

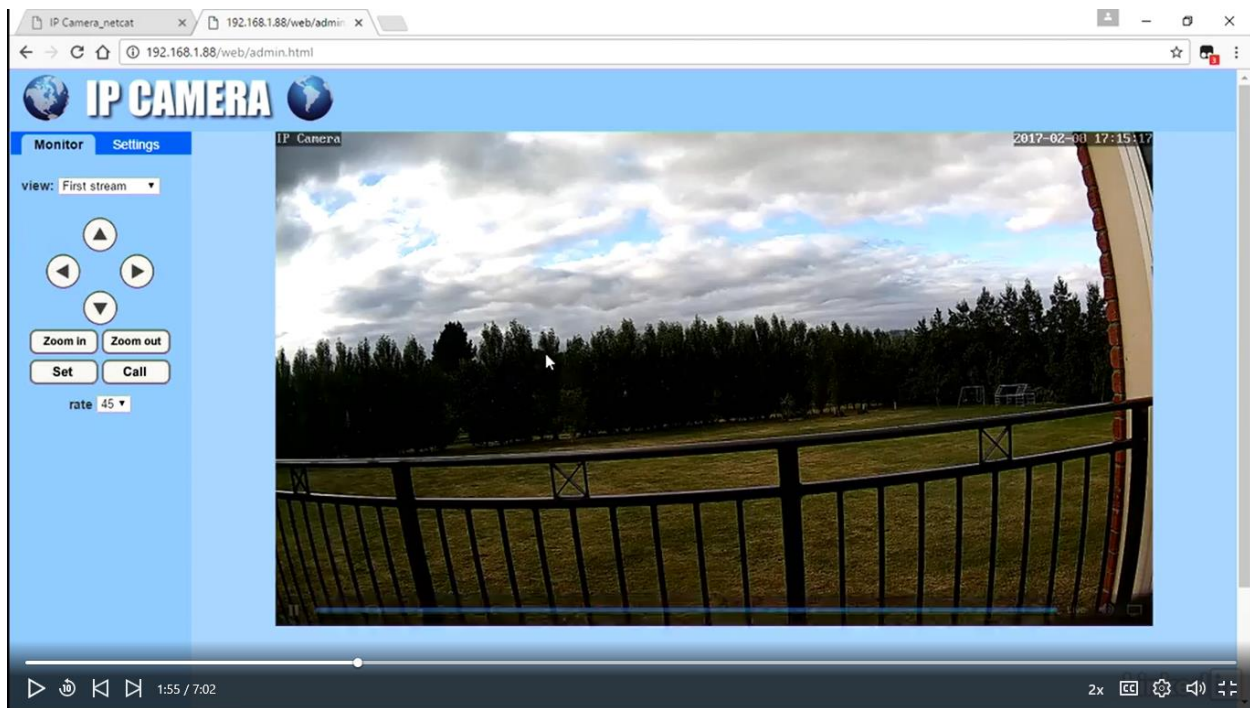
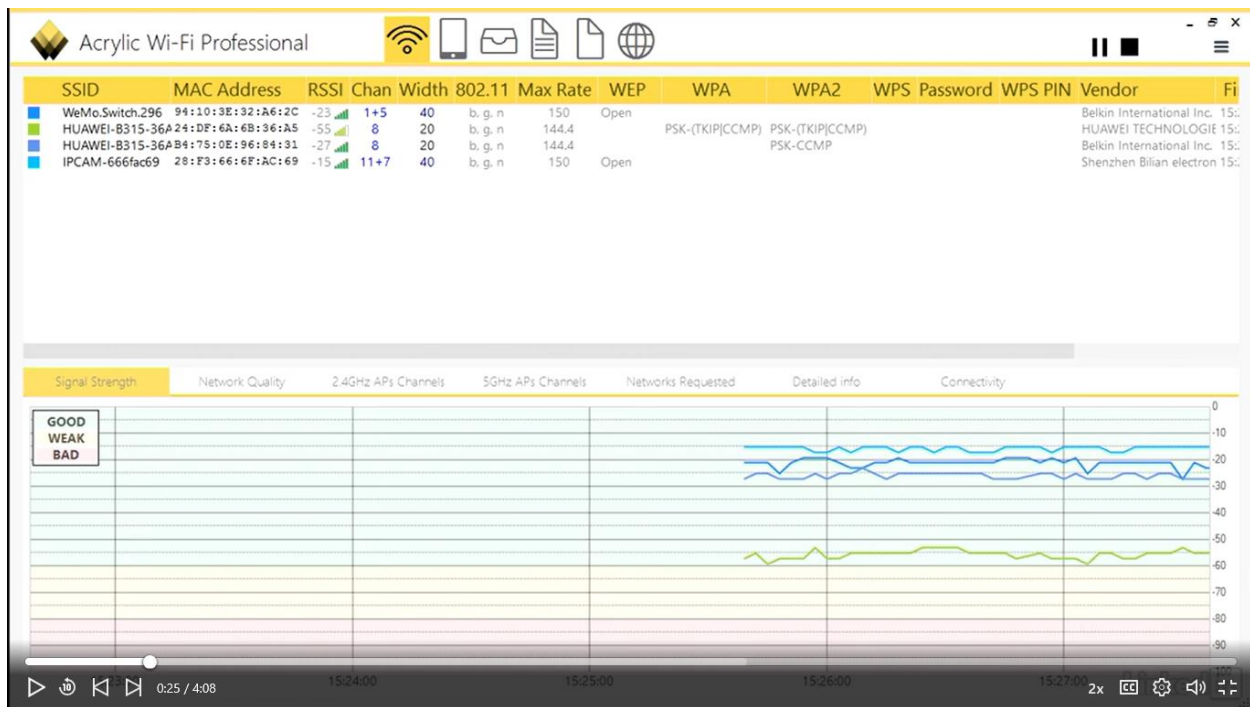
# HNAP

Is the

## Home Network Automation Protocol

0:22 / 8:43

2x CC Settings Audio Full Screen



杭州吉北电子科技 Broadlink X python-broadlink/protoc X Packet Capture - Androi X

GitHub, Inc. [US] | <https://github.com/mjg59/python-broadlink/blob/master/protocol.md>

Personal Open source Business Explore Pricing Blog Support This repository Search Sign in Sign up

mjg59 / python-broadlink Watch 47 Star 101 Fork 43

Code Issues 19 Pull requests 4 Projects 0 Pulse Graphs

Branch: master python-broadlink / protocol.md Find file Copy path

mjg59 Update documentation to cover RF packets 9257427 on Oct 31, 2016 1 contributor

135 lines (103 sloc) 4.43 KB Raw Blame History

## Broadlink RM2 network protocol

### Encryption

6-based encryption in CBC mode. The initial key is 0x09, 0x76, 0x28, 0x34, 0x3f, 0xe9, 0x9e, 0x23, 0x76, 0xac, 0xcf, 0x8b, 0x02. The IV is 0x56, 0x2e, 0x17, 0x99, 0x6d, 0x09, 0x3d, 0x28, 0xdd, 0xb3, 0xba, 0x69, 0x5a.

<https://goo.gl/sVVAHJ>


Network discovery 0:17 / 9:07 2x

杭州吉北电子科技 Broadlink X python-broadlink/protoc X Packet Capture - Androi X

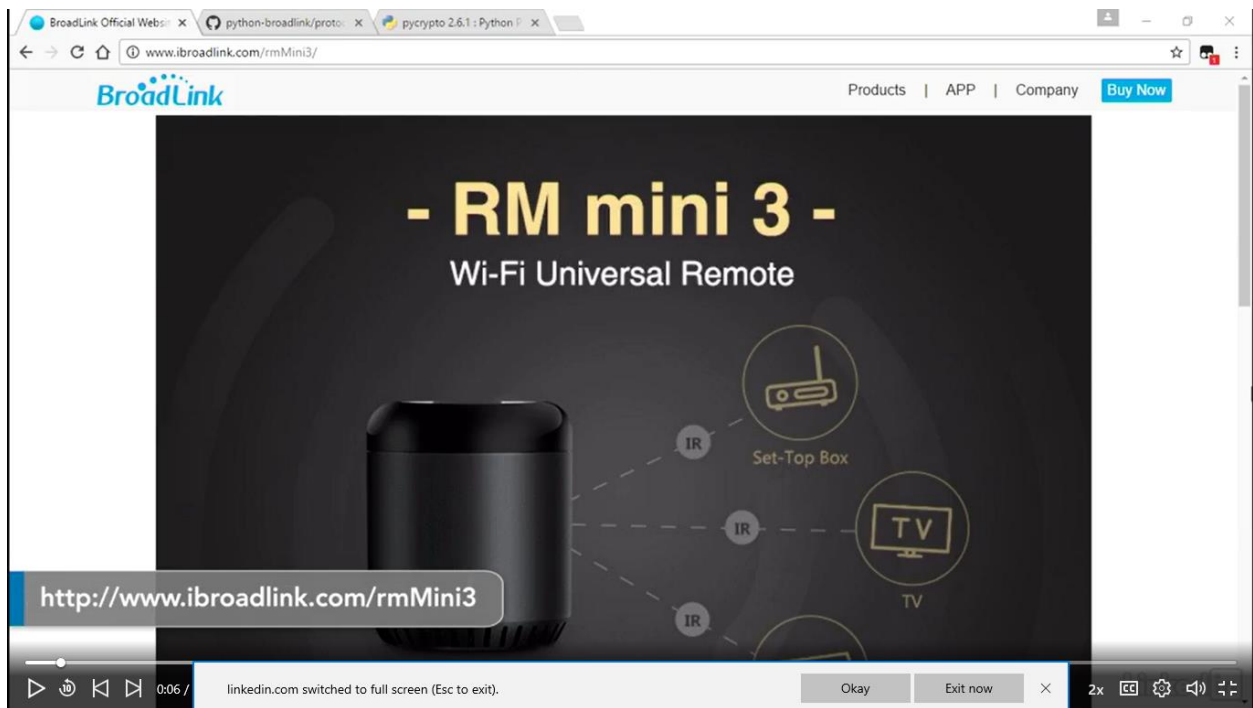
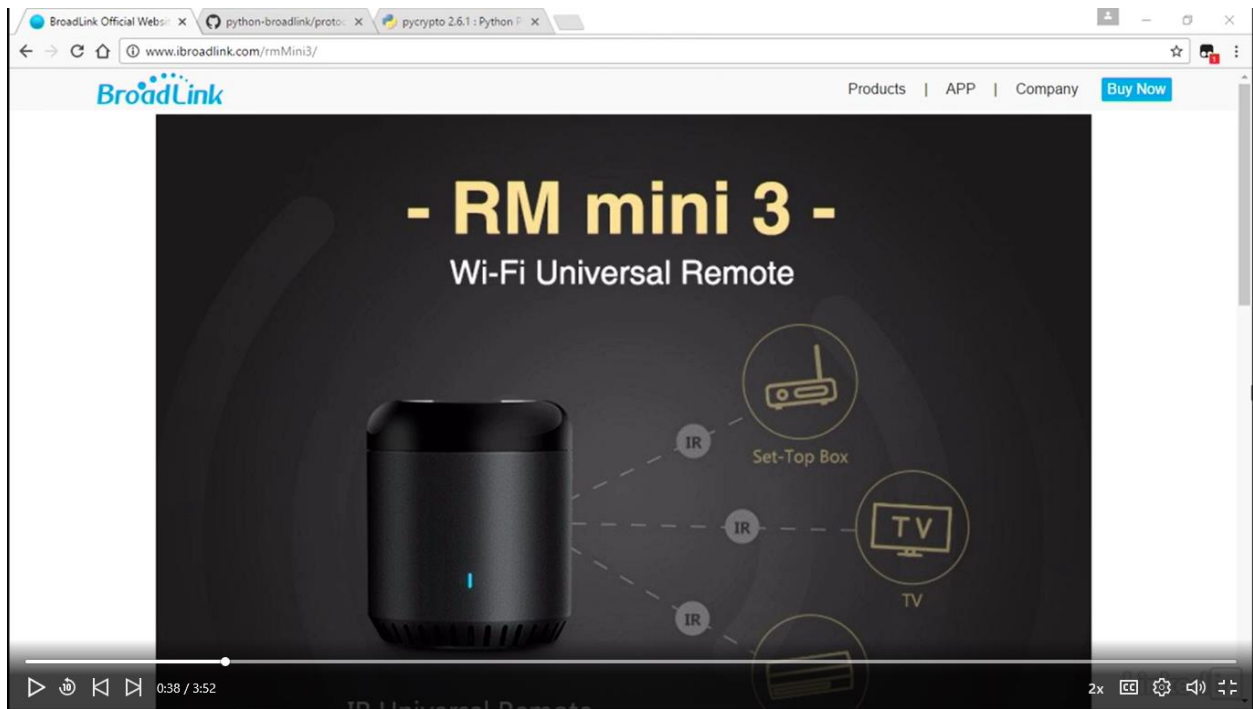
[www.ibroadlink.com](http://www.ibroadlink.com) Products APP Company Buy Now

# Throw Away Many Remote Redefine Your Home Life

Wi-Fi Smart Universal Remote RM Pro



0:14 / 9:07 RF Universal Remote Setting Timer Over 5000 kinds of appliances clouds 2x



BroadLink Official Website | python-broadlink/protocol | pycrypto 2.6.1 : Python

GitHub, Inc. [US] | <https://github.com/mjg59/python-broadlink/blob/master/protocol.md>

Personal Open source Business Explore Pricing Blog Support This repository Search Sign in Sign up

mjg59 / python-broadlink

Watch 47 Star 101 Fork 43

Code Issues 19 Pull requests 4 Projects 0 Pulse Graphs

Branch: master python-broadlink / protocol.md Find file Copy path

mjg59 Update documentation to cover RF packets 9257427 on Oct 31, 2016

1 contributor

135 lines (103 sloc) 4.43 KB Raw Blame History

## Broadlink RM2 network protocol

### Encryption

SHA256-based encryption in CBC mode. The initial key is 0x09, 0x76, 0x28, 0x34, 0x3f, 0xe9, 0x9e, 0x23, 0x76, 0xac, 0xcf, 0x8b, 0x02. The IV is 0x56, 0x2e, 0x17, 0x99, 0x6d, 0x09, 0x3d, 0x28, 0xdd, 0xb3, 0xba, 0x69, 0x5a.

<https://goo.gl/sVVAHJ>

Network discovery

3:00 / 3:52

2x CC

BroadLink Official Website | python-broadlink/protocol | pycrypto 2.6.1 : Python

Python Software Foundation [US] | <https://pypi.python.org/pypi/pycrypto>

python™

Package Index > pycrypto > 2.6.1

PACKAGE INDEX >>>

- Browse packages
- Package submission
- List trove classifiers
- RSS (latest 40 updates)
- RSS (newest 40 packages)
- PyPI Tutorial
- PyPI Security
- PyPI Support
- PyPI Bug Reports
- PyPI Discussion
- PyPI Developer Info

ABOUT >>>

NEWS >>>

DOCUMENTATION >>>

DOWNLOAD >>>

COMMUNITY >>>

FOUNDATION >>>

CORE DEVELOPMENT >>>

## pycrypto 2.6.1

Cryptographic modules for Python.

Package Documentation

### Python Cryptography Toolkit (pycrypto)

This is a collection of both secure hash functions (such as SHA256 and RIPEMD 160), and various encryption algorithms (AES, DES, RSA, ElGamal, etc.). The package is structured to make adding new modules easy. This section is essentially complete, and the software interface will almost certainly not change in an incompatible way in the future; all that remains to be done is to fix any bugs that show up. If you encounter a bug, please report it in the Launchpad bug tracker at <https://launchpad.net/products/pycrypto/+bugs>

An example usage of the SHA256 module is:

```
>>> from Crypto.Hash import SHA256
>>> hash = SHA256.new()
>>> hash.update('message')
>>> hash.digest()
'\xab5\x13\x13\xe4\xf1\x14\x98+y\xfb7\xe3\xfb\x94\xcf\xd1\xf3\xfb\xf7\x1c\xe8\x1a\xfb\xf0\xf0\x0c\x1d'
```

usage of an encryption algorithm (AES, in this case) is:

```
>>> from Crypto.Cipher import AES
>>> obj = AES.new('This is a key123', AES.MODE_CBC, 'This is an IV456')
>>> message = 'This is a message'
>>> ciphertext = obj.encrypt(message)
>>> ciphertext
'\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'
```

Download pycrypto-2.6.1.tar.gz

Not Logged In

- Login
- Register
- Lost Login?
- Use OpenID
- Login with Google

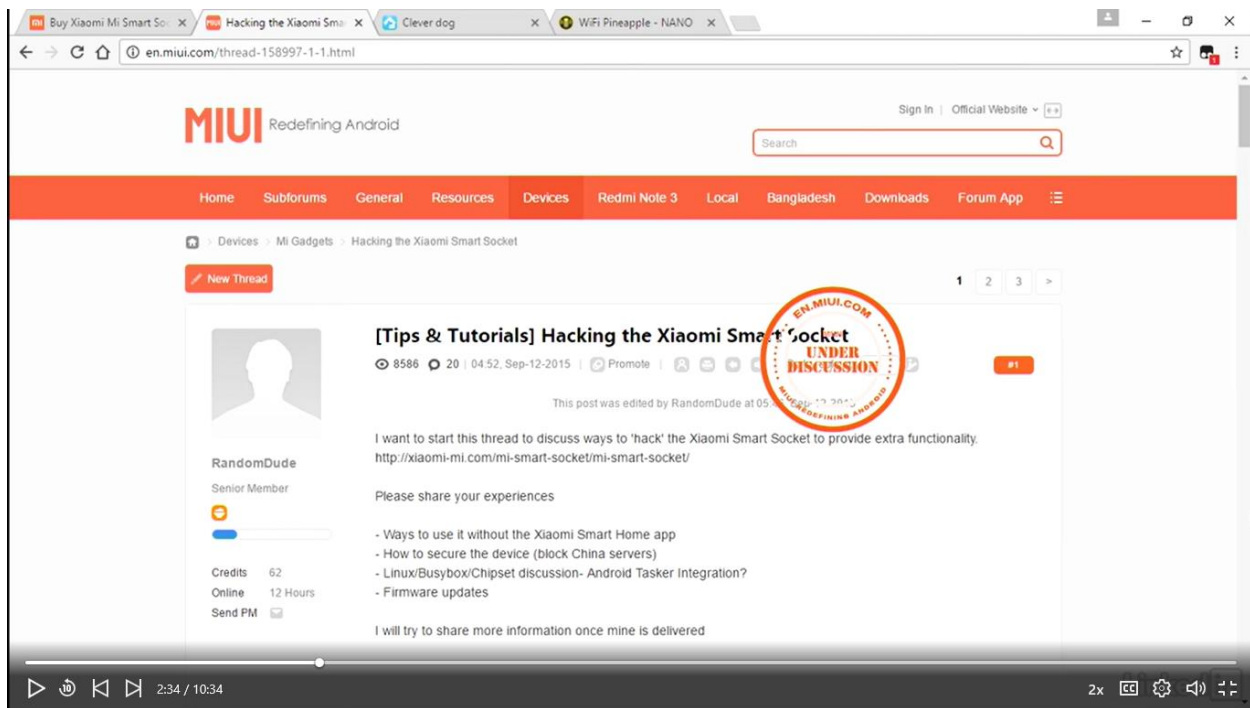
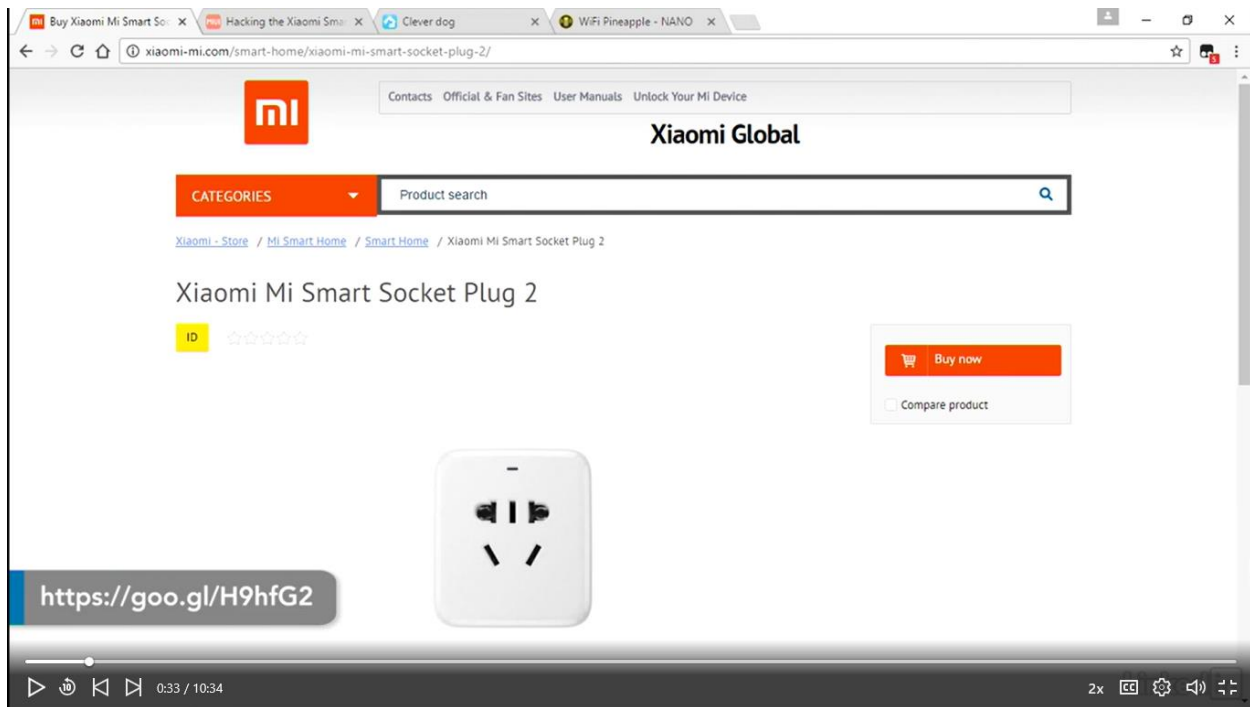
Status

- Nothing to report

<https://goo.gl/y0XHqn>

3:25 / 3:52

2x CC





Buy Xiaomi Mi Smart So... X Hacking the Xiaomi Smi... X Clever dog X WiFi Pineapple - NANO X

www.cleverdog.com.cn

Clever Dog

HOME Smart Camera Smart DoorBell Store Clever Dog News Service Centre 中文

# Clever Dog New Style

BLACK & GOLDEN – FROM CLASSIC

<http://www.cleverdog.com.cn>

在线咨询  
ONLINE CONSULTATION

2:38 / 10:34

2x

Buy Xiaomi Mi Smart So... Hacking the Xiaomi Smi... Clever dog WiFi Pineapple - NANO


Secure | https://wifipineapple.com/pages/nano

ABOUT US | HELP | LOGIN

HOME BLOG RESOURCES SUPPORT PORTAL

## The WiFi Pineapple NANO


Home / NANO



Hak5 is proud to introduce its 6th generation wireless network auditing tool – the WiFi Pineapple NANO.

Engineered from the ground up, The WiFi Pineapple NANO was first stripped to its core. Then building on the successes and feedback from its predecessors, we developed a platform centered around performance and usability.

[Purchase Now](#)



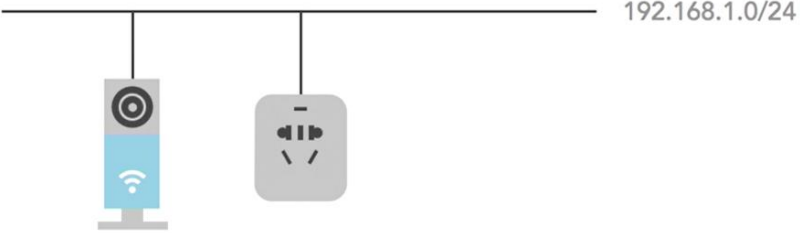
INTRODUCING THE  
WiFi Pineapple NANO

The end result is like nothing else that's come before. It isn't a simple client radio, nor just a router or access point. The WiFi Pineapple NANO is a powerful wireless network auditing tool that integrates its unique hardware and intuitive software to integrate with your current workflow.

Micro SD Storage Expansion  
Configurable Reset Button  
USB 2.0 Host Port  
Atheros AR9331 High Gain Radio

4:54 / 10:34

## Smart Devices



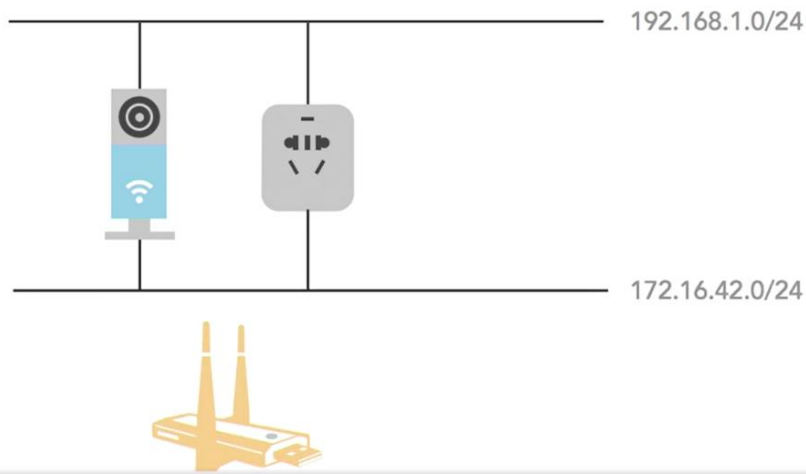
192.168.1.0/24

Aren't always easy to test!

5:14 / 10:34



# Network Interception



WiFi Pineapple

172.16.42.1:1471/#/modules/Recon

WiFi Pineapple

Dashboard

Recon

Profiling

Clients

Modules

Filters

PineAP

Tracking

Logging

Reporting

Networking

Configuration

Advanced

Help

Scan Settings

☐ Continuous

1 Minute

Scan

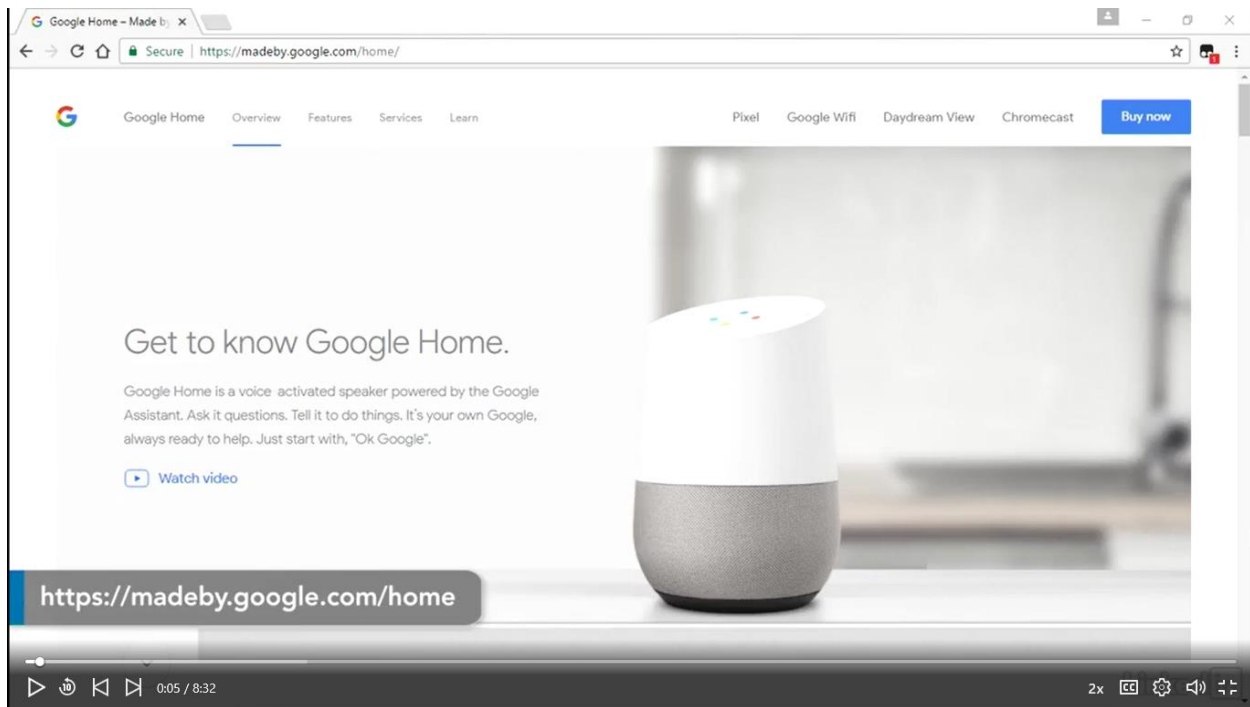
Scan Results

SSID	MAC	Security	WPS	Channel	Signal
HUAWEI-B315-36A5	24:DF:6A:6B:36:A5	Mixed WPA	no	8	-75
	B4:75:0E:96:84:31				
	E8:AB:FA:6C:3E:B1				
HUAWEI-B315-36A5	B4:75:0E:96:84:31	WPA2	yes	8	-58
	0C:D6:BD:46:D0:3E				
	28:6C:07:70:EC:0D				
	7C:11:BE:CB:25:C3				
	9C:B7:0D:42:DC:9E				

Unassociated Clients

# Capturing the Stream

```
ssh root@172.16.42.1 tcpdump -U -s0 -i br-lan -w - 'not port 22' | wireshark -k -i -
```



```
Command Prompt
C:\nmap>nmap -PS 192.168.1.134

Starting Nmap 7.31 ( https://nmap.org ) at 2017-03-09 07:48 AUS Eastern Daylight Time
Nmap scan report for 192.168.1.134
Host is up (0.0045s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
8008/tcp  open  http
8009/tcp  open  ajp13
10001/tcp open  scp-config
MAC Address: F4:F5:D8:D7:C2:68 (Google)

Nmap done: 1 IP address (1 host up) scanned in 21.08 seconds
C:\nmap>
```

0:58 / 8:32

2x CC

# Capturing the Stream

- `echo 1 > /proc/sys/net/ipv4/ip_forward`
- `arp spoof -i wlan0 -t 192.168.1.1 192.168.1.134`
- `arp spoof -i wlan0 -t 192.168.1.134 192.168.1.1`

GHOME.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 172.16.42.178

No.	Time	Source	Destination	Protocol	Length	Info
4121	38.784591	192.168.1.134	172.217.25.142	TCP	1434	[TCP segment of a reassembled PDU]
4123	38.785127	192.168.1.134	172.217.25.142	TCP	1434	[TCP segment of a reassembled PDU]
4125	38.785196	192.168.1.134	172.217.25.142	TLSv1.2	796	Application Data
4128	38.790135	172.217.25.142	192.168.1.134	TCP	66	443 → 55812 [ACK] Seq=11154 Ack=8798 Win=794 Len=0 TSval=3253710068 TSecr=195387
4129	38.797153	192.168.1.134	172.217.25.142	TCP	1434	[TCP segment of a reassembled PDU]
4131	38.797288	192.168.1.134	172.217.25.142	TCP	1434	[TCP segment of a reassembled PDU]
4133	38.797317	192.168.1.134	172.217.25.142	TLSv1.2	797	Application Data
4135	38.797336	192.168.1.134	172.217.25.142	TLSv1.2	247	Application Data
4137	38.799879	192.168.1.134	172.217.25.142	TLSv1.2	251	Application Data
4140	38.850056	172.217.25.142	192.168.1.134	TCP	66	443 → 55821 [ACK] Seq=2843 Ack=36221 Win=131072 Len=0 TSval=972485054 TSecr=195393
4141	38.853018	192.168.1.134	172.217.25.142	TCP	1434	[TCP segment of a reassembled PDU]
4143	38.853097	192.168.1.134	172.217.25.142	TCP	1434	[TCP segment of a reassembled PDU]
4146	38.878186	172.217.25.142	192.168.1.134	TCP	66	443 → 55821 [ACK] Seq=2843 Ack=39687 Win=137984 Len=0 TSval=972485080 TSecr=195397
4148	38.878789	172.217.25.142	192.168.1.134	TCP	66	443 → 55821 [ACK] Seq=2843 Ack=43335 Win=147712 Len=0 TSval=972485081 TSecr=195399

Header Length: 32 bytes

Flags: 0x010 (ACK)

Window size value: 311

[Calculated window size: 19904]

[Window size scaling factor: 64]

Checksum: 0x11e7 [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps

Options: (NOP)

Options: (NOP)

Options: Timestamps: TSval 195397, TSecr 972484951

0000 44 6d 57 4f 75 6e f4 f5 d8 d7 c2 68 00 00 45 00 DmWUn...h..E.

0010 05 0c 79 9e 40 00 40 06 33 38 c0 a8 01 86 ac d9 ..y.8.38.....

0020 19 8e da 0d 01 bb 48 34 19 4d 40 50 4d fc 80 10 .....M4.M8PM...

0030 01 37 11 e7 00 00 01 01 08 0a 00 02 fb 45 39 f6 .7.....E9.

0040 f1 57 17 03 03 0d 85 d3 22 81 15 21 5c 13 c3 44 .W.....!\\.D

0050 f9 58 0c 21 24 7f 6d 1b e9 91 9c 3f 3b a6 6a .X.1\$.m. ...?;.j

0060 f5 d1 48 c0 ee 4e 9a 9e 4a 3e fa a9 67 73 c9 01 ..H..N..>..gs..

0070 d8 a7 e9 67 87 74 d6 9c 74 aa 80 52 5a 95 6f d2 ...g.t...t..RZ.o.

0080 8e 05 c3 b0 a0 08 00 3c a3 0a 4c 6c 07 f4 c1 64 .e...t...N..

0090 d0 38 8b b1 40 b4 5c 87 dc b3 a0 f6 57 1e 29 a3 .8....N..

3:01 / 8:32

Packets: 12272 - Displayed: 6073 (49.5%) - Load time: 0:0.215 - Profile: Default

