# IDS, NAT, and Online Privacy Management

DR KAMI VANIEA

## First the news…

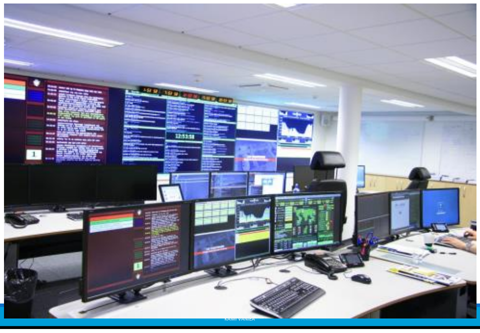
## Tutorials/Labs

- New times!
  - Monday 12-1pm,
  - Tuesday: 9am-10am
  - Wed: 11am-12pm
  - Fri: 10am-11am
- All in Forest Hill 3.D01

## Today

- Intrusion Detection Systems (IDS)
- Network Address Translation (NAT)
- Data leakage on the web
  - Why it matters
  - What it looks like
  - How to protect yourself

# Intrusion Detection Systems (IDS)



## Firewalls are preventative, IDS detects a potential incident in progress

- At some point you have to let some traffic into and out of your network (otherwise users get upset)
- Most security incidents are caused by a user letting something into the network that is malicious, or by being an insider threat themselves
- These cannot be prevented or anticipated in advance
- The next step is to identify that something bad is happening quickly so you can address it

## Signature based

- Perform simple pattern matching and report situations that match the pattern
- Requires that admin anticipate attack patterns in advance
- Attacker may test attack on common signatures
- Impossible to detect a new type of attack
- High accuracy, low false positives

## Heuristic based

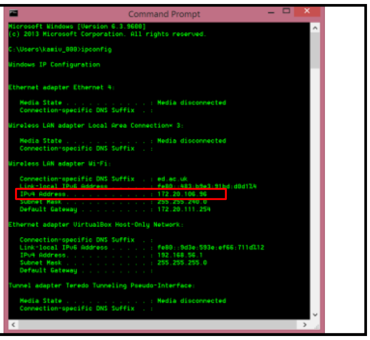
- Dynamically build a model of acceptable or “normal” behavior and flag anything that does not match
- Admin does not need to anticipate potential attacks
- System needs time to warm up to new behavior
- Can detect new types of attacks
- Higher false positives, lower accuracy

## Number of alarms is a big problem

- In the Target breach the IDS did correctly identify that there was an attack on the Target network
- There were too many alarms going off to investigate all of them in great depth
- Some cyberattack insurance policies state that if you know about an attack and do nothing they will not cover the attack.
- Having a noisy IDS can potentially be a liability

# Network Address Translation (NAT)

## Looking at the IP address of my laptop which is connected to the University WIFI.



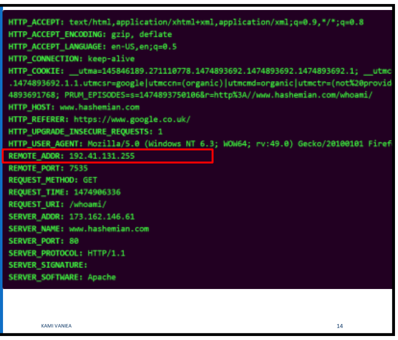
```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kamiv_000>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 4:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : ed.ac.uk
   Link-local IPv6 Address . . . . . : fe80::483:b9e3:91bd:d0d1%4
   IPv4 Address. . . . . . . . . . . : 172.20.106.96
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 172.20.111.254

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::9d3e:593e:ef66:711d%12
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

## My computer as seen from a remote server

(http://www.hashemian.com/whoami/)

My IP previously showed as: 172.20.106.96

What happened?



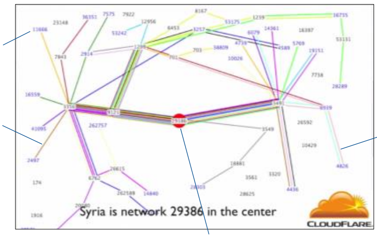
```
HTTP_ACCEPT: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
HTTP_ACCEPT_ENCODING: gzip, deflate
HTTP_ACCEPT_LANGUAGE: en-US,en;q=0.5
HTTP_CONNECTION: keep-alive
HTTP_COOKIE: __utma=145846189.271110778.1474893692.1474893692.1474893692.1; __utmc
.1474893692.1.1.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provid
4893691768; PRUM_EPISODES=s=1474893750106&r=http%3A//www.hashemian.com/whoami/
HTTP_HOST: www.hashemian.com
HTTP_REFERER: https://www.google.co.uk/
HTTP_UPGRADE_INSECURE_REQUESTS: 1
HTTP_USER_AGENT: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:49.0) Gecko/20100101 Firef
REMOTE_ADDR: 192.41.131.255
REMOTE_PORT: 7535
REQUEST_METHOD: GET
REQUEST_TIME: 1474906336
REQUEST_URI: /whoami/
SERVER_ADDR: 173.162.146.61
SERVER_NAME: www.hashemian.com
SERVER_PORT: 80
SERVER_PROTOCOL: HTTP/1.1
SERVER_SIGNATURE:
SERVER_SOFTWARE: Apache
```

## IPv4 and address space exhaustion

- Version 4 of the Internet Protocol
  - 192.168.2.6
- There are less than 4.3 billion IPv4 addresses available
- We do not have enough addresses for every device on the planet
- Answer: Network Address Translation
  - Internal IP different than external IP
  - Border router maps between its own IP and the internal ones

Each number is an AS, which is a network run by a single group.

Each colored line is the current shortest path between two AS's. All lines on this graph connect Syria to other parts of the world.



Syria is network 29386 in the center

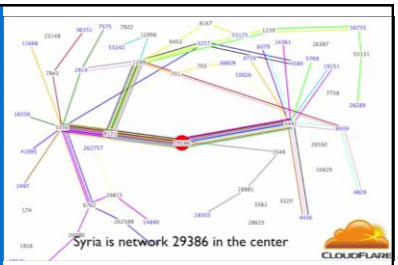
Paths shift all the time. This is normal on the internet as the current shortest path is dynamically negotiated (BGP routing).

Syria's AS is, directly connected to three other AS's.

Each number is an Autonomous System (AS)

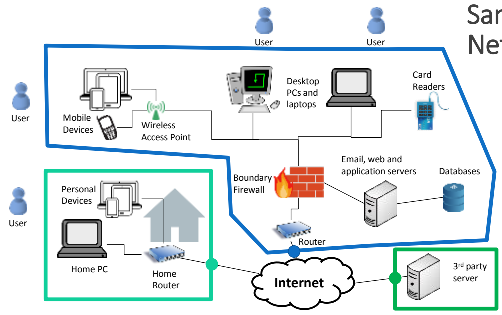
Each AS has the ability to manage its own IPs how it sees fit

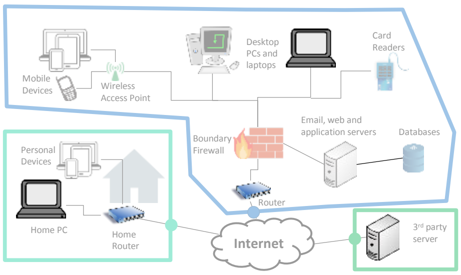
Each network has a similar ability

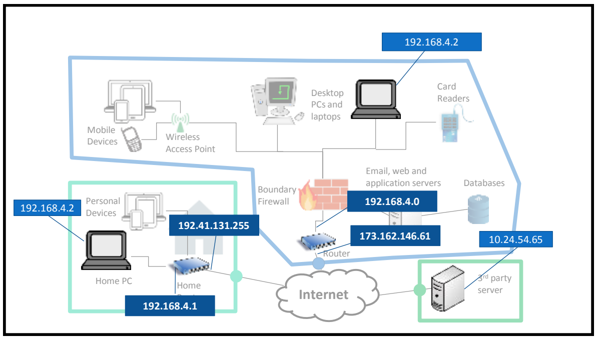


Syria is network 29386 in the center

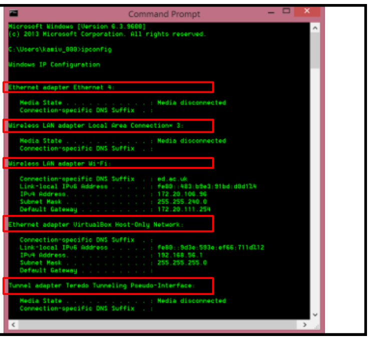
## Sample Network



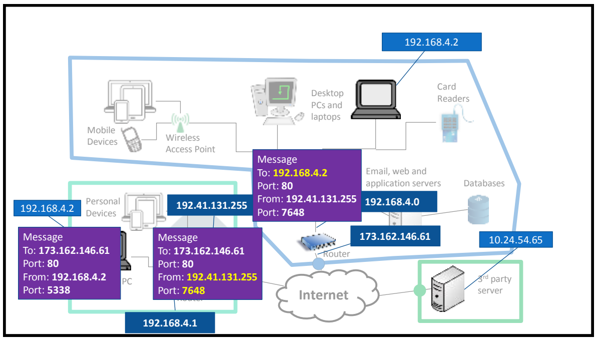




My laptop can have multiple IPs and bridge networks too. Here it shows IPs for both my VirtualBox and my WIF.



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kamiv_000>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 4:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : ed.ac.uk
   Link-local IPv6 Address . . . . . : fe80::483:b9e3:91bd:d0d124
   IPv4 Address. . . . . . . . . . . : 172.20.106.96
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 172.20.111.254

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::9d3e:593e:ef66:711d%12
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```



Message
To: 192.168.4.2
Port: 80
From: 192.41.131.255
Port: 7648

Message
To: 173.162.146.61
Port: 80
From: 192.168.4.2
Port: 5338

Message
To: 173.162.146.61
Port: 80
From: 192.41.131.255
Port: 7648

# Online Privacy Management

**The following is copied from talks I give groups like lawyers, policy makers, and the general public about privacy protections.**

**I have added some extra technical details, but these are the kinds of issues they worry about.**

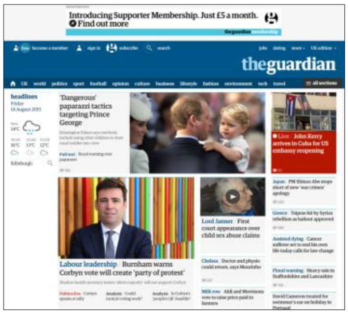
## Firefox add-ons

- The following set of screenshots were created using these addons. These are all safe to download and use from home.
  - Tilt
  - uMatrix
  - Ghostery
  - Lightbeam
  - Firebug
  - Built-in Firefox developer tools

# Web pages are built dynamically

Websites are made up of many elements from many sources

Lets take a look at how The Guardian's website is built dynamically



Introducing Supporter Membership. Just £5 a month.
Find out more

'Dangerous' paparazzi tactics targeting Prince George

Live John Kerry arrives in Cuba for US embassy reopening

Japan PM Shinzo Abe stops short of new 'war crimes' apology

Greece Tsipras hit by Syriza rebellion as bailout approved

Lord Janner First court appearance over child sex abuse claims

Assisted dying Cancer sufferer set to end his own life today calls for law change

Labour leadership Burnham warns Corbyn vote will create 'party of protest'

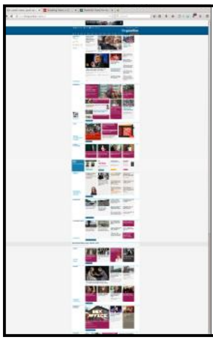
Chelsea Doctor and physio could return, says Mourinho

Flood warning Heavy rain in Staffordshire and Lancashire

Milk row Aldi and Morrisons vow to raise price paid to farmers

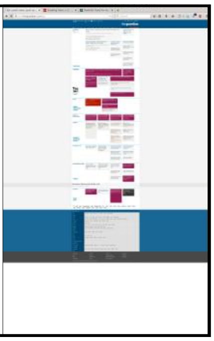
David Cameron treated for swimmer's ear on holiday in Portugal

Zoomed out…



**Loading all content**

Only loading content from theguardian.com



## The Guardian: content sources

- guim.co.uk
- ophan.co.uk
- revsci.net
- guardianapps.co.uk
- scorecardresearch.com
- googleadservices.com
- doubleclick.net
- imrworldwide.com
- krxd.net
- google.com
- google.co.uk
- d935jy3y59lth.cloudfront.net
- rubiconproject.com
- dqwufkbc3sdtr.cloudfront.net
- d1mbyzj6lih1pj.cloudfront.net
- googlesyndication.com
- googletagservices.com
- adnxs.com
- moatads.com

## The Telegraph: content sources

- optimizely.com
- d3c3cq33003psk.cloudfront.net
- quantserve.com
- ooyala.com
- google.com
- criteo.com
- parsely.com
- visualrevenue.com
- googletagservices.com
- effectivemeasure.net
- demdex.net
- outbrain.com
- youtube.com
- ytimg.com
- omtrdc.net
- akamaihd.net

- scorecardresearch.com
- doubleclick.net
- disqus.com
- skimresources.com
- qubitproducts.com
- serving-sys.com
- googlesyndication.com
- moatads.com
- adsafeprotected.com
- imrworldwide.com
- opta.net
- twitter.com
- vdna-assets.com
- mediavoice.com
- krxd.net
- msn.com
- bing.com

- t.co
- visualdna.com
- facebook.net
- polarmobile.com
- matheranalytics.com
- facebook.com
- chartbeat.com
- d3ujids68p6xmq.cloudfront.net
- pagefair.com
- pagefair.net
- ml314.com
- linkedin.com
- chartbeat.net
- clarifyingquack.com
- flappysquid.net
- mathtag.com
- rlcdn.com

## The Guardian: content sources

- guim.co.uk
- ophan.co.uk
- revsci.net
- guardianapps.co.uk
- scorecardresearch.com
- googleadservices.com
- doubleclick.net
- imrworldwide.com
- krxd.net

- google.com
- google.co.uk
- d935jy3y59lth.cloudfront.net
- rubiconproject.com
- dqwufkbc3sdtr.cloudfront.net
- d1mbyzj6lih1pj.cloudfront.net
- googlesyndication.com
- googletagservices.com
- adnxs.com
- moatads.com

## The Guardian: content sources

**Content Delivery**
- guim.co.uk
- guardianapps.co.uk
- d935jy3y59lth.cloudfront.net
- dqwufkbc3sdtr.cloudfront.net
- d1mbyzj6lih1pj.cloudfront.net

**Trackers / Other**
- scorecardresearch.com
- rubiconproject.com
- adnxs.com
- moatads.com
- revsci.net
- imrworldwide.com
- krxd.net
- doubleclick.net
- google.com
- google.co.uk
- googleadservices.com
- googletagservices.com
- googlesyndication.com
- ophan.co.uk

**Javascript**

✓ theguardian.com

✓ Guardian owned

✓ Others

**Content**

✓ theguardian.com

✓ Guardian owned

✓ Others

**Javascript**

✗ theguardian.com

✗ Guardian owned

✗ Others

**Content**

✓ theguardian.com

✗ Guardian owned

✗ Others

**Javascript**

✓ theguardian.com

✗ Guardian owned

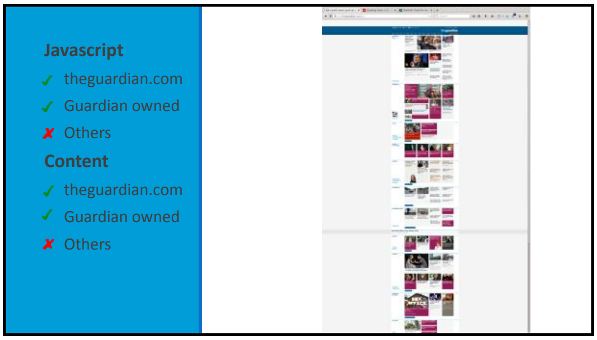
✗ Others

**Content**

✓ theguardian.com

✗ Guardian owned

✗ Others

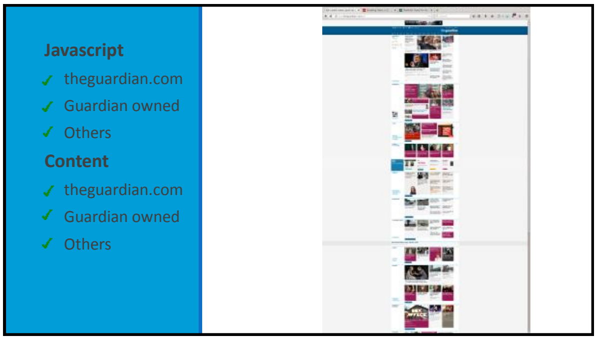


**Javascript**

- ✓ theguardian.com
- ✓ Guardian owned
- ✘ Others

**Content**

- ✓ theguardian.com
- ✓ Guardian owned
- ✘ Others

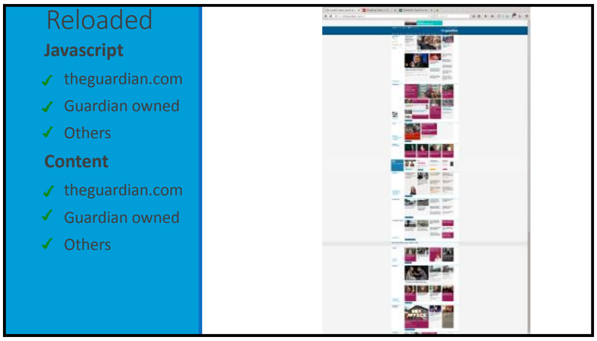


**Javascript**

- ✓ theguardian.com
- ✓ Guardian owned
- ✓ Others

**Content**

- ✓ theguardian.com
- ✓ Guardian owned
- ✓ Others



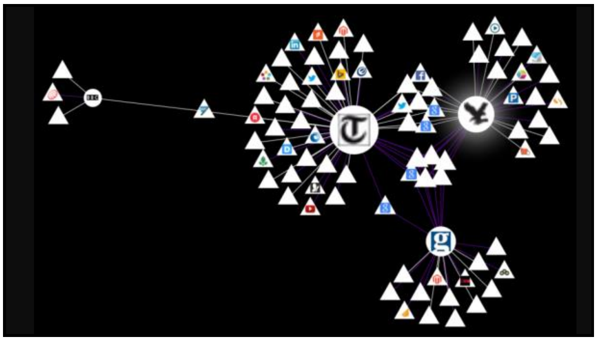
Reloaded

**Javascript**

- ✓ theguardian.com
- ✓ Guardian owned
- ✓ Others

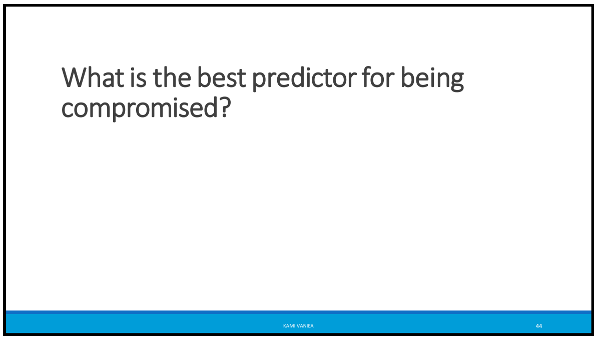
**Content**

- ✓ theguardian.com
- ✓ Guardian owned
- ✓ Others



**Who cares?**

KAMI VANIEA 43



What is the best predictor for being compromised?

KAMI VANIEA 44

The Washington Post

The Switch

## Thousands of visitors to yahoo.com hit with malware attack, researchers say

"Malicious payloads were being delivered to around **300,000 users per hour**. The company guesses that around **9 percent of those, or 27,000 users per hour**, were being infected."

https://www.washingtonpost.com/blogs/the-switch/wp/2014/01/04/thousands-of-visitors-to-yahoo-com-hit-with-malware-attack-researchers-say

The Washington Post

The Switch

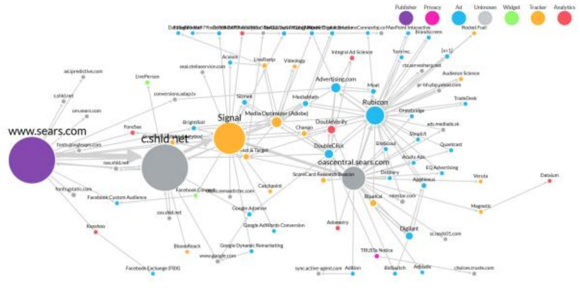
## Thousands of visitors to yahoo.com hit with malware attack, researchers say

"Clients visiting yahoo.com received advertisements served by **ads.yahoo.com**. Some of the advertisements are malicious … Instead of serving ordinary ads, the Yahoo's servers reportedly sends users an 'exploit kit.'"

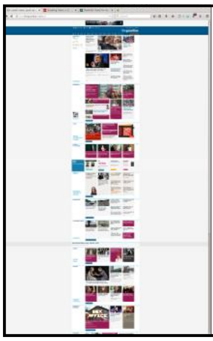
https://www.washingtonpost.com/blogs/the-switch/wp/2014/01/04/thousands-of-visitors-to-yahoo-com-hit-with-malware-attack-researchers-say

**"Ya, but website owners are careful about the content they present to users… I can trust big websites."**

KAMI VANIEA 48



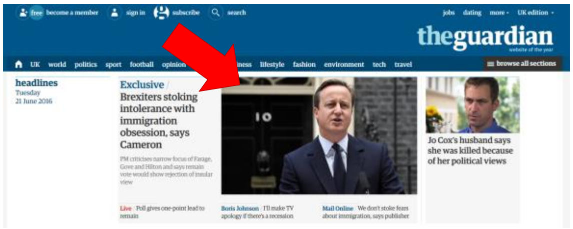
https://app.ghosteryenterprise.com/TM/RIIV26



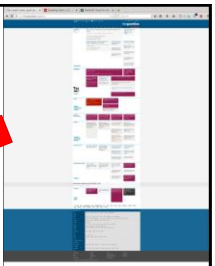
**Loading all content**

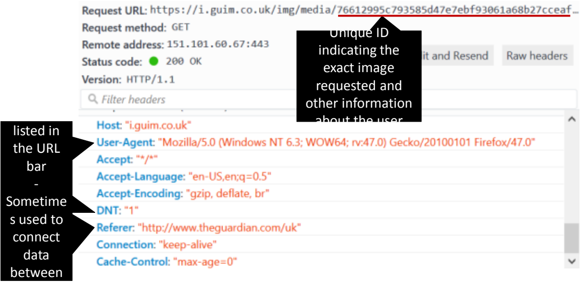
Only loading content from theguardian.com

```
<html>
<body>
   Hello World!
   <img src="http://example.com/img5.jpg"/>
   <script src="http://example.com/script.js"/>
</body>
</html>
```


free become a member
sign in
subscribe
search
jobs dating more UK edition
theguardian
website of the year
UK world politics sport football opinion
lifestyle fashion environment tech travel
browse all sections
headlines
Tuesday 21 June 2016
Exclusive Brexiters stoking intolerance with immigration obsession, says Cameron
Jo Cox's husband says she was killed because of her political views
Live Poll gives one-point lead to remain
Boris Johnson I'll make TV apology if there's a recession
Mail Online We don't stoke fears about immigration, says publisher

```
<html>
<body>
   Hello World!
   <img src="http://example.com/img5.jpg"/>
   <script src="http://example.com/script.js"/>
</body>
</html>
```



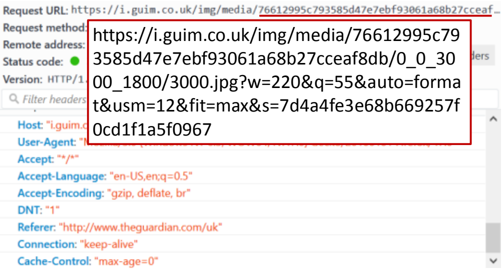


Request URL: https://i.guim.co.uk/img/media/76612995c793585d47e7ebf93061a68b27cceaf…
Request method: GET
Remote address: 151.101.60.67:443
Status code: ● 200 OK
Version: HTTP/1.1

Host: "i.guim.co.uk"
User-Agent: "Mozilla/5.0 (Windows NT 6.3; WOW64; rv:47.0) Gecko/20100101 Firefox/47.0"
Accept: "*/*"
Accept-Language: "en-US,en;q=0.5"
Accept-Encoding: "gzip, deflate, br"
DNT: "1"
Referer: "http://www.theguardian.com/uk"
Connection: "keep-alive"
Cache-Control: "max-age=0"

Unique ID indicating the exact image requested and other information about the user

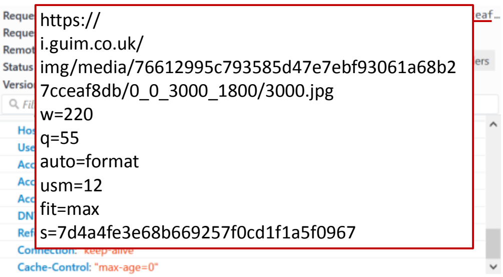
listed in the URL bar - Sometimes used to connect data between



Request URL: https://i.guim.co.uk/img/media/76612995c793585d47e7ebf93061a68b27cceaf…
Request method:
Remote address:
Status code: ●
Version: HTTP/1.

https://i.guim.co.uk/img/media/76612995c793585d47e7ebf93061a68b27cceaf8db/0_0_3000_1800/3000.jpg?w=220&q=55&auto=format&usm=12&fit=max&s=7d4a4fe3e68b669257f0cd1f1a5f0967

Host: "i.guim.c
User-Agent: "
Accept: "*/*"
Accept-Language: "en-US,en;q=0.5"
Accept-Encoding: "gzip, deflate, br"
DNT: "1"
Referer: "http://www.theguardian.com/uk"
Connection: "keep-alive"
Cache-Control: "max-age=0"

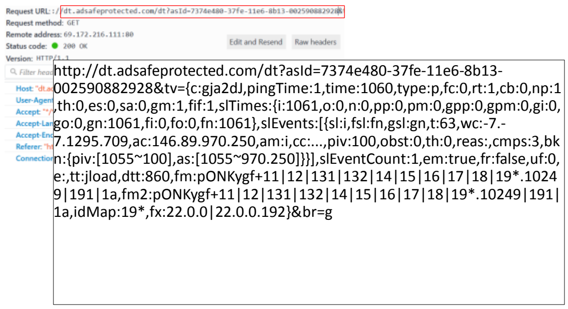


https://
i.guim.co.uk/
img/media/76612995c793585d47e7ebf93061a68b27cceaf8db/0_0_3000_1800/3000.jpg
w=220
q=55
auto=format
usm=12
fit=max
s=7d4a4fe3e68b669257f0cd1f1a5f0967

Cache-Control: "max-age=0"

```
GET
   http://b.scorecardresearch.com/b?c1=1&c2=3000007&c3=&c4=3000007&c5=010201&c6=The%20Daily%20Show%20With%20Jon%20
   Stewart--
   122&c13=CF2919C8FAC2632F49751F9063A81473&c14=PC&c15=07d2d1f87461cf1fbd708c7539cbc028&c16=0&ca1=3&ca2=3000007
   &ca3=66809&ca4=515223&ca5=Comedy&cb1=3&cb2=&cb3=66809&cb4=515223_03&cb5=the-daily-show-with-jon-
   stewart&rn=1434947801124_794 HTTP/1.1

Host: b.scorecardresearch.com

User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

DNT: 1

Referer: http://www.hulu.com/site-player/300561/playerwrapper.swf

Cookie: UID=17523a67a60a1291c75f1b21434510914; UIDR=1434510914

Connection: keep-alive
```

```
<html>
<body>
   Hello World!
   <img src="http://example.com/img5.jpg"/>
   <script src="http://example.com/script.js"/>
</body>
</html>
```



Request URL: ://dt.adsafeprotected.com/dt?asId=7374e480-37fe-11e6-8b13-002590882928&

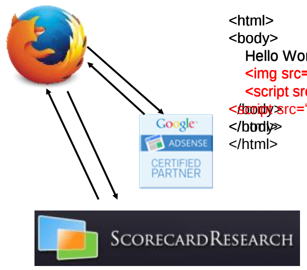
Request method: GET

Remote address: 69.172.216.111:80

Status code: ● 200 OK

Version: HTTP/1.1

http://dt.adsafeprotected.com/dt?asId=7374e480-37fe-11e6-8b13-002590882928&tv={c:gja2dJ,pingTime:1,time:1060,type:p,fc:0,rt:1,cb:0,np:1,th:0,es:0,sa:0,gm:1,fif:1,slTimes:{i:1061,o:0,n:0,pp:0,pm:0,gpp:0,gpm:0,gi:0,go:0,gn:1061,fi:0,fo:0,fn:1061},slEvents:[{sl:i,fsl:fn,gsl:gn,t:63,wc:-7.-7.1295.709,ac:146.89.970.250,am:i,cc:...,piv:100,obst:0,th:0,reas:,cmps:3,bkn:{piv:[1055~100],as:[1055~970.250]}}],slEventCount:1,em:true,fr:false,uf:0,e:,tt:jload,dtt:860,fm:pONKygf+11|12|131|132|14|15|16|17|18|19*.10249|191|1a,fm2:pONKygf+11|12|131|132|14|15|16|17|18|19*.10249|191|1a,idMap:19*,fx:22.0.0|22.0.0.192}&br=g



```
<html>
<body>
   Hello World!
   <img src="http://example.com/img5.jpg"/>
   <script src="http://adsense.com/script.js"/>
</body>
<script src="http://scorecardresearch.com/sr.js"/>
</html>
</body>
</html>
```

## Questions