How to recover forgotten IP address or root password using Wireshark

Article Number: 4 | Last Updated: Fri, Mar 3, 2017 at 5:03 PM

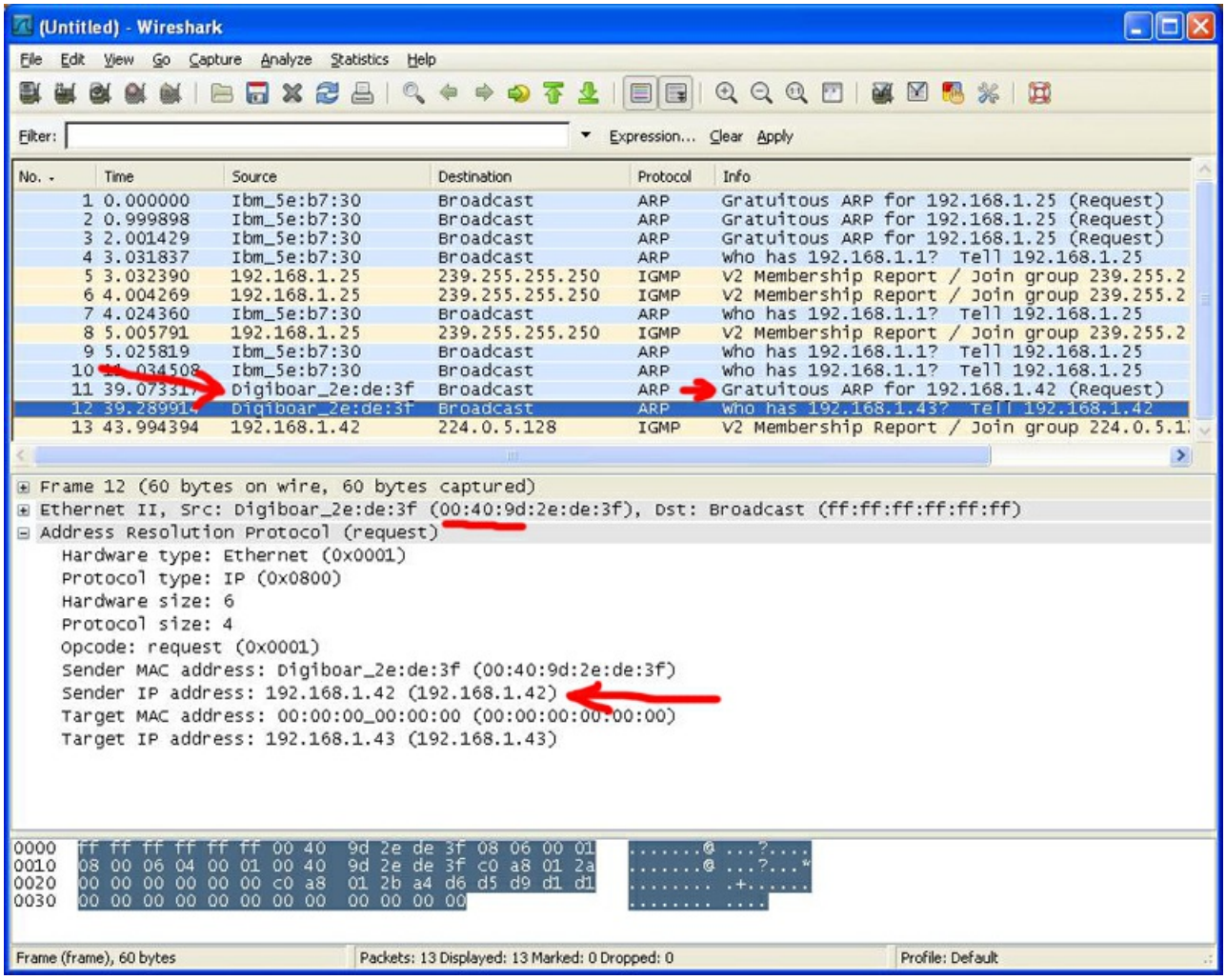
Forgotten IP Address:

You will need a network packet sniffer such as Wireshark (available at no cost at www.wireshark.org) and must be locally connected to the i.CanDoIt (or Babel Buster, etc.) since the packets of interest will not pass through routers. We say "must"because we don't guarantee it will work without being connected locally even though we don't guarantee it will fail either. It depends on your network configuration. But since you will need to power cycle the i.CanDoIt (or Babel Buster), you will need to have somebody local anyway.

Upon power up, the device will ping its own IPaddress one or more times. This is part of its duplicate address resolution mechanism. If it finds another device with its own IPaddress, it will set its own IPaddress to a default pseudo-random address generally starting with 192.

To recover the lost IPaddress, connect a PC withWireshark to the network, start Wireshark capturing packets, then power cycle the i.CanDoIt (or Babel Buster). Wait until you are certain the device has booted up, or wait 2-3 minutes to be sure if you don't recognize the bootup LEDsequence. Now look for the ARP packets and note what IPaddress they came from. This is your device. (To make sure it is your device, connect only i.CanDoIt or Babel Buster and your PC to a switch while doing this exercise.)

Your device will have a MAC address that starts with 00:40:9D, also labeled with a source that starts with "Digiboar_". This label comes from the fact that the server modules used on Control Solutions IP products are made by Digi International, previously known as "Digiboard".



Forgotten root password:

Follow the same process above, but look closer. The last ARP in the series of ARP's will be a ping to an IPaddress whose last field is one greater than the previous pings. This magic packet contains the root password in encrypted form in the packet padding at the end of the ARP. You will need to examine this packet in raw form (expand the view in Wireshark), and make a note of the hex bytes in the "payload". This is the encrypted root password. You should do a screen capture, or text copy and paste, and post this to a support ticket at https://ticket.csimn.com. Your password will be decrypted for you and we will post your password to your support ticket. The program that does this decryption for us is not, and never will be, available on the Internet for reasons we think are obvious.

Posted - Tue, Dec 11, 2012 at 10:09 PM.

Online URL: https://info.csimn.com/article.php?id=4