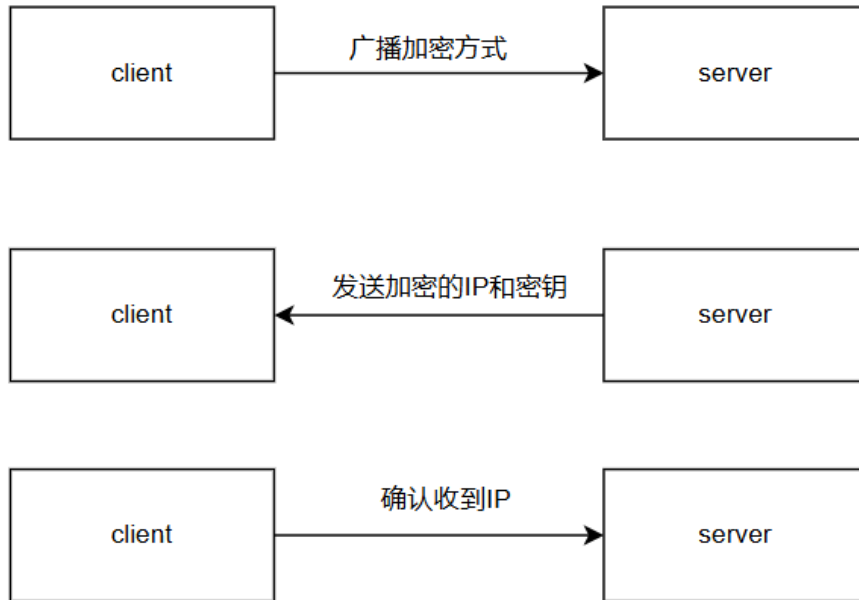


Write up

802.11 帧数据交换如下：



进入 pack, 通过 SSID 发现给予的提示, 即字符加'A' (0x41):

029 4.516420949	02:5e:ca:00:30:98 (- 802.11)	50 Acknowledgement, Flags=.....L
630 4.516611128	fe:48:2a:e6:bb:c7 Intel_aa:e3:26	802.11 118 Beacon frame, SN=0, FN=0, Flags=....., BI=100, SSID="plusA"
631 4.517821024	fe:48:2a:e6:bb:c7 Intel_aa:e3:26	802.11 118 Beacon frame, SN=0, FN=0, Flags=....., BI=100, SSID="plusA"
632 4.519506194	fe:48:2a:e6:bb:c7 Intel_aa:e3:26	802.11 118 Beacon frame, SN=0, FN=0, Flags=....., BI=100, SSID="plusA"
633 4.521072795	fe:48:2a:e6:bb:c7 Intel_aa:e3:26	802.11 118 Beacon frame, SN=0, FN=0, Flags=....., BI=100, SSID="plusA"
634 4.529374478	fe:48:2a:e6:bb:c7 Intel_aa:e3:26	802.11 123 Beacon frame, SN=0, FN=0, Flags=....., BI=100, SSID="plusA"

在 plusA 的帧内, 有一个标记为 null 的字段:

```
> Extended Capabilities: 0x75 (octet 8)
  Tag: Vendor Specific: (null)
    Tag Number: Vendor Specific (221)
    Tag length: 32
    OUI: 39:73:32
    Vendor Specific OUI Type: 50
    Vendor Specific Data: 323232333536353400494234714a4467694e694d35497945724d673d3d
```

该字段存在 base64:

0000	00 00 08 00 00 00 00 00	80 00 00 00 50 e0 85 aaP...
0010	e3 26 fe 48 2a e6 bb c7	fe 48 2a e6 bb c7 00 00	..&H*...H*....
0020	00 00 00 00 00 00 00 00	64 00 11 00 00 05 70 6cd....pl
0030	75 73 41 01 04 82 84 8b	96 03 01 05 bf 0c fa 79	usA.....y
0040	9b 33 fa ff 00 00 00 00	00 00 7f 08 fb eb 83 7a	..3.....z
0050	9c 8f 9e 75 dd 20 39 73	32 32 32 33 35 36 35	...u. 9s 22223565
0060	34 00 49 42 34 71 4a 44	67 69 4e 69 4d 35 49 79	4IB4qJD giNiM5Iy
0070	45 72 4d 67 3d 3d		ErMg==

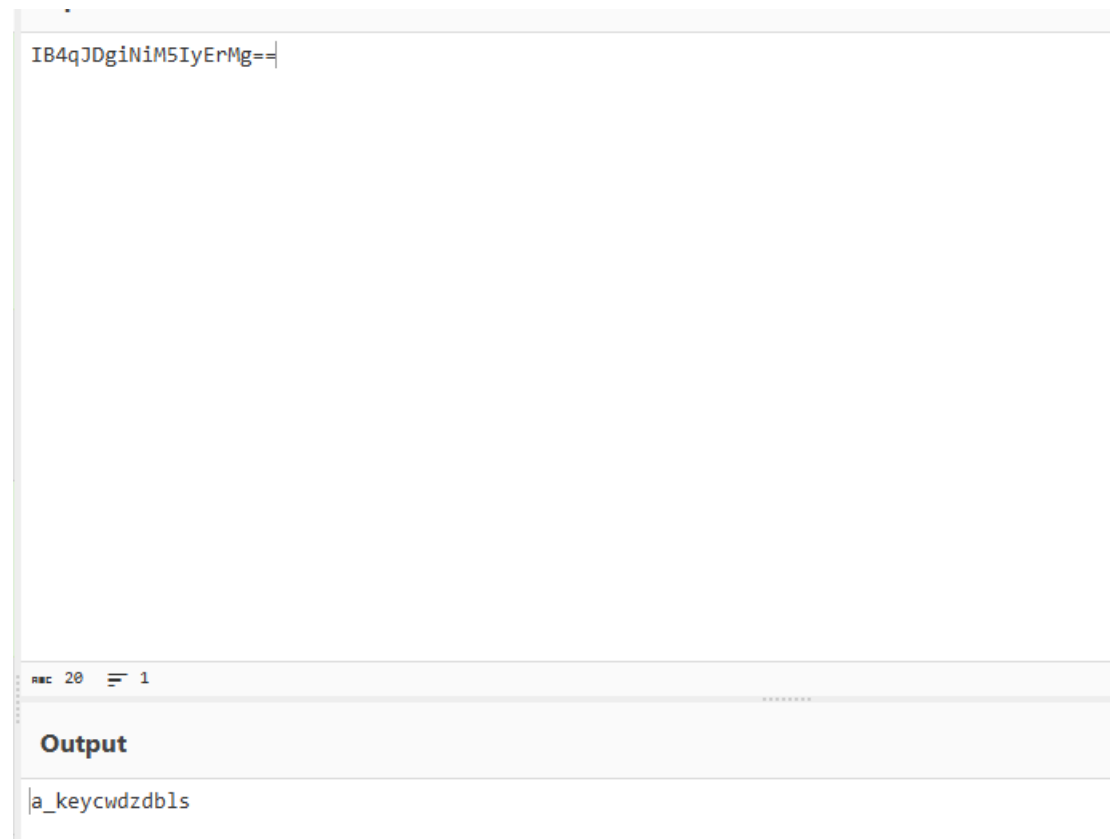
把 base64 解开：

IB4qJDgiNiM5IyErMg==

Output

RS*\$8"6#9#+2

用上 ssid 给予的提示，加上'A'：

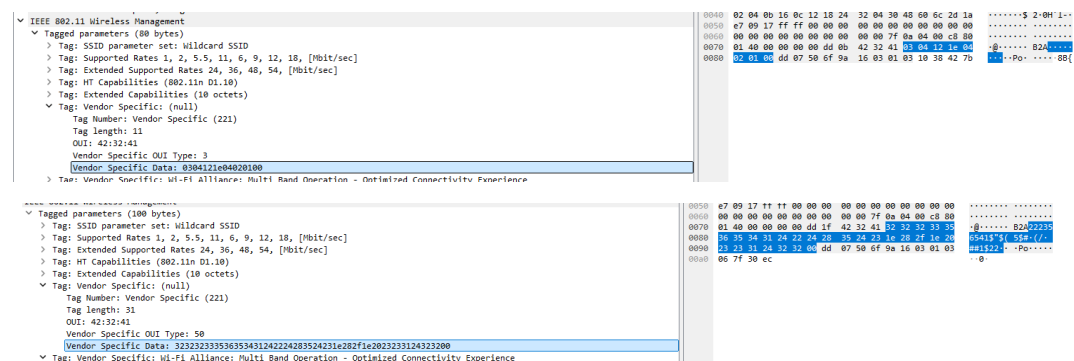


得到一个 key ：“cwndzdbls”

plusA 帧发给指定 mac 地址 intel_aa:e3:26:

628	4.516090611	02:5e:cf:08:36:98	BilianElectr_d2:f3:...	802.11	66	QoS Null function (No data), SN=2892, FN=0, Flags=.....TC
629	4.516420949	02:5e:cf:08:36:98	02:5e:cf:08:36:98	802.11	50	Acknowledgement, Flags=.....C
630	4.516611128	fe:48:2a:e6:bb:c7	Intel_aa:e3:26	802.11	118	Beacon frame, SN=0, FN=0, Flags=....., BI=100, SSID="plusA"
631	4.517821024	fe:48:2a:e6:bb:c7	Intel_aa:e3:26	802.11	118	Beacon frame, SN=0, FN=0, Flags=....., BI=100, SSID="plusA"
632	4.519506194	fe:48:2a:e6:bb:c7	Intel_aa:e3:26	802.11	118	Beacon frame, SN=0, FN=0, Flags=....., BI=100, SSID="plusA"
633	4.521072795	fe:48:2a:e6:bb:c7	Intel_aa:e3:26	802.11	118	Beacon frame, SN=0, FN=0, Flags=....., BI=100, SSID="plusA"
634	4.529374478	fe:48:2a:e6:bb:c7	Intel_aa:e3:26	802.11	123	Beacon frame, SN=0, FN=0, Flags=....., BI=100, SSID="plusA"
635	4.532621412	02:5e:cf:08:36:98	BilianElectr_d2:f3:...	802.11	66	QoS Null function (No data), SN=2893, FN=0, Flags=...P...TC

查看 intel_aa:e3:26 向外广播的帧。所有帧的 vendor specific 字段皆被标记为 null，有两种不同的 vendor specific 内容：



处理第一种，对 vendor specific 字段数据加'A'，得到加密方式 DES_ECB:

Input

0304121e040201

REC 14 1 14

Output

DES_ECB

对第二种的 vendor specific 字段数据加'A'，得到信息 intel_aa:e3:26 已收到某个 IP 地址：



查看帧发送顺序并总结已知信息：

1. intel_aa:e3:26 先向外广播加密方式 DES_ECB。
2. plusA 向 intel_aa:e3:26 发送密钥"cwdzdbls"和其他数据。
3. intel_aa:e3:26 广播收到 IP 地址。

根据 DES_ECB 密钥为八字节，加密输出结果为八字节的倍数，再次分析 plusA 数据包，并发现刚好有一个字段为 8 字节：

```
> IEEE 802.11 Beacon frame, Flags: .....
▼ IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  ▼ Tagged parameters (74 bytes)
    > Tag: SSID parameter set: "plusA"
    > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 6
    > Tag: VHT Capabilities
    ▼ Tag: Extended Capabilities (8 octets)
      Tag Number: Extended Capabilities (127)
      Tag length: 8
      > Extended Capabilities: 0xfb (octet 1)
      > Extended Capabilities: 0xeb (octet 2)
      > Extended Capabilities: 0x83 (octet 3)
      > Extended Capabilities: 0x7a (octet 4)
      > Extended Capabilities: 0x9c (octet 5)
      > Extended Capabilities: 0x8f (octet 6)
      > Extended Capabilities: 0x9e (octet 7)
      > Extended Capabilities: 0x75 (octet 8)
    > Tag: Vendor Specific: (null)
```

对该字段进行 DES_ECB 解密，得到一个 ip 地址，16 进制为 192.168.72.128：

Input

fbeb837a9c8f9e75

Output

c0a8488d

查看下方 udp 包，提取发向 192.168.72.128 的 udp 包 data：

898	19393.223207	10.255.8.25	192.168.72.122	UDP	74	56406 → 9732	Len=32
899	19393.223560	10.255.8.25	192.168.72.121	UDP	74	56407 → 9732	Len=32
900	19393.223631	10.255.8.25	192.168.72.128	UDP	82	56408 → 9732	Len=40
901	19393.223602	10.255.8.25	192.168.72.130	UDP	74	56410 → 9732	Len=32
902	19393.223738	10.255.8.25	192.168.72.122	UDP	74	56409 → 9732	Len=32
903	19393.224053	10.255.8.25	192.168.72.133	UDP	82	56411 → 9732	Len=40
904	19393.224114	10.255.8.25	192.168.72.132	UDP	82	56412 → 9732	Len=40
905	19393.224420	10.255.8.25	192.168.72.139	UDP	82	56413 → 9732	Len=40
906	19393.224500	10.255.8.25	192.168.72.124	UDP	82	56414 → 9732	Len=40
907	19393.224553	10.255.8.25	192.168.72.132	UDP	66	56415 → 9732	Len=24
908	19393.224601	10.255.8.25	192.168.72.127	UDP	82	56416 → 9732	Len=40
909	19393.224933	10.255.8.25	192.168.72.129	UDP	82	56418 → 9732	Len=40
910	19393.225054	10.255.8.25	192.168.72.136	UDP	66	56417 → 9732	Len=24
911	19393.225120	10.255.8.25	192.168.72.124	UDP	66	56420 → 9732	Len=24
912	19393.225219	10.255.8.25	192.168.72.128	UDP	82	56419 → 9732	Len=40
913	19393.225363	10.255.8.25	192.168.72.138	UDP	74	56421 → 9732	Len=32
914	19393.226213	10.255.8.25	192.168.72.139	UDP	74	56422 → 9732	Len=32
915	19393.226274	10.255.8.25	192.168.72.120	UDP	82	56423 → 9732	Len=40
916	19393.226328	10.255.8.25	192.168.72.139	UDP	82	56424 → 9732	Len=40
917	19393.226372	10.255.8.25	192.168.72.133	UDP	66	56425 → 9732	Len=24
918	19393.226418	10.255.8.25	192.168.72.131	UDP	74	56426 → 9732	Len=32

> Frame 900: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF_{A51EEC43-20B4-4491-AD03-AE67768F903B},
> Ethernet II, Src: Dell_ba:ci:4b (00:be:43:ba:ci:4b), Dst: HuaweiTechno_e1:26:7a (84:3e:92:e1:26:7a)
> Internet Protocol Version 4, Src: 10.255.8.25, Dst: 192.168.72.128
> User Datagram Protocol, Src Port: 56408, Dst Port: 9732
▼ Data (40 bytes)
Data: 681dea78518fbc5b7191bd393a8c9aafdc049c3165997d8a99808ec670807c7f8456f14ac2e12f04

0000 84 3e 92 e1 26 7a 00 be 43 ba c1 4b 08 00 45 00 >...&z...C..K..E:
0010 00 44 a1 e3 00 00 00 11 00 00 0a ff 00 19 c0 ad D.....
0020 48 80 dc 58 26 04 00 30 33 b0 58 1d ea 78 51 01 H..X&..0 3.....
0030 bc 5b 71 91 bd 39 3a 8c 9a af dc 04 9c 31 65 99 [q..9!.....l&
0040 fd 8a 09 85 8c c6 c0 80 2c 7f 84 56 f1 40 c2 e1p.....
0050 2f 84

根据提示，对 data 进行 DES_ECB 解密，再用获取到 IP 的 Extended Capabilities 字段的 Tag number（127）进行异或，得到 flag{4nt1y_c3rt_Apt_@n41y51s_gr0up}：

Input

681dea78518fbc5b7191bd393a8c9aafdc849c3165997d8a89880ec670807c7f8456f14ac2e12f04|

REC 80 1

Tr R

Output

flag{4nt1y_c3rt_Apt_@n41y51s_gr0up}|