User Manual

DICOM Network Analyzer 5.1.1

A DVTk based tool

May 6, 2020

Table of Contents

1 Introduction

1.1 General

DICOM Network analyzer is a GUI network protocol analyzer. It is the combination of Network sniffer and DICOM protocol analyzer. **DICOM Network analyzer** 's native capture file format is **libpcap** format, which is also the format used by various other sniffer tools.

This application has the capability to:

- Sniff the live DICOM network stream.
- Save DICOM stream to a capture (.cap) file by filtering DICOM communication only between two IP addresses.
- Read cap files (saved network stream).
- Evaluate/validate DICOM communication in single/multiple DICOM association and display the overview and detail report in HTML format.
- Display Service element list and Association details per association.
- Saving the Service element (DICOM object) as DICOM (DCM) file.
- Storing/opening the current configuration/setting (.setup) files.

1.2 System Requirements

1.2.1 Operating system

The following operating systems are supported:

- Windows 7
- Windows 8
- Windows 10

1.2.2 Software requirements

The DICOM Analyzer tool requires the installation of the software packages:

- Microsoft .NET framework 4
- Npcap driver, which can be found on https://nmap.org/npcap/ .

Only the Microsoft .NET framework 4 is included in the installer package of DICOM Network analyzer.

See: http://www.dvtk.org for new versions and features.

2 Software installation

The software installation procedure of the DICOM network analyzer tool consists of the following steps:

- installation of the Microsoft .NET Framework 4
- installation of the DICOM network analyzer tool
- installation of the Npcap driver, which can be found on https://nmap.org/npcap/ (please read the license details on this website).

The first two steps of the installation process will be controlled by the DICOM network analyzer installer package. During the installation process, the installer will check if the Microsoft .NET Framework 4 is already installed on the system. If present, this step of the installation process is be skipped.

Important: before starting with the DICOM network analyzer installation, remove any previous installed version of the DICOM network analyzer tool.
Use windows “Add or Remove Programs” to remove the program.

2.1 Installation of Microsoft .NET Framework 4

Download .NET Framework 4 from Microsoft website. “Microsoft .NET Framework 4 setup” select “ I agree” to accept the license agreement. Press “install” to start the installation process. At the end of the installation procedure press “OK”
The Microsoft .NET Framework 4 software is installed.

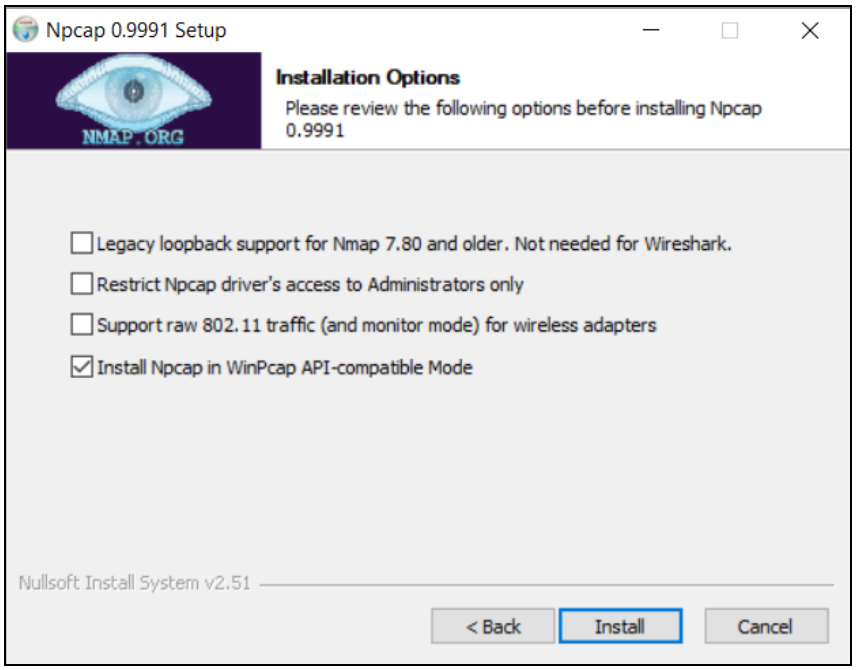
2.2 Installation of the DICOM network analyzer software

Download DICOM Network Analyzer installer (setup.exe) to a temp directory on the PC. Double click (left mouse button) on the installer and follow the installation procedure accept the license agreement.
After the button “install” is pressed, the installation will start. At the end, press the “Finish” button. The DICOM network analyzer package is installed.

2.3 Installation of the Npcap driver

Install the Npcap driver, which can be found on https://nmap.org/npcap/ .

During installation, make sure that the option “Install Npcap in WinPCap API-compatible mode” is selected.



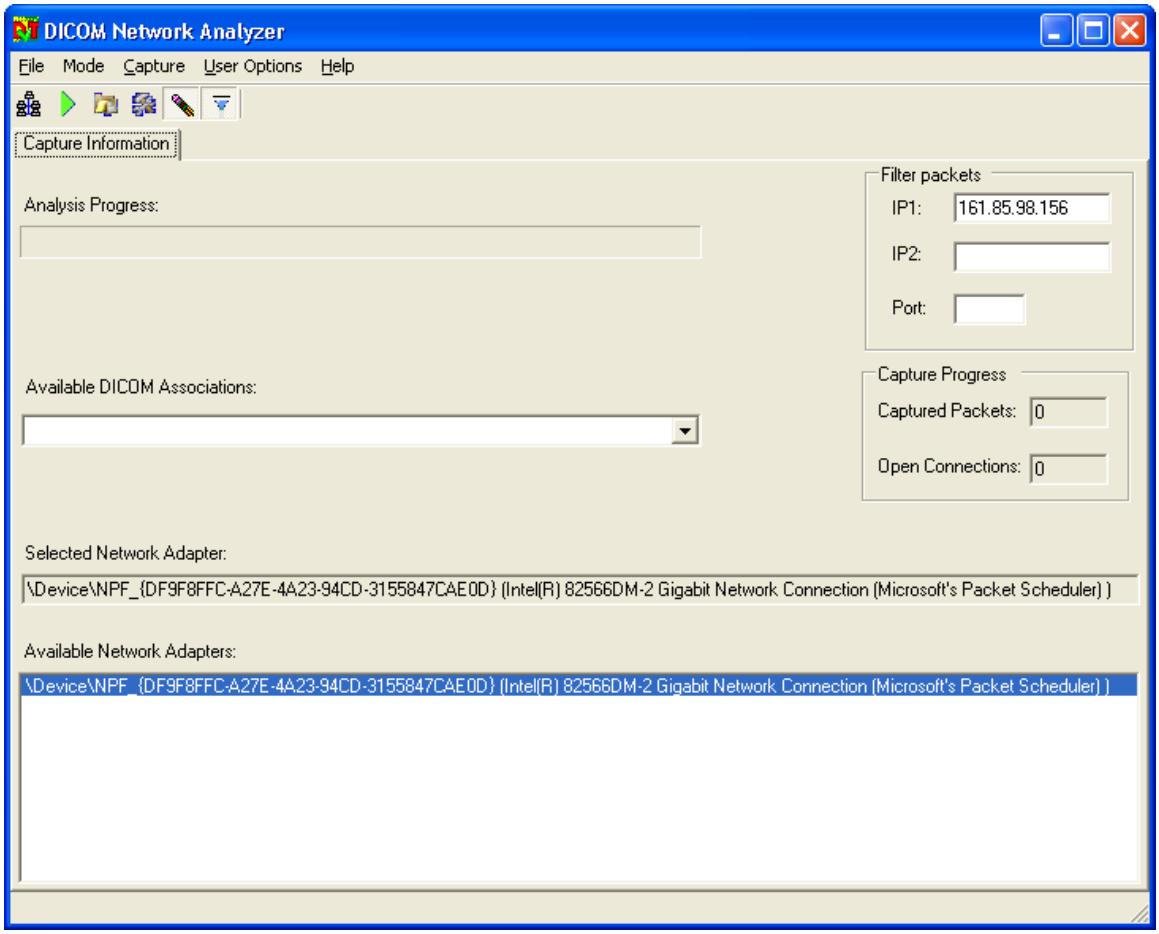
After the Npcap driver is installed, the DICOM network analyzer tool is completely installed and is ready for use.

In windows “All programs” there is an entry created “DVTK”. When selecting DVTK, a submenu with all installed DVTK applications will be opened. From this submenu the DICOM network analyzer tool can be started.

There is also a shortcut created on the desktop.

3 Capturing data

In the screen capture below, the User Interface of the capture mode is displayed.
The UI has a “menu” bar, a “toolbar” and a capture control section.
An overview of the various controls of the capture mode is given below.



Toolbar

Mode selection (toggle between capture or analysis mode)

Save results as

Save current configuration

Auto clean up enabled

Start capturing

Stop capturing

Menu

- **File**
  - **Capture File**
    - **Save in Capture File**
  - **Setup File**
    - **Load**
    - **Save**
  - **Save results as …**
  - **Exit**

- **Mode**
  - **Capture**
  - **Analysis**

- **Capture**
  - **Start**
  - **Stop**

- **User options**
  - **Dicom pixel viewer application**

- **Help**
  - **About DICOM Network Analyzer**

3.1 Capturing the live network

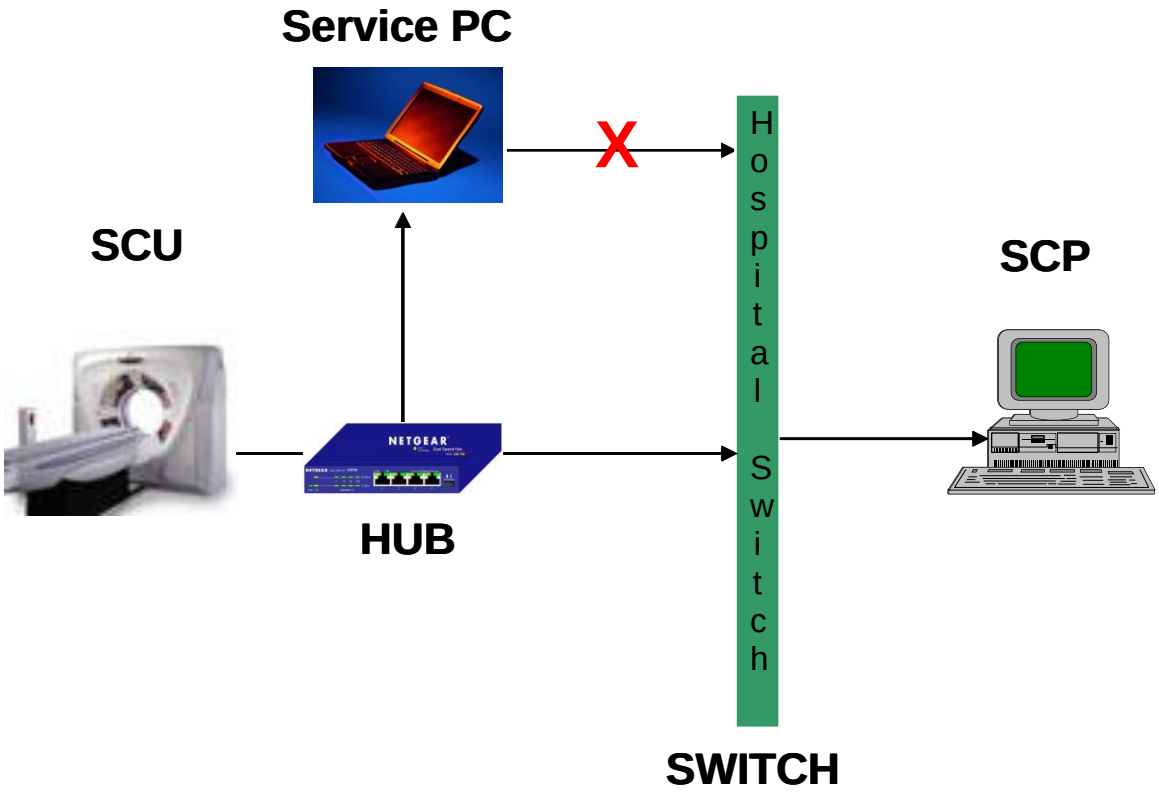
By default, the DICOM Network Analyzer tool will be started in capture mode.
In this mode, the system shows the available network adaptors that are present in the service PC. In case multiple network adaptors are present, select the network adaptor that is connected to the DICOM network to be analyzed.

3.1.1 Preparing a network capture

In the fields “IP1” and / or “IP2”, the IP addresses of the systems that are exchanging DICOM information have to be entered.
Remark: In case a system is communicating with more than 1 system, only 1 IP address has to be entered.

In case the systems are connected to the Hospital network via a switch, it is not possible to capture the data between 2 systems. In this case it is important that a HUB is used to

connect the service PC and one of the DICOM devices to the network (see drawing below)

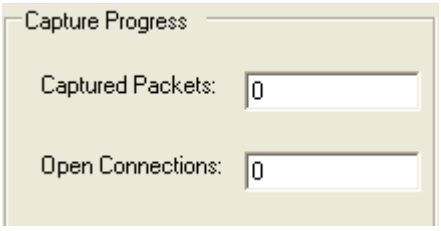


3.1.2 Starting a network capture

After all preparations are done, the network capture can be started by pressing the green arrow in the icon bar.  (= start capturing button)

During capturing, this green arrow is changed to a red square  By pressing this red square button, the network capturing can be stopped.

During capturing, the tool indicates the number of open DICOM Associations and the number of captured Packets in the “capture progress” area.



3.1.3 Stopping the network capture

At the moment that the number of captured packets is not increasing anymore and the number of open connections is 0, the capturing of data can be stopped by pressing the "stop capturing" button 

3.1.4 Saving the captured data

The captured data is stored in the internal memory of the Service PC and can be saved into a file on the internal disk by using the toolbar button  or via "File", "Capture File". "Save in Capture File".
The saved capture file will be in libpcap format and can be read by other standard tools like. Ethereal, Merge DPM etc.

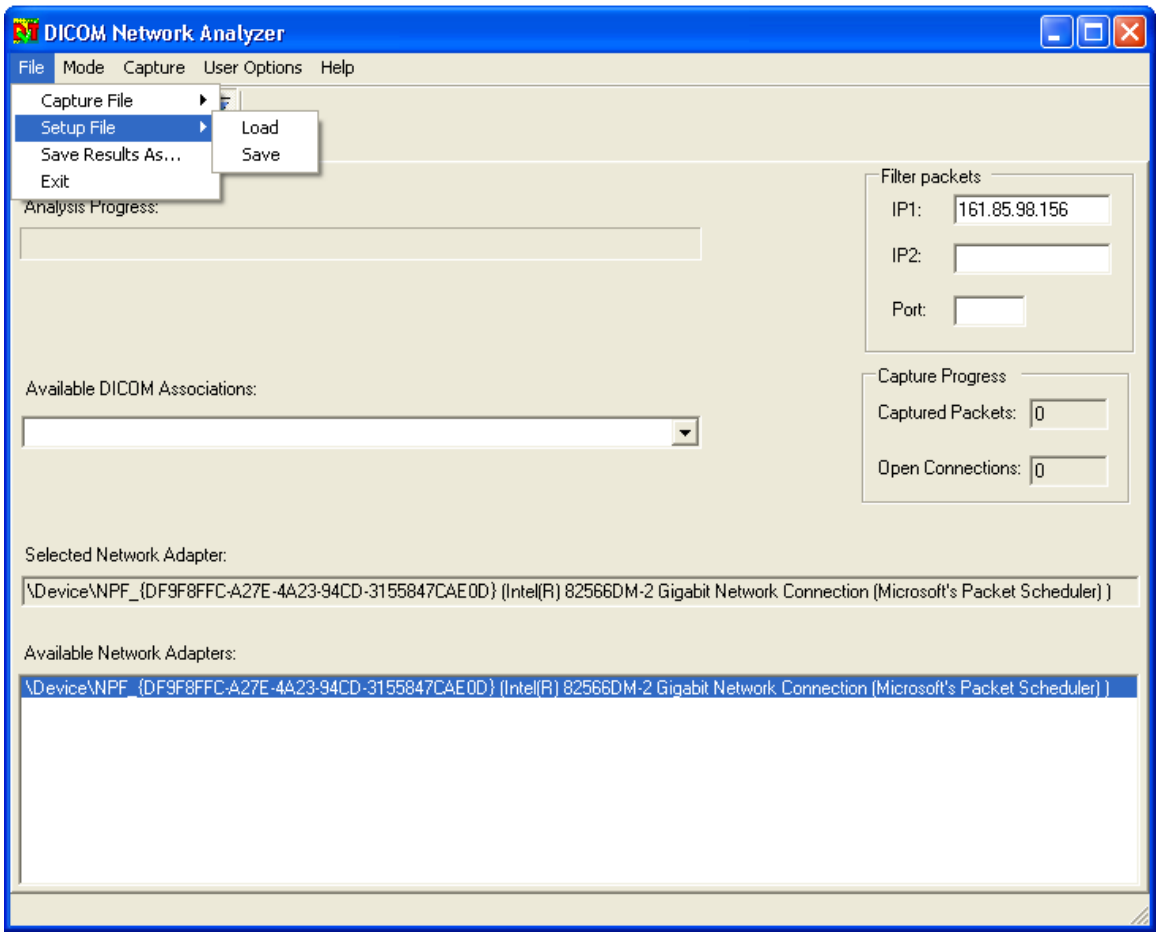
It is advisable to create a separate directory for the saved files.

Warning: do not save the capture file in the directories "C:\Program Files\DVTk\DICOM Sniffer\dcm" and " C:\Program Files\DVTk\DICOM Sniffer\results", since the contents of these directories is automatically cleared when the DICOM Network Analysis application is ended.

In case it is not required to save the capture file, an analysis of the captured data can be made without saving the data. Switching from capture mode to analysis mode can be done via the toolbar button  or via the menu "Mode", "Analysis".

3.1.5 Saving the settings (setup) of the capture tool

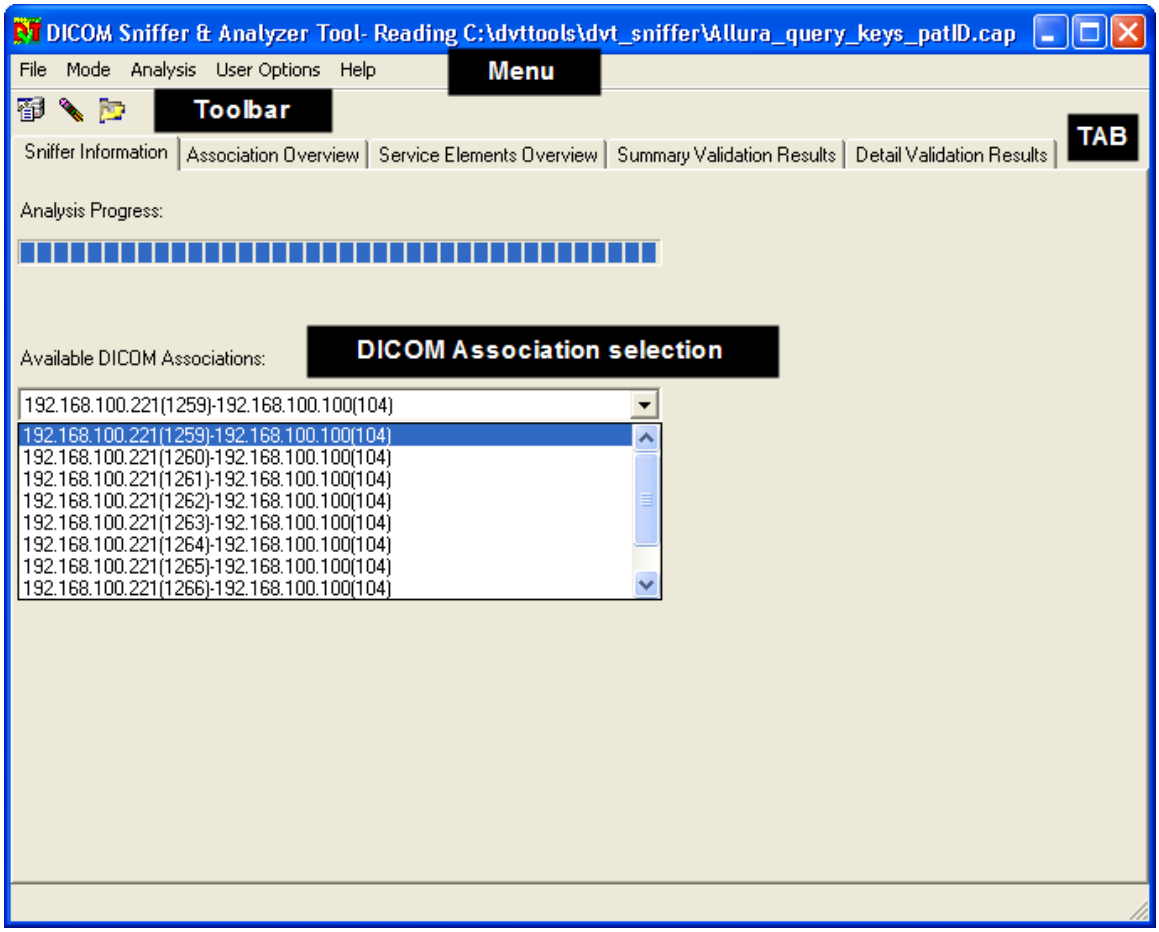
Users can save the current setup of the tool in a so called setup files.
The setup file is a XML file and contains the IP addresses that were used as filter during capturing.
With the button  (= save current configuration) or via "File", "setup file", "save" the configuration will be saved. It is advisable to create a separate "Setup" directory in the file system on disk.



4 Analyzing captured data

The DICOM network analyzer tool is able to evaluate DICOM associations that are present in the captured data.
Switching the tool from “capture” mode to analysis mode can be done with the toolbar button  or by selecting from the menu bar, “Mode”, “Analysis.

The User Interface of the DICOM network analyzer contains the following information in analysis mode:



Toolbar

Mode selection (Analysis mode selected)

Auto clean-up enabled

Read capture (.cap) file

4.1 Auto clean-up function

During the evaluation/validation process, the DVT network analyzer tool saves the following data into the file system on disk:

- all DICOM objects that are exchanged during the association are saved into the directory “C:\Program Files\DVTk\DICOM Sniffer\dcm”. For each evaluated DICOM association a separate subdirectory is created.
- All validation result files are saved into the directory “C:\Program Files\DVTk\DICOM Sniffer\results”

By default, all saved data will be automatically deleted from the file system to prevent that the file system will be filled-up completely.
The automatic deletion of data on exit of the “DICOM Network Analyzer” application can be switched off with the “Auto clean-up function” (**).**
Every time the DICOM Network Analyzer is started, the “auto clean-up” function is enabled.

4.2 Reading and analyzing captured data

The analysis mode can be started with data that has been captured and that is still in the internal memory of the system, or by loading a file with captured data from the file system on disk.

In Analysis mode, the following “Tabs” can be selected:

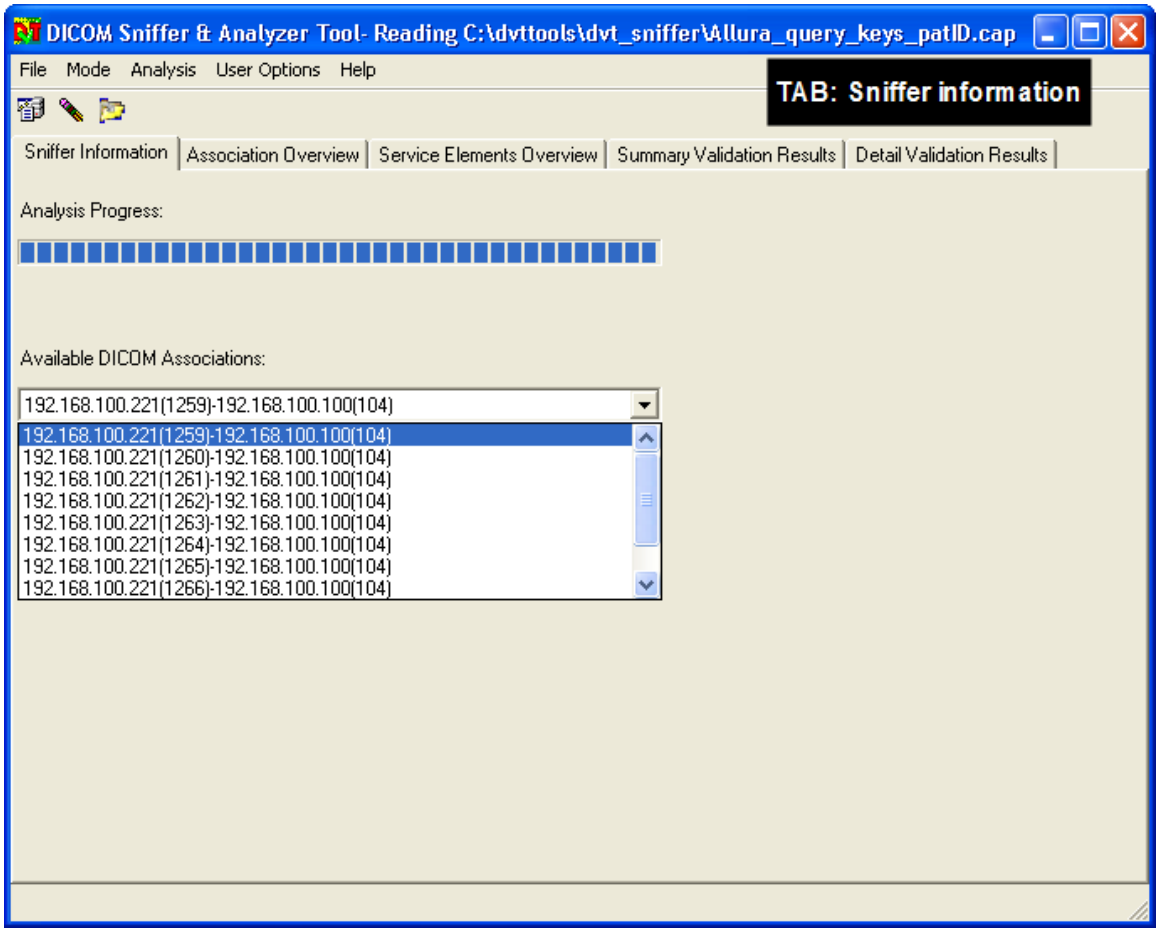
- Capture information
- Association overview
- Service elements overview
- Summary validation results
- Detail validation results.

Each “Tab” will open a new window. For each tab, an explanation of the displayed information is given in the chapters below.

4.2.1 Capture information

In this TAB, the overview is given of all DICOM associations that are available in the analyzed network capture data.

Remark: in case the capture data is loaded from a file, the name of this file is displayed at the top of the window.

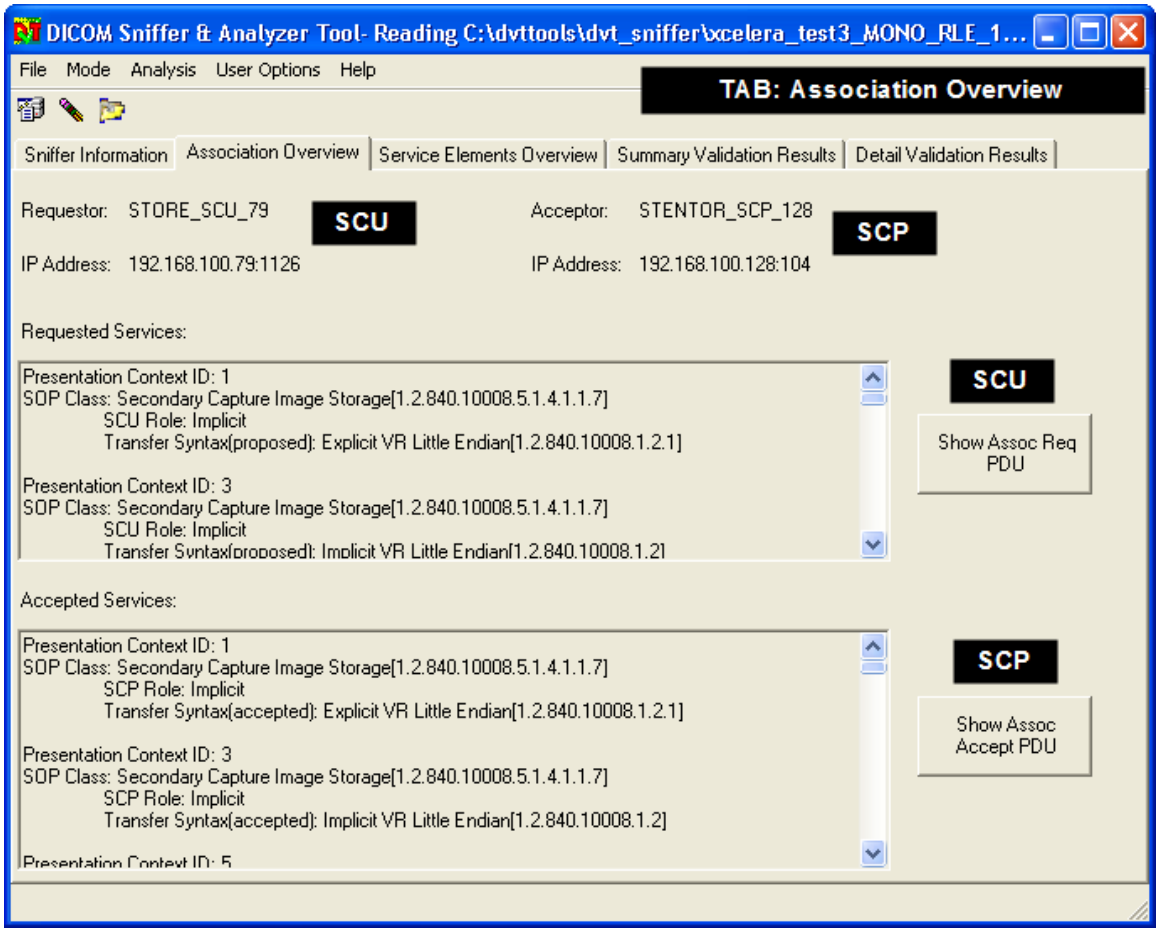


Each of the available DICOM associations can be selected for analysis.

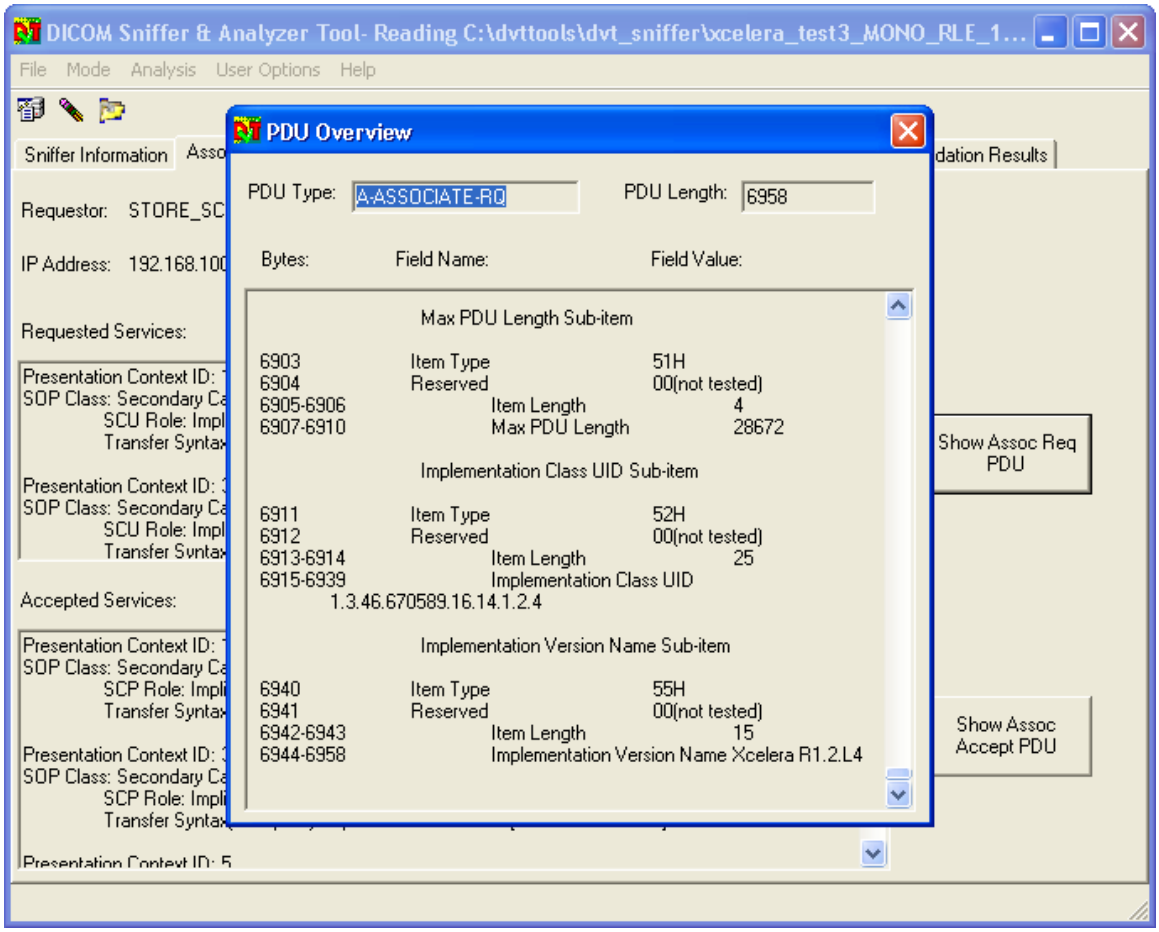
4.2.2 Association overview

In the Association Overview Tab, information is given about:

- AE title SCU
- Port number used by SCU
- IP address of SCU
- AE title of SCP
- Port number of SCP
- IP Address of SCP
- Proposed combinations of DICOM SOP class and transfer syntax (Presentation context ID) by SCU
- Accepted presentation context ID's (DICOM SOP classes and transfer syntax) by SCP
- Rejected presentation context ID's by SCP



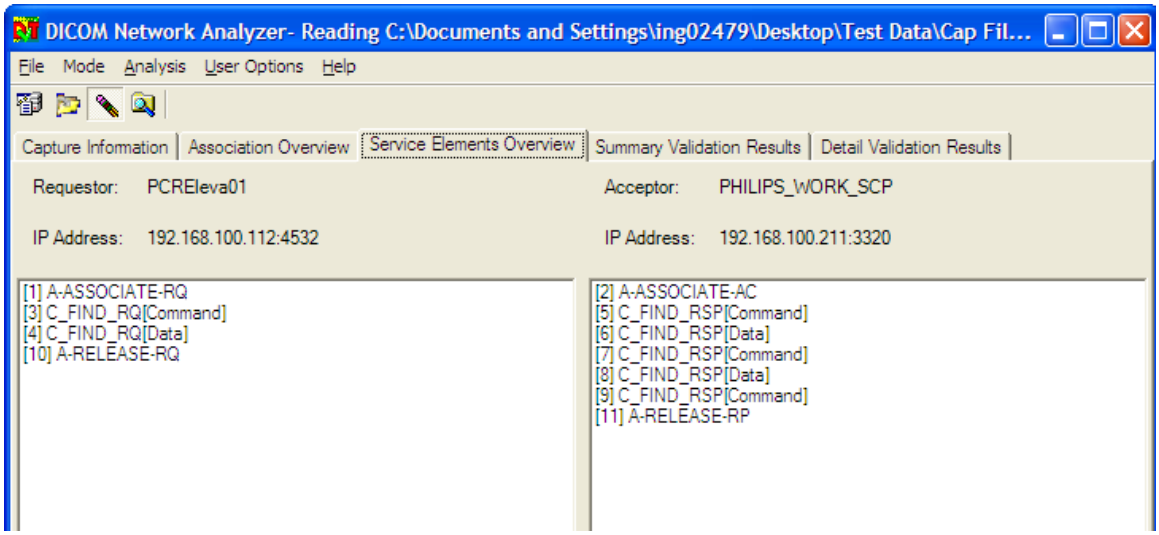
Details about implementation class UID's, Implementation Name, PDU size etc. are displayed by pressing the "Show Assoc Req/Accept PDU" button.



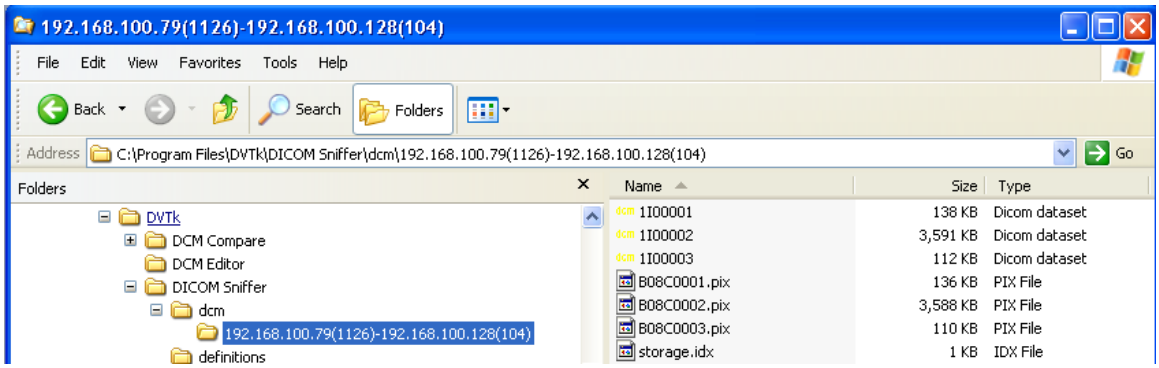
In this example, the DICOM SCU proposes a PDU size of 28672 bytes, is using the Implementation class UID = 1.3.46.670589.16.14.1.2.4 and Implementation Version Name = Xcelera R1.2L4. By using the scroll bar in the PDU Overview window, more association information is given.

4.2.3 Service elements overview

In the tab “Service elements Overview” an overview is given of the service elements that are included in the association.



In this example, in the analyzed association 4 image objects are transferred from the DICOM SCU (192.168.100.112:4532) to the SCP system (192.168.100.211:3320)

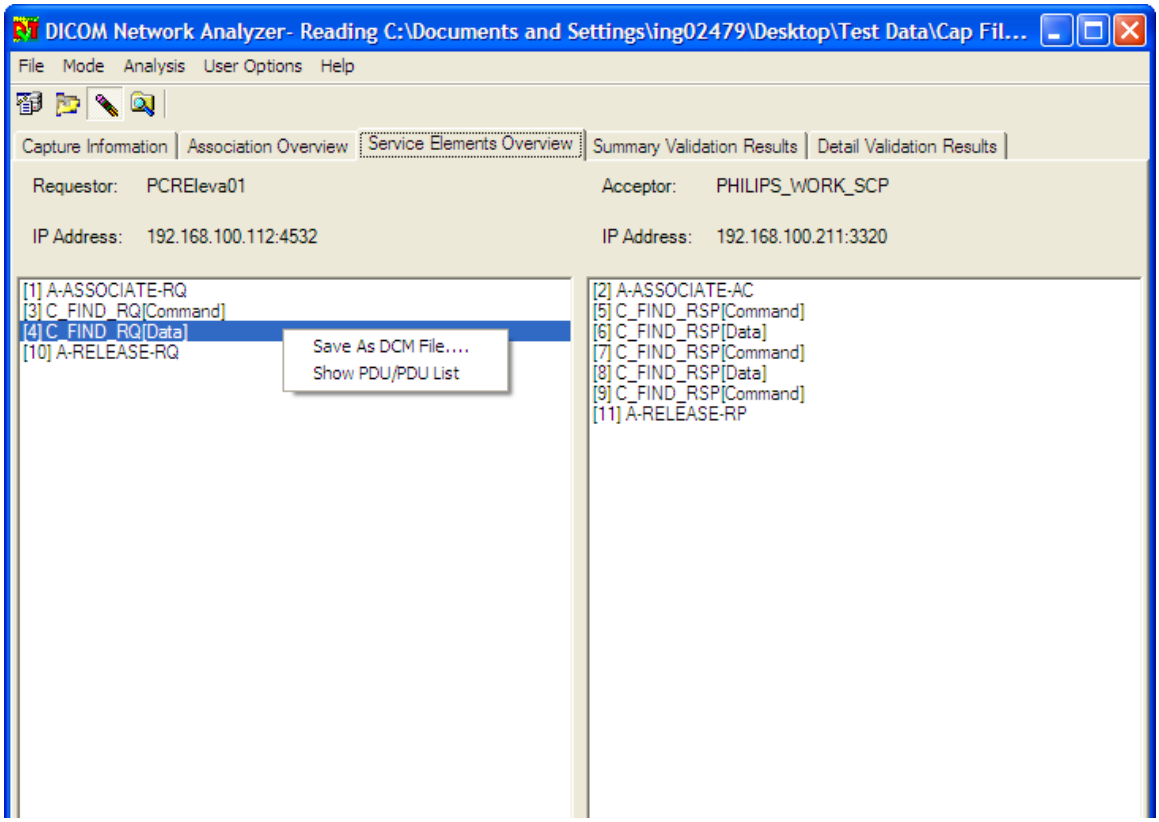


The transferred DICOM Image objects are saved in the directory: "C:\Program Files\DVTk\DICOM Sniffer\dcm\192.168.100.79(1126)-192.168.100.124(104) with file names 1I00001.dcm. 1I00002.dcm and 1I00003.dcm. The other files in this directory (.pix and .idx) are for internal use by the DICOM network analysis application.

The saved DICOM objects can be used as input for other DICOM applications like DICOM Viewer, DICOM editor, DICOM compare etc.

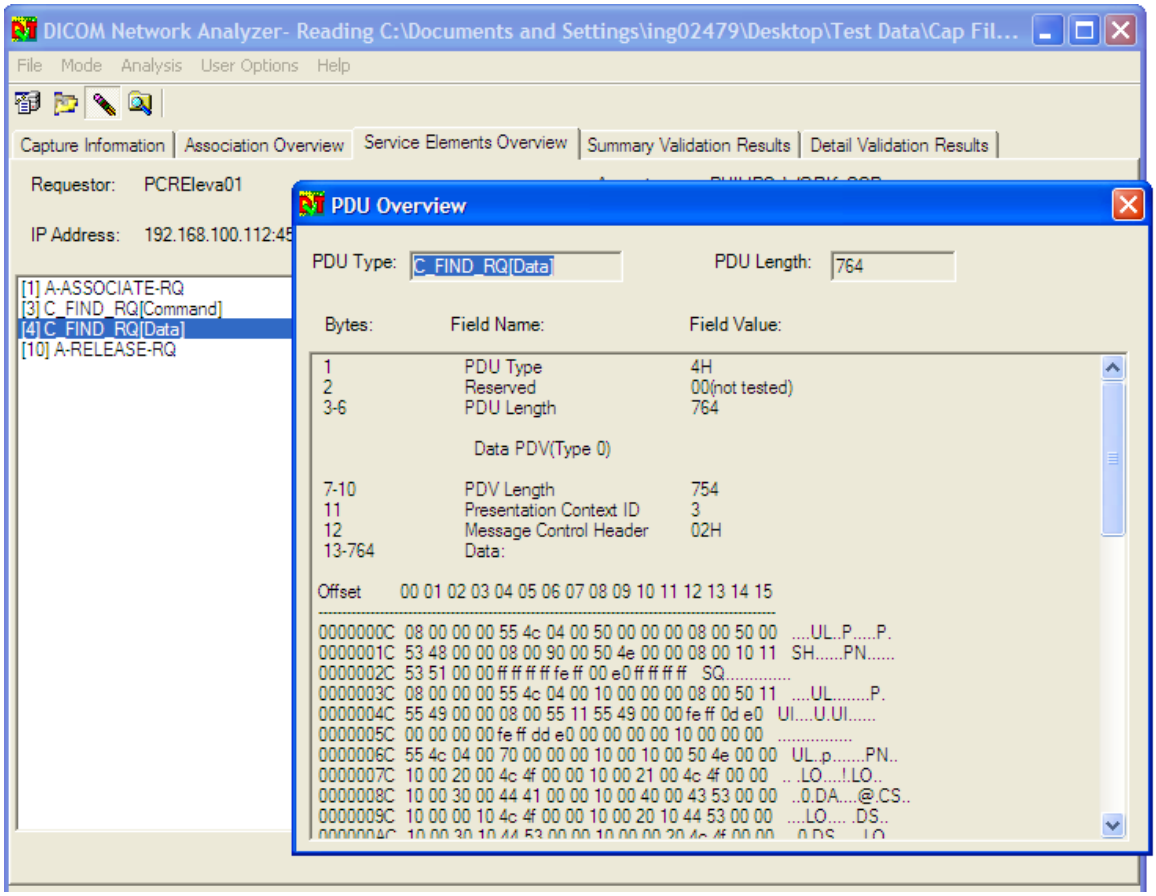
Saving individual DIMSE (DICOM object)

In the service elements overview window, it is also possible to save individual DICOM data objects. This can be done by selecting a DIMSE that contains "data" information and pressing the right mouse button and selecting the function "Save as DCM file "from the drop down list.



Show overview of all PDU's

From the same drop down list, the function "Show PDU/PDU list " can be used to get an overview of all PDU's of the selected DIMSE. Also user can view the PDU byte dump for in-depth analysis as shown in the screen shot below.

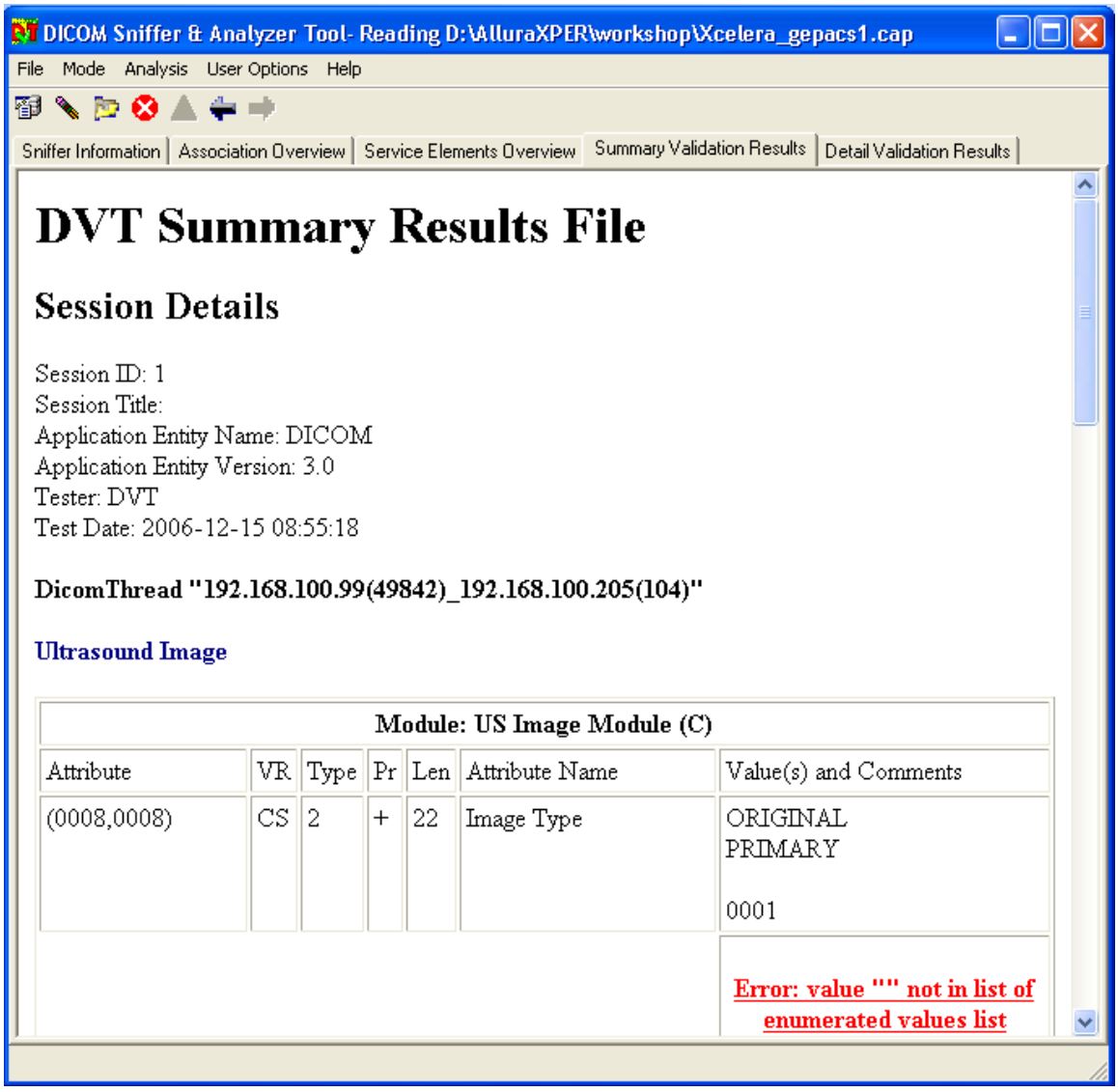


Viewing DICOM objects

For C-STORE-RQ data DIMSE elements, it is possible to view the pixel data in a DICOM viewer. This will only work in case in “user options” in the menu bar a link is made to a DICOM viewing application.
By clicking on “Show pixel data” in the drop down list, automatically the viewing application is launched with the selected pixel data of the selected C-STORE-RQ (data) DIMSE.

4.2.4 Summary validation results

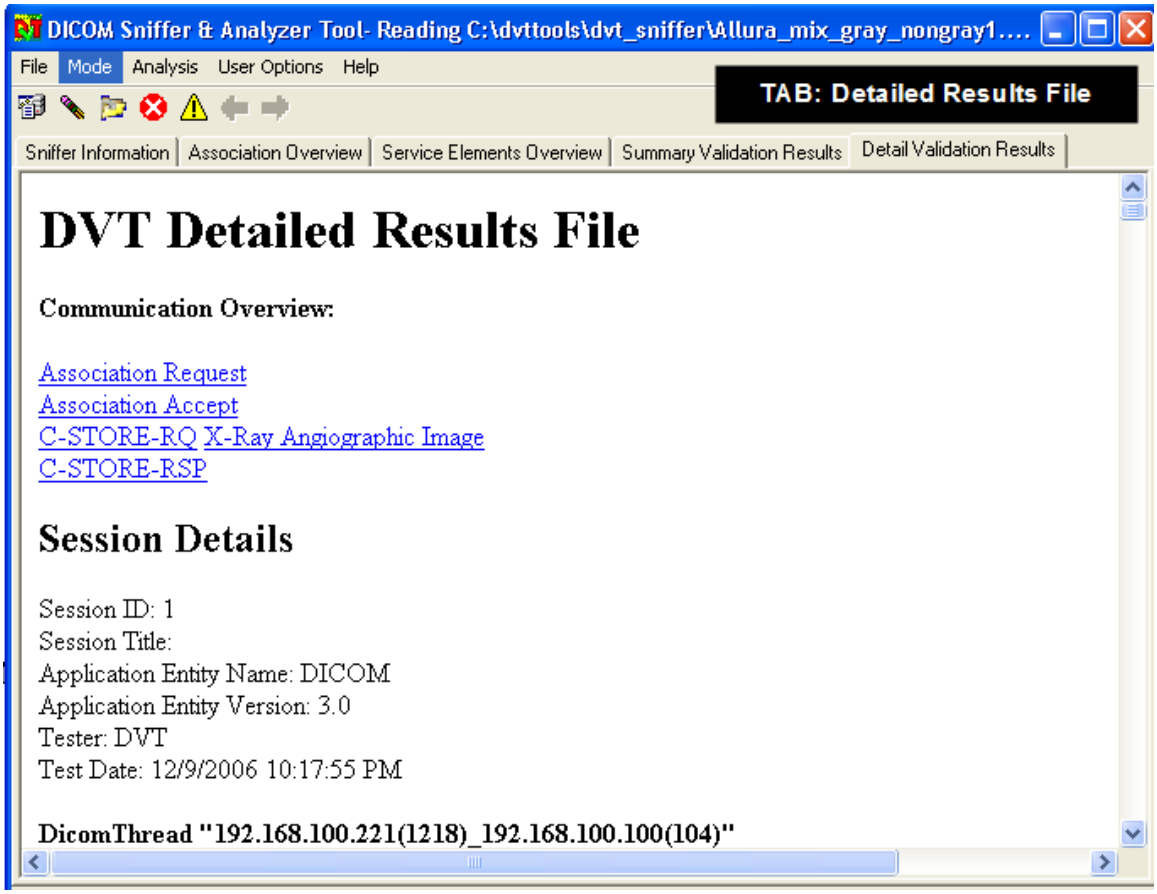
By pressing the tab “summary validation results”, the system shows the results of the DICOM validation process. DICOM violations like missing type 1,2 attributes or type 1 attributes present without a value, will be reported as validation errors.
Also syntax and semantic violations against the DICOM standard will be reported here. In the example below, there is an error reported with the value of the Image Type attribute (0008,0008).



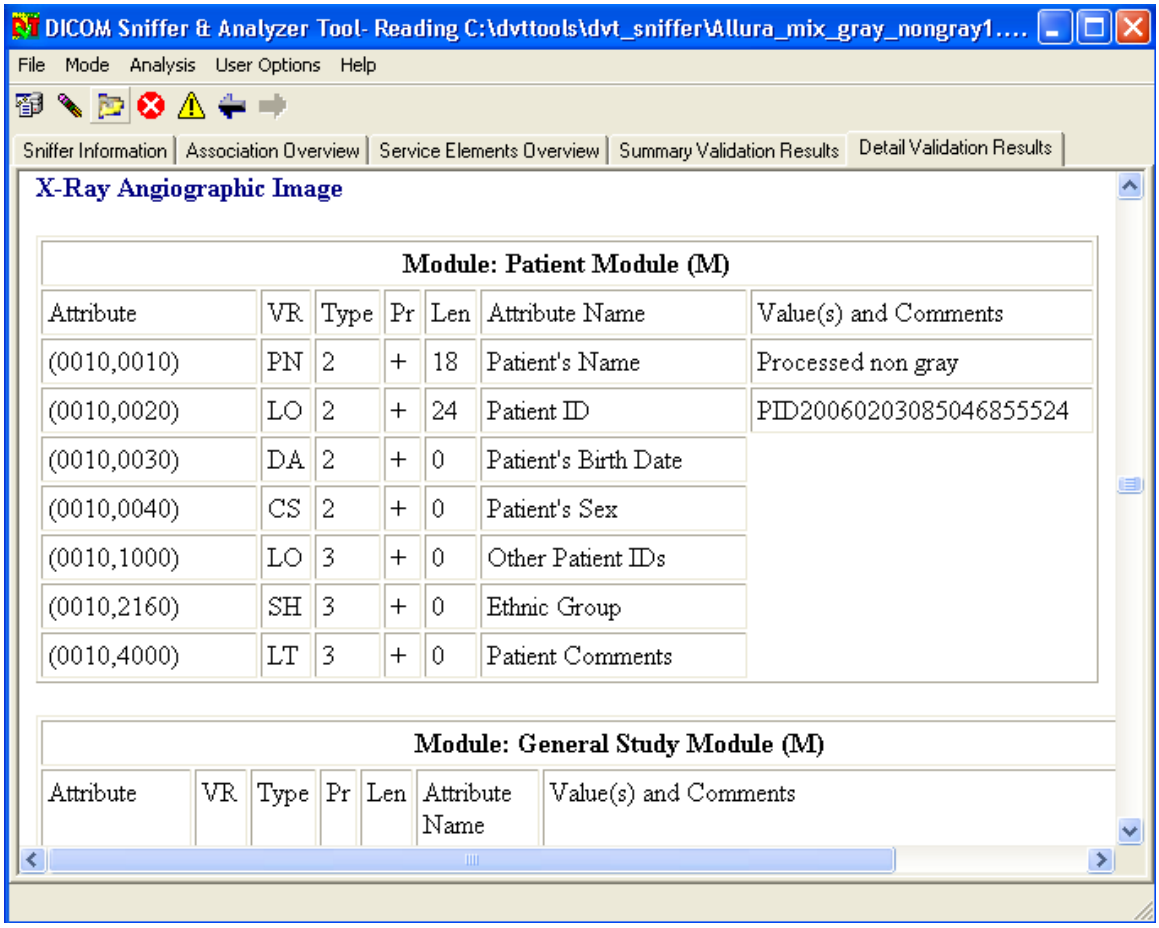
4.2.5 Detail Validation Results

By pressing the tab “Detail Validation Results”, the system shows in the section “Communication Overview” an overview of all Service elements (DIMSE) that are present in the selected DICOM association.
In the example below, the analyzed association contains an Association Request, an Association Accept, a C-STORE-RQ and a C_STORE-RSP DIMSE.

In the directory C:\Program Files\DVTk\DICOM Sniffer\results\20061205_215432 the validation results file and a summary document is saved. For each DICOM object in the association a validation results file is created. A summary document is made for each association.



By pressing in the communication overview on one of the listed “links”, the analyzer will jump to the section in the results file where the validation results are given for the selected DIMSE.
In the screen capture below, the validation result for the DIMSE “C-STORE-RQ X-Ray angiographic Image” is displayed.
Just above the validation result section, a complete dump of the DICOM object is listed. (Use the window slider to scroll through the validation result file)



The summary and detailed results files are also saved in the file system on disk.
In case these results files are required for further analysis, take care that these files are not automatically deleted when the DICOM network analyzer application is ended. (Disable the “auto clean-up” function before stopping the application or copy the files manually to another directory in the file system).