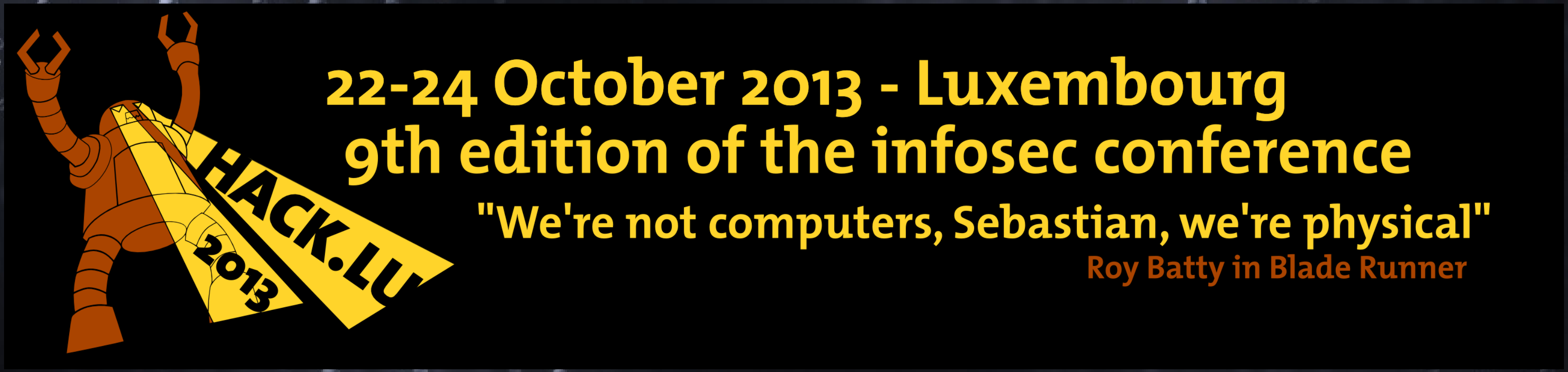
Pcap2Bubbles

Extended Version (more text, more images, less jokes)

Bubble your packets!

By Sébastien Larinier / @Sebdraven & Guillaume Arcas / @y0m



22-24 October 2013 - Luxembourg
9th edition of the infosec conference

"We're not computers, Sebastian, we're physical"
Roy Batty in Blade Runner

Network Forensics Paradigm

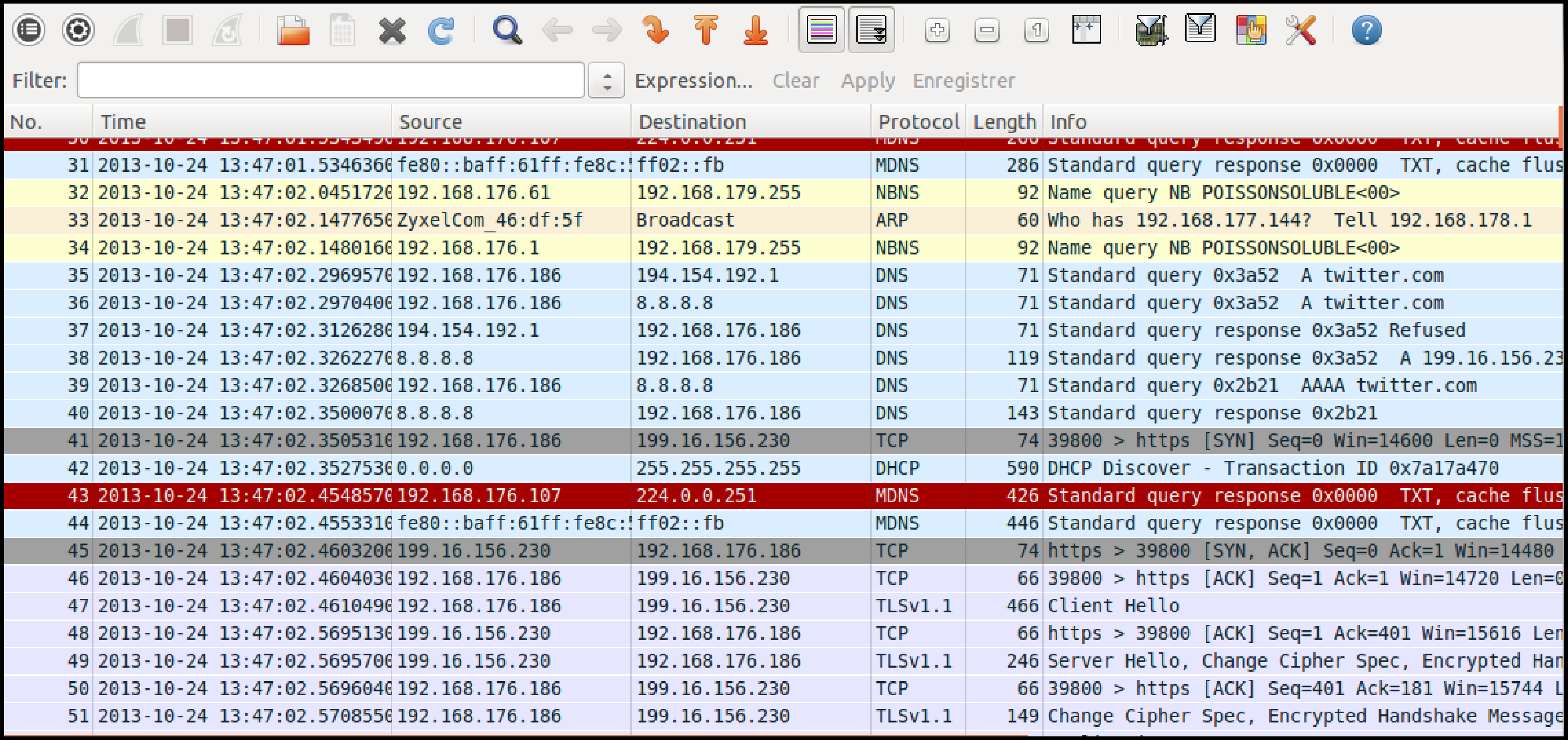
- Finding a needle in a haystack is not an easy thing...
- So what about finding a needle in hundred or thousand haystacks...
- ...when burning the haystacks is not an option ?

Pcap Analysis

- Top-to-bottom approach:
  1. Statistics: # of packets, timeline, etc.
  2. Session: dest./src, protocols & ports used, etc.
  3. Graphical approach
  4. Alerts: IDS rules, etc.
  5. Full Content Analysis
- Graphical Approach
  1. A picture worth thousand words.
  2. Best-readable for a human

Wireshark

WireShark is the worst tool for network analysis except all the others that have been coded.



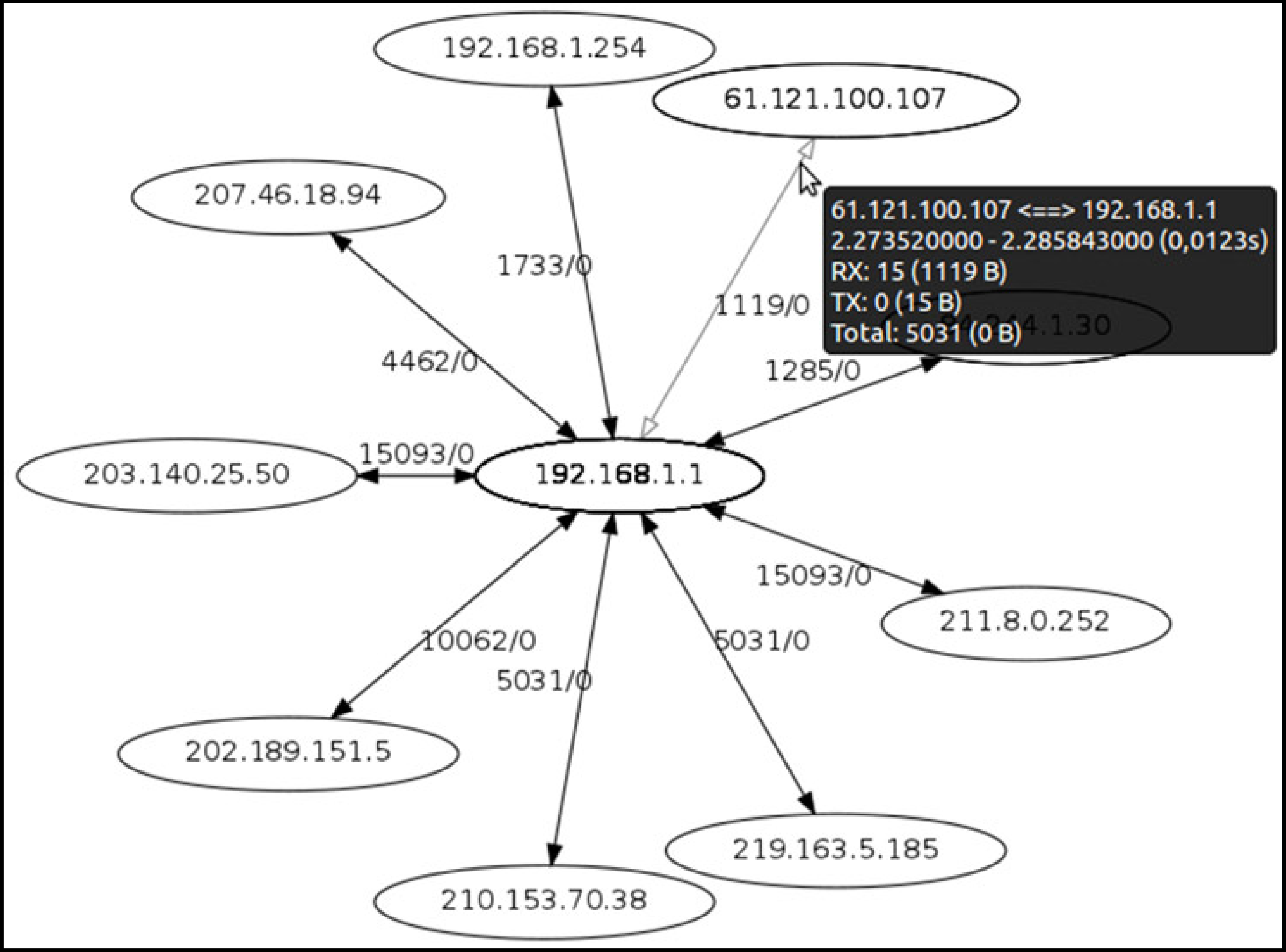
No.	Time	Source	Destination	Protocol	Length	Info
31	2013-10-24 13:47:01.5346360	fe80::baff:61ff:fe8c:!	ff02::fb	MDNS	286	Standard query response 0x0000 TXT, cache flus
32	2013-10-24 13:47:02.0451720	192.168.176.61	192.168.179.255	NBNS	92	Name query NB POISSONSOLUBLE<00>
33	2013-10-24 13:47:02.1477650	ZyxelCom_46:df:5f	Broadcast	ARP	60	Who has 192.168.177.144? Tell 192.168.178.1
34	2013-10-24 13:47:02.1480160	192.168.176.1	192.168.179.255	NBNS	92	Name query NB POISSONSOLUBLE<00>
35	2013-10-24 13:47:02.2969570	192.168.176.186	194.154.192.1	DNS	71	Standard query 0x3a52 A twitter.com
36	2013-10-24 13:47:02.2970400	192.168.176.186	8.8.8.8	DNS	71	Standard query 0x3a52 A twitter.com
37	2013-10-24 13:47:02.3126280	194.154.192.1	192.168.176.186	DNS	71	Standard query response 0x3a52 Refused
38	2013-10-24 13:47:02.3262270	8.8.8.8	192.168.176.186	DNS	119	Standard query response 0x3a52 A 199.16.156.23
39	2013-10-24 13:47:02.3268500	192.168.176.186	8.8.8.8	DNS	71	Standard query 0x2b21 AAAA twitter.com
40	2013-10-24 13:47:02.3500070	8.8.8.8	192.168.176.186	DNS	143	Standard query response 0x2b21
41	2013-10-24 13:47:02.3505310	192.168.176.186	199.16.156.230	TCP	74	39800 > https [SYN] Seq=0 Win=14600 Len=0 MSS=1
42	2013-10-24 13:47:02.3527530	0.0.0.0	255.255.255.255	DHCP	590	DHCP Discover - Transaction ID 0x7a17a470
43	2013-10-24 13:47:02.4548570	192.168.176.107	224.0.0.251	MDNS	426	Standard query response 0x0000 TXT, cache flus
44	2013-10-24 13:47:02.4553310	fe80::baff:61ff:fe8c:!	ff02::fb	MDNS	446	Standard query response 0x0000 TXT, cache flus
45	2013-10-24 13:47:02.4603200	199.16.156.230	192.168.176.186	TCP	74	https > 39800 [SYN, ACK] Seq=0 Ack=1 Win=14480
46	2013-10-24 13:47:02.4604030	192.168.176.186	199.16.156.230	TCP	66	39800 > https [ACK] Seq=1 Ack=1 Win=14720 Len=0
47	2013-10-24 13:47:02.4610490	192.168.176.186	199.16.156.230	TLSv1.1	466	Client Hello
48	2013-10-24 13:47:02.5695130	199.16.156.230	192.168.176.186	TCP	66	https > 39800 [ACK] Seq=1 Ack=401 Win=15616 Len
49	2013-10-24 13:47:02.5695700	199.16.156.230	192.168.176.186	TLSv1.1	246	Server Hello, Change Cipher Spec, Encrypted Han
50	2013-10-24 13:47:02.5696040	192.168.176.186	199.16.156.230	TCP	66	39800 > https [ACK] Seq=401 Ack=181 Win=15744 L
51	2013-10-24 13:47:02.5708550	192.168.176.186	199.16.156.230	TLSv1.1	149	Change Cipher Spec, Encrypted Handshake Message

Can you see the needle?

AfterGlow & Wireshark

First approach: use AfterGlow & Wireshark (GSoC 2011 - Honeynet Project)

http://honeynet.org/gsoc2011/slot8

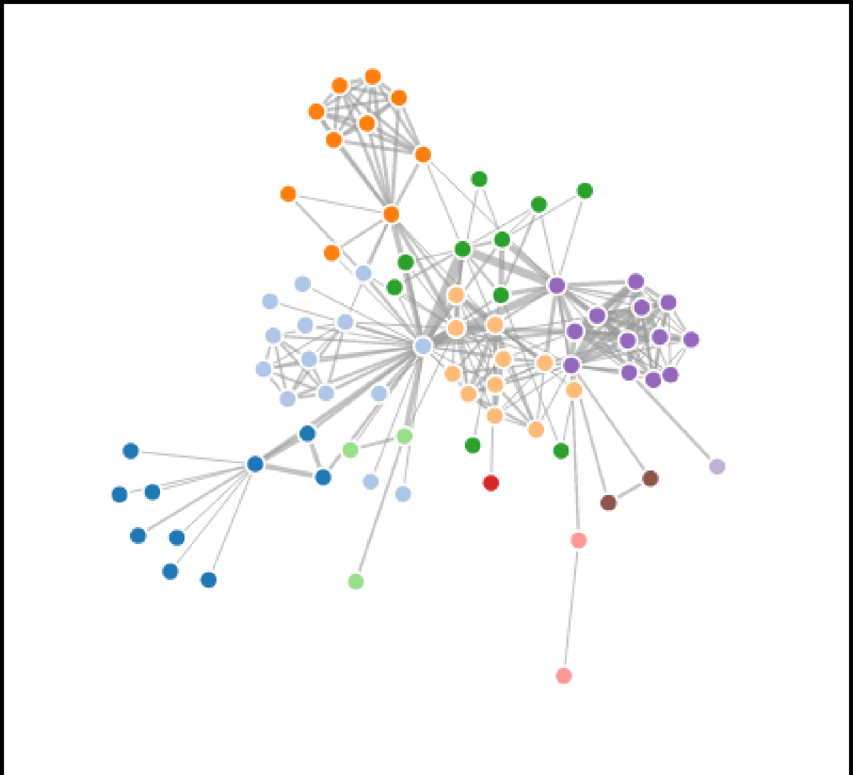


61.121.100.107 <==> 192.168.1.1
2.273520000 - 2.285843000 (0,0123s)
RX: 15 (1119 B)
TX: 0 (15 B)
Total: 5031 (0 B)

D3.js

D3.js is a JavaScript library for manipulating documents based on data. D3 helps you bring data to life using HTML, SVG and CSS.

http://d3js.org

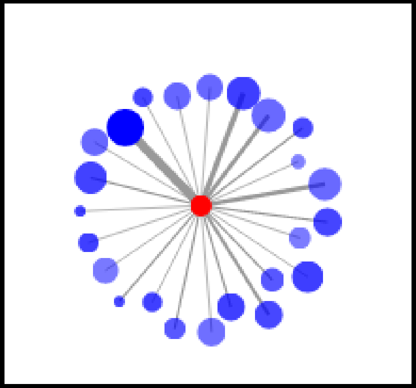


D3.js & Honeyproxy

Integration of D3js in Honeyproxy (GSoC 2012 - Honeynet Project)

HTTP Session live bubbling

http://honeyproxy.org/

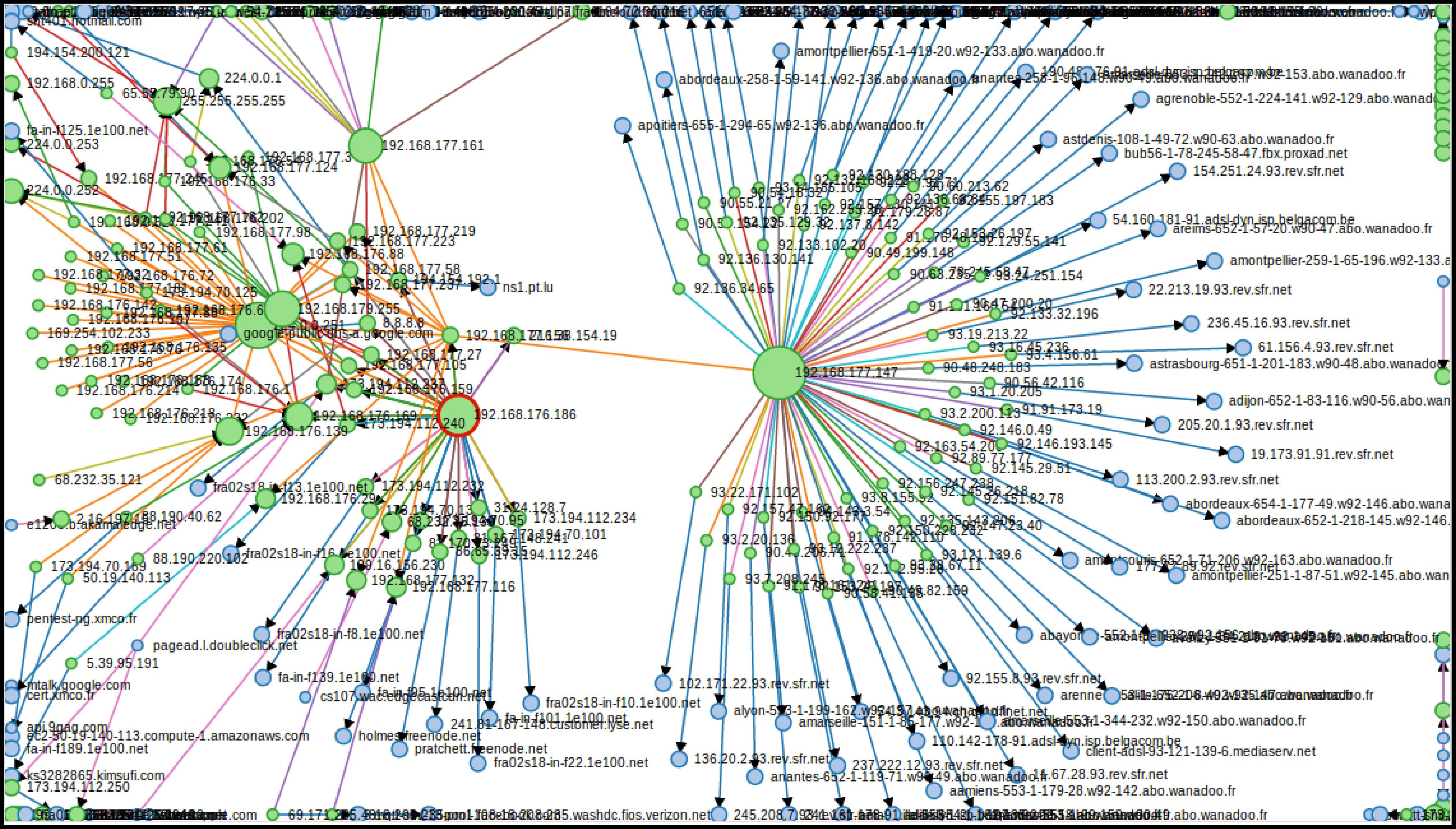


Malcom

- Data collection:
  - IP, domains, URLs, malware MD5, etc.
  - From public sources: DShield, AlienVault, Spamhaus, ZeusTracker, etc
  - From private sources: logs from your firewall, proxy, etc
  - From files: text and pcap
- Data enhancement:
  - Extend collected data: reversing IP, domains WHOIS, etc
- Data visualization with D3.js
- Pcap2Bubbles

https://github.com/tomchop/malcom/

Demo



Want an access to demo website? Send me a mail [guillaume.arcas@retiaire.org]

Pcap2Bubbles Project

1. **Upload a PCAP**
2. **Bubble it with D3.js**
3. **Enhance it with collected data**
4. **Add intelligence (add your own tags, etc)**
    - **Run Snort/Suricata-IDS/Bro-IDS on uploaded Pcap**
    - **Extract content, like files, send them to VirusTotal, malwr.com, etc**
5. **Share it (or not...)**

Build a Malware Intelligence Lightweight FrameworK

Thank You!

You Liked the Dog?