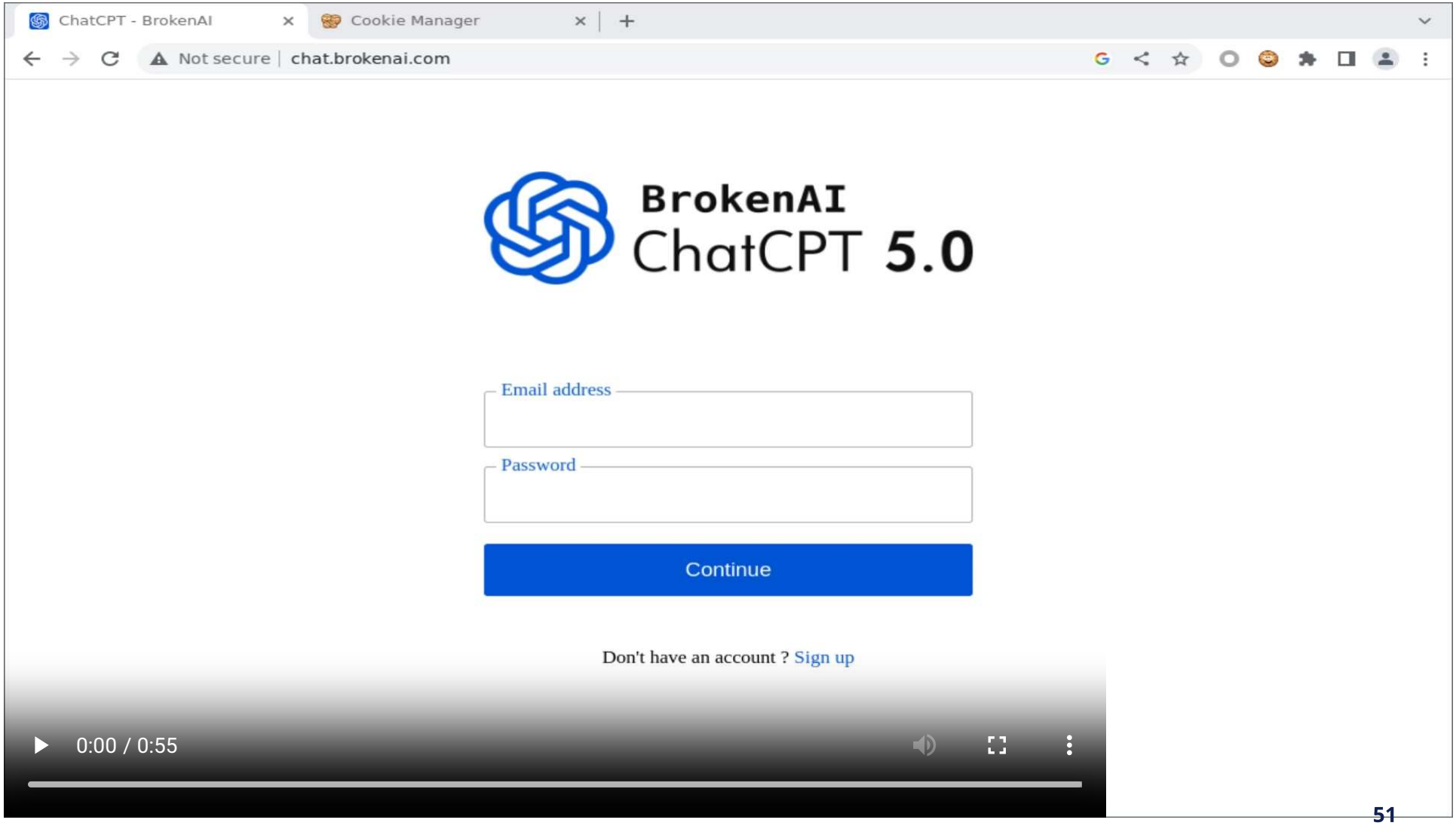
Web sessions expiry



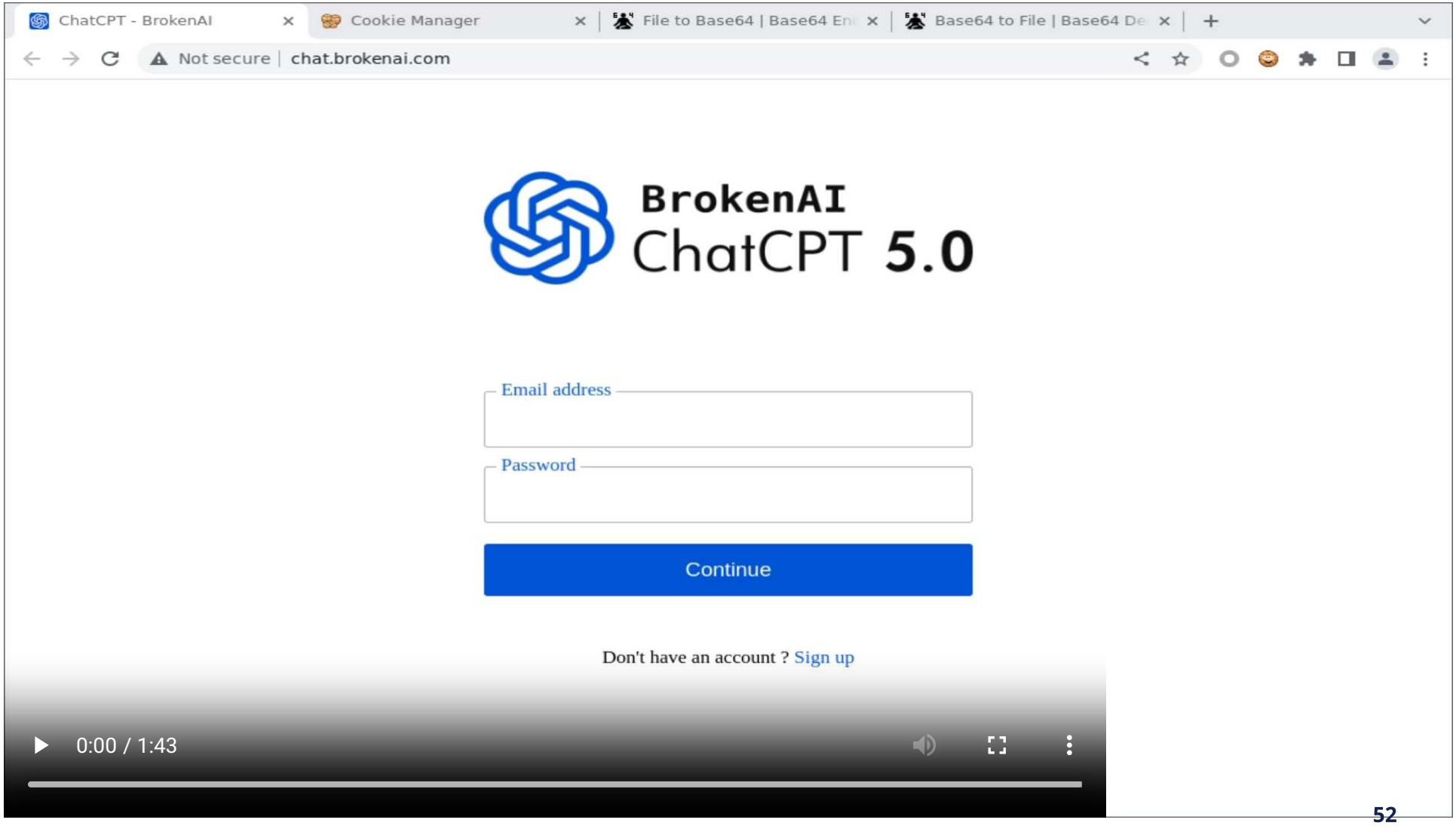
Web sessions expiry



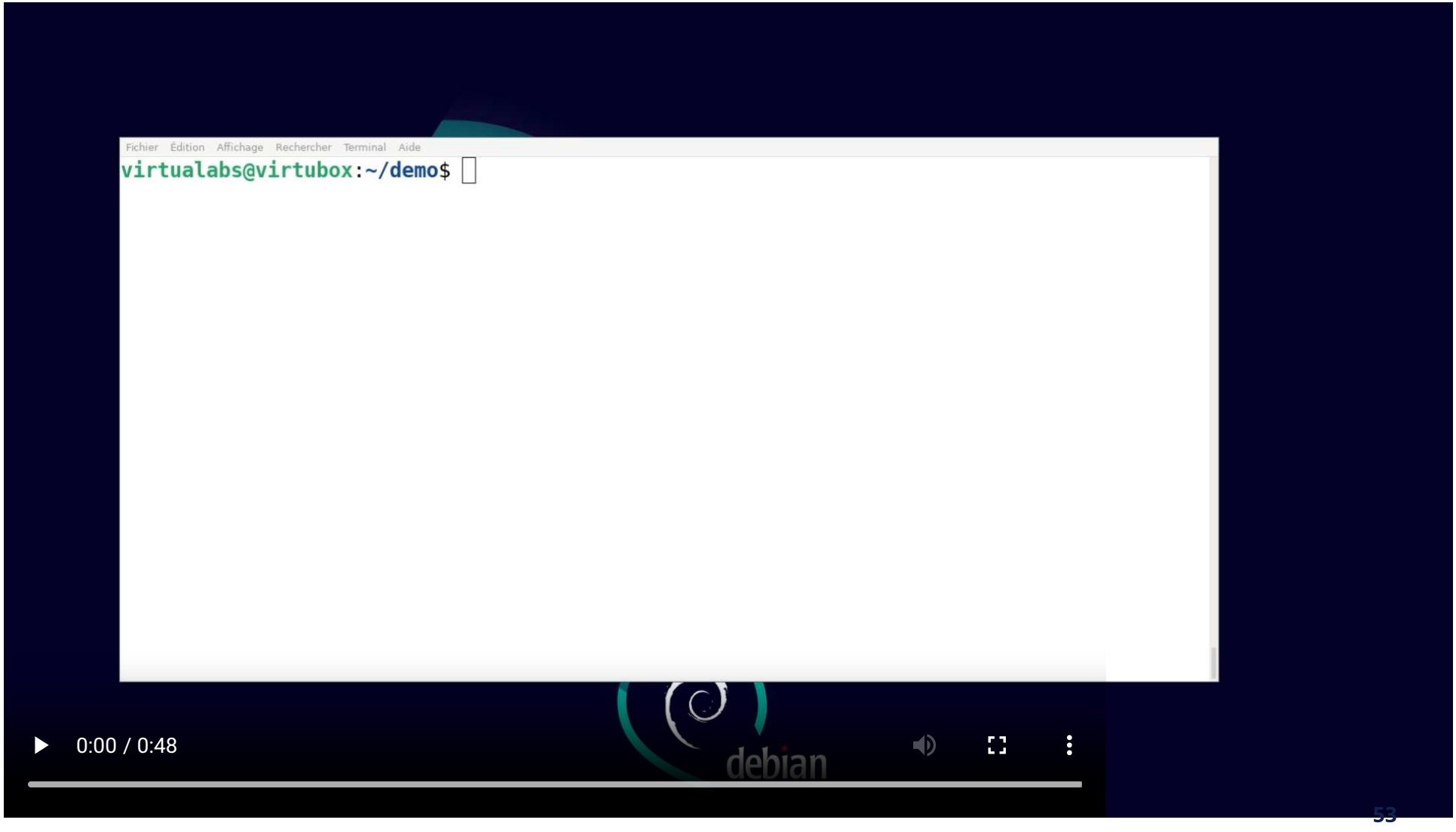
Web sessions



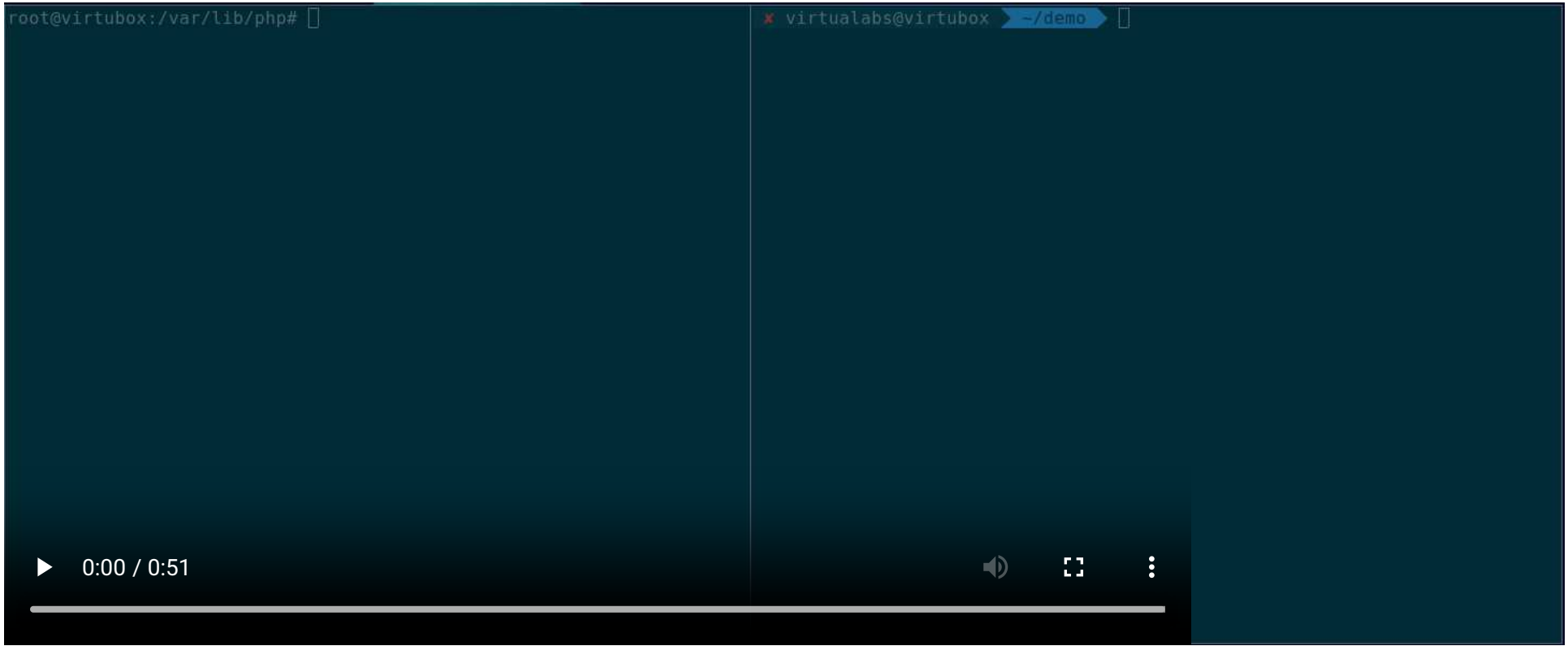
Uploading and downloading



Tooling


Fichier Édition Affichage Rechercher Terminal Aide
virtualabs@virtubox:~/demo$
0:00 / 0:48
debian

Server perspective



Sessions as cloud storage ?

- **Limited lifetime** (from 5 minutes to multiple months)
- **Limited storage size**
- Content is **rarely tracked/monitored**

What are the risks ?

- **Unsollicited file upload** on a server
- **C2** covert channel
- **Illegal** file storage/sharing
- **Denial of service** through storage space exhaustion
- **Alert messages spamming** in case a malicious file is repeatedly uploaded

How frequent is it ?

- **Many well-known websites** are/were vulnerable (some of them have already been notified)
- **Bad practices** in session management are **quite common**

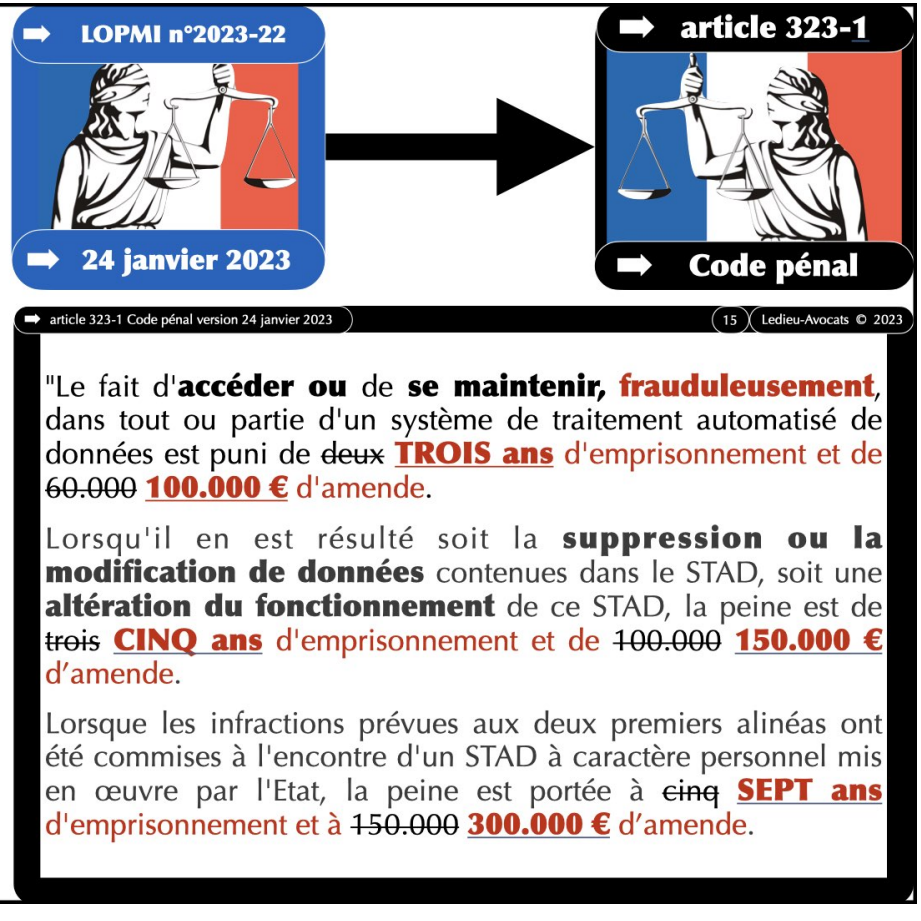
Remediation

- Input validation: **check input format and size**
- Don't let your **sessions live for months** !
- Store data in **localStorage** instead !

Legal warning

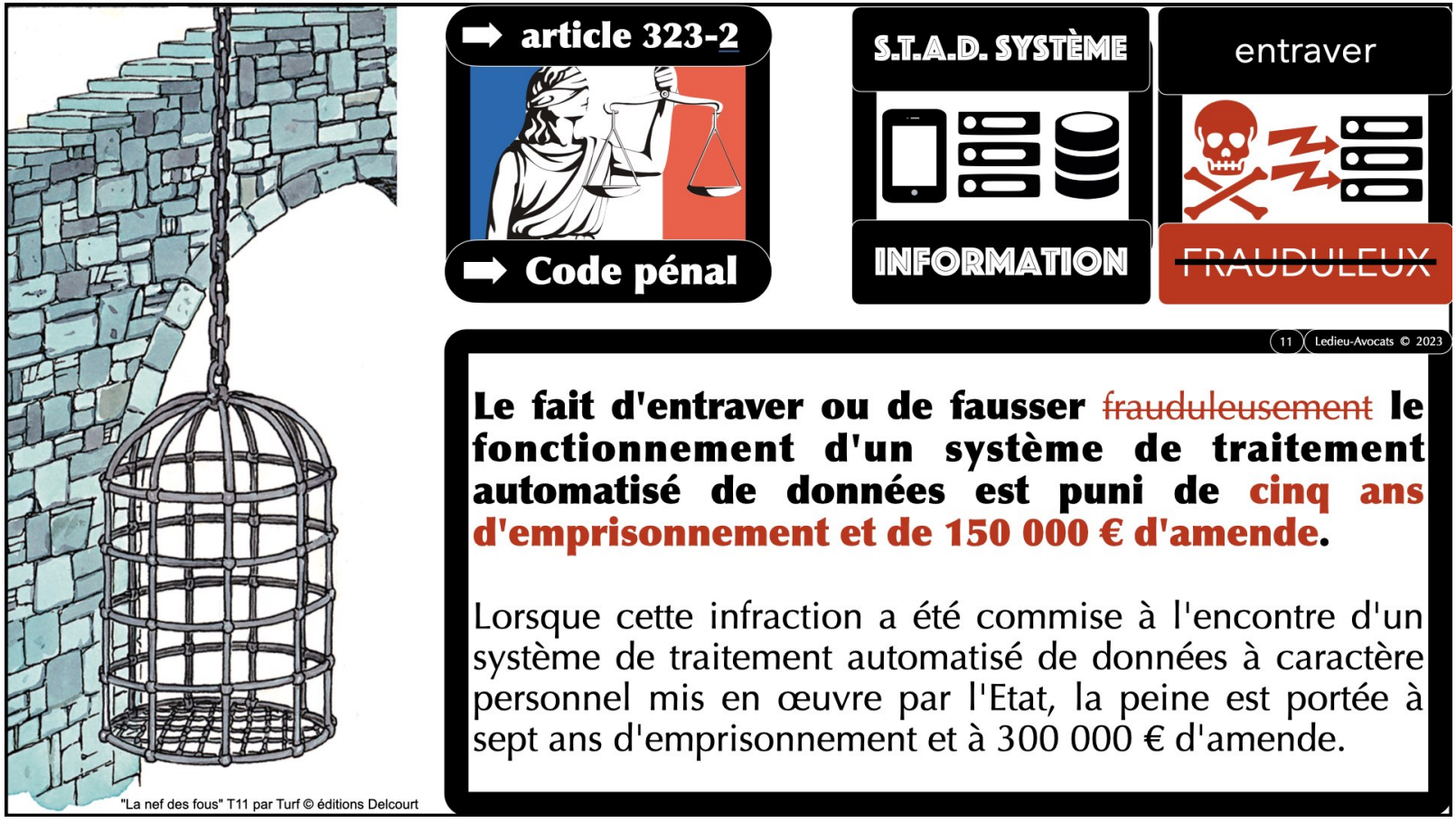
(French law only)

Article 323-1 du CP



© 2023 Marc-Antoine Ledieu - https://technique-et-droit-du-numerique.fr/

Article 323-2 du CP



© 2023 Marc-Antoine Ledieu - https://technique-et-droit-du-numerique.fr/

Article 323-3 du CP

© 2023 Marc-Antoine Ledieu - https://technique-et-droit-du-numerique.fr/

Conclusion

Takeaways

- Any temporary **image storage service** can be turned into a **file sharing service**
- **Web sessions** can be used to anonymously **store and retrieve files**
- **Follow best practices** to avoid abuse

Code, PoC, tools

https://github.com/virtualabs/lehack23-parasite

Special thanks to Guillaume Valadon, Philippe Teuwen and Jean-Philippe Gaulier for their reviews & Marc-Antoine Ledieu for his amazing work and advices

Thanks ! Questions ?

Damien Cauquil

dcauquil@quarkslab.com
@virtualabs@mamot.fr
quarkslab