

Privacy Lost

Jonathan Fudem

Some Magic

* Wi-Fi: en0 [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
10	0.0003386000	10.0.7.23	239.255.255.250	SSDP	239	M-SEARCH * HTTP/1.1
20	0.011232000	10.0.6.137	239.255.255.250	SSDP	247	M-SEARCH * HTTP/1.1
118	0.070657000	10.0.10.158	239.255.255.250	SSDP	247	M-SEARCH * HTTP/1.1
187	0.106447000	10.0.7.23	239.255.255.250	SSDP	239	M-SEARCH * HTTP/1.1
190	0.113782000	10.0.4.167	239.255.255.250	SSDP	239	M-SEARCH * HTTP/1.1
262	0.222395000	10.0.45.38	239.255.255.250	SSDP	546	NOTIFY * HTTP/1.1
263	0.222755000	fe80::347f:96bb:5dfe:f26d	ff02::c	SSDP	577	NOTIFY * HTTP/1.1
273	0.229120000	10.0.32.95	239.255.255.250	SSDP	612	NOTIFY * HTTP/1.1
274	0.231625000	fe80::75f7:3ef6:f26c:5105	ff02::c	SSDP	639	NOTIFY * HTTP/1.1
277	0.232202000	10.0.32.95	239.255.255.250	SSDP	551	NOTIFY * HTTP/1.1
278	0.232252000	fe80::75f7:3ef6:f26c:5105	ff02::c	SSDP	582	NOTIFY * HTTP/1.1
279	0.232260000	10.0.32.95	239.255.255.250	SSDP	598	NOTIFY * HTTP/1.1
281	0.232689000	fe80::75f7:3ef6:f26c:5105	ff02::c	SSDP	625	NOTIFY * HTTP/1.1
282	0.232699000	10.0.32.95	239.255.255.250	SSDP	606	NOTIFY * HTTP/1.1
283	0.232705000	fe80::75f7:3ef6:f26c:5105	ff02::c	SSDP	637	NOTIFY * HTTP/1.1

Frame 4075: 292 bytes on wire (2336 bits), 292 bytes captured (2336 bits) on interface 0

Radiotap Header v0, Length 48

IEEE 802.11 QoS Data, Flags:,F.C

Logical-Link Control

Internet Protocol Version 4, Src: 10.0.7.123 (10.0.7.123), Dst: 239.255.255.250 (239.255.255.250)

User Datagram Protocol, Src Port: 61677 (61677), Dst Port: 1900 (1900)

Hypertext Transfer Protocol

M-SEARCH * HTTP/1.1\r\n

[Expert Info (Chat/Sequence): M-SEARCH * HTTP/1.1\r\n]

Request Method: M-SEARCH

Request URI: *

Request Version: HTTP/1.1

Host: 239.255.255.250:1900\r\n

ST: urn:dial-multiscreen-org:service:dial:1\r\n

User-Agent: iPhone OS/8.3 UPnP/1.1 ConnectSDK/1.2.1\r\n

MAN: "ssdp:discover"\r\n

0000 00 00 30 00 6b 08 1c 00 c9 fc 29 52 00 00 00 00 .0.k...)R...

0010 10 00 50 14 40 01 db a1 01 2c 81 0e 40 01 01 00 ..P.@... ,.,@...

0020 50 14 28 22 1f 00 0f 00 25 03 00 00 04 00 00 P."...%.....

0030 88 02 30 00 60 03 08 a0 b9 76 2c e6 cc 3b 2a fc ..0.'... .v,...;*

0040 24 a2 e1 b9 cc a6 50 32 01 00 aa aa 03 00 00 00 \$....P2

File: "/var/folders/t4/bc4qb... | Packets: 38683 · Displayed: 831 (2.1%) · Dropped: 0 (0.0%)

Profile: Default

WIRESHARK



Caught In The Cookie Jar

Dabbling with Data Collection

```
<?php
```

```
//JonathanFudem.com Web Beacon

header("Cache-Control: no-cache, must-revalidate");
header("Expires: Sat, 26 Jul 1997 05:00:00 GMT"); //Date in the past

date_default_timezone_set('America/Los_Angeles');

$time = rawurlencode(date("D dS M,Y h:i a"));

$query = isset($_SERVER['QUERY_STRING']) ? "beacon/" . rawurlencode($_SERVER['QUERY_STRING']) : "beacon/no_query";
$ip = isset($_SERVER['REMOTE_ADDR']) ? rawurlencode($_SERVER['REMOTE_ADDR']) : "no_ip";
$host = isset($_SERVER['REMOTE_ADDR']) ? rawurlencode(gethostbyaddr($_SERVER['REMOTE_ADDR'])) : "no_host";
$ua = isset($_SERVER['HTTP_USER_AGENT']) ? rawurlencode($_SERVER['HTTP_USER_AGENT']) : "no_user_agent";
$referer = isset($_SERVER['HTTP_REFERER']) ? rawurlencode($_SERVER['HTTP_REFERER']) : "direct";

$geoip = isset($_SERVER['REMOTE_ADDR']) ? rawurlencode(file_get_contents('http://freegeoip.net/json/' . rawurlencode($_SERVER['REMOTE_ADDR']))) : null;
$friendlyua = isset($_SERVER['HTTP_USER_AGENT']) ? rawurlencode(file_get_contents('http://www.useragentstring.com/?uas=' . rawurlencode($_SERVER['HTTP_USER_AGENT']) . '&getText=all')) : null;

header("content-type: image/gif");

//43byte 1x1 transparent pixel gif

echo base64_decode("R0lGODlhAQABAAAAAAACH5BAEAAAALAAAAAABAAEAAAICRAEA0w==");

//Redirect Form Field ID is Different for JonathanFudem.com and Indulgencesdesigns.com

$lines = file("https://docs.google.com/forms/d/1rrDe3o247HFX0DdpGpKSASGBJ4aItbvSZKSK_DM1i1U/formResponse?ifq&entry.202717044=". $time
."&entry.1388108608=". $query ."&entry.1366919222=". $ip ."&entry.228601374=". $host ."&entry.525632565=". $ua ."&entry.1713784820=". $referer ."&entry.51352101=beacon.gif&entry.1923984710=". $
geoip ."&entry.1896468032=". $friendlyua ."&submit=Submit");

exit;
```

Beacon of Hoax

```
<?php
```

Beacon of Hoax

```
header("Cache-Control: no-cache, must-revalidate");
header("Expires: Sat, 26 Jul 1997 05:00:00 GMT");

date_default_timezone_set('America/Los_Angeles');

$time = rawurlencode(date("D dS M,Y h:i a"));

$query = isset($_SERVER['QUERY_STRING']) ? "beacon/" . rawurlencode($_SERVER['QUERY_STRING']) : "beacon/no_query";

$ip = isset($_SERVER['REMOTE_ADDR']) ? rawurlencode($_SERVER['REMOTE_ADDR']) : "no_ip";
$host = isset($_SERVER['REMOTE_ADDR']) ? rawurlencode(gethostbyaddr($_SERVER['REMOTE_ADDR'])) : "no_host";
$ua = isset($_SERVER['HTTP_USER_AGENT']) ? rawurlencode($_SERVER['HTTP_USER_AGENT']) : "no_user_agent";
$referer = isset($_SERVER['HTTP_REFERER']) ? rawurlencode($_SERVER['HTTP_REFERER']) : "direct";

$geoip = isset($_SERVER['REMOTE_ADDR']) ? rawurlencode(file_get_contents('http://freegeoip.net/json/' . rawurlencode($_SERVER['REMOTE_ADDR']))) : null;
$friendlyua = isset($_SERVER['HTTP_USER_AGENT']) ? rawurlencode(file_get_contents('http://www.useragentstring.com/?uas=' . rawurlencode($_SERVER['HTTP_USER_AGENT'])). '&getText=all')) : null;

header('Content-Type: image/gif');
echo base64_decode('
![Thanks for Reading](http://www.jonathanfudem.com/specialprojects/beacon.gif?
email/campaign_name/subject=subject_line/tag/Jonathan_Fudem_/
_jfudem@me.com)
```

```
<?php

// JonathanFudem.com Web Beacon

header("Cache-Control: no-cache, must-revalidate"); // HTTP/1.1
header("Expires: Sat, 26 Jul 1997 05:00:00 GMT"); // Date in the past

date_default_timezone_set('America/Los_Angeles');

$time = rawurlencode(date("D dS M,Y h:i a"));

$query = isset($_SERVER['QUERY_STRING']) ? "beacon/" . rawurlencode($_SERVER['QUERY_STRING']) : "beacon/no_query";
$ip = isset($_SERVER['REMOTE_ADDR']) ? rawurlencode($_SERVER['REMOTE_ADDR']) : "no_ip";
$host = isset($_SERVER['REMOTE_ADDR']) ? rawurlencode(gethostbyaddr($_SERVER['REMOTE_ADDR'])) : "no_host";
$ua = isset($_SERVER['HTTP_USER_AGENT']) ? rawurlencode($_SERVER['HTTP_USER_AGENT']) : "no_user_agent";
$referer = isset($_SERVER['HTTP_REFERER']) ? rawurlencode($_SERVER['HTTP_REFERER']) : "direct";

$geoip = isset($_SERVER['REMOTE_ADDR']) ? rawurlencode(file_get_contents('http://freegeoip.net/json/' . rawurlencode($_SERVER['REMOTE_ADDR']))) : null;
$friendlyua = isset($_SERVER['HTTP_USER_AGENT']) ? rawurlencode(file_get_contents('http://www.useragentstring.com/?uas=' . rawurlencode($_SERVER['HTTP_USER_AGENT']) . '&getText=all')) : null;

header("content-type: image/gif");

// 43byte 1x1 transparent pixel gif
echo base64_decode("R0lGODlhAQABAAAAAAACH5BAEAAAALAAAAAABAAEAAAICRAEA0w==");

// Redirect Form field ID is different for JonathanFudem.com and Indulgencesdesigns.com

$lines = file("https://docs.google.com/forms/d/1rrDe3o247HFX0DdpGpKSASGBJ4aItbvSZKSK_DM1i1U/formResponse?ifq&entry.202717044=". $time
."&entry.1388108608=". $query ."&entry.1366919222=". $ip ."&entry.228601374=". $host ."&entry.525632565=". $ua ."&entry.1713784820=". $referer ."&entry.51352101=beacon.gif&entry.1923984710=". $
geoip ."&entry.1896468032=". $friendlyua ."&submit=Submit");

exit;
```

```
<?php

// JonathanFudem.com Web Beacon

header("Cache-Control: no-cache, must-revalidate"); // HTTP/1.1
header("Expires: Sat, 26 Jul 1997 05:00:00 GMT"); // Date in the past

date_default_timezone_set('America/Los_Angeles');

$time = rawurlencode(date("D dS M,Y h:i a"));

$query = isset($_SERVER['QUERY_STRING']) ? "beacon/" . rawurlencode($_SERVER['QUERY_STRING']) : "beacon/no_query";
$ip = isset($_SERVER['REMOTE_ADDR']) ? rawurlencode($_SERVER['REMOTE_ADDR']) : "no_ip";
$host = isset($_SERVER['REMOTE_ADDR']) ? rawurlencode(gethostbyaddr($_SERVER['REMOTE_ADDR'])) : "no_host";
$ua = isset($_SERVER['HTTP_USER_AGENT']) ? rawurlencode($_SERVER['HTTP_USER_AGENT']) : "no_user_agent";
$referer = isset($_SERVER['HTTP_REFERER']) ? rawurlencode($_SERVER['HTTP_REFERER']) : null;
$geoip = isset($_SERVER['REMOTE_ADDR']) ? rawurlencode(file_get_contents('http://www.geoplugin.net/php.gi?ip=' . $_SERVER['REMOTE_ADDR'])) : null;
$friendlyua = isset($_SERVER['HTTP_USER_AGENT']) ? rawurlencode(file_get_contents('http://www.ubertech.com/?uas=' . rawurlencode($_SERVER['HTTP_USER_AGENT']))) : null;

header("content-type: image/gif");

// 43byte 1x1 transparent pixel gif
echo base64_decode("R0lGODlhAQABAAAAAAACH5BAEAAAALAAAAAABAAEAAAICRAEA0w==");

// Redirect Form field ID is different for JonathanFudem.com and Indulgencesdesigns.com

$lines = file("https://docs.google.com/forms/d/1rrDe3o247HFX0DdpGpKSASGBJ4aItbvSZKSK_DM1i1U/formResponse?ifq&entry.202717044=". $time
."&entry.1388108608=". $query ."&entry.1366919222=". $ip ."&entry.228601374=". $host ."&entry.525632565=". $ua ."&entry.1713784820=". $referer ."&entry.51352101=beacon.gif&entry.1923984710=". $geoip
."&entry.1896468032=". $friendlyua ."&submit=Submit");

exit;
```

```
<?php
```

```
// JonathanFudem.com Web Beacon

header("Cache-Control: no-cache, must-revalidate"); // HTTP/1.1
header("Expires: Sat, 26 Jul 1997 05:00:00 GMT"); // Date in the past

date_default_timezone_set('America/Los_Angeles');

$time = rawurlencode(date("D dS M,Y h:i a"));
$query = isset($_SERVER['QUERY_STRING']) ? "beacon/" . rawurlencode($_SERVER['QUERY_STRING']) : "beacon/no_query";
$ip = isset($_SERVER['REMOTE_ADDR']) ? rawurlencode($_SERVER['REMOTE_ADDR']) : "no_ip";
$host = isset($_SERVER['REMOTE_ADDR']) ? rawurlencode(gethostbyaddr($_SERVER['REMOTE_ADDR'])) : "no_host";
$ua = isset($_SERVER['HTTP_USER_AGENT']) ? rawurlencode($_SERVER['HTTP_USER_AGENT']) : "no_useragent";
$referer = isset($_SERVER['HTTP_REFERER']) ? rawurlencode($_SERVER['HTTP_REFERER']) : "no_referer";
$geoip = isset($_SERVER['REMOTE_ADDR']) ? rawurlencode(file_get_contents('http://www.geoplugin.net/php.gi?ip=' . rawurlencode($_SERVER['REMOTE_ADDR']))) : null;
$friendlyua = isset($_SERVER['HTTP_USER_AGENT']) ? rawurlencode(file_get_contents('http://www.ubersmith.com/?uas=' . rawurlencode($_SERVER['HTTP_USER_AGENT'])). '&getText=all') : null;

header("content-type: image/gif");
// 43byte 1x1 transparent pixel gif
echo base64_decode("R0lGODlhAQABIAAAAAAAAACH5BAEAAAALAAAAAABAAEAAAICRAEA0w==");

// Redirect Form field ID is different for JonathanFudem.com and Indulgencesdesigns.com
$lines = file("https://docs.google.com/forms/d/1rrDe3o247HFX0DdpGpKSASGBJ4aItbvSZKSK_DResponse?ifq&entry.202717044=". $time
."&entry.1388108608=".$query."&entry.1366919222=".$ip."&entry.228601374=".$host."&entr
geoip."&entry.1896468032=".$friendlyua."&submit=Submit");

exit;
```

```
<?php

// JonathanFudem.com Web Beacon

header("Cache-Control: no-cache, must-revalidate"); // HTTP/1.1
header("Expires: Sat, 26 Jul 1997 05:00:00 GMT"); // Date in the past

date_default_timezone_set('America/Los_Angeles');

$time = rawurlencode(date("D dS M,Y h:i a"));
$query = isset($_SERVER['QUERY_STRING']) ? "beacon/" . rawurlencode($_SERVER['QUERY_STRING']) : "beacon/no_query";
$ip = isset($_SERVER['REMOTE_ADDR']) ? rawurlencode($_SERVER['REMOTE_ADDR']) : "no_ip";
$host = isset($_SERVER['REMOTE_ADDR']) ? rawurlencode(gethostbyaddr($_SERVER['REMOTE_ADDR'])) : "no_host";
$ua = isset($_SERVER['HTTP_USER_AGENT']) ? rawurlencode($_SERVER['HTTP_USER_AGENT']) : "no_useragent";
$referer = isset($_SERVER['HTTP_REFERER']) ? rawurlencode($_SERVER['HTTP_REFERER']) : "no_referer";
$geoip = isset($_SERVER['REMOTE_ADDR']) ? rawurlencode(file_get_contents('http://www.geoplugin.net/php.gi?ip=' . $_SERVER['REMOTE_ADDR'])) : null;
$friendlyua = isset($_SERVER['HTTP_USER_AGENT']) ? rawurlencode(file_get_contents('http://www.ubertech.net/uas/' . $_SERVER['HTTP_USER_AGENT'])) : null;
null;

header("content-type: image/gif");
// 43byte 1x1 transparent pixel gif
echo base64_decode("R0lGODlhAQABIAAAAAAAAACH5BAEAAAALAAAAAABAAEAAAICRAEA0w==");

// Redirect Form field ID is different for JonathanFudem.com and Indulgencesdesigns.com
$lines = file("https://docs.google.com/forms/d/1rrDe3o247HFX0DdpGpKSASGBJ4aItbvSZKSK_D...response?ifq&entry.202717044=". $time
."&entry.1388108608=".$query."&entry.1366919222=".$ip."&entry.228601374=".$host."&entr...s=".$ua."&entry.1713784820=".$referer."&entry.51352101=beacon.gif&entry.1923984710=".$
geoip."&entry.1896468032=".$friendlyua."&submit=Submit");

exit;
```

The diagram illustrates the data flow of a beacon request. It starts with a mobile phone icon at the bottom, which sends a signal to a local router. This router then connects to a central cloud icon representing the internet. From the cloud, the signal travels through a series of intermediate routers and finally reaches a destination server icon. The server icon contains the PHP code shown in the screenshot, which processes the request and generates a response.

```
<?php

// JonathanFudem.com Web Beacon

header("Cache-Control: no-cache, must-revalidate"); // HTTP/1.1
header("Expires: Sat, 26 Jul 1997 05:00:00 GMT"); // Date in the past

date_default_timezone_set('America/Los_Angeles');

$time = rawurlencode(date("D dS M,Y h:i a"));
$query = isset($_SERVER['QUERY_STRING']) ? "beacon/" . rawurlencode($_SERVER['QUERY_STRING']) : "beacon/no_query";
$ip = isset($_SERVER['REMOTE_ADDR']) ? rawurlencode($_SERVER['REMOTE_ADDR']) : "no_ip";
$host = isset($_SERVER['REMOTE_ADDR']) ? rawurlencode(gethostbyaddr($_SERVER['REMOTE_ADDR'])) : "no_host";
$ua = isset($_SERVER['HTTP_USER_AGENT']) ? rawurlencode($_SERVER['HTTP_USER_AGENT']) : "no_useragent";
$referer = isset($_SERVER['HTTP_REFERER']) ? rawurlencode($_SERVER['HTTP_REFERER']) : "no_referer";
$geoip = isset($_SERVER['REMOTE_ADDR']) ? rawurlencode(file_get_contents('http://www.geoplugin.net/php.gi?ip=' . $_SERVER['REMOTE_ADDR'])) : null;
$friendlyua = isset($_SERVER['HTTP_USER_AGENT']) ? rawurlencode(file_get_contents('http://www.owasp.org/index.php/OWASP_Friendly_UA_Extractor/index.php?uas=' . rawurlencode($_SERVER['HTTP_USER_AGENT']))) : null;

header("content-type: image/gif");
// 43byte 1x1 transparent pixel gif
echo base64_decode("R0lGODlhAQABIAAAAAAAAACH5BAEAAAALAAAAAABAAEAAAICRAEA0w==");

// Redirect Form field ID is different for JonathanFudem.com and Indulgencesdesigns.com
$lines = file("https://docs.google.com/forms/d/1rrDe3o247HFX0DdpGpKSASGBJ4aItbvSZKSK_D...response?ifq&entry.202717044=". $time
."&entry.1388108608=".$query."&entry.1366919222=".$ip."&entry.228601374=".$host."&entr...s=".$ua."&entry.1713784820=".$referer."&entry.51352101=beacon.gif&entry.1923984710=".$
geoip."&entry.1896468032=".$friendlyua."&submit=Submit");

exit;
```

The diagram illustrates the flow of data from a mobile device to a web server and then to a global network. A smartphone at the bottom left represents the user's device. An arrow points from the phone to a laptop, which represents the web server. From the laptop, an arrow points upwards to a globe, representing the global network. The code in the image corresponds to the logic that processes data from the user's device and sends it to the server, which then forwards it to the network.

A Brief History of Privacy

Free Expression
and Capitalism

Consumer Media

Foundation for
Other Freedoms

A Brief History of Privacy



Consumer Media

Foundation for
Other Freedoms

A Brief History of Privacy



Consumer Media

Foundation for
Other Freedoms

A Brief History of Privacy

Free Expression
and Capitalism



Foundation for
Other Freedoms

A Brief History of Privacy

Free Expression
and Capitalism

Consumer Media



Where Does Data Come From



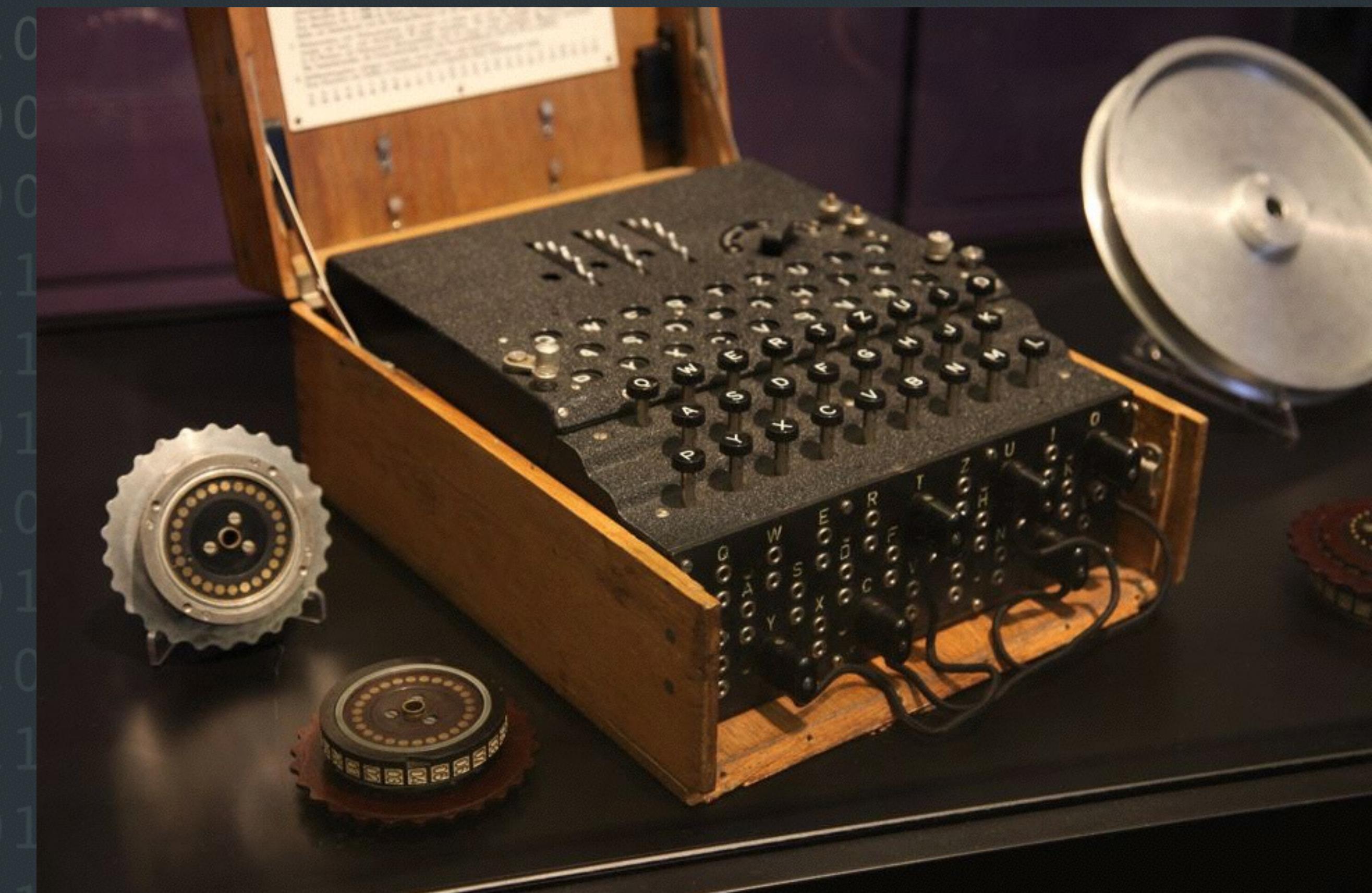
Companies + Advertisers

Where Does Data Come From?



The Government

Sympathy for the Devil



Privacy Myths

Your Data is Worth a Lot

Your Data is Worth a Lot

.0065 Cents

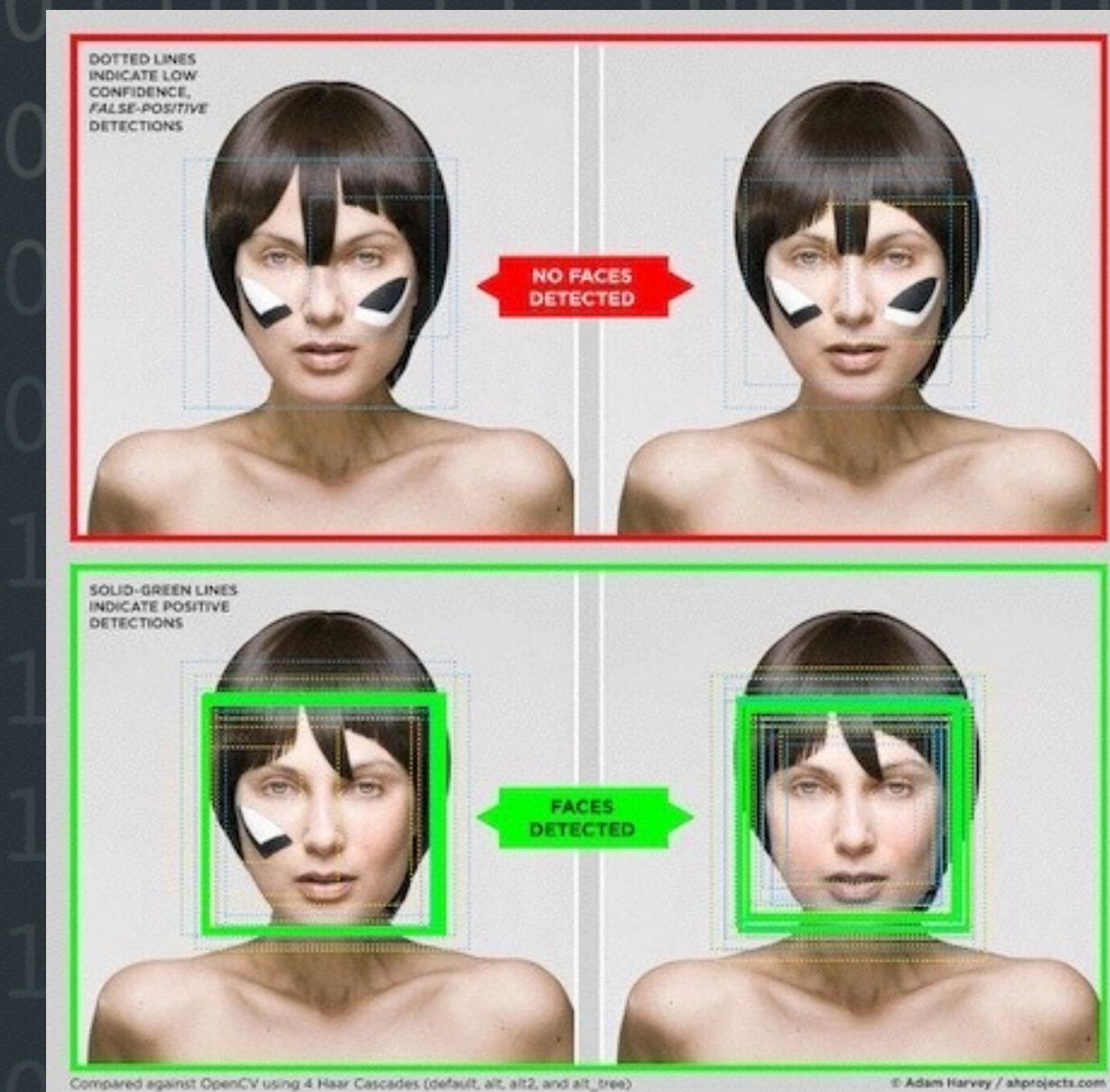
15,385 people = \$1.00

If You Have Nothing To Fear You Have Nothing To Hide

Increased Surveillance Makes Us More Secure

It's Just Metadata, Nothing Personal

Tinfoil Makeup?





[About us](#) [Facebook](#) [Blog](#)



**Honest reviews
about people**

[Learn more](#)

What Am Doing About it?

LOVEINT: A Game of Love and Intel



You are an analyst for the NSA.

Your duty is to intercept Facebook Messages from potential terrorists using the PRISM Database.

You are worried your spouse is cheating on you.

Since your boss is out of town, use the next three days and your security clearance to find out what your spouse is up to.

Don't Get Caught.

LOVEINT: A Game of Love and Intel

TOP SECRET//SI//ORCON//NOFORN

Day **1** // Remaining Peeks: **3** // Chance of Firing: **0%** // Clock Out

Database:

PRISM

Provider:

FACEBOOK

App UserLookUp:

Felicity Jones

App Quried UserID:

FB44271

METADATA: CONV-VIEW

Recipient UserID: FB96233;

X-Recieved-BY: FB44271; X-Recieved-ON: 14:10:37
UTC-05:00;

Recipient UserID: FB26934;

X-Recieved-BY: FB44271; X-Recieved-ON: 12:48:51
UTC-05:00;

Recipient UserID: FB59077;

X-Recieved-BY: FB44271; X-Recieved-ON: 11:17:02
UTC-05:00;

METADATA: QUERY VIEW

Look Up Recipient ID

UserID: Felicity.Jones
Date: 11/17/2015 at 14:06:22;
Message: Entry Encrypted

Request Content Lookup

UserID: FB96233;
Date: 11/17/2015 at 14:07:31;
Message: Entry Encrypted

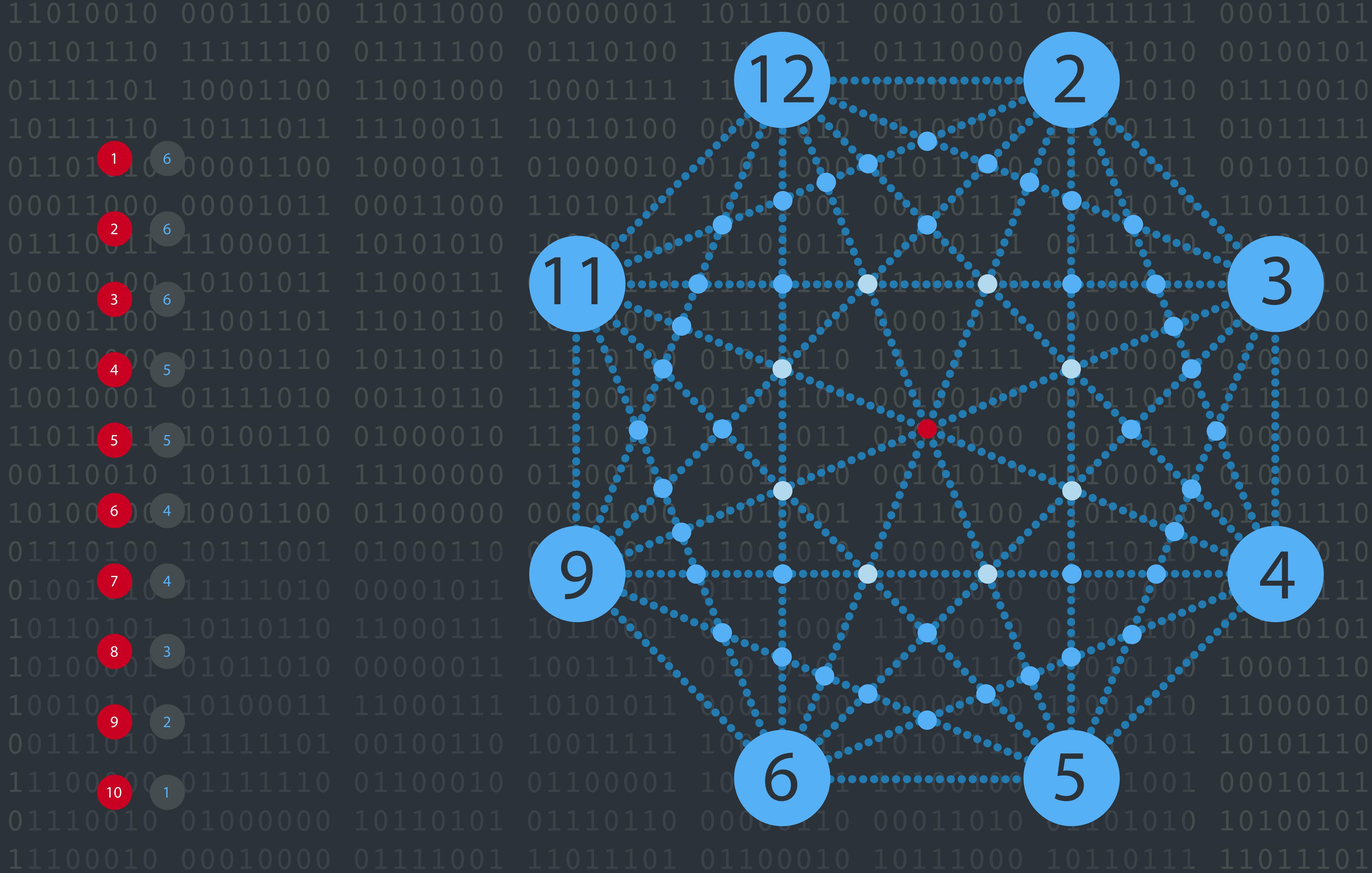
Request Content Lookup

UserID: Felicity.Jones
Date: 11/17/2015 at 14:08:14;
Message: Entry Encrypted

Request Content Lookup

UserID: FB96233;
Date: 11/17/2015 at 14:08:38;
Message: Entry Encrypted

Request Content Lookup



Thank You