Description

Someone might have hidden the password in the trace file.Find the key to unlock this file. This tracefile might be good to analyze.

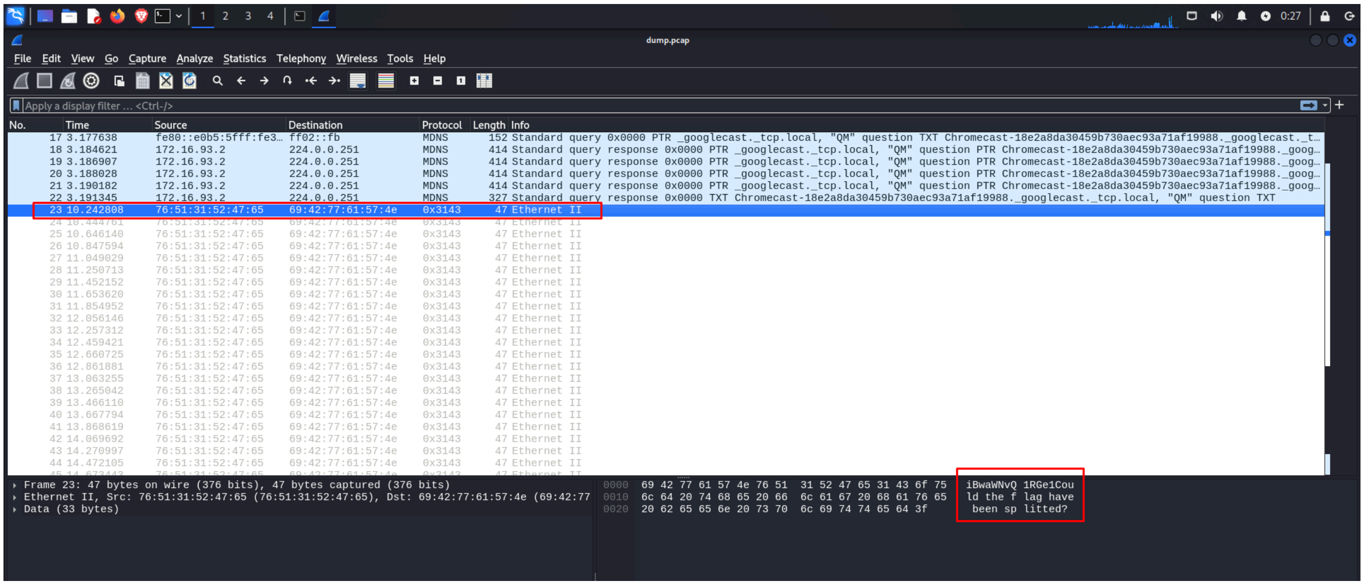
Hints

- Download the pcap and look for the password or flag.
- Don't try to use a password cracking tool, there are easier ways here.

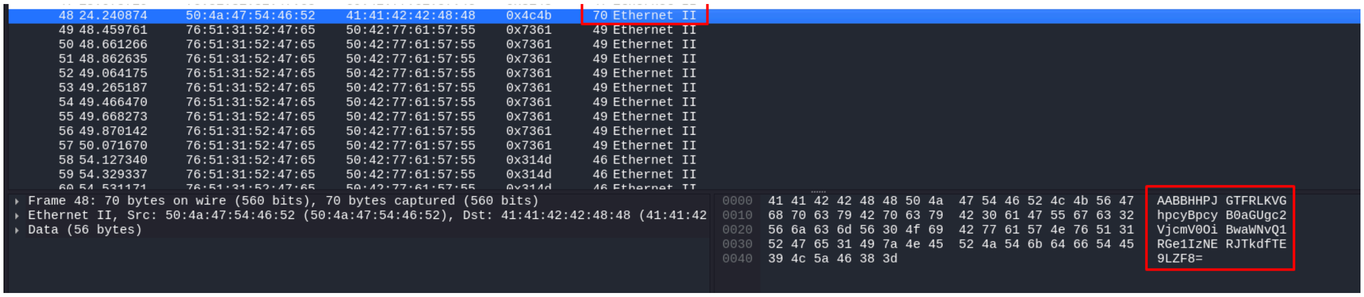
Solución

```
┌──(kali㉿kali)-
[~/…/parciales/parcial_02/parte_03_forensic_01/find_and_open]
└─$ wget https://artifacts.picoctf.net/c/496/flag.zip
--2024-11-06 01:23:29--  https://artifacts.picoctf.net/c/496/flag.zip
Resolving artifacts.picoctf.net (artifacts.picoctf.net)... 3.161.55.64,
3.161.55.26, 3.161.55.61, ...
Connecting to artifacts.picoctf.net
(artifacts.picoctf.net)|3.161.55.64|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 231 [application/octet-stream]
Saving to: ‘flag.zip’

flag.zip               100%[===========================>]     231  --.-KB/s
in 0s

2024-11-06 01:23:30 (113 MB/s) - ‘flag.zip’ saved [231/231]


┌──(kali㉿kali)-
[~/…/parciales/parcial_02/parte_03_forensic_01/find_and_open]
└─$ wget https://artifacts.picoctf.net/c/496/dump.pcap
--2024-11-06 01:23:38--  https://artifacts.picoctf.net/c/496/dump.pcap
Resolving artifacts.picoctf.net (artifacts.picoctf.net)... 3.161.55.100,
3.161.55.61, 3.161.55.26, ...
Connecting to artifacts.picoctf.net
(artifacts.picoctf.net)|3.161.55.100|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7413 (7.2K) [application/octet-stream]
Saving to: ‘dump.pcap’

dump.pcap              100%[===========================>]   7.24K  --.-KB/s
```

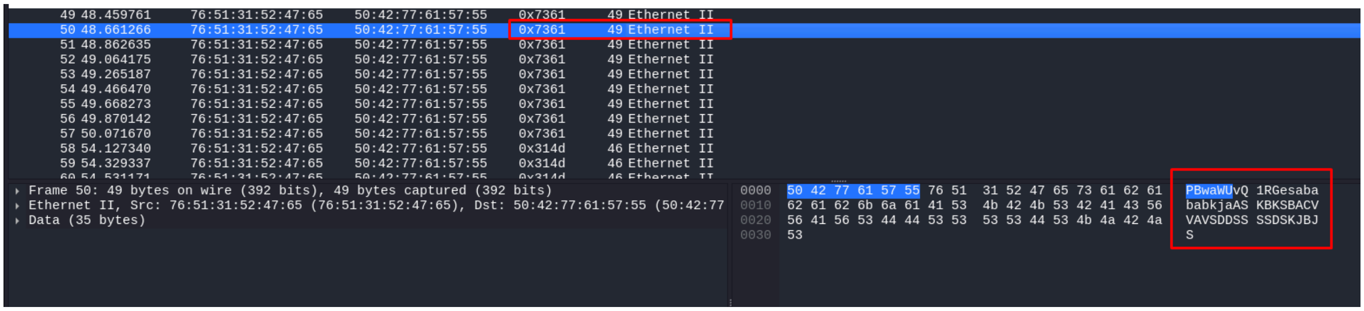
```
in 0.001s

2024-11-06 01:23:39 (4.96 MB/s) - ‘dump.pcap’ saved [7413/7413]


┌──(kali㉿kali)-
[~/…/parciales/parcial_02/parte_03_forensic_01/find_and_open]
└─$ ls
dump.pcap  find-and-open.md  flag.zip

┌──(kali㉿kali)-
[~/…/parciales/parcial_02/parte_03_forensic_01/find_and_open]
└─$ wireshark dump.pcap &
[1] 44330

┌──(kali㉿kali)-
[~/…/parciales/parcial_02/parte_03_forensic_01/find_and_open]
└─$ unzip flag.zip
Archive:  flag.zip
[flag.zip] flag password:
```


dump.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time       Source                  Destination          Protocol Length Info
   17 3.177638   fe80::e0b5:5fff:fe3…    ff02::fb             MDNS     152 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question TXT Chromecast-18e2a8da30459b730aec93a71af19988._googlecast._t…
   18 3.184621   172.16.93.2             224.0.0.251          MDNS     414 Standard query response 0x0000 PTR _googlecast._tcp.local, "QM" question PTR Chromecast-18e2a8da30459b730aec93a71af19988._goog…
   19 3.186907   172.16.93.2             224.0.0.251          MDNS     414 Standard query response 0x0000 PTR _googlecast._tcp.local, "QM" question PTR Chromecast-18e2a8da30459b730aec93a71af19988._goog…
   20 3.188028   172.16.93.2             224.0.0.251          MDNS     414 Standard query response 0x0000 PTR _googlecast._tcp.local, "QM" question PTR Chromecast-18e2a8da30459b730aec93a71af19988._goog…
   21 3.190182   172.16.93.2             224.0.0.251          MDNS     414 Standard query response 0x0000 PTR _googlecast._tcp.local, "QM" question PTR Chromecast-18e2a8da30459b730aec93a71af19988._goog…
   22 3.191345   172.16.93.2             224.0.0.251          MDNS     327 Standard query response 0x0000 TXT Chromecast-18e2a8da30459b730aec93a71af19988._googlecast._tcp.local, "QM" question TXT
   23 10.242808  76:51:31:52:47:65       69:42:77:61:57:4e    0x3143    47 Ethernet II
   24 10.444761  76:51:31:52:47:65       69:42:77:61:57:4e    0x3143    47 Ethernet II
   25 10.646140  76:51:31:52:47:65       69:42:77:61:57:4e    0x3143    47 Ethernet II
   26 10.847594  76:51:31:52:47:65       69:42:77:61:57:4e    0x3143    47 Ethernet II
   27 11.049029  76:51:31:52:47:65       69:42:77:61:57:4e    0x3143    47 Ethernet II
   28 11.250713  76:51:31:52:47:65       69:42:77:61:57:4e    0x3143    47 Ethernet II
   29 11.452152  76:51:31:52:47:65       69:42:77:61:57:4e    0x3143    47 Ethernet II
   30 11.653620  76:51:31:52:47:65       69:42:77:61:57:4e    0x3143    47 Ethernet II
   31 11.854952  76:51:31:52:47:65       69:42:77:61:57:4e    0x3143    47 Ethernet II
   32 12.056146  76:51:31:52:47:65       69:42:77:61:57:4e    0x3143    47 Ethernet II
   33 12.257312  76:51:31:52:47:65       69:42:77:61:57:4e    0x3143    47 Ethernet II
   34 12.459421  76:51:31:52:47:65       69:42:77:61:57:4e    0x3143    47 Ethernet II
   35 12.660725  76:51:31:52:47:65       69:42:77:61:57:4e    0x3143    47 Ethernet II
   36 12.861881  76:51:31:52:47:65       69:42:77:61:57:4e    0x3143    47 Ethernet II
   37 13.063255  76:51:31:52:47:65       69:42:77:61:57:4e    0x3143    47 Ethernet II
   38 13.265042  76:51:31:52:47:65       69:42:77:61:57:4e    0x3143    47 Ethernet II
   39 13.466110  76:51:31:52:47:65       69:42:77:61:57:4e    0x3143    47 Ethernet II
   40 13.667794  76:51:31:52:47:65       69:42:77:61:57:4e    0x3143    47 Ethernet II
   41 13.868619  76:51:31:52:47:65       69:42:77:61:57:4e    0x3143    47 Ethernet II
   42 14.069692  76:51:31:52:47:65       69:42:77:61:57:4e    0x3143    47 Ethernet II
   43 14.270997  76:51:31:52:47:65       69:42:77:61:57:4e    0x3143    47 Ethernet II
   44 14.472105  76:51:31:52:47:65       69:42:77:61:57:4e    0x3143    47 Ethernet II

› Frame 23: 47 bytes on wire (376 bits), 47 bytes captured (376 bits)
› Ethernet II, Src: 76:51:31:52:47:65 (76:51:31:52:47:65), Dst: 69:42:77:61:57:4e (69:42:77
› Data (33 bytes)

0000  69 42 77 61 57 4e 76 51  31 52 47 65 31 43 6f 75   iBwaWNvQ 1RGe1Cou
0010  6c 64 20 74 68 65 20 66  6c 61 67 20 68 61 76 65   ld the f lag have
0020  20 62 65 65 6e 20 73 70  6c 69 74 74 65 64 3f       been sp litted?
```



```
   48 24.240874  50:4a:47:54:46:52  41:41:42:42:48:48  0x4c4b  70 Ethernet II
   49 48.459761  76:51:31:52:47:65  50:42:77:61:57:55  0x7361  49 Ethernet II
   50 48.661266  76:51:31:52:47:65  50:42:77:61:57:55  0x7361  49 Ethernet II
   51 48.862635  76:51:31:52:47:65  50:42:77:61:57:55  0x7361  49 Ethernet II
   52 49.064175  76:51:31:52:47:65  50:42:77:61:57:55  0x7361  49 Ethernet II
   53 49.265187  76:51:31:52:47:65  50:42:77:61:57:55  0x7361  49 Ethernet II
   54 49.466470  76:51:31:52:47:65  50:42:77:61:57:55  0x7361  49 Ethernet II
   55 49.668273  76:51:31:52:47:65  50:42:77:61:57:55  0x7361  49 Ethernet II
   56 49.870142  76:51:31:52:47:65  50:42:77:61:57:55  0x7361  49 Ethernet II
   57 50.071670  76:51:31:52:47:65  50:42:77:61:57:55  0x7361  49 Ethernet II
   58 54.127340  76:51:31:52:47:65  50:42:77:61:57:55  0x314d  46 Ethernet II
   59 54.329337  76:51:31:52:47:65  50:42:77:61:57:55  0x314d  46 Ethernet II

› Frame 48: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
› Ethernet II, Src: 50:4a:47:54:46:52 (50:4a:47:54:46:52), Dst: 41:41:42:42:48:48 (41:41:42
› Data (56 bytes)

0000  41 41 42 42 48 48 50 4a  47 54 46 52 4c 4b 56 47   AABBHHPJ GTFRLKVG
0010  68 70 63 79 42 70 63 79  42 30 61 47 55 67 63 32   hpcyBpcy B0aGUgc2
0020  56 6a 63 6d 56 30 4f 69  42 77 61 57 4e 76 51 31   VjcmV0Oi BwaWNvQ1
0030  52 47 65 31 49 7a 4e 45  52 4a 54 6b 64 66 54 45   RGe1IzNE RJTkdfTE
0040  39 4c 5a 46 38 3d                                  9LZF8=
```

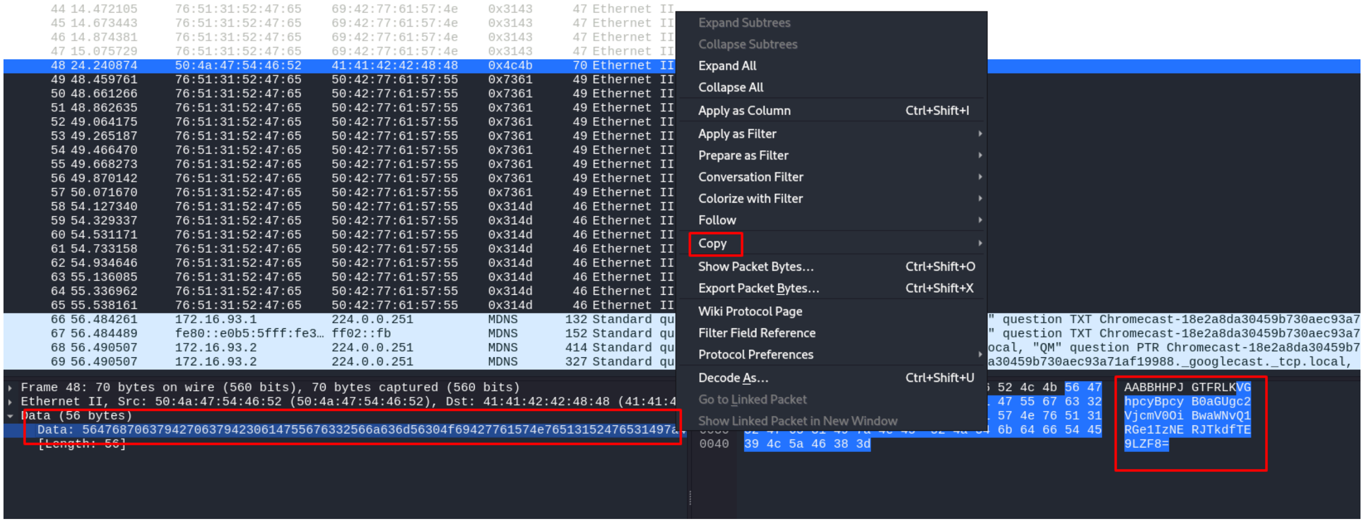


```
49 48.459761   76:51:31:52:47:65   50:42:77:61:57:55   0x7361   49 Ethernet II
50 48.661266   76:51:31:52:47:65   50:42:77:61:57:55   0x7361   49 Ethernet II
51 48.862635   76:51:31:52:47:65   50:42:77:61:57:55   0x7361   49 Ethernet II
52 49.064175   76:51:31:52:47:65   50:42:77:61:57:55   0x7361   49 Ethernet II
53 49.265187   76:51:31:52:47:65   50:42:77:61:57:55   0x7361   49 Ethernet II
54 49.466470   76:51:31:52:47:65   50:42:77:61:57:55   0x7361   49 Ethernet II
55 49.668273   76:51:31:52:47:65   50:42:77:61:57:55   0x7361   49 Ethernet II
56 49.870142   76:51:31:52:47:65   50:42:77:61:57:55   0x7361   49 Ethernet II
57 50.071670   76:51:31:52:47:65   50:42:77:61:57:55   0x7361   49 Ethernet II
58 54.127340   76:51:31:52:47:65   50:42:77:61:57:55   0x314d   46 Ethernet II
59 54.329337   76:51:31:52:47:65   50:42:77:61:57:55   0x314d   46 Ethernet II
60 54.531171   76:51:31:52:47:65   50:42:77:61:57:55   0x314d   46 Ethernet II
```

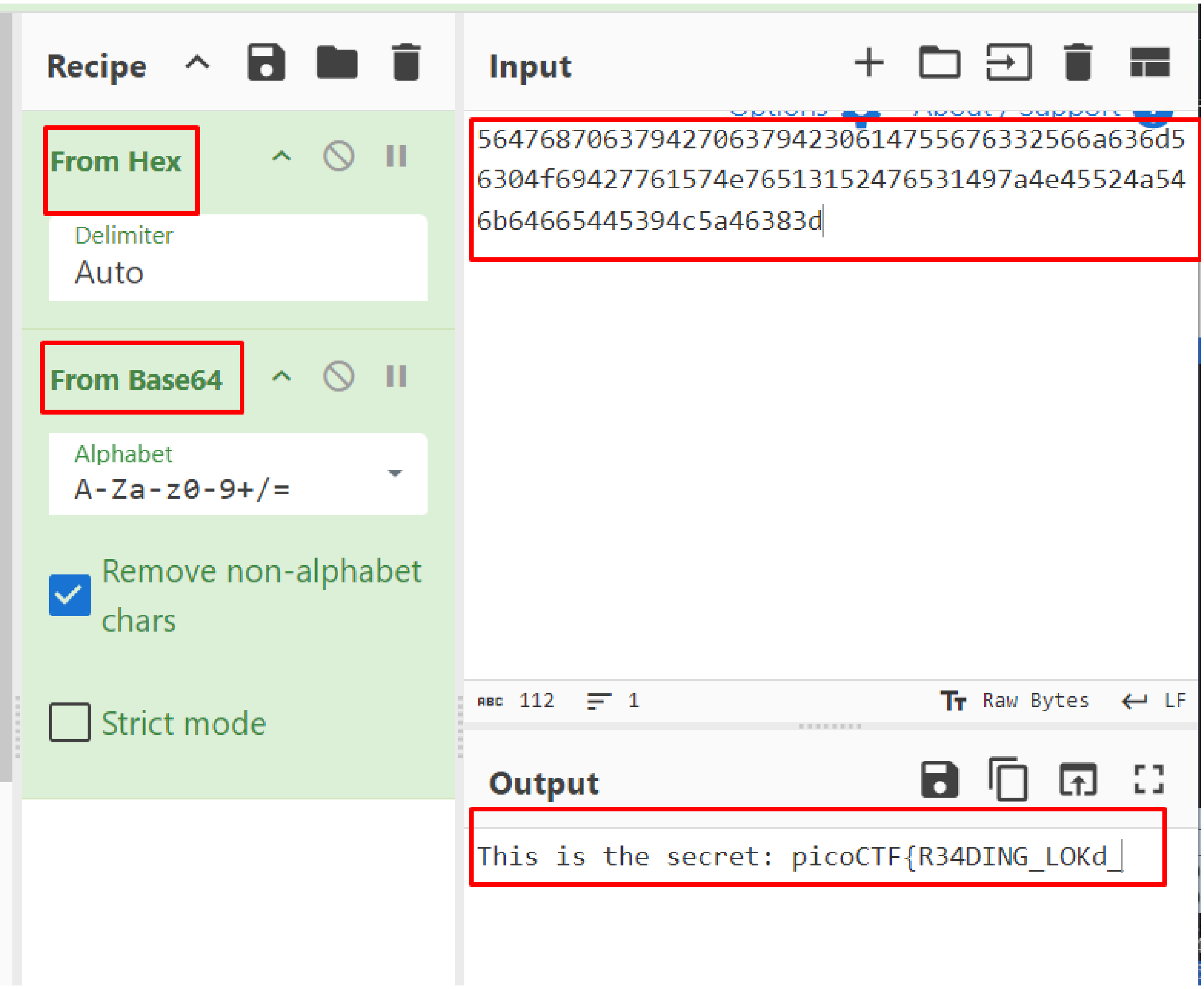
```
▸ Frame 50: 49 bytes on wire (392 bits), 49 bytes captured (392 bits)
▸ Ethernet II, Src: 76:51:31:52:47:65 (76:51:31:52:47:65), Dst: 50:42:77:61:57:55 (50:42:77
▸ Data (35 bytes)
```

```
0000  50 42 77 61 57 55 76 51  31 52 47 65 73 61 62 61   PBwaWUvQ 1RGesaba
0010  62 61 62 6b 6a 61 41 53  4b 42 4b 53 42 41 43 56   babkjaAS KBKSBACV
0020  56 41 56 53 44 44 53 53  53 53 44 53 4b 4a 42 4a   VAVSDDSS SSDSKJBJ
0030  53                                                 S
```

Al inspeccionar los paquetes encontramos algunas referencias, que pudieran darnos la clave para descomprimir el `.zip` se observan cadenas que pudieran estar en `base64`.



```
 44 14.472105   76:51:31:52:47:65   69:42:77:61:57:4e   0x3143    47 Ethernet II
 45 14.673443   76:51:31:52:47:65   69:42:77:61:57:4e   0x3143    47 Ethernet II
 46 14.874381   76:51:31:52:47:65   69:42:77:61:57:4e   0x3143    47 Ethernet II
 47 15.075729   76:51:31:52:47:65   69:42:77:61:57:4e   0x3143    47 Ethernet II
 48 24.240874   50:4a:47:54:46:52   41:41:42:42:48:48   0x4c4b    70 Ethernet II
 49 48.459761   76:51:31:52:47:65   50:42:77:61:57:55   0x7361    49 Ethernet II
 50 48.661266   76:51:31:52:47:65   50:42:77:61:57:55   0x7361    49 Ethernet II
 51 48.862635   76:51:31:52:47:65   50:42:77:61:57:55   0x7361    49 Ethernet II
 52 49.064175   76:51:31:52:47:65   50:42:77:61:57:55   0x7361    49 Ethernet II
 53 49.265187   76:51:31:52:47:65   50:42:77:61:57:55   0x7361    49 Ethernet II
 54 49.466470   76:51:31:52:47:65   50:42:77:61:57:55   0x7361    49 Ethernet II
 55 49.668273   76:51:31:52:47:65   50:42:77:61:57:55   0x7361    49 Ethernet II
 56 49.870142   76:51:31:52:47:65   50:42:77:61:57:55   0x7361    49 Ethernet II
 57 50.071670   76:51:31:52:47:65   50:42:77:61:57:55   0x7361    49 Ethernet II
 58 54.127340   76:51:31:52:47:65   50:42:77:61:57:55   0x314d    46 Ethernet II
 59 54.329337   76:51:31:52:47:65   50:42:77:61:57:55   0x314d    46 Ethernet II
 60 54.531171   76:51:31:52:47:65   50:42:77:61:57:55   0x314d    46 Ethernet II
 61 54.733158   76:51:31:52:47:65   50:42:77:61:57:55   0x314d    46 Ethernet II
 62 54.934646   76:51:31:52:47:65   50:42:77:61:57:55   0x314d    46 Ethernet II
 63 55.136085   76:51:31:52:47:65   50:42:77:61:57:55   0x314d    46 Ethernet II
 64 55.336962   76:51:31:52:47:65   50:42:77:61:57:55   0x314d    46 Ethernet II
 65 55.538161   76:51:31:52:47:65   50:42:77:61:57:55   0x314d    46 Ethernet II
 66 56.484261   172.16.93.1         224.0.0.251         MDNS     132 Standard qu                         " question TXT Chromecast-18e2a8da30459b730aec93a7
 67 56.484489   fe80::e0b5:5fff:fe3… ff02::fb           MDNS     152 Standard qu                         " question TXT Chromecast-18e2a8da30459b730aec93a7
 68 56.490507   172.16.93.2         224.0.0.251         MDNS     414 Standard qu                         ocal, "QM" question PTR Chromecast-18e2a8da30459b7
 69 56.490507   172.16.93.2         224.0.0.251         MDNS     327 Standard qu                         a30459b730aec93a71af19988._googlecast._tcp.local,

› Frame 48: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
› Ethernet II, Src: 50:4a:47:54:46:52 (50:4a:47:54:46:52), Dst: 41:41:42:42:48:48 (41:41:4
⌄ Data (56 bytes)
    Data: 564768706379427063794230614755676332566a636d56304f69427761574e765131524765314497a
    [Length: 56]

                                          52 4c 4b 56 47   AABBHHPJ GTFRLKVG
                                          47 55 67 63 32   hpcyBpcy B0aGUgc2
                                          57 4e 76 51 31   VjcmV0Oi BwaWNvQ1
                                          6b 64 66 54 45   RGe1IzNE RJTkdfTE
0040  39 4c 5a 46 38 3d                                    9LZF8=
```



Recipe

From Hex

Delimiter: Auto

From Base64

Alphabet: A-Za-z0-9+/=

☑ Remove non-alphabet chars

☐ Strict mode

Input

```
564768706379427063794230614755676332566a636d5
6304f69427761574e76513152476531497a4e45524a54
6b64665445394c5a46383d
```

Output

```
This is the secret: picoCTF{R34DING_LOKd_
```

```
┌──(kali㉿kali)-
[~/…/parciales/parcial_02/parte_03_forensic_01/find_and_open]
└─$ unzip flag.zip
Archive:  flag.zip
[flag.zip] flag password: picoCTF{R34DING_LOKd_
 extracting: flag
```

```
┌──(kali㉿kali)-
[~/…/parciales/parcial_02/parte_03_forensic_01/find_and_open]
└─$ cat flag
picoCTF{R34DING_LOKd_fil56_succ3ss_5ed3a878}
```

Bandera

```
flag: picoCTF{R34DING_LOKd_fil56_succ3ss_5ed3a878}
```

Notas Adicionales

Referencias

-