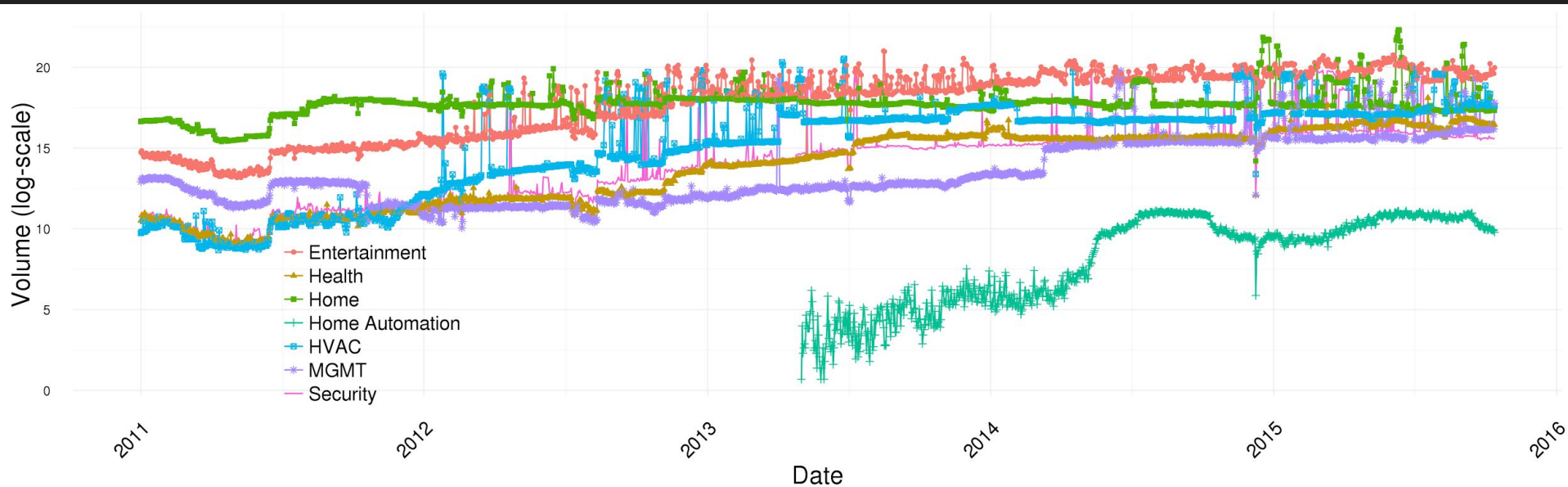


Passive DNS-based Device Identification

Yacin Nadji --- yacin@{gatech.edu,netrisk.io}
NANOG 67, Chicago

IoT Deployment in ISP

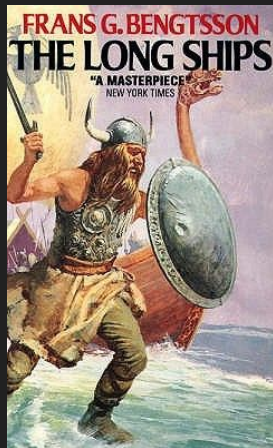


Goals

- No endpoint management (network-based)
- Scalable (DNS!)
- Automated (machine learning)

ML 101: Document Classification

- “Vector-space Model”, i.e., document $\rightarrow$ words $\rightarrow$ vector



ML 101: Document Classification

- Along **the** coast **the** people lived together ...
- In **the** week before their departure to ...
- Once when I was six years old ...

- [1 2 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 ...]
- [0 1 0 0 0 0 1 1 1 1 1 1 0 0 0 0 0 0 0 ...]
- [0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 ...]

ML 101: Term Weighting

- **Binary:** 1 if term present, 0 otherwise
- **Term Frequency (tf):** n if term is present n times, 0 otherwise
 - *the/and/to, the/of/a, the/to/i*
- **Inverse Document Frequency (idf):** $\log(|D|/N)$
 - *ale, almanak, almanac*
- **tf-idf:** product of tf & idf
 - *orm/aviking, arrakis/spice, prince/fox/flower*

Automated Device Identification Process

1. Classify known non-IoT devices on network (by browser/OS/device)
 - a. Classify **only** using DNS lookups
 - b. Ground truth from HTTP headers/MAC addresses
 - c. **OS**: ~90% accuracy; **Browser**: ~80% accuracy; **Device**: ~62% accuracy
 - d. Great initial results for multi-class classification (random guessing: ~14% accuracy)
 - e. Differentiates sub-versions of Windows!
2. Ignore non-IoT devices
3. Cluster unknown devices to build models for IoT devices

Automated Device Identification

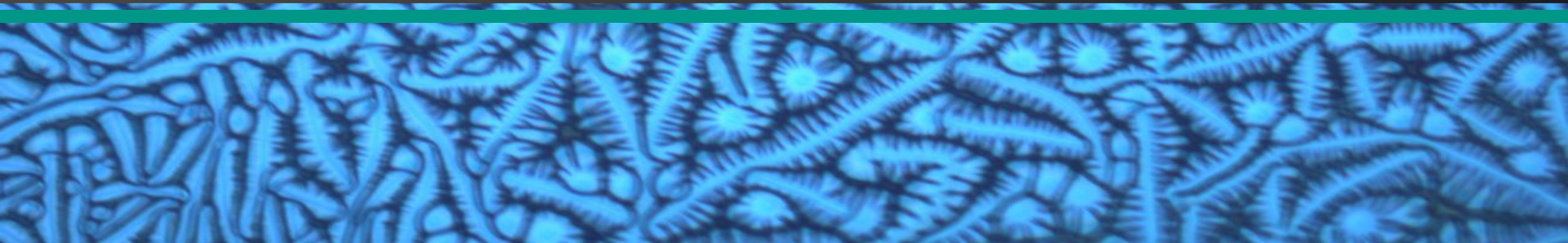
True	Predicted							
		Android	Linux	OS X	Win 10	Win 7	Win 8.1	iOS
	Android	3,020	3	77	67	30	27	86
	Linux	18	83	31	9	51	11	9
	OS X	51	3	3,716	130	195	45	71
	Win 10	31	1	110	2,655	77	26	56
	Win 7	18	4	78	61	2,330	50	20
	Win 8.1	21	0	47	58	260	779	22
	iOS	80	2	117	84	34	25	6,395

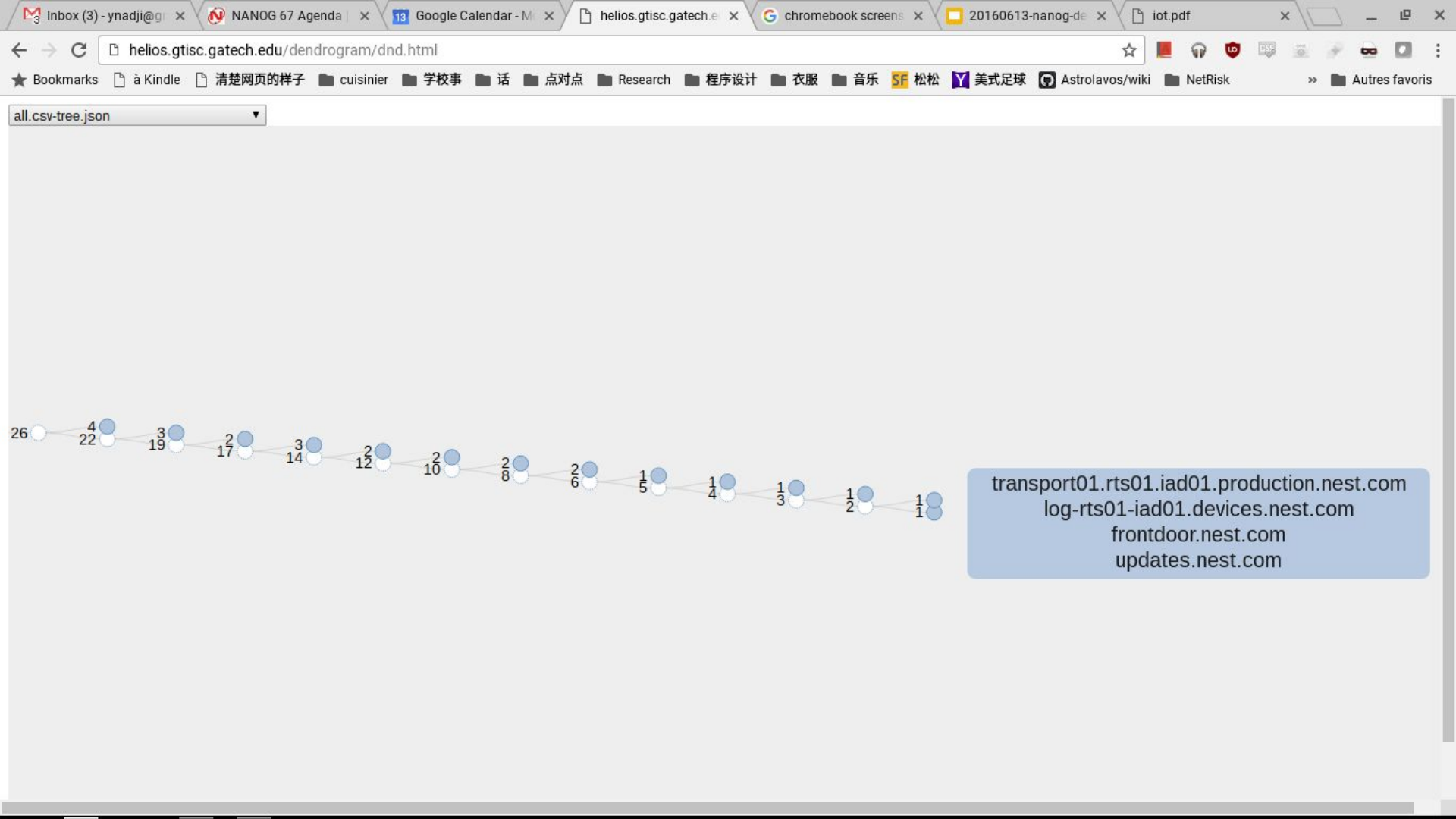
- Android: **settings.crashlytics.com.**, **android.com.**, connectivitycheck.android.com., mclients.googleapis.com., connectivitycheck.gstatic.com., **android.googleapis.com.**, **play.googleapis.com.**, **android.l.google.com.**, **android.clients.google.com.**, safebrowsing.googleapis.com.
- Linux: **ppa.launchpad.net.**, **us.archive.ubuntu.com.**, dl.l.google.com., dl.google.com., **security.ubuntu.com.**, glotorrents.pw., ntp.ubuntu.com., daisy.ubuntu.com., 55y44.com., ping3.teamviewer.com.
- Mac OS X: **1-courier.push.apple.com.**, b._dns-sd._udp.lawn.gatech.edu., db._dns-sd._udp.lawn.gatech.edu., 1-courier.sandbox.push.apple.com., 1.courier-sandbox-push-apple.com.akadns.net., lb._dns-sd._udp.lawn.gatech.edu., p01-swscan.apple.com.akadns.net., **swscan.apple.com.**, **time.apple.com.**, **radarsubmissions.apple.com.**
- iOS: **pancake.apple.com.edgekey.net.**, e6428.g.akamaiedge.net., **pancake.apple.com.**, **b.gslb.aaplimg.com.**, **a.gslb.aaplimg.com.**, **iphonesubmissions.apple.com.**, **g.aaplimg.com.**, **mesu.g.aaplimg.com.**, mesu.apple.com.akadns.net., **mesu.apple.com.**

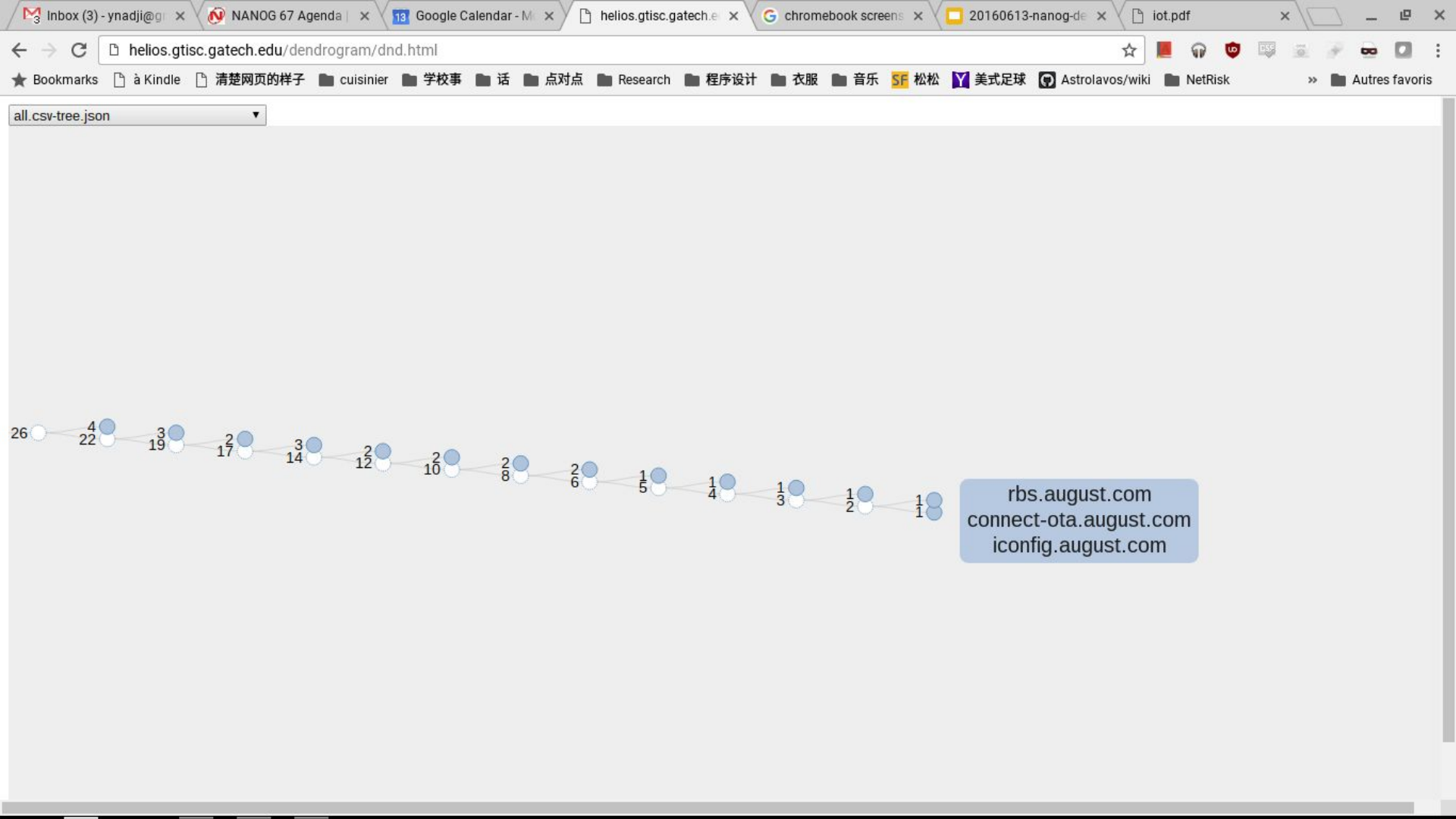
- Windows 10: e1898.b.akamaiedge.net., livetileedge.dsx.mp.microsoft.com.edgekey.net., livetileedge.dsx.mp.microsoft.com.akadns.net., livetileedge.dsx.mp.microsoft.com., a1784.g2.akamai.net., cdn.content.prod.cms.msn.com., cdn.content.prod.cms.msn.com.edgesuite.net., vortex-db5.metron.live.com.nsadc.net., **v10.vortex-win.data.metron.live.com.nsadc.net., v10.vortex-win.data.microsoft.com.**
- Windows 7: vortex-win.data.metron.live.com.nsadc.net., vortex-win.data.microsoft.com., fg.ds.dl.windowsupdate.com.nsadc.net., main-ds.dl.windowsupdate.com.nsadc.net., ds.download.windowsupdate.com.edgesuite.net., ds.download.windowsupdate.com., a1363.dscg.akamai.net., crl.www.ms.akadns.net., crl.microsoft.com., teredo.ipv6.microsoft.com.
- Windows 8.1: sqm.telemetry.microsoft.com.nsadc.net., sqm.telemetry.microsoft.com., e7341.g.akamaiedge.net., yp.www.cn856.com., statsfe2.ws.microsoft.com., ds.ssw.live.com., statsfe2.ws.microsoft.com.nsadc.net., img.stb.s-msn.com., **win8.ipv6.microsoft.com.nsadc.net., win8.ipv6.microsoft.com.**

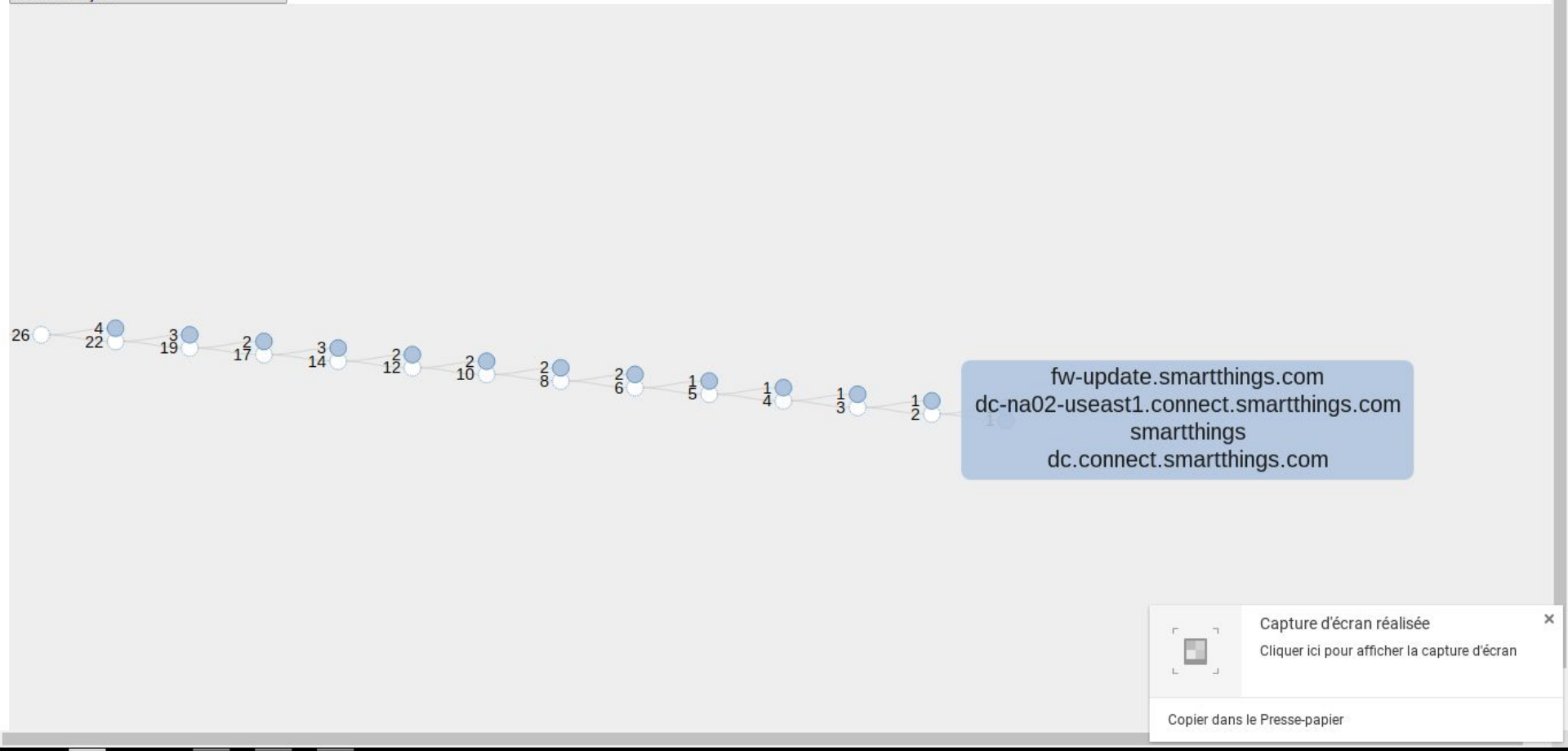


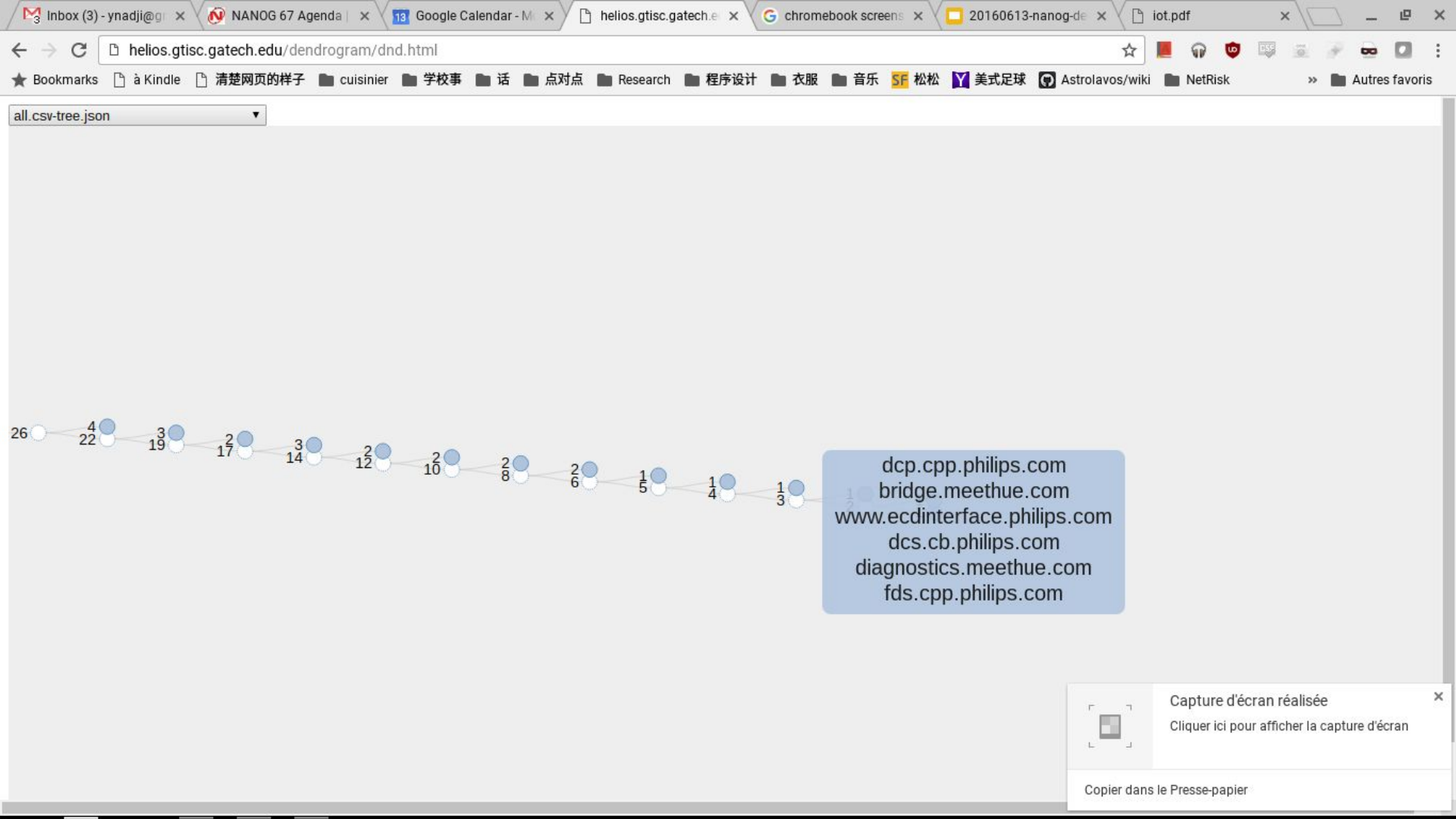
Clustering Unknown







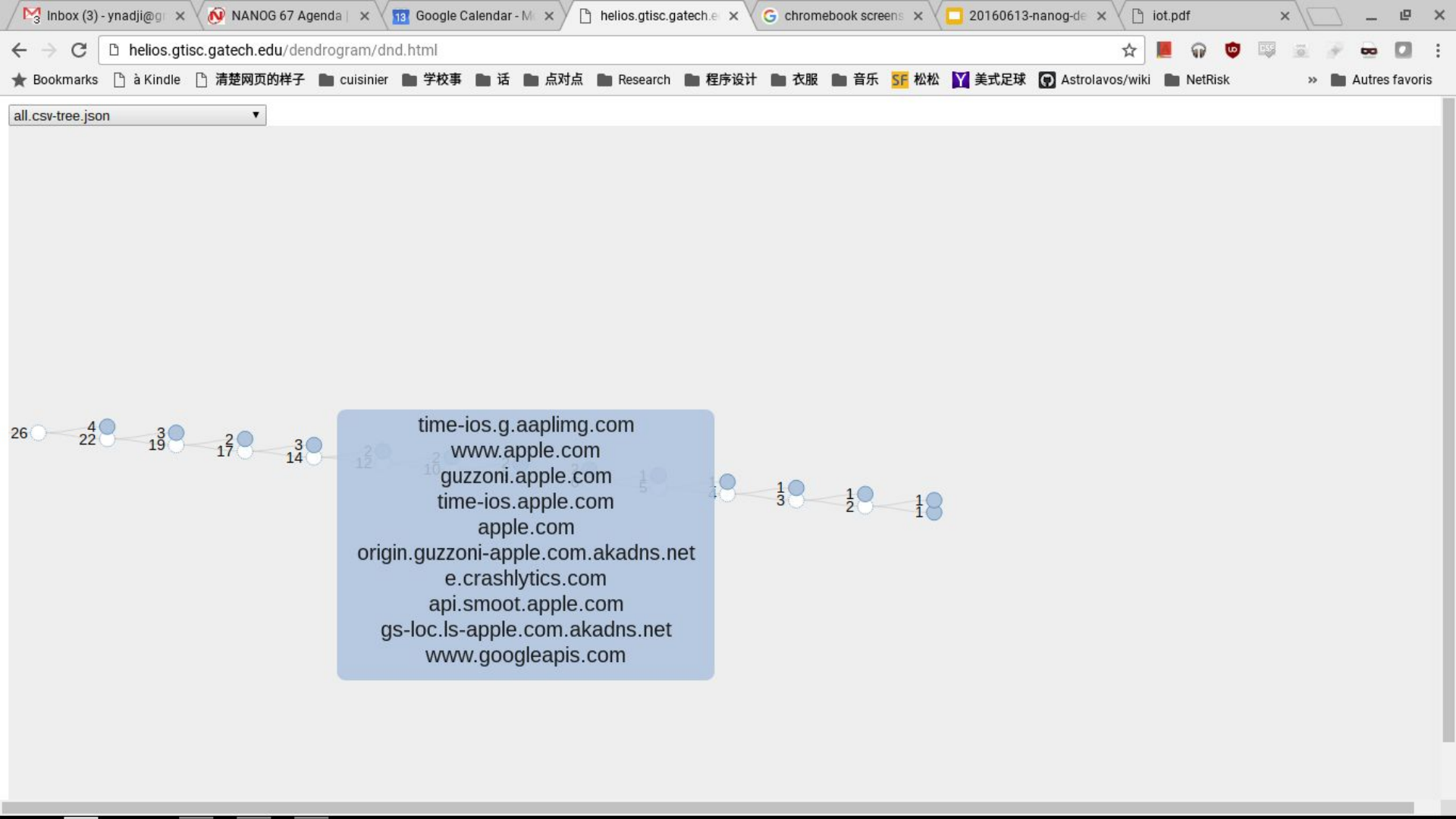


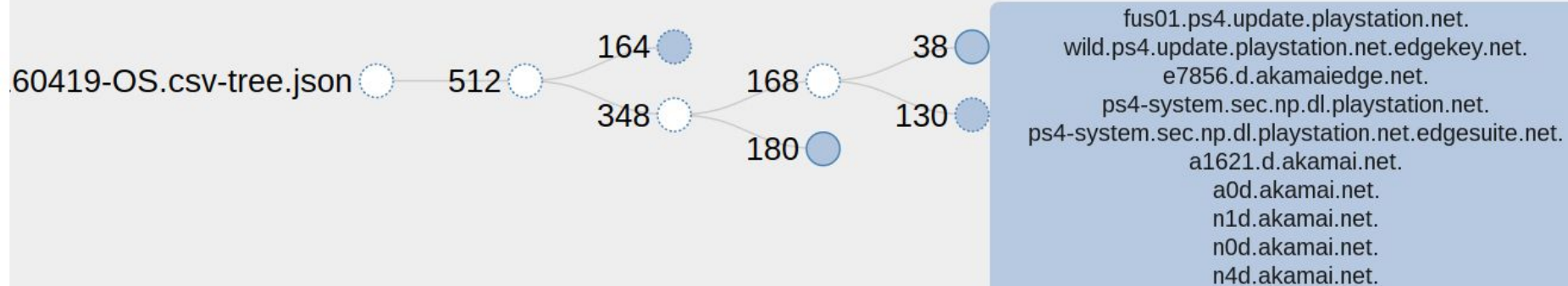


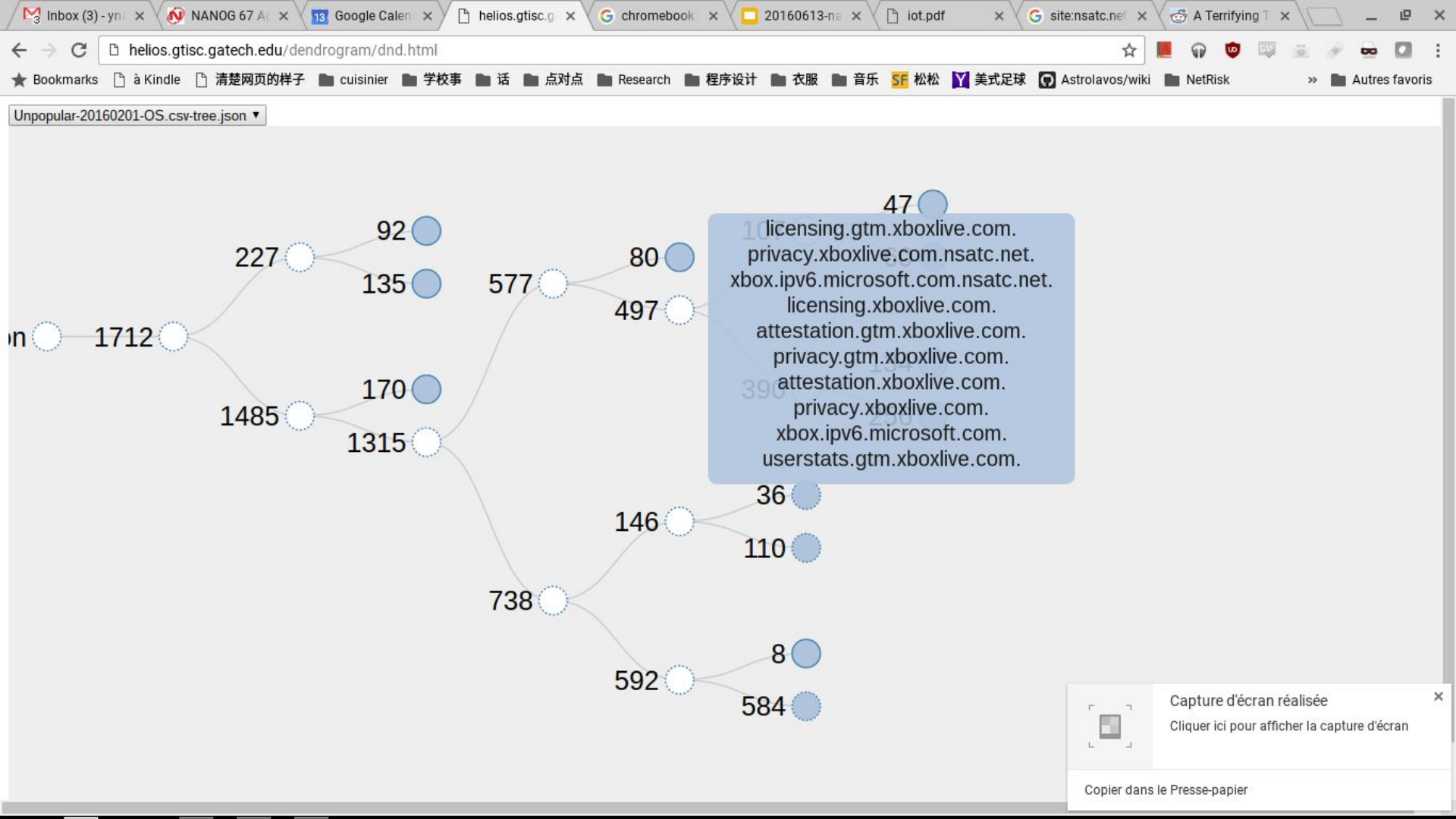
Capture d'écran réalisée

Cliquer ici pour afficher la capture d'écran

Copier dans le Presse-papier

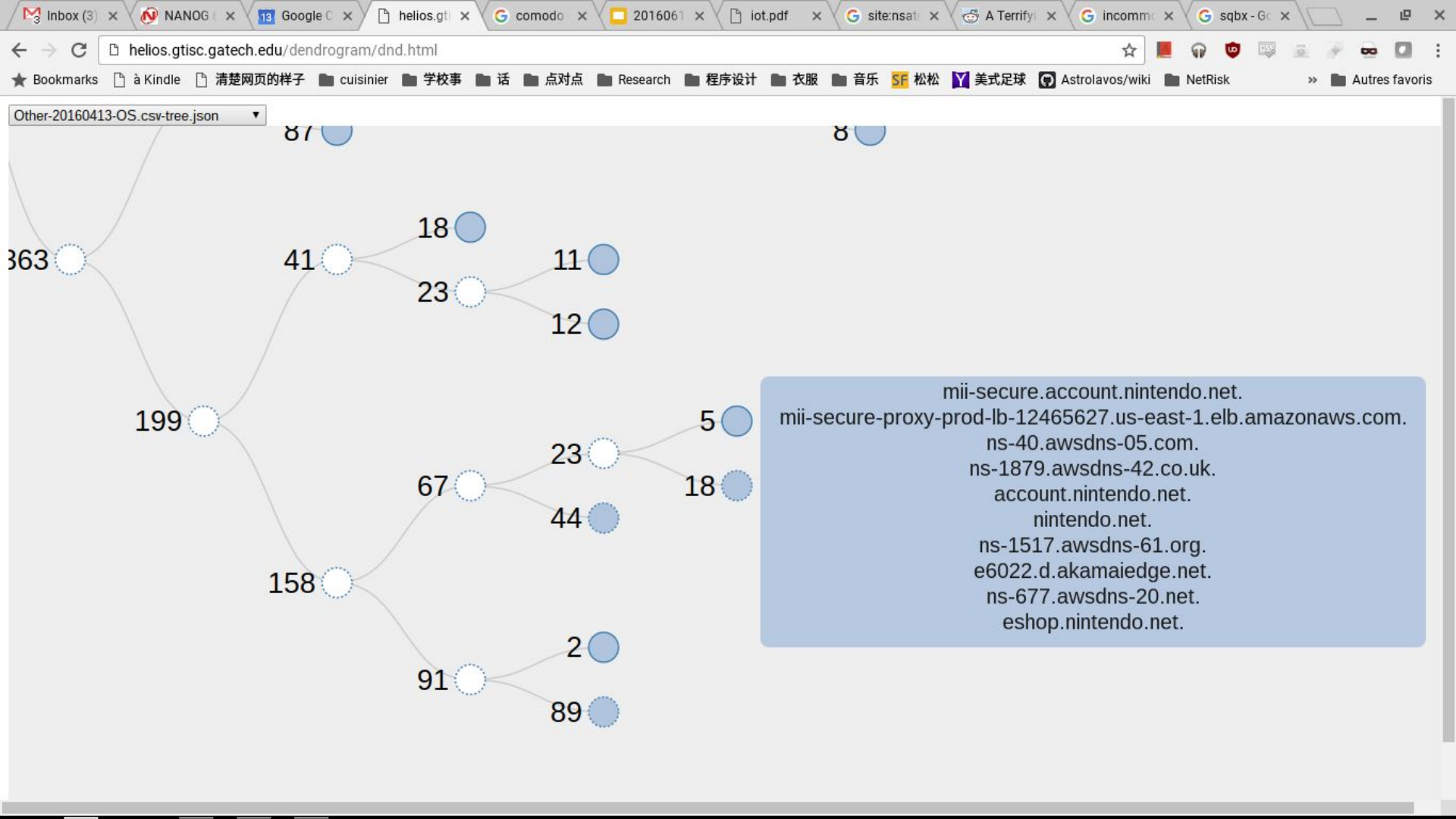






Capture d'écran réalisée
Cliquez ici pour afficher la capture d'écran

Copier dans le Presse-papier



Questions? Thanks!