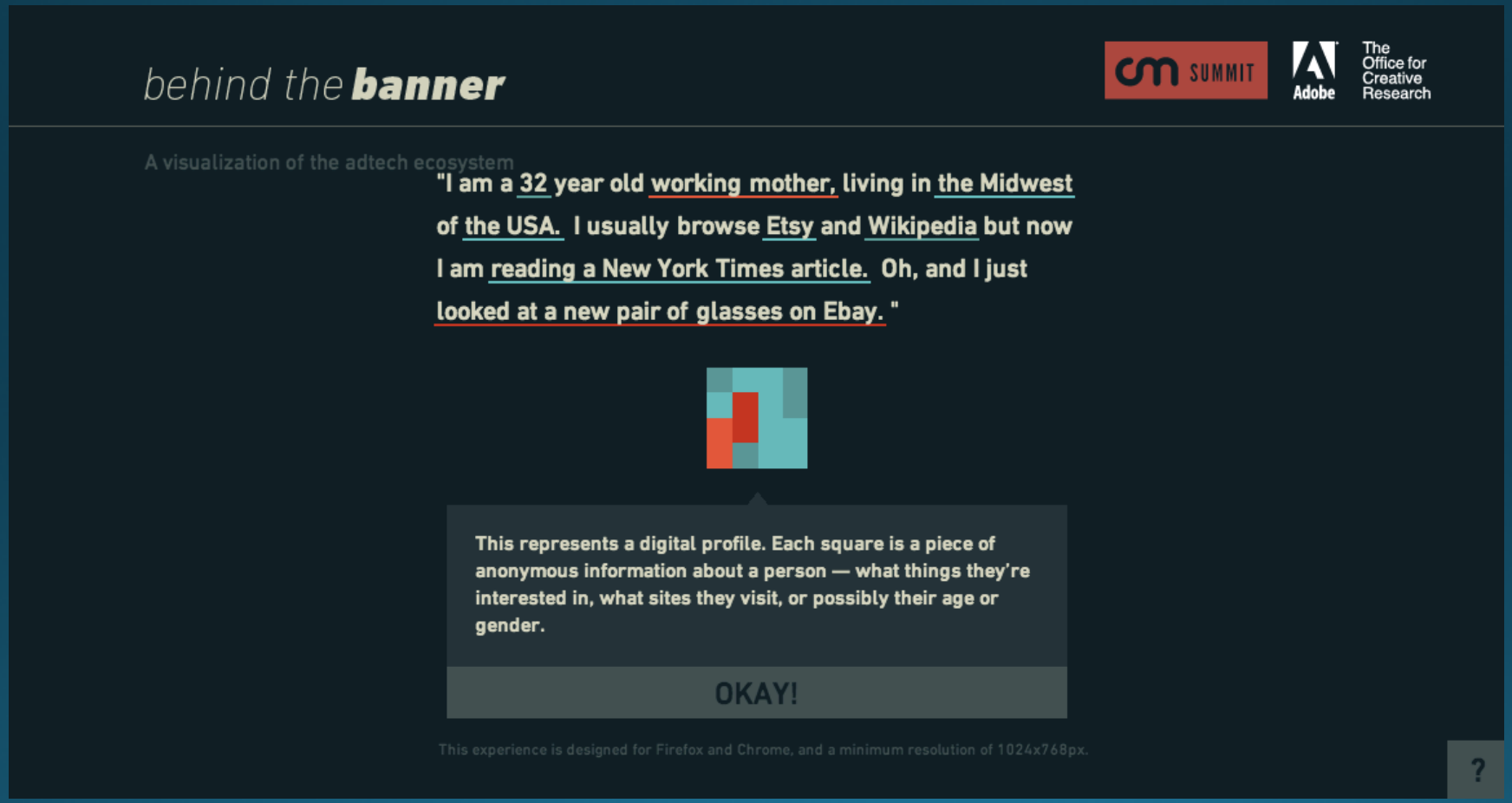
created by @sysaaron, inspired by @triw0lf

Let Me Show You my Pi-hole ;)

credz

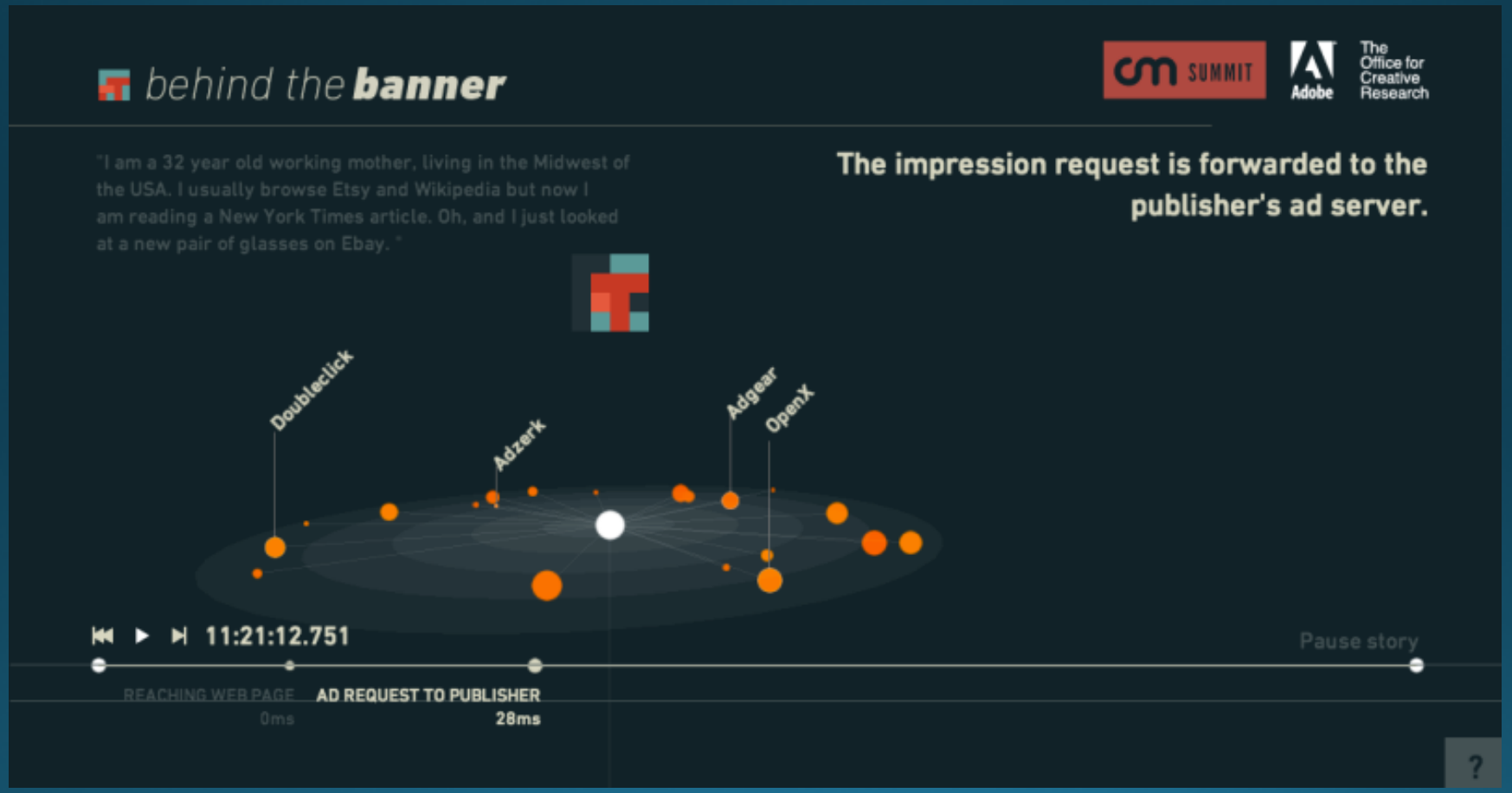
- Aaron J. Scantlin (@sysaaron)
- Security Analyst – University of Missouri
- GSEC, GCFA
- Vice President – Columbia, MO Infragard Chapter
- Treasurer – University of Missouri Upsilon Pi Epsilon Chapter
- Member – SANS Advisory Board
- Member – REN-ISAC

How do Online Ads Work?



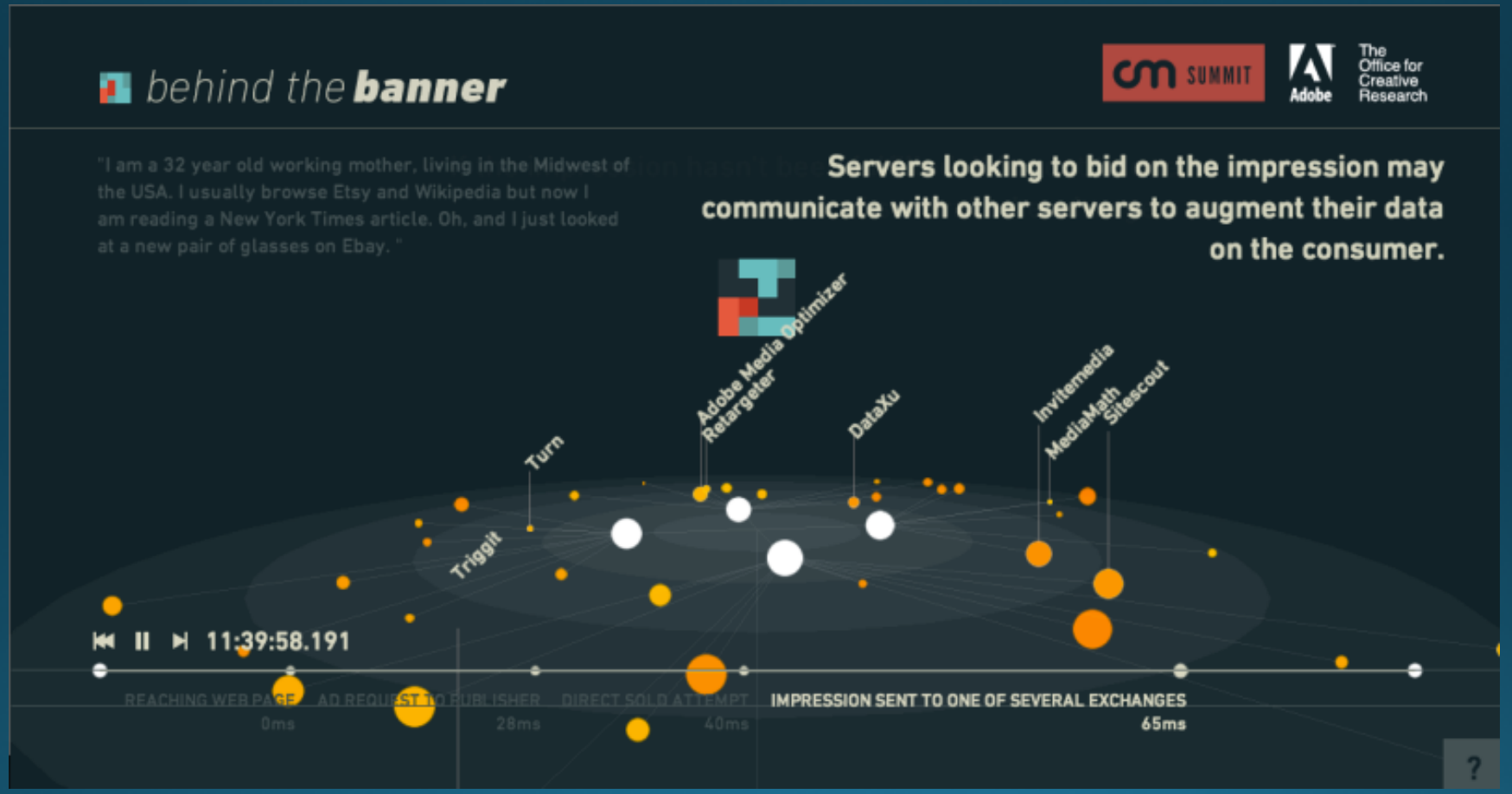
Source: http://cmsummit.com/behindthebanner/

How do Online Ads Work?



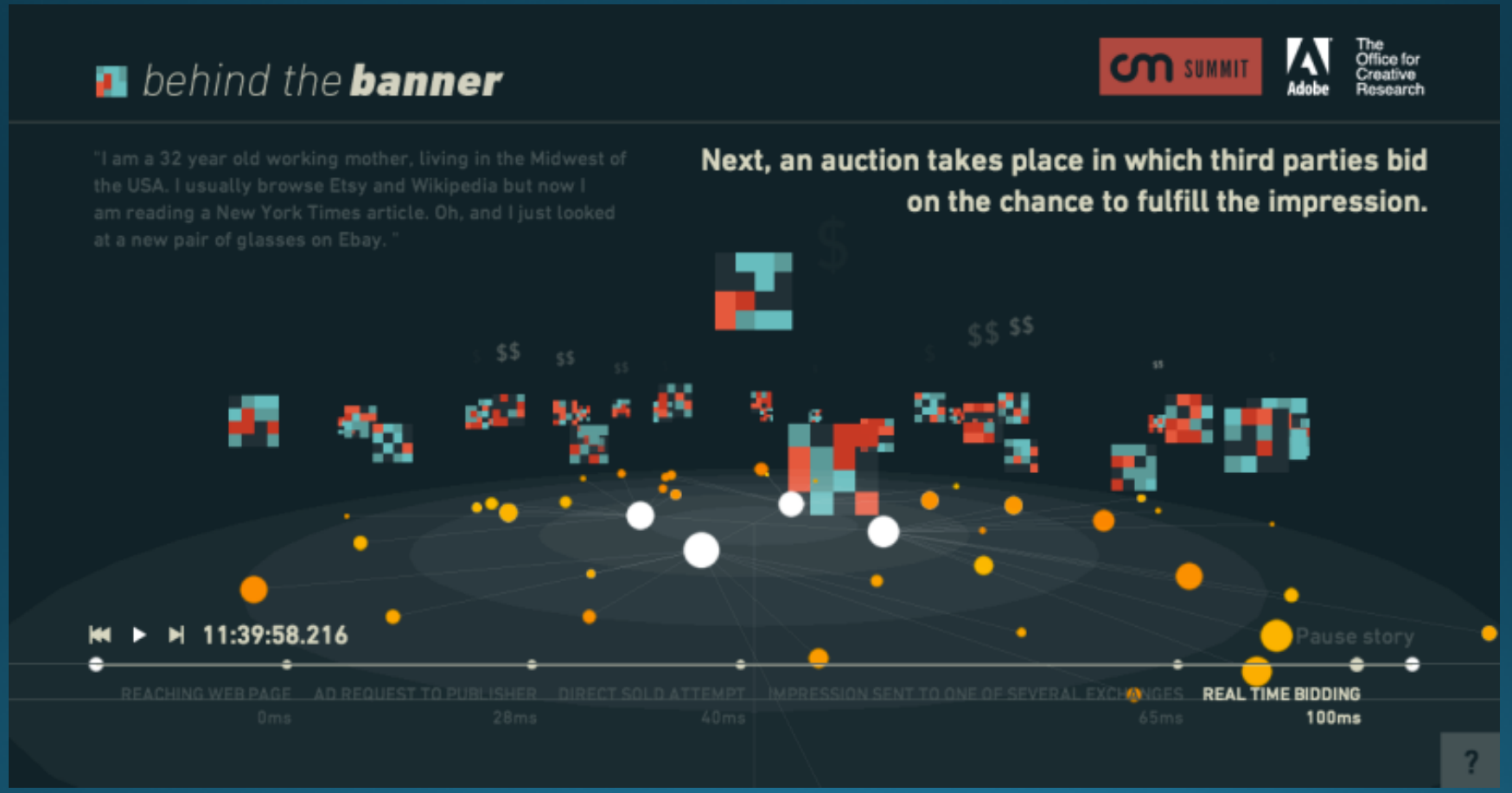
Source: http://cmsummit.com/behindthebanner/

How do Online Ads Work?



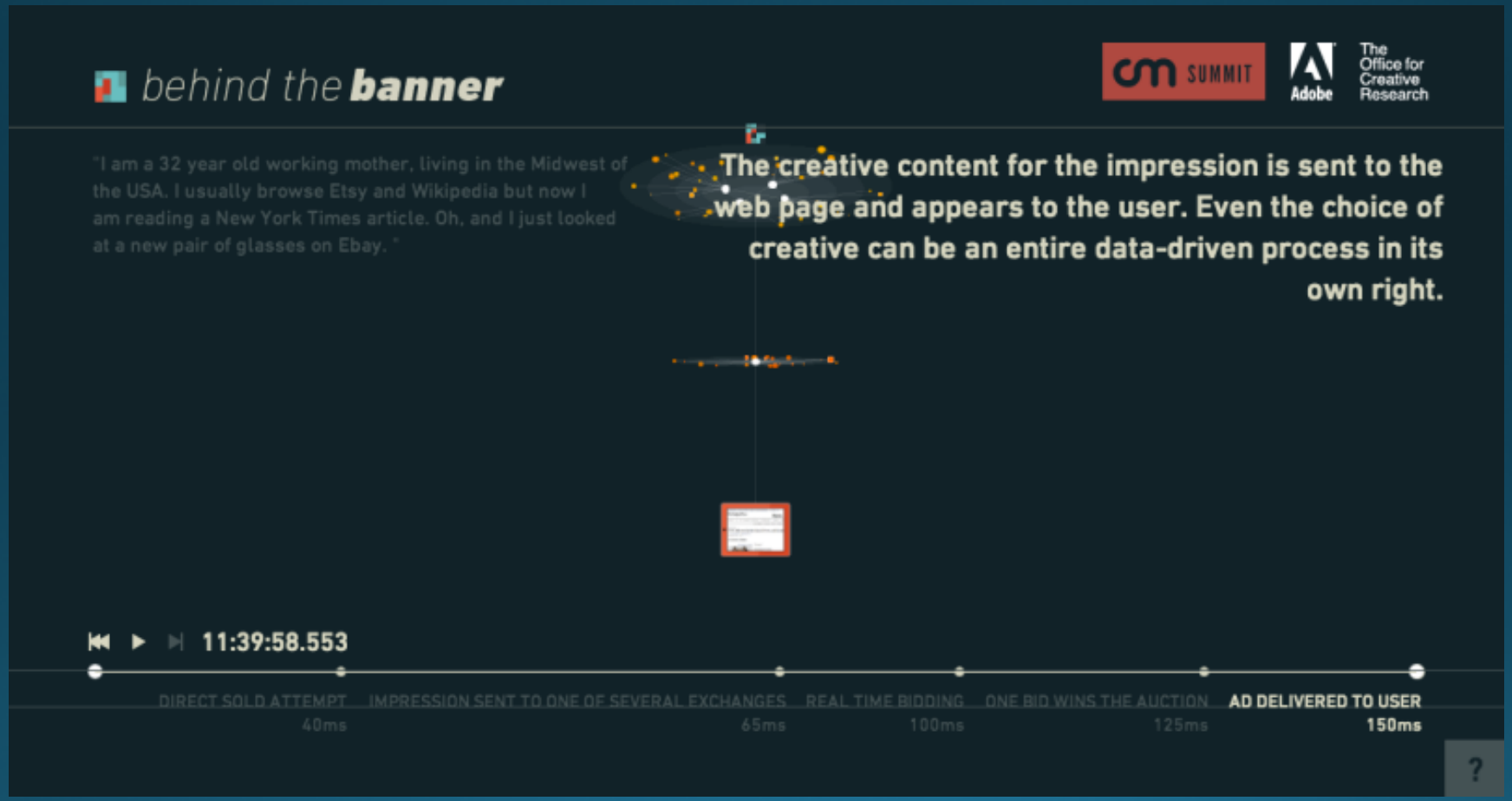
Source: http://cmsummit.com/behindthebanner/

How do Online Ads Work?



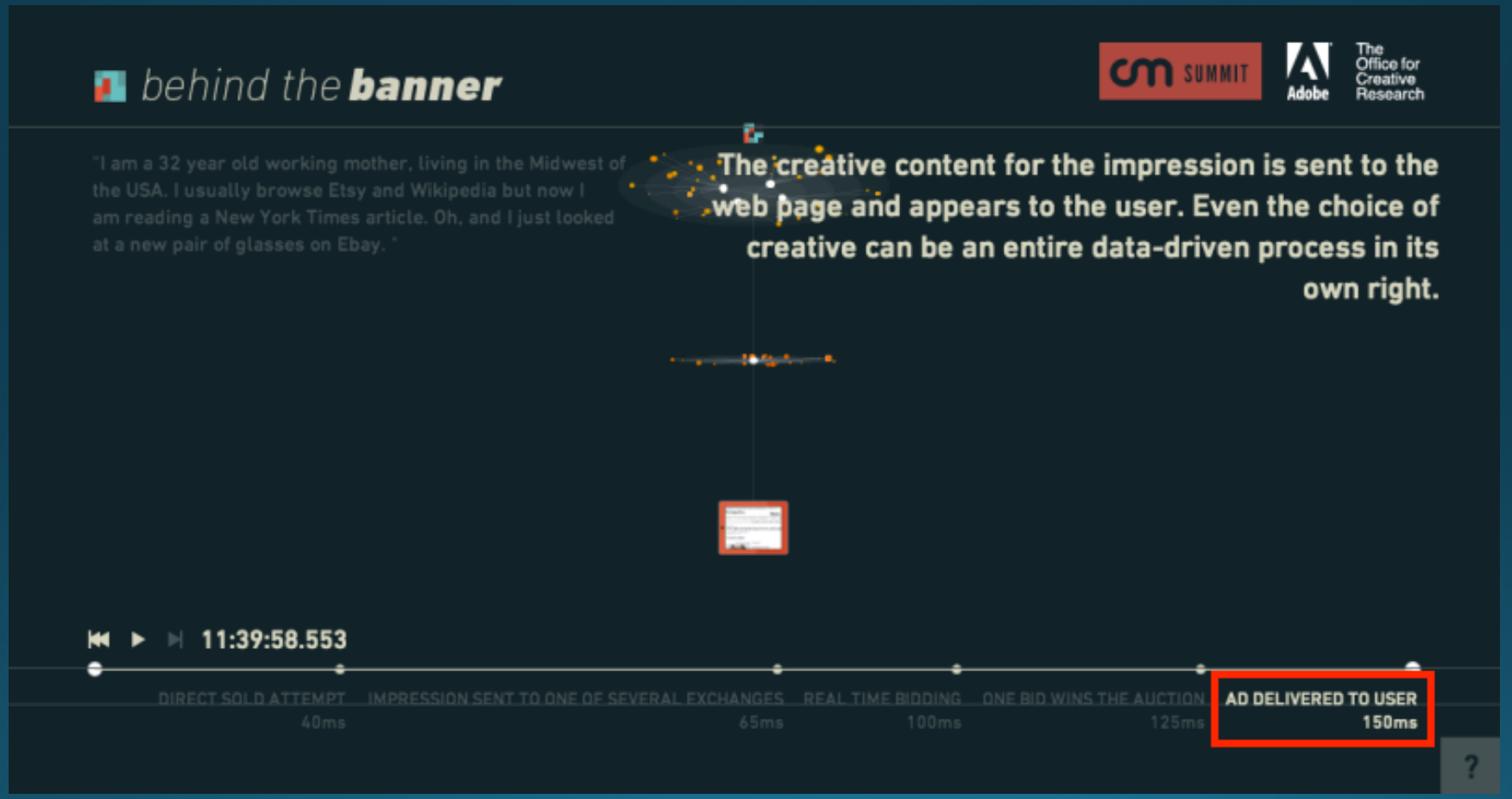
Source: http://cmsummit.com/behindthebanner/

How do Online Ads Work?



Source: http://cmsummit.com/behindthebanner/

How Long Did That Take…?



Why Does This Matter?

Types and modes [edit]

By visiting websites that are affected by malvertising, users are at risk of infection. There are many different methods used for injecting malicious advertisements or programs into webpages:

- Pop-up ads for deceptive downloads, such as fake anti-virus programs that install malicious software on the computer[2]
- In-text or in-content advertising
- Drive-by downloads[2]
- Web widgets in which redirection can be co-opted into redirecting to a malicious site[3]
- Hidden iframes that spread malware into websites[3]
- Content delivery networks exploited to share malware[3]
- Malicious banners on websites[3]
- Third-party advertisements on webpages[21]
- Third-party applications, such as forums, help desks, and customer relationship management and content management systems[21]

Source: Wikipedia

Why Does This Matter?

Non-security reasons as well:

- Adds complication to UI/UX
- Consumes additional network resources
- Bloats browser cache

Also…

THEY'RE JUST *#@%ING ANNOYING

Source: life experience

One Solution:

Pi-hole

What's a Pi-hole?

Pi-hole is a free advertisement-blocking software

- Runs on a Raspberry Pi (and other stuff, too, if you'd rather)
- Known ad-serving domains are pulled from third party sources and compiled into one list
- Network-level blocking allows any device to block ads, regardless of hardware or OS
- Since **ads are blocked *before* they are downloaded**, your network will perform better
- The Web interface shows how many ads were blocked, a query log, and more

Source: https://pi-hole.net


PI-HOLES
PI-HOLES FOR EVERYBODY
imgflip.com

Preparation List

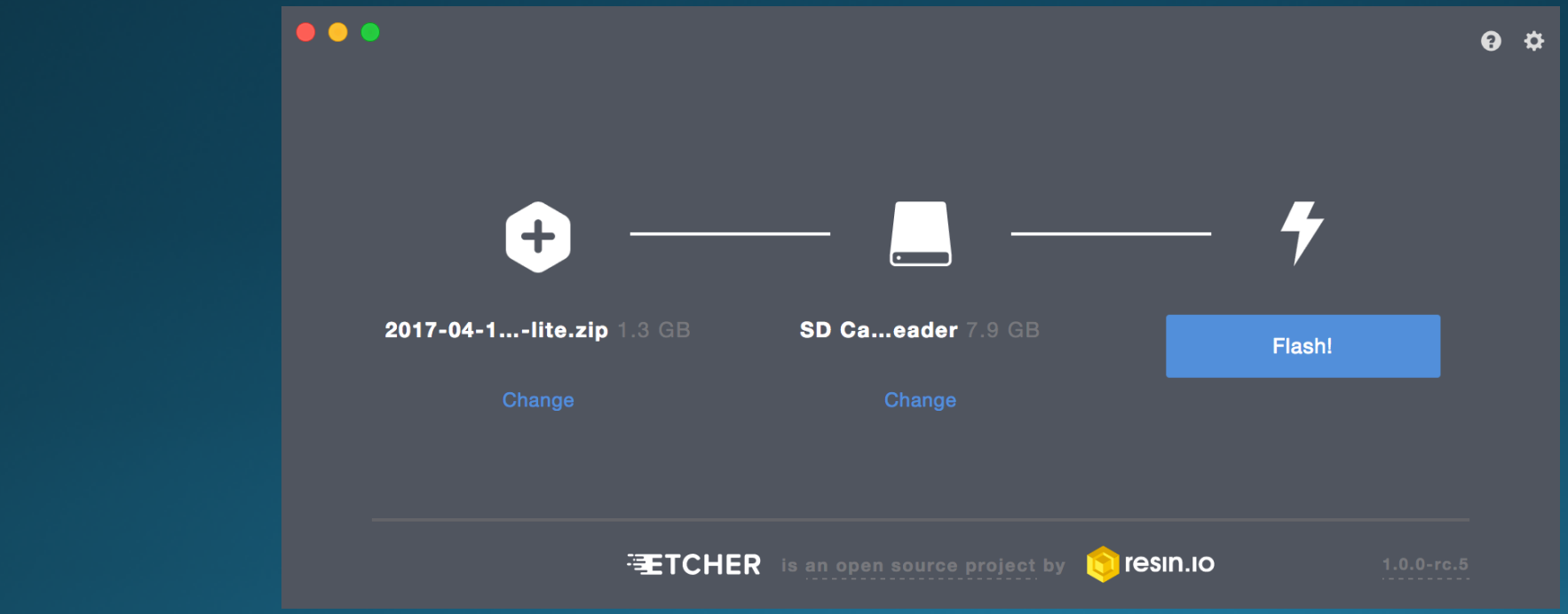
- Computer/Laptop
- Raspberry Pi (ideally a 3, but whatever you got)
- 8 GB+ microSD Card
- microSD card reader
- Raspbian Lite.zip
- Etcher
- Ethernet cable
- Micro USB cable
- Two beers

Workshop

- STEP 1: Grab the appropriate .zip: https://downloads.raspberrypi.org/raspbian_lite_latest
- STEP 2: Grab & install Etcher: https://etcher.io
- STEP 3: Insert microSD card into laptop (using any adapters as needed)

Workshop

- STEP 4: Fire up Etcher, select the .zip archive you downloaded in STEP 1, ensure the microSD card is selected as the destination device, then click “Flash!”



Workshop

- STEP 4.5: Drink a beer

Workshop

- STEP 5: Add a blank file called ‘ssh’ to the root directory of your newly-flashed microSD card
  a) OS X (from terminal): cd /Volumes/boot/ && sudo touch ssh
  b) Debian: cd /media/<username>/boot/ && sudo touch ssh
  c) Fedora: cd /run/media/<username>/boot/ && sudo touch ssh
  d) Windows: backup data, delete all partitions, install Ubuntu, see b.)

- STEP 6: Insert the newly-flashed microSD card into the Raspberry Pi, connect one end of the Ethernet cable and micro USB cable to the Raspberry Pi and the other ends to your computer.

Workshop

- STEP 8: Acquire Internets (needed for Pi-hole setup)
  - If you have a RPi3, you can setup wlano to connect to a nearby AP
  - Edit /etc/wpa_supplicant/wpa_supplicant.conf to include the following:

```
network {
 ssid="SSID"
 #use the directive below if your wireless network is hidden
 scan_ssid=1
 psk="PASSWORD"
}
```

  - ...making sure to replace SSID and PASSWORD with appropriate values

You can also use an external wireless adapter

Workshop

- STEP 9: Update (because best practice… but don't do it now, ain't got time!)
- STEP 10: Pull the PiHole repo from GitHub
  - *sudo apt-get install git*
  - *git clone https://github.com/pi-hole/pi-hole.git*
- STEP 11: Install PiHole
  - *cd pi-hole/automated\ install/ && sudo ./basic-install.sh*

Workshop

- During Pi-hole setup…
  - Follow the prompts; select "eth0" when prompted
  - Select your desired upstream DNS (Google is fine; more info here: https://github.com/pi-hole/pi-hole/wiki/Upstream-DNS-Providers)
  - You want to block ads via both IPv4 and IPv6, so hit OK
  - When asked about using the current IP as the static IP, select "NO"
  - Enter a static IP that can be used by your Pi-Hole at home*

*For example, my home network is on 192.168.200.0/24; I happen to know 192.168.200.10 is available, so I'd choose that… then, at home, I can tell my router to give the RPi's eth0 MAC address the same static. Note that some routers will force itself as the DNS server… you'll need to use the PiHole's DHCP server if that's the case. More here: https://discourse.pi-hole.net/t/router-dns-settings/1233/2

Workshop

- Step 11.5: Drink a beer

Workshop

At this point, you'd want to configure your router to use the Pi-Hole as its DNS server. The steps for this vary by router manufacturer, but if you're not sure, just Google "$ROUTER_BRAND $ROUTER_MODEL dns configuration"

E.x.: *NETGEAR R7300 dns configuration*

Once setup has completed, you're all finished! Reboot the Pi-hole, plug it in to your router, then connect to http://$STATIC_IP/admin/index.php

E.x. *http://192.168.200.10/admin/index.php*

Results

- Pi-hole Dashboard
  - Home page: high-level info such as number of queries made/blocked, domains blocked, usage graphs, etc
  - Query log: search through any DNS requests made on your network
  - Whitelist: domains you're ok with accepting ad content from
  - Blacklist: domains you explicitly want to refuse connections to
  - Disable: kill Pi-hole functionality for an arbitrary time period
  - Tools: Pi-hole management functions
  - Settings: Pi-hole service functions

Now You Can…

- Block ad delivery to your entire network using one device; no more browser plugins or supposedly helpful smartphone apps!
- Monitor DNS queries made on your network
- Blackhole DNS queries for arbitrary domains of your choosing
- ???
- Profit

Aaron J. Scantlin – Security Analyst, University of Missouri
@sysaaron

Questions?