

Block the blocker: Studying the effects of Anti Ad-Blocking

Rohit Gupta, Rohit Panda

Master of Science, Informatics, Technical University of Munich
rohit.gupta@tum.de, rohit.panda@tum.de

Abstract. Advertisements are an important revenue stream for a lot of websites. However to address various privacy concerns and improve their browsing experience for these websites, many users are using ad blocking programs and tracker blocking programs.[2] Adblock Plus is one of the more popular ones. Increasing popularity of Ad-Blockers pose a significant threat to the advertising revenues. To combat Ad-Blockers two major strategies have emerged:

1. Acceptable ad programs used by the likes of Google, Microsoft
2. Anti Ad-Blockers used by Yahoo! Mail, WIRED and Forbes.

In our paper, we will discuss the usage of such anti ad blockers, their mechanisms and the impact they have on the economy and the legal sector in Germany, Europe and the world.

Keywords: Advertisements, Ad-blocker, Privacy, Anti Ad-Blocker

1 Introduction

1.1 Motivation

Advertisement is a technique used by product or service manufacturers that detail the unique selling points of a product by means of which it becomes known to the general people. Marketers usually place ads at strategic locations for their products such that they are able to draw the attention of potential consumers and persuade them to buy it. Every product that is built comes along with it a unique set of features, functions and options that is targeted for a specific user base.

A demand is created for a product whose advertisement has been done in a unique way. These demands also lead to a brand name or an identity being created in the market. Ads build an image around the product being marketed such that customers always feel valued. In most cases, good ads trigger promotions of newer or existing products in the portfolio and also generate a possibility of a business to enter into various geographical sectors.

Online advertising or online marketing is a technique of delivering promotional messages to various consumers. It is what drives the economy of the World Wide Web. Most modern websites, in general, tend to monetize their user visits. They include certain spaces across their websites aimed at advertisers to come

and put their promotional content. Thus there is an implicit agreement between the website owner and the advertisers on displaying only genuine promotional content and not include malwares or trick users into any sort of scams.

Most users view online advertisements as a major distraction with few or no benefits and are getting aware of ad blocking techniques. However, a good chunk of users can now use their favorite websites without even glancing at the advertisement sections as they are pretty used to it.

Ad blockers have emerged as the trend that blocks such advertisements to improve users' web-browsing experience, maintaining privacy, and recently protecting themselves against malware. This has impacted businesses that rely on revenues from advertisements.

Anti ad blockers have emerged as an increasingly popular solution. Anti Ad-blockers detect the presence of ad blockers and use several techniques such as simply notifying the user that the tool interferes with the content and the user-experience or other-times when the message blocks the user from accessing the content until they have turned off the ad-blocker.[1] In extreme cases the goal is to circumvent the tool completely.

Interactive Advertising Bureau (IAB) recently released a script to DEAL (Detect, Explain, Ask, Limit) with ad blockers: Ad Block Detection Code Access Request.[3]

1.2 Roadmap

In our paper we propose to study (and/or develop) approaches to:

- Study the usage of these Anti Ad-blocker scripts and their mechanism.
- Find the primary providers of these scripts.
- Their usage on top 5K Alexa websites.[4]
- Their impact on popular ad-blockers.
- Economic impact of Anti Ad-blockers.[5]
- Legality and ethics of Ad-blocking and Anti Ad-blocking.
- Alternatives to Anti Ad-blocking such as whitelisting and acceptable ads program and also taking a look at Anti Ad-block killers.

This paper is structured as follows:

Section 2: In this section, we discuss the background related to online advertising, popularity of ads, how ad-blockers work and also take a look at the related work on the same.

Section 3: In this section, we discuss how Anti Ad-blockers are detected and discuss the methodology behind the same.

Section 4: In this section, we discuss the data sets and results for the methodology used in the previous section.

Section 5: In this section, we analyze Anti Ad-blocker scripts, suppliers and responses.

Section 6: In this section, we discuss alternatives to Anti Ad-blocking such as Acceptable Ads and Whitelists.

Section 7: In this section, we discuss how Anti Ad-block killers work.

Section 8: This section details the legality and ethics of Anti Ad-blocking.

Section 9: We conclude our discussion of our work and provide the roadmap ahead.

2 Background and Related Work

2.1 Background

Online advertising provides a viable way to support online businesses that offer content free of charge to their users, such as news, blogs and social networks. To achieve targeted and hence more effective advertising however, advertisers and tracking companies record user browsing behavior, e.g. pages viewed, searches conducted, products purchased [6,7,8]. Such techniques are known as online profiling and have raised significant privacy concerns because online user profiles can be used to infer private sensitive information and user interests [9,10].

Ad-blockers aim to improve the user experience and privacy by eliminating undesired advertising content, as well as preventing the leakage of sensitive user information towards third-party servers. The most well-known Ad-blocker solutions are browser extensions such as Ghostery or Adblock Plus which suppress unnecessary requests to third-party advertisements and tracking servers, thereby limiting the risk of data leakage towards these servers. Recently, we have experienced a proliferation of Ad-blocker browser extensions in the wild which might be due to users' privacy concerns and awareness about online profiling as well as due to the increasingly intrusive advertisements. According to Google usage statistics [11], already more than ten million surfers are actively using a browser with the Adblock Plus extension enabled. In a measurement study [12], researchers show that 22% of the most active users are using the Adblock Plus Ad-blocker while surfing the Web.

Online Advertising. Online advertising or online marketing is a technique of delivering promotional messages to various consumers. It is what drives the economy of the World Wide Web. Most modern websites, in general, tend to monetize their user visits. They include certain spaces across their websites aimed at advertisers to come and put their promotional content. Thus there is an implicit agreement between the website owner and the advertisers on displaying only genuine promotional content and not include malwares or trick users into any sort of scams [13].

Most users view online advertisements as a major distraction with few or no benefits and are getting aware of ad blocking techniques. However, a good chunk of users can now use their favorite websites without even glancing at the advertisement sections as they are pretty used to it. Online advertising includes marketing strategies such as:

- E-mail marketing
- Search Engine Marketing or Optimization
- Social Media Marketing

- Display Advertising
- Mobile Advertising

Revenue Generation for Ads. The online advertising market has significantly increased in importance over the last few years and is now one of the key forms of advertising, thereby generating a significant amounts of revenue [14]. In 2015, online advertising revenues worldwide amounted to about \$170B, a figure that is expected to grow to more than \$330B by 2021. In a 2017 global comparison, the United Kingdom, Germany and France ranked among the largest online advertising markets in the world (Figure 1), with digital ad revenues of \$11.72B, \$7.37B and \$5.13B, respectively. Overall, the European online ad market grew

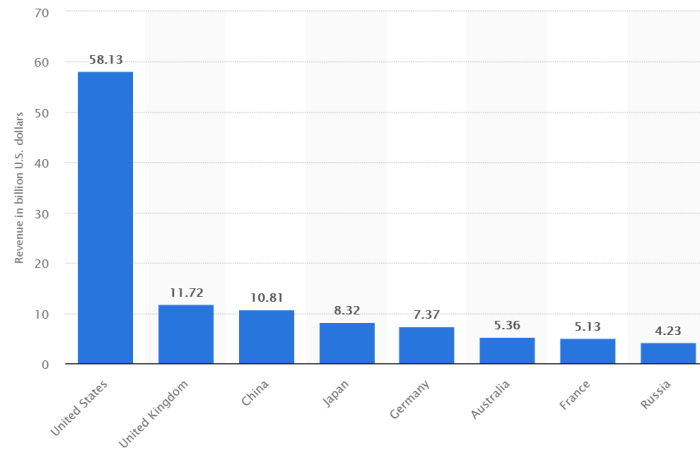


Fig. 1. Largest online advertisement markets in 2017. [15]

by 12.3 percent in 2016 on 2015. The fastest growing online advertising markets that year were Slovenia and Ireland.

In the United Kingdom, online advertising expenditures increased by nearly five billion British pounds between 2007 and 2015, from 2.81 billion British pounds to 7.71 billion British pounds [14]. Paid search and display advertising accumulated the highest share of spending. Google’s net digital advertising revenue was the highest in the UK and is projected to grow further in future years. While Google generated more than 2.5 billion British pounds in revenue through its digital advertising channels in 2013, Facebook’s digital ad revenue accounted for 371 million British pounds.

In the U.S., the first quarter of 2017 marked the highest ever Q1 earnings for online advertising, at \$19.6B, according to the latest IAB Internet Advertising Revenue Report by the Interactive Advertising Bureau (IAB) and prepared by PwC US. These numbers show the increasing amount of revenue generated by

online advertisement and why they are so crucial to industries and businesses across the world.


In Germany, the 2017 revenues stood at \$7.37B. This number is expected to grow to \$8.40B by 2020 and to \$9.21B by 2022. The major revenue categories ranked by percentage shares are as follows:

- Search Advertising with \$3.44B - 48%
- Banner Advertising with \$1.46B - 20.5%
- Classified Advertising with \$0.95B - 13%
- Social Media advertising with \$0.89B - 12.5%
- Video Advertising with \$0.40B - 6%

The popularity of ad-blockers. The issues with online ads have resulted in the increasing usage of ad-blocking software. Ad-blocking software (or ad-blocker) is an effective tool that blocks ads seamlessly, generally published as extensions in web browsers such as Chrome and Firefox. The soaring popularity of ad-blockers now mean that mobile Ad-block usage has surpassed desktop Ad-block usage. The total number of devices that use Ad-block encompassed 615 million devices by 2016 end [16]. Some of the top reasons to use ad-blockers include security, interruption, website load time, too many ads or privacy issues. In a survey of U.S. demographics, men were 34% more likely to use ad-blockers than women on desktop and laptop computers. Suburban and urban internet users were 17% more likely to install ad-blockers than those in rural areas.

The popularity of ad-blockers in Germany. According to PageFair statistics [16], Germany ranked highest in Ad-block penetration when it came to desktop ad-blockers (Figure 2). These statistics indicate a tremendous potential

Adblock penetration per online capita, %



	Desktop	Mobile	Overall
U. States	18%	1%	18%
China	1%	13%	13%
U. Kingdom	16%	1%	16%
Japan	3%	-	3%
Germany	29%	1%	29%
Australia	20%	2%	20%
Canada	24%	-	25%
France	11%	1%	11%
Brazil	6%	1%	6%
South Korea	4%	-	4%
Russia	6%	3%	6%
Italy	17%	1%	17%
Netherlands	17%	2%	17%
Spain	19%	-	19%
Mexico	8%	-	9%
Sweden	27%	-	27%
Indonesia	8%	58%	58%
Denmark	25%	2%	25%
India	1%	28%	28%
Argentina	14%	-	14%
Finland	23%	-	23%

Fig. 2. Top Ad Markets (ad spend) statistics.

for European markets since there is no clear single solution for mobile Ad-block

usage. Legacy desktop Ad-block installations are not yet being replaced with mobile equivalents and as such the first mobile Ad-block solution to gain traction in Europe will connect with a large audience of former desktop Ad-block users.

On the contrary, a report by Bundesverband Digitale Wirtschaft (BVDW) and Online-Vermarkterkreis (OVK) titled "Zentrale Adblocker-Rate des OVK" [17] in December, 2016 showed a dip in ad block incidence rates from Q1 to Q3 of 2016 (Figure 3).

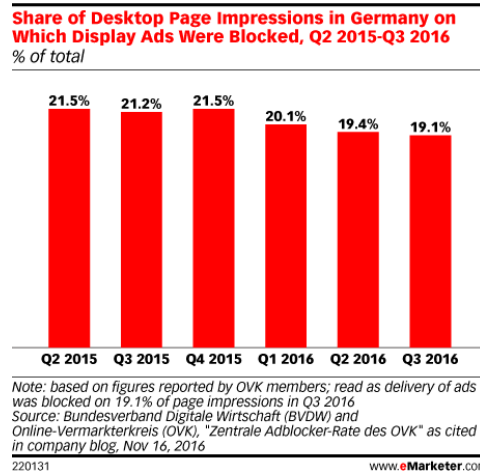


Fig. 3. Share of Desktop Page Impressions in Germany on Which Display Ads Were Blocked [17]

The critical difference to be noted in the two sources cited above is that PageFair looked at the number of penetration/installations of ad-blockers while BVDW & OVK focused on the actual number of websites that were affected by such ad-blockers.

Economic Impact of Ad-blocking. Ad block usage in the United States resulted in an estimated \$5.8B in blocked revenue during 2014 [18]. It had been estimated to cost \$10.7B in 2015 and \$20.3B in 2016. With the ever increasing number of Ad-block users the global cost of ad blocking surpassed the projected numbers of \$40B in 2016 making it crucial for the understanding of the effects of Ad-block on the economy.

How do ad-blockers work? Ad-blockers remove ads by either page element removal or web request blocking. For web request blocking, ad-blockers look for certain URLs and remove the ones that belong to advertisers. For page element removal, ad-blockers use various CSS selectors to access elements and end up removing them. For both of these actions, ad-blockers are dependent on filter lists that contain the set of rules (as regular expressions) specifying

the element selectors and domains to remove. There are various kinds of filter lists available which can be included in ad-blockers. Each of these lists serves a different purpose. For example, Adblock Plus by default includes EasyList [19], which provides rules for removing ads from English websites. EasyPrivacy [20] helps ad-blockers to protect user privacy by removing trackers.

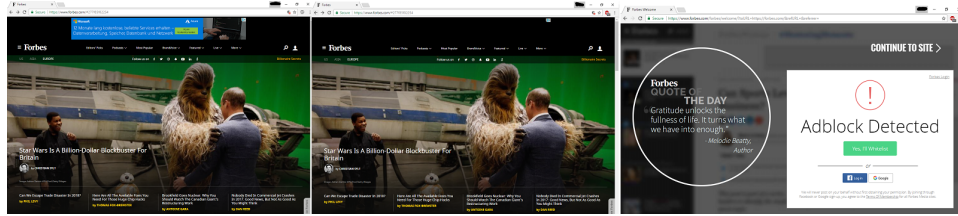


Fig. 4. Web page evolution for Forbes shows from left to right web page with ads, with ad-blocker enabled and with an Anti Ad-blocker.

Source: www.forbes.com

Listing 1 shows ad code for display on the website.

Listing 2 shows code how the ad-blocker is detected on the website's JavaScript code. Ad-blockers also work on the following two techniques:

Filter Lists: FilterLists [21] helps to protect privacy and security when using the Internet. It provides a comprehensive directory of subscription lists to block advertisements, malware, trackers, and other general annoyances. As users browse the Internet, they compare HTTP requests to their list of hosts and filters to selectively block advertisements, trackers, and general annoyances. This filtering helps to protect the surfer's privacy, prevents malware attacks, and reduces bandwidth requirements.

Filter Matching: Usually Adblock Plus treats filters as if it had a wildcard at its beginning and end, e.g. there is not difference between the filters `ad` and `*ad*`. Sometimes we want the filter to only match at the beginning or the end of an address. In such a case, Adblock Plus has come up with a solution that uses a pipe symbol to skip or start from any particular point in a website's URL [22].

Ad-blocker extensions. The following are the most common ad-blocker extensions used in desktop and mobile browsers based on ratings and number of downloads:

- μ Block Origin for Chrome and Firefox
- Adblock for Chrome
- Adblock Plus for Firefox, Chrome, Opera and Safari
- Adblock Pro for Chrome
- Aduard for Chrome and Firefox
- AdRemover for Chrome
- Ghostery for Chrome, Firefox, Opera, Safari, Internet Explorer, Android and iPhone iOS

```

1 <script>
2   try {
3       fbs_settings.blocked_classes = ["sidebar_ADBOX", "textlinkads",
4       "advertisement-banner", "externalAdComponent", "ad_label2a",
5       "adseparator", "content-advertisement", "review_ad1", "loop-ad",
6       "BottomGoogleAds", "ad-160-160", "aopsadvert", "sidebar_advertising",
7       "yan-sponsored", "advertBox", "ad-parent-hockey", "block-maniad",
8       "advertising-block", "google_ad_wide", "txtAd", "rightSideSponsor",
9       "adwolf-holder", "view-display-id-ads_all", "ad_links",
10      "advertisement-tag", "widget_ad_rotator", "ad-caption",
11      "ads-bottom-block", "gemini-ad", "rightColAdBox"];}
12  catch(err) {
13      fbs_settings.blocked_classes = null;
14  }
15 </script>
16 <script type="text/javascript">setTimeout(function() {
17     document.getElementById('main-content').className = '';
18 }, 1000);
19 try {
20     performance.mark('blocking_scripts_start');
21 } catch (e) {}
22 </script>
23 <script src="//i.forbesimg.com/forbes/scripts/b4b56484.vendor.js"></script>
24 <script src="//i.forbesimg.com/forbes/scripts/0d9abc37.scripts.js"></script>
25 <div id="css-js-dynamic"><span class="dynamic-css">false</span>
26     <span class="dynamic-js"></span>
27 </div>
28 <div ng-if="!$root.is_mobile" id="teconsent"></div>
29 <script>$(window).on("touchstart", function(e){});</script>
30 <script type="text/javascript">
31     try {
32         performance.mark('blocking_scripts_end');
33     } catch (e) {}
34 </script>

```

Listing 1: Script to show how an ad is displayed on the website

- Simply Block Ads! for Chrome
- SuperBlock AdBlocker for Chrome
- μ Adblock for Firefox

```

1 j = document.createElement("div"),
2 j.setAttribute("class", r.join(" ")),
3 document.body.appendChild(j), "none" === window.getComputedStyle(j).display
4 && (this.removeWelcomeCookies(), this.adblock_state = "on")
5 }
6 }, this.removeWelcomeCookies = function() {
7     var b = function() {
8         s = !0, window.advBidxc && advBidxc.adBlockDetected
9         window.uabfunc && window.uabfunc.detected
10        (a.remove("welcomeAd", {
11            path: "/",
12            domain: ".forbes.com"
13        }), a.remove("dailyWelcomeCookie", {
14            path: "/",
15            domain: ".forbes.com"
16        }), a.put("re_ab", 1, {
17            path: "/",
18            domain: ".forbes.com"
19        })))
20    };

```

Listing 2: Script to show how an ad-blocker code is detected on a website's Javascript code

– uMatrix for Firefox, Chrome and Opera

The rise of Anti Ad-blockers. The online advertising industry considers such ad-blockers as a threat to their business models which revolves heavily around advertisements. This has led to a strong conflict between publishers and ad-blocking tools. IAB's script "DEAL"s (Detect, Explain, Ask, Limit) with such ad-blockers [3]. Such scripts help publishers detect ad-blockers in browsers when users visit their websites (detection). Once detected, publishers ask users to turn off their ad-blocking tool. These can range from a small message on the website to more aggressive blocking of website content and/or functionality.

Figure 5 shows a couple of examples of ad-block detection responses. This is done by employing Anti Ad-blocking tools or scripts that detect the usage of such ad-blockers. When a user with the ad-blocking tool opens such a website, these scripts typically identify if any ads have their visibility altered. If ads are found hidden or removed by an ad-blocker, publishers take countermeasures according to their policies.

Impact of Anti Ad-blockers. Around 9% of today's most popular websites [24] deploy Anti Ad-blocker scripts to fight off the usage of ad-blockers

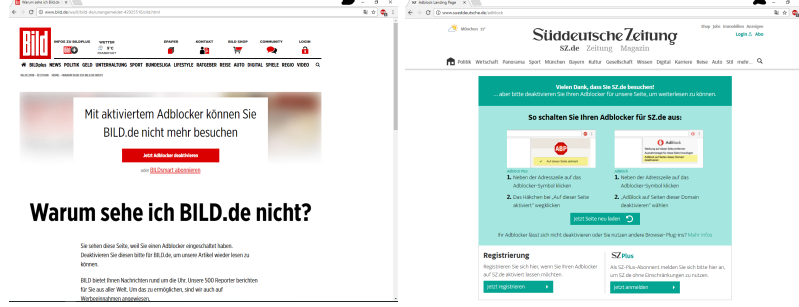


Fig. 5. German websites using ad-blocker detection scripts.

that generate significant advertising revenues. Researchers at the University of Iowa and University of California-Riverside scanned Alexa Top 5K websites for anti Ad-block tools Anti Ad-block Killer List [27] and Combined EasyList for anti Ad-block scripts. The results (Figure 6) showed a gradual increase in Anti Ad-blocking scripts, that prove the online advertising industry reacting to the immediate losses incurred by the use of ad-blockers on their websites.

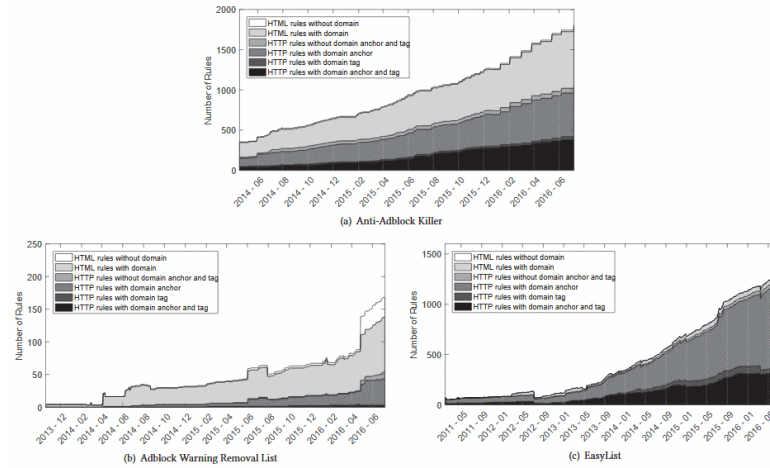


Fig. 6. Anti Ad-blocking scripts with their gradual rise in usage [23]

When it comes to economy, ad-block usage in the United States resulted in an estimated \$5.8B in blocked revenue during 2014 [18]. These numbers are expected to grow to \$60B in 2018 making it crucial for businesses, industries and publishers to deploy Anti Ad-blockers.

Economic impact of ad-blockers on browser performance and page load times. In an extensive analysis on browser performance and page load

times, Kiran et al. [25] conclude that (i) uBlock has the best performance, in terms of ad and third party tracker filtering, and least privacy tracking, (ii) the time to load pages is not necessarily faster when using ad-blockers, and (iii) this is partly the case due to additional trackers and libraries being introduced by the ad-blocking tools.

2.2 Related Work

Online Advertising. Online advertising has emerged as one of the main sources of revenue on the web [15]. While advertisers claim that ads on the web help keep most parts of the web free for consumers, consumers find advertising annoying and potentially dangerous. Moreover, many users perceive such ads as a threat to privacy and tracking making it an important reason to install ad-blockers [16]. Yu et al. [26] found that 95% of the pages visited contain 3rd party requests to potential trackers and 78% attempt to transfer unsafe data. Ad-blockers also remove tracking buttons (such as Facebook’s ‘like’ button) and protect their users from known malware domains.

Ad-blockers. The topic of ad-blockers have encouraged researchers to study it’s usage and effects. Pujol et al. conducted a measurement study using passive network traces of thousands of users from a European ISP to quantify ad-block usage [12]. Their results show that 22% of users use Adblock Plus. They also found that ad-block users still generate significant ad traffic due their enrollment in the acceptable ads program. They also found little evidence that Adblock Plus users install the EasyPrivacy [20] list of filters, which aims to protect end users’ privacy by blocking trackers. Also, they concluded that Adblock Plus users are mostly interested in blocking annoying ads rather than protecting their privacy, or that they are not aware of these options or how to change them.

Anti Ad-blockers. Our paper discusses in length the Anti Ad-blocking techniques and their effects adopted by Nithyanand et al. [4] and Haris et al. [1]. Nithyanand et al. [4] clustered JavaScript snippets and manually analyzed these clusters to identify third-party Anti Ad-blockers. They found that 6.7% of top 5K Alexa websites employ anti ad-blockers. They also consider all websites that include Anti Ad-block scripts in their analysis. Haris et al. [1] observed that at least 686 websites in the Alexa top-100K currently deploy Anti Ad-blockers at their home page to detect ad-block users and respond with visible notifications. The notifications ask users to either disable ad-blockers, consider donation, or pay a subscription fee. Such notifications cannot be disabled unless users disable ad-blockers or pay up. These could potentially harm their business. To counter such Anti Ad-blockers, ad-blockers now use filter lists to remove Anti Ad-block scripts and ad-block detection warnings. EasyList [19], which is used by ad-blockers to block ads, now contains rules that specifically target Anti Ad-blockers. Anti Ad-block Killer list [27] mostly contains web request blocking rules to remove Anti Ad-block scripts. The rules in these independently run crowd-sourced lists are tailored to specific Anti Ad-blockers.

3 Detecting Anti Ad-blockers

In this paper we are trying to replicate, reproduce and improve upon the work done by Haris et al. [1] in a German context. Haris et al. were working primarily on a Global context using sites in the Alexa top-100K which may have a slight bias towards sites used by users in America and China. This can be seen from the country of origin of Alexa top-100 websites. [36]. Google Germany and Amazon Germany being the only German sites in that list. Haris et al. also don't provide any source code of their work but explain their methodology in the paper which has been adopted by us. In this section we design and implement an approach for automatically identifying websites that employ Anti Ad-Blockers. It has been observed that websites employing Anti Ad-Blockers generally make some changes to the content of the web page for users using Ad-block extensions. Here we identify, extract and use these features to train a machine learning model which can then automatically detect websites that employ Anti Ad-blockers.

3.1 Overview

For a robust approach we rely mostly on changes and additions made by Anti Ad-blockers to the HTML content of the web pages.

The changes made by anti ad-blockers to the HTML content can be broadly categorized into

- addition of extra HTML elements
- change in the style of existing HTML elements
- changes in the textual content

An overview is provided below:

Node Changes: To show a message to the users to disable anti ad-blockers to whitelist their sites, websites may add extra DOM elements. So the presence of such elements can maybe suggest the use of Anti ad-blockers.

Style Changes: Some websites have hidden div elements with notifications which may become visible on detecting ad-blockers. We can measure changes to the style attributes on a web page.

Textual Changes: Some websites change the textual content on detecting ad-blockers. Therefore, we can measure changes to the textual content of a web page and addition of text-related nodes.

Structural Changes: We also check for URL redirections as some websites have been found to redirect users using Ad-blockers to a separate URL and also check for cosine similarity between the same web page in each instance.

3.2 Methodology

To simplify the process we consider only Node features and textual features and ignore style changes from our experiments. We do A/B testing with ad-blocker extension and without one and compare the websites in both cases.

Crawler overview To automate this we make use of Selenium Chrome Webdriver [37] to launch two separate instances of Google Chrome web browser one with an ad-block extension and one without one. We open the sites under test with each instance.

A/B testing A/B testing is a way to compare two versions of a single variable typically by testing a subject's response to variable A against variable B, and determining which of the two variables is more effective. As the name implies, two versions (A and B) are compared, which are identical except for one variation that might affect a user's behavior. Version A might be the currently used version (no ad-blocker extension), while version B is modified in some respect (ad-blocker extension). [38]

Browser profiles We create two new browser profiles. In one of the profiles we install ad-blocker extension and in the other we don't. We use Adblocker Pro due to its popularity. It has options to configure various filter lists. We use the EasyList filter [19] after removing all the anti ad-block rules as well as disallow Acceptable Ads. The anti ad-block rules are marked by the comments ! Anti-Adblock these rules try to circumvent Anti ad-blockers

Data Collection We then open the site in each instance and record changes in the various Node Features and Textual Features using a python script. BeautifulSoup Library is used for screen-scraping. The results are collected in a csv file.

Feature Extraction

Node Features. For each instance we extract the number of anchor, div, h1, h2, h3, img, table, p, iframe and text nodes. Then we compare A with B and find the difference.

Textual features. For each instance we extract the number of lines, words and text. We gain compare A vs B. We also detect whether the web page contains key words like adblocker, adblock, ad block, ad-block, whitelist, block-adblock, pagefair, fuckadblock in A.

Structural features. We apply the cosine similarity metric to the two web pages. Cosine similarity gives a useful measure of how similar two documents are likely to be in terms of their subject matter. If the cosine similarity between A and B is very low it indicates significant content change. We also check for URL redirection.

Model Training and Testing We then feed the extracted features to a machine learning classifier which can be then used to identify websites employing anti ad-blockers. For the learning phase we need labelled data. For this purpose we need some negative samples (websites that do not employ anti ad-blockers) and positive samples (websites that employ anti ad-blockers). To collect positive samples we look into the issue list of anti-adblock-killer [39], websites on the issue list employ anti ad-blockers. They were checked manually to confirm this. For negative samples we took some websites from the Alexa top-100 websites list and manually checked them. We used the weka toolkit for its machine learning algorithms.

4 Datasets and Results

4.1 Characterizing websites that employ Anti Ad-blocking

4.2 Comparison of different ad-blockers and profiles

4.3 Website response to detection of Ad-blockers

4.4 Geographical Comparison

4.5 Limitations

- We remove all anti ad-block filters in EasyList. This may not be the default configuration used by most people. But as we are attempting to quantify websites which employ Anti ad-blockers we feel that this configuration will give us a clearer picture.

5 Discussion

5.1 How Anti Ad-blockers work: Analyzing Anti Ad-blocker scripts

Anti Ad-blocker scripts perform two basic operations (1) detect the presence of ad-block plugins (2) display a message asking the user to either disable ad-block or to whitelist the website or silently track the usage of the ad-blocker and report back to a server. These scripts employ a wide variety of tactics to achieve this. These may range from using simple scripts from first-party domains which check display-related attributes e.g. height, width of ads to detect ad-blockers to more sophisticated scripts from third-party domains that provide baits, do continuous detection, use cookies to track ad-block detection across various visits. These scripts are usually highly obfuscated and use different mechanisms so it becomes a challenge to detect and understand them.

First-Party Anti Ad-blocking scripts

Listing 3 shows a simple first-party ad-blocking script taken from a real-world website. They rely mostly on a bait.

Timing: These scripts typically work on page load but may add a delay of a few seconds using `setInterval()`. The aim is to wait for the ad-blocker to remove the ads before trying to detect them.

Detection Logic: We note that the Anti Ad-blocking script injects an empty div whose class is set to `banner_ads` which is a known class type that will trigger blocking. This is the bait. The code then simply checks whether the ad frame is blocked to determine the presence of ad-blockers. Specifically, when an ad-blocker is used, the ad frame will become undefined, and its length and height values will be zero. The if condition in the Anti Ad-blocking script checks the values of these attributes. If the script detects that the value of either of these attributes is zero, it detects ad-blocker and reacts by displaying an alert and subsequently redirecting the user to a subscription page (code omitted for brevity). Without ad-blocker, the if condition will not be satisfied.

```

1 <div class="banner_ads">&nbsp;</div>
2 <script>
3 var ads = document.getElementsByClassName('banner_ads'),
4 ad = ads[ads.length - 1];
5 if (!ad || ad.innerHTML.length == 0 || ad.
6 clientHeight === 0)
7 alert("We've detected an ad blocker running on
8 your browser." + ...);
9 }
10 </script>

```

Listing 3: A simple Anti Ad-blocking example from a real website

Third-Party Anti Ad-blocking scripts

Now we take a look at third-party ad-blocking scripts. These are more sophisticated than the First-Party techniques and employ several detection techniques at the same time. They also provide options to customize messages seen by the user and the action that the user has to take.

```

1 var e = {
2     adblock: "chrome-extension://gighmmpiobklfepjocnamgkkbiglidom/
3     img/icon24.png",
4     adblock_plus: "chrome-extension://cfhdojbkjhnlbpkdaibccddilifddb/
5     block.html",
6     adblock_pro: "chrome-extension://ocifcklkibdehekfnmflempfgjhbedch/
7     components/block/block.html",
8     adblock_premium: "chrome-extension://fndlhnanhedoklpdaacidomdnplcjcpj/
9     img/icon24.png",
10    adblock_super: "chrome-extension://knebimhcckndhiglamoabbnifdkijidd/
11    widgets/block/block.html",
12    adguard: "chrome-extension://bgnkhnnamicmpeenaenljfhikgbkllg/
13    elemhidehit.png",
14    adremover: "chrome-extension://mcefmojpghnaceadnghednjhbmphipkb/img/
15    icon24.png",
16    ublock: "chrome-extension://epcnnfbjfcgphgdmggkamkmgjdagdnn/
17    document-blocked.html"
18 }

```

Listing 4: Identifying installed extensions

Timing: PageFair script performs periodic checks at various times of pageLoad to detect ad-blockers.

Detection Logic: PageFair detects ad-blockers by looking for various extension resources (as shown in Listing 4) exposed by popular ad-blockers like adblock, adguard, adremover and ublock at chrome-extensions://. Each ad-blocker has an unique extension identifier. It also uses multiple baits (Listing 5) such as divs whose id is set to an identifier which is blocked by ad-blocker. The second method is a script bait where it tries to download a script "adsense.js".

6 Alternatives to Anti Ad-blocking

6.1 Acceptable Ads

Acceptable ads programme (by Adblock Plus) lays down a technique that is focussed on effecting ads on websites. They define a certain set of criterias that ensure that ads placed on websites are not annoying to users, disrupt or distort the web page content and are transparent such that there are no hidden ads or popups that violate the ad being accepted as an acceptable ad. The criterias [29] are defined as follows:

Placement: Ads must be placed such that they do not disrupt the user's natural reading flow. Such ads must be inserted in the top, side or beneath the Primary Content. The Primary Content is either directly related or expands upon the central topic of a document or the central functionality of a software application.

Distinction: Ads should not be mixed with any other content such that the user is misled into thinking of it as a primary content. Ads should be clearly marked with the word "Advertisement" or its equivalent.

Size: Individual ad size requirements depend on the placement of the ad:

- When placed above the primary content, the maximum height of an ad should be 200px.
- When placed on the side of the primary content, the maximum width of an ad should be 350px.
- When placed below the primary content, the maximum height of an ad should be 400px.

In addition to the above mentioned acceptable ads, there are various types or categories of ads that are not acceptable. They are listed as follows:

- Ads that visibly generate new ads if the Primary Content does not change
- Ads with excessive or non user-initiated hover effects
- Animated ads
- Autoplay on sound or video ads
- Ads that expand
- Oversized image ads
- Interstitial page ads
- Overlay ads and overlay in-video ads

```

1      function v(a, e, d) {
2          var b = document.createElement("DIV");
3          b.id = d;
4          b.className = e;
5          b.style.width = "1px";
6          b.style.height = "1px";
7          b.style.top =
8              "-1000px";
9          b.style.left = "-1000px";
10         document.body.appendChild(b);
11         e = jQuery("#" + d);
12         d = e.is(":hidden") ? 1 : 0;
13         q[a + "_hid_t0"] = c.browser.mozilla ? 0 : d;
14         e.remove();
15         g()
16     }
17
18     function d(a) {
19         function e(a) {
20             var b = c.m(q);
21             0 < c.t(b, "s_blk") (b = jQuery("#" + d), q.s_blk = a, b.remove(), g())
22         }
23         var d = c.j(),
24             b = document.createElement("SCRIPT");
25         9 > c.J c.browser.safari c.browser.mozilla ? setTimeout(function() {
26             e(0)
27         }, 1) : (c.d(b, "load", function() {
28             e(0)
29         }), c.d(b, "error", function() {
30             e(1)
31         }));
32         b.id = d;
33         b.type = "text/javascript";
34         document.getElementsByTagName("head")[0].appendChild(b);
35         b.src = a
36     }

```

Listing 5: Multiple baits and timeout

- Pop-ups and Pop-unders
- Pre-roll video ads
- Rich media ads (e.g. Flash ads, Shockwave ads, etc.)

6.2 WhiteLists

Websites that adhere to the Acceptable Ads programme can apply for their websites to be whitelisted with Adblock Plus. This is very similar to anti-viruses marking some applications as "safe" and allowing them to run, while blocking other potentially harmful ones. As a common practice, publishers that detect ad-blockers ask users to whitelist their websites using the Disable or Whitelist option for the respective ad-blocker they are using. While most ad-blockers allow users to configure their browsers to whitelist individual websites, users rarely make use of this. That is where ad-blockers like Adblock Plus provide a default whitelist.

6.3 User Perception

Websites such as Forbes, request users to whitelist their site so that they can get "ad-light experience" for a few days. The Atlantic has started charging users for an ad-free version of their website if users do not disable ad-blockers. For users, it is about all or nothing.

7 Anti Ad-block killers

7.1 How do they work

It tricks sites that use Anti Ad-blocker technology into thinking you aren't using an Ad-blocker. The Ad-blocker blocker lets you keep your Ad-blocker on when you visit a page that would usually disable it by using a JavaScript file and filter list. This means you can work around bans on Ad-blockers from common news companies, like Forbes, which lock you out when you're detected.

It works against a number of different technologies used to detect Ad-block users, and is likely to be a part of the next armsrace as publishers work out how to block the Ad-blockers using Ad-blocker blockers. Anti Ad-block killers like AAK [28] are composed of a user script «AakScript» written in javascript and a filter list «AakList» using the same syntax as filter lists of Adblock and Adblock Plus. It helps one to keep Ad-Blocker active, when we visit a website and it asks us to disable. Script managers like Greasemonkey for Firefox or Tampermonkey for Chrome, Opera, Safari are necessary to install AakScript. Now AakList filter list can be added to Ad-block plugins like Adblock, Adblock Plus, uBlock Origin or Adguard Blocker.

8 Legality and Ethics of Anti Ad-blocking

8.1 Increasing Transparency

The argument of Anti Ad-blocking ensues on the topic of maintenance of websites and henceforth businesses. Ad-block users often fail to understand how these websites pay for their monthly server and bandwidth charges. For most of such "free" sites, their revenue is generated through advertisements. Other websites use subscription services while the rest consume the costs. The latter ones are those that have another source of revenue which is usually not Internet based.

The bottom line of any business is that labor must be paid. It must be in accordance to what a writer, producer, musician, developer or any professional creates. This also revolves around the fact that the cost of living varies across the globe. Websites are compensated based on impressions measured by pay per click or cost per click on the adverts. While significantly bigger businesses could potentially hire more people to keep their websites running on profit, the smaller businesses are the ones who suffer the most. An analogy of going to a shop, purchasing an item and paying for the item collaborates with the model of advertisements. It is unethical to leave the shop without paying appropriately for the item. With the increasing cost of maintenance of websites and the cost of living, publishers rely heavily on such revenue sources.

There is a noticeable trend in publishers who detect the presence of ad-blockers are now fighting back against ad-blockers by asking users to disable ad-blockers or by subscribing for an ad-free version. This poses an ethical dilemma to users, using an ad-block and stopping revenue income for publishers as well as for publishers, using an Anti Ad-blocker to prevent users' intentions of blocking ads.

8.2 Legality in European Union

The Interactive Advertising Bureau (IAB) are of the opinion that ad block detection is not illegal. The European Commission had in a letter to privacy campaigner Alexander Hanff [30] specified that ad-blocker detection tool requires access to user data to determine if they have extensions or tools to block ads. Article 5.3 of the European Union's ePrivacy Directive [31] states: "Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user."

Under this EU law, publishers must ask for permission before accessing a user's personal information, similar to how websites must ask for permission to store cookies on user devices. However the other side of the argument is that publishers are only detecting via Javascript if the ads have been delivered, not checking if any ad-blocker is installed, thus complying with the ePrivacy directive.

8.3 Legality in Germany

Media groups *Süddeutsche Zeitung*, *Pro-Sieben-Sat.1*, and *IP Deutschland*, an RTL subsidiary recently fought a legal battle against Cologne-based ad-blocking vendor Eyeo for banning of Eyeo's ad-blocking software Adblock Plus. The Munich higher regional court ruled [32] that the ad-blocking software Adblock Plus is legal. The Munich higher regional court also noted that the software did not violate any competition laws in Germany, with Eyeo's business model not qualifying as "forbidden aggressive advertising". Although joining Eyeo's whitelist is free, the media groups are objecting to the fact that Eyeo is making money from the extra revenues that the advertisers are making by joining these whitelists under the Acceptable Ads programme.

This court order comes in contrast to another similar court order ruling in Cologne, where publisher Axel Springer secured a partial victory [33] against Eyeo stating that Adblock Plus must add Axel Springer to the whitelist for free but must abide by the Acceptable Ads criteria. The contrast in such verdicts could potentially build up these cases to Germany's Federal Court of Justice.

In a blog post detailing the court decisions [34] Adblock Plus maintain their legality under German laws and as such the German judges have since not favored the usage of ad-blocking detectors.

In a Hamburg judgement for *Spiegel versus Eyeo*, which has since been made public, Eyeo cited [35] that as of August 2015, Adblock Plus was installed on approximately 9.55 million browsers with German IP addresses, which accounted for around 5% of the computers in Germany used to access the Internet. Almost 3,500 websites were whitelisted for Adblock Plus' Acceptable Ads to be viewed by default. From these, around 90% did not pay, but the largest 10% did. The judges concluded that Internet users have a genuine interest in the removal of such undesired advertising, protection from potentially malicious softwares and control of their data.

9 Conclusion

Building on the work done by Nithyanand et al.[4], Haris et al. [1] we have tried to present a quantitative and qualitative analysis of anti ad-blockers and their usage in a German context. We found that...

9.1 Future Work

If any opportunities arise in the future we would like to conduct a more exhaustive evaluation of websites in Germany and also refine our methodology to account for the fast changing world of Ad-Blockers and Anti Ad-Blockers.

9.2 Acknowledgements

The authors would like to thank Professor Jens Grossklags and fellow students taking part in the seminar and for providing valuable inputs and insights.

9.3 Source code and data release

Source code for this project can be found at the link: <https://github.com/RohitPanda/seminar-blocking-adblockers>

References

1. Haris Mughees, Muhammad, Qian, Zhiyun, Shafiq, and Zubair. Detecting Anti Ad-blockers in the wild. proceedings on privacy enhancing technologies (2015)
2. Garimella, Kiran, Kostakis, Orestis, Mathioudakis, and Michael. Ad-blocking: A study on performance, privacy and counter-measures (2017)
3. Interactive Advertising Bureau. Ad block detection code access request (2017) <https://github.com/InteractiveAdvertisingBureau/AdBlockDetection>
4. Rishab Nithyanand, Sheharbano Khattak, Mobin Javed, Narseo Vallina-Rodriguez, Marjan Falahrastegar, Julia E. Powles, Emiliano De Cristofaro, Hamed Haddadi, and Steven J. Murdoch. Ad-blocking and counter blocking: A slice of the arms race (2016)
5. Tech Crunch. Blocking ad blockers boosted facebook’s desktop ad revenue 18 percent (2016) <https://techcrunch.com/2016/11/02/add-cash-plus>
6. Barford, P., Canadi, I., Krushevskaja, D., Ma, O., Muthukrishnan, S.: Adscape: harvesting and analyzing online display ads. In: Proceedings of the 23rd International Conference on World Wide Web, pp. 597-608 (2014)
7. Gill, P., Erramilli, V., Chaintreau, A., Krishnamurthy, B., Papagiannaki, K., Rodriguez, P.: Best paper - follow the money: understanding economics of online aggregation and advertising. In: Proceedings of the 2013 Conference on Internet Measurement Conference, IMC 2013, pp. 141-148 (2013)
8. Mayer, J.R., Mitchell, J.C.: Third-party web tracking: policy and technology. In: 2012 IEEE Symposium on Security and Privacy (SP), pp. 413-427 (2012)
9. Castelluccia, C., Kaafar, M.-A., Tran, M.-D.: Betrayed by your ads!. In: Fischer-Hubner, S., Wright, M. (eds.) PETS 2012. LNCS, vol. 7384, pp. 1-17. Springer, Heidelberg (2012)
10. Datta, A., Tschantz, M.C., Datta, A.: Automated experiments on ad privacy settings. Proc. Priv. Enhanc. Technol. 2015(1), 92-112 (2015)
11. Google chrome adblock plus. <https://chrome.google.com/webstore/detail/adblock-plus/cfhdojbkjhnklbpkdaibdcddlifddb/support?hl=en-GB>
12. Pujol, E., Hohlfeld, O., Feldmann, A.: Annoyed users: ads and ad-block usage in the wild. In: Proceedings of the 2015 ACM Conference on Internet Measurement Conference, pp. 93-106 (2015)

13. Apostolis Zarras, Alexandros Kapravelos, Gianluca Stringhini, Thorsten Holz, Christopher Kruegel, and Giovanni Vigna. The Dark Alleys of Madison Avenue: Understanding Malicious Advertisements. In Proceedings of the 2014 Conference on Internet Measurement Conference (IMC '14). ACM, New York, NY, USA, 373-380 (2014) <https://doi.org/10.1145/2663716.2663719>
14. Digital advertising in Europe - Statistics and Facts (2017) <https://www.statista.com/topics/3983/digital-advertising-in-europe/>
15. Online advertising revenue in major online advertising markets in 2017 (2017) <https://www.statista.com/statistics/246570/largest-online-advertising-markets/>
16. PageFair: 2017 Adblock Report (2017) <https://pagefair.com/blog/2017/adblockreport/>
17. Desktop Ad Blocking Continues Unexpected Decline in Germany (2016) <https://www.emarketer.com/Article/Desktop-Ad-Blocking-Continues-Unexpected-Decline-Germany/1014768?mod=djemCMOToday>
18. The cost of ad blocking: PageFair and Adobe report (2015) https://downloads.pagefair.com/wp-content/uploads/2016/05/2015_report-the_cost_of_ad_blocking.pdf
19. EasyList. <https://easylist.to/easylist/easylist.txt>
20. EasyPrivacy. <https://easylist.to/easylist/easyprivacy.txt>
21. Filter Lists. <https://filterlists.com/>
22. Matching filters through Adblock Plus. <https://adblockplus.org/filters#anchors>
23. 9% of Popular Websites Use Anti Ad-block Scripts (2018) <https://www.bleepingcomputer.com/news/technology/9-percent-of-popular-websites-use-anti-adblock-scripts/>
24. Shitong Zhu, Xunchao Hu, Zhiyun Qian, Zubair Shafiq and Heng Yin. Measuring and Disrupting Anti Ad-blockers Using Differential Execution Analysis (2017)
25. Kiran Garimella, Orestis Kostakis, and Michael Mathioudakis. Ad-blocking: A Study on Performance, Privacy and Counter-measures. In Proceedings of the 2017 ACM on Web Science Conference (WebSci '17). ACM, New York, NY, USA, 259-262 (2017) <https://doi.org/10.1145/3091478.3091514>
26. Zhonghao Yu, Sam Macbeth, Konark Modi, and Josep M Pujol. Tracking the Trackers. 121-132 (2016)
27. Anti Adblock Killer List. <https://raw.githubusercontent.com/reek/anti-adblock-killer/master/anti-adblock-killer-filters.txt>
28. Anti Ad-block Killer <https://reek.github.io/anti-adblock-killer/>
29. Acceptable Ads Criteria <https://acceptableads.com/en/about/criteria>
30. European Commission's letter to privacy campaigner Alexander Hanff <https://twitter.com/alexanderhanff/status/722861362607747072>
31. Article 5.3 of the European Union's ePrivacy Directive (2002) <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0058>
32. Adblock Plus: Werbeblocker bleiben in Deutschland legal (2017) <https://www.wired.de/collection/business/gerichtsurteil-adblock-plus-verlage>
33. What Axel Springer's loss in ad-blocking suit means for UK publishers (2016) <https://digiday.com/uk/axel-springers-loss-ad-blocking-suit-means-uk-publishers/>
34. Adblock Plus and (a little) more (2016) <https://adblockplus.org/blog/it-s-still-perfectly-legal-to-block-ads-in-germany-after-latest-court-victory-over-spiegel>

35. Urteil des Landgerichts Hamburg (Az. 315 O 293/15) (2016) <http://www.landesrecht-hamburg.de/jportal/portal/page/bsharpprod.psml?showdoccase=1&doc.id=JURE170021729&st=ent>
36. Principal Country of Most Popular Websites according to Alexa https://en.wikipedia.org/wiki/List_of_most_popular_websites#List_of_websites
37. Selenium Chrome Webdriver <https://github.com/SeleniumHQ/selenium/wiki/ChromeDriver>
38. A/B Testing https://en.wikipedia.org/wiki/A/B_testing
39. Reek Github issues <https://github.com/reek/anti-adblock-killer/issues>
40. Weka Machine Learning Toolkit <https://www.cs.waikato.ac.nz/ml/weka/>