* Introduction
  + What is AdBlocking
    - Adblocking is a software used to block advertisements from being shown or block the website from contacting advertising providers. Adblocking is typically done by browser extensions but can also be done via software on a machine or by changing DNS resolutions.
    - Adblocking is done for a multitude of reasons including protecting privacy, limiting exposure to malicious ads, and better web usability. The ads that are blocked result in lost revenue from advertising providers creating a systemic problem in which countermeasures are fabricated against adblocking technologies.
    - There are many models to adblocking, the basic idea is to block advertisements from being displayed to a user. There are two interesting models of adblocking permitting non-tracking advertisements and obfuscating privacy by simulating impressions on an advertisement. Each model has its pros and cons for the end-user and ad providers, but each has its consequences towards the industry.
  + Types of ad blockers
    - Hosts file / DNS
      * Host-based DNS manipulation is a rudimentary method of blocking hosts that provide advertisements. It is done by modifying the host files on the machine, pointing hostnames or IP addresses to a blackhole (0.0.0.0 or 127.0.0.1).
      * Using DNS filtering is another method, though this is a network-based solution. Setting a specific ip address as your DNS – typically provided by services like NextDNS, AdGuard, or PiHole. DNS filtering functions similarly to host-based DNS blocking, though it is more effective to use this solution due to the time it takes to parse large files locally.
    - Browser Extensions
      * There are two primary forms of browser extensions, ad-blockers, and content blockers. Ad blockers are limited to blocking or limiting the display of the advertisements., while content blockers block a range of tracking elements including advertisements, blocking WebRTC leaks and CNAME cloaking. One of the most used browser extensions, uBlock Origin was created by Raymond Hill is an open-source solution to blocking browser tracking mechanisms.
    - Software
      * There are various software’s built to block advertisements on the internet, some use an internal proxy while others block advertisements on a network device (router). AdMuncher is an example of a host-based adblocking solution that has extended functionality of DNS-based solutions. It can block advertisements that include JavaScript, ad containers, and basic advertisements.
  + Methods AdBlockers use
    - Block flash
    - Block scripts
    - Block popups
    - Lists
      * Regex
      * Blacklist
      * Whitelist
  + New CNAME cloaking methods used
    - In late 2019 Aeris, a user on GitHub posted an issue on uBlock Origin’s repository in regards to first-party CNAME tracking. The site, <https://www[.]liberation[.]fr> embedded a *first party* tracker under their own subdomain. This subdomain, however pointed to a third-party tracking source: Eulerian. It was understood that this form of hiding tracking content was superior to other methods for a few reasons including randomized subdomains (1); CNAME resolution is typically done within a DNS resolver (i.e., Cloudflare, Google, local ISP) (2); filtering ip addresses is inefficient and would slow browsing experiences (3).
    - (Abrams)
    - (Aeris)
* Hypothesis
  + What is CNAME cloaking
    - CNAME cloaking is a technique used to bypass browser-level methods of tracking protection. By using CNAME’s websites are trick a browser into believing it is contacting a first-party domain – which they are initially – however, the subdomain contacts may be mapped to resolve a third-party domain. This cloaking method works because browser extensions are not permitted to access DNS requests, including CNAME responses – Firefox has addressed this – AdBlock extensions will now have to maintain a massive list regarding all subdomains that use CNAME cloaking, which is inefficient and unreasonable to do on many devices. This third-party domain looks like a first-party domain and therefore has access to all first-party resources including cookies, browser parameters, and other metadata help within the browser session.
    - (Gorhill)
    - (Aeris)
    - (Adobe Inc.)
  + There has been an ongoing technical war between tracking protection technologies and anti-tracking technologies. CNAME tracking is one of the many methods used to track users of the internet including, bounce trackers, fingerprinting, and AdBlock detection.
  + What is a CNAME
    - A canonical name or CNAME is a DNS record that points to a domain name, although it can point to another CNAME. CNAME’s are used to ensure that DNS records are updated by a hierarchal structure, rather than manual updates; this ensures there is a limited area in which mistakes are made. It is often the case that websites will use CNAMES within their subdomains that point at their root domain, this helps limit reconfiguration when an IP address is changes. However, this is how CNAME cloaking hides itself.
    - (Mockapertric)
  + Methods to limit CNAME tracking
* Research tasks
  + What I did to find CNAME trackers
    - Make a script in python
    - Iterate through all packets
    - Filter out those that are not DNS
    - Resolve hostnames of all ip addresses
    - Compare is the initial domain requrest matches the response
    - Match the destination response to known tracking providers
    - Find cname trackers
  + Methods for finding CNAME trackers
    - Dynamic resolution
      * Monitor each DNS request and send to get resolved, if the resolved subdomain is a tracking providor block it
        + May result in slower loading speeds
        + Potential privacy breach
    - Resolve all DNS requests
      * Would place all dns queries through a filter, which would also filter out CNAME cloaking because the application has access to DNS responses
        + Adguard
        + NextDNS
        + Pi-Hole
    - Issue regulations regarding permitted tracking
      * Like GPDR
* Methods I used
  + Dynamic resolution
    - The is preferable in terms of performance because typical tracking domains will not require a DNS query because they have already been blocked. Meaning that the only necessary DNS requests are from legitimate or cloaked domains. After checking if a domain is cloaking we can cache the response to ensure for x minutes to ensure that we do not saturate our DNS provider.