How to capture packets with Wireshark

Tim Chung

Version 1.0 (AUG, 2009)

Introduction

This document describes how to use the **Wireshark** – a network protocal analyzer – to capture the packets of iSCSI communication over the ethernet.

Environment

Host OS:	Windows XP
Necessary package:	Wireshark 1.2.1
iSCSI port:	192.168.11.87/24
Network Switch	HP Procurve Switch 1800-24G
iSCSI target:	QSAN P200C
RAM:	1GB DDR2-533
Firmware:	1.1.6 (20090625_1800)
iSCSI data port:	192.168.11.200/24

Diagram

Windwos XP Pro
iSCSI port
192.168.11.87/24
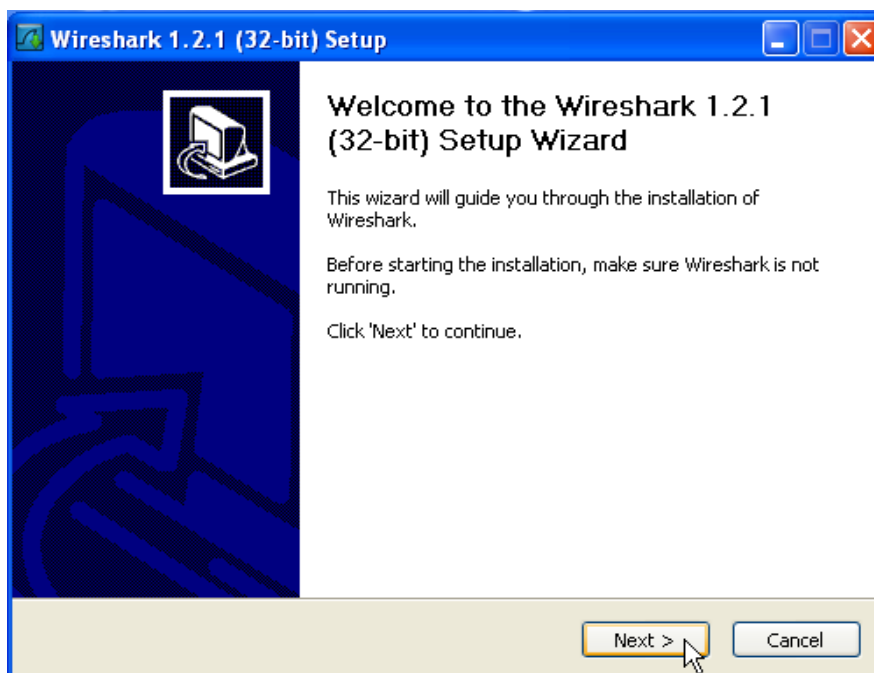
HP Procurve 1800-24G

-Gigabit Switch

iSCSI data port
192.168.11.200/24

QSAN P200C
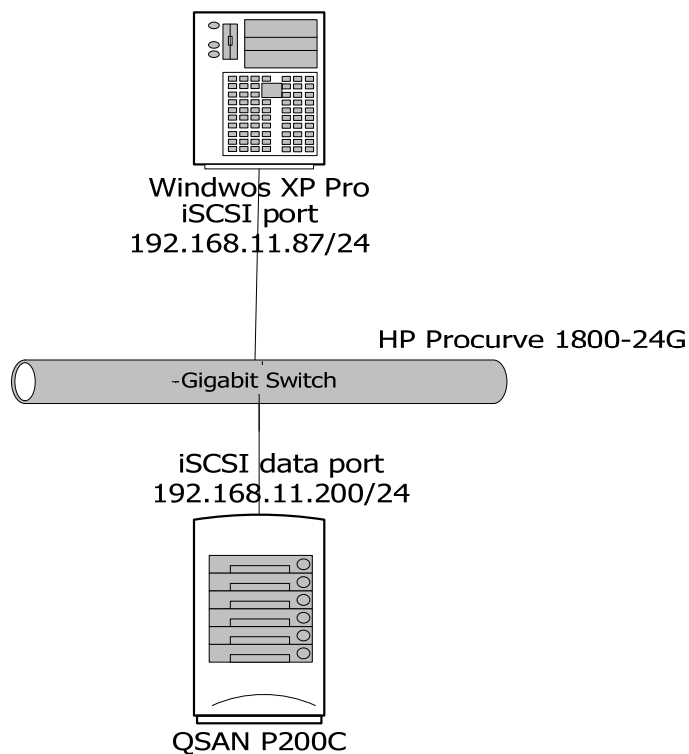
Installation
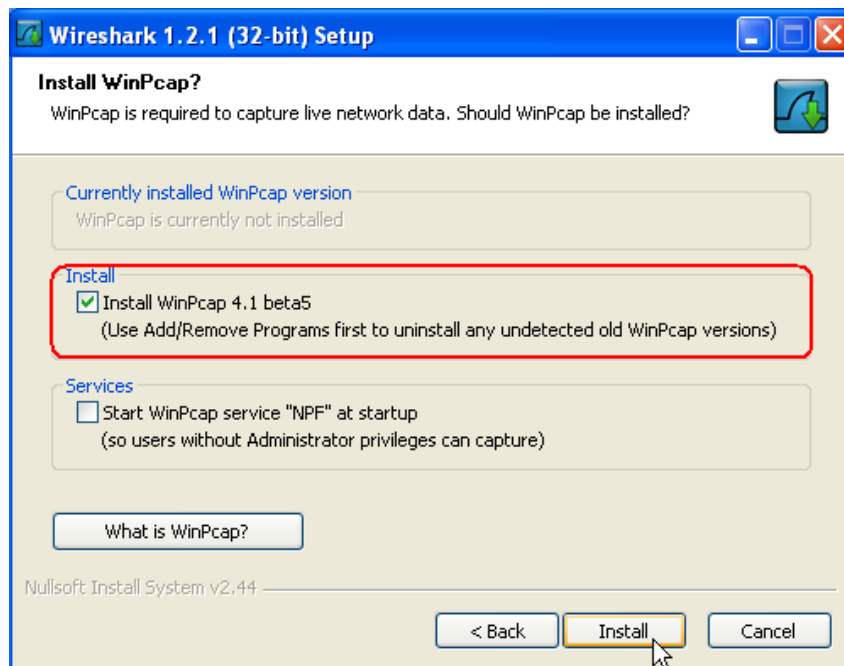
1. Please download the **Wireshark** first from the website: www.wireshark.org. The **Wireshark** version of this example is **1.2.1**.
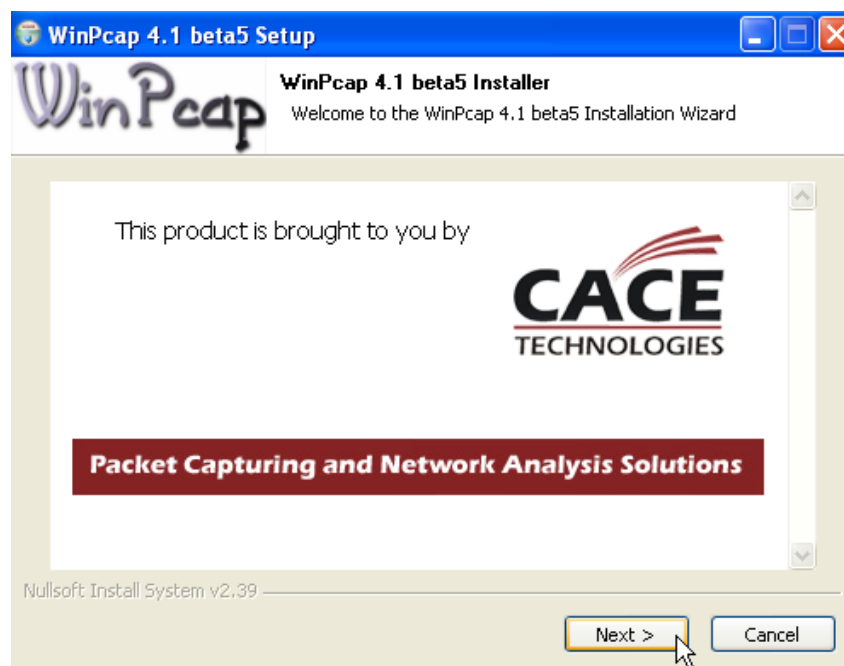

2. Run the Setup program and follow the instructions to install the **Wireshark**.

3. Be sure to select the install option of **WinPcap** which is the library for capturing the packets in Windows platform.
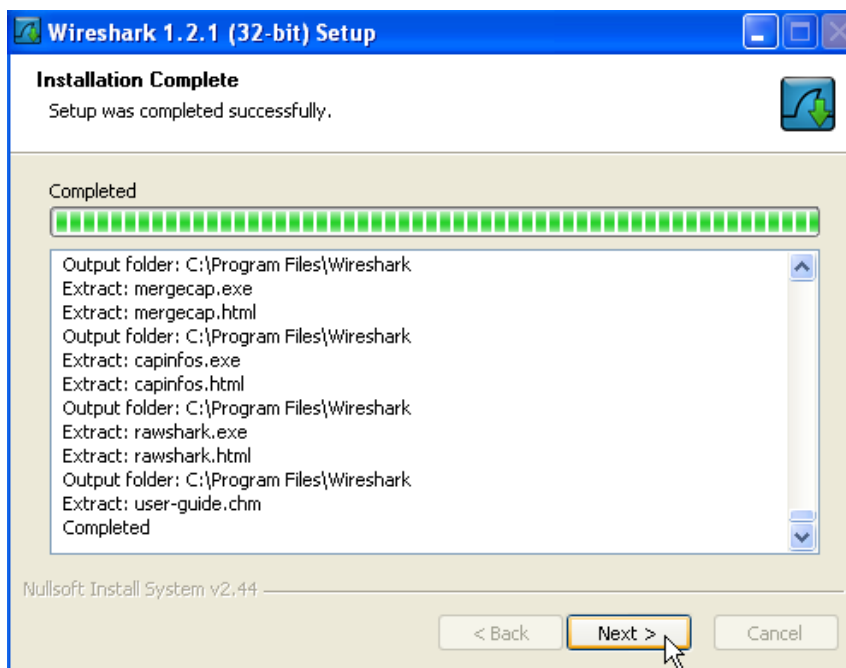
- 3 -

4. The **WinPcap** will be installed first if it has been selected, follow the instructions to finish the setup.

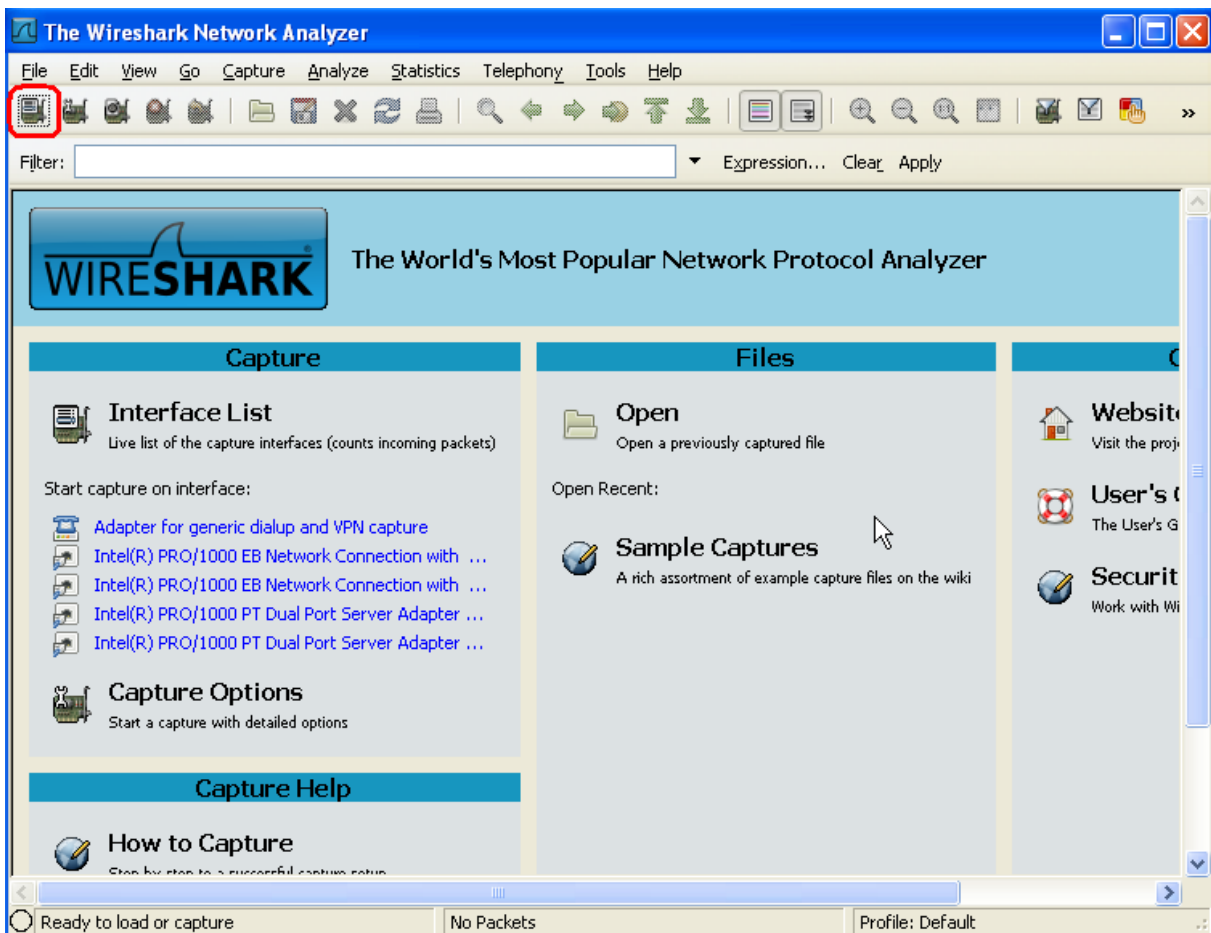5. After the installation of **WinPcap**, it continues the setup of **Wireshark**.
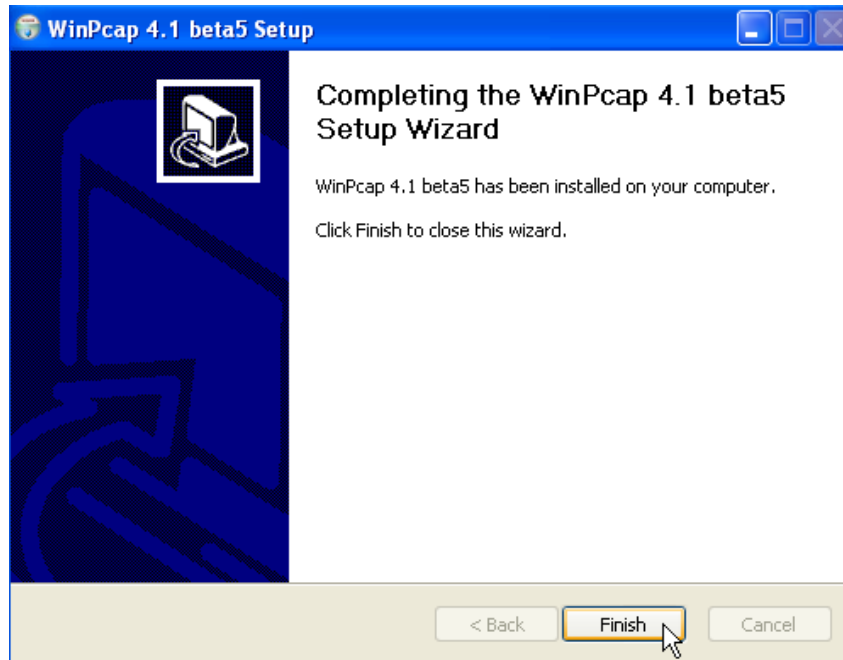
6. The setup of **Wireshark** is completed now.

Operation

Capture the network packets with **Wireshark** is very easy, please follow the procedure on the following.

1. Run **Wireshark** program and click the **List the available capture interfaces** icon which is circled in red-circled.


2. All the network interfaces will be listed. Choose the one which is used to connect to the iSCSI target, and then click **Start** button. The **Wireshark** starts to capture the entire packets which pass through this interface.
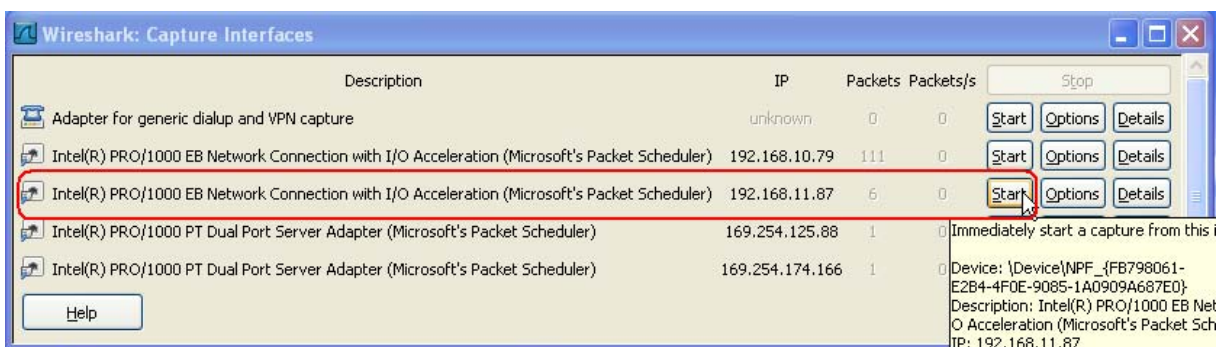
3. After **Wireshark** starts to capture the network packets, we can do the regular operation of iSCSI. For example, login the iSCSi target and have some IO with iSCSI disk. All the packets of the communication between the initiator and the iSCSI target will be captured completely.
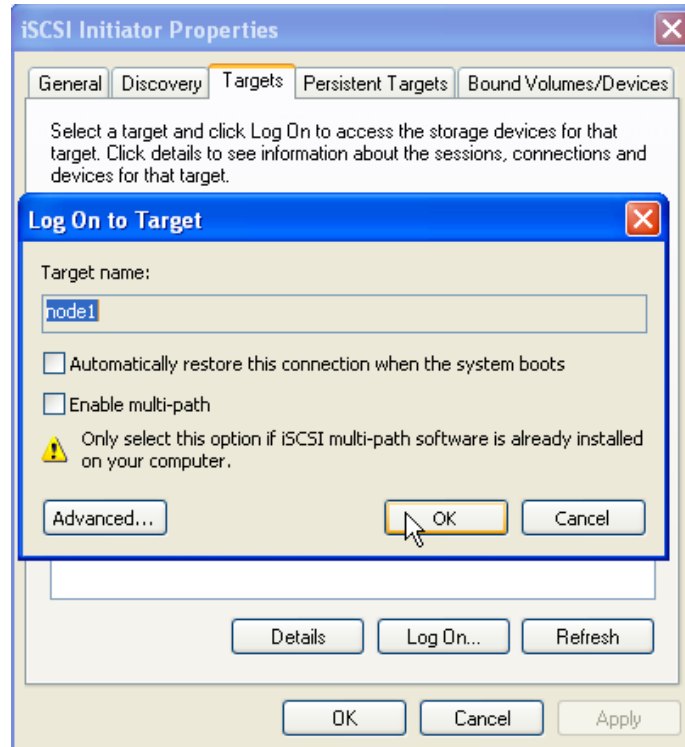

4. Click **Stop** button to stop the running capture.
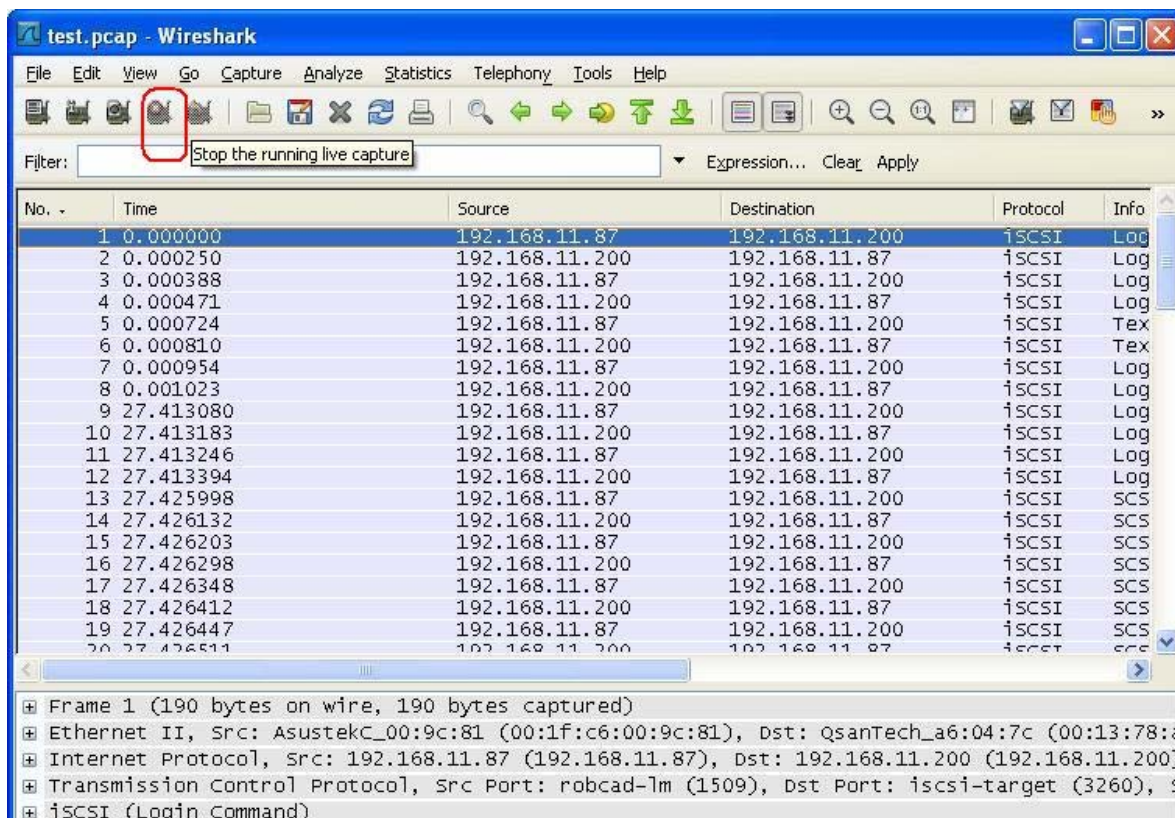
5. Because **Wireshark** will capture the entire packets pass through the specified network interface, you may get a lot of packets which you don't need. The **Filter** function can filter out the unnecessary packets.
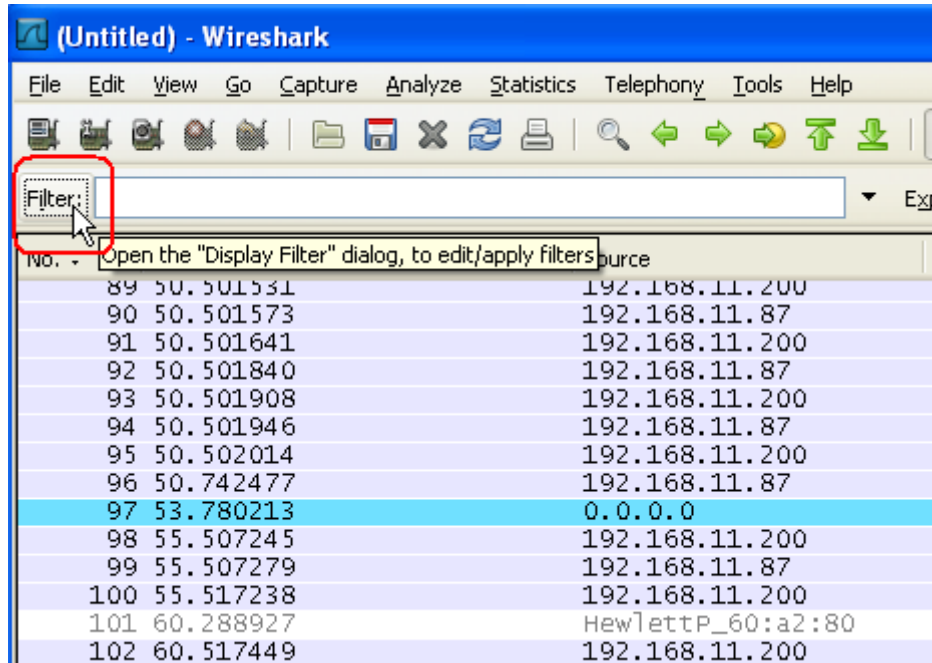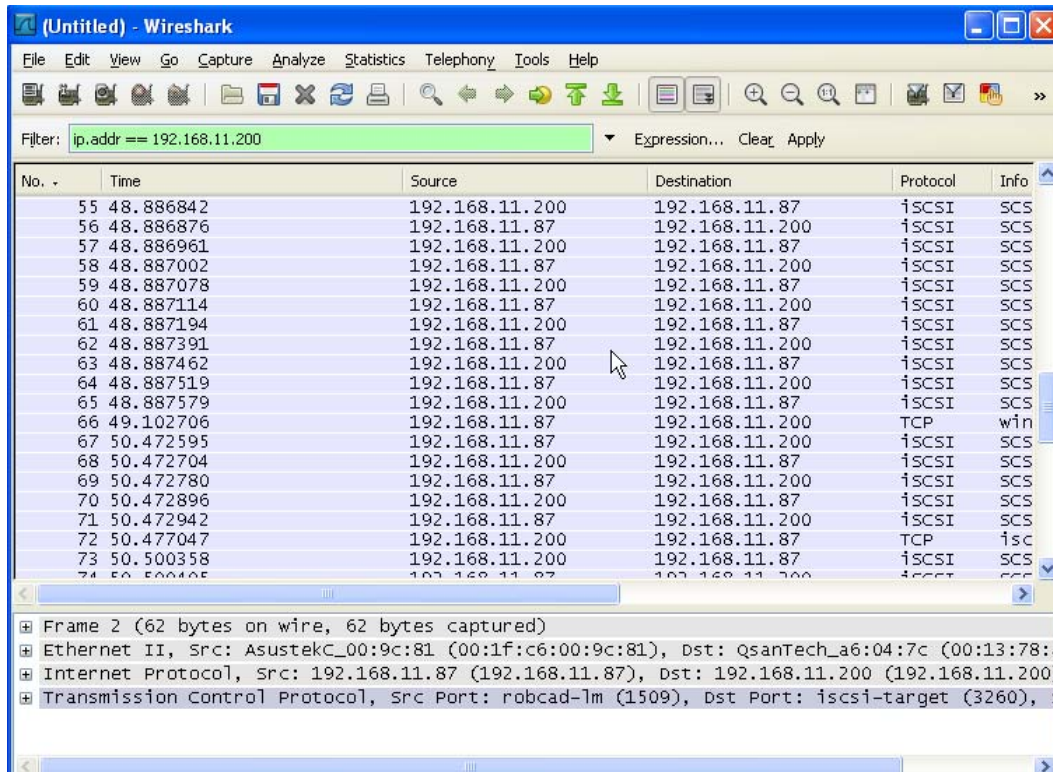

6. Click **Filter** button to pop up a dialog window. Here I use the condition of IP address which will matches the IP address of iSCSI target. Remember to change **Filter string** column with the IP address of iSCSI target.
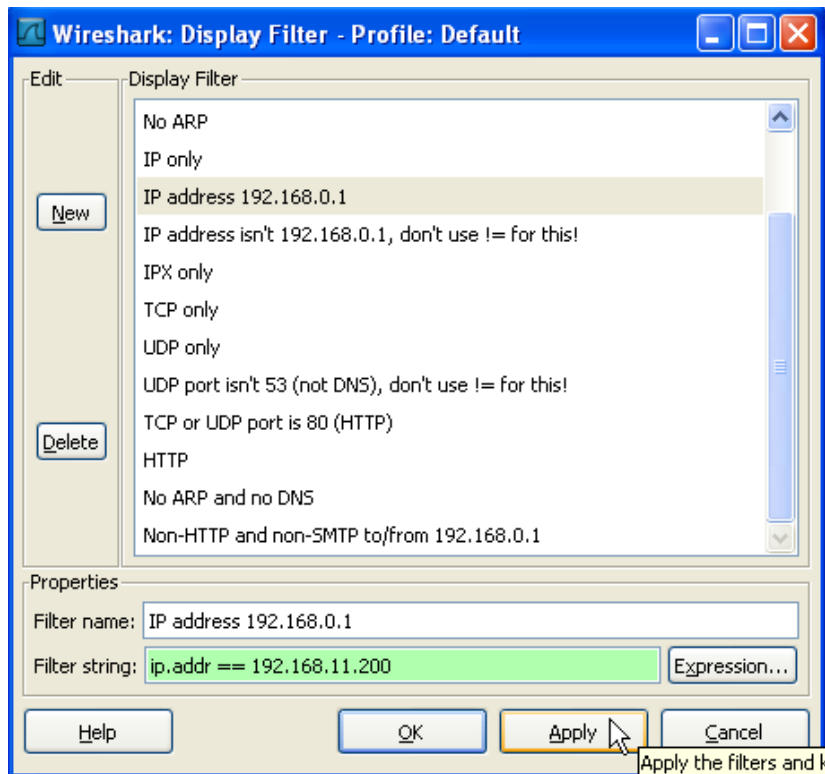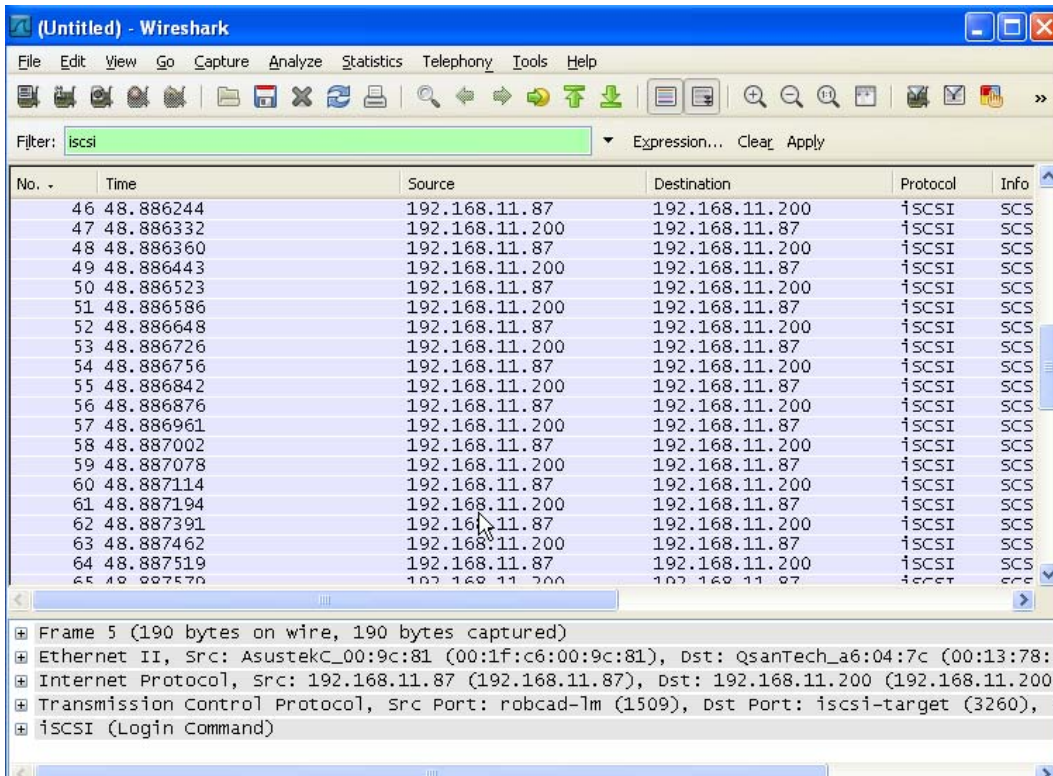
7. Now, only the packets which match the IP are kept.

8. If you want to filter out the packets which do not belong to iSCSI protocol, you can use the filter again. Input the string **"iSCSI"** in **Filter** column and click **Apply**. Then all packets which do not belong to iSCSI protocol will be filter out.

9. You can save the capture result to a file, remember to choose the radio button of **Displayed** in the **Packet Range**. This will save the packets which have been filtered.
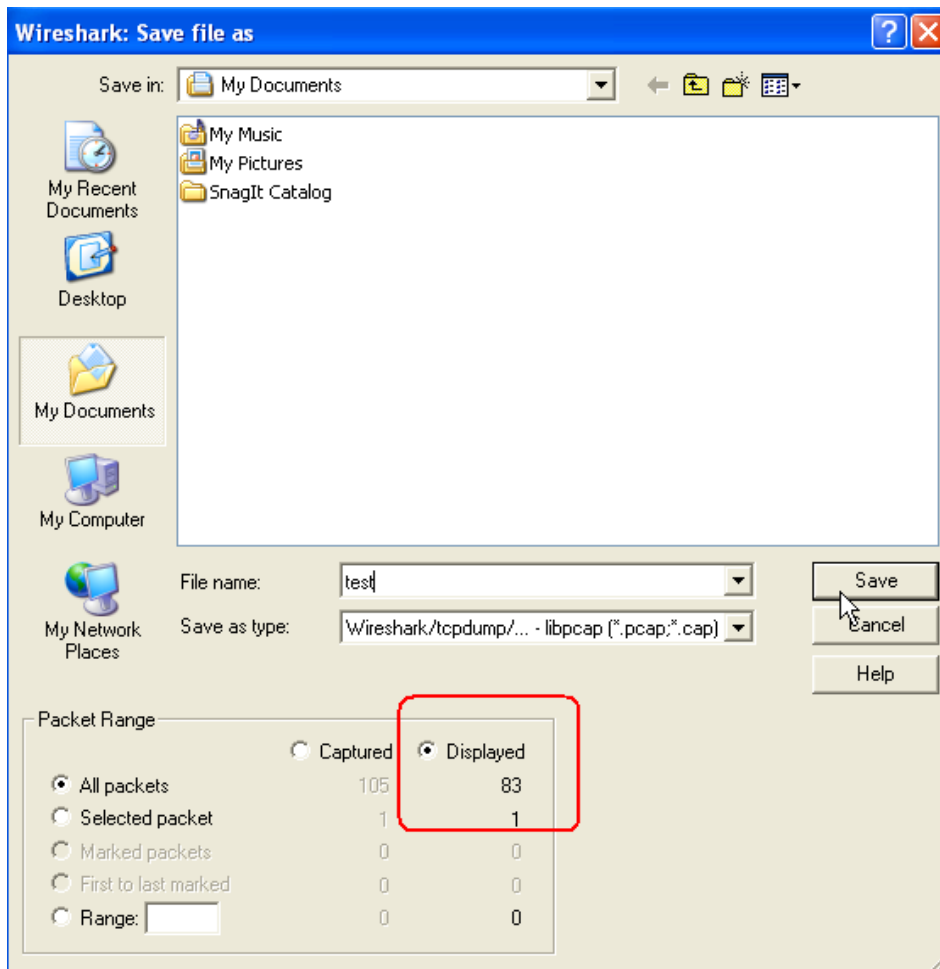
Special case

How can I capture the packets of the communication between **QSAN P series** controller and the surveillance device? In this case, you could not install **Wireshark** program in iSCSI target or surveillance device. The solution is to use the **Port Mirror** function which can mirror the network traffic from one port to another in a specified network switch. Setup a mirror port to iSCSI target or surveillance device, and then connect this port to a host with **Wireshark**. When the traffic begins, the host with **Wireshark** can do the good job.

Here I use the HP Procurve switch as an example. In the picture below, port 6 is connected to **P200C** iSCSI data port and port 1 is connected to a host with **Wireshark** installed. After setup port mirror, all packets which pass through to port 1 will mirror a copy to port 6. So I can capture the entire packets between the iSCSI target and any other network device.

Summary

In case of iSCSI initiator can not work with the iSCSI target properly, you can use the **Wireshark** to capture the packets and send them to **QSAN** Support Team. We will find out the problem by analyzing the packets. The ability of capturing the network packets will be helpful when you meet problem with the connection between the IP SAN.

Applies to

- All **QSAN P series** controllers

References

- Wireshark
  http://www.wireshark.org/