SecTalks London 0x11

Introduction to Hardware Hacking

Patrick Coleman blinken@gmail.com

sectalks

Wifi: Meraki-Guest -> Windows/OS X: install the PL2303 USB/serial driver

About us

Monthly (in)security talks and Capture-the-Flag challenges.

- Community run with a strict no-bullshit policy
- Different skill sets welcome: ops, devs, sysadmins, security researchers etc.

{**Perth**,**Sydney**,**Brisbane**,**Melbourne**,**Canberra**,**Adelaide**,**Hobart**}, Australia; **Beijing**, China; **Ljubljana**, Slovenia; **Christchurch**, New Zealand

Don’t let the hardware hack you

- Disconnect power before opening up the case
  - Even low input-voltage DC devices can generate high internal voltages; home entertainment devices with vacuum fluorescent displays are a common example
  - Telecoms cabling runs at 48V
  - Capacitors can hold a lot of energy, even when the device is unplugged
- Handle circuit boards by the edges
- Be aware of where your hands and tools are
- PCBs and solder contain lead, and stuff
  - Don’t lick anything
  - Wash your hands

Roll over image to zoom in

ZEEPIN Mini WiFi 720P Smart IP Camera Home Security System , Night Vision Motion Detection 4X Digital Zoom Two-way Intercom

by Zeepin

★★★★★ 1 customer review

Currently unavailable.

We don't know when or if this item will be back in stock.

- Mini WiFi monitor IP camera smart home security system , 720P HD resolution, provides clear image
- Built-in IR lens, support night vision , Two-way intercom , allows you to talk with your family anywhere anytime
- Motion detection function will send you message when detects something moving
- Support max up to 64G Micro SD card , Please download APP " V380 " from Google Play or Apple Store
- It can be hung upside down to use , Compatible with ONVIF device

Compare with similar items

Report incorrect product information.

Dione M. Gray

★★★★★ **Five Stars**

18 February 2018

Verified Purchase

Love it, I can talk to my pets whilst at work!

"Easy to achieve real-time remote viewing"

Wireless Home Security IP Camera, DIGOO DG-M1Z Security Surveillance System, Baby Camera Pet Monitor with 1080P WIFI Pan/Tilt Cam, Two Way Audio, Motion Detection, Night Version f Pet, Baby, Home, Elder White

by DIGOO

37 customer reviews | 36 answered questions

Price: £37.99 prime

Product description

Colour Name:**White**

Is your baby safe with babysitter?
what your pet doing when you leave home?
Is there anything happen when you fall asleep?
Do you want to talk with your baby when you out of home?
Now, DIGOO security camera can make you reach above wishes!
No matter where you are, you can get the real-time image of your home and talk wi

Feature
1. Vivid 1080p full HD performance provide you a more shape and clear video, to keep
2. 130°2.8mm Wide Angle Lens, putting one in your home is enough to view a whole r
3. 2 way talking audio, you can hear and talk to your baby and family members at any
5. Download "DIGOOEYE" from app store or GOOGLE shop, makes you know the situat

Specifications
Video Streams: 1080p/25 fps
Lens: 2.8mm 130°Wide Angle Lens & 5.0MP Lens More Clear Vision
Pictures Zoom: 4X Digital Zoom
Memory: Support Micro TF Card Slot (Max to 64GB)
IR Light: 11Pcs IR LED
IR Distance: Night Visibility 10m+

Importance
The camera only works with 2.4GHz network (Incompatible with 5GHz)

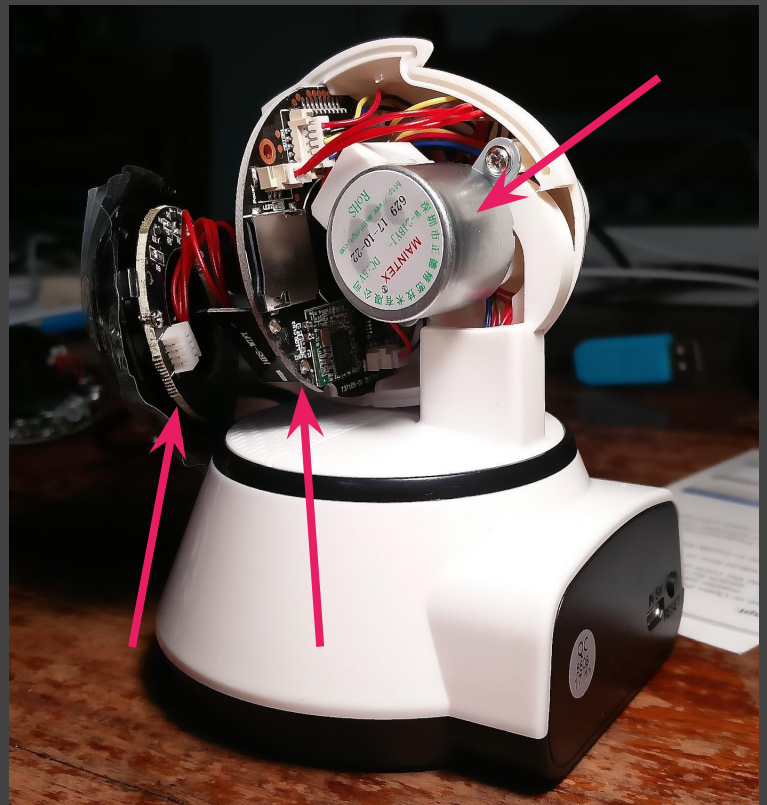
Package Includes
1 x Digoo DG-M1Z 1080P SHARK IP Camera (Black / White Optional)
1 x Digoo DG-M1Z Micro USB Power Cable (3 Meters Long)
1 x Digoo DG-M1Z Full English User Manual
1 x Digoo DG-M1Z Original Color Gift Package
1 x Pack of Installing Accessories

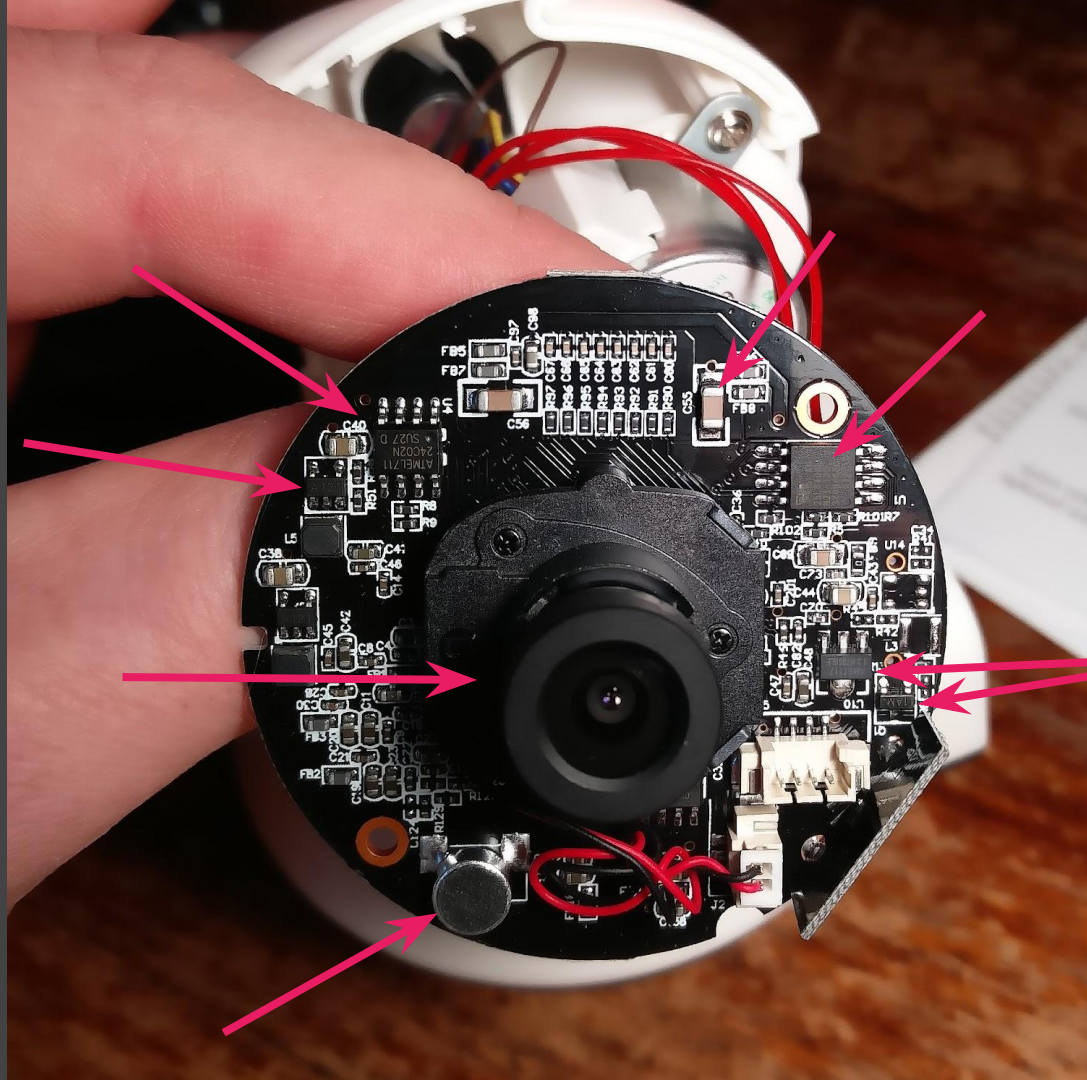
Objectives

- Power it up and see what it does
- Pull it apart and see how it works
- Get to a console login prompt on the device
  - Capture debug information from the console
- Identify the OS the device runs, and figure out who actually made it
- Find out what the device does, how it communicates, and whether it’s secure enough to put in my house

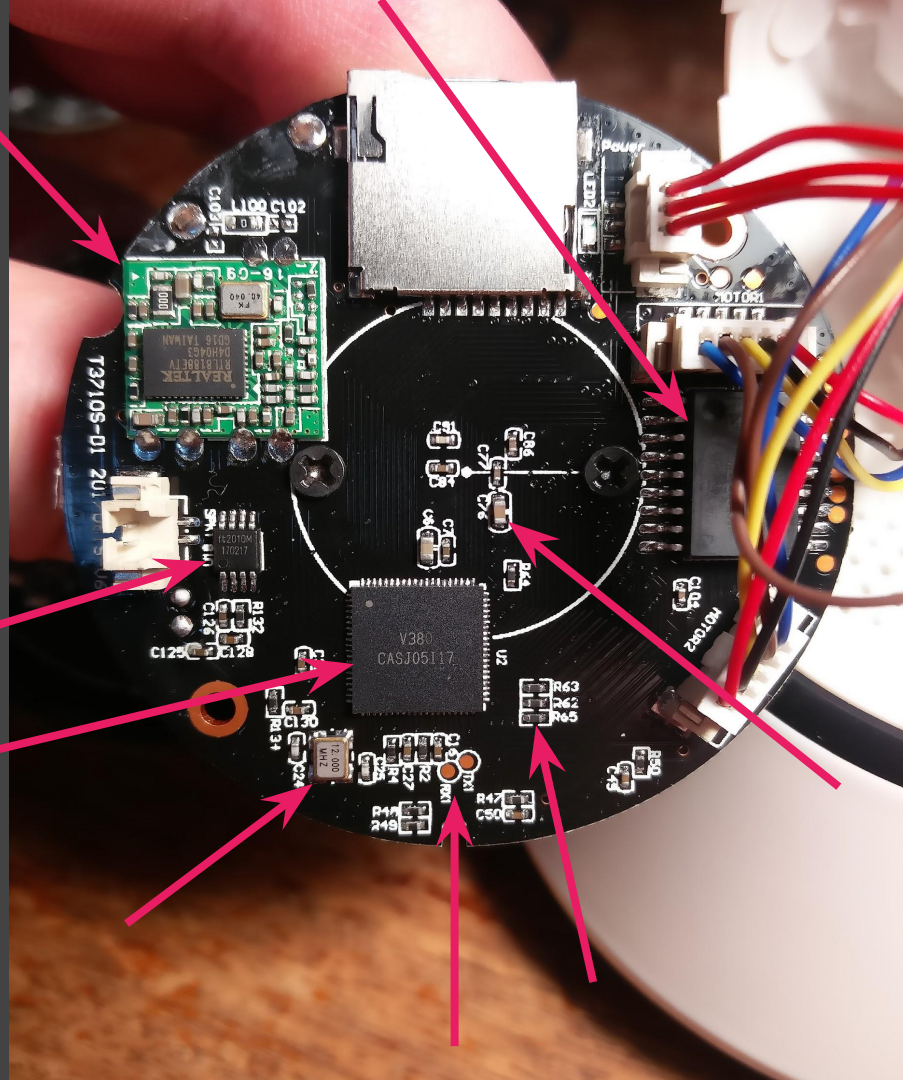
1. Power up the camera
    - See what it does
2. Rip open the top cover
    - Don’t break the tiny wires
    - Don’t lick anything

Component identification



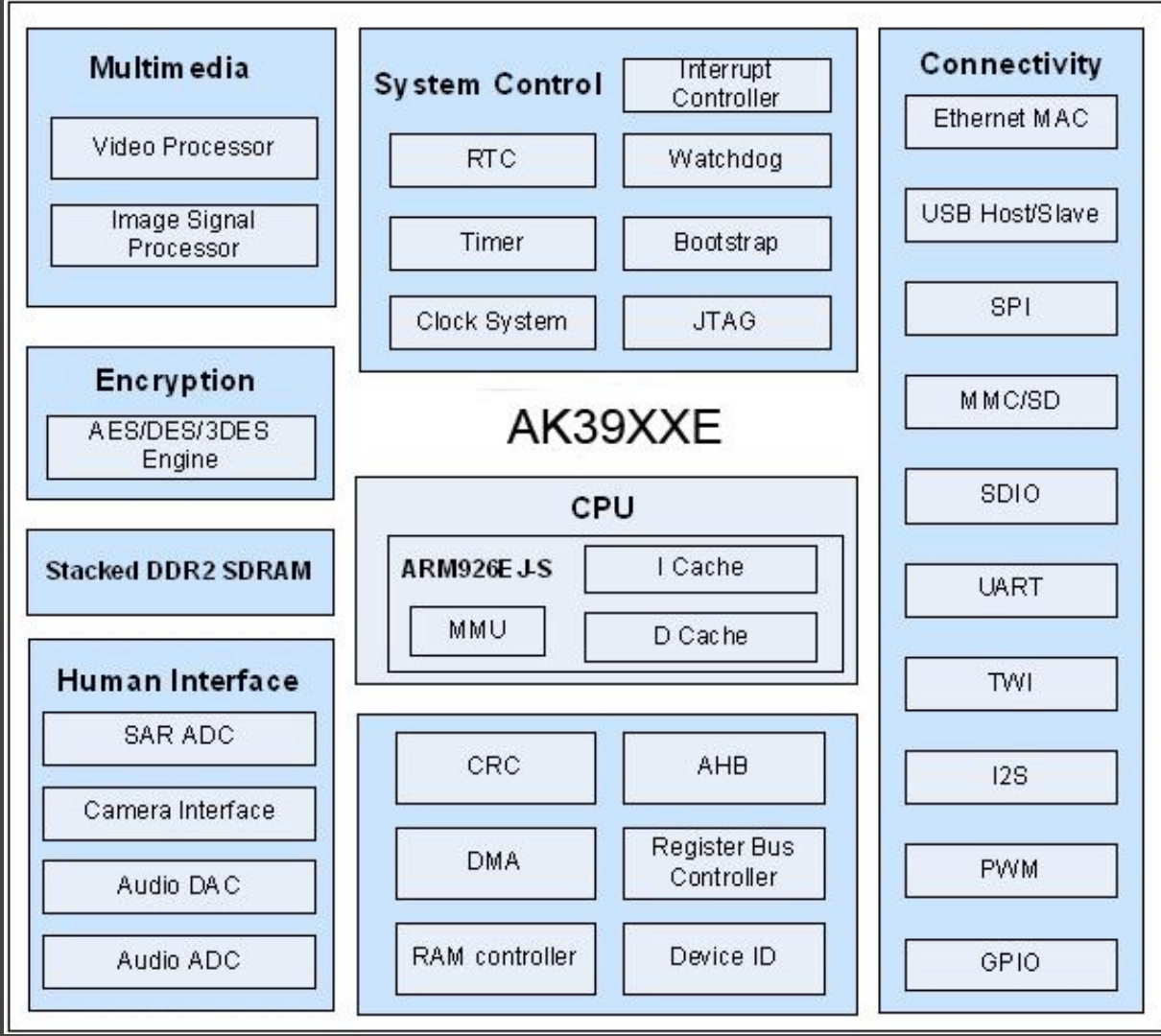


Component identification



Anyka AK3918E

- ARM926EJ-S
  - 400MHz, single core
  - 40MB DDR2
- Image Signal Processor (ISP)
- H.264 encoder
- JPEG encoder
- Ethernet MAC 10/100Mbps, full-duplex mode
- USB 2.0 Host & Slave
- TWI
- I2S
- SPI
- UART
- MMC/SD/SDIO
- PWM
- 3.3V logic



Hunting debug ports

- Access for testing / debugging is often left in place on the finished product
- Look for unpopulated pins or pads suspiciously near the SoC
  - Often still labelled!
- Serial UART (aka “RS232”) - machine console
  - Uses certain fixed speeds by convention: 1200, 2400, 4800, 19200, 38400, 57600, and 115200
  - Wires: transmit, receive, ground
  - Should be your first target in any embedded system
- JTAG - debugger attachment at CPU level
- USB - often used for firmware download; depends on device

1. Connect USB-Serial cable
    - +5V Ground Transmit Receive
2. Open a terminal emulator
    - screen /dev/tty.usbserial 9600
3. Power up the camera

```
Cloud39E spiboot V1.1.01
load spiflash bios ......
asic clk:60000000, pre-scaler=1 (wanted 20Mhz, got 15Mhz)
the manufacture id is 001720c2
spi param: id=001740ef, total_size=8388608, page_size=256, program_size=16.
erase_size=4096, clock=25000000, flag=0, protect_mask=0.
asic clk:60000000, pre-scaler=1 (wanted 25Mhz, got 15Mhz)
file cnt:4
Read file BIOS
start:560
file len:2095880
ld addr:0x82008000
Load bios from spiflash successfuly!
Uncompressing Linux... done, booting the kernel.
Anyka Linux Kernel Version: 2.1.06
Booting Linux on physical CPU 0
Linux version 3.4.35 (root@lin) (gcc version 4.4.1 (Sourcery G++ Lite 2009q3-67) ) #2 Fri
Sep 1 15:13:49 CST 2017
CPU: ARM926EJ-S [41069265] revision 5 (ARMv5TEJ), cr=00053177
CPU: VIVT data cache, VIVT instruction cache
Machine: Cloud39E_AK3918E+H42_V1.0.2
Memory policy: ECC disabled, Data cache writeback
ANYKA CPU AK3916 (ID 0x20150200)
Built 1 zonelists in Zone order, mobility grouping on.  Total pages: 10160
Kernel command line: root=/dev/mtdblock1 ro rootfstype=squashfs init=/sbin/init mem=64M
console=ttySAK0,115200
PID hash table entries: 256 (order: -2, 1024 bytes)
Dentry cache hash table entries: 8192 (order: 3, 32768 bytes)
Inode-cache hash table entries: 4096 (order: 2, 16384 bytes)
Memory: 40MB = 40MB total
Memory: 36592k/36592k available, 4368k reserved, 0K highmem
...
```

```
...
ak-spiflash spi0.0: mx25l6405d (8192 Kbytes)
FHA:fhalib V1.0.25
FHA:FHA_S SPIFlash_Init: BinPageStartblock:35,
FHA:FHA_S SPIFlash_Init: BinPageStart:560,
FHA:FHA_S G_P_S:558
nr_parts=0x5
...
Creating 5 MTD partitions on "spi0.0":
0x000000260000-0x000000440000 : "A"
0x000000440000-0x000000540000 : "B"
0x000000540000-0x000000660000 : "C"
0x000000660000-0x0000006e0000 : "D"
0x0000006e0000-0x000000800000 : "E"
Init AK SPI Flash finish.
...
VFS: Mounted root (squashfs filesystem) readonly on device 31:1.
devtmpfs: mounted
Freeing init memory: 104K
mount all file system...
starting mdev...
**************************
    Love Linux ! ! !
**************************
200+0 records in
200+0 records out
102400 bytes (100.0KB) copied, 0.016370 seconds, 6.0MB/s


V380E login:
```

Who made this?

- We bought the device from ZEEPIN
- The chip is made by Anyka, model AK3918E
  - ...but their website has zero technical information
- Who designed the board and the OS?
- Who runs the “cloud” services the camera connects to?
  - We might be able to get a firmware image there

```
nvan1.av380.net
nvan2.nvcam.net
ak701.av380.net
rg59ak.nvcam.net
time3.nvcam.net
alarm1.nvdvr.cn
update.nvcam.net
```

=> TO THE DARK WEB

Related Category

Electronic Components & Supplies
Integrated Circuits

Security & Protection
CCTV Camera

Product Features

Type
- Drive IC

Sample Order NEW
- Paid samples

Min Order: Less Than | OK

Supplier Features

Supplier by Area
- Asia

Suppliers by Country/Region
- China (Mainland)
- Hong Kong
- Thailand

Products | Suppliers

Supplier Types: Trade Assurance | Gold Supplier | Assessed Supplier
Supplier Location: All Countries & Regions | Past Export Countries: All Countries & Regions

View **509** Product(s) | Min Order: Less Than | Price: – | Sort By : Best Match

6 Photos

Linux based BPI D1 HD Camera Module Features Anyka AK3918 ARM9 Processor

US $30-37 / Piece
100 Pieces (Min. Order)

Place of Origin: Guangdong...
Type: Drive IC
Brand Name: Banana PI
Model Number: BPI-D1 IP C...

6YR Shenzhen Yuanchuang Communicatio...
China (Mainland) | Trade Assurance
Transaction Level:
4 Transactions(6 months) | Response Rate
20,000+ | 38.2%

Add to Compare | Similar Products | Contact Supplier | Chat Now!

Cheap AK3918E Wireless & Wireless cctv camera poe ip camera free CMS platform

US $5-25 / Piece
100 Pieces (Min. Order)

Sensor: CMOS
Special Features: Two-way ...
Technology: NetWork
Type: IP Camera
Model Number: RL21

13YR Shenzhen Relee Electronics & Technol...
China (Mainland) | Trade Assurance
Transaction Level:
18 Transactions(6 months) | Response Rate
9,000+ | 85.8%

Browsing History


TPS65218B1RSLT ...
US $0.01-9
1 Piece


XMR-JK66 wholes...
US $1.0-14.5
1 Set


Factory price of AN...
US $1-30
1 Piece


in stock IP surveill...
US $5-25
100 Pieces


Cheap AK3918E Wi...
US $5-25
100 Pieces


AnyKa AK3918E+1...
US $18.9-21.9
1 Piece


The best recording ...
US $1-30
1 Piece

Manage Browsing History

AK3918E

Trade Assurance

Add to Compare | Similar Products | Contact Supplier | Leave Messages

Hd wifi camera 720 P smart ip camera real - time security camera XMR-JK66

US $1.0-14.5 / Set

1 Set (Min. Order)

Sensor: CMOS
Special Features: 360eye v...
Style: Mini Camera
Technology: NetWork
Brand Name: XMR
Place of Origin: Guangdong...

3YR Shenzhen Xiao Ma Technology Co., Ltd.
China (Mainland) | Trade Assurance
Transaction Level:
16 Transactions(6 months) Response Rate
$ 10,000+ 83.9%

Add to Compare | Similar Products | Contact Supplier | Chat Now!

WIFI IP Camera Support V380 APP 360 Light Bulb Camera Hidden 1.3MP With LED Light

US $10-19.9 / Piece

5 Pieces (Min. Order)

Sensor: CMOS
Technology: Infrared
Type: IP Camera
Model Number: AS-J130FB...
Brand Name: AST
Place of Origin: Guangdong...

2YR AST Enterprise (Shenzhen) Co., Ltd.
China (Mainland) | Trade Assurance
Transaction Level:
42 Transactions(6 months) Response Rate
$ 30,000+ 96.6%

Add to Compare | Similar Products | Contact Supplier | Chat Now!

4CH WIFI NVR KITs 720P Outdoor IP Wireless Camera security 12v cctv camera

US $75-85 / Piece

1 Piece (Min. Order)

Sensor: CMOS
Special Features: Waterpro...
Style: Bullet Camera

11YR MACRO PLUS
Hong Kong
Transaction Level:
Response Rate
97.9%

RFQ
TOP

Alibaba.com Global trade starts here.™ Sourcing Solutions Services & Membership Help & Community One Request, Multiple Quotes | Get the App

Categories Products AK3918E Search 1 My Alibaba Order Protection 0 Favorites

Related Searches: csi camera

Related Category

Electronic Components & Supplies
Integrated Circuits

Security & Protection
CCTV Camera

Product Features

Type
- Drive IC

Sample Order NEW
- Paid samples

Min Order: Less Than OK

Supplier Features

Supplier by Area
- Asia

Suppliers by Country/Region
- China (Mainland)
- Hong Kong
- Thailand

Products Suppliers

Supplier Types: Trade Assurance Gold Supplier Assessed Supplier

Supplier Location: All Countries & Regions Past Export Countries: All Countries & Regions

View **509** Product(s) Min Order: Less Than Price: – Sort By : Best Match

6 Photos

Linux based BPI D1 HD Camera Module Features Anyka AK3918 ARM9 Processor

US $30-37 / Piece

100 Pieces (Min. Order)

Place of Origin: Guangdong...
Type: Drive IC
Brand Name: Banana PI
Model Number: BPI-D1 IP C...

6YR Shenzhen Yuanchuang Communicatio...
China (Mainland) Trade Assurance
Transaction Level:
4 Transactions(6 months) Response Rate
20,000+ 38.2%

Add to Compare Similar Products Contact Supplier Chat Now!

Cheap AK3918E Wireless & Wireless cctv camera poe ip camera free CMS platform

US $5-25 / Piece

100 Pieces (Min. Order)

Sensor: CMOS
Special Features: Two-way ...
Technology: NetWork
Type: IP Camera
Model Number: RL21

13YR Shenzhen Relee Electronics & Technol...
China (Mainland) Trade Assurance
Transaction Level:
18 Transactions(6 months) Response Rate
9,000+ 85.8%

Buyer Community

- Get Insights
- Hear Experts
- Build Relationships

Have A Look

RFQ TOP

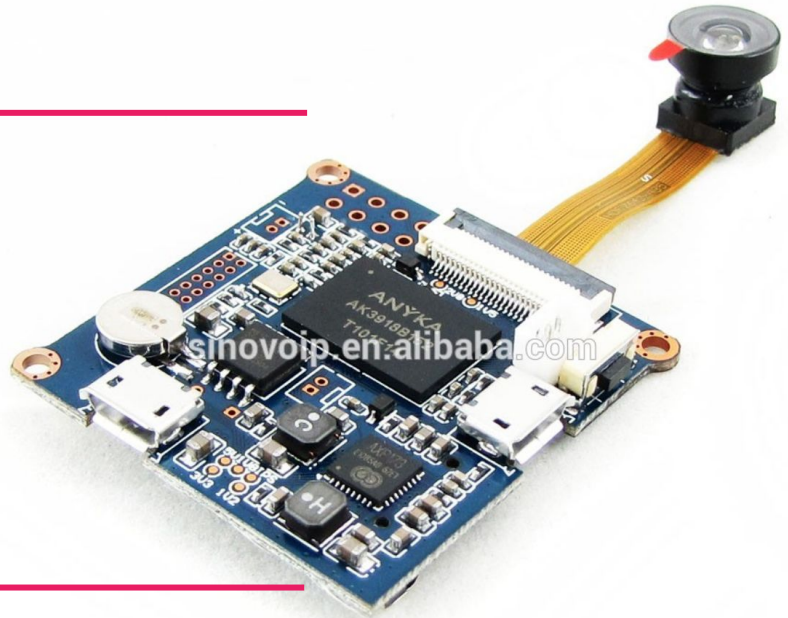
The Banana Pi D1 is a small open-source development board with an on-board HD video camera capable of capturing 720p videos at 30fps.

The D1 comes with all you need to set-up a web connected video camera including a USB OTG WiFi support, external battery connector, microphone, and more. This is the perfect board that can provide the hardware platform for many fun projects.

Banana Pi is an open platform device, it is for anyone who wants to play and build with developer technology instead of simply using consumer technology. Backed by our community, starting a project and building servers is fun and rewarding. We welcome all companies, DIYers, and tech loving people within our community! Together, we can make a difference, we can discover our passions, inspire others, and build a practical project.

SPECS

Product size	PCB 36x36mmM7*P0.35 EFL=3.0mm/F.NO=2.8/View Angle=60°
CPU	400MHz ARM926EJ 32Bits RISC Core
RAM	64MB DDR2
Flash	16MB SPI-FLASH
Storage	SD Card Seat ,supportable for 8G,16G, 32G TF cards
CMOS	CMOS Image Sensor SoC30FPS@720P, Visible light with 940 nm two-way infrared lens filter, with infrared night vision function
Lens	M7*P0.35 EFL=3.0mm/F.NO=2.8/View Angle=60°
Video	It achieves H.264 hardware encoding at 1280x720p_30fps. 32 gb TF card can store 120 hours of video data
Audio	MP3/WMA/AAC
WIFI	RTL8188EUS WIFI module embedded, support 802.11bgn and can switch AP or Normal mode
RTC	RTC circuit and supporting OSD
PM	Support Li-ion Charging with Built-in AXP173 power management chip
Mic	Embedded electret microphone
Power Consumption	Recording: 5V-200mA; WiFi On: 5V-350mA; continuously record 720P video or audio data for 24hour when a mobile power of 10000mAH is available.
GPIO	1UART/2GPIO;2PWM/2GPIO;I2C;AudioLineIN;HPAudioOutL;HPAudioOutR;1SPI Interface
UART	Independent UART debugging interface
USB	USB programmatic interface/ OTG device (WiFi module/USB drive)
DC IN	Micro-USB single +5V power input
Battery	3.7V Li-ion socket
OS	Running on Linux3.4.35, Kernel Operation system that makes secondary development possible



Program the Firmware

Important Notes before You Start:

1. You must use the compatible version of the firmware programingsoftware with source codes.
2. The software works on Windows XP Service Pack 3 and newer versions.
3. The software file path is located at: /lamobo.dev/tool/burntool in the code directory
4. Before programming the firmware, please make sure to copy and paste the3compiled files “zImage,” “root.sqsh4,” and “root.jffs2” to the root directory. (Note: The complied files are saved at: /lamobo.dev/output)
5. image download and forum: http://www.banana-pi.org

How to Program the Firmware

1. Battery mode, press and hold the "primary key" 5 seconds off BPI-D1 power. Before the PC inserts BPI-D1 micro - USB programming cable, double-click firm programming tools icon, runs the burn tool. Holding down the "function key" and the micro - USB programming cable connecting to the PC, the module enters the programming mode. At this time BPI-D1 LED no instructions. If there is no lithium battery, you do not need to connect the micro USB power cable.

Looking at the cloud services some more

```
curl -v
update.nvcam.net:8888/AppManage/AppVersionUpdateCheck?param=eyJhcHBfaWQiOi…
{"app_id":"750","app_name":"V380E2_C","app_version":"2050004","system_id":"750
","system_ver":"2050004"}

< HTTP/1.1 200 OK
< Server: Apache-Coyote/1.1
< Content-Type: text/html;charset=utf-8
< Transfer-Encoding: chunked
< Date: Sat, 17 Feb 2018 16:15:23 GMT
< Connection: close
<
* Closing connection 0
{"result":0,"new_version_info":{}}
```

Looking at the cloud services some more

```
curl -v
update.nvcam.net:8888/AppManage/AppVersionUpdateCheck?param=eyJhcHBfaWQiOi…
{"app_id":"750","app_name":"V380E2_C","app_version":"0","system_id":"750","sys
tem_ver":"0"}

{"result":2,"new_version_info":{"appSite":"http://as4.nvdvr.cn/IPC/manual/AK-V
200_V380/V380E2_C_V2.5.0.14.patch","appName":"E2_C_V2.5.0.14","appID":750,"app
Description":"c34111620
8fdc13b51657893a7c617cb","appVersionNum":1,"appReleaseDate":"2017-11-28","appC
ompany":"macro-video","forceUpdate":0,"appVersionName":"E2_C_V2.5.0.14","appSi
ze":1118668}}
```

M@CRO-VIDEO Technologies Co.,LTD

Products

- **WIFI Camera**
  - V380 (Indoor)
  - V380 (Outdoor)
  - Babay monitor
- **DVR CARD**
- **VR CAMREA**

V380 (Indoor)

MVT8610 -Q10

MVT8610 -Q9

MV-C8410-X1

MV-C8410-R1

MV -C8310-S1

MVT8610 -Q5

MVT8610 -Q4

MVT8610 -Q2

Development Platform

AnyCloud is a Linux development platform for mobile applications based on AK39E processor, including IoT Cameras, visible doorbells, Wi-Fi driving recorders, and aerial cameras.

Functions

•Supports 1M/1.3M pixels CMOS Image Sensor

•ISP: Image parameter adjustment (contrast, brightness and saturation), motion detection, privacy mask and OSD

•Video Decoder

-H.264 decoder

-MJPEG decoder

-Dual streams output

•Video recording modes: cyclic, ordinary, and alarm mode

•Supports motion detection and voice detection

•Audio Codec: AAC, ADPCM, AMR, and G.711

•Supports two-way intercom with echo cancellation

•Cloud services support: Tencent QQ Internet of Things (IoT) platform and Danale Cloud platform

•Supports viewing video remotely via APPS (iOS, Android)

•Memory

-Supports TF card extension, up to 64GB

-Supports standard ONVIF, compatible with mainstream NVR systems

•Network:

-Supports 10/100M full duplex Ethernet

-Supports Wi-Fi network, supporting Smartlink/Airlink rapid network configuration.

Anyka Product Information Application

Welcome to the Internet of Cheap Things

- Proprietary and secretive
- Long, opaque supply chains
  ⇒ homogeneity: the same code runs in devices from many manufacturers
- Extremely rapid product development cycle
  ⇒ security is not a priority
- No ongoing updates

```
POST /GetAlarmMsg/NVGetAlarmPostServerList?param=eyJkZXZfaWQiOjAsI... HTTP/1.0
Connection: Keep-Alive
Host: alarm1.nvdvr.cn:8888
Content-Length: 127

# {"dev_id":0,"key":"abc"}
```

Further work

- Investigate the unencrypted information being sent by the camera to the cloud service
- Investigate the variety of open ports, and what they’re used for
- Dump the root filesystem from the SPI flash
  - Use a raspberry pi, spidev and the datasheet for the 25L6406E
  - Find out how much control the cloud service has over the device
  - Identify whether the root password aka *manufacturer backdoor* is common to all devices (it almost certainly is)
  - HN thread with useful resources

Links

- AK3918E SoC datasheet
- 24C02N (2kbit EEPROM) datasheet and information
- 25L6406E (64Mbit Flash) datasheet

- Anyka website
- Macro-video website
- Banana Pi docs

Future meetups

We meet here once a month on Thursdays for a talk (sometimes) and a Capture-the-Flag challenge (always). Usually free.

Next meetup here, 22nd March.

http://sectalks.org/london
sectalks.slack.com -> email london@sectalks.org for an invite
Slides up at https://github.com/sectalks/sectalks