User Manual

Revision 2.00

Manual of the DICOM Detective Enterprise

Copyright© 2009 by DICOM Tool Co.

Do not duplicate

DICOM Tool

THIS PAGE LEFT INTENTIONALLY BLANK

Revision History

Revision	Date	Description
0	October, 2003	Creation of the document.
1.0	December, 2003	Release 1.0.
1.01	June, 2005	Release 1.01. Find function and support for structure report viewer added.
1.02	December, 2006	Release 1.02. Support Chinese, Japanese JIS and Shift JIS; Export file name changed.
1.1	October, 2007	Release 1.1. Following functions added: • Export DVT script. • Export Merge DPM User Info. • Auto Encoding. • Chinese, Korean, Western Europe language support. • Verify DICOM Tag, VR, VM and Value length. • Add Error column to display errors. • Drag a capture file or DICOM file from windows explorer and drop to DICOM Detective to open the file. • Show packet number and time for PDUs and service elements. • Show binary detail for PDUs. • Display general information in content column for folded nodes. • Add DICOM Image viewer button to dataset. • Add Continue button to continue the simulation without hesitation. • Add save dataset function to dataset.
1.11	February, 2008	• 2008 DICOM Dictionary. • Open capture file from Merge toolkit. • View image embedded in sequence element.
1.12	May, 2008	Release 1.12. Following functions added: • Find DICOM Files • Support invalid VR OX and XS.
1.13	June, 2008	Release 1.13. Following functions added: • Added VR column
1.14	April, 2009	Release 1.14. Following functions added: • Undefined length is calculated and displayed.
2.00	June, 2009	Release 2.00. Following functions added: • New file format supported: Accenlent 5views capture, Wireshark – nanosecond libpcap, Wireshark big-endian libpcap. • Inserting/Deleting/Editing DICOM elements (include sequence elements) for DICOM file and save it.

		• Inserting/Deleting/Editing DICOM elements (include sequence elements) for capture file and save it. • Statistics Views for capture file to show data transmission rate, patient transmission rate, study transmission rate, series transmission rate, image transmission rate and frame transmission rate etc. • Time display format selection (Sec.since beginning of capture, YYY-MM-DD HH:MM:SS.M and Sec. since Epoch(1970-01-01)) for capture file. • Option to open capture file directly if only one connection. • Option to skip error message while opening capture file. • Supports WinPcap packets Capture, analyzes data while capturing (Dynamic Analyze). • Support remote capture of WinPcap. • Support Gateway Capture for devices that cannot install capturing software. • Dynamic dump DICOM info to text file while DICOM transferring. • Dynamic gathering data transmission rate, patient transmission rate, study transmission rate, series transmission rate, image transmission rate and frame transmission rate etc. while DICOM transferring. • Show transmission rates dynamically in tables and a line chart. • Show network interface status dynamically. • Records DICOM network transmission rates in history files and show the history of transmission rates in line chart. • Command line for exporting txt, DVT script and MergeDPM User Info.

Manual of the DICOM Detective Enterprise

TABLE OF CONTENTS

1 OVERVIEW

1.1 Intended Audience and User

The reader of this document is concerned with DICOM product service and DICOM software source codes tracing and debugging. It is assumed that the reader of this document is familiar with the DICOM v3.0 standard.

The obvious users of the software described in this menu are DICOM service man, programmer and consultant.

1.2 Scope and Purpose

This document presents the DICOM Detective. It describes how to use the supported network protocol analyzers with the DICOM Detective; it also describes the installation and usage of the DICOM Detective and serves as a user's menu.

1.3 Terminology

Following Terms are used in this document.

ASCII	American Standard Code for Information Interchange.
ACSE	Association Control Service Element.
AE	Application Entity.
C-ECHO	The C-ECHO service is invoked by a DIMSE-service-user to verify end-to-end communications with a peer DIMSE-service-user. It is a confirmed service.
C-MOVE	The C-MOVE service is used by a DIMSE-service-user to match a set of Attributes against the Attributes of a set of composite SOP Instances maintained by a peer DIMSE-service-user, and retrieve all composite SOP Instances which match. It triggers one or more C-STORE sub-operations on a separate Association. It is a confirmed service.
C-STORE	The C-STORE service is used by a DIMSE-service-user to store a composite SOP Instance on a peer DIMSE-service-user. It is a confirmed service.
CT	Computerized Tomography.
Data	A unit of information as defined by a single entry in the data dictionary.
element	An encoded Information Object Definition (IOD) Attribute that is composed of, at a minimum, three fields: a Data Element Tag, a Value Length, and a Value Field. For some specific Transfer Syntaxes, a Data Element also contains a VR Field where the Value Representation of that Data Element is specified explicitly.
DICOM	Digital Imaging and Communications in Medicine.
DIMSE	DICOM Message Service Element.
DVT	DICOM Validation Tool.
GB18030	GB18030 is the registered Internet name for the official character set of the People's Republic of China (PRC) superseding GB2312. This character set is formally called "Chinese National Standard GB 18030-2000: Information Technology -- Chinese ideograms coded character set for information interchange -- Extension for the basic set".
GB2312	GB2312 is the registered internet name for a key official character set of the People's Republic of China, used for simplified Chinese characters.

	GB abbreviates Guojia Biaozhun, which means national standard in Chinese.
IP	Internet Protocol.
ISO	The International Organization for Standardization (Organisation internationale de normalisation), widely known as ISO, is an international standard-setting body composed of representatives from various national standards organizations.
JIS	JIS encoding refers to several Japanese Industrial Standards (JIS X 0201, JIS X 0208, JIS X 0213 and JIS X 0202) for encoding the Japanese language.
MDI	Multi-Document Interface.
PDU	Protocol Data Unit.
PDV	Presentation Data Values.
SCP	Service Class Provider. We deem that SCP is the application that accepts the communication.
SCU	Service Class User. We deem that SCU is the application that initializes the communication.
Shift-JIS	Shift-JIS is a character encoding for the Japanese language originally developed by a Japanese company called ASCII Corporation in conjunction with Microsoft and standardized as JIS X 0208 Appendix 1.
SOP	Service-Object Pair.
UID	Unique Identifier.
UTF-8	Unicode Transformation Format – 8.
VM	Value Multiplicity.
VR	Value Representation.

2   SYSTEM REQUIREMENTS

Following system requirement is required to install and use DICOM Detective.

Category	Requirement
Operation System	Microsoft Windows 95, 98 or Microsoft Windows NT/2000/XP/2003/Vista

One of following network analyzers is required to get the input for the DICOM Detective.

Category	Requirement
Capture Driver	WinPcap (http://www.winpcap.org)
Network Analyzer	One of the following: • NetXRay® 2.5 or greater (e.g. Sniffer Pro® 4.5) • Distinct Network Monitor® 4.2 or greater (use *.dnm files) (http://www.distinct.com) • Shomiti Surveyor® 2.4 or greater, snoop file format (http://www.shomiti.com) • Ethereal® 0.9.15 or greater (http://www.ethereal.com/) • WireShark® 0.99.6 or greater (http://www.wireshark.org) • 5 view Product Suite (http://www.infovista.com)

3   INSTALLATION

You must have the administrator privileges to install the DICOM Detective. Run the setup.exe (install.exe for trial version) to install the DICOM Detective. Figure 1 to Figure 7 illustrate steps for the DICOM Detective installation.

During installation, user should enter authorized user name, company name and product ID. **Without authorized product ID, the installer would not proceed and no warning is given.** Ask service@dicomtool.com for authorized product ID.

Although user can make many selections, basically what user needs to do is only click "Next" button and "Finish" button.
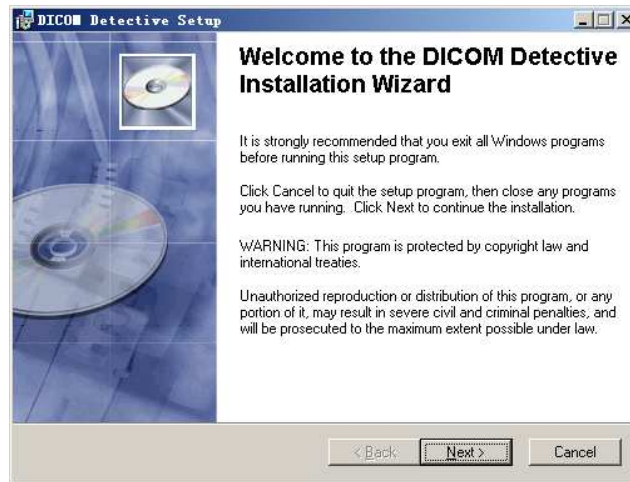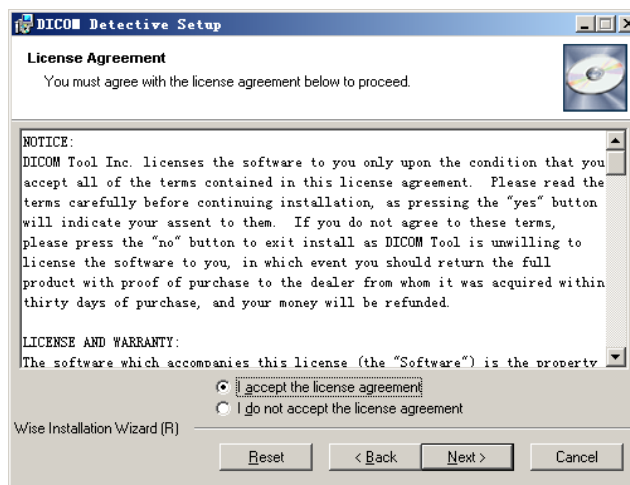

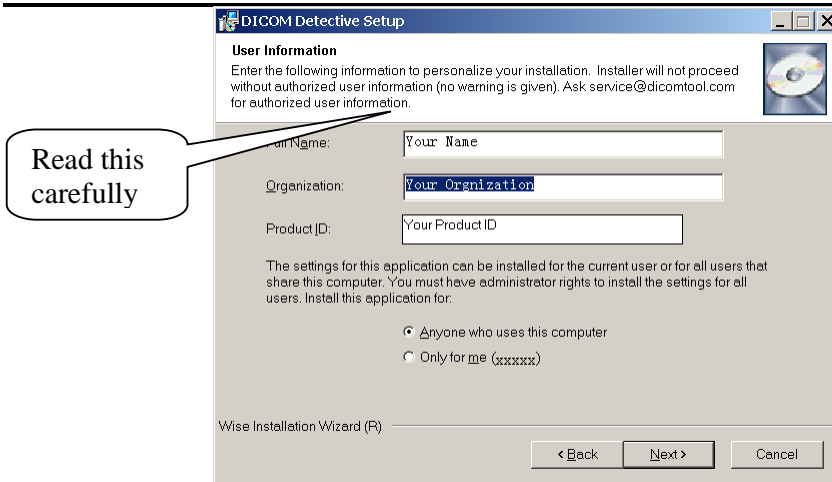**Figure 1 Installation Step 1**

Figure 2 Installation Step 2

Read this carefully

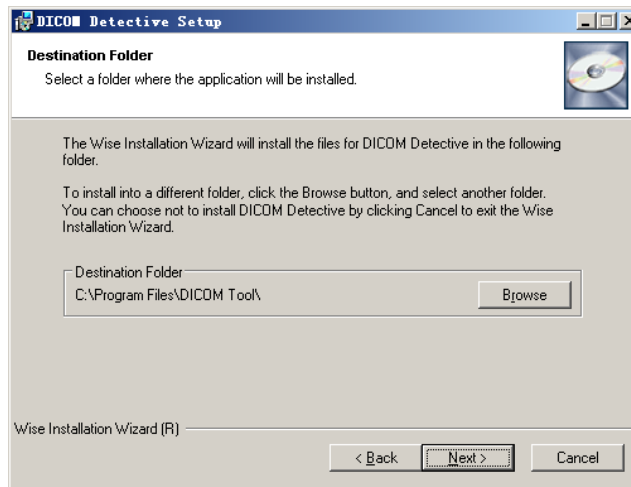**Figure 3 Installation Step 3**

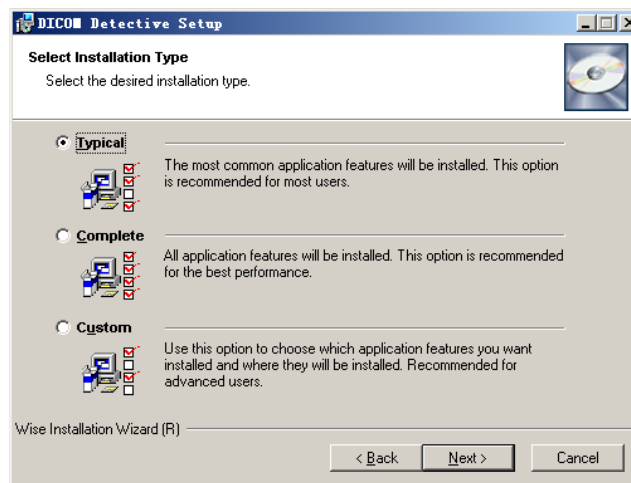**Figure 4 Installation Step 4**
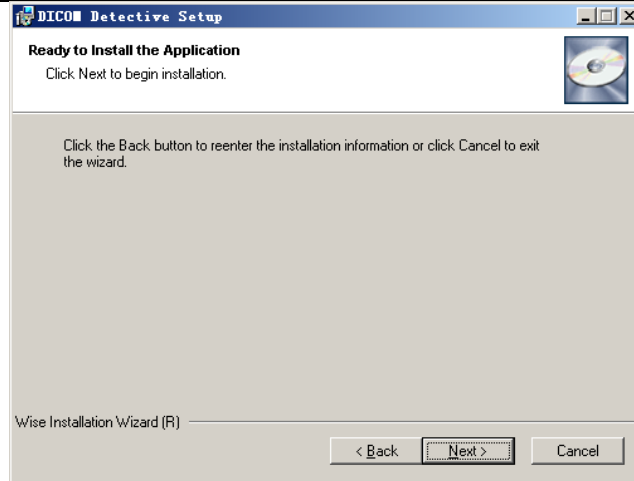
Figure 5 Installation Step 5

4

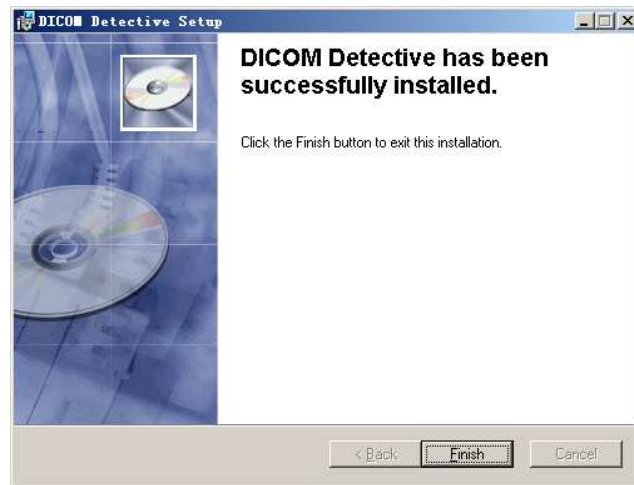**Figure 6 Installation Step 6**

Figure 7 Installation Step 7

4   DICOM DETECTIVE USER'S MANUAL

4.1   DICOM Detective Functionality Overview

The DICOM Detective works in conjunction with an off the shelf network analyzer to allow the ability to examine, simulate and debug the DICOM network communication.
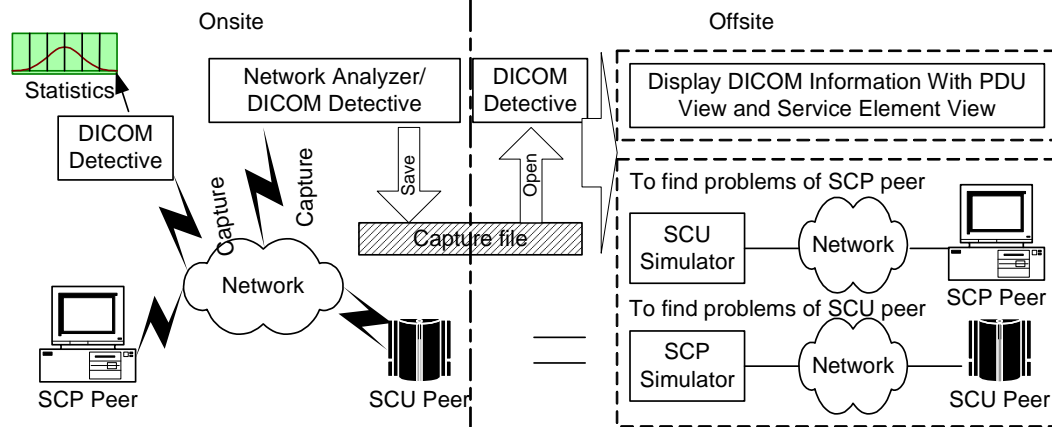
Figure 8 DICOM Detective Usage

Figure 8 shows the Usage of DICOM Detective. Usually, the service man gets the network capture data (or sometimes called network sniffer data) [1] onsite and send the capture data to programmers or consultants for analyzing offsite.

Following is three main functions of the DICOM Detective that the user can use to analyze the DICOM communication:

● The DICOM Detective takes network capture data (captured by a supported network analyzer) or a DICOM file as input. It parses the DICOM information from the inputted capture data or DICOM file and presents the information in a readable format through the DICOM Detective user interface. This DICOM information can then be used to find the problems in the DICOM communication.

● By using the capture data, the DICOM Detective can also simulate DICOM communication peers by simulating their input and output. It can reproduce the DICOM communication by interacting with one of the DICOM communication peer. This means, after getting the capture data and using the DICOM Detective simulator, DICOM communication problems can be reproduced without one of the DICOM communication peers. This is helpful for programmers to trace and debug their DICOM communication programs without traveling to locale.

● DICOM Detective calculates the DICOM traffic statistics and display the statistics report for a capture file or dynamically makes the statistics report while capturing. The statistics report can be used to evaluate the DICOM network performance.

DICOM Detective provides 5 views for a DICOM association.

4.1.1   PDU View
The PDU view gives a view of the PDUs used in the association. DICOM PDUs include A-ASSOCIATE-RQ, A-ASSOCIATE-AC, A-ASSOCIATE-RJ, P-DATA-TF, A-RELEASE-RQ, A-RELEASE-RP and A-ABORT. DICOM Detective shows the

---

[1] Network capture data (or sometimes called network sniffer data) will be abbreviated as capture data in the following context.

details of these PDUs for both requesting application and accepting application using a tree list in time sequence. Figure 9 is an example of PDU view.
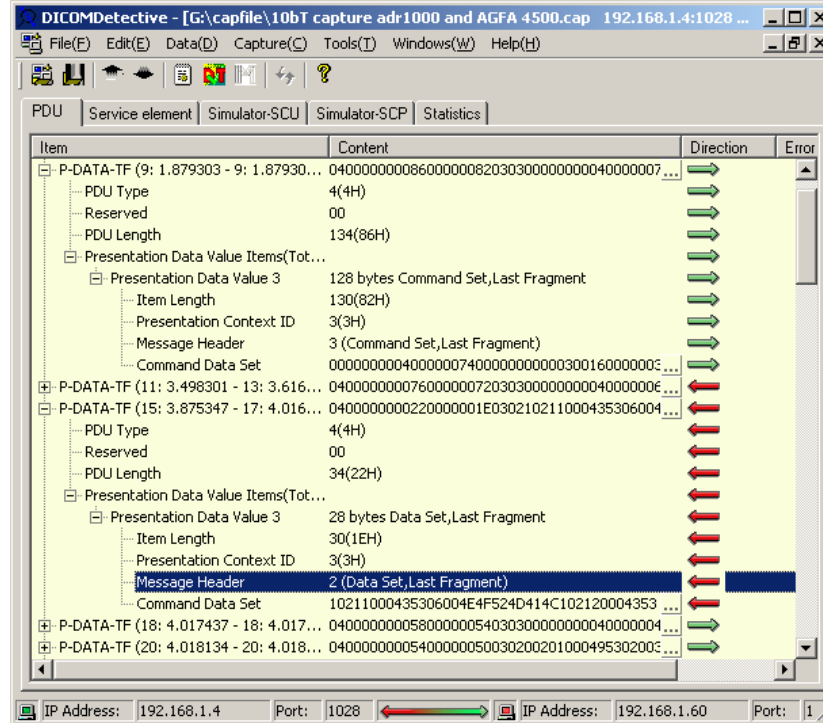

Figure 9 PDU View

4.1.2 Service Elements View

In the Service Elements view, the DICOM ACSEs (association control service elements) and DIMSEs (DICOM message service elements) are shown in a treelist for both the requesting application and accepting application in time sequence.

The ACSE message contains data controlling the communication. DICOM Detective shows the details of the ACSE by a tree list.

Every DIMSE message contains a Command Set (with Command Elements) and/or a Data Set (with Data Elements). DICOM Detective shows details of the DIMSE message (includes Command/Data Elements) by the tree list. Figure 10 is an example of service elements view.
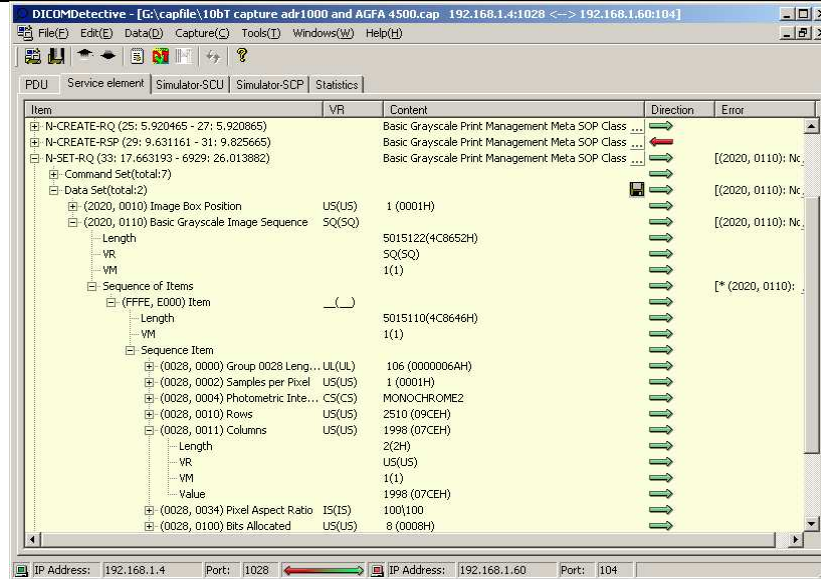
Figure 10 Service Elements View

4.1.3 SCP Simulator

The SCP Simulator view is used to simulate the SCP peer to reproduce the DICOM communication and helps to trace and debug SCU products. The DICOM Detective can start a daemon to listen to the specific port that entered by the user to simulate the SCP peer. Users can use their own SCU product to interact with the DICOM Detective SCP simulator as interacting with the real on-site SCP product. After the SCU peer initializes the communication, the DICOM Detective SCP simulator will receive all packets sent from SCU peer and send back capture packets that were originally sent by the simulating SCP product to SCU peer using DICOM communication protocol. The receiving and sending are done in original time sequence.

Using SCP Simulator, user can reproduce the problem that happened onsite and trace and debug the SCU program without the on-site SCP product. Figure 11 is an example of SCP Simulator view.
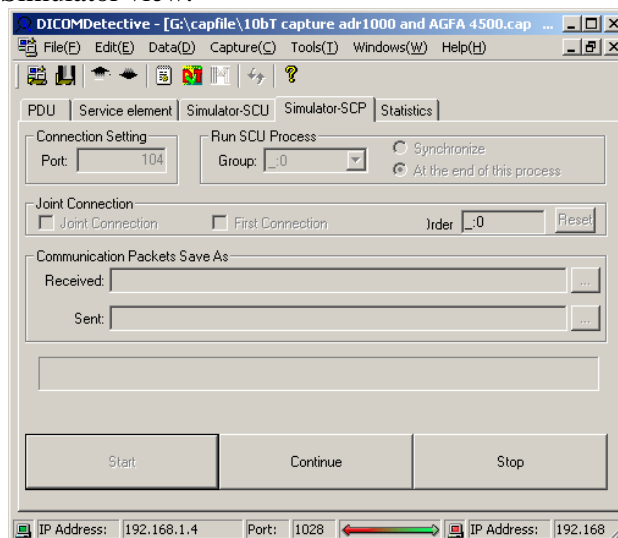

Figure 11 SCP Simulator

4.1.4   SCU simulator

The SCU Simulator view is used to simulate the SCU peer to reproduce the DICOM communication and helps to trace and debug SCP products. The DICOM Detective can start a DICOM connection to simulate the SCU peer. Users can use their own SCP product to interact with the DICOM Detective SCU simulator as interacting with the real on-site SCU product. The DICOM Detective SCU simulator can send all capture packets that were originally sent by the simulating SCU product to SCP peer using DICOM communication protocol and receive all data from SCP peer. The receiving and sending are done in original time sequence.

Using SCU Simulator, the user can reproduce the problem that happens online and trace and debug the SCP program without the on-site SCU product. Figure 12 is an example of SCU simulator view.
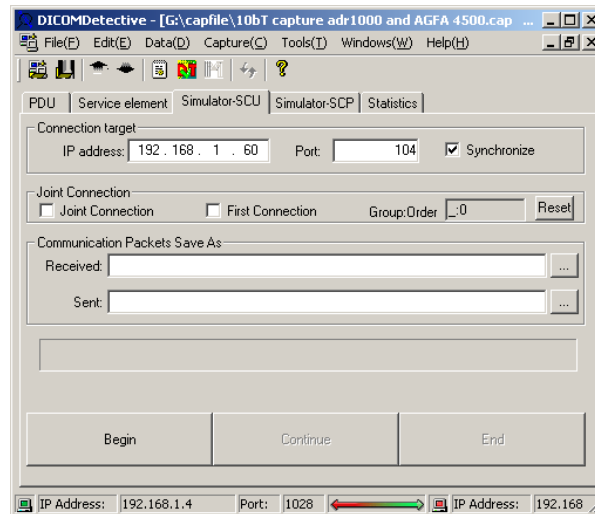

Figure 12 SCU simulator

4.1.5   Statistics View

The statistics view shows data transmission rate, patient transmission rate, study transmission rate, series transmission rate, image transmission rate and frame transmission rate etc. in table. Figure 13 is an example of Statistics View.
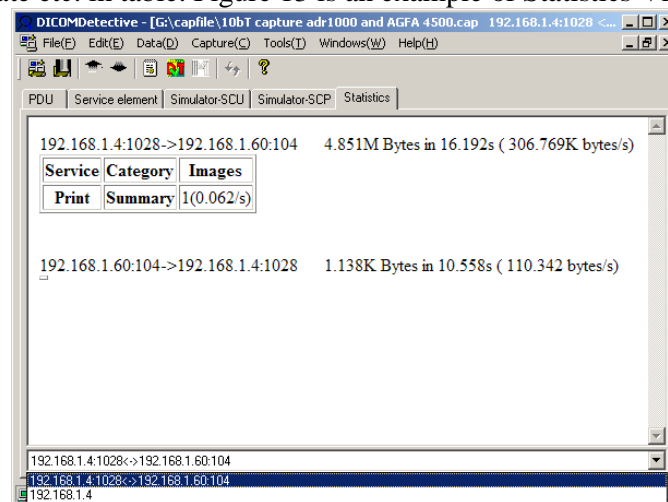

Figure 13 Statistics View

9

4.2 DICOM Detective User Interface

4.2.1 Menus and Toolbar

4.2.1.1 File->Open a Capture File

1. The "Open a Capture File" menu pops up an "Open file" dialog. User should select a capture file and hit open.
2. User also can drag a capture file in windows explorer and drop it to DICOM Detective.
3. Then a dialog will be popped up as Figure 14. User may enter start and end packet number. The packet number is 1 based regardless of type of network protocol analyzer. Usually, user needs not to set the start and end packet number, The DICOM Detective will do it for the user. It is for the case that user wants to avoid some bad packets of the capture data. (The hint for seeking a start packet of a DICOM communication using network protocol analyzer is to seek the Calling and Called AE Titles in the packets just by viewing the content of the binary packets. For the most cases, the first packet that contains the desired calling and called AE Titles is the start packet.)

   a. User can change file to be opened at the top edit box. Button would pops up an "Open file" dialog to help. Dragging a capture file in windows explorer and drop it into the edit box would also work.
   b. The option of ***Keep disordered and duplicated packets*** is default checked, when you get errors for opening a capture file, you may try to open the capture file without checking this option.
   c. If ***Open directly if only one connection*** is checked, DICOM Detective would skip the connection selection dialog in the next step. This option is remembered every time user changes it.
   d. If ***Skip error message*** is checked, DICOM Detective would not popup error message even there are errors while analyzing the DICOM data.
   e. User can choose following time format displayed in the views. (Note: Time format changing is not supported after the views are displayed.)
      i. Sec. since beginning of capture.
      ii. YYY-MM-DD HH:MM:SS.M.
      iii. Sec. since Epoch (1970-01-01).
         Changing time format in this wizard page would also affects default time format setting of WinPcap capture. It means if the time format is change to a certain one, next time the WinPcap capture would use the same selection as the default time format. Please also refer 4.2.1.12.1.
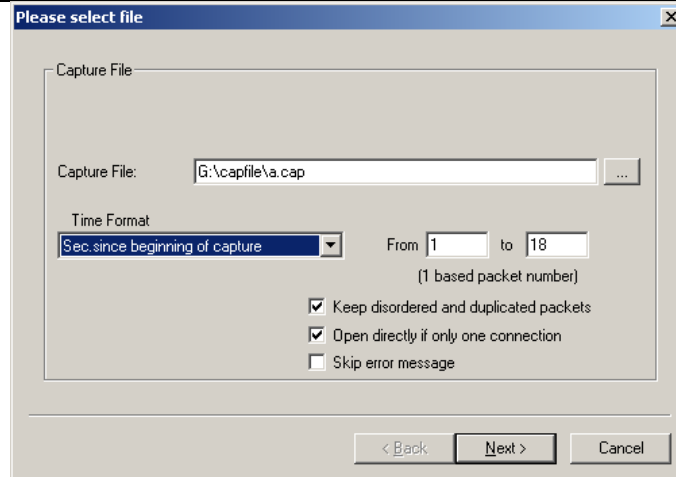
Figure 14 Dialog for Setting Start and End Packets

4. After user clicks next button, a dialog will be popped up as Figure 15. It displays the available connections. User should only select DICOM connections to be analyzed and click next. Non-DICOM connection may result in unexpected errors. This dialog might be skipped by checking *Open directly if only one connection* in the previous wizard page if there is only one connection to analyze.
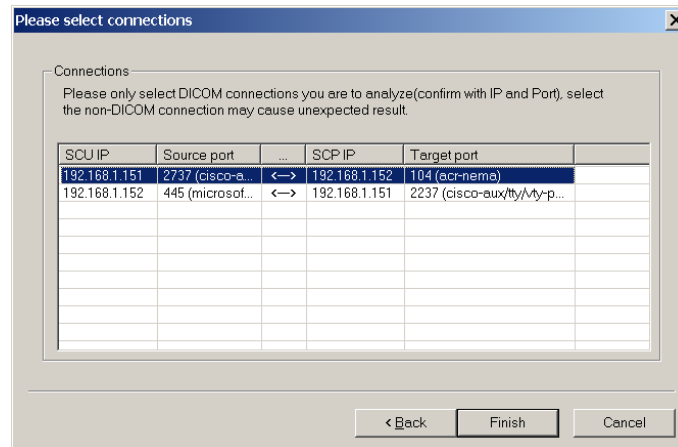
Figure 15 Dialog for Selecting Connection

5. After user clicks finish button, the DICOM Detective may popup error messages for bad connections (like Figure 16), and user can choose OK to continue or Cancel to stop analyzing the file. The error message dialog can be skipped by checking *Skip error message* in the first wizard page.

Figure 16 Error message dialog

6. After user clicks finish button for *Please select connections* dialog and/or OK button for error message dialog, A MDI window containing 5 views will be opened for each DICOM connection. Details of 5 views will be described in section 4.2.2
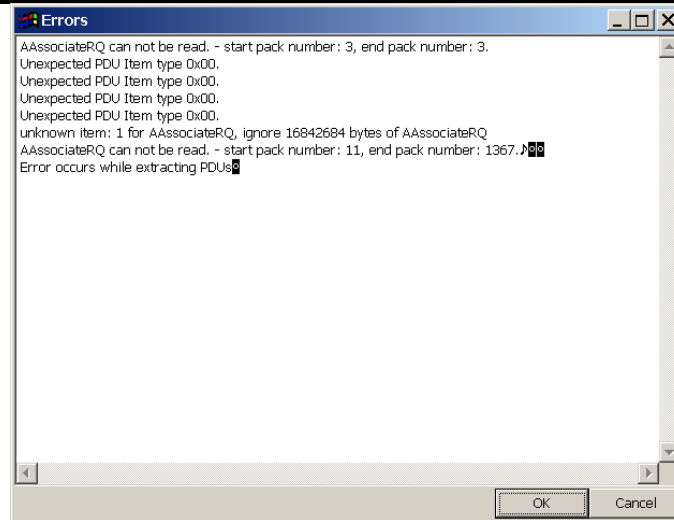
4.2.1.2   File->Open a Dicom File
After user selects "Open a Dicom File" menu, the DICOM Detective will popup an "Open file" dialog, User should select a DICOM file and hit open. Then, the DICOM Detective will open a MDI window to show all the DICOM elements inside the DICOM file using a tree list.

4.2.1.3   File->Save (Only active when a DICOM file is opened)
When a DICOM file is opened, this menu becomes active. When this menu is selected, the DICOM Detective would save user changes of the DICOM file in the current MDI window to the original file.

4.2.1.4   File->Save As…(Only active when a DICOM file is opened)
When a DICOM file is opened, this menu becomes active. When this menu is selected, the DICOM Detective would popup a "Save as file" dialog. User should select a directory and enter new file name and click save. The DICOM Detective would save user changes of the DICOM file in the current MDI window to the specified file. **This menu would not change the current file to the file saved as.**

4.2.1.5   File->Close
Close all the MDI windows for the current activated capture file or close an opened DICOM file.

4.2.1.6   Edit->Insert
When a DICOM or a capture file is opened, you can insert a DICOM element to the file. When this menu is selected (The menu is only active when an element is selected. The menu can also be popped up by right clicking the selected element.), the DICOM Detective would popup an "Insert DICOM Element" dialog as Figure 17.
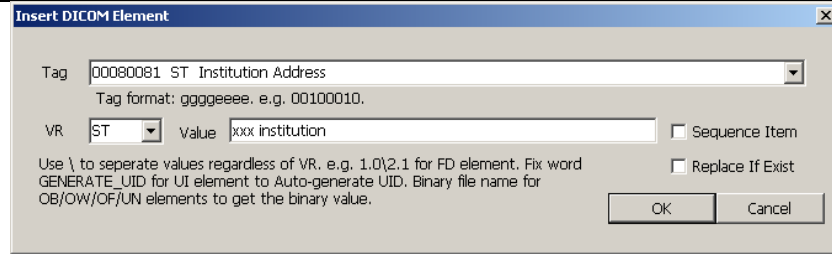
Figure 17 Insert DICOM Element

User should enter the element Tag, VR and value in the dialog to insert an element.

1. If user wants to insert a sequence item under the selected item, the "Sequence Item" should be checked.
   a. Inserting a sequence item to a non-SQ element is not allowed.
   b. User must insert FFFEE000 (Sequence Item) first to the SQ element, then insert sub elements to the FFFEE000 (Sequence Item). Trying to insert an element that is not FFFEE000 (Sequence Item) or FFFEE0DD (Sequence Delimitation Item) to a SQ element would raise an error dialog like Figure 18.
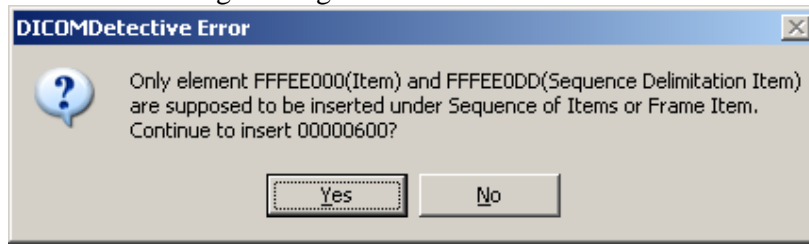
Figure 18 Error Dialog for inserting SQ item

   c. To insert sub elements to the FFFEE000 (Sequence Item), FFFEE000 (Sequence Item) should be selected and the "Sequence Item" should be checked. While inserting a sub element to the FFFEE000 (Sequence Item), a dialog may asks if the new element is in explicit VR, yes means explicit VR, no means implicit VR.

2. If the user wants to replace element already exist, the "Replace If Exist" should be checked. Otherwise if an element already exists, the element would not be inserted.
3. The Tag field is an auto-complete field. It means user can enter parts of the tag or tag name, system would list up tags that match what entered. E.g. user enters "sequence", and then all tag that relates to "sequence" would be listed up.
4. Following rules applies to the value field:
   a. Use backslash to separate multi-value regardless VR, e.g. 1.0\2.1 for FD (Float Double) type element.
   b. When the VR is UI and the value field is "GENERATE_UID", DICOM Detective would generate an UID to fill the value.
   c. When the VR is OB or OW or OF or UN and the value field is filled with an existing file name, the binary content of the file would be filled to the value. Otherwise, the string in the value field would be converted to binary to be filled into the value.

    d. If the value is hex number, add prefix 0x, e.g. 0x1ef3. (Only apply to
       UL,US,SS, SL elements)

    e. For AT element, do not add prefix 0x. E.g. 7fe00010\7fe00011

4.2.1.7　Edit->Delete

When a DICOM or a capture file is opened, you can delete DICOM elements. When this menu is selected (The menu is only active when an element is selected. The menu can also be popped up by right clicking the selected element.), the selected element would be deleted.

4.2.1.8　Edit->Reload

When a DICOM file is opened, user can reload the opened DICOM file from the disk by selecting this menu. Reloading the file would discard any change made to the file. A warning dialog would warn user that all changes would be lost before reloading.

4.2.1.9　Data->Export Data

This function is used for DICOM experts to compose their own communication data for simulation. DICOM experts can export the original communication data of the current connection into files in a directory. The exported data is pure DICOM communication data. It contains no redundant packet wrapping data made by network analyzer. DICOM experts can modify the binary files to compose new communication data. Then DICOM Detective can import the composed communication data and do simulation.

User can export the real captured communication data into files in a directory. A file may contain one or more capture packets. Files are named by following convention:

$$\textbf{pppppppppp\_xxx.xxx.xxx.xxx\_port}$$

where:
- pppppppppp is the 1000 times of packet number of the first packet in the file. The packet number is 1 based regardless of type of the network analyzer.
- xxx.xxx.xxx.xxx is the destination IP address of packets.
- port is the destination port of packets.

After user selects "Export Data" menu, the DICOM Detective will popup an "Open folder" dialog, user should enter a directory name and hit open. Then, the DICOM Detective will create a directory and export the communication data into files in the directory[2]. **Always export connections to different directories, importing 2 connections in one directory may result in wrong analysis.**

User can modify the exported binary files using any available tools.

"Export Data" only export original communication data. It will not export edited data. See 4.2.1.11.

---

[2] Export data is managed by files in a directory. Only packets related to the current activated connection is exported. Packets that are sent/received continuously will be combined into one file.

4.2.1.10 Data->Import Data

The modified exported data can be imported into the DICOM Detective as a capture file.

After user selects "Import Data" menu, the DICOM Detective will popup an "Open folder" dialog, user should select a directory and hit open[3]. Then, the DICOM Detective will import the communication data and open a MDI window containing 5 views. User can do analysis and simulation using the imported data as what he can do for a capture file.

4.2.1.11 Data->Export Edited Data

This menu is for saving information for an edited capture file. It will only become active when the capture file is changed. It acts same as "Data->Export Data" menu. The difference is "Data->Export Edited Data" menu exports changed data, but "Data->Export Data" exports original data even if the data is changed. The exported edited data can be imported using "Data->Import Data".

4.2.1.12 Capture->Capture Packets

DICOM Detective can capture packets onsite. This menu would bring up Capture Packets dialog. DICOM Detective supports following 2 ways to capture packets:

4.2.1.12.1 WinPcap Capture

The first way to capture packets is to use WinPcap, which is a famous free network data-capturing driver. User must download the WinPcap and install it for using this function. The official home page of WinPcap is http://www.winpcap.org.
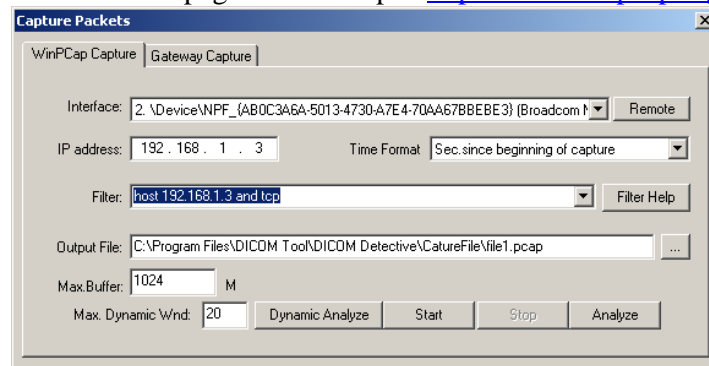
Figure 19 WinPcap Capture

Figure 19 is WinPcap Capture user interface.

1. User should select a network *Interface* (or network card) to capture the packets.
2. DICOM Detective supports remote capturing function of WinPcap (WinPcap remote daemon should be run in the remote computer). *Remote* button is used to get remote network interfaces. When the *Remote* button is clicked, a dialog like Figure 20 would be shown.
   a. The remote host IP address should be entered in **Host** field, and *Port* is for WinPcap remote capturing port, default value is 2002.

---

[3] You must make sure that all files in the directory are exported by DICOM Detective. Otherwise, it might cause problem.

    b.   If the remote capturing needs authentication, the ***Authentication*** should be checked and ***Username*** and ***Password*** should be entered.

    c.   When ***Get Interfaces*** is clicked, the ***Interfaces*** list box would list all available remote network interface.

    d.   If ***Automatically getting interfaces while starting up*** is checked, next time when DICOM Detective starts the WinPcap capture function or Dynamic statistics and Text dump function, it would automatically gets network interfaces from the remote host. Notice that it would take time if the remote host is not online.

    e.   ***OK*** button would close the dialog and bring all remote interfaces to WinPcap capture dialog. If a interface is selected in the ***Interfaces*** list box, it would be selected as default interface for WinPcap capture dialog.

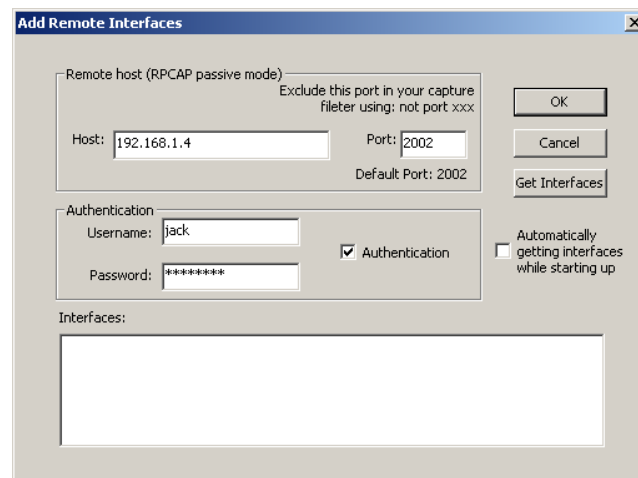   f.   ***Cancel*** button closes the dialog.

Figure 20 Remote Interface

3. ***IP address*** displays IP address of the current selected network interface.
4. ***Time format*** defines time format displayed in the views opened for captured data analysis. The selections are same as described in 4.2.1.1. They are:
   a. Sec. since beginning of capture.
   b. YYY-MM-DD HH:MM:SS.M.
   c. Sec. since Epoch (1970-01-01).
   Time format selection in this page affects the selection in the open file wizard dialog. It means if the time format selection in this page is changed to a certain one, next time the open file wizard dialog would choose same selection as default.
5. ***Filter*** is used to filter capture data, e.g. "host 192.168.1.2 and tcp" means only capturing TCP data that goes into/out of host 192.168.1.2. The filter follows rules of WinPcap filter. User can go to WinPcap's pages to get help, or the "Filter Help" button shows a help menu.
6. "***Filter Help***" button shows a help menu.
7. ***Output file*** defines the capture file to be saved. Button ⬚ brings up a Save As dialog to help to specify capture file.
8. ***Max. Buffer*** defines maximum buffer size used for DICOM data analysis.

9. ***Max. Dynamic Wnd*** defines maximum number of MDI windows opened for dynamic analysis.
10. ***Start*** would start the data capturing and save the data to the file.
11. ***Stop*** would stop the data capturing.
12. ***Analyze*** would open the capture file and display the contents of it.
13. ***Dynamic Analyze*** would start the data capturing. And same time, it would analyze the coming capture data dynamically. When a DICOM communication is fully completed, a MDI window would be opened, and the contents of the DICOM communication would be displayed in it. The maximum number of MDI windows is defined by ***Max. Dynamic Wnd***. When the maximum number is reached, the capture would be stopped automatically.

Typically WinPcap capture use cases are like this:
- Start->Stop->Analyze to open the capture file in MDI windows.
- Dynamic Analyze->Stop. (MDI windows are automatically opened.)

4.2.1.12.2 Gateway Capture
The second way to capture packets is to use Gateway Capture. Usually, the network analyzers and WinPcap cannot capture all the packets between 2 devices if the network analyzers or WinPcap are not installed in one of the device, because routers would not always broadcast all the communications. Gateway Capture is for solving this problem.

When it is not possible to install WinPcap to one of the communicating pair devices (SCU and SCP), and the DICOM communication between them should be captured, connects the PC that has DICOM Detective installed to the network. Then set the SCP IP and port to DICOM Detective Gateway Capture Deamon in the SCU device (From the view of SCU device, the DICOM Detective Gateway Capture Deamon is a SCP device to replace the original SCP); and set the SCP IP and port to the real SCP device in the DICOM Detective Gateway Capture Deamon (From the view of SCP device, the DICOM Detective Gateway Capture Deamon is a SCU device to replace the original SCU). Then when the SCU device sends data, the data would be sent to the DICOM Detective Gateway Capture Deamon first. The DICOM Detective Gateway Capture Deamon will make a copy of the data to local disk and then forward the data to SCP devices. Data from SCP is also transferred through this tunnel, it first is sent to the DICOM Detective Gateway Capture Deamon, the DICOM Detective Gateway Capture Deamon would make a copy of the data to local disk, and then the data is forward to SCU devices. The captured data would be stored as files in the format of "Data->Export Data". Figure 21 illustrates how Gateway Capture works.
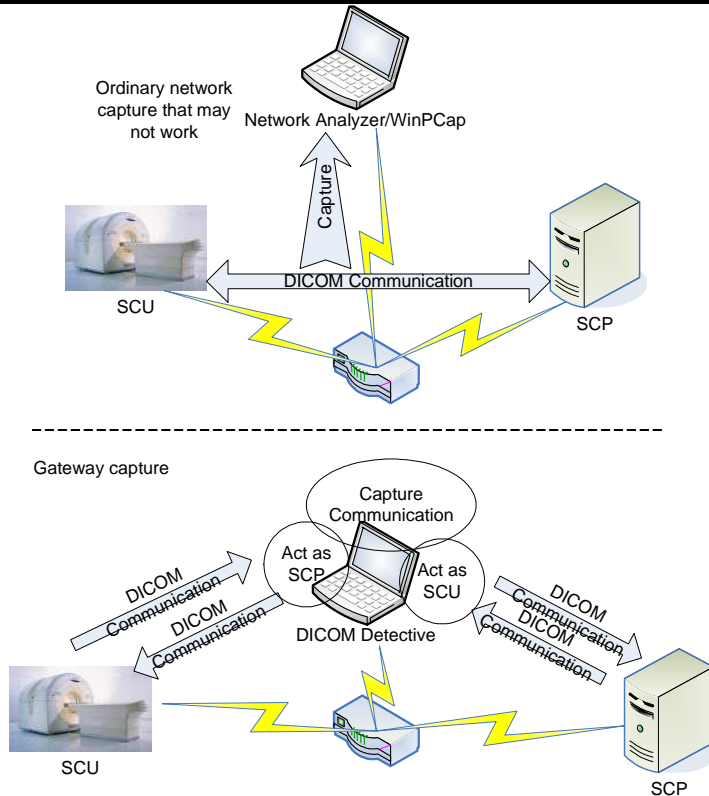
Figure 21 Gateway Capture illustration

Figure 22 is Gateway Capture user interface:

1. SCU→Gateway Capture Daemon block defines the DICOM Detective Gateway Capture Deamon listening port for listening SCU request.

   - *IP address* is for displaying the IP addresses of current available network interface, it is not editable, just for information.
   - *Port* defines listening port for listening SCU request.
   - *Timeout* defines timeout of connection with SCU

2. Gateway Capture Daemon block → SCP defines the SCP connection parameter.

   - *IP address* should be set to the IP address of SCP.
   - *Port* should be set to the listening port of SCP.
   - *Timeout* defines timeout of connection with SCP

3. *Output Folder* defines the folder that holds capture data, which is stored in the format of "Data->Export Data". User can import the data using "Data->Import Data".

4. *Start* would start the Gateway Capture Daemon to listen to request from SCU. The Gateway Capture Daemon will stop until the *Stop* is pressed or **one DICOM communication is finished**. The captured data would be stored as files in the format of "Data->Export Data".

5. *Stop* would stop the Gateway Capture Daemon.

6. *Analyze* would open the capture data in a MDI window.
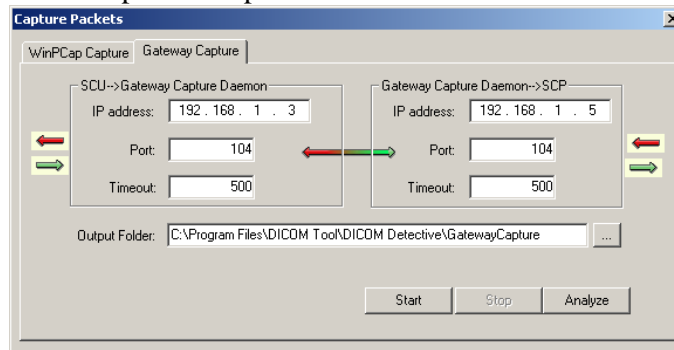
Figure 22 Gateway Capture UI

4.2.1.13   Capture->Dynamic Statistics and Text Dump

DICOM Detective supports dynamic DICOM traffic rates and network interface status statistics and dynamic dumping communication contents to text files that can serve as DICOM communication log.

4.2.1.13.1 Dynamic Statistics

Dynamic Statistics function uses WinPcap to capture DICOM network communications and dynamically extracts the DICOM statistical information to save and display. Which statistical information should be calculated is configurable, e.g. you can gather statistical traffic information for bytes/sec in/out of an IP and/or port, and you also can gather statistical traffic information for images/sec in/out of an IP and/or port. Figure 23 shows Dynamic Statistics user interface.
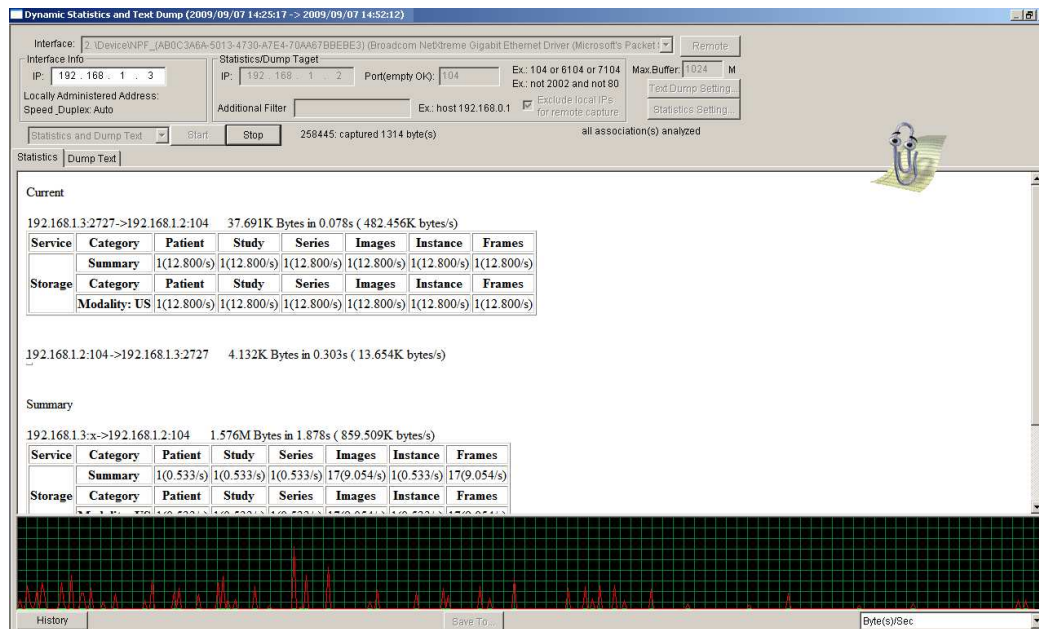
Figure 23 Dynamic Statistics

1. Statistical traffic information report is categorized into 2 sections:
   - *Current* section displays the current DICOM statistical traffic information.

- *Summary* section displays the summary DICOM statistical traffic information of certain time span. This time span can be configured by user, e.g. 5 minutes.

2. The history gram on the bottom shows the traffic rates dynamically. The dropdown combo box on the right bottom corner is for selecting which parameter to show.
3. *Save To* button brings up a save as dialog for user to specify a file in order to save the current displaying report to a html file.
4. *History* button brings up a statistics history dialog like Figure 24.
   - Left drop down combo box is used to select history file.
   - Right drop down combo box is used to select parameter to show.

Figure 24 Statistics History

4.2.1.13.2 Text Dump

Text Dump function uses WinPcap to capture DICOM network communications and extracts the DICOM communication information and translates the communication information into text files, so that the text files can serve as DICOM communication log. Figure 25 shows Text Dump user interface.

Figure 25 Text Dump

1. *Clear* button clears the current displaying log.
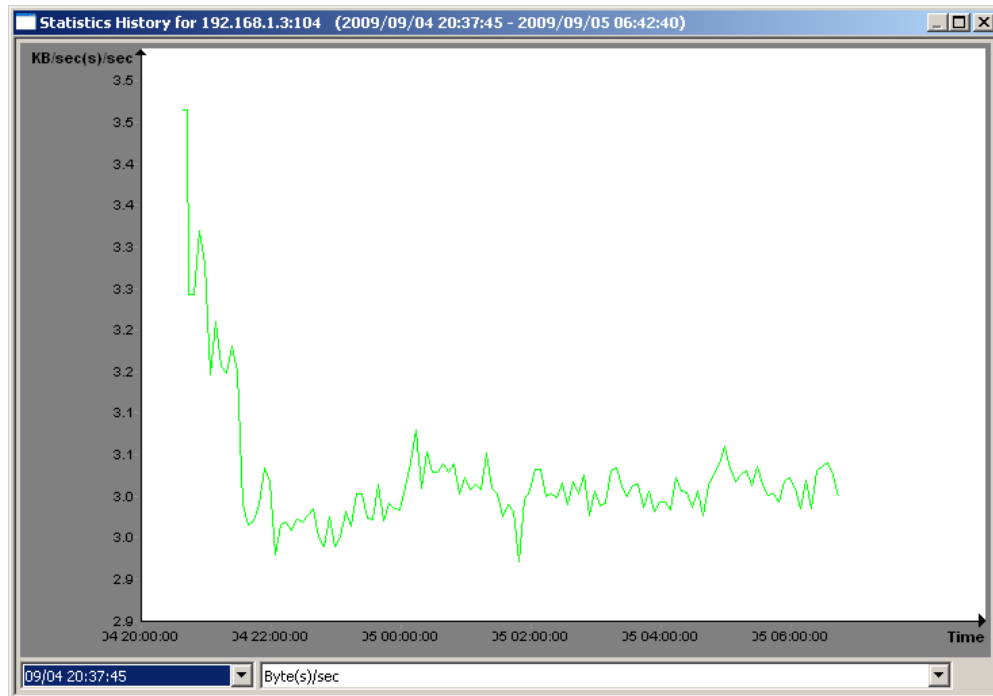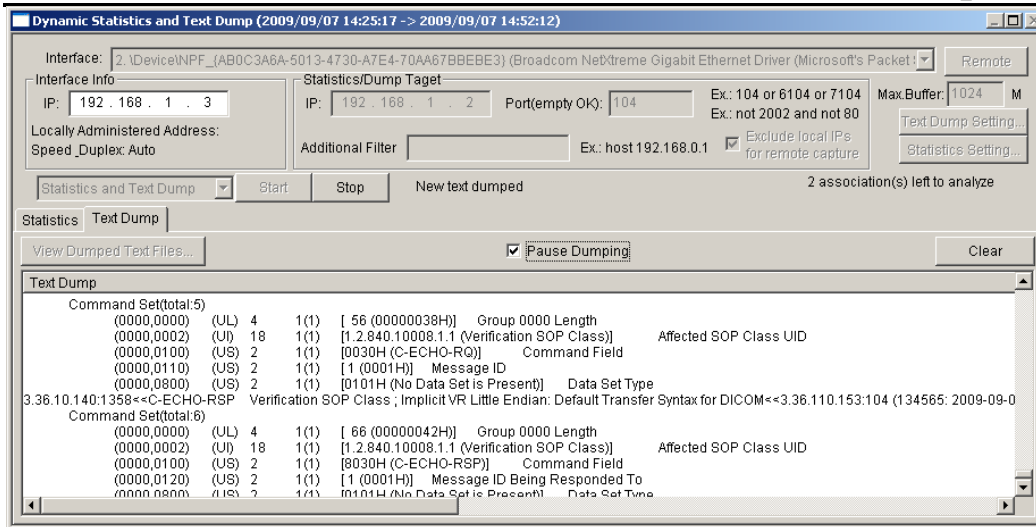2. Checking *Pause Dumping* check box would pause the log display, un-checking it would continue the log display.
3. *View Dumped Text Files* would bring up an open file dialog, you can select a log file and open it with notepad.

To do Dynamic Statistics or Text Dump:
1. User should select a network *Interface* (or network card) to capture the packets.
2. DICOM Detective can gather statistical traffic information from remote interface using WinPcap. *Remote* button is used to get remote network interfaces, please refer 4.2.1.12.1 for how to get remote network interfaces.
3. *Interface Info-IP* displays the IP of the current selected network interface. The area below the IP displays the current network interface information, e.g. configuration information like speed (duplex 100M, 10M etc.). It would display all the information of the current network interface in a tool tip box if the mouse is moved over this area.
4. *Stactistics/Dumping Taget-IP* is to define which IP you want to gather statistical traffic information from / dump text from.
5. *Stactistics/Dumping Taget-Port* is to define which port you want to gather statistical traffic information from/dump text from. This field can be empty, and then it means all ports would be involved for statistical traffic information gathering/text dumping. The *Port* field can be entered with "not", "and" and "or" key words. E.g. "104 or 6104 or 7104" means gathering statistical traffic information/dumping text for ports: 104, 6104 and 7104; "not 2002 and not 80" means gathering statistical traffic information/dumping text for all ports except 2002 and 80.
6. *Stactistics/Dumping Taget-Additional Filter* is to define additional capture filter, the filter follows the WinPcap filter rules and the filter would be jointed to the internal filter with keyword "and". E.g. host 192.168.0.1 means gathering statistical traffic information /dumping text from host 192.168.0.1.
7. WinPcap would generate packets between remote host and local host for remote capturing. When capturing DICOM communication between remote

hosts, checking *Stactistics/Dumping Taget-Exclude local IPs for remote capture* would avoid capturing those packets WinPcap generated.

8. *Max. Buffer* defines maximum buffer size used for DICOM data analysis.
9. You can choose to do "*Statistics*", "*Text Dump*" or "*Statistics and Text Dump*" by selecting a selection from the drop-down combo box under *Interface Info*.
10. *Start* would start the traffic Statistics and/or Text Dump.
11. *End* would end the traffic Statistics and/or Text Dump.
12. An information bar besides stop button shows capturing and analysis information.
13. *Text Dump Setting* brings up Text Dump Setting dialog like Figure 26.
    - *Dump to folder* defines the log files location.
    - *Max files* defines max number of log files.
    - *Max file size* defines max file size of each log file.
    - *Max lines in log window* defines the max lines of log window.

Figure 26 Text Dump Setting

14. *Statistics Setting* brings up Statistics Setting dialog like Figure 27.

Figure 27 Statistics Setting

- User must define which service DICOM Detective should calculate the traffic statistics for. To define the service, user must enter the service name, then hit *Add Service* button.

- User must specify the command tags and values of the service, e.g. when command field(0000,0100) is 0x8020 and Affected Sop Class UID(0000,0002) is 1.2.840.10008.5.1.4.1.2.2.1 or 1.2.840.10008.5.1.4.1.2.1.1, the service is DICOM instance query. Properties is used to specify the service. User may *Add/Update/Delete* command tags and values to the service, multi-value should be separated with back slash.
- User must specify which parameter should be calculated for traffic statistics and how that parameter is calculated. Currently, DICOM Detective supports following calculations for traffic statistics.

  - *Count* would count total occurrence of the specified tag. (Not includes tag in sequence elements)
  - *UniqCount* would count total occurrence of the specified tag without duplication.
  - *DeepCount* would count total occurrence of the specified tag. (Includes tag in sequence elements)
  - *AccumulateFrame* would summary the value of the specified tag (usually (0028, 0008) Number of Frames), and if the tag is absent but Pixel Data (7FE0, 0010) is present, the value of the specified tag is deemed as 1. This is used to calculate frame rates of DICOM transmission.

  User should provide following information to specify a statistics item.

  - Tag: DICOM element tag to be calculated.
  - Label: Label to be displayed in the statistics report.
  - Statistics Action: which calculation should be taken.
  - Max Rate(/s): Maximum transmission rate. It is used for upper border of historical gram.

- User also can specify category for a service to categorize different transmissions in a service. E.g. to categorize storage service with modality so that the statistics report would display the transmission rates for different modality. To define the category, user must select a service first and enter the category name, then hit *Add Category* button to add the category to the service.
- User must specify the tags to define the category, e.g. Modality (0008,0060) can makes the statistics report categorized with Modality. User may *Add/Update/Delete* tags and labels to the category, label is used for category display in the report.
- User should define *Dynamic Statistics sum every* time span. The time span is used for *Summary* section of the statistics report.
- *Statistics History folder* holds statistics history files generated by dynamic statistics function. User may define the folder.
- *Max TCP/IP Rate (Bytes/sec)* defines maximum TCP/IP transmission rates. It is used for upper border of historical gram.
- *Refresh Statistics Screen every* time span defines the time span to refresh the dynamic statistics report screen. Zero means refresh the

report immediately. –1 means never display the statistics report, just collects the statistics history file.
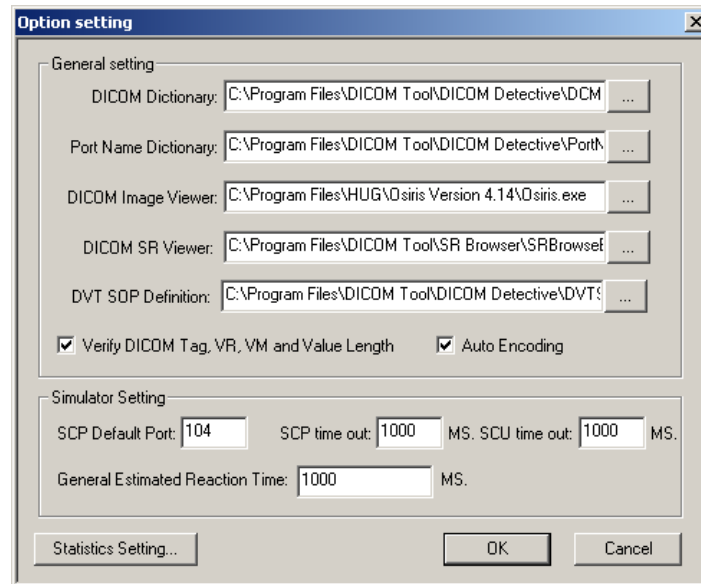
Figure 28 Option Dialog

4.2.1.14   Tools->Option
User can change DICOM Detective settings by clicking "Option" menu. Figure 28 shows the option settings.

● **DICOM Dictionary:** The path of the DICOM dictionary file. The system default DICOM dictionary file is DCMDict.txt.

● **Port Name Dictionary:** The path of port name dictionary file. The system default port name dictionary file is PortName.txt.

● **DICOM Image Viewer:** The path of DICOM image viewer executable file. It can be any DICOM image viewer that can take DICOM image file path as the first parameter to open the DICOM image file. The DICOM image viewer will be lunched to open the image while user clicks the ![icon] button in the service element view.

● **DICOM SR Viewer:** The path of DICOM Structure Report viewer executable file. It can be any DICOM Structure Report viewer that can take DICOM SR file path as the first parameter to open the DICOM SR file. The DICOM SR viewer will be lunched to open the structure report while user clicks the ![icon] button in the service element view.

● **DVT SOP Definition:** The file path of DICOM SOP class to DVT definition map. It is used for generating DVT scripts. The system default file is DVTSOP.txt.

- **Verify DICOM Tag, VR, VM and Value Length:** Check this if you want DICOM Detective to verify whether all the DICOM Tag, VR, VM and Value Length are following the DICOM standard. Uncheck this to save analysis time. The default is checked.

- **Auto Encoding:** Check this if you what DICOM Detective to translate the special characters in the file to you local characters according to the Special Character Set (0008, 0005).

- **SCP Default Port:** It is the default listening port of the SCP simulator daemon.

- **SCP Timeout:** It is timeout for connection while performing SCP simulation.

- **SCU Timeout:** It is timeout for connection while performing SCU simulation.

- **General Estimated Reaction Time:** It is an assumed time span between the communication actions of the opposite peer. (DICOM Detective assumes that, after the DICOM Detective simulator sends a DICOM message to the opposite peer, it will take the assumed time for the opposite peer to response.)

- **Statistics Setting…:** It bring up the statistics setting dialog. Please refer to 4.2.1.13.

4.2.1.15 Tools->Report

After user selects "Report" menu, the DICOM Detective will popup a "Save as" dialog, user should enter a file name and hit save. Then, the DICOM Detective will generate a report for the current active view and save it to the file. A sample report file is present in Appendixes.

4.2.1.16 Tools->Export DVT Script

After user selects "Export DVT Script" menu, the DICOM Detective will popup a "Select Folder" dialog, user should enter a folder name and hit open (if it is a no existing folder, please answer yes to create the folder). Then, the DICOM Detective will generate DVT Scripts to the folder for the current active view. To use the generated scripts, user have to create a DVT project file and a DVT session file and include all generated scripts to the session file.

4.2.1.17 Tools->Export MergeDPM User Info

After user selects "Export MergeDPM User Info" menu, the DICOM Detective will popup a "Save as" dialog, user should enter a file name and hit save. Then, the DICOM Detective will generate a MergeDPM compatible User Info for the current active view and save it to the file.

4.2.1.18 Tools->Encoding

The encoding function is for the DICOM communication that uses special character sets. It only applicable to elements with type of SH (Short String), LO (Long String), ST (Short Text), LT (Long Text), PN (Person Name) or UT (Unlimited Text).

- Reset

By default, the system will not use any encoding mechanism. It just uses windows default encoding mechanism. Use "Reset" to select windows default encoding.

● Unicode (UTF-8)
This function is used to display Unicode (UTF-8) special characters.

● ASCII
This function forces the DICOM Detective to display special character sets by DICOM specified ASCII way.

● Japanese (JIS)
This function is used to display Japanese (JIS) special characters.

● Japanese (Shift-JIS)
This function is used to display Japanese (Shift-JIS) special characters.

● Chinese Simplified (GB2312)
This function is used to display Chinese Simplified (GB2312) special characters.

● Chinese Simplified (GB18030)
This function is used to display Chinese Simplified (GB18030) special characters.

● Korean (iso-ir-149)
This function is used to display Korean (iso-ir-149) special characters.

● Western Europe (ISO) (iso-ir-100)
This function is used to display Western Europe (ISO) (iso-ir-100) special characters.

4.2.1.19   Tools->Find and Find Next
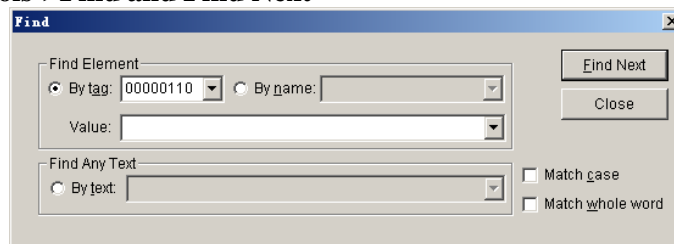
Figure 29 Find Dialog

User can find DICOM data element in the Service Element view and DICOM File view by entering the element tag/name and value as search criteria in the Find dialog showed in Figure 29. User can also find any text displayed in the Service Element view and DICOM File view. Besides using menu, find dialog can also be started by the accelerate key Ctrl+F, and user can continue the search by the accelerate key F3.

4.2.1.20   Tools->Find DICOM Files
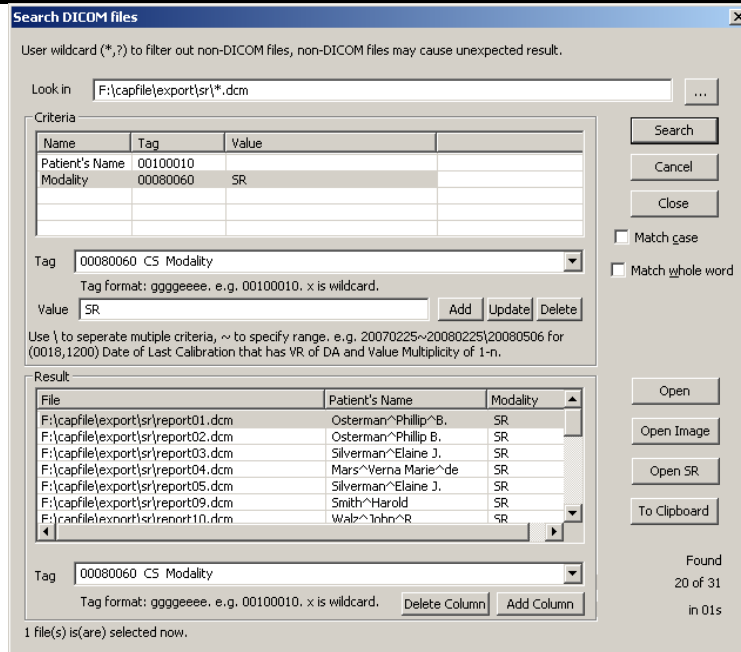
Figure 30 Search DICOM Files Dialog

User can find DICOM files under a directory and its sub-directory. Figure 30 is the Search DICOM files dialog.

- Enter the directory or file specification with wildcard (*, ?) to be searched in the "Look in". The ▭ button helps to locate the directory. Try to use wildcard (*, ?) to filter out no DICOM files.
- User may add/update/delete search criteria by providing DICOM tag and value. The criteria are in the relationship of the "AND".
- No value element criteria would test if the DICOM file contains the element.
- Use backslash to separate multiple criteria value. E.g. For Image Type (0008,0008), criteria "ORIGINAL\PRIMARY" means to search DICOM files that contains element Image Type (0008,0008) that has values include string ORIGINAL and string PRIMARY.
- The multiple criteria for an element are in the relationship of the "AND".
- Use "~" to specify range matching. "x~" means >=x; "~x" means <=x, "x~y" means between x and y. Range matching applies to DS, DT, FL, FD, IS, SL, SS, TM, UL and US. Use range matching for FL and FD to avoid mismatch. Below table shows matching support for different VR.

VR	Value Matching	Range Matching
AE	String Matching, backslash for multiple criteria.	Not support
AS	String Matching, backslash for multiple criteria.	Not support
AT	Format is ggggeeee, e.g. 00100010, backslash for multiple criteria.	Not support
CS	String Matching, backslash for multiple criteria.	Not support
DA	String Matching, backslash for multiple criteria.	e.g 2007~20080930 means from 2007/01/01 to 2008/09/30. ~200805 means less then 2008/05/01.

DS	String Matching, backslash for multiple criteria.	e.g. –1~1 means between –1 and 1. ~1.2e2 means less then or equal to 1.2e2.
DT	String Matching, backslash for multiple criteria.	e.g 2007~20080930112230 means from 2007/01/01 to 2008/09/30 11:22:30. ~200805 means less then 2008/05/01 00::00::00.
FL	Float value matching, backslash for multiple criteria.	e.g. 1.3415926~1.3415972, 1.34~, ~-1.02e8…
FD	Double float value matching, backslash for multiple criteria.	e.g. 1.3415926~1.3415972, 1.34~, ~-1.02e8…
IS	String Matching, backslash for multiple criteria.	e.g. 1~20, -3~, 20~
LO	String Matching, backslash for multiple criteria.	Not support
LT	String Matching, backslash is deemed as part of the criteria.	Not support
OB	Not support (No value means to test if the element exists)	Not support
OF	Not support (No value means to test if the element exists)	Not support
OW	Not support (No value means to test if the element exists)	Not support
PN	String Matching, backslash for multiple criteria.	Not support
SH	String Matching, backslash for multiple criteria.	Not support
SL	Signed long value matching, backslash for multiple criteria.	e.g. -1~10, 2~, ~-15…
SQ	Not support	Not support
SS	Signed short value matching, backslash for multiple criteria.	e.g. -1~10, 2~, ~-15…
ST	String Matching, backslash is deemed as part of the criteria.	Not support
TM	String Matching, backslash for multiple criteria.	e.g 112233~154456 means from 11:22:33 to 15:44:56. ~1540 means less then 15:40:00.
UI	String Matching, backslash for multiple criteria.	Not support
UL	Unsigned long value matching, backslash for multiple criteria.	e.g. 1~10, 2~, ~15…
UN	Not support	Not support
US	Unsigned short value matching, backslash for multiple criteria.	e.g. 1~10, 2~, ~15…
UT	String Matching, backslash is deemed as part of the criteria.	Not support

- The "Search" button executes the search action. User can cancel the search by "Cancel" button.

- Result list displays the files searched. User can add column to the list by providing the DICOM tag that user wants to display.
- The "Open" button opens files selected in the result list using DICOM file view.
- The "Open Image" button opens files selected in the result list using DICOM image viewer.
- The "Open SR" button opens files selected in the result list using DICOM SR viewer.
- The "To Clipboard" button copies the selected items in the result list to the clipboard.
- User can add columns to the result list. It will display the first element that has same tag with the column.
- Type tag or name in the "Tag" dropdown box would list all elements matched to the word typed.
- X and x are deemed as wildcards for tag. x can be used for criteria, e.g. 60xx0010.

4.2.2   Detail of 5 views
4.2.2.1   PDU View
Figure 31 is a sample of PDU view. PDU view lists PDU details with a tree list.

Notes:
- IP and port of communication peers are showed in the status bar.
- The arrows in the "Direction" column present the data direction. E.g., for Figure 31, Right (Green) arrow indicates that the data was sent from 192.168.0.150:32882 to 192.168.0.230:1024.
- Error column displays analysis errors, DICOM verify warnings and errors.
- For user's convenience, the number is displayed in both decimal and hex format.
- For long hex data, user can click the ⋯ button to open a hex view to display the full hex data. User can also save the hex data to a file. Figure 32 is a sample of the hex data view.
- For long text data, user can click the ⋯ button to open a text view to display the full text data. Figure 33 is a sample of text data view.
- The binary content of PDU is displayed in the content column, click the ⋯ button to open a hex view to display the full binary data.
- Packet number and time is displayed for every PDU in the following format:

 xx: ssssss.ssssss – yy: tttttt.tttttt

 Where[4]:
- **xx** is start packet number of the PDU;
- **ssssss.ssssss** is start time of the PDU;
- **yy** is end packet number of the PDU;
- **tttttt.tttttt** is end time of the PDU.

---

[4] DICOM Detective defines the first packet number as 1 and the first packet time as 0.
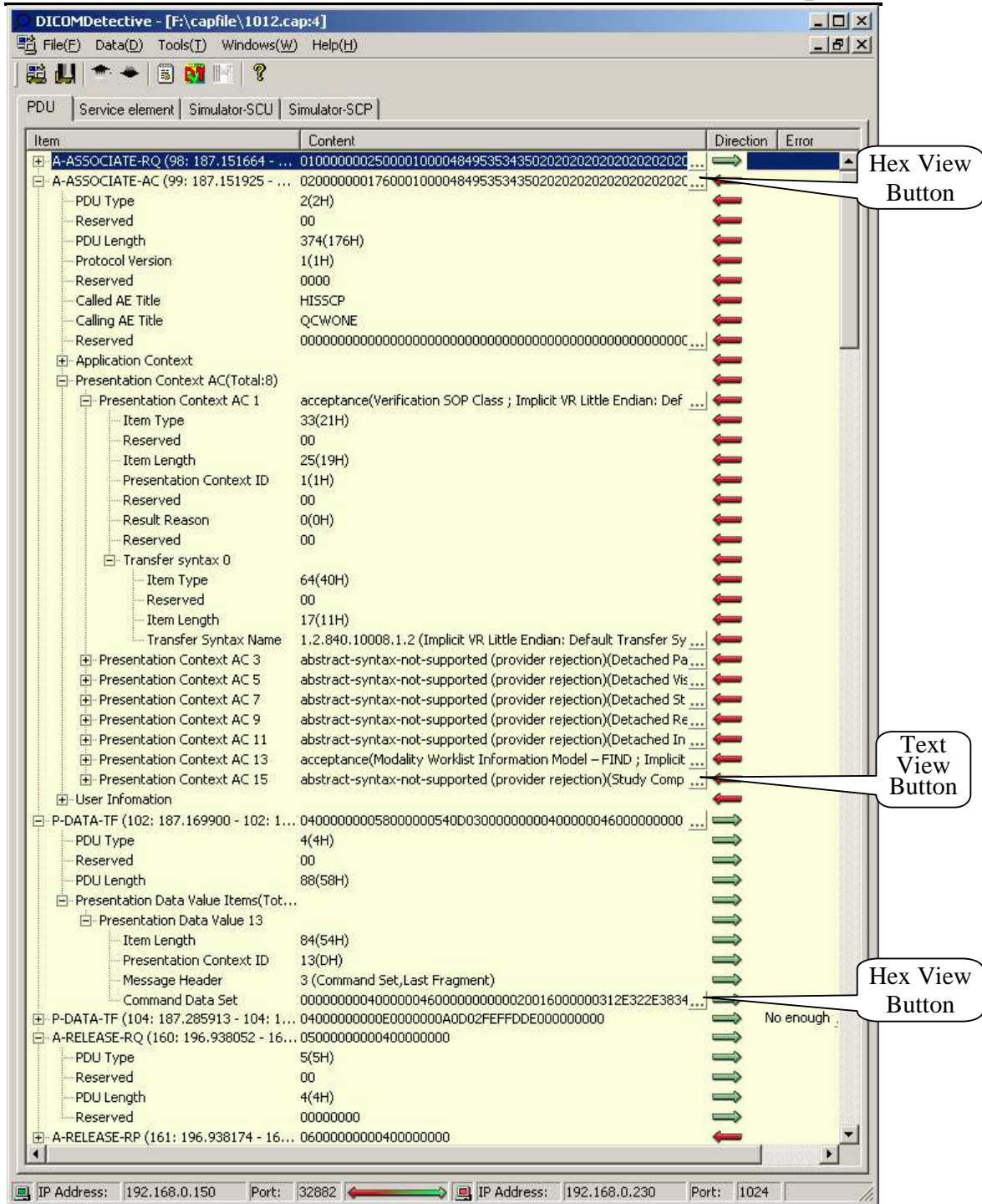
Figure 31 Sample of PDU View
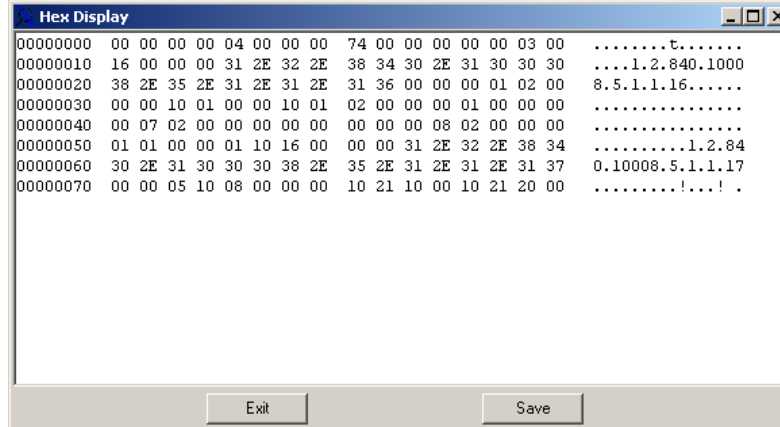
Figure 32 Hex Data View
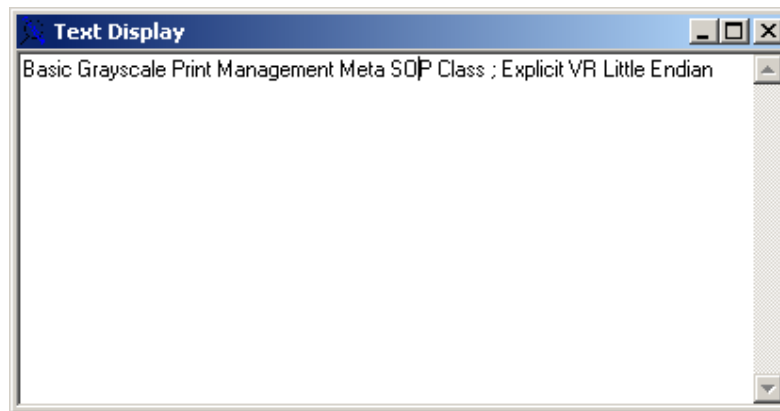
Figure 33 Text Data View

4.2.2.2 Service Element View
Figure 35, Figure 36 and Figure 37 are samples of service element view.

Notes:
- Error column displays analysis errors, DICOM verify warnings and errors.
- Packet number and time is displayed for every service element, format is same as what in PDU view.
- Values are displayed in the content column just beside the DICOM tag.
- In different cases of DICOM communication (e.g. explicit/implicit VR transfer syntax), a data element may have a VR or not. In DICOM Detective, The VR is displayed only when the data element has a VR. The VR is displayed in following format:

  XX(YY)

  Where XX is from the capture data; YY is DICOM defined VR, it is from the dictionary.

- VM is displayed in the following format:

  M(N)

Where M is the real number of values; N is DICOM defined VM, it is from the dictionary.

- When an element has undefined length (0xFFFFFFFF), it will be displayed with the actual length as Figure 34 demonstrated.

Figure 34 Undefined length display

Figure 35 Sample 1 of Service Element View
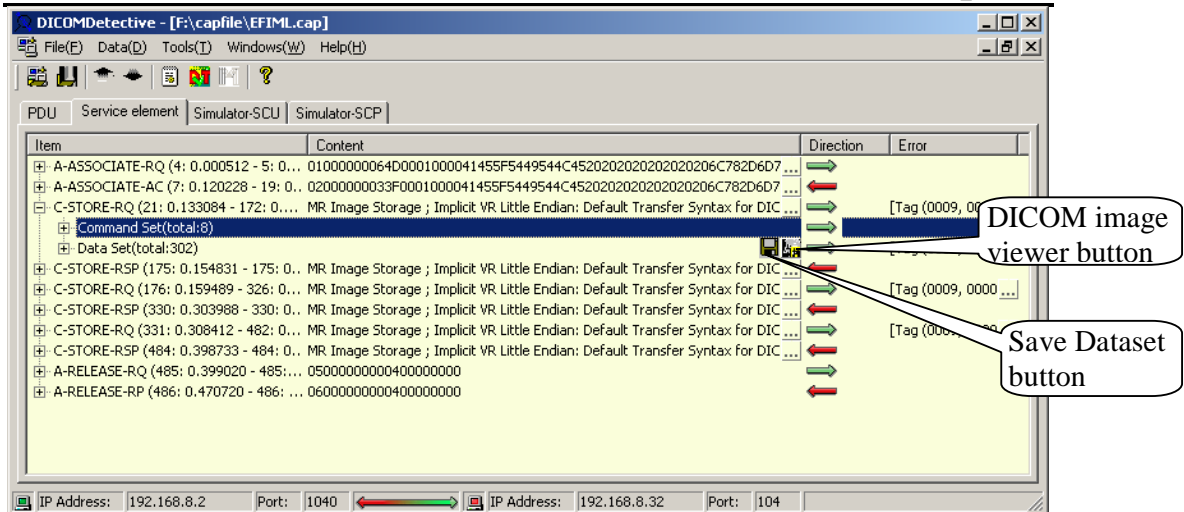
Figure 36 Sample 2 of Service Element View

- When a data set contains a pixel data element (7FE0, 0010), a ▦ button will be attached to the data set and the pixel data element. User can click the button to start the DICOM image viewer to view the image contained in the data set. This is special convenient for user to see what images are sent for DICOM storage and DICOM print.
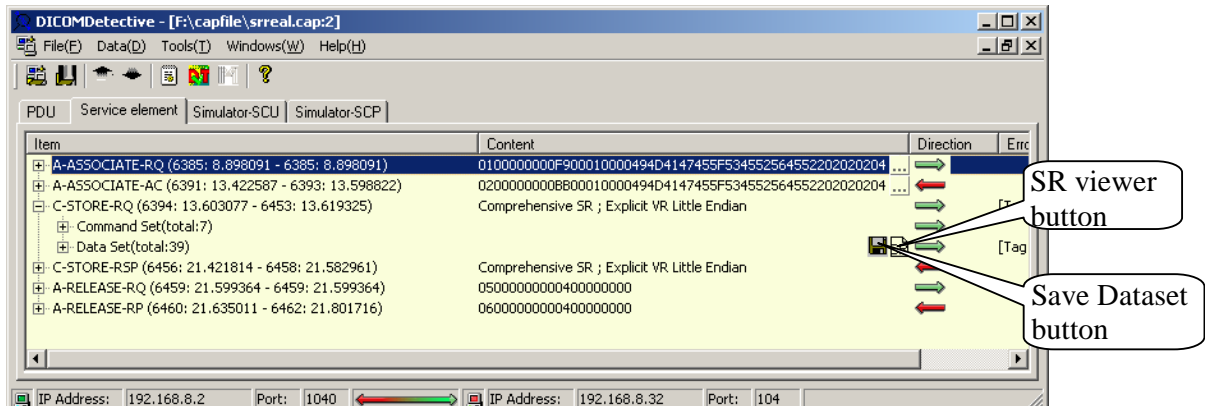
Figure 37 Data set contains SR

- When a data set contains a structure report (like Figure 37), a ▦ button will be attached to the data set. User can click the button to start the DICOM structure report viewer to view the structure report contained in the data set. User can set the SR viewer in the option dialog. Figure 38 shows the SR viewer that comes with the DICOM Detective.
- User can save a dataset to a file by clicking 💾 button.
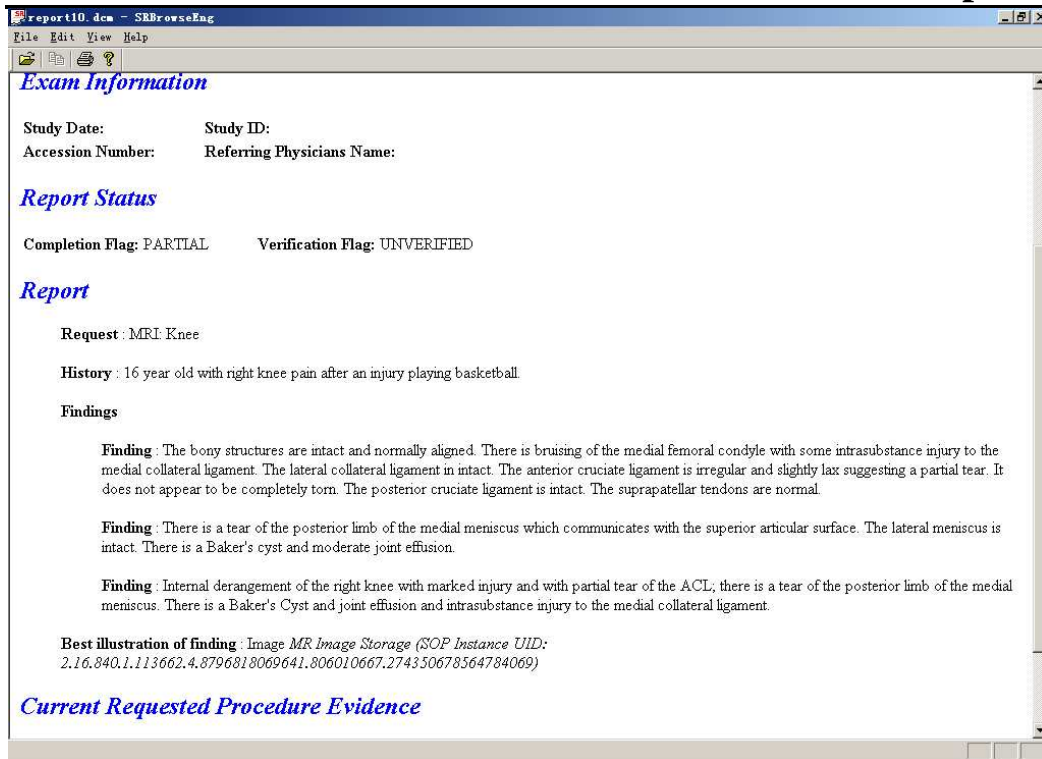
Figure 38 Sample of SR Viewer

4.2.2.2.1 Editing Element

User can insert and delete elements in the Service Element View. Please refer 4.2.1.6 and 4.2.1.7. The insert and delete menu can also be popped up by right click the selected element.

User can also edit existing element by double clicking the cell in the content column and the element row or double clicking the cell in the content column and value row. See Figure 39.

Figure 39 Editing element

When double clicking the cell, an edit box with the value is provided for editing. After entering the value, clicking outside the edit box would finish the editing. Following rules applies to the value field:

- Use backslash to separate multi-value regardless VR, e.g. 1.0\2.1 for FD (Float Double) type element.
- When the VR is UI and the value field is "GENERATE_UID", DICOM Detective would generate an UID to fill the value.
- When the VR is OB or OW or OF or UN and the value field is filled with an existing file name, the binary content of the file would be filled to the value. Otherwise, the string in the value field would be converted to binary to be filled into the value.

- If the value is hex number, add prefix 0x, e.g. 0x1ef3. (Only apply to UL, US, SS and SL elements)
- For AT element, do not add prefix 0x. E.g. 7fe00010\7fe00011.
- DICOM Detective provides value explanation with parentheses. When editing the value, the characters in the parentheses and the parentheses should be removed.

The menu Edit->Export Edited Data can export edited data.

4.2.2.3 Simulator-SCU View

Figure 40 is a sample of simulator-SCU view.
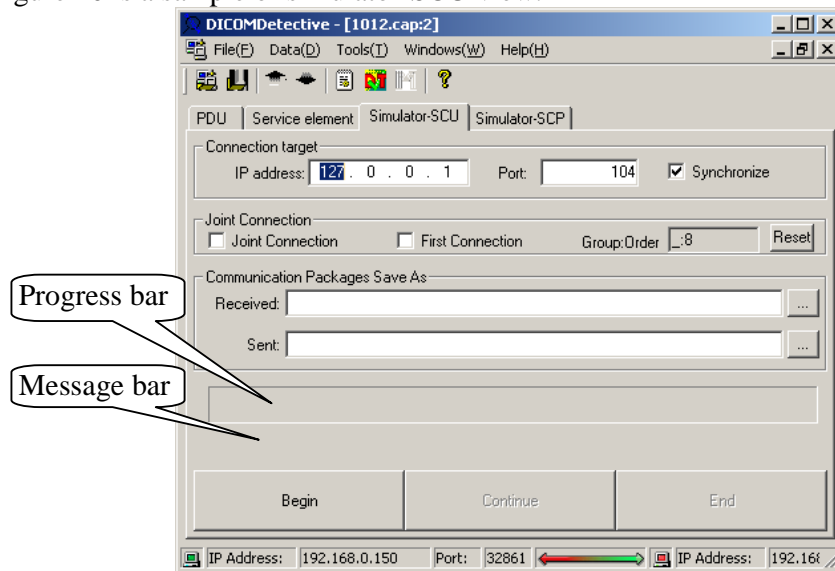
Figure 40 Sample of Simulator-SCU View

User should enter the **IP address** and **Port** of the destination SCP that is about to be tested. IP address and port may not be same with what is displayed in the status bar, but the IP address must be the IP address of the destination SCP and the port must be what the destination SCP is listening to.

Synchronize is use to synchronize the **IP address** and **Port**, all connections with **Synchronize** checked in a connection group will have the same **IP address** and **Port.** The connection group will be introduced afterward.

If user enters the file path for **Communication Packets Save As** (**Received or/and Sent**), the received and/or sent packets during the simulation will be saved to the corresponding files (binary file). Often time, user can leave this field empty. It is for users who want to know details of the network communication for the simulation.

User should click **Begin** button to start simulation. If the simulation starts, the **progress bar** will indicate the simulation progress and **message bar** under the progress bar will show simulation messages. If the simulator pauses while simulation, it is waiting for data from the other communication peer, user can click **Continue**

button to skip receiving the data and accelerate the simulation. **End** button is used to stop the simulation.

About connection group:
Simulation can be done by a single connection or a group of connections. User can use controls in **Joint Connection** group box to joint deferent connections (displayed in deferent MDI windows) into one group. Then the simulator will do simulation sequentially for the grouped connections in the order of connection jointing. The function of grouping connections is used to simulate DICOM communications of which that the time sequence is sensitive. E.g., to store images, some DICOM implementation sends C-ECHO ahead of C-STORE to verify the network, and C-ECHO and C-STORE are usually done in 2 different connections. To simulate this, user needs to joint these two connections into one group, and then DICOM Detective will do simulations continuously for user. (Do the C-ECHO first, then C-STORE)

Following is the way to joint connections into groups and disjoint connections:
- User should check the **First Connection** check box to create a new connection group and make the connection the first connection in the group.
- User should check the **Joint Connection** check box to joint the connection into the last created connection group.
- The group number and the connection order is displayed in the format of "**group:order**", where group is 0 base integer to distinguish different groups and order is also 0 based integer to indicate the simulation order. The **group:order** will be displayed in format of "_:order" for standalone connection, where the underscore indicates that the connection has not been grouped and the **order** just gives identification to the connection.
- User can uncheck the **Joint Connection** check box to kick a connection and the followed connections out of the group.
- User can uncheck the **First Connection** check box or hit **Reset** button to delete the group.
- User can click **Begin** button of any connection in a group to start simulations in the group.
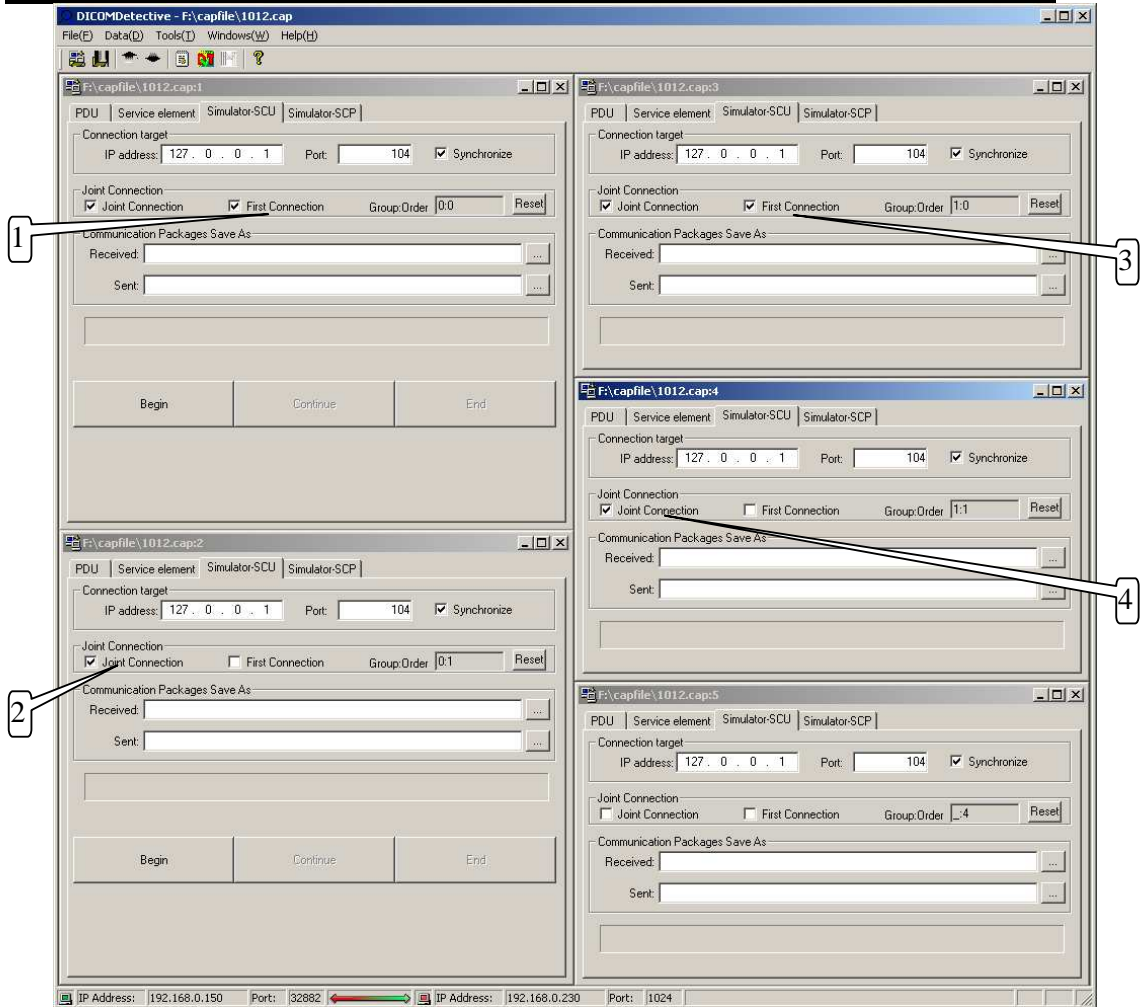
Figure 41 Example of Jointing Connection

Figure 41 is an example of how jointing connections works.

- First, user checked the **First Connection** check box in connection "1012.cap:1" to make the connection group 0 and make the "1012.cap:1" as the first connection (Order 0) in group 0;
- Second, user checked the **Joint Connection** check box in connection "1012.cap:2" to joint the connection into connection group 0. The connection "1012.cap:2" became the second connection (Order 1) in connection group 0.
- Third, user checked the **First Connection** check box in connection "1012.cap:3" to make a new connection group (group 1) and make the connection "1012.cap:3" as the first connection (Order 0) in group 1;
- Forth, user checked the **Joint Connection** check box in connection "1012.cap:4" to joint the connection into connection group 1. The connection "1012.cap:4" became the second connection (Order 1) in connection group 1.
- "1012.cap:5" is a standalone connection that is not grouped, so the group is displayed as underscore.
- Then 2 groups of connections were made. For group 0, if user clicks "**Begin**" button of "1012.cap:1" or "1012.cap:2", simulator will start simulation for "1012.cap:1" first and then "1012.cap:2". It is similar for group 1.

- "1012.cap:5" is a standalone connection, user can click "**Begin**" button to start this simulation.

4.2.2.4 Simulator-SCP View
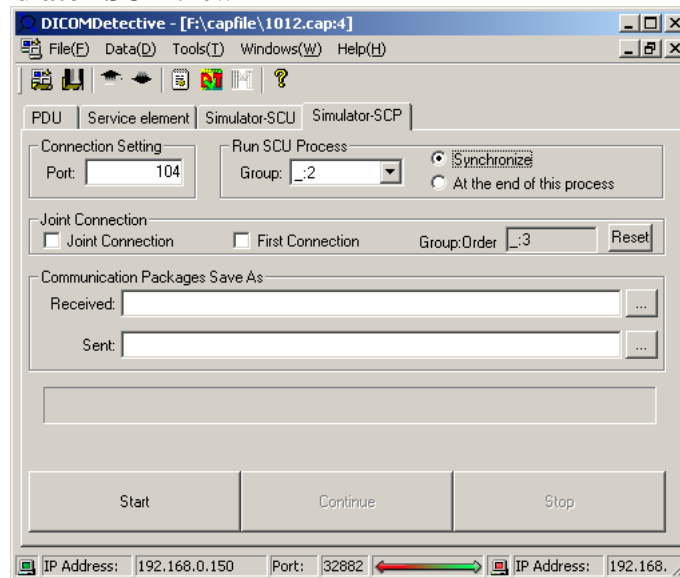
Figure 42 Sample of Simulator-SCP View

Figure 42 is a sample of simulator-SCP view.

User should enter a **Port** for the SCP simulator to listen to (The port is synchronized for all connections in a group).

If user enters the file path for **Communication Packets Save As** (**Received or/and Sent**), the received and/or sent packets during simulation will be saved to the corresponding files (binary file). Often time, user can leave this field empty. It is for users who want to know details of the network communication for the simulation.

User should click **Start** button to start simulation. If the simulation starts, the **progress bar** will indicate the simulation progress and **message bar** under the progress bar will show simulation messages. If the simulator pauses while simulation, it is waiting for data from the other communication peer, user can click **Continue** button to skip receiving the data and accelerate the simulation. **Stop** button is used to stop the simulation.

SCP simulator can start the SCU simulator during the SCP simulation to simulate one connection or a group of connections by using **Run SCU Process** function to synchronize the SCP simulations and SCU simulations. E.g., for DICOM image server implementations, after receiving a C-MOVE request in a connection, a series of C-STORE should be sent in another connection. In this case, the DICOM image server implementation will play the SCP role for C-MOVE and SCU role for C-STORE. **Run SCU Process** function is used to simulate this kind of implementations.
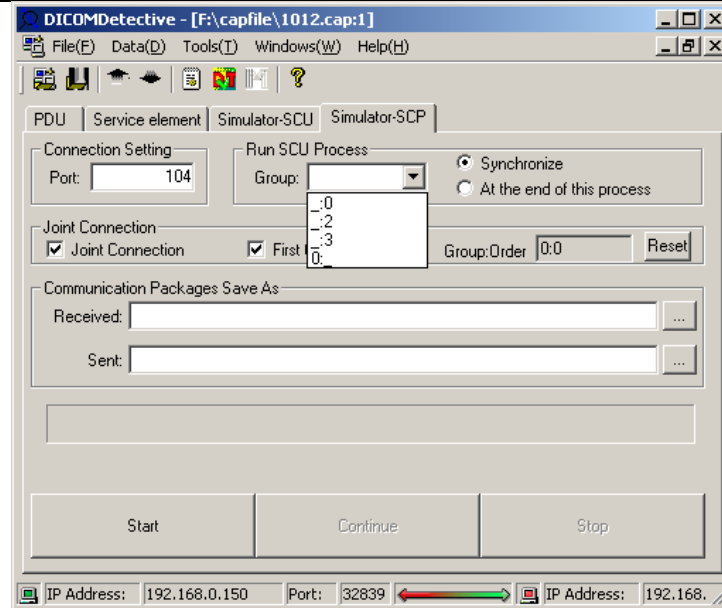
Figure 43 Run SCU Process

Figure 43 shows choices for **Run SCU Process** function. User can choose a connection or a group of connections using the "**Group**" combo box. The listed connection groups or standalone connections are made in the Simulator-SCU view, they are not from the Simulator-SCP view. Group is displayed in the format of "group:_". The choice of "**synchronize**" will synchronize the simulation of the selected SCU connection(s) with the simulation of the current SCP connection (E.g. to simulate DICOM retrieve service, this choice should be used). The choice of "**At the end of this process**" will make the SCP simulator start to simulate SCU connection(s) at the end of this SCP simulation (E.g., to simulate DICOM storage commitment, this choice can be used).

About connection group:
- SCP simulator can also do simulation for a group of connections. The way to joint connections is same as the way described in section 4.2.2.3.
- All connections in a group can only have a same port for the SCP simulator to listen to.
- The SCP simulator will do simulations for each connection in the group in the sequence of connection jointing.
- User can combine SCP group simulation function with the **Run SCU Process** function to make complicated simulations.

Notice: During the simulation, do not close any window of DICOM Detective.

4.2.2.5   Statistics View

Figure 44 shows statistics view. It displays the DICOM traffic statistics information report for a capture file. The combo box at the bottom is for selecting target to calculate the statistics. The configuration of DICOM traffic statistics information

report is done by using Tool->Option menu and Statistics Setting button. Please refer 4.2.1.13.
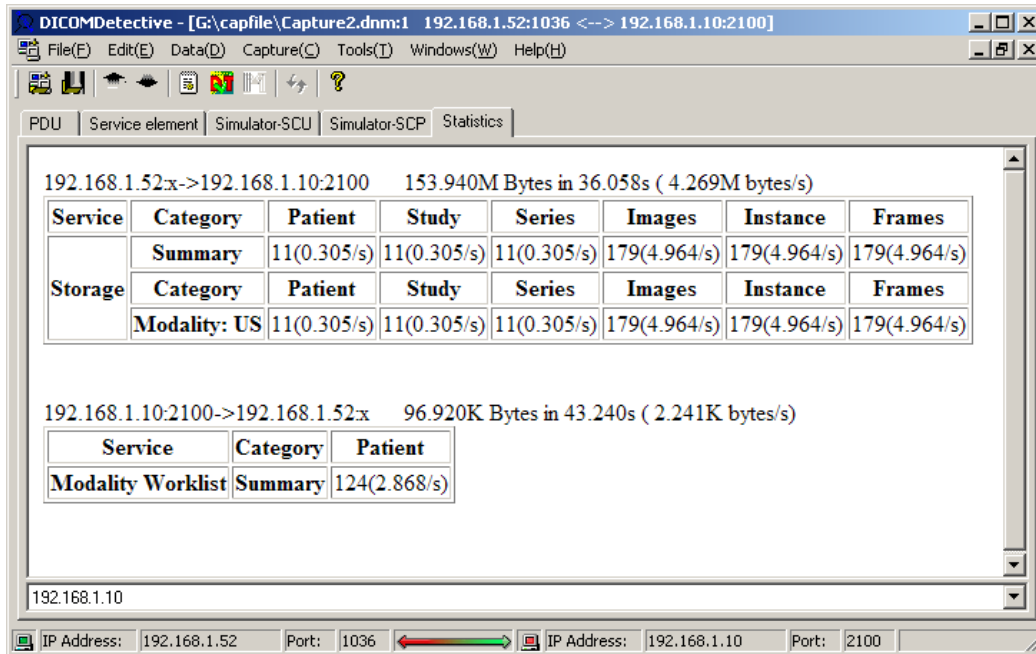
Figure 44 Statistics View

4.2.3   Command Line

DICOM Detective supports command line to export text report, merge DPM user info and DVT script. The usage is:

DICOMDetective.exe –i inputpath –o outputpath [–et –ed –em –s –v]

-I inputpath   Input path. Could be a file name or a folder name. If it is a folder name, all files inside the folder would be processed.

-o outputpath   Output path.
- For text report dumping:
  - If the input path is a file name, the output path could be an output file name or a path that the output file would be generated in.
  - If the input path is a folder name, the output path must be a path that the output files would be generated in.
- For merge DPM user info:
  - If the input path is a file name, the output path could be an output file name or a path that the output file would be generated in.
  - If the input path is a folder name, the output path must be a path that the output files would be generated in.
- For DVT script:
  - If the input path is a file name, the output path must be **a path** that the output files would be generated

in.

- o If the input path is a folder name, the output path must be a path that the output files would be generated in.

-et	Export text dump. (At least one of –et, -ed, -em should be specified)
-ed	Export DVT script. (At least one of –et, -ed, -em should be specified)
-em	Export merge DPM user info. (At least one of –et, -ed, -em should be specified)
-s	Silent mode. No popup dialog.
-v	Verbose mode.

Appendix A: Examples of Simulator Function Usages

Case 1. Simulator SCU
Suppose that your DICOM archive server could not function well with a third part
DICOM conforming CT in a customer's site 1000 kilometers away. You could not
travel to the customer's site in short time to solve the problem. Then a service man
there captured the DICOM communication by Sniffer Pro 4.5 and sent you the
network capture file. You opened the capture file with the DICOM Detective and
checked the DICOM communication detail between your DICOM archive server and
the third part CT. You found that the communication is like below.

The third part CT >> A- ASSOCIATE -RQ >> Your DICOM archive server
The third part CT << A-ASSOCIATE-AC << Your DICOM archive server
The third part CT >> C-STORE-RQ >> Your DICOM archive server
The third part CT << A-ABORT << Your DICOM archive server

You checked every communication detail using PDU view and Service Element View
and found that neither the third part CT nor your archive server violated the DICOM
standard. But you do not know why you archive server sent back an "A-ABORT"
instead of a "C-STORE-RSP" after receiving a C-STORE-RQ. Then you need to
debug your archive server software with the DICOM Detective.

To debug you archive server:
1. You should setup the network environment.
2. Choose the correct version of your archive server and use same settings with
   what is used onsite[5].
3. You should set break points and start you archive server with the debug mode,
   then your archive server can listen to a certain port.
4. Open the capture file came from the service man with the DICOM Detective.
5. Select the correct connection and switch to the Simulator-SCU view.
6. Enter the IP address and port of your archive server
7. Presses "**begin**" to start simulation.

Then the DICOM Detective simulator SCU begins to interact with your archive
server (The progress bare indicates the progress and messages are displayed in the
message bar). You archive server will stop at the break point and you can trace and
debug you source codes.

Case 2. Simulator SCP
Suppose that your DICOM conforming CT could not function well with a third part
DICOM archive server in a customer's site 1000 kilometers away. You could not
travel to the customer's site in short time to solve the problem. Then a service man
there captured the DICOM communication by Sniffer Pro 4.5 and sent you the
network capture file. You opened the capture file with the DICOM Detective and
checked the DICOM communication detail between the third part DICOM archive
server and your CT. You found that the communication is like below.

---

[5] The importance to make the simulator works is that you must use the same version software (also
same settings) to interact with the DICOM Detective.

Your CT >> A- ASSOCIATE -RQ >> The third part DICOM archive server
Your CT << A-ASSOCIATE-AC << The third part DICOM archive server
Your CT >> A-ABORT >> The third part DICOM archive server

You checked every communication detail using PDU view and Service Element View and found that neither your CT nor the third part archive server violated the DICOM standard. But you do not know why you CT sent an "A-ABORT" instead of a "C-STORE-RQ" after receiving an A-ASSOCIATE-AC since the third part DICOM archive server accepted the abstract syntax and transfer syntax your CT proposed. Then you need to debug your CT software with the DICOM Detective.

To debug you CT software:
1. Setup the network environment.
2. Open the capture file with the DICOM Detective.
3. Switch to the Simulator-SCP view.
4. Enter a port number
5. Press "start", then the Simulator-SCP daemon can listen to a certain port.
6. You should set break points and start your CT software (use same version and same setting) with the debug mode.
7. Do exact operation sequence that was done in the customer site to send image to the DICOM Detective simulator SCP.
8. Then the DICOM Detective simulator SCP begins to interact with your CT.
9. Your CT software will stop at the break point, you can trace and debug you source codes.

Case 3. Advanced Usage of Export and Import Function
Suppose that your DICOM print server could not function well with a third part DICOM conforming CT in a customer's site 1000 kilometers away. You could not travel to the customer's site in short time to solve the problem. Then a service man there captured the DICOM communication by Sniffer Pro 4.5 and sent you the network capture file. You opened the capture file with the DICOM Detective and checked the DICOM communication between your DICOM print server and the third part CT. You found that the communication is like below.

The third part CT >> A-ASSOCIATE-RQ >> Your DICOM print server
The third part CT << A-ASSOCIATE-AC << Your DICOM print server
The third part CT >> N-GET-RQ >> Your DICOM print server
The third part CT << N-GET-RSP << Your DICOM print server
The third part CT >> N-CREATE-RQ >> Your DICOM print server
The third part CT << N- CREATE -RSP << Your DICOM print server
The third part CT >> N- CREATE -RQ >> Your DICOM print server
The third part CT << N- CREATE -RSP << Your DICOM print server
The third part CT >> N-SET-RQ >> Your DICOM print server
The third part CT << N-SET-RSP << Your DICOM print server
The third part CT >> N-ACTION-RQ >> Your DICOM print server
The third part CT << A-ABORT << Your DICOM print server

You checked every communication detail using PDU view and Service Element View and found that neither the third part CT nor your print server violated the DICOM

standard. But you do not know why you print server sent back an "A-ABORT" instead of a "N-ACTION-RSP" after receiving a N-ACTION-RQ. Then you need to debug your archive server software with the DICOM Detective.

Most cases, for DICOM print service, The Referenced SOP Instance UID (0008,1155) inside Referenced Film Session Sequence (2010,0500) and the Referenced SOP Instance UID (0008,1155) inside Referenced Image Box Sequence (2010,0510) are dynamically created in print server, so these two UIDs fixed in the capture data would not fit for simulation of the DICOM print SCU peer. So, you need to make modification to the capture data.

So, first, you need to export the raw communication data to a directory using the DICOM Detective. Then you should find and modify the Referenced SOP Instance UID (0008,1155) inside Referenced Film Session Sequence (2010,0500) and the Referenced SOP Instance UID (0008,1155) inside Referenced Image Box Sequence (2010,0510) using binary editor to edit the communication data sent by the CT.

Because these two UIDs are going to be created by your print server, you know what UIDs should be set to the raw communication data. If you changed the length of these two UIDs, you should also modify the element length, group length, PDV length and PDU length. After modification, you can import the modified data into the DICOM Detective.

Then you can trace and debug your print server using the similar procedures described in Case 1.

Case 4. Usage of Joint Connection and Run SCU process
Suppose that your DICOM image viewer could not function well with a third part DICOM archive server in a customer's site 1000 kilometers away. You could not travel to the customer's site in short time to solve the problem. Then a service man there captured the DICOM communication by Sniffer Pro 4.5 and sent you the network capture file. You opened the capture file with the DICOM Detective and checked the DICOM communication detail between the third part DICOM archive server and your image viewer. You found that the communication is like below.

Connection 1 (The image viewer send C-ECHO to the archive server to verify the network for retrieving image):
Image viewer >> A- ASSOCIATE -RQ >> The third part DICOM archive server
Image viewer << A-ASSOCIATE-AC << The third part DICOM archive server
Image viewer >> C-ECHO-RQ >> The third part DICOM archive server
Image viewer << C-ECHO-RSP << The third part DICOM archive server
Image viewer >> A-RELEASE-RQ >> The third part DICOM archive server
Image viewer << A-RELEASE-RP << The third part DICOM archive server

Connection 2 (The image viewer sent C-MOVE to the archive server to retrieve image):
Image viewer >> A- ASSOCIATE -RQ >> The third part DICOM archive server
Image viewer << A-ASSOCIATE-AC << The third part DICOM archive server
Image viewer >> C-MOVE-RQ >> The third part DICOM archive server
Image viewer << C-MOVE-RSP << The third part DICOM archive server

Image viewer << C-MOVE-RSP << The third part DICOM archive server
Image viewer >> A-RELEASE-RQ >> The third part DICOM archive server
Image viewer << A-RELEASE-RP << The third part DICOM archive server

Connection 3 (The archive server sent the C-ECHO to the image viewer to verity network for image storage):
The third part DICOM archive server >> A- ASSOCIATE -RQ >> Image viewer
The third part DICOM archive server << A-ASSOCIATE-AC << Image viewer
The third part DICOM archive server >> C-ECHO-RQ >> Image viewer
The third part DICOM archive server << C-ECHO-RSP << Image viewer
The third part DICOM archive server >> A-RELEASE-RQ >> Image viewer
The third part DICOM archive server << A-RELEASE-RP << Image viewer

Connection 4 (The archive server sent C-STORE to the image viewer to store image):
The third part DICOM archive server >> A- ASSOCIATE -RQ >> Image viewer
The third part DICOM archive server << A-ASSOCIATE-AC << Image viewer
The third part DICOM archive server >> C-STORE-RQ >> Image viewer
The third part DICOM archive server << A-ABORT << Image viewer

You checked every communication detail using PDU view and Service Element View and found that none of your image viewer or the third part archive server violated the DICOM standard. But you do not know why you image viewer sent an "A-ABORT" instead of a "C-STORE-RSP" after receiving a C-STORE-RQ since the image viewer accepted the abstract syntax and transfer syntax that the archive server proposed. Then you need to debug your image viewer with the DICOM Detective.

For this case, you must use the functions of **Joint Connection** and **Run SCU Process** to simulate. After open the capture file:

First, setup the network environment.

Second, you should joint connections (connection 3 for C-ECHO and connection 4 for C-STORE) for SCU.

1. Select connection 3 (C-ECHO).
2. Switch to **Simulator-SCU** view.
3. Check "**Synchronize**" to ensure the C-ECHO and C-STORE have the same destination.
4. Enter the **IP address** and **Port** of the image viewer.
5. Check the "First Connection", then the "Joint Connection" is automatically checked, the "**group:order"** is displayed as 0:0.
6. Select connection 4 (C-STORE).
7. Switch to **Simulator-SCU** view.
8. Check "**Synchronize**" to ensure the C-ECHO and C-STORE have the same destination. (The **IP address** and **Port** will be automatically changed to be same with the IP address and port of connection 3.)
9. Check "**Joint Connection**", keep the "First Connection" unchecked, then the "**group:order"** is displayed as 0:1.

Third, you should joint connections (connection 1 for C-ECHO and connection 2 for C-MOVE) for SCP.

1. Select connection 1 (C-ECHO).
2. Switch to **Simulator-SCP** view.
3. Enter the "**Port**" to which the simulator daemon will listen.
4. Check the "First Connection", then the "Joint Connection" is automatically checked, the "**group:order"** is displayed as 0:0.
5. Select connection 2 (C-MOVE).
6. Switch to **Simulator-SCP** view.
7. Check "**Joint Connection**", keep the "First Connection" unchecked, then the "**group:order"** is displayed as 0:1 and the port is automatically changed to be same with the port of connection 1.

Forth, you should combine the SCU of C-ECHO and C-STORE with the SCP of C-ECHO and C-MOVE using **Run SCU Process**.

1. Select connection 2 (C-MOVE).
2. Switch to **Simulator-SCP** view.
3. Check "**Synchronize**" to enable synchronize simulation for C-MOVE.
4. Select "0:_" (that is created in the first step) from the **Group** combo box.

Fifth, start the SCP daemon by clicking the "Start" button in the **Simulator-SCP** view of connection 1. Then the DICOM Detective SCP simulator starts to listen to the port.

Sixth, you should make preparation for the image viewer.
1. You should set break points and start your image viewer (use same version and same setting) with the debug mode.
2. Do exact operation sequence that was done in the customer site to retrieve image from the DICOM Detective simulator SCP.

Then, the DICOM Detective simulator SCP begins to interact with your image viewer. It will start to send image (C-ECHO and C-STORE) using the SCU simulator during the C-MOVE process.

Your image viewer will stop at the break point (after the DICOM Detective sends the image to you image viewer if you set the break point at the right place), you can trace and debug you source codes.

Appendix B: Report Sample

```
192.168.10.1:1083 >> A-ASSOCIATE-RQ >> 192.168.10.2:5104
          Called Ap Title:       IMAGE_SERVER
          Calling Ap Title:      RADDEM-000000
          Application Context: 1.2.840.10008.3.1.1.1(DICOM Application Context Name)
          Presentation Context ID:       1
                    SOP Classs:        1.2.840.10008.5.1.4.1.1.7(Secondary Capture Image Storage)
                    Transfer Syntax(Proposed):       1.2.840.10008.1.2.1(Explicit VR Little Endian)
                    Transfer Syntax(Proposed):       1.2.840.10008.1.2.2(Explicit VR Big Endian)
                    Transfer Syntax(Proposed):       1.2.840.10008.1.2(Implicit VR Little Endian: Default Transfer Syntax
                                                                            for DICOM)
          Presentation Context ID:       3
                    SOP Classs:        1.2.840.10008.5.1.4.1.1.6.1(Ultrasound Image Storage)
                    Transfer Syntax(Proposed):       1.2.840.10008.1.2.1(Explicit VR Little Endian)
                    Transfer Syntax(Proposed):       1.2.840.10008.1.2.2(Explicit VR Big Endian)
                    Transfer Syntax(Proposed):       1.2.840.10008.1.2(Implicit VR Little Endian: Default Transfer Syntax
                                                                            for DICOM)
          Presentation Context ID:       5
                    SOP Classs:        1.2.840.10008.5.1.4.1.1.3.1(Ultrasound Multi-frame Image Storage)
                    Transfer Syntax(Proposed):       1.2.840.10008.1.2.1(Explicit VR Little Endian)
                    Transfer Syntax(Proposed):       1.2.840.10008.1.2.2(Explicit VR Big Endian)
                    Transfer Syntax(Proposed):       1.2.840.10008.1.2(Implicit VR Little Endian: Default Transfer Syntax
                                                                            for DICOM)
          Presentation Context ID:       7
                    SOP Classs:        1.2.840.10008.5.1.4.1.1.6(Ultrasound Image Storage)
                    Transfer Syntax(Proposed):       1.2.840.10008.1.2.1(Explicit VR Little Endian)
                    Transfer Syntax(Proposed):       1.2.840.10008.1.2.2(Explicit VR Big Endian)
                    Transfer Syntax(Proposed):       1.2.840.10008.1.2(Implicit VR Little Endian: Default Transfer Syntax
                                                                            for DICOM)
          Presentation Context ID:       9
                    SOP Classs:        1.2.840.10008.5.1.4.1.1.3(Ultrasound Multi-frame Image Storage)
                    Transfer Syntax(Proposed):       1.2.840.10008.1.2.1(Explicit VR Little Endian)
                    Transfer Syntax(Proposed):       1.2.840.10008.1.2.2(Explicit VR Big Endian)
                    Transfer Syntax(Proposed):       1.2.840.10008.1.2(Implicit VR Little Endian: Default Transfer Syntax
                                                                            for DICOM)
          User Information
                    Max Sub-Length:      32768
                    Implementation Class:       1.2.840.146759.7.119
                    Implementation Version:       RADDEM_3
192.168.10.1:1083 << A-ASSOCIATE-AC << 192.168.10.2:5104
          Called Ap Title:       IMAGE_SERVER
          Calling Ap Title:      RADDEM-000000
          Application Context: 1.2.840.10008.3.1.1.1(DICOM Application Context Name)
          Presentation Context ID:       1
                    SOP Classs:        1.2.840.10008.5.1.4.1.1.7(Secondary Capture Image Storage)
                    Transfer Syntax(accepted):       1.2.840.10008.1.2.1(Explicit VR Little Endian)
          Presentation Context ID:       3
                    SOP Classs:        1.2.840.10008.5.1.4.1.1.6.1(Ultrasound Image Storage)
                    Transfer Syntax(accepted):       1.2.840.10008.1.2.1(Explicit VR Little Endian)
          Presentation Context ID:       5
                    SOP Classs:        1.2.840.10008.5.1.4.1.1.3.1(Ultrasound Multi-frame Image Storage)
                    Transfer Syntax(accepted):       1.2.840.10008.1.2.1(Explicit VR Little Endian)
          Presentation Context ID:       7
                    SOP Classs:        1.2.840.10008.5.1.4.1.1.6(Ultrasound Image Storage)
                    Transfer Syntax(accepted):       1.2.840.10008.1.2.1(Explicit VR Little Endian)
          Presentation Context ID:       9
                    SOP Classs:        1.2.840.10008.5.1.4.1.1.3(Ultrasound Multi-frame Image Storage)
                    Transfer Syntax(accepted):       1.2.840.10008.1.2.1(Explicit VR Little Endian)
          User Information
                    Max Sub-Length:      32768
                    Implementation Class:       1.2.826.0.1.3680043.2.60.0.1
                    Implementation Version:       softlink_jdt103
192.168.10.1:1083>>C-STORE-RQ           Ultrasound Image Storage ; Explicit VR Little Endian>>192.168.10.2:5104
          Command Set(total:7)
                    (0000,0000)        (UL)    4        1        [ 124 (0000007CH)]  Group 0000 Length
                    (0000,0002)        (UI)    28       1(1)     [1.2.840.10008.5.1.4.1.1.6.1(Ultrasound Image
Storage)]   Affected SOP Class UID
                    (0000,0100)        (US)    2        1(1)     [0001H (C-STORE-RQ)]        Command Field
                    (0000,0110)        (US)    2        1(1)     [12 (000CH)]        Message ID
                    (0000,0700)        (US)    2        1(1)     [0000H (MEDIUM)]  Priority
                    (0000,0800)        (US)    2        1(1)     [0000H (Data Set is Present)]     Data Set Type
                    (0000,1000)        (UI)    40       1(1)     [1.2.840.146759.7.119.1.1064606707.0.66.4]
                                                                            Affected SOP Instance UID
```

47

Data Set(total:44)

Tag	VR	Len	VM	Value	Name
(0008,0008)	CS(CS)	58	6(1-n)	[ORIGINAL\PRIMARY\VASCULAR\0001\DEMOMULTIFRAME\DEMOMTCOUNT1]	Image Type
(0008,0016)	UI(UI)	28	1(1)	[1.2.840.10008.5.1.4.1.1.6.1(Ultrasound Image Storage)]	SOP Class UID
(0008,0018)	UI(UI)	40	1(1)	[1.2.840.146759.7.119.1.1064606707.0.66.4]	SOP Instance UID
(0008,0020)	DA(DA)	8	1(1)	[20030926]	Study Date
(0008,0021)	DA(DA)	8	1(1)	[20030926]	Series Date
(0008,0023)	DA(DA)	8	1(1)	[20030926]	Content Date
(0008,0030)	TM(TM)	6	1(1)	[162420]	Study Time
(0008,0031)	TM(TM)	6	1(1)	[162420]	Series Time
(0008,0033)	TM(TM)	6	1(1)	[162426]	Content Time
(0008,0050)	SH(SH)	0	0(1)	[]	Accession Number
(0008,0060)	CS(CS)	2	1(1)	[US]	Modality
(0008,0070)	LO(LO)	18	1(1)	[DEMOCH Med. System]	Manufacturer
(0008,0080)	LO(LO)	12	1(1)	[Development]	Institution Name
(0008,0090)	PN(PN)	0	0(1)	[]	Referring Physician's Name
(0008,1010)	SH(SH)	6	1(1)	[M0000]	Station Name
(0008,1040)	LO(LO)	12	1(1)	[Development]	Institutional Department Name
(0008,1070)	PN(PN)	4	1(1-n)	[ADM]	Operators' Name
(0008,1090)	LO(LO)	6	1(1)	[RADDEM]	Manufacturer's Model Name
(0010,0010)	PN(PN)	0	0(1)	[]	Patient's Name
(0010,0020)	LO(LO)	4	1(1)	[DGW]	Patient ID
(0010,0030)	DA(DA)	0	0(1)	[]	Patient's Birth Date
(0010,0032)	TM(TM)	6	1(1)	[000000]	Patient's Birth Time
(0010,0040)	CS(CS)	2	1(1)	[O]	Patient's Sex
(0018,1020)	LO(LO)	16	1(1-n)	[RADDEM:R3.0.0DF]	Software Versions
(0018,6011)	SQ(SQ)	208	1(1)	[]	Sequence of Ultrasound Regions

Sequence of Items

Tag	VR	Len	VM	Value	Name
(FFFE,E000)	(NE)	200	1(1)	[]	Item

Sequence Item

Tag	VR	Len	VM	Value	Name
(0018,6012)	US(US)	2	1(1)	[1 (0001H)]	Region Spatial Format
(0018,6014)	US(US)	2	1(1)	[1 (0001H)]	Region Data Type
(0018,6016)	UL(UL)	4	1(1)	[0 (00000000H)]	Region Flags
(0018,6018)	UL(UL)	4	1(1)	[2 (00000002H)]	Region Location Min X0
(0018,601A)	UL(UL)	4	1(1)	[48 (00000030H)]	Region Location Min Y0
(0018,601C)	UL(UL)	4	1(1)	[535 (00000217H)]	Region Location Max X1
(0018,601E)	UL(UL)	4	1(1)	[437 (000001B5H)]	Region Location Max Y1
(0018,6020)	SL(SL)	4	1(1)	[267 (0000010BH)]	Reference Pixel X0
(0018,6022)	SL(SL)	4	1(1)	[10 (0000000AH)]	Reference Pixel Y0
(0018,6024)	US(US)	2	1(1)	[3 (0003H)]	Physical Units X Direction
(0018,6026)	US(US)	2	1(1)	[3 (0003H)]	Physical Units Y Direction
(0018,6028)	FD(FD)	8	1(1)	[0.000000]	Reference Pixel Physical Value X
(0018,602A)	FD(FD)	8	1(1)	[0.000000]	Reference Pixel Physical Value Y
(0018,602C)	FD(FD)	8	1(1)	[0.037225]	Physical Delta X
(0018,602E)	FD(FD)	8	1(1)	[0.037225]	Physical Delta Y
(0018,6030)	UL(UL)	4	1(1)	[3750 (00000EA6H)]	Transducer Frequency
(0020,000D)	UI(UI)	38	1(1)	[1.2.840.146759.7.119.1.1064606707.0.64]	Study Instance UID
(0020,000E)	UI(UI)	38	1(1)	[1.2.840.146759.7.119.1.1064606707.0.65]	Series Instance UID
(0020,0010)	SH(SH)	0	0(1)	[]	Study ID
(0020,0011)	IS(IS)	4	1(1)	[0001]	Series Number
(0020,0013)	IS(IS)	4	1(1)	[0001]	Instance Number
(0020,0020)	CS(CS)	0	0(2)	[]	Patient Orientation
(0028,0002)	US(US)	2	1(1)	[1 (0001H)]	Samples per Pixel

(0028,0004)	CS(CS)	12	1(1)	[MONOCHROME2] Photometric Interpretation
(0028,0006)	US(US)	2	1(1)	[0 (0000H)]	Planar Configuration
(0028,0010)	US(US)	2	1(1)	[480 (01E0H)]	Rows
(0028,0011)	US(US)	2	1(1)	[640 (0280H)]	Columns
(0028,0100)	US(US)	2	1(1)	[8 (0008H)]	Bits Allocated
(0028,0101)	US(US)	2	1(1)	[8 (0008H)]	Bits Stored
(0028,0102)	US(US)	2	1(1)	[7 (0007H)]	High Bit
(0028,0103)	US(US)	2	1(1)	[0 (0000H)]	Pixel Representation
(0028,1050)	DS(DS)	4	1(1-n)	[127]	Window Center
(0028,1051)	DS(DS)	4	1(1-n)	[256]	Window Width
(0028,2110)	CS(CS)	2	1(1)	[00]	Lossy Image Compression
(7FE0,0010)	OB(OW\OB)	307200	1(1\1)		

[2E1515151515151515151515151515151515151515151515151515151515151515151515...]   Pixel
Data
192.168.10.1:1083<<C-STORE-RSP   Ultrasound Image Storage ; Explicit VR Little Endian<<192.168.10.2:5104

Command Set(total:8)

(0000,0000)	(UL)	4	1	[154 (0000009AH)] Group 0000 Length
(0000,0002)	(UI)	28	1(1)	[1.2.840.10008.5.1.4.1.1.6.1(Ultrasound Image Storage)] Affected SOP Class UID
(0000,0100)	(US)	2	1(1)	[8001H (C-STORE-RSP)] Command Field
(0000,0120)	(US)	2	1(1)	[12 (000CH)] Message ID Being Responded To
(0000,0800)	(US)	2	1(1)	[0101H (No Data Set is Present)] Data Set Type
(0000,0900)	(US)	2	1(1)	[45056 (B000H)] Status
(0000,0902)	(LO)	22	1(1)	[set StudyID to <null>] Error Comment
(0000,1000)	(UI)	40	1(1)	[1.2.840.146759.7.119.1.1064606707.0.66.4] Affected SOP Instance UID

192.168.10.1:1083 >> A-ASSOCIATE-RQ >> 192.168.10.2:5104
192.168.10.1:1083 << A-ASSOCIATE-RP << 192.168.10.2:5104