Lookyloo

What the heck are these webpages up to?

Quinn Norton - @quinnnorton

Raphaël Vinot - @rafi0t

circl.lu
Computer Incident
Response Center
LUXEMBOURG

Des manifestants entrent de force dans le Parlement à Hongkong
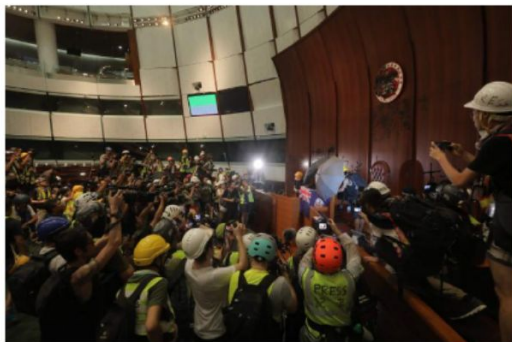
Alors que des dizaines de milliers de personnes ont investi les grandes artères de la ville pour marquer le 22e anniversaire de la rétrocession à la Chine, des contestataires ont pénétré dans le siège du Parlement.

• A Hongkong, la désobéissance civile s'installe dans la durée

• « Il n'y a rien d'autre à faire, en tant que Hongkongais il faut manifester »

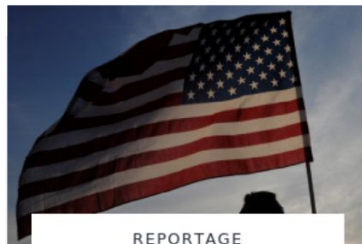**Polémique Marion Maréchal : le premier faux pas de Roux de Bézieux, pacificateur du Medef**

ANALYSE

« Quand j'ai mes règles, je dois choisir entre manger ou
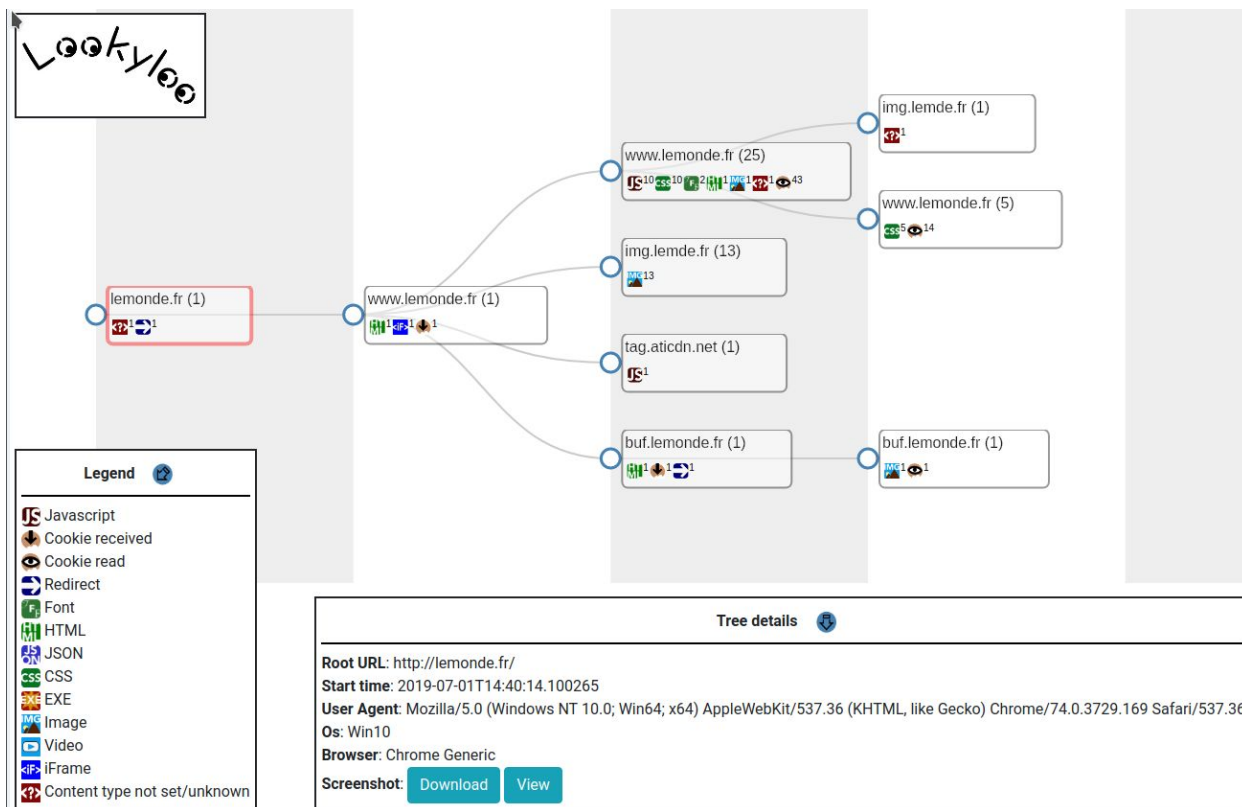

REPORTAGE

Arnaud Leparmentier

Les camps d'été capitalistes, ou le rêve américain

A Miami, des jeunes âgés de 14 à 17 ans participent à des stages leur permettant d'appréhender le monde des affaires. Ils ont une semaine pour préparer et présenter un business plan.

5 min de lecture

S'abonner c'est...

Simple site

Le Scan Politique | International | Economie | Bourse | Décideurs | Le Scan Eco | Sport24 | Le Scan Sport | Culture | ‹ ›

LE FIGARO PREMIUM Abonnez-vous

EN CE MOMENT Balkany : un procès hors normes Affaire Vincent Lambert Brexit La Lettre du Figaro Premium

CRISE À HONGKONG

Hongkong: des manifestants sont entrés dans le siège du Parlement

Une contestation historique se déroule dans le pays depuis désormais plusieurs semaines. Une grande manifestation se tenait ce lundi pour l'anniversaire de la rétrocession d'Hongkong à la Chine. Les manifestants ont déployé un drapeau de l'époque britannique dans le Parlement.

💬 38 ↱ 12 ⊕ International

Crise à Hongkong: les six questions qui se posent 𝐅

FOCUS - La débâcle politique qui entoure la suspension du projet de loi d'extradition témoigne de la fragilité du statut semi-indépendant de la ville, que Pékin ne cesse de bafouer.

💬 ↱ ⊕ International

Entre Hongkong et Pékin, un long bras de fer pour la démocratie 𝐅

Le Flash

Actualité | Économie | Sport

14:24 Hongkong: un drapeau de l'époque britannique déployé dans le Parlement

14:17 Migrants: trois nouveaux centres d'accueil vont ouvrir à Paris

14:14 Djokovic fait le job contre Kohlschreiber

14:10 Donald Trump avait prévenu dès lundi qu'il pourrait rencontrer Kim Jong-un

14:07 Grenoble: le procès de l'école musulmane d'Échirolles renvoyé en novembre

14:02 Au Louvre, manifestation contre le financement du musée par l'argent des opiacés

13:55 Militants écologistes évacués: EELV, le PS et Marion Cotillard s'insurgent

13:46 Benjamin Griveaux prédit le rassemblement des candidats LREM à Paris
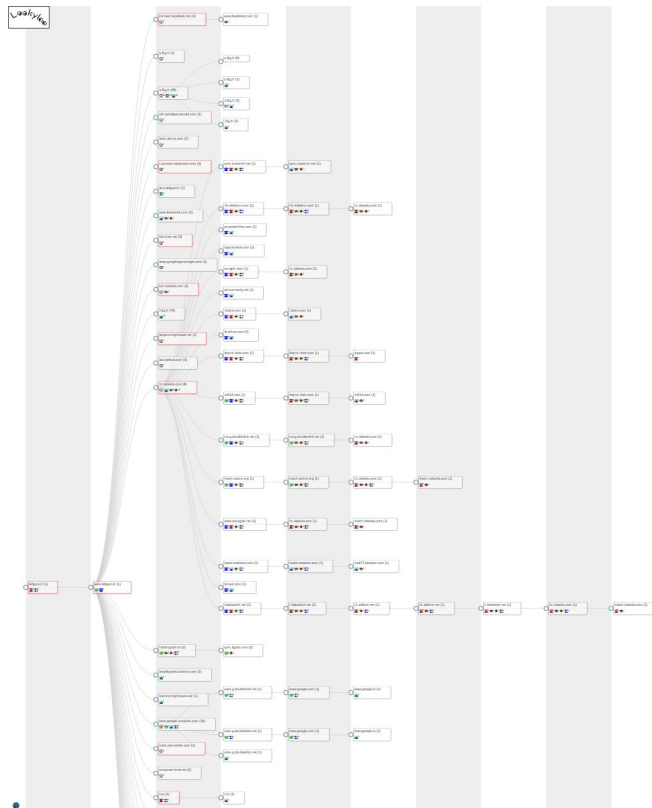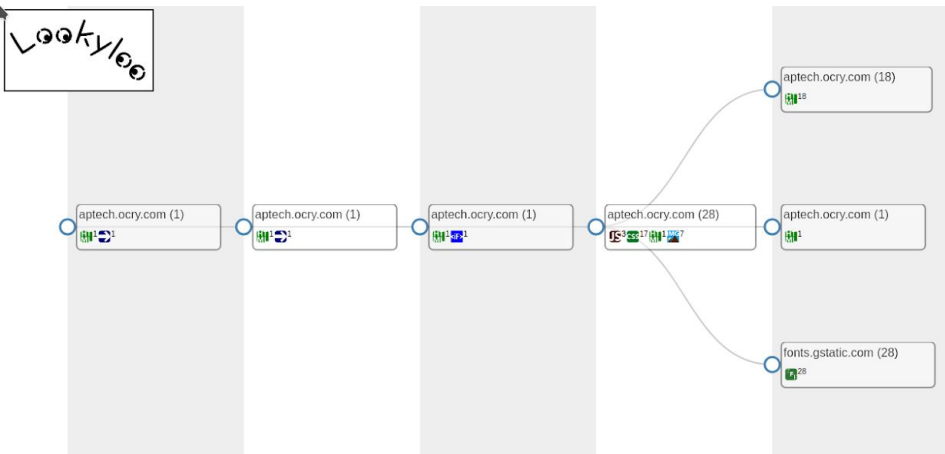
📶 Tout le flash actu ›   ‹ 1 /8 ›

LE FIGARO ET SES MAGAZINES

LE FIGARO

Édition du 01 juillet 2019

Not so simple

Lookyloo

aptech.ocry.com (1)

aptech.ocry.com (1)

aptech.ocry.com (1)

aptech.ocry.com (28)

aptech.ocry.com (18)

aptech.ocry.com (1)

fonts.gstatic.com (28)

Try Dropbox Business

Dropbox

Download the app

Email Validation

🔒 Please select your email provider and sign in to view the file.

G

Y

AOL.

EMAIL

Dropbox
Install
Mobile
Pricing
Business
Enterprise

About us
Dropbox Blog
About
Branding
News
Jobs

Support
Help Center
Contact us
Copyright
Cookies
Privacy & Terms

Community
Referrals
Forum
Twitter
Facebook
Developers

English (United States)

Tree details

Root URL: https://aptech.ocry.com/
Start time: 2019-07-01T06:59:49.177266
User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36
Screenshot: Download   Hide

What makes sites complicated?

What makes sites complicated?

… and how do we capture that?

Under the hood

Reading the tree

URL:	URL to scrape

Link Depth:	1 ▾

☑ Display on main page

Browser Configuration

Operating System:	Win10 ▾
Browser Type:	Chrome Generic ▾
User Agent:	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 ▾

Start looking!

Reading the tree
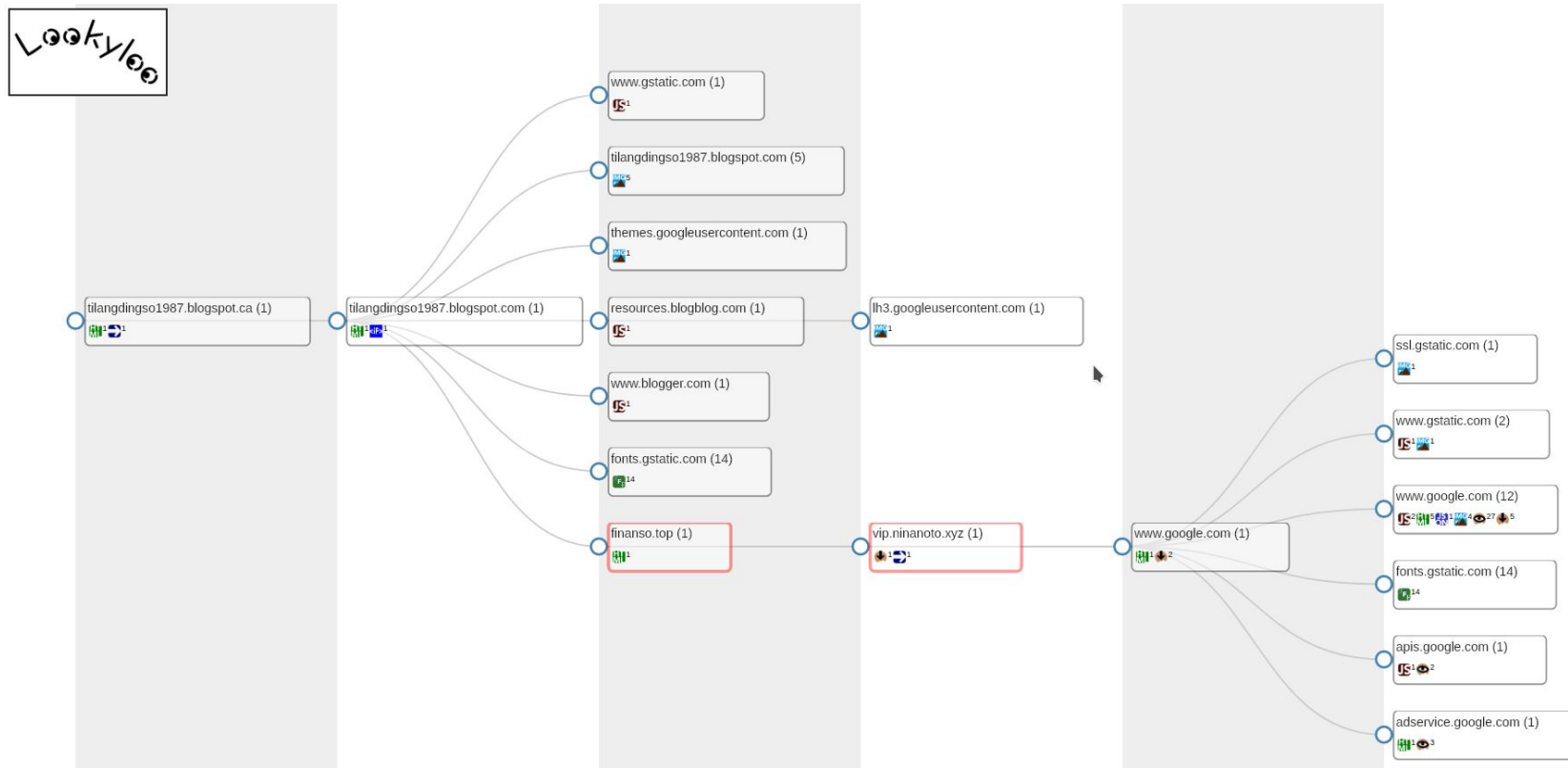
Reading the tree
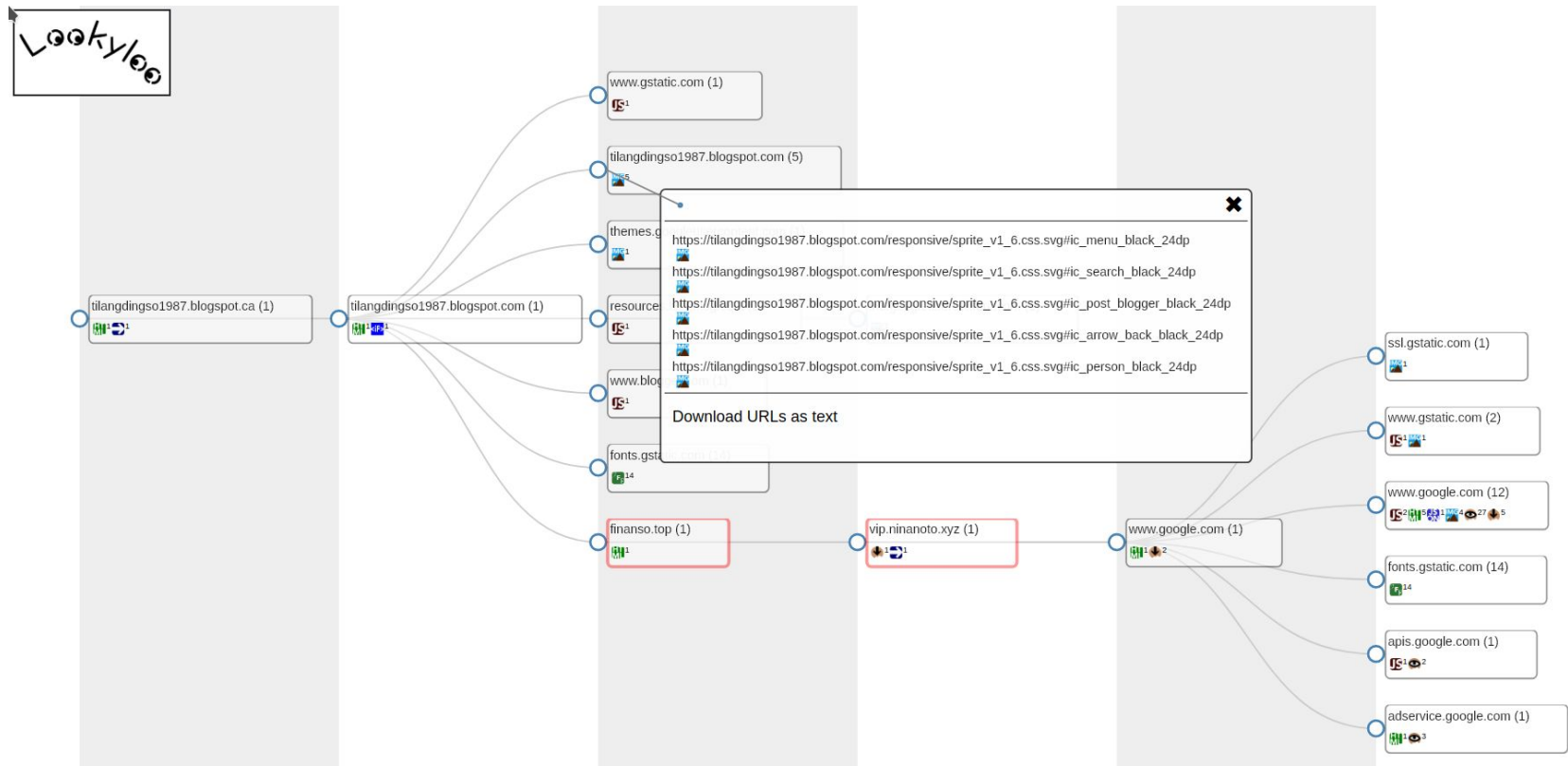
Reading the tree

Legend

- JS Javascript
- Cookie received
- Cookie read
- Redirect
- Font
- HTML
- JSON
- CSS
- EXE
- Image
- Video
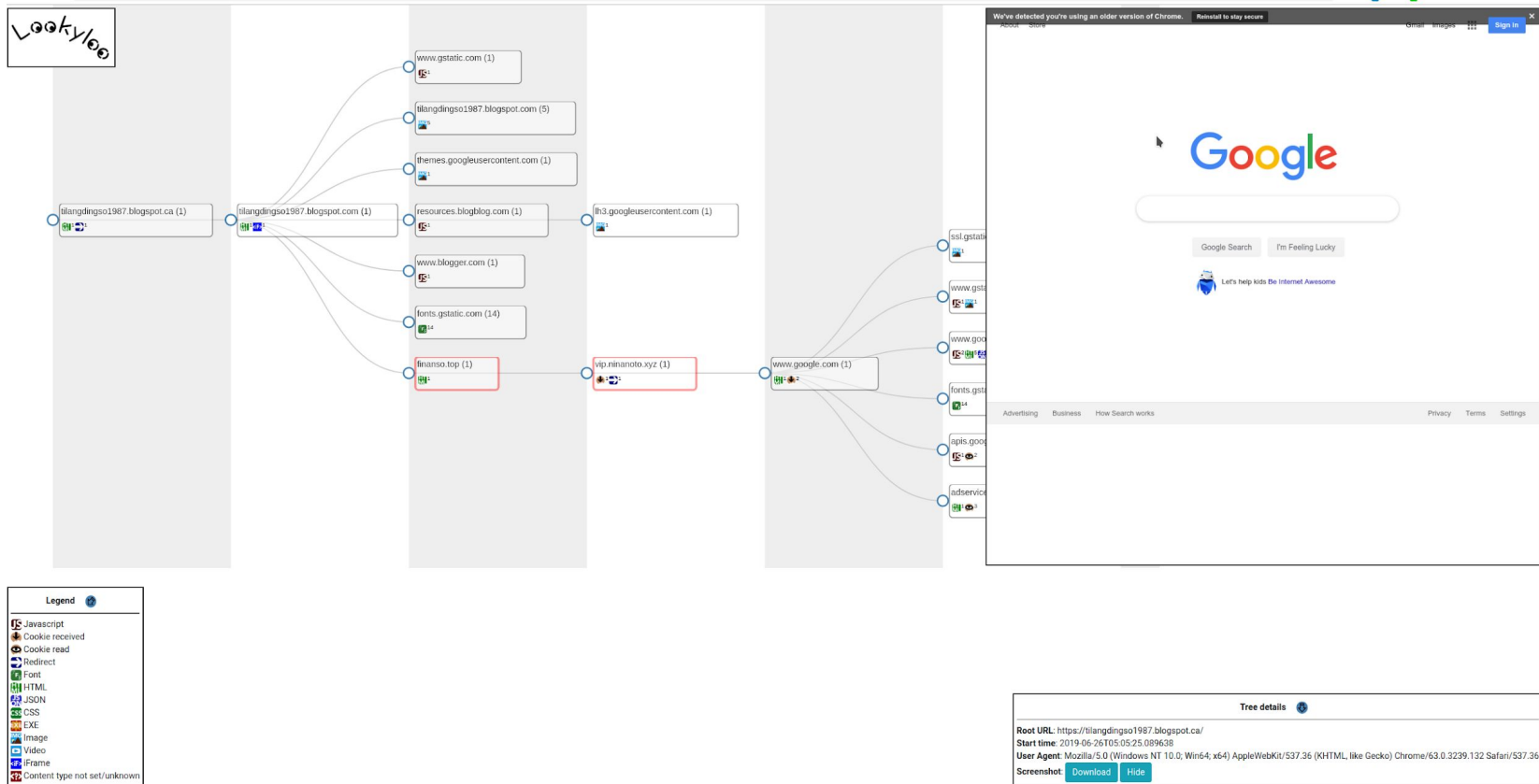- iFrame
- Content type not set/unknown

Tree details

Root URL: https://tilangdingso1987.blogspot.ca/
Start time: 2019-06-26T05:05:25.089638
User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36
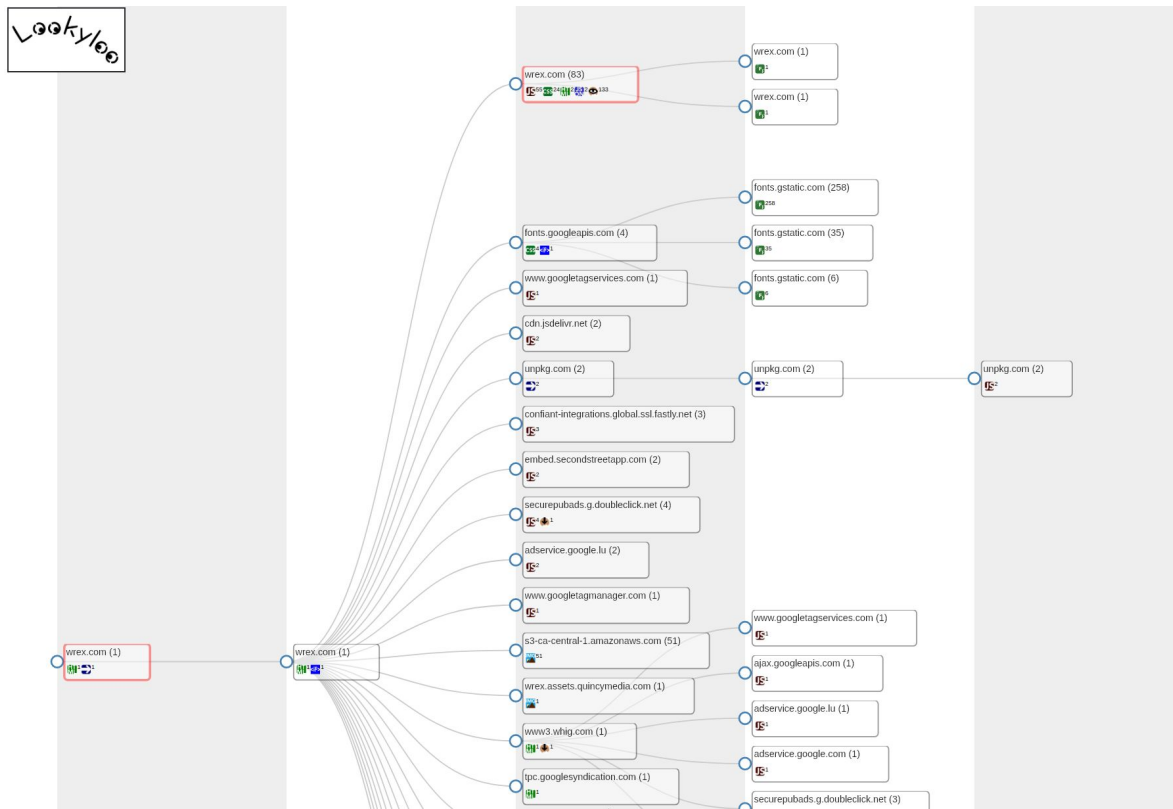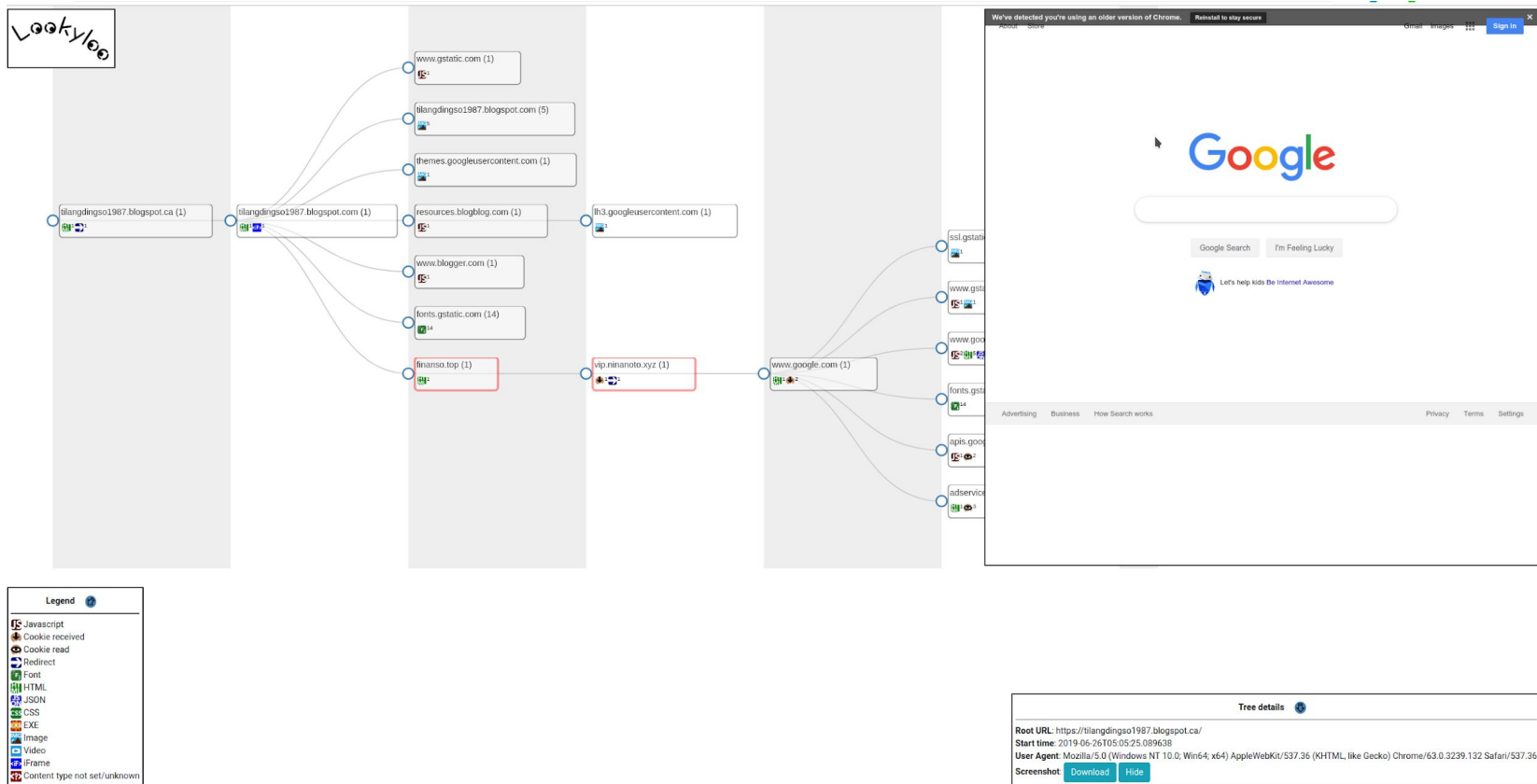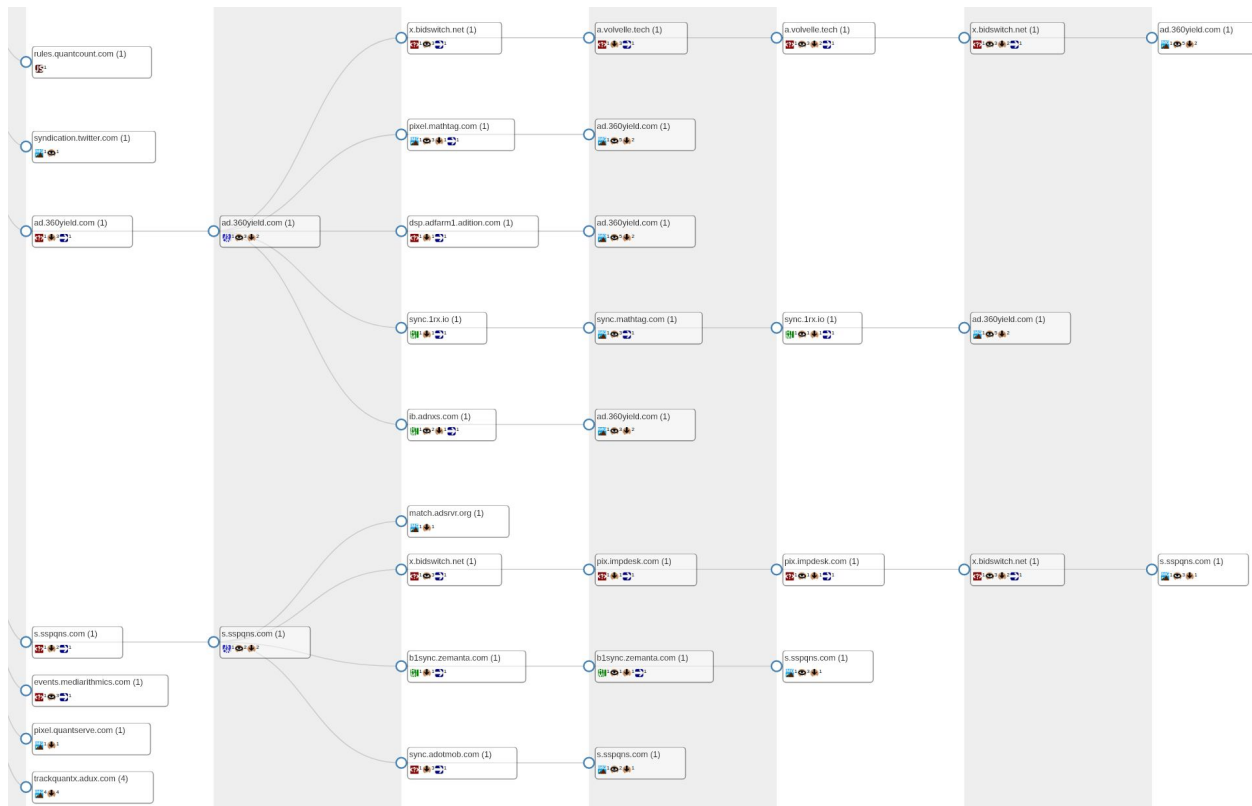**Screenshot**: Download View

Reading the tree

Lookyloo

www.gstatic.com (1)

tilangdingso1987.blogspot.com (5)

themes.googleusercontent.com (1)

tilangdingso1987.blogspot.ca (1)

tilangdingso1987.blogspot.com (1)

resources.blogblog.com (1)

lh3.googleusercontent.com (1)

www.blogger.com (1)

fonts.gstatic.com (14)

finanso.top (1)

vip.ninanoto.xyz (1)

www.google.com (1)

ssl.gstati

www.gsta

www.goo

fonts.gsta

apis.goo

adservice

Legend 🦉

🔵 Javascript
⬇️ Cookie received
👁️ Cookie read
↪️ Redirect
🔤 Font
📄 HTML
📋 JSON
📋 CSS
📦 EXE
🖼️ Image
📹 Video
📺 iFrame
📄 Content type not set/unknown

We've detected you're using an older version of Chrome. Reinstall to stay secure   ✕
About Store   Gmail Images ▦ Sign in

Google

Google Search   I'm Feeling Lucky

Let's help kids Be Internet Awesome

Advertising Business How Search works   Privacy Terms Settings

Tree details 🦉

Root URL: https://tilangdingso1987.blogspot.ca/
Start time: 2019-06-26T05:05:25.089638
User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36
Screenshot: Download Hide

Weird shit we've found

Sneaky mixed TLS content (defeats browser warning)

HTTP Meta redirect

Ad tech and widgets

GDPR Violations (hilarious)

GDPR Violations (hilarious)

Future

URL:

Link Depth:

☐ Display on main page

Browser Configuration

Operating System :   sfd

Browser Type :   sfd

User Agent :   sfd

Create Domain Whitelist

☑ Resolve IPs (Useful for Virus Total, Whois, Required for BGP Ranking)

☐ Virus Total

☐ Google Safe Browsing

☐ Phishtank

☐ EU Phishing initiative

☐ uBlock Filter List

☐ Whois data

☐ Passive DNS/SSL

☐ BGP Ranking

☐ Select All Services (will be slow)

Start Looking!

Moar future

- Passing a cookie
- Whitelist (internal / expected domains)
- Searching inside of trees
- Comparing trees
- Node inspector
- Highlighting meta redirects
- … aaaand?

- https://lookyloo.circl.lu
- https://github.com/CIRCL/lookyloo
- Contact:
  - Quinn Norton - quinn@quinnnorton.com
  - Raphaël Vinot - raphael.vinot@circl.lu