Product Version: Since nChronos 3.0

Intended Audience:

- nChronos Standard users (including *Evaluation* users)

In last chapter we've learned:

1. The user interface and components of the stat view
2. How to perform drill-down analysis among the views

Continue with our discussion on drill-down analysis that conversation (transport layer of OSI) is the deepest layer that nChronos goes, and, you may wonder, what if we need take one more step forward down to the packet level. So in this chapter we'll see how to download the packets (remember that all packets are saved on the server now) to a local file. And then we can use common network analysis tools to look into the packets.

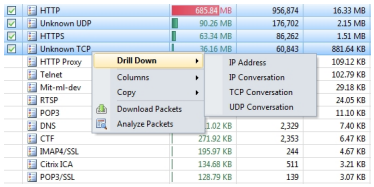
Before we jump into doing this we need to understand that the packets are on the server and we are probably using nChronos console to view the traffic analysis stats on our laptop. This means the server and console talk through network or even the Internet. Given that the server has been monitoring the network for a long time and there might be hundred gigabytes of packet volume stored on the server, it definitely not a good idea to download such huge volume of packets to our laptop through the network. Also this could be devastating to the server because it requires lots of CPU power to do this job and it dramatically affects the analysis performance (we shouldn't forget that when we download packets, the server is still capturing, analyzing and storing the packets). We should also pay attention to this even when the console and server installed on the same machine.

Well, don't be overwhelmed that we can still use packet download function. It's just that we'd better not to download a big sum of packets. We should always use the drill-down feature to narrow down the time range, IP addresses counts and packet counts that we need to download to desktop. For example, we need to check all packets that related with the **email server** only

between
23:00 – 23:15
PM yesterday. So here we know we should first locate the time range, from 23:00 – 23:15 PM yesterday night, and then we can go to the IP Address view, and find the email server's IP. Then we check the checkbox of this IP, right-click on it and we have two options on the context-menu:
Download Packets
and
Analyze Packets
.

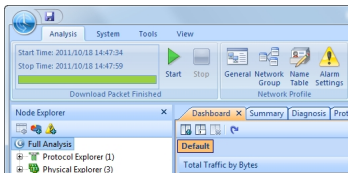
Download Packets

Download packets will retrieve the packets of the checked items on the server and send them to a packet file on our desktop. When we click the menu item, we see a new window showing the time range and filters which are the conditions to narrow down the packet range. Then select the file path and file name. We can see that nChronos is able to save the packets in two types of packet file formats; *.rawpkt* is Colasoft packet format and the popular Wireshark *.pcap* format. Lastly click
Start
to start downloading process. Downloading done, we can use analysis tools like Colasoft Capsa or Wireshark to load and analyze the packets.



Analyze Packets

Downloading packets to a local file and then running another analyzer to load the file takes too many clicks, don't you think? Don't be surprised that nChronos console has a professional network analyzer software provided by Colasoft, nChronos Network Analyzer, which is installed together with the console program. We save lots of click if we use Analyzer Packets function. It automatically downloads the packets to nChronos Network Analyzer's buffer and starts analyzing. It's a powerful yet free analyzer with all features that the commercial editions have.


Analysis
System
Tools
View
Start Time: 2011/10/18 14:47:34
Stop Time: 2011/10/18 14:47:59
Start
Stop
General
Network Group
Name Table
Alarm Settings
Download Packet Finished
Network Profile
Node Explorer
Full Analysis
Protocol Explorer (1)
Physical Explorer (3)
Dashboard
Summary
Diagnosis
Default
Total Traffic by Bytes