

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.CanDolt (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.CanDolt (or Babel Buster), you will need to have somebody local anyway.

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

To recover the lost IP address, connect a PC with Wireshark to the network, start Wireshark capturing packets, then power cycle the i.CanDolt (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 LED sequence. Now look for the ARP packets and note what IP address they came from. This is your device. (To make sure it is your device, connect only i.CanDolt 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".

The screenshot shows the Wireshark interface with a capture of network traffic. The packet list pane shows several ARP requests. Packet 12 is highlighted, showing an ARP request from source MAC 00:40:9d:2e:3f to target IP 192.168.1.42. The packet details pane shows the ARP request structure with the sender IP address 192.168.1.42 highlighted. The packet bytes pane shows the raw hex data of the ARP request.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	Ibm_5e:b7:30	Broadcast	ARP	Gratuitous ARP for 192.168.1.25 (Request)
2	0.999898	Ibm_5e:b7:30	Broadcast	ARP	Gratuitous ARP for 192.168.1.25 (Request)
3	2.001429	Ibm_5e:b7:30	Broadcast	ARP	Gratuitous ARP for 192.168.1.25 (Request)
4	3.031837	Ibm_5e:b7:30	Broadcast	ARP	who has 192.168.1.1? Tell 192.168.1.25
5	3.032390	192.168.1.25	239.255.255.250	IGMP	V2 Membership Report / Join group 239.255.2
6	4.004269	192.168.1.25	239.255.255.250	IGMP	V2 Membership Report / Join group 239.255.2
7	4.024360	Ibm_5e:b7:30	Broadcast	ARP	who has 192.168.1.1? Tell 192.168.1.25
8	5.005791	192.168.1.25	239.255.255.250	IGMP	V2 Membership Report / Join group 239.255.2
9	5.025819	Ibm_5e:b7:30	Broadcast	ARP	who has 192.168.1.1? Tell 192.168.1.25
10	5.034508	Ibm_5e:b7:30	Broadcast	ARP	who has 192.168.1.1? Tell 192.168.1.25
11	39.073317	Digiboar_2e:de:3f	Broadcast	ARP	Gratuitous ARP for 192.168.1.42 (Request)
12	39.289914	Digiboar_2e:de:3f	Broadcast	ARP	who has 192.168.1.43? Tell 192.168.1.42
13	43.994394	192.168.1.42	224.0.0.1	IGMP	V2 Membership Report / Join group 224.0.0.1

Frame 12 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: Digiboar_2e:de:3f (00:40:9d:2e:de:3f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
Hardware type: Ethernet (0x0001)
Protocol type: IP (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (0x0001)
Sender MAC address: Digiboar_2e:de:3f (00:40:9d:2e:de:3f)
Sender IP address: 192.168.1.42 (192.168.1.42)
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.1.43 (192.168.1.43)

```
0000 ff ff ff ff ff ff 00 40 9d 2e de 3f 08 06 00 01
0010 08 00 06 04 00 01 00 40 9d 2e de 3f c0 a8 01 2a
0020 00 00 00 00 00 00 c0 a8 01 2b a4 d6 d5 d9 d1 d1
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

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 IP address 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.csimm.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.csimm.com/article.php?id=4>