Fall 2019: ITIS 6167: Network Security

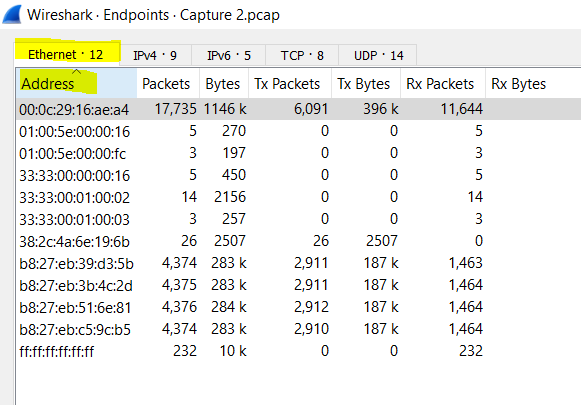
Project: Network Security Monitoring Tools

**Task 1:**

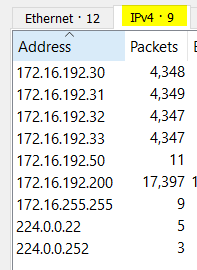
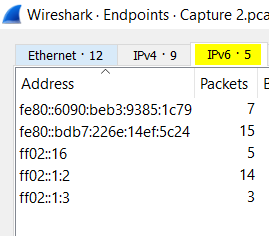
1. How many unique MAC addresses were on the network?

There are 12 unique MAC Addresses in total as shown below:

Go to Statistics🡪Endpoints:

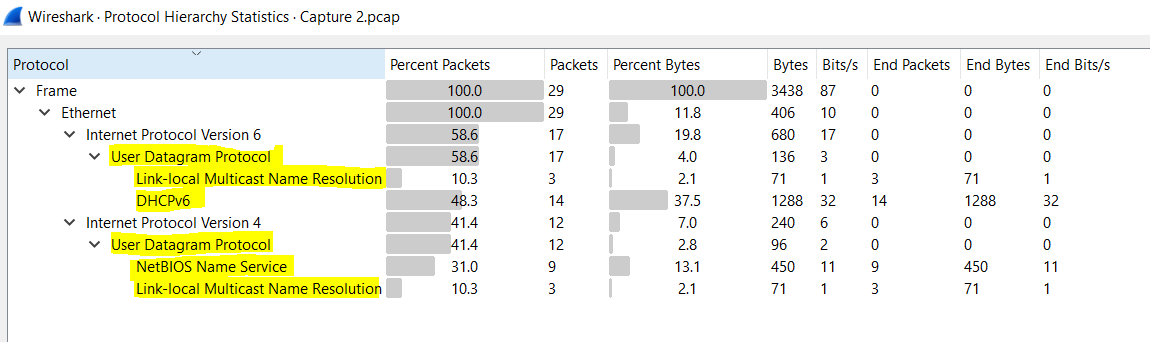


1. How many unique IP addresses were on the network (IPv4 and IPv6)?

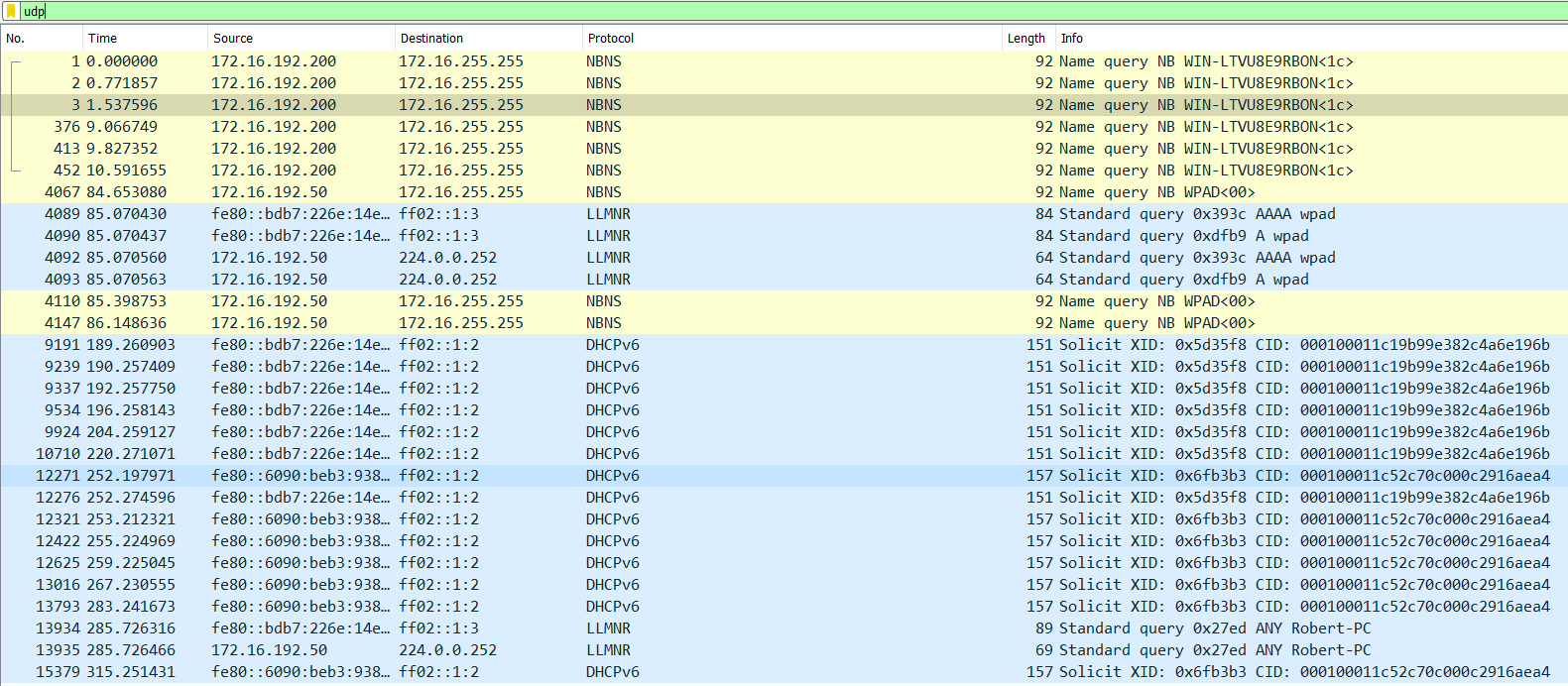
There are 5 unique IPv6 addresses and 9 unique IPv4 addresses. A total of 14 unique IP addresses.

1. What were the two UDP protocols used?

Following are the UDP protocols which I could find by navigating to Statistics🡪Protocol Hierarchy:

* + Link-local Multicast Name Resolution
  + DHCPv6
  + NetBIOS Name Service

These protocols can also be found by typing “udp” in filter search:

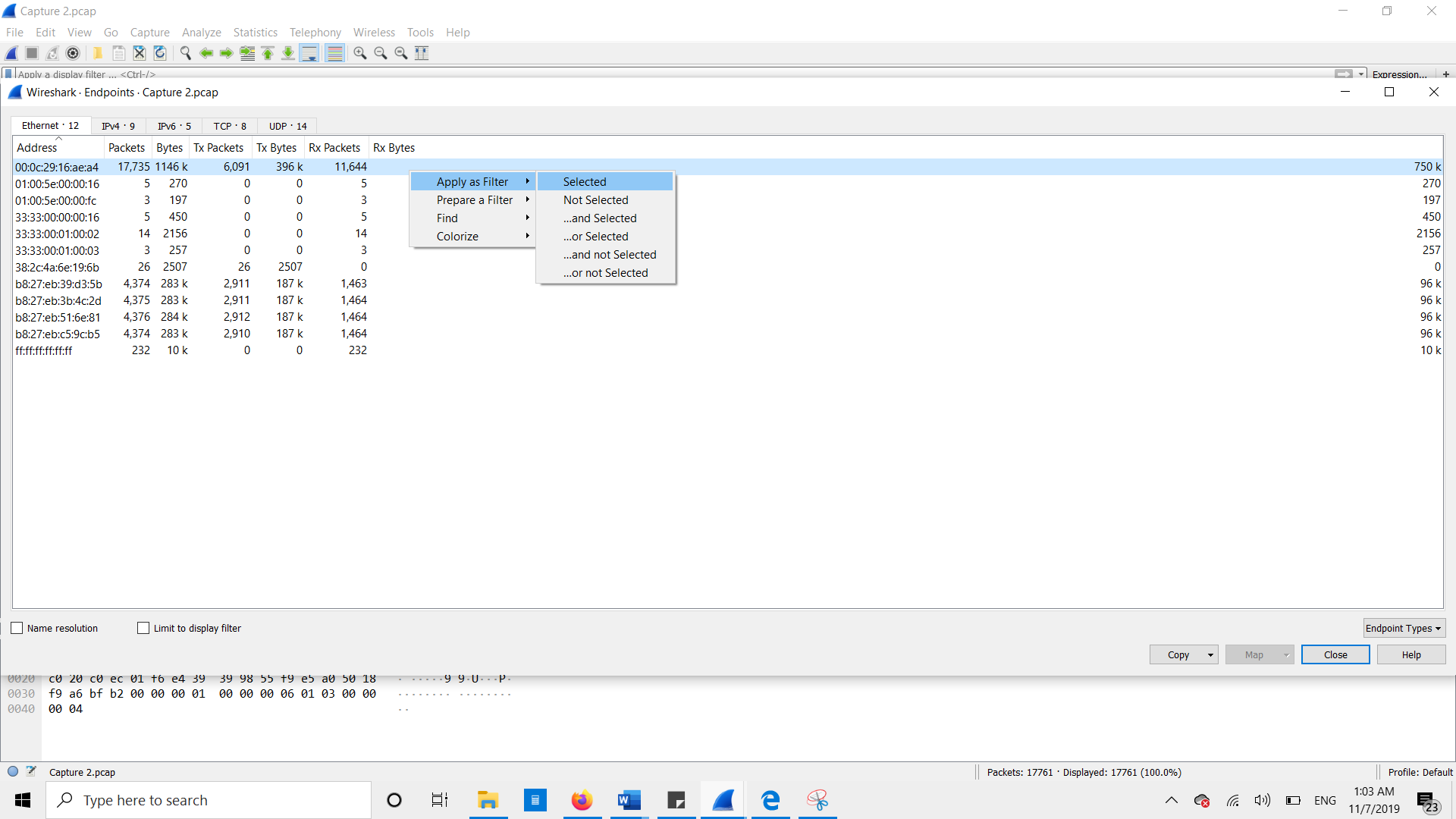
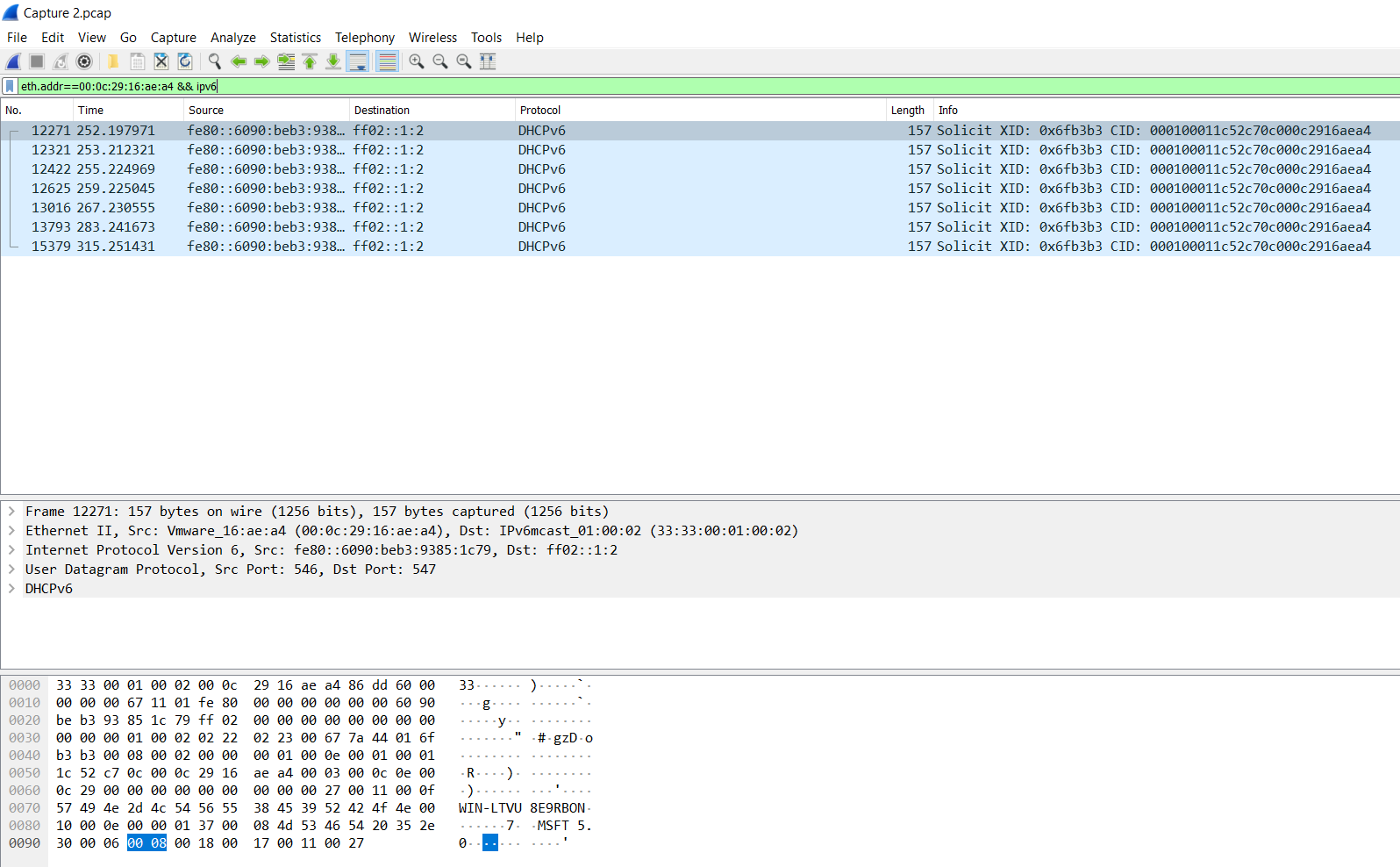
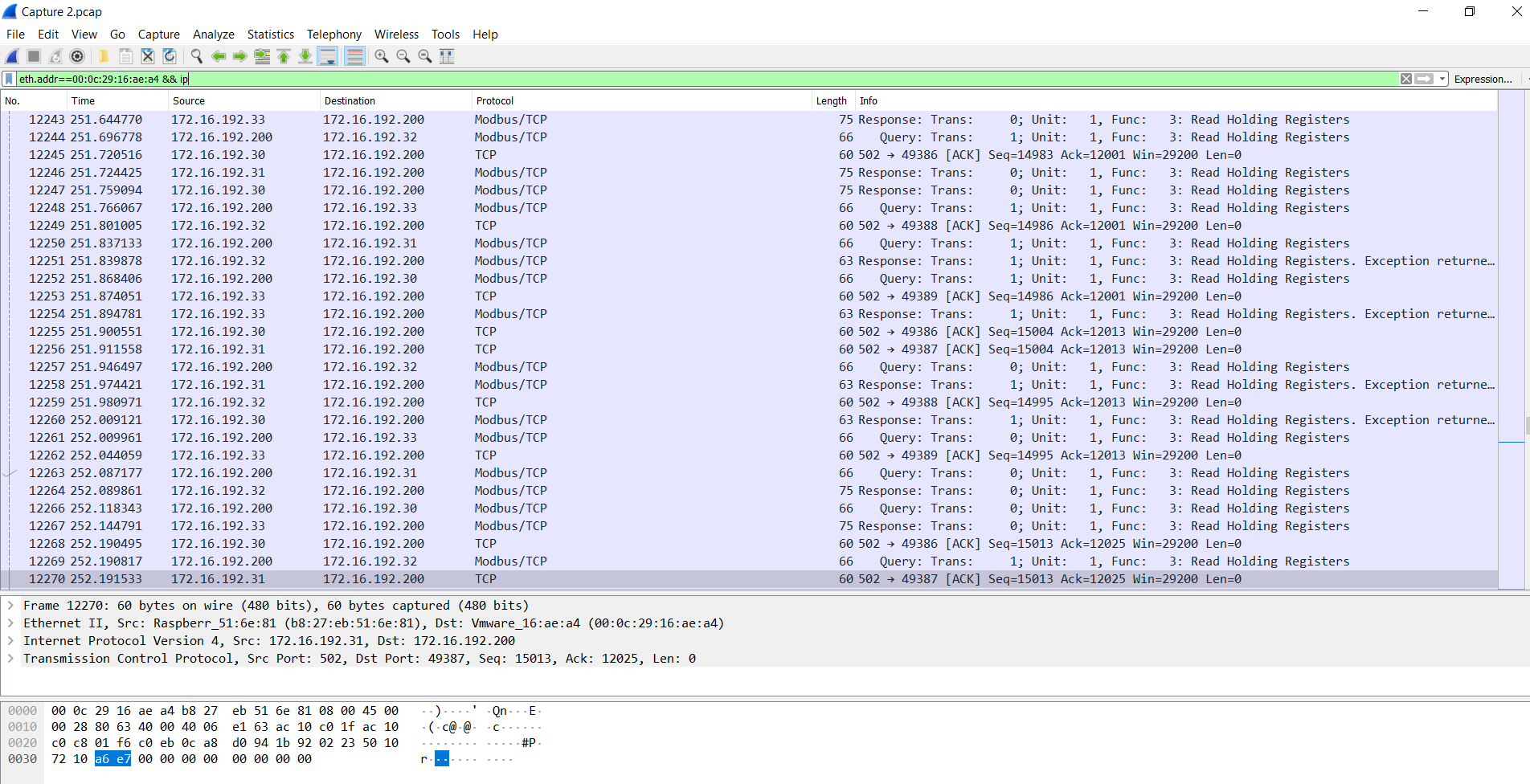


1. Which Ethernet address was shared between an IPv4 and IPv6 address?  
     
   After applying custom filters and observing the results, I found that **00:0c:29:16:ae:a4** and **38:2c:4a:6e:19:6b** are the ethernet addresses shared between IPv4 and IPv6 addresses.

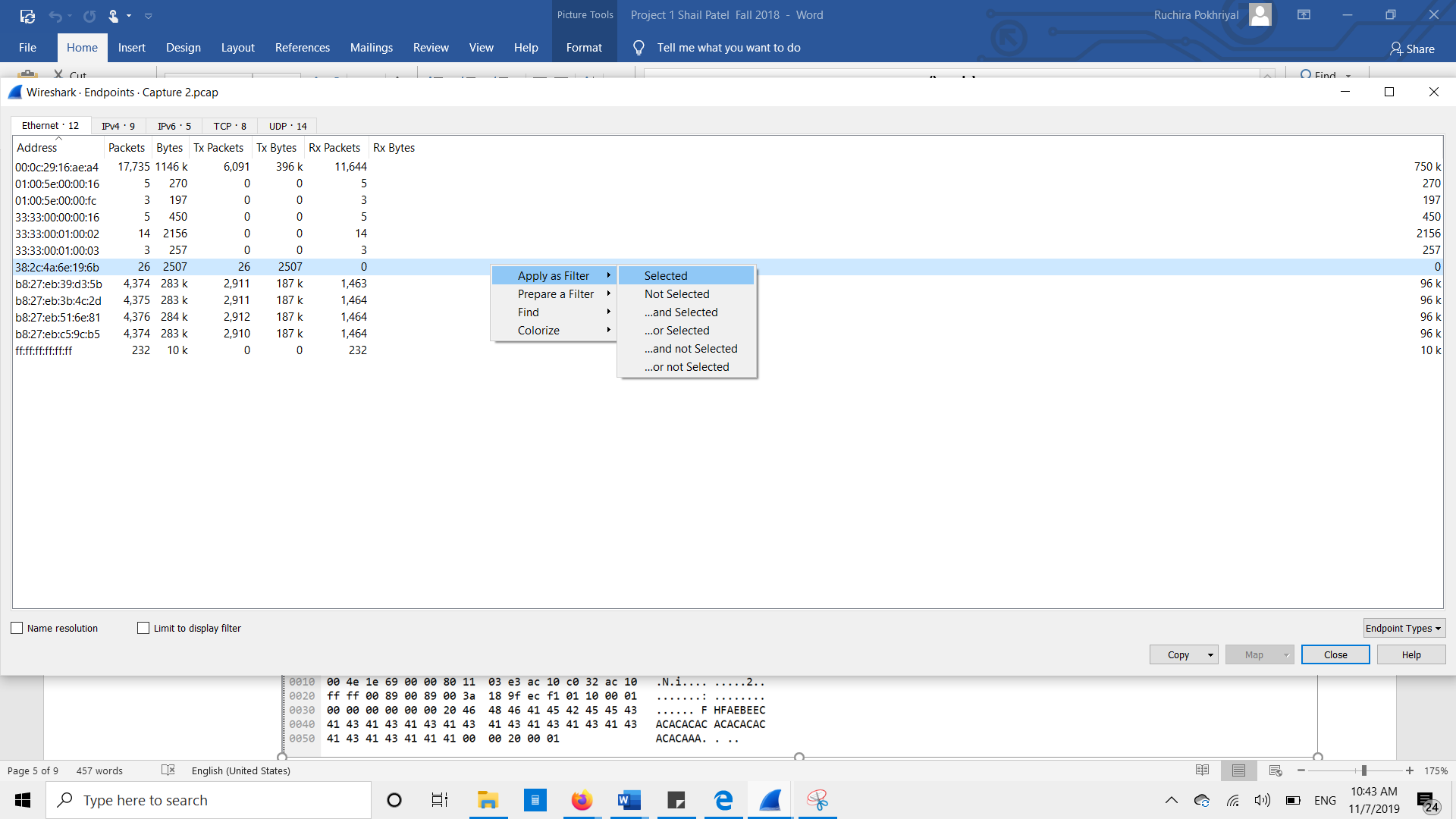
**Steps to conclude this:**

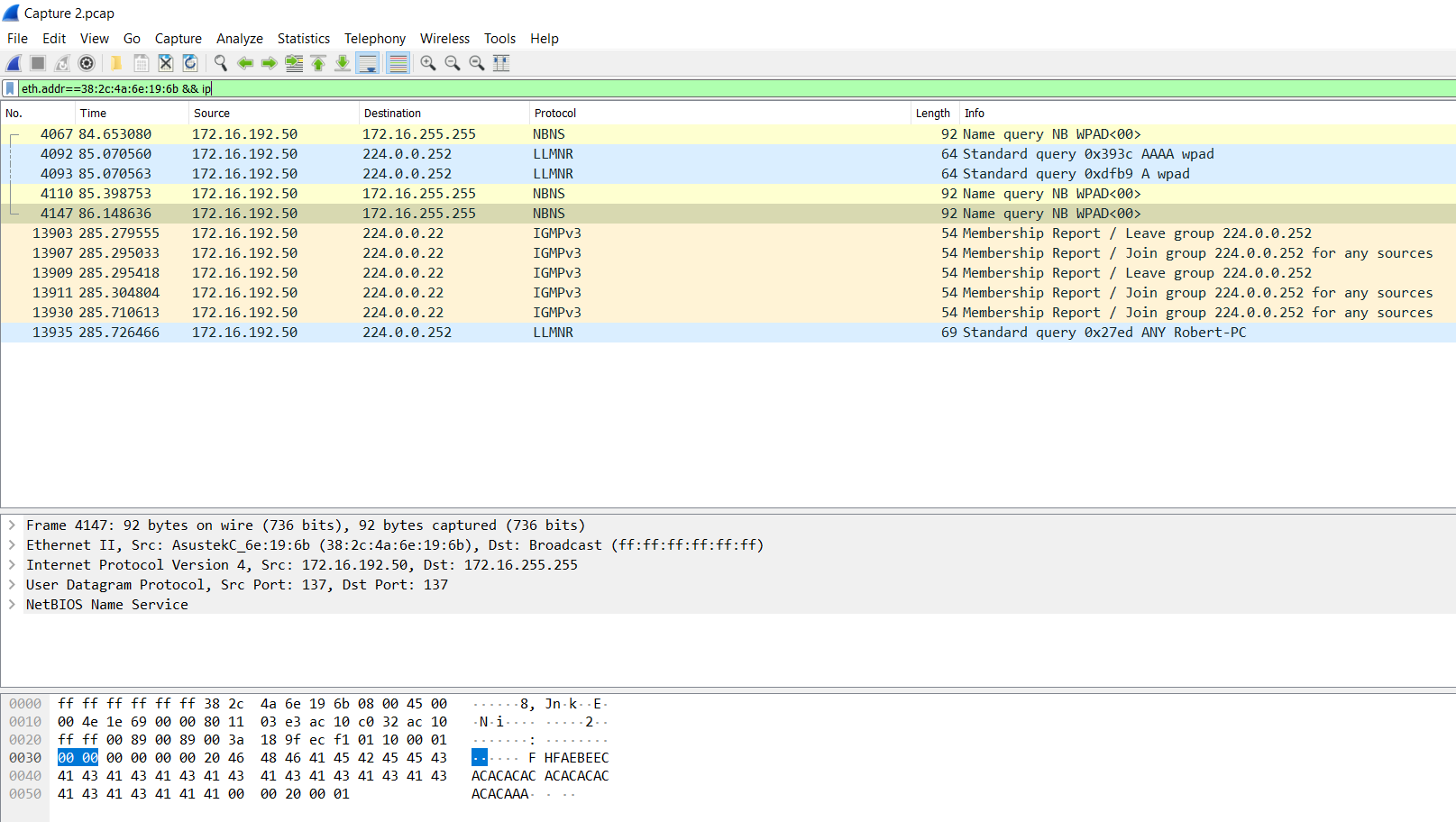
1. To find out the result, select ‘Endpoints’ option from statistics option on top.
2. Next, right click on an ethernet address and apply it as a filter. Observe the result set displayed after applying the filter.
3. The condition to use the filter is that the conversation is happening between this Ethernet address and any other ethernet addresses (source or source).
4. You could even apply customized filter conditions as shown in below screenshots.

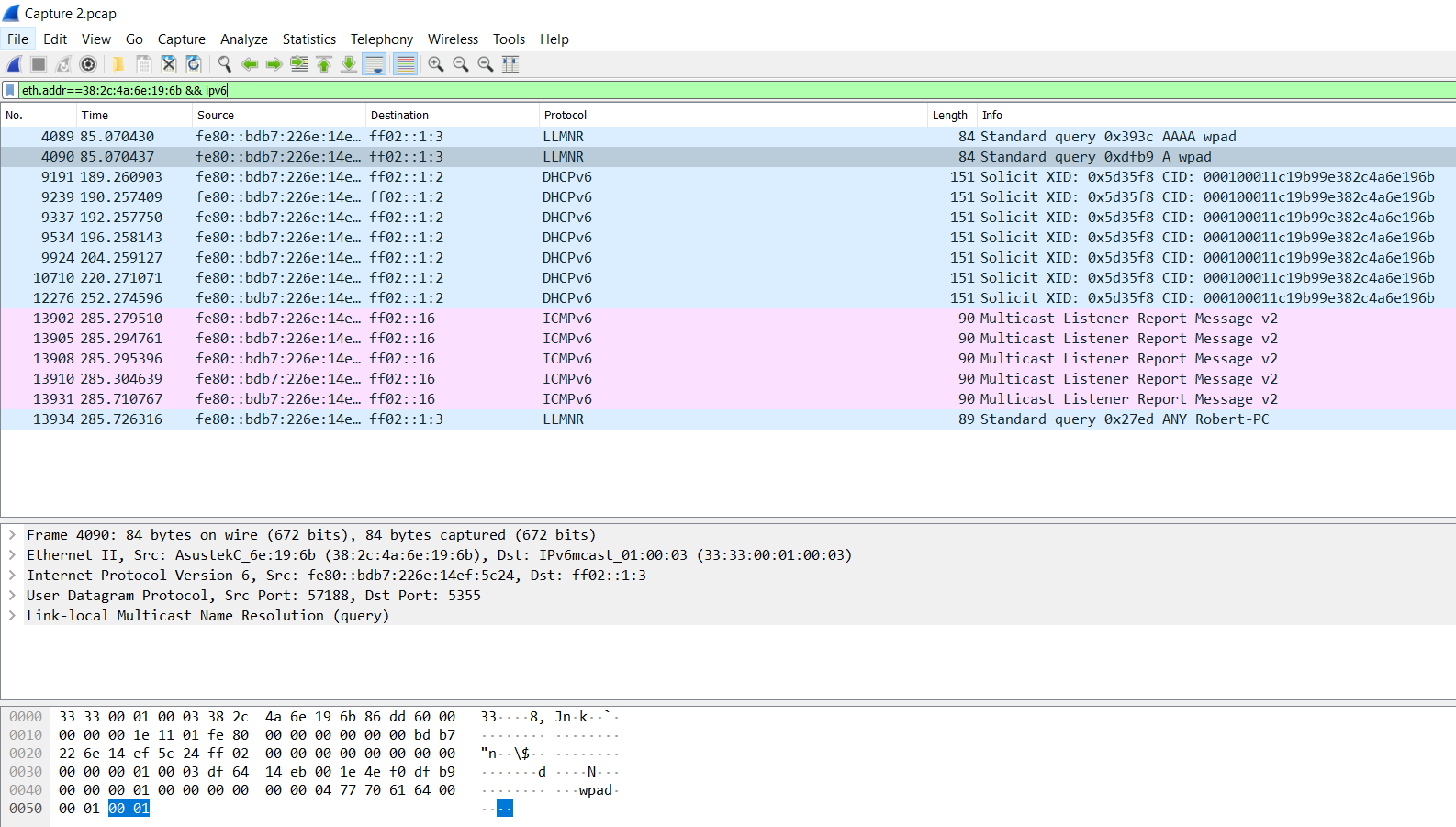
For Ethernet address: **00:0c:29:16:ae:a4**:-

For Ethernet address: **38:2c:4a:6e:19:6b** :-



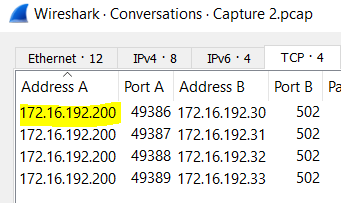




1. It seems that there is a Human-Machine Interface (HMI) server that interacts with multiple devices in the network through Modbus. What is the IP address of the server?

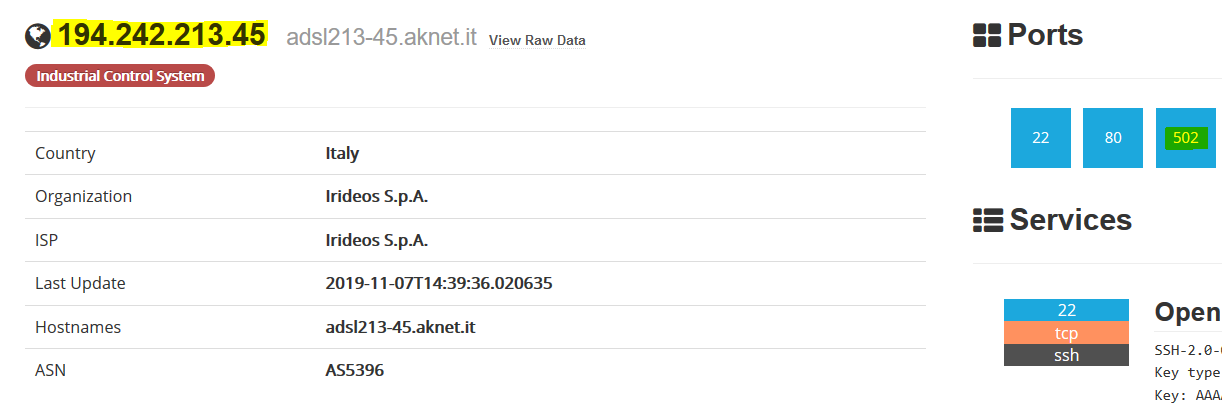
The IP address of the HMI server is **172.16.192.200.**

Modbus protocol uses TCP port 502. In conversations and endpoints tab, I could see that this IP address is communicating with multiple devices over port 502 using TCP:



**TASK 2:**

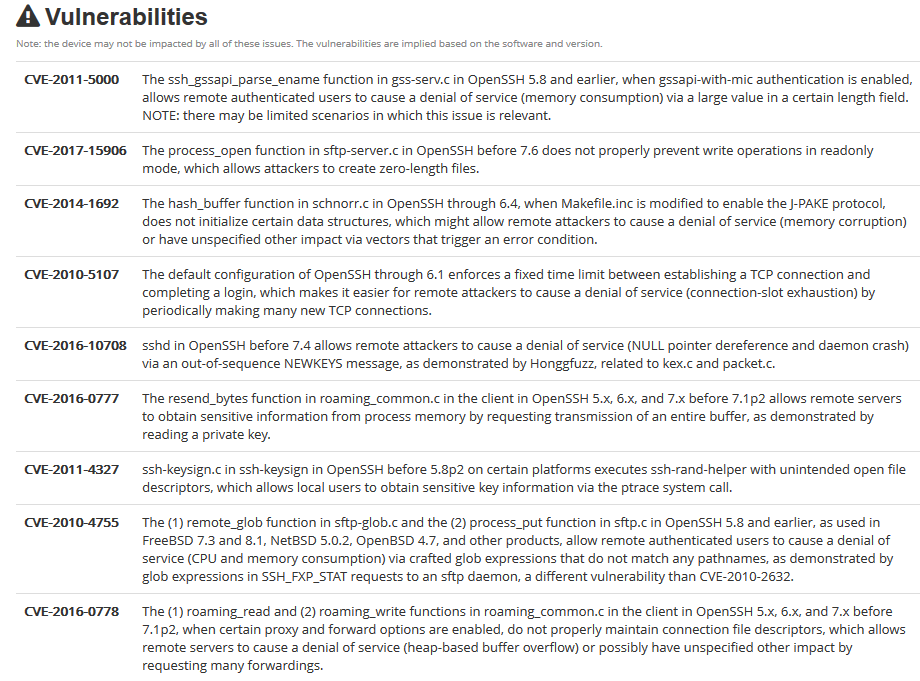
The IP address is **194.242.213.45** as shown in the below screenshot:



Scrolling belowor by simply clicking on Port 502 option on top, I found the device type, which is:   
**BM PP34 2020 v2.9**

  
  
This is a Schneider Electric Modicon CPU Module:





**Vulnerability Report Summary:**

I did some research and found the vulnerability report for this device [here](https://www.cvedetails.com/product/45632/Schneider-electric-Bmxp342020-Firmware.html?vendor_id=11651). There are several vulnerabilities associated with BM PP34 2020. In year 2019, its reported to have Reflected Cross Site Scripting and Remote File Inclusion. In year 2018, it had 6 major security flaws such as Buffer Overflow, arbitrary code execution, authorization bypass, vulnerable hash algorithms, hard coded accounts and finally in year 2017 there was a resource exhaustion vulnerability. Details of all of these vulnerabilities are listed below:

**Year 2019:**

[**CVE-2015-6462**](https://www.cvedetails.com/cve/CVE-2015-6462/): Reflected Cross-Site Scripting vulnerability which would allow an attacker to craft a URL containing malicious Java script which can be executed on the Schneider Electric Modicon BMXNOC0401, BMXNOE0100, BMXNOE0110, BMXNOE0110H, BMXNOR0200H, **BMXP342020**, BMXP342020H, BMXP342030, BMXP3420302, BMXP3420302H, or BMXP342030H PLC client browser.

[**CVE-2015-6461**](https://www.cvedetails.com/cve/CVE-2015-6461/)**:** This remote file inclusion vulnerability would allow an attacker to craft a malicious URL referencing the Schneider Electric Modicit would redirect the browser to a remote file via the javascript loaded with the web page. Effected models are: BMXNOC0401, BMXNOE0100, BMXNOE0110, BMXNOE0110H, BMXNOR0200H, BMXP342020, BMXP342020H, BMXP342030, BMXP3420302, BMXP3420302H, or BMXP342030H PLC web server, which, when launched, will result in the browser redirecting to a remote file via a Java script loaded with the web page.

**Year 2018:**

[**CVE-2018-7762**](https://www.cvedetails.com/cve/CVE-2018-7762/)**:** This is a vulnerability which exists in the web services to process SOAP requests in Schneider Electric's Modicon M340, Modicon Premium, Modicon Quantum PLC, **BMXNOR0200** and could cause a buffer overflow.

[**CVE-2018-7761**](https://www.cvedetails.com/cve/CVE-2018-7761/)**:** This flaw would allow arbitrary code execution if the vulnerability existing in the HTTP request parser in Schneider Electric's Modicon is exploited. Effected models are: M340, Modicon Premium, Modicon Quantum PLC, **BMXNOR0200**.

[**CVE-2018-7760**](https://www.cvedetails.com/cve/CVE-2018-7760/)**:** This is probably is like a mix of privilege escalation and backdoor as with this vulnerability, any requests to CGI functions would allow an attacker to bypass authorization. Effected models are: Schneider Electric's Modicon M340, Modicon Premium, Modicon Quantum PLC, BMXNOR0200.

[**CVE-2018-7759**](https://www.cvedetails.com/cve/CVE-2018-7759/) This is a buffer overflow vulnerability effecting in Schneider Electric's Modicon M340, Modicon Premium, Modicon Quantum PLC, BMXNOR0200. This vulnerability is caused by the length of the source string specified (instead of the buffer size) as the number of bytes to be copied.

[**CVE-2018-7242**](https://www.cvedetails.com/cve/CVE-2018-7242/) Existance of vulnerable hash algorithms in the sense that the password encryption algorithm is prone to hash collision. This vulnerability exists in Schneider Electric's Modicon Premium, Modicon Quantum, Modicon M340, and BMXNOR0200 controllers, in all versions of the communication modules.

[**CVE-2018-7241**](https://www.cvedetails.com/cve/CVE-2018-7241/) Hard coded accounts exist in Schneider Electric's Modicon Premium, Modicon Quantum, Modicon M340, and BMXNOR0200 controllers in all versions of the communication modules.

**Year 2017:**

[**CVE-2017-6017**](https://www.cvedetails.com/cve/CVE-2017-6017/) This is a Resource Exhaustion vulnerability, which could be exploited by a remote attacker to be able to send a specially crafted set of malicious packets to the PLC, causing it to freeze, and requiring the operator to physically press the reset button on the PLC in order to recover. This vulnerability was discovered in Schneider Electric Modicon M340 PLC BMXNOC0401, BMXNOE0100, BMXNOE0110, BMXNOE0110H, BMXNOR0200H, BMXP341000, BMXP342000, BMXP3420102, BMXP3420102CL, BMXP342020, BMXP342020H, BMXP342030, BMXP3420302, BMXP3420302H, and BMXP342030H.

**References:**

<https://www.shodan.io/host/194.242.213.45#502>

<https://www.cvedetails.com/product/45632/Schneider-electric-Bmxp342020-Firmware.html?vendor_id=11651>