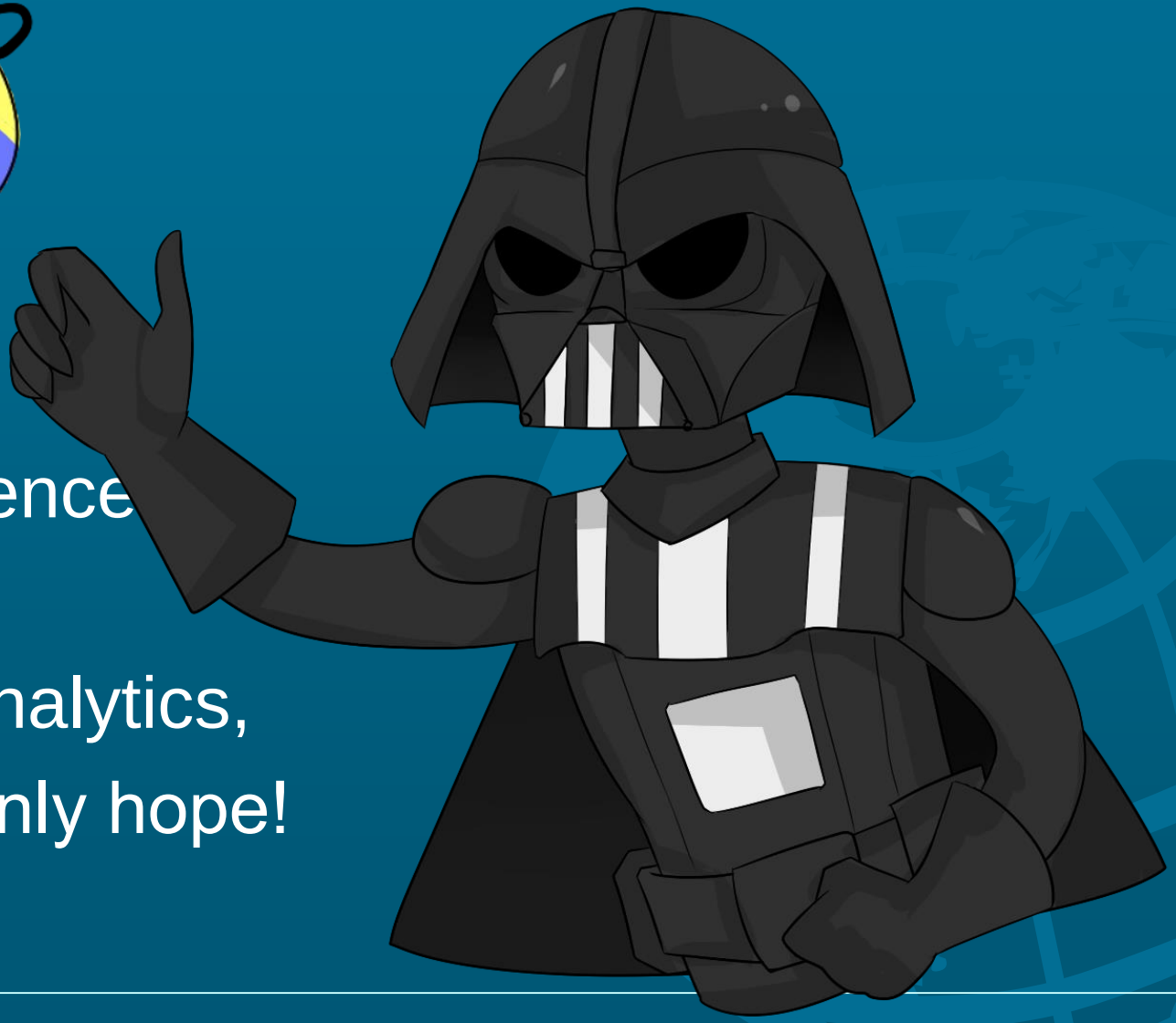
SuperSize Your Internet Timeline

with Google Analytics

Another Forensics Blog

az4n6.blogspot.com

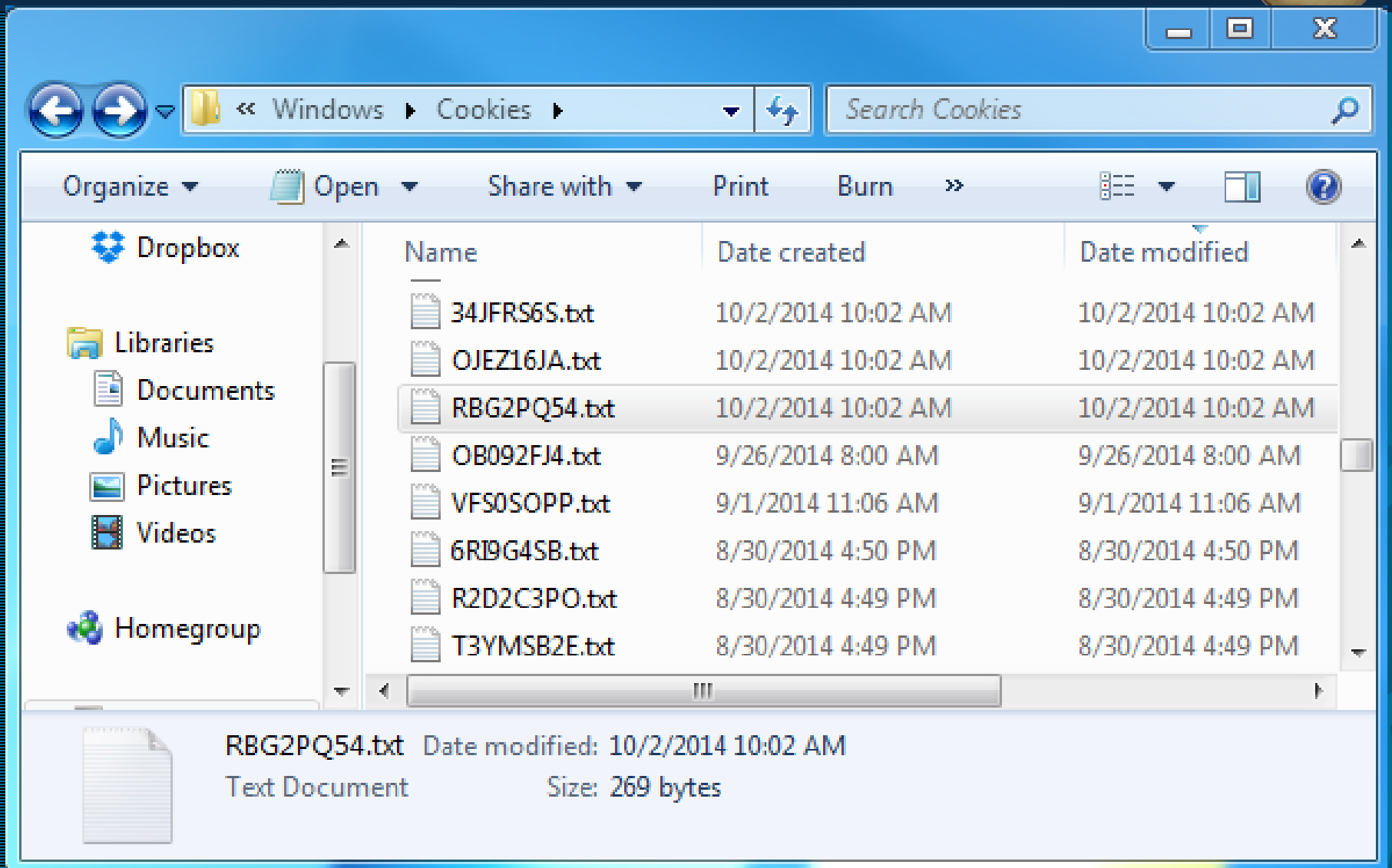
Why should you care?



- Find evidence
- Google Analytics, you’re my only hope!

Three Sources

IE Cookie


« Windows ▸ Cookies ▸
Search Cookies
Organize
Open
Share with
Print
Burn
Dropbox
Libraries
Documents
Music
Pictures
Videos
Homegroup
Name
Date created
Date modified
34JFRS6S.txt 10/2/2014 10:02 AM 10/2/2014 10:02 AM
OJEZ16JA.txt 10/2/2014 10:02 AM 10/2/2014 10:02 AM
RBG2PQ54.txt 10/2/2014 10:02 AM 10/2/2014 10:02 AM
OB092FJ4.txt 9/26/2014 8:00 AM 9/26/2014 8:00 AM
VFS0SOPP.txt 9/1/2014 11:06 AM 9/1/2014 11:06 AM
6RI9G4SB.txt 8/30/2014 4:50 PM 8/30/2014 4:50 PM
R2D2C3PO.txt 8/30/2014 4:49 PM 8/30/2014 4:49 PM
T3YMSB2E.txt 8/30/2014 4:49 PM 8/30/2014 4:49 PM
RBG2PQ54.txt Date modified: 10/2/2014 10:02 AM
Text Document Size: 269 bytes

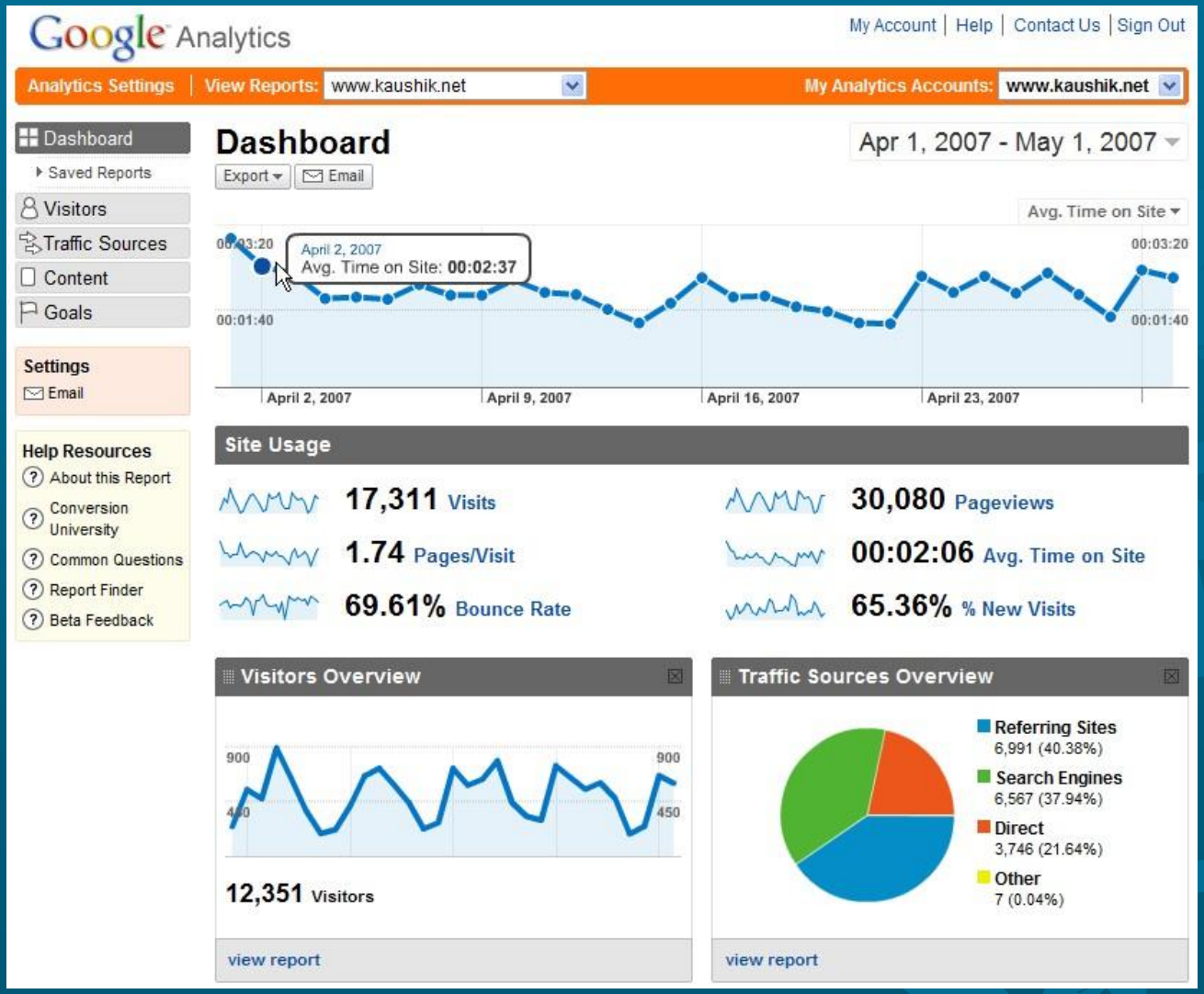
IE Cookie

```
1  WT_FPC
2  id=2c395695eea83e635188306873392836:lv=1385094034083:ss=1385094034083
3  microsoft.com/
4  1024
5  3888600320
6  31071080
```

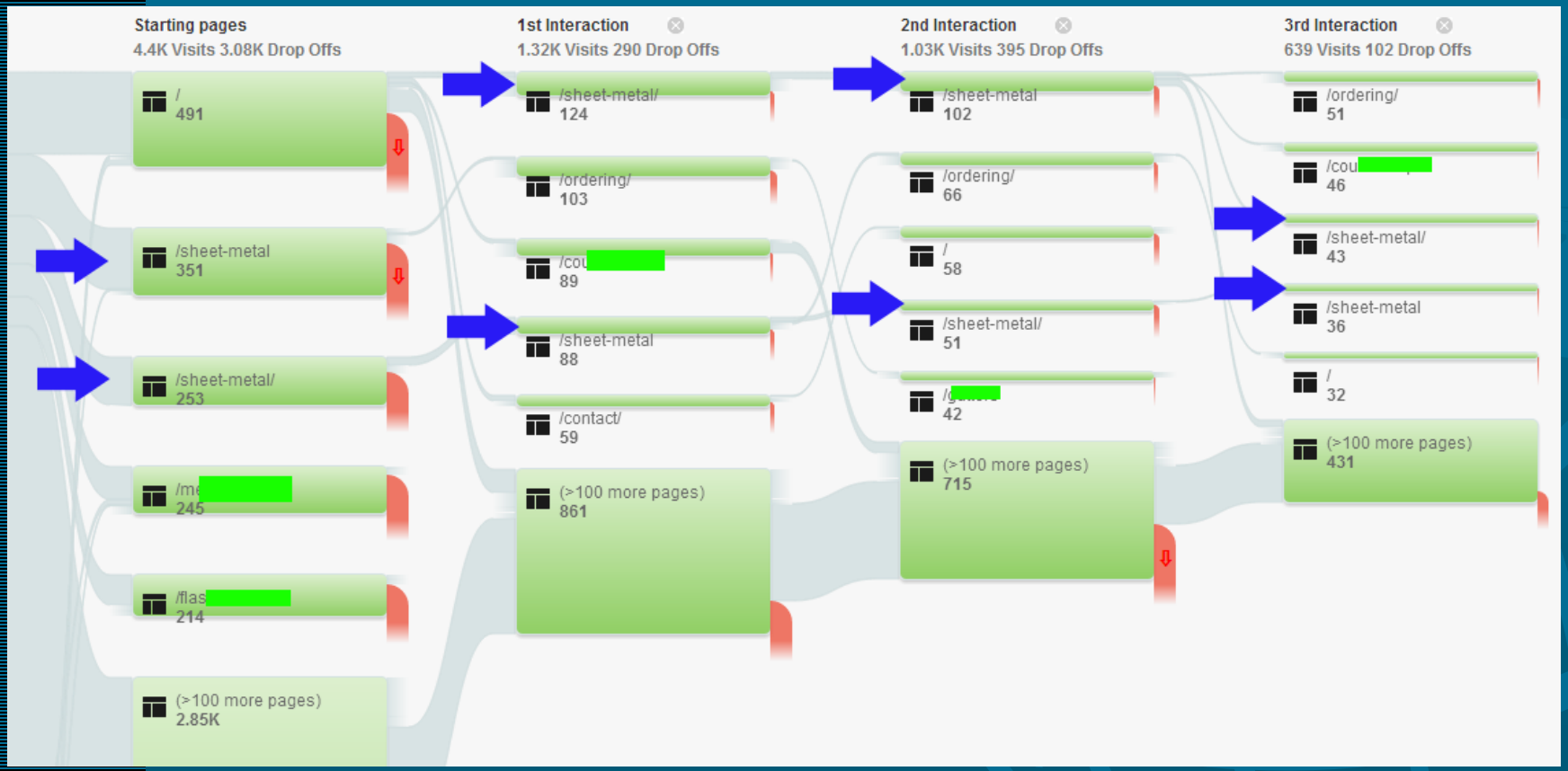
Type		Last Visited [UTC]	Last Visited [Local]	Hits	User	URL	Host
cookie	☐	10/26/2013 10:32:03 PM Sat	10/26/2013 3:32:03 PM Sat	1513	administrator	Cookie:administrator@adnxs.com/	adnxs.com
cookie	☐	10/26/2013 10:32:03 PM Sat	10/26/2013 3:32:03 PM Sat	150	administrator	Cookie:administrator@openx.net/	openx.net
cookie	☐	10/26/2013 10:32:04 PM Sat	10/26/2013 3:32:04 PM Sat	34	administrator	Cookie:administrator@pointroll.com/	pointroll.com
cookie	☐	10/26/2013 10:32:04 PM Sat	10/26/2013 3:32:04 PM Sat	170	administrator	Cookie:administrator@ads.pointroll.com/	ads.pointroll.com
cookie	☐	10/26/2013 10:32:15 PM Sat	10/26/2013 3:32:15 PM Sat	285	administrator	Cookie:administrator@tribalfusion.com/	tribalfusion.com
cookie	☐	10/26/2013 10:32:33 PM Sat	10/26/2013 3:32:33 PM Sat	404	administrator	Cookie:administrator@pubmatic.com/	pubmatic.com

```
17 30332812
18 *
19 A
20 I&I=AxUFAAAAAAC1CQAAtd985NlH9L85BG6vEPmPSw!!&V=4
21 microsoft.com/
22 1024
23 2652160384
24 30479671
25 1245742060
26 30332812
27 *
```

What is GA?


Google Analytics
My Account | Help | Contact Us | Sign Out
Analytics Settings | View Reports: www.kaushik.net
My Analytics Accounts: www.kaushik.net
Dashboard
Saved Reports
Visitors
Traffic Sources
Content
Goals
Settings
Email
Help Resources
About this Report
Conversion University
Common Questions
Report Finder
Beta Feedback
Dashboard
Export
Email
Apr 1, 2007 - May 1, 2007
Avg. Time on Site
00:03:20
April 2, 2007
Avg. Time on Site: 00:02:37
00:01:40
April 2, 2007
April 9, 2007
April 16, 2007
April 23, 2007
Site Usage
17,311 Visits
30,080 Pageviews
1.74 Pages/Visit
00:02:06 Avg. Time on Site
69.61% Bounce Rate
65.36% % New Visits
Visitors Overview
900
450
12,351 Visitors
view report
Traffic Sources Overview
Referring Sites
6,991 (40.38%)
Search Engines
6,567 (37.94%)
Direct
3,746 (21.64%)
Other
7 (0.04%)
view report

Behavior Flow



GA Process


<a href="/de/Die-Welt-verstehen/360_C2_BO-GE
dung der Vorwoche um (...)

<div class="header header_3" title="360° - GEO Re
<div style="position:absolute;top:0px;left:0px;hei
<a href="http://plus7.arte.tv/de/streamin
Sendung verp
<img src="/i18n/content/tv/02_Univer
08.12.21/fr/arte_2B7.jpg/2384230,templatefreeabed.p


ON THE INTERNET
NOBODY KNOWS YOU'RE A DOG


KA-POW!

GA Cookie


```
1  __utma
2  226104841.611228744.1387124603.1387126762.1387132234.3
3  bitwiseforensics.com/
4  1088
5  3713353088
6  30488422
7  3956575207
8  30341571
9  *
10 __utmz
11 226104841.1387132234.3.3.utmcsr=bing|utmccn=(organic)|utmcmd=organic|utmctr=tucson%20forensics
12 bitwiseforensics.com/
13 1088
14 2821399936
15 30378284
16 3956385196
17 30341571
18 *
19
20 __utmb
21 226104841.12.10.1387132234
22 bitwiseforensics.com/
23 1088
24 480901504
25 30341576
26 3956585207
27 30341571
28 *
29
```

Created

2nd Most Recent Visit

Most Recent Visit

Session # (Hits)

Most Recent Visit

Source

Keywords

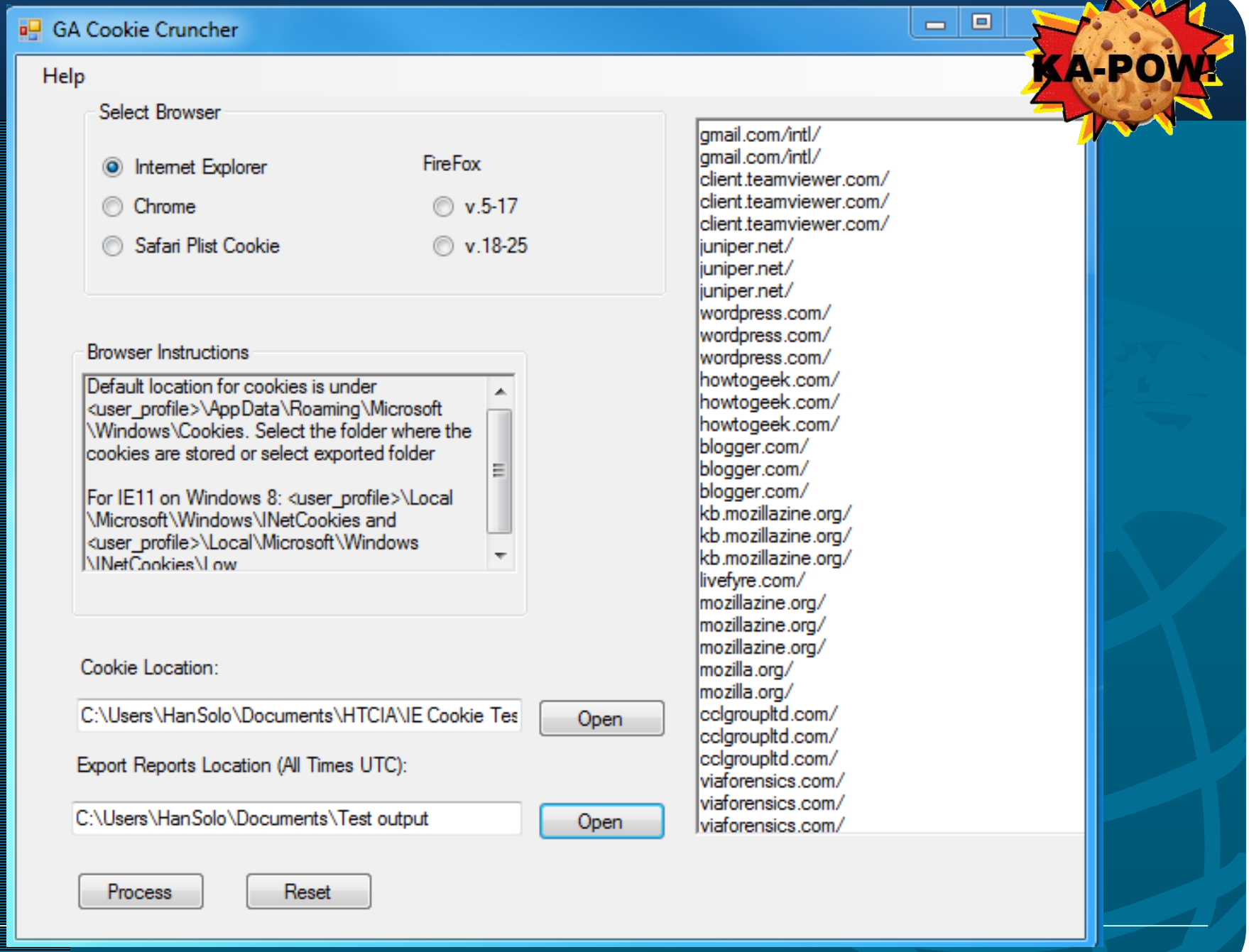
Pageviews

Time of session

Cookie vs Ga Cookie

- 1 Date
- Host Name
- Hit Count

- 3 Dates
- Host Name
- Hit Count/Page View
- Source
- Keyword
- Referring Page


GA Cookie Cruncher
KA-POW!
Help
Select Browser
Internet Explorer
Chrome
Safari Plist Cookie
FireFox
v.5-17
v.18-25
Browser Instructions
Default location for cookies is under <user_profile>\AppData\Roaming\Microsoft\Windows\Cookies. Select the folder where the cookies are stored or select exported folder
For IE11 on Windows 8: <user_profile>\Local\Microsoft\Windows\INetCookies and <user_profile>\Local\Microsoft\Windows\INetCookies\Low
Cookie Location:
C:\Users\HanSolo\Documents\HTCIA\IE Cookie Tes
Open
Export Reports Location (All Times UTC):
C:\Users\HanSolo\Documents\Test output
Open
Process
Reset
gmail.com/intl/
gmail.com/intl/
client.teamviewer.com/
client.teamviewer.com/
client.teamviewer.com/
juniper.net/
juniper.net/
juniper.net/
wordpress.com/
wordpress.com/
wordpress.com/
howtogeek.com/
howtogeek.com/
howtogeek.com/
blogger.com/
blogger.com/
blogger.com/
kb.mozillazine.org/
kb.mozillazine.org/
kb.mozillazine.org/
livefyre.com/
mozillazine.org/
mozillazine.org/
mozillazine.org/
mozilla.org/
mozilla.org/
cclgroupltd.com/
cclgroupltd.com/
cclgroupltd.com/
viaforensics.com/
viaforensics.com/
viaforensics.com/

Output utma

Host	Cookie Creation Time	2nd Most Recent	Most Recent Visit	Hits
.reddit.com	10/18/2013 3:59	12/14/2013 6:24	12/14/2013 15:48	164
imgur.com	10/18/2013 3:59	12/14/2013 6:25	12/14/2013 15:49	148
.twitter.com	8/19/2013 5:33	12/14/2013 19:57	12/14/2013 20:05	76
.stipple.com	10/18/2013 4:23	12/14/2013 7:27	12/14/2013 15:49	74
.lastpass.com	8/18/2013 2:13	12/13/2013 4:17	12/14/2013 20:05	63
.blogger.com	8/18/2013 14:13	12/14/2013 21:31	12/14/2013 21:41	63
.stackoverflow.com	10/16/2013 17:22	12/13/2013 5:35	12/13/2013 17:13	19
.elfster.com	12/3/2013 2:05	12/6/2013 5:01	12/6/2013 7:28	10
.code.google.com	11/7/2013 14:45	12/12/2013 18:02	12/12/2013 22:43	9

Output utmb

Host	Page Views	Outbound Links	Start Current Session
.dfinews.com	1	10	12/14/2013 21:42
.blogger.com	4	10	12/14/2013 21:41
.forensicfocus.com	1	10	12/14/2013 21:57
.nirsoft.net	2	10	12/14/2013 21:58

Output utmz

Host	Last Update	Source	Keyword
.yorkphoto.com	12/11/2013 17:15	google	cheap%20photo%20prints

Google

Cheap photo prints

yorkphoto.com

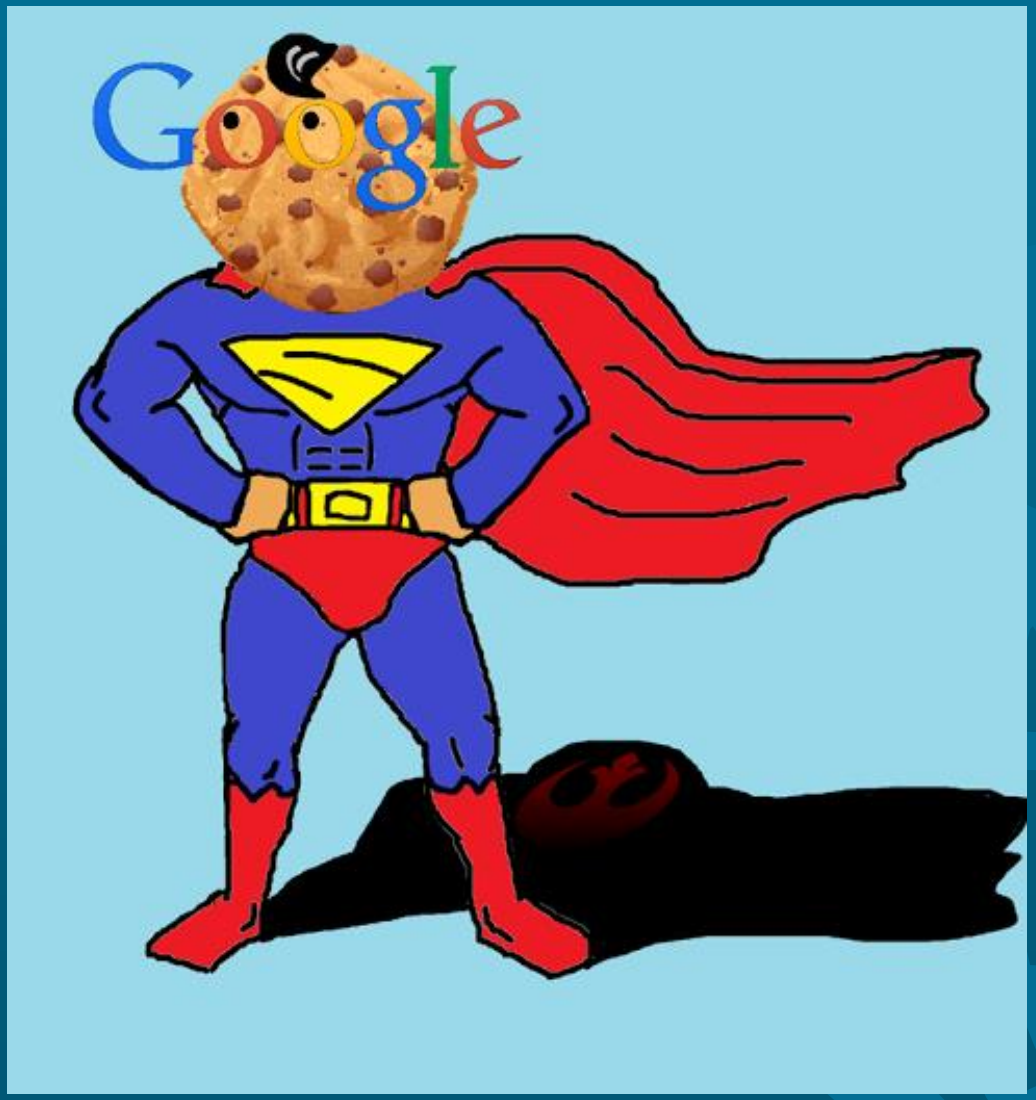
Host	Last Update	Source	Keyword	ReferringPage
.secureworks.com	5/7/2014 10:16	windowsir.blogspot.com	not found	/2014/05/new-stuff.html

Windowsir.blogspot.com

/2014/05/new-stuff.html

Secureworks.com

Elevate it even further



Carving


```
__utma
55650728.1836601702.1401669429.1401669429.1401669429.1
reddit.com/
1600
3125285376
30522269
3376106274
30375418
*
__utmb
55650728.2.9.1401669429
reddit.com/
1600
4187801088
30375422
3376116274
30375418
*
```

Scalpel.conf


```
#GOOGLE ARTIFACTS
#-------------------------------------
--

    txt y    1000      __utma   *
    txt y    1000      __utmb   *
    txt y    1000      __utmz   *

#
#-------------------------------------
```

GA-Parser

- GA-Parser.py –f filename –o directory --ie
- GA-Parser.py –d directory–o directory --ie
- --chrome, --firefox, --apple
- RAM
- Pagefile / Hiberfil.sys
- DD Image

Build out __utma

Host	Created	2nd Most Recent	Most Recent	Hits
.youtube.com	5/12/2013 6:40	7/6/2013 7:16	7/6/2013 19:18	28
.youtube.com	5/12/2013 6:40	7/13/2013 18:05	7/14/2013 21:39	30
.youtube.com	5/12/2013 6:40	8/11/2013 21:18	8/17/2013 6:03	32
.youtube.com	5/12/2013 6:40	9/13/2013 7:37	9/15/2013 9:07	39
.youtube.com	5/12/2013 6:40	9/15/2013 9:07	9/24/2013 6:43	40
.youtube.com	5/12/2013 6:40	9/29/2013 6:14	9/29/2013 8:01	44
.youtube.com	5/12/2013 6:40	10/3/2013 22:46	10/4/2013 0:41	66
.youtube.com	5/12/2013 6:40	10/4/2013 0:41	10/4/2013 6:23	65
.youtube.com	5/12/2013 6:40	10/8/2013 1:14	10/8/2013 5:52	72
.youtube.com	5/12/2013 6:40	10/8/2013 5:52	10/18/2013 6:18	98
.youtube.com	5/12/2013 6:40	10/18/2013 6:18	10/26/2013 10:31	136

Build out __utmb

Host	Page Views	Start Current Session
.youtube.com	15	7/6/2013 19:18
.youtube.com	30	7/14/2013 21:39
.youtube.com	30	8/17/2013 6:03
.youtube.com	30	9/15/2013 9:07
.youtube.com	96	9/24/2013 6:43
.youtube.com	24	9/29/2013 8:01
.youtube.com	296	10/4/2013 0:41
.youtube.com	2	10/4/2013 6:23
.youtube.com	51	10/8/2013 5:52
.youtube.com	51	10/18/2013 6:18
.youtube.com	299	10/26/2013 10:31

Build out __utmz

Host	Last Update	Keyword
.youtube.com	7/6/2013 19:18	NSFW Videos
.youtube.com	7/14/2013 21:39	Stuff to get me fired
.youtube.com	8/17/2013 6:03	Grumpy Cat
.youtube.com	9/15/2013 9:07	NSFW Videos
.youtube.com	9/24/2013 6:43	NSFW Videos
.youtube.com	9/29/2013 8:01	Best 2013 NSFW Videos
.youtube.com	10/4/2013 0:41	NDFW Vidoes
.youtube.com	10/4/2013 6:23	How to Embezzle
.youtube.com	10/8/2013 5:52	Really NSFW Videos
.youtube.com	10/18/2013 6:18	!!! Ewoks gone wild !!!
.youtube.com	10/26/2013 10:31	Really Really NSFW Videos

Combine

utma utma utmb utma utmz utmz

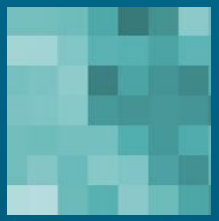
Host	Creation Time	2nd Most Recent	Most Recent	Page Views	Hits	Source	Keyword
.youtube.	5/12/2013 6:40	7/6/2013 7:16	7/6/2013 19:18	15	28	google	NSFW Videos
.youtube.	5/12/2013 6:40	7/13/2013 18:05	7/14/2013 21:39	30	30	google	Stuff to get me fired
.youtube.	5/12/2013 6:40	8/11/2013 21:18	8/17/2013 6:03	30	32	google	NSFW Videos
.youtube.	5/12/2013 6:40	9/13/2013 7:37	9/15/2013 9:07	30	39	google	NSFW Videos
.youtube.	5/12/2013 6:40	9/15/2013 9:07	9/24/2013 6:43	96	40	google	NSFW Videos
.youtube.	5/12/2013 6:40	9/29/2013 6:14	9/29/2013 8:01	24	44	google	Best 2013 NSFW Vidoes
.youtube.	5/12/2013 6:40	10/3/2013 22:46	10/4/2013 0:41	296	66	google	NSFW Vidoes
.youtube.	5/12/2013 6:40	10/4/2013 0:41	10/4/2013 6:23	2	65	google	How to Embezzle
.youtube.	5/12/2013 6:40	10/8/2013 1:14	10/8/2013 5:52	51	72	google	Really NSFW Videos
.youtube.	5/12/2013 6:40	10/8/2013 5:52	10/18/2013 6:18	51	98	google	NSFW Vidoes Gone Wild
.youtube.	5/12/2013 6:40	10/18/2013 6:18	10/26/2013 10:31	299	136	google	Really Really NSFW Vidoes

Cookie vs Ga Cookie

- 1 Date
- Host Name
- Hit Count

- Many Dates
- Host Name
- Hit Count/Page Views
- Source
- Keyword
- Referring Page

GA Process



Google

__utm.gif?

- http://www.google-analytics.com/__utm.gif?utmwv=5.4.3&utms=4&utmn=1046933378&utmhn=www.deviantart.com&utme=8(user-type)9(visitor)11(1)&utmcs=windows-1252&utmsr=1600x900&utmvp=1583x754&utmsc=24-bit&utmul=en-us&utmje=0&utmfl=11.7%20r700&utmdt=deviantART%20%3A%20Log%20In&utmhid=1021688701&utmr=0&utmp=%2Fusers%2Fwrongpassword%3Fusername%3Dmdegrazia%26ref%3Dhttp%25253A%25252F%25252Fwww.deviantart.com%25252F&utmht=1373048611329&utmac=UA-322734-1&utmcc=__utma%3D212885643.1758037532.1373048500.1373048500.1373048500.1%3B%2B__utmz%3D212885643.1373048500.1.1.utmcsr%3Dgoogle%7Cutmccn%3D(organic)%7Cutmcmd%3Dorganic%7Cutmctr%3D(not%2520provided)%3B&utmu=qR~

Cheat Sheet

Cheatography

Google Analytics UTM Parameters (v2) Cheat Sheet

by Jay Taylor (Jay Taylor) via cheatography.com/573/cs/254/

Hit / Campaign Parameters

utmac	Account ID *(e.g. UA-123456-1)*
utmcc	Analytics Cookie string
utmcn	New campaign visit?
utmcr	Repeat campaign visit?
utmdt	Page title
utmhn	Hostname
utmp	Page path
utmr	Full referral URL

utmcc contains the combined strings of the __utma and __utmz Google Analytics cookies. This string is URL encoded.

The **utmcn** and **utmcr** parameters never appear in the same request and both only appear with a value of '1'.

Environment Parameters

utmcs	Character set *(e.g. ISO-8859-1)*
utmfl	Flash version
utmip	IP address

e-Commerce Parameters (Transactions)

utmtci	Billing City
utmtco	Billing Country
utmtrg	Billing Region
utmtid	Order ID
utmtst	Affiliation / Store name
utmtsp	Shipping cost
utmtto	Order Total *(inc. tax and shipping)*
utmttx	Tax cost

The **utmtid** order ID must be unique for each order, otherwise Google Analytics will group multiple transactions under a single entry. All monetary fields should be filled in without a currency symbol, e.g.: **12.50**

e-Commerce Parameters (Items)

utmtid	Order ID
utmipc	Product code / SKU
utmipn	Product name
utmipr	Product price
utmiqt	Quantity

Social Parameters

utmsa	Social action (e.g. 'share', 'tweet')
utmsid	Social destination (optional)
utmsn	Social network name

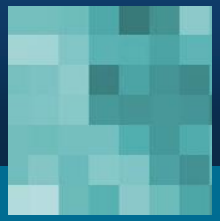
These values are sent by _trackSocial requests only.

Internal Parameters

utmhid	Hit ID, random number
utmn	Random ID to prevent gif caching
utms	Requests made this session (max. 500)
utmt	Request type (e.g. 'event', 'tran' etc...)
utmu	Client usage / Error data (encoded)
utmvid	Visitor ID
utmwv	Tracking code version
guid	Send Globally Unique Identifier

utms increments with each successive request made for the current session. After 500, hits will be ignored.

Manually Parsed



Host Title: www.deviantart.com

Page Title: deviantART : Log In

Page Request:
/users/wrongpassword?username=admackbar
&ref=http://www.deviantart.com

First Visit =7/5/2013 6:21:40 PM
Previous =7/5/2013 6:21:40 PM
Last Visit =7/5/2013 6:21:40 PM

Locations

C:\Users\%USERNAME%\AppData\Local\Mozilla\Firefox\Profiles\%RANDOM%.default\Cache

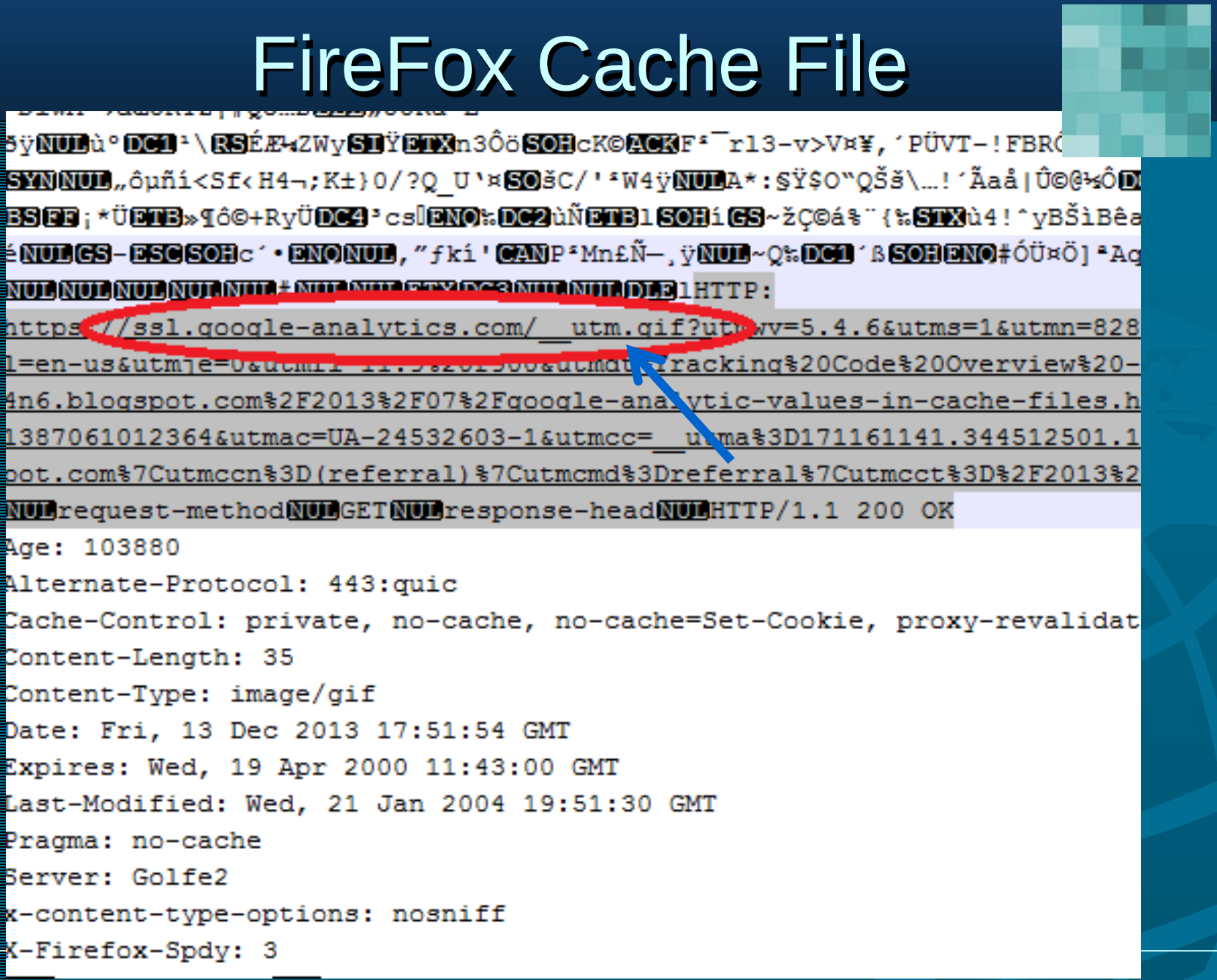
C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\Default\Cache

C:\Users\%USERNAME%\Library\Caches\com.apple.Safari\cache.db

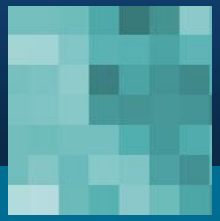
C:\Users\%USERNAME%\Local\Microsoft\Windows\WebCache\WebCacheV01.dat

Supersize it!

FireFox Cache File

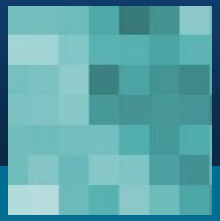


Scalpel.conf



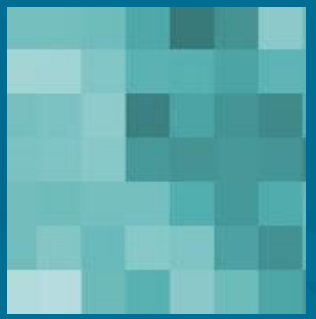
```
#-----------------------------------------------------------
#GOOGLE ARTIFACTS
#-----------------------------------------------------------

    txt y    1000     __utma   *
    txt y    1000     __utmb   *
    txt y    1000     __utmz   *

    cache    n    1000     google-analytics.com/__utm.gif?
#
#-----------------------------------------------------------
```

GA-Parser



- GA-Parser.py –f webcacheVD1.dat –o directory --gif
- GA-Parser.py –d “C:\path\exportedfiles” –o output --gif
- Ram
- Pagefile / Hiberfil.sys
- DD Image

Cookie vs (GA Cookie+Cache)

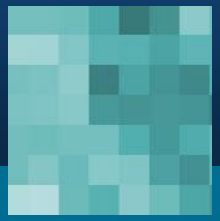


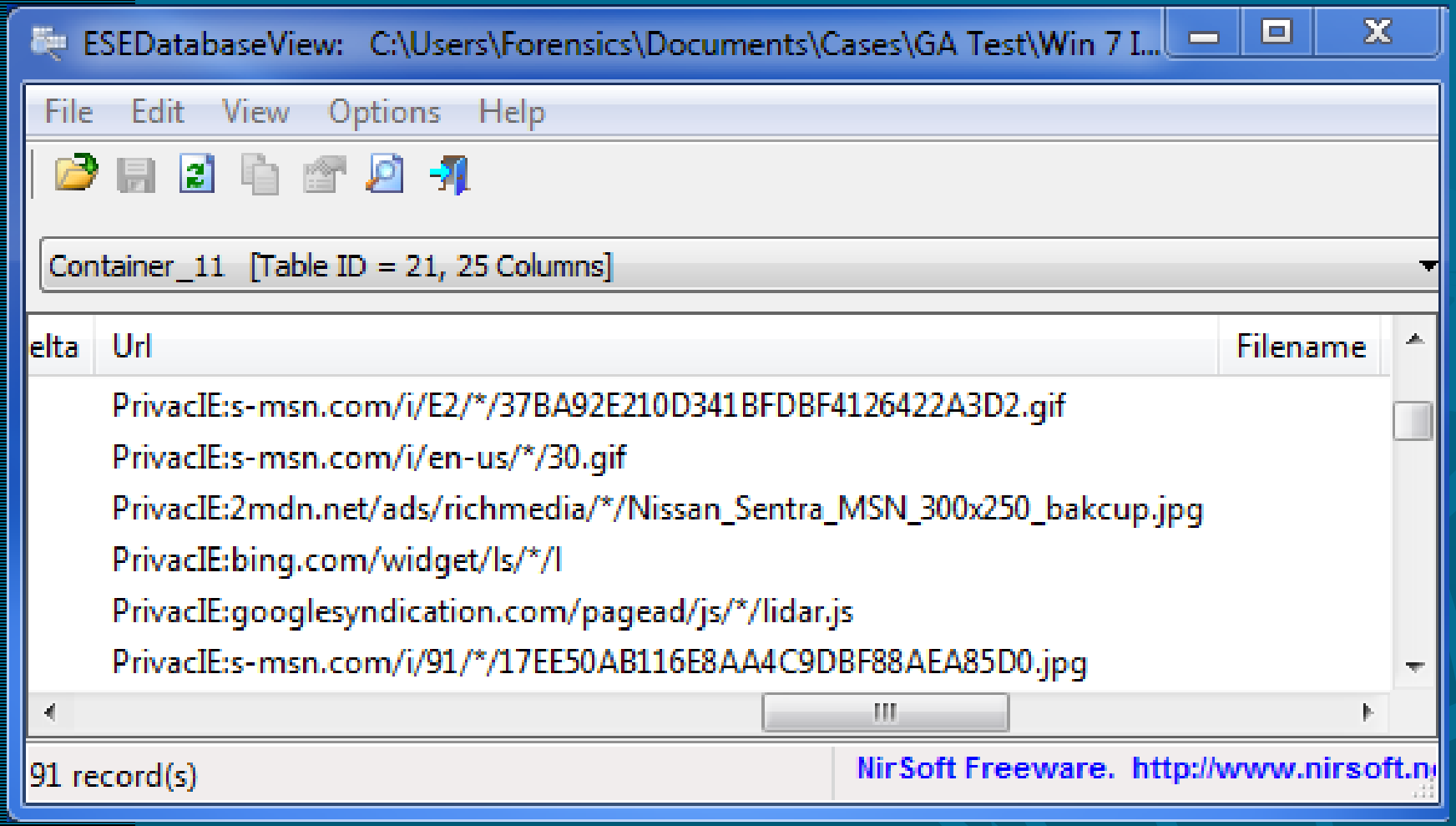
- 1 Date
- Host Name
- Hit Count

- Many Dates
- Host Name
- Hit Count
- Source
- Keyword
- Referring Page

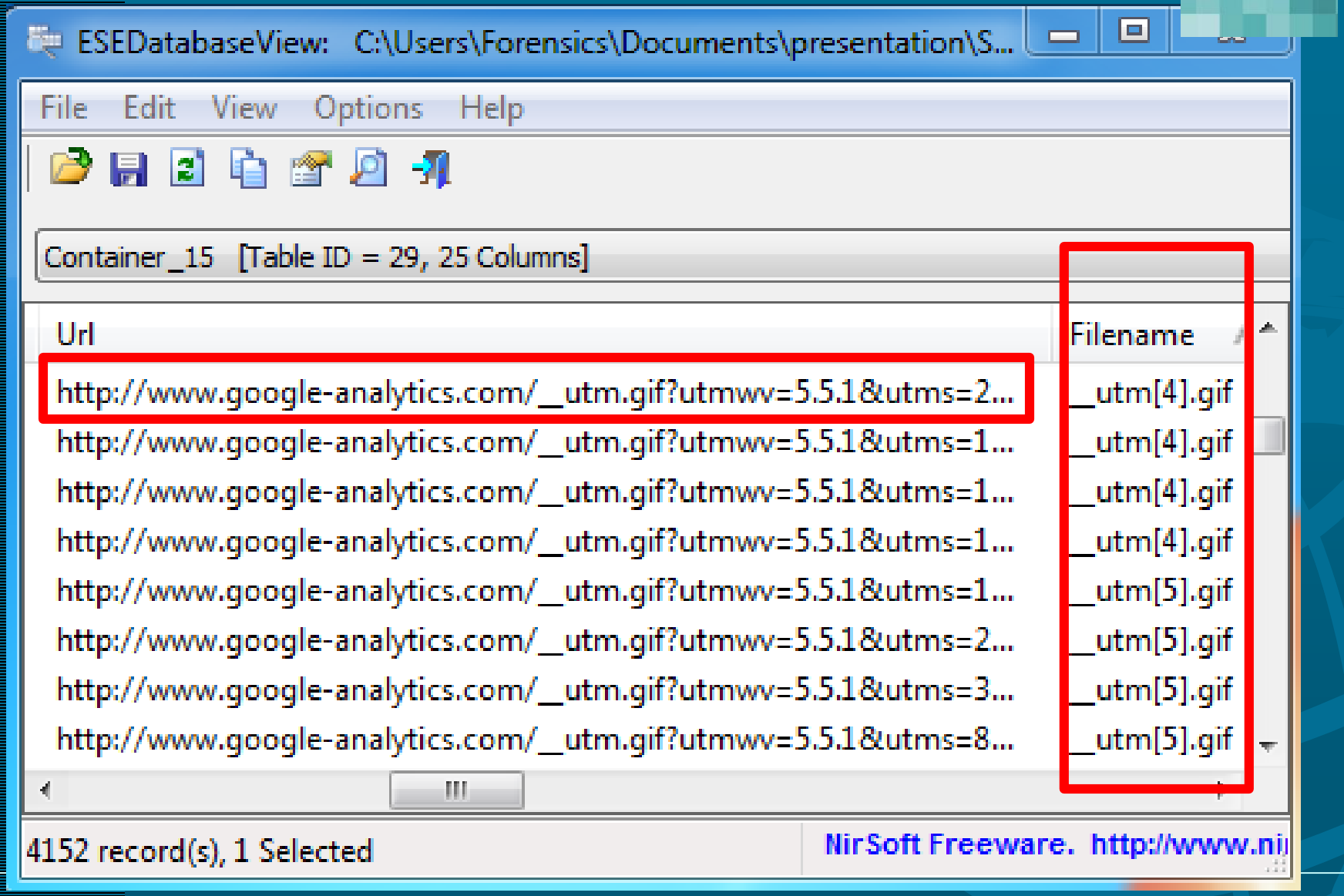
- GA Cookie
- Page Title
- Page Req
- Source
- Keyword

inPrivate




ESEDatabaseView: C:\Users\Forensics\Documents\Cases\GA Test\Win 7 I...
File Edit View Options Help
Container_11 [Table ID = 21, 25 Columns]
elta Url Filename
PrivacIE:s-msn.com/i/E2/*/37BA92E210D341BFDBF4126422A3D2.gif
PrivacIE:s-msn.com/i/en-us/*/30.gif
PrivacIE:2mdn.net/ads/richmedia/*/Nissan_Sentra_MSN_300x250_bakcup.jpg
PrivacIE:bing.com/widget/ls/*/l
PrivacIE:googlesyndication.com/pagead/js/*/lidar.js
PrivacIE:s-msn.com/i/91/*/17EE50AB116E8AA4C9DBF88AEA85D0.jpg
91 record(s)
NirSoft Freeware. http://www.nirsoft.n

InPrivate


ESEDatabaseView: C:\Users\Forensics\Documents\presentation\S...
File Edit View Options Help
Container_15 [Table ID = 29, 25 Columns]
Url
Filename
http://www.google-analytics.com/__utm.gif?utmwv=5.5.1&utms=2... __utm[4].gif
http://www.google-analytics.com/__utm.gif?utmwv=5.5.1&utms=1... __utm[4].gif
http://www.google-analytics.com/__utm.gif?utmwv=5.5.1&utms=1... __utm[4].gif
http://www.google-analytics.com/__utm.gif?utmwv=5.5.1&utms=1... __utm[4].gif
http://www.google-analytics.com/__utm.gif?utmwv=5.5.1&utms=1... __utm[5].gif
http://www.google-analytics.com/__utm.gif?utmwv=5.5.1&utms=2... __utm[5].gif
http://www.google-analytics.com/__utm.gif?utmwv=5.5.1&utms=3... __utm[5].gif
http://www.google-analytics.com/__utm.gif?utmwv=5.5.1&utms=8... __utm[5].gif
4152 record(s), 1 Selected
NirSoft Freeware. http://www.ni

Not So Private

http://a.abcnews.com/assets/images/navigation/weather/36.png

http://a.abcnews.com/assets/player/amp/common/bar.png

F	G	H	I	J	K
utma_last	utma_h	utmhn_hostname	udmt_page_title	utmp_page_request	tutmr_full_referral URL
6/2/2014 22:42	1	www.mysanantonio.com	NRA blasts Open Carry Texas after San Antonio inciden	/default/article/NRA-blasts-Open-C	http://www.reddit.com/r/news/
6/2/2014 22:42	1	abcnews.go.com	12-Year-Old Wisconsin Girls Charged in Stabbing - ABC	/US/wireStory/12-year-wisconsin-gi	http://www.reddit.com/r/news/
6/2/2014 22:42	1	bringmethenews.com	Charges: Neighbor pulls gun on dad teaching daughter	/2014/06/02/neighbor-pulls-gun-on	http://www.reddit.com/r/news/
6/2/2014 22:43	1	www.monroenews.com	Al Barron reinstated as Monroe Public Schools teacher	/news/2014/jun/01/al-barron-reins	http://www.reddit.com/r/news/
6/2/2014 22:43	1	www.rawstory.com	Virginia atheist couple: Court-appointed officiant told	/rs/2014/05/30/virginia-atheist-cou	http://www.reddit.com/r/news/
6/2/2014 22:44	1	www.wsbtv.com	Woman shoots at would-be home intruders | www.ws	/news/news/local/woman-shoots-v	http://www.reddit.com/r/news/
6/2/2014 22:44	1	www.kirotv.com	Seattle to get $15 minimum wage -- nation's highest | v	/news/news/seattle-city-coucil-ma	http://www.reddit.com/r/news/

Host Name: abcnews.go.com

Page Title: 12-Year-Old Wisconsin Girls Charged in Stabbing - ABC News

Request: /US/wireStory/12-year-wisconsin-girls-stab-friend-19-times-23959855

Hit Count : 1

Cell Phones

- Backups
- Cookies
- Cache
- Applications
- Unallocated

Three Sources

Summary

- Search __utm[abz] , __utm.gif?
- Export out relevant files
- Run Cookie Cruncher (logical cookies)
- Run GA-Parser (unallocated / kitchen sink)
- Build out Timeline (gray matter)

Questions

github.com/mdegrazia

http://az4n6.blogspot.com

arizona4n6@gmail.com

Twitter @maridegrazia