Network Security

Project 1

Sahil Bhirud

Task 1:

a. **How many unique MAC addresses were on the network?**

12

b. **How many unique IP addresses were on the network (IPv4 and IPv6)?**

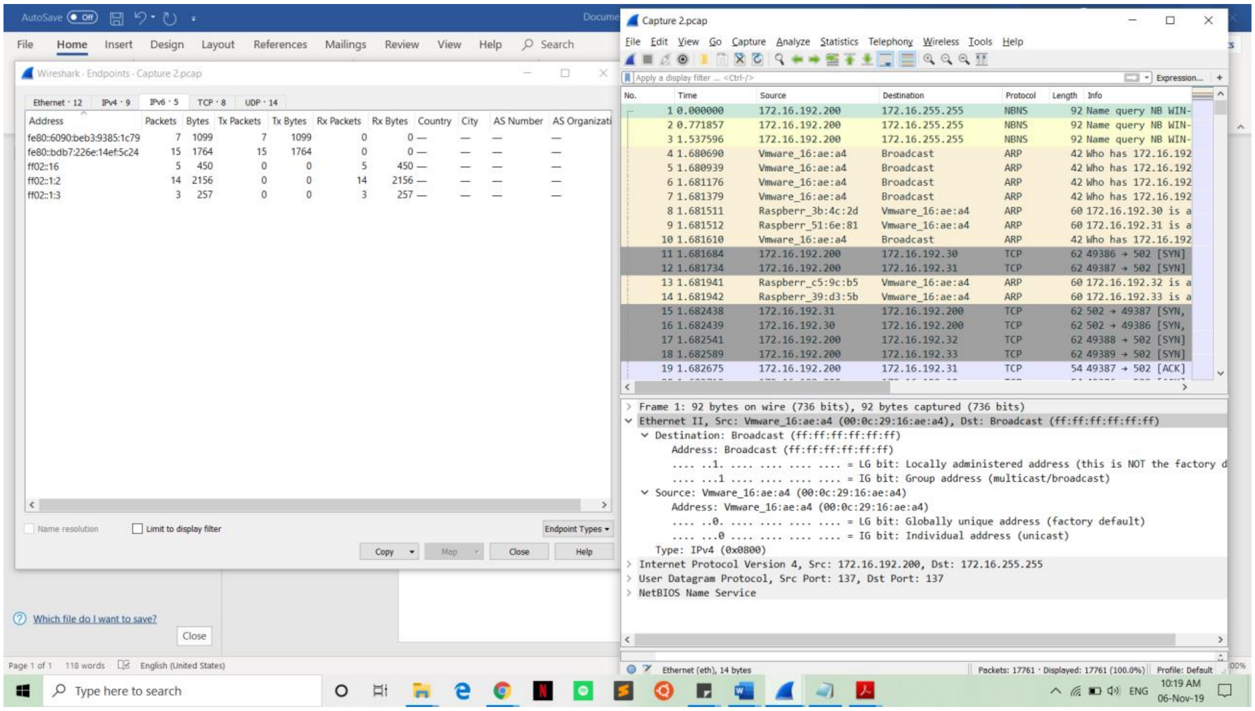
9 of IPv4 and 5 of IPv6

c. **What were the two UDP protocols used?**

LLMNR and NBNS

d. **Which Ethernet address was shared between an IPv4 and IPv6 address?**

Step 1: I went on the Endpoints tab under Statistics and displayed all the IPv6 addresses.

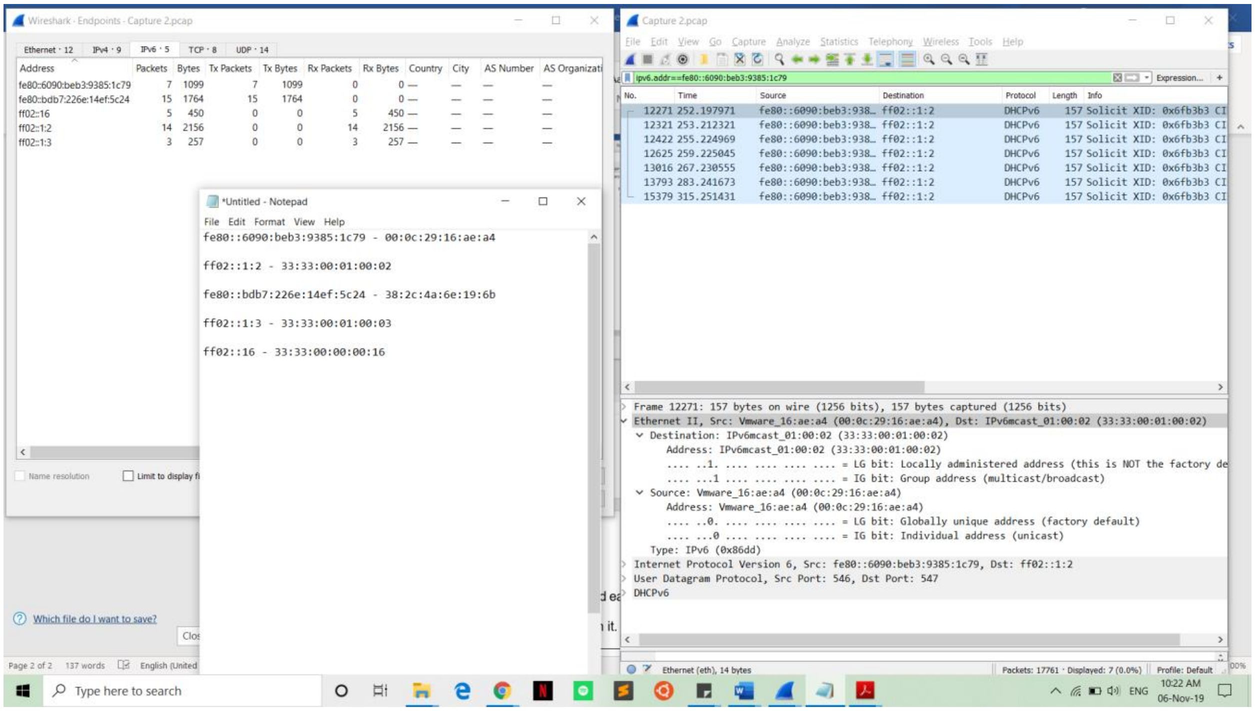


Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organizati
fe80::6090:beb3:9385:1c79	7	1099	7	1099	0	0	—	—	—	—
fe80::bdb7:226e:14ef:5c24	15	1764	15	1764	0	0	—	—	—	—
ff02::16	5	450	0	0	5	450	—	—	—	—
ff02::1:2	14	2156	0	0	14	2156	—	—	—	—
ff02::1:3	3	257	0	0	3	257	—	—	—	—

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.192.200	172.16.255.255	NBNS	92	Name query NB WIN-
2	0.771857	172.16.192.200	172.16.255.255	NBNS	92	Name query NB WIN-
3	1.537596	172.16.192.200	172.16.255.255	NBNS	92	Name query NB WIN-
4	1.680690	Vmware_16:ae:a4	Broadcast	ARP	42	Who has 172.16.192
5	1.680939	Vmware_16:ae:a4	Broadcast	ARP	42	Who has 172.16.192
6	1.681176	Vmware_16:ae:a4	Broadcast	ARP	42	Who has 172.16.192
7	1.681379	Vmware_16:ae:a4	Broadcast	ARP	42	Who has 172.16.192
8	1.681511	Raspberr_3b:4c:2d	Vmware_16:ae:a4	ARP	60	172.16.192.30 is a
9	1.681512	Raspberr_51:6e:81	Vmware_16:ae:a4	ARP	60	172.16.192.31 is a
10	1.681610	Vmware_16:ae:a4	Broadcast	ARP	42	Who has 172.16.192
11	1.681684	172.16.192.200	172.16.192.30	TCP	62	49386 → 502 [SYN]
12	1.681734	172.16.192.200	172.16.192.31	TCP	62	49387 → 502 [SYN]
13	1.681941	Raspberr_c5:9c:b5	Vmware_16:ae:a4	ARP	60	172.16.192.32 is a
14	1.681942	Raspberr_39:d3:5b	Vmware_16:ae:a4	ARP	60	172.16.192.33 is a
15	1.682438	172.16.192.31	172.16.192.200	TCP	62	502 → 49387 [SYN,
16	1.682439	172.16.192.30	172.16.192.200	TCP	62	502 → 49386 [SYN,
17	1.682541	172.16.192.200	172.16.192.32	TCP	62	49388 → 502 [SYN]
18	1.682589	172.16.192.200	172.16.192.33	TCP	62	49389 → 502 [SYN]
19	1.682675	172.16.192.200	172.16.192.31	TCP	54	49387 → 502 [ACK]

```
> Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
v Ethernet II, Src: Vmware_16:ae:a4 (00:0c:29:16:ae:a4), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  v Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory d
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  v Source: Vmware_16:ae:a4 (00:0c:29:16:ae:a4)
      Address: Vmware_16:ae:a4 (00:0c:29:16:ae:a4)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 172.16.192.200, Dst: 172.16.255.255
> User Datagram Protocol, Src Port: 137, Dst Port: 137
> NetBIOS Name Service
```

Step 2: I applied each IPv6 address as a filter and noted down the ethernet address associated with it.



Wireshark · Endpoints · Capture 2.pcap

Ethernet · 12 | IPv4 · 9 | IPv6 · 5 | TCP · 8 | UDP · 14

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organizati
fe80::6090:beb3:9385:1c79	7	1099	7	1099	0	0	—	—	—	—
fe80::bdb7:226e:14ef:5c24	15	1764	15	1764	0	0	—	—	—	—
ff02::16	5	450	0	0	5	450	—	—	—	—
ff02::1:2	14	2156	0	0	14	2156	—	—	—	—
ff02::1:3	3	257	0	0	3	257	—	—	—	—

*Untitled - Notepad

```
fe80::6090:beb3:9385:1c79 - 00:0c:29:16:ae:a4

ff02::1:2 - 33:33:00:01:00:02

fe80::bdb7:226e:14ef:5c24 - 38:2c:4a:6e:19:6b

ff02::1:3 - 33:33:00:01:00:03

ff02::16 - 33:33:00:00:00:16
```

Capture 2.pcap

Filter: ipv6.addr==fe80::6090:beb3:9385:1c79

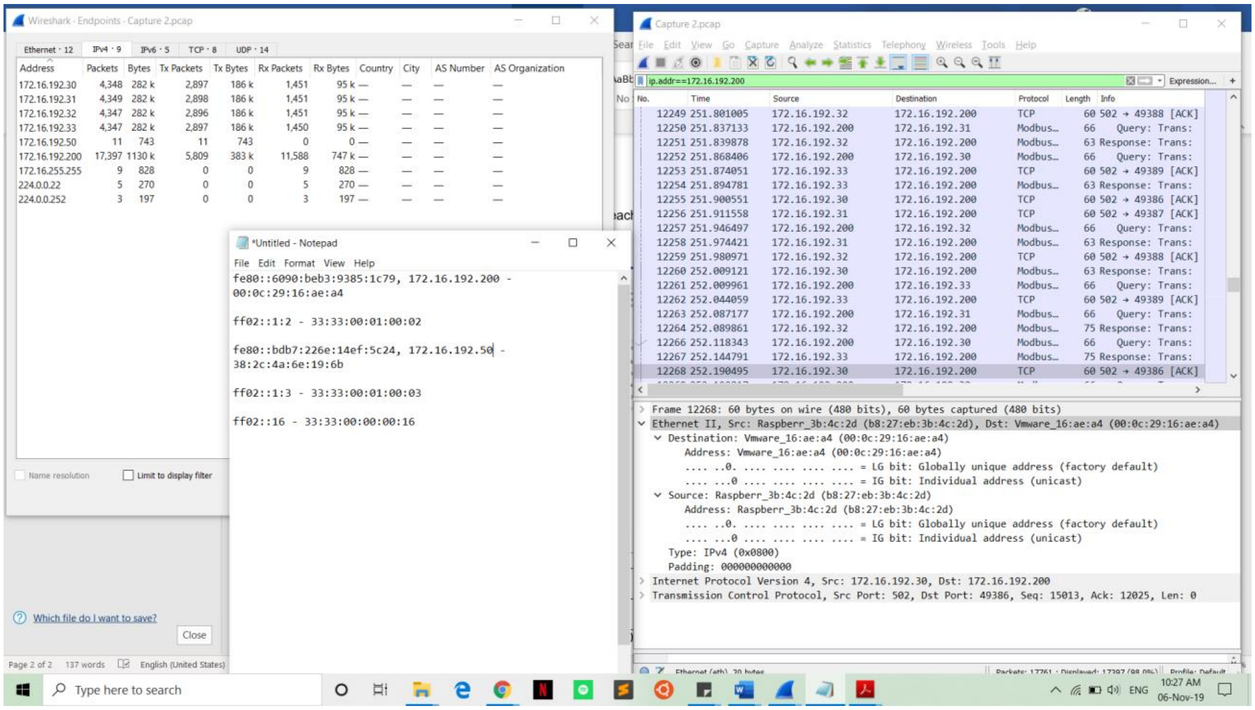
```
No.    Time        Source                Destination  Protocol  Length Info
12271 252.197971  fe80::6090:beb3:938…  ff02::1:2    DHCPv6    157 Solicit XID: 0x6fb3b3 CI
12321 253.212321  fe80::6090:beb3:938…  ff02::1:2    DHCPv6    157 Solicit XID: 0x6fb3b3 CI
12422 255.224969  fe80::6090:beb3:938…  ff02::1:2    DHCPv6    157 Solicit XID: 0x6fb3b3 CI
12625 259.225045  fe80::6090:beb3:938…  ff02::1:2    DHCPv6    157 Solicit XID: 0x6fb3b3 CI
13016 267.230555  fe80::6090:beb3:938…  ff02::1:2    DHCPv6    157 Solicit XID: 0x6fb3b3 CI
13793 283.241673  fe80::6090:beb3:938…  ff02::1:2    DHCPv6    157 Solicit XID: 0x6fb3b3 CI
15379 315.251431  fe80::6090:beb3:938…  ff02::1:2    DHCPv6    157 Solicit XID: 0x6fb3b3 CI
```

```
> Frame 12271: 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits)
v Ethernet II, Src: Vmware_16:ae:a4 (00:0c:29:16:ae:a4), Dst: IPv6mcast_01:00:02 (33:33:00:01:00:02)
  v Destination: IPv6mcast_01:00:02 (33:33:00:01:00:02)
      Address: IPv6mcast_01:00:02 (33:33:00:01:00:02)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory de
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  v Source: Vmware_16:ae:a4 (00:0c:29:16:ae:a4)
      Address: Vmware_16:ae:a4 (00:0c:29:16:ae:a4)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv6 (0x86dd)
> Internet Protocol Version 6, Src: fe80::6090:beb3:9385:1c79, Dst: ff02::1:2
> User Datagram Protocol, Src Port: 546, Dst Port: 547
> DHCPv6
```

Ethernet (eth), 14 bytes | Packets: 17761 · Displayed: 7 (0.0%) | Profile: Default

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
☐ Name resolution
☐ Limit to display filter
Which file do I want to save?
Page 2 of 2 137 words English (United
Type here to search
ENG
10:22 AM
06-Nov-19

Step 3: I applied each IPv4 address as a filter and checked if it was sharing a MAC address with an IPv6 address.



Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
172.16.192.30	4,348	282 k	2,897	186 k	1,451	95 k	—	—	—	—
172.16.192.31	4,349	282 k	2,898	186 k	1,451	95 k	—	—	—	—
172.16.192.32	4,347	282 k	2,896	186 k	1,451	95 k	—	—	—	—
172.16.192.33	4,347	282 k	2,897	186 k	1,450	95 k	—	—	—	—
172.16.192.50	11	743	11	743	0	0	—	—	—	—
172.16.192.200	17,397	1130 k	5,809	383 k	11,588	747 k	—	—	—	—
172.16.255.255	9	828	0	0	9	828	—	—	—	—
224.0.0.22	5	270	0	0	5	270	—	—	—	—
224.0.0.252	3	197	0	0	3	197	—	—	—	—

```
fe80::6090:beb3:9385:1c79, 172.16.192.200 -
00:0c:29:16:ae:a4

ff02::1:2 - 33:33:00:01:00:02

fe80::bdb7:226e:14ef:5c24, 172.16.192.50 -
38:2c:4a:6e:19:6b

ff02::1:3 - 33:33:00:01:00:03

ff02::16 - 33:33:00:00:00:16
```

ip.addr==172.16.192.200

```
No.   Time       Source          Destination     Protocol Length Info
12249 251.801005 172.16.192.32   172.16.192.200  TCP       60 502 → 49388 [ACK]
12250 251.837133 172.16.192.200  172.16.192.31   Modbus…   66    Query: Trans:
12251 251.839878 172.16.192.32   172.16.192.200  Modbus…   63 Response: Trans:
12252 251.868406 172.16.192.200  172.16.192.30   Modbus…   66    Query: Trans:
12253 251.874051 172.16.192.33   172.16.192.200  TCP       60 502 → 49389 [ACK]
12254 251.894781 172.16.192.33   172.16.192.200  Modbus…   63 Response: Trans:
12255 251.900551 172.16.192.30   172.16.192.200  TCP       60 502 → 49386 [ACK]
12256 251.911558 172.16.192.31   172.16.192.200  TCP       60 502 → 49387 [ACK]
12257 251.946497 172.16.192.200  172.16.192.32   Modbus…   66    Query: Trans:
12258 251.974421 172.16.192.31   172.16.192.200  Modbus…   63 Response: Trans:
12259 251.980971 172.16.192.32   172.16.192.200  TCP       60 502 → 49388 [ACK]
12260 252.009121 172.16.192.30   172.16.192.200  Modbus…   63 Response: Trans:
12261 252.009961 172.16.192.200  172.16.192.33   Modbus…   66    Query: Trans:
12262 252.044059 172.16.192.33   172.16.192.200  TCP       60 502 → 49389 [ACK]
12263 252.087177 172.16.192.200  172.16.192.31   Modbus…   66    Query: Trans:
12264 252.089861 172.16.192.32   172.16.192.200  Modbus…   75 Response: Trans:
12266 252.118343 172.16.192.200  172.16.192.30   Modbus…   66    Query: Trans:
12267 252.144791 172.16.192.33   172.16.192.200  Modbus…   75 Response: Trans:
12268 252.190495 172.16.192.30   172.16.192.200  TCP       60 502 → 49386 [ACK]
```

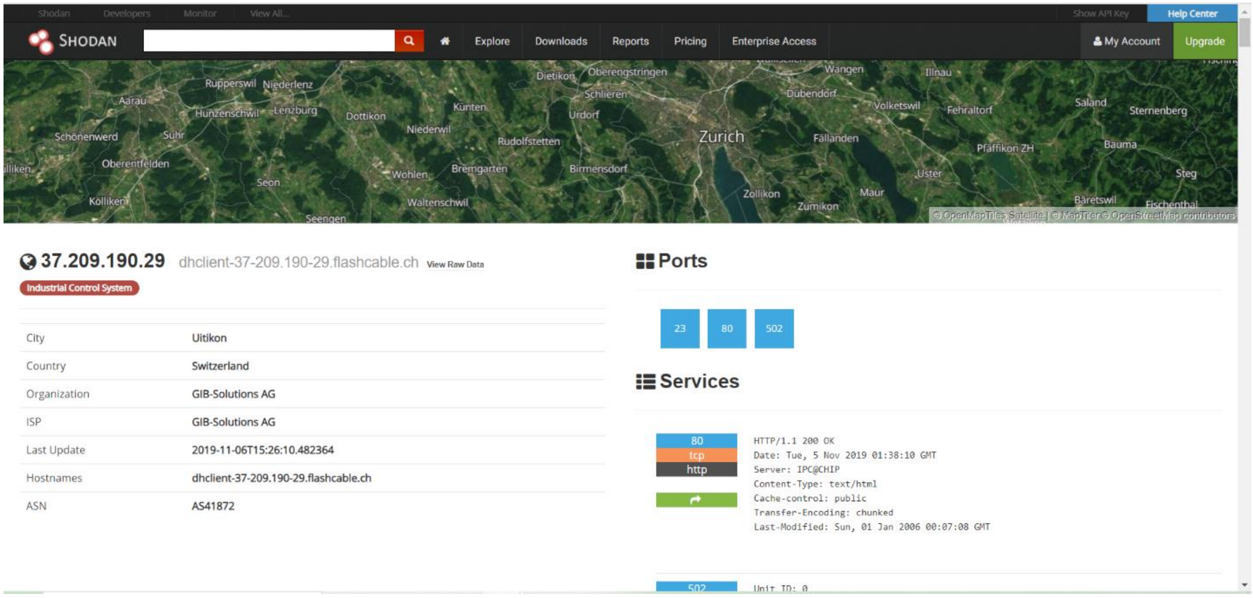
```
> Frame 12268: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
v Ethernet II, Src: Raspberr_3b:4c:2d (b8:27:eb:3b:4c:2d), Dst: Vmware_16:ae:a4 (00:0c:29:16:ae:a4)
  v Destination: Vmware_16:ae:a4 (00:0c:29:16:ae:a4)
      Address: Vmware_16:ae:a4 (00:0c:29:16:ae:a4)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: Raspberr_3b:4c:2d (b8:27:eb:3b:4c:2d)
      Address: Raspberr_3b:4c:2d (b8:27:eb:3b:4c:2d)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    Padding: 000000000000
> Internet Protocol Version 4, Src: 172.16.192.30, Dst: 172.16.192.200
> Transmission Control Protocol, Src Port: 502, Dst Port: 49386, Seq: 15013, Ack: 12025, Len: 0
```

IPv4	IPv6	MAC Address
172.16.192.50	fe80::bdb7:226e:14ef:5c24	38:2c:4a:6e:19:6b
172.16.192.200	fe80::6090:beb3:9385:1c79	00:0c:29:16:ae:a4

e. It seems that there is a Human-Machine Interface (HMI) server that interacts with multiple devices in the network through Modbus. What is the IP address of the server?

172.16.192.200

Task 2:



37.209.190.29 dhclient-37-209.190-29.flashcable.ch

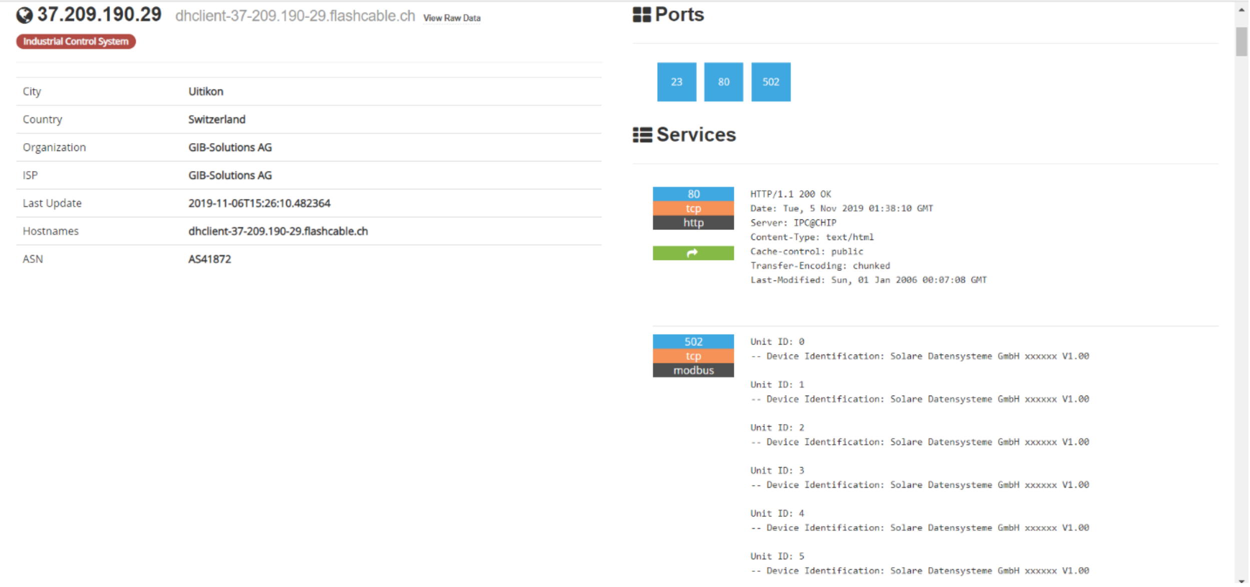
City	Uitikon
Country	Switzerland
Organization	GIB-Solutions AG
ISP	GIB-Solutions AG
Last Update	2019-11-06T15:26:10.482364
Hostnames	dhclient-37-209.190-29.flashcable.ch
ASN	AS41872

80 tcp http

```
HTTP/1.1 200 OK
Date: Tue, 5 Nov 2019 01:38:10 GMT
Server: IPC@CHIP
Content-Type: text/html
Cache-control: public
Transfer-Encoding: chunked
Last-Modified: Sun, 01 Jan 2006 00:07:08 GMT
```

502

```
Unit ID: 0
```



37.209.190.29 dhclient-37-209.190-29.flashcable.ch

City	Uitikon
Country	Switzerland
Organization	GIB-Solutions AG
ISP	GIB-Solutions AG
Last Update	2019-11-06T15:26:10.482364
Hostnames	dhclient-37-209.190-29.flashcable.ch
ASN	AS41872

80 tcp http

```
HTTP/1.1 200 OK
Date: Tue, 5 Nov 2019 01:38:10 GMT
Server: IPC@CHIP
Content-Type: text/html
Cache-control: public
Transfer-Encoding: chunked
Last-Modified: Sun, 01 Jan 2006 00:07:08 GMT
```

502 tcp modbus

```
Unit ID: 0
-- Device Identification: Solare Datensysteme GmbH xxxxxx V1.00

Unit ID: 1
-- Device Identification: Solare Datensysteme GmbH xxxxxx V1.00

Unit ID: 2
-- Device Identification: Solare Datensysteme GmbH xxxxxx V1.00

Unit ID: 3
-- Device Identification: Solare Datensysteme GmbH xxxxxx V1.00

Unit ID: 4
-- Device Identification: Solare Datensysteme GmbH xxxxxx V1.00

Unit ID: 5
-- Device Identification: Solare Datensysteme GmbH xxxxxx V1.00
```

Solare Datensysteme GmbH vulnerabilities:

There are 7 vulnerabilities of this device and they are explained below:

1. Unauthenticated Download of Configuration including Device-Password (present at least on firmware 2.8.4-56)

   An attacker can download configuration file and extract the password and later login as an administrator, gaining full access to the device without any prior authentication.

2. Cross-Site Request Forgery (CSRF) (present at least on firmware 3.5.2-85)

   Enables an attacker to remove/modify a password of a device by luring an authenticated user to click on a crafted link.

3. Unauthenticated Arbitrary File Upload (present at least on firmware 3.5.2-85)

   Any files can be uploaded on the Solar-Log by using a crafted POST request. An attacker can start a malicious website or store illegal contents on the Solar-Log.

4. Information Disclosure (CVE-2001-1341) (present in firmware 2.8.4-56 / 3.5.2-85)

   The network configuration of the internal network including the gateway and the MAC address of the device are leaked.

5. Unauthenticated Change of Network-Configuration (present in firmware 2.8.4-56 / 3.5.2-85)

   The server allows to change the IP configuration over a specific UDP port. This functionality can be protected with a password, but this is not set in the affected firmware versions.

6. Unauthenticated Denial of Service (present in firmware 2.8.4-56 / 3.5.2-85)

   The Beck IPC UDP configuration server on Solar-Log device can be attacked with arbitrary UDP packets to permanently disable the Solar-Log until a manual reboot is triggered.

7. Potential Unauthenticated Reprogram of IPC@CHIP Flash Memory (present in firmware 2.8.4-56 / 3.5.2-85)

   The “CHIPTOOL” from BECK IPC enables a developer to reprogram the chip over the network via UDP. A missing password in this case, can enable an attacker to perform this on a Solar-Log device (exploit-db).

References:

1. Exploit-db: https://www.exploit-db.com/exploits/41671