# 初窥竞品

* 1. CCleaner

Healther Check-》隐私，内含有Cookie、临时Internet文件、历史记录

设置-》智能清理-》浏览器清理；

或者自动义清理-》windwos，应用程序；

* 1. 360国内版

算的上的只有痕迹清理

Cookie

注册表

痕迹信息

* 1. Privacy Reviver Premium

Cookie

历史记录

* 1. 360国际版

隐私返追踪 只支持IE、chorme、firefox、Opera、YandeX

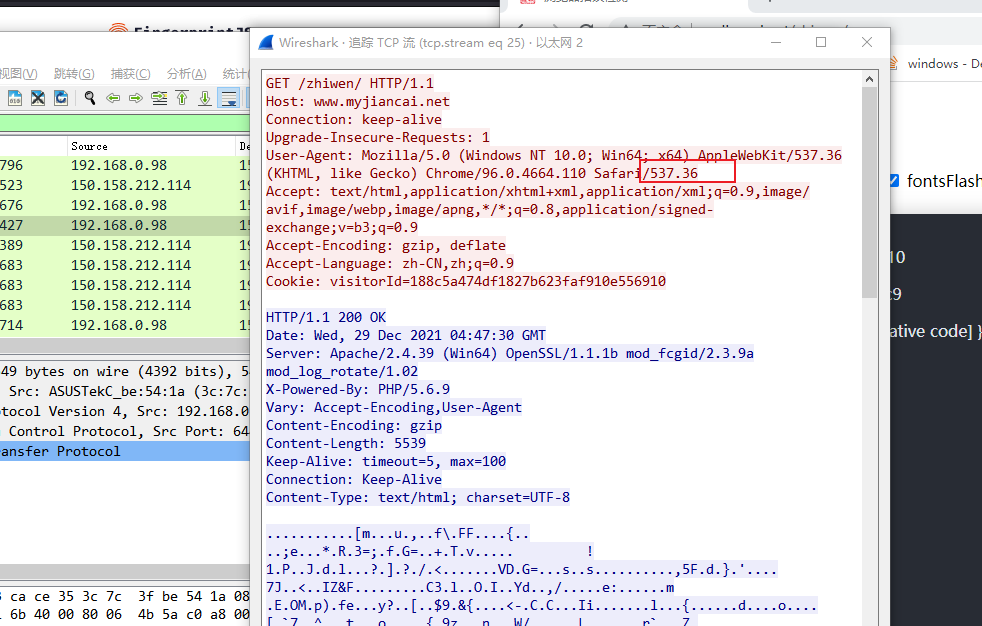
* 1. Avast AntiTrack

1反跟踪功能 DNT功能？ 未使用DNT

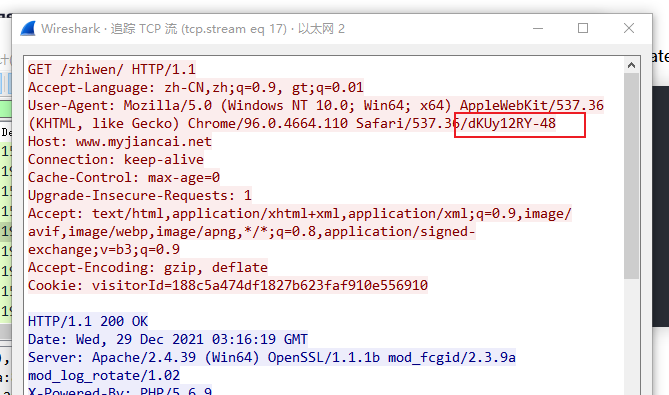
2浏览器保护 插件实现 控制指纹是否启用 如果启用userAgent和

pugin信息会发生改变

未启动浏览器保护：



启动浏览器保护：



3浏览器清理

4白名单

5系统隐私防止系统和程序收集和分享计算机上的操作，如手写痕迹。驱动？

保护特定数据？

提高登陆安全性？在系统输入框中加入保护字符串？

6更改浏览器指纹，提示规则

7报告

Ie、edg自带禁止跟踪请求DNT实现

实测对比相比于360要弱很多，比如同一网页会计算多次（可能多次触发）、同一网页偶尔不显示（可能bug，间隔快一小时不给与提示。插件中内容拦截正常，与app通讯异常）

### Firefox增强跟踪保护拦截什么

* + 1. 社交媒体跟踪器
    2. 跨网站跟踪性 cookie（也会隔离其他 cookie）
    3. 挖矿器
    4. 内容跟踪器：这些跟踪器隐藏在广告、视频和其他页面内容里。在 **标准** 模式下，这些跟踪器在隐私窗口被拦截。要在所有窗口添加这个保护，请访问隐私首选项并选择 **严格** 或 **定制**。

Firefox 默认屏蔽在 [Disconnect](https://disconnect.me/trackerprotection) 提供的列表中的已知跟踪器

卖点：

想要更多针对 Facebook 的保护？ 其他网站上的 Facebook 赞和分享按钮允许 Facebook 跟踪你的浏览行为（即使你从未点击过它们）。要想从这些按钮中去除跟踪器，你可以安装 [Facebook Container 附加组件](https://support.mozilla.org/zh-CN/kb/Facebook %E5%AE%B9%E5%99%A8%EF%BC%9A%E9%98%B2%E6%AD%A2 Facebook %E5%9C%A8%E5%85%B6%E4%BB%96%E7%BD%91%E7%AB%99%E4%B8%8A%E8%B7%9F%E8%B8%AA%E4%BD%A0)。

# 涉及技术

## DNT

Do Not Track（简称 DNT，中文叫"请勿追踪"）

## 浏览器指纹

* + 1. userAgent变更：

之前：

userAgent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36 Edg/96.0.1054.62

之后：

userAgent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36 Edg/96.0.1054.62/FO3zVDhf-51

* + 1. pugin信息会发生改变：

之前：

plugins : PDF Viewer,Portable Document Format,application/pdf,pdf,text/pdf,pdf,Chrome PDF Viewer,Portable Document Format,application/pdf,pdf,text/pdf,pdf,Chromium PDF Viewer,Portable Document Format,application/pdf,pdf,text/pdf,pdf,Microsoft Edge PDF Viewer,Portable Document Format,application/pdf,pdf,text/pdf,pdf,WebKit built-in PDF,Portable Document Format,application/pdf,pdf,text/pdf,pdf

之后：

plugins : Microsoft Edge PDF Viewer,Portable Document Format,application/pdf,pdf,,,,,,,WebKit built-in PDF,Portable Document Format,application/pdf,pdf,,,,,,,RafWebPlugin,rafwebplugin.dll,,,,,,,,,PDF Viewer,Portable Document Format,application/pdf,pdf,,,,,,,VT AudioPlayback,vtaudioplayback.dll,,,,,,,,,SpecialPlayer,specialplayer.dll,,,,,,,,,Chromium PDF Viewer,Portable Document Format,application/pdf,pdf,,,,,,,Chrome PDF Viewer,Portable Document Format,application/pdf,pdf,,,,,,,ChanWebPlugin,chanwebplugin.dll,,,,,,,,

## 浏览器信息清理

"浏览历史"

网址的历史

下载的历史

页面缓存

各种Cookies

## 跟踪保护

* + 1. Cookie
       1. Http Cookie
       2. Flash Cookie
    2. ETag

在chrome中注册监听

eg：

chrome.webRequest.onBeforeSendHeaders.addListener(onBeforeSendHeaders, {'urls': ['\*://\*/\*', 'ws://\*/\*', 'wss://\*/\*']}, ['blocking', 'requestHeaders']);

## 储备知识点

**一、技术层面**

1. Paper

* 雅虎研究院的[publication](http://labs.yahoo.com/areas/?areas=computational-advertising&section=publication" \t "https://blog.csdn.net/niushuai666/article/details/_blank)。

**二、业务层面**

1. 精准广告定向

* 一篇[总结](http://www.iamniu.com/2012/05/26/summary-internet-precise-ad-targeting-technology/?hmsr=top main content&hmmd=&hmpl=&hmkw=&hmci=" \t "https://blog.csdn.net/niushuai666/article/details/_blank)，该文介绍了User-Agent、Cookie、各种定向技术和网络广告反作弊，并侧重在业务介绍。该文博主的[首页](http://www.iamniu.com/" \t "https://blog.csdn.net/niushuai666/article/details/_blank)。

2. 在线展示广告

* 在线展示广告的[进化](http://wayinwayout.com/%E5%9C%A8%E7%BA%BF%E5%B1%95%E7%A4%BA%E5%B9%BF%E5%91%8A%E7%9A%84%E8%BF%9B%E5%8C%96-evolution-online-display-advertising/" \t "https://blog.csdn.net/niushuai666/article/details/_blank)，从Ad network谈到Ad Exchange（RTB）。

**三、技术课程**

1. 刘鹏老师的[计算广告学](http://study.163.com/course/courseMain.htm?courseId=321007" \l "/courseMain" \t "https://blog.csdn.net/niushuai666/article/details/_blank)（video）
2. 斯坦福大学的[计算广告学](https://www.stanford.edu/class/msande239/" \t "https://blog.csdn.net/niushuai666/article/details/_blank)（slide）
3. 百度的[计算广告学](http://guanggaoxue.csdn.net/module/zone/baidu_data/index" \l "video_course" \t "https://blog.csdn.net/niushuai666/article/details/_blank)（video）
4. 百度在清华大学开的[计算广告学](http://ctech.baidu.com/?r=courses/content&c_id=203&qq-pf-to=pcqq.c2c" \t "https://blog.csdn.net/niushuai666/article/details/_blank)（slide）

在广告定向设定中，浏览器定向和操作系统定向均是针对User-Agent中的信息进行定向。

**驻留技术**

　　通过各种属性生成的指纹需要长期保存,防止被用户删除,或者可恢复,这就需要驻留技术,驻留技术比较成熟的是evercookie.其存储cookie的思路从以下几个方面

标准HTTP Cookie

Flash本地共享对象

Silverlight隔离存储

CSS历史

将cookie存储在HTTP ETag中（需要后端服务器）

将cookie存储在Web缓存中（需要后端服务器）

window.name缓存

Internet Explorer userData存储

HTML5会话存储

HTML5本地存储

HTML5全球存储

通过SQLite的HTML5数据库存储

HTML5画布 - 将Cookie值存储在自动生成的RGB数据中,强制缓存PNG图像（需要后端服务器）

HTML5 IndexedDB

Java JNLP 持久化服务

Java漏洞利用CVE-2013-0422 - 尝试将applet沙箱转储并将cookie数据直接写入用户的硬盘驱动器。

　　以上维度,不是所有浏览器都是支持,但是evercookie提供一个很好的支持.

**关于Flash Cookie**

FlashCookie是由FlashPlayer控制的客户端共享存储技术，鉴于目前Flash技术的普遍性，几乎所有的网站都采用，所以具有同Http Cookie一样的作用。在技术上，通过使用JavaScript与ActionScript可以将Http Cookie和Flash Cookie进行互通。

Flash cookie的优势在于：

1、跨浏览器

不管用户的计算机上安装了多少个浏览器或者浏览器的不同版本，使用Flash Cookie能够使所有的浏览器共用一个Cookie。

2、不易删除

所有的浏览器均提供了清除Http Cookie的快捷方式，但Flash Cookie并没有此种方式，并且其保存位置非常隐蔽，网民难以删除。

3、容量更大

Flash Cookie可以容纳最多100千字节的数据，而一个标准的HTTP Cookie只有4千字节。

**Cookie的数量**

1、大多数浏览器支持最大为 4096 字节的 Cookie。因此最好用 Cookie 来存储用户 ID 之类的标识符，用户的详细信息则通过用户 ID从数据库或其他数据源中读取。

2、浏览器还限制站点可以在用户计算机上存储的 Cookie 的数量。大多数浏览器只允许每个站点存储 20 个 Cookie；当存储更多 Cookie时，最旧的 Cookie 便会被丢弃。有些浏览器还会对它们将接受的来自所有站点的 Cookie 总数作出绝对限制，通常为 300 个。

**Cookie的失效时间**

1、浏览器的Cookie设置会决定是否保存Cookie数据。如果浏览器不允许Cookie保存，则关掉浏览器后，这些数据就消失。

2、如果浏览器允许保存Cookie，那么Cookie的时间由服务器的设置决定。Cookie有一个Expires（有效期）属性，这个属性决定了Cookie的保存时间，服务器可以通过设定Expires字段的数值，来改变Cookie的保存时间。如果不设置该属性，那么Cookie只在浏览网页期间有效，关闭浏览器，这些Cookie自动消失，绝大多数网站属于这种情况。通常情况下，Cookie包含Server、Expires、Name、value这几个字段，其中对服务器有用的只是Name和value字段，Expires等字段的内容仅仅是为了告诉浏览器如何处理这些Cookies。

国内主流浏览器[User-Agent](http://www.iamniu.com/2012/02/23/detailed-information-of-user-agent/)

* 1. 社交媒体跟踪器
  2. 跨网站跟踪 cookie
  3. 挖矿脚本
  4. 跟踪内容
  5. 指纹收集器

# 至少要会世界主流浏览器插件编写

**Google 不支持隐私**

**FireFox DNT 跟踪保护**

**Edge DNT 跟踪保护**

**IE DNT 跟踪保护**

# 盈利困难点

* 1. 如果用户登录了账号，跟踪保护起到的效果十分有限（主要看网站）；

# 实现思路

* 1. 反跟踪:
     1. 实现DNT;
     2. 禁用第三方cookie(需要白名单功能);
  2. 修改浏览器指纹:
     1. 修改user-agent;
     2. 修改pugin中数据;
  3. 隐私返追踪成功次数统计，通过获取浏览器指纹函数？