CSCI-4448/5448: Project #2

Special Note: we used "StarUML" as a modeling tool, but it does not support exact the same diagram features with the lecture. For example, we can neither underline object names nor add special characters such as ":" to the name of the object in the sequence diagram. Also, it is not possible to add actor icon in the sequence diagram.

1. **Team:** Woncheol Song
   Tae Gu Kim
   Hui Soon Kim

2. **Title:** Packet Analyzer

3. **Project Summary:** An application program to analyze network protocols, visualize packet information and network statistics from packet data in order to assist network administrator for network management.

4. **Project Requirements**

   4.1. Business Requirements: None

   4.2. User Requirements

ID	Requirement	Topic Area	User	Priority
US-01	As a user, I should be able to start capturing network packet so that I can see the contents of network packet	Capture	All	Critical
US-02	As a user, I should be able to stop capturing network packet so that I don't waste storage to save uninterested data	Capture	All	High
US-03	As a user, I want to select network device to be used in capture so that I can collect network data from interested interface	Capture	All	High
US-04	As a user, I want to analyze a specific packet in the main screen so that I can see the contents of the packet in detail	Display	All	Critical
US-05	As a user, I want to select a specific	Display	All	High

	layer from the selected packet so that I can check the range of content corresponding to selected layer			
US-06	As a user, I want to filter packets so that I can see only interesting packets.	Filter	All	Critical
US-07	As a user, I want to choose the range of time period in the filter screen so that I can see packets only for interested period of time	Filter	All	High
US-08	As a user, I want to choose the type of protocol in the filter screen so that I can see packets only for interested type of packets.	Filter	All	High
US-09	As a user, I want to see the statistics of network traffic as a visual graph so that I can the network status intuitively	Statistics	All	Critical
US-10	As a user, I want to see packet traffic per second in the statistics screen so that I can see the network traffic rate	Statistics	All	High
US-11	As a user, I want to see traffic for each protocol in the statistics screen so that I can see the protocol variation	Statistics	All	High
US-12	As a user, I want to terminate the program whenever I don't need any use of it	Display	All	High
US-13	As a user, I want to search specific packet so that I can see packets which contain specific string	Display	All	High
US-14	As a user, I want to save the incoming packets so that I can use the packets later	DB	All	Critical

4.3.   Functional Requirements

| ID	Requirement	Topic Area	User	Priority
FR-01	Upon starting capture, the system will invoke "Select Interface" dialog if there is no chosen NIC which will be used	Capture	All	Critical

	on packet capture			
FR-02	When the user requires to stop packet capture, the system should release all resources used in capturing	Capture	All	Critical
FR-03	When the system captures a packet, it is automatically parsed	Capture	All	Critical
FR-04	When the system captures a packet, it is automatically saved in the DB	Capture	All	Critical
FR-05	When the user require to filter packets, the system will fetch the matched packets from the database using the sql statement	Filter	All	Critical
FR-06	When the system start capturing packets, it shows at least Time, Source IP, Destination IP, Protocol, Length of packet when it shows the list of the packets in the main screen.	Capture	All	Critical
FR-07	When the system captures a packet, it is automatically updated in the list	Display	All	Critical
FR-08	The system will provide options which enables user to select specific packet layer so that the user can see the contents corresponding to that layer	Display	All	High
FR-09	The system will highlight the specific range of the contents when a user select a specific layer of the packet	Display	All	High
FR-10	When the user change the type of statistics, the system should calculate it again	Statistics	All	High
FR-11	When the user change the type of graph, the system should draw with the chosen type of graph	Statistics	All	High
FR-12	When the user requires to search specific packet, the system should build SQL statement for searching it	Search	All	Critical
FR-13	When creating statistics graph window for the first time, the system displays	Statistics	All	Medium

ID	Requirement	Topic Area	User	Priority
	the graph windows using default statistics type " packet per second"			
FR-14	When creating statics graph window for the first time, the system displays the graph windows using default graph type "bar graph"	Statistics	All	Medium

4.4.   Non-Functional Requirements

ID	Requirement	Topic Area	User	Priority
NF-01	Storage space should be enough to save 10-minutes seamless packet capturing	Reliability	All	Medium
NF-02	During the packet capturing, the user should be able to interact with the UI so that he or she can select and see the contents of the packet	Usability	All	High
NF-03	Query should be performed within 3 seconds	Performance	All	High
NF-04	Upon starting packet capture, the program should process all of the packets on the network in real time	Performance	All	Critical
NF-05	A notification should be generated if there has been no network traffic for more than 1 minute	Usability	All	Medium

5. Use Cases Diagram
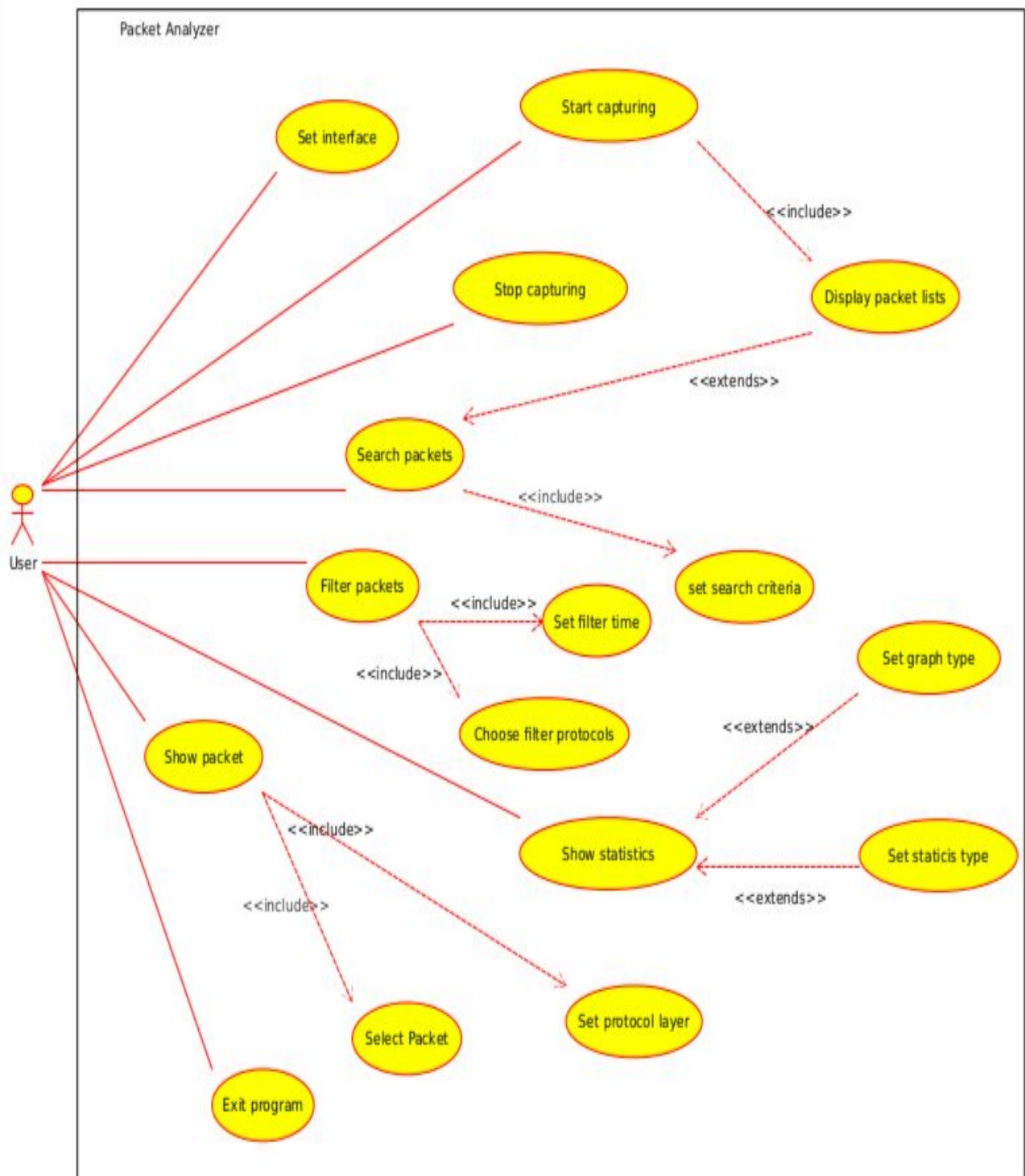
Use Case ID:	UC-01
Use Case Name:	Set Interface
Description:	User can set the network interface controller(NIC) whose data will be captured among the LAN adaptors installed on the user computer.

Actors:	User		
Pre-Conditions:	The computer has to include at least one LAN adaptors in it.		
Post-Conditions:	The program selected only one interface to capture network packets.		
Frequency of Use:	Rare		
Flow of Events:		Actor Action	System Response
	1	Click on interface button in program menu	Invoke a dialog box to list all the equipped interface lists of the computer
	2	Choose a specific interface on the dialog box	
	3	Click on "OK" on the dialog box	Ready to start capturing the network packet from the selected interface
Variations:			
Notes and Issues:			
Developer Notes:			

Use Case ID:	UC-02
Use Case Name:	Start Capturing
Description:	When user clicks "Start" button, the system should start capturing network packets from the chosen network interface.

Actors:	User		
Pre-Conditions:	Network interface card which will be used in packet capturing should be selected in advance.		
Post-Conditions:	Display all packet lists which have been captured on the screen in real time. All packets which have been captured should be saved in DB.		
Frequency of Use:	Very often		
Flow of Events:		Actor Action	System Response
	1	Click "Start" button	Start capturing packets
	2		Parse captured packets
	3		Save parsed packets in DB
	4		Display packet lists on the screen in real time
Variations:	1. If there is no network interface card chosen in advance, invoke a dialog in which user can choose NIC before starting capturing		
Notes and Issues:			
Developer Notes:			

Use Case ID:	UC-03
Use Case Name:	Stop Capturing
Description:	User can stop capturing packets whenever user wants.

Actors:	User		
Pre-Conditions:	Capturing packets should be started.		
Post-Conditions:	Start button is activated again and DB process for archiving is finalized.		
Frequency of Use:	Often		
Flow of Events:		Actor Action	System Response
	1	Click "Stop" button	Activate start button
	2		Displaying lists and saving packets procedure are stopped automatically
Variations:			
Notes and Issues:			
Developer Notes:			

Use Case ID:	UC-04
Use Case Name:	Search Packets
Description:	User can search packets which contain the particular string in the packet contents

Actors:	User		
Pre-Conditions:	There should be packets in the current lists obtained by querying packets from DB or by capturing from network interface		
Post-Conditions:	Display the search result in the screen		
Frequency of Use:	Rare		
Flow of Events:		Actor Action	System Response
	1	Click "Search Packets"	Display search dialog
	2	Input search text	Search packets based on the user input
	3		Display search result
Variations:			
Notes and Issues:			
Developer Notes:			

Use Case ID:	UC-05
Use Case Name:	Filter Packets
Description:	Choose packets which user want to analyze

Actors:	User		
Pre-Conditions:	Network packets have already been collected in DB		
Post-Conditions:	Display the packets which match user choice.		
Frequency of Use:	Often		
Flow of Events:		Actor Action	System Response
	1	Click filter button	Display filter dialogue
	2	Choose the time and protocol which user want to filter	
	3	Click "OK" button	Make a query statement using the chosen time and protocol
	4		Query from Database
	5		Show the matched results
Variations:			
Notes and Issues:			
Developer Notes:			

Use Case ID:	UC-06
Use Case Name:	Show Packet
Description:	When user select a specific packet from the lists, display detailed packet contents in the screen

Actors:	User		
Pre-Conditions:	There should be packets in the lists by querying packets from DB or by capturing from network interface		
Post-Conditions:	Display the whole contents of the chosen packet		
Frequency of Use:	Very often		
Flow of Events:		Actor Action	System Response
	1	Select a packet in the lists	Show whole list of layer for the selected packet
	2		Show whole contents of the packet in the screen
	3	Select a network layer in the layer list	Highlight the portion of selected layer in the contents of the packet
Variations:			
Notes and Issues:			
Developer Notes:			

Use Case ID:	UC-07
Use Case Name:	Show Statistics
Description:	Display the statistics for the lists of packets queried from DB

Actors:	User
Pre-Conditions:	There should be stored packets in DB
Post-Conditions:	Display the statistics of packets as a graph
Frequency of Use:	Very often

Flow of Events:		Actor Action	System Response
	1	Click "Statistics" button	Invoke statistics screen
	2		Display graph for the lists using defaulting setting
	3	Choose statistics type	Display graph for specified type of statistics
	4	Choose graph type	Change graph type as user selected

Variations:	
Notes and Issues:	
Developer Notes:	

Use Case ID:	UC-08
Use Case Name:	Display Packet Lists
Description:	User can see packet lists on the main screen

Actors:	User		
Pre-Conditions:	Capturing packets or filtering packets should be executed in advance.		
Post-Conditions:	The lists of packets is displayed on the main screen		
Frequency of Use:	Very Often		
Flow of Events:		Actor Action	System Response
	1	Select "Start" button or "Filter" button	Main screen displays the lists of packets
Variations:			
Notes and Issues:			
Developer Notes:			

Use Case ID:	UC-09
Use Case Name:	Set Search Criteria
Description:	Set search criteria which will be used in searching packets

Actors:	User		
Pre-Conditions:	"Search Packets" dialog should be invoked in advance.		
Post-Conditions:	Display the packet lists which correspond to search criteria in the screen.		
Frequency of Use:	Rare		
Flow of Events:		Actor Action	System Response
	1	Choose search criteria	
	2	Click "OK" button	Search next packet from the current selected packet
	3		Highlight the first matching packet in the packet lists
Variations:	3. If there is no packets that corresponds to the search criteria, display a warning dialog indicating the result.		
Notes and Issues:			
Developer Notes:			

Use Case ID:	UC-10
Use Case Name:	Set Filter Time
Description:	User can set the time interval so that the system can filter and display only packets from DB which had been captured during that time.

Actors:	User		
Pre-Conditions:	The system is not in the packet capturing mode because the user can't set filter during packet capturing.		
Post-Conditions:	Display filter result in the screen.		
Frequency of Use:	Often		
Flow of Events:		Actor Action	System Response
	1	Set time condition	
	2	Click "OK" button	Search packets which had been captured during the time condition
	3		Display result packets in the scree
Variations:	3. If there is no packets that corresponds to the filter criteria, display a warning dialog indicating the result.		
Notes and Issues:			
Developer Notes:			

Use Case ID:	UC-11
Use Case Name:	Choose Filter Protocols
Description:	User can choose protocols so that the system can filter and display only packets from DB whose protocols are in filter condition

Actors:	User		
Pre-Conditions:	The system is not in the packet capturing mode because the user can't set filter during packet capturing.		
Post-Conditions:	Display filter result in the screen		
Frequency of Use:	Often		
Flow of Events:		Actor Action	System Response
	1	Set protocol condition	
	2	Click "OK" button	Search packets whose protocols are in search condition
	3		Display result packets in the screen
Variations:	3. If there is no packets that corresponds to the filter criteria, display a warning dialog indicating the result.		
Notes and Issues:			
Developer Notes:			

Use Case ID:	UC-12
Use Case Name:	Set Graph Type
Description:	User can choose a graph type among at least five types(Bar, Area, Line, Pie, and Point chart) so that the user can see the statistics using various type of graph

Actors:	User		
Pre-Conditions:	Statistics dialog should be invoked in advance		
Post-Conditions:	Display statistics as a graph type which the user had chosen		
Frequency of Use:	Often		
Flow of Events:		Actor Action	System Response
	1	Select graph type	Show statistics as a graph type which the user had chosen
Variations:			
Notes and Issues:			
Developer Notes:			

Use Case ID:	UC-13
Use Case Name:	Set Statistics Type
Description:	User can set the statistics type when they want to see the packet statistics

Actors:	User		
Pre-Conditions:	Statistics dialog should be invoked in advance		
Post-Conditions:	The previously displayed statistics type is changed depending on the selected type		
Frequency of Use:	Often		
Flow of Events:		Actor Action	System Response
	1	Select the statistics type	Update the type of statistics according to the selected type
	2		Calculate the statistics depending on the selected criteria
	3		Update the whole statistics display screen
Variations:			
Notes and Issues:			
Developer Notes:			

Use Case ID:	UC-14
Use Case Name:	Set Protocol Layer
Description:	User can choose the specific protocol layer in the chosen packet

Actors:	User		
Pre-Conditions:	User should have chosen the interesting packet		
Post-Conditions:	Display highlighted portion which corresponds to the chosen protocol layer		
Frequency of Use:	Very often		
Flow of Events:		Actor Action	System Response
	1	Choose the interesting protocol layer	Highlights specific portion which corresponds to the chosen protocol layer in the packet contents
Variations:			
Notes and Issues:			
Developer Notes:			

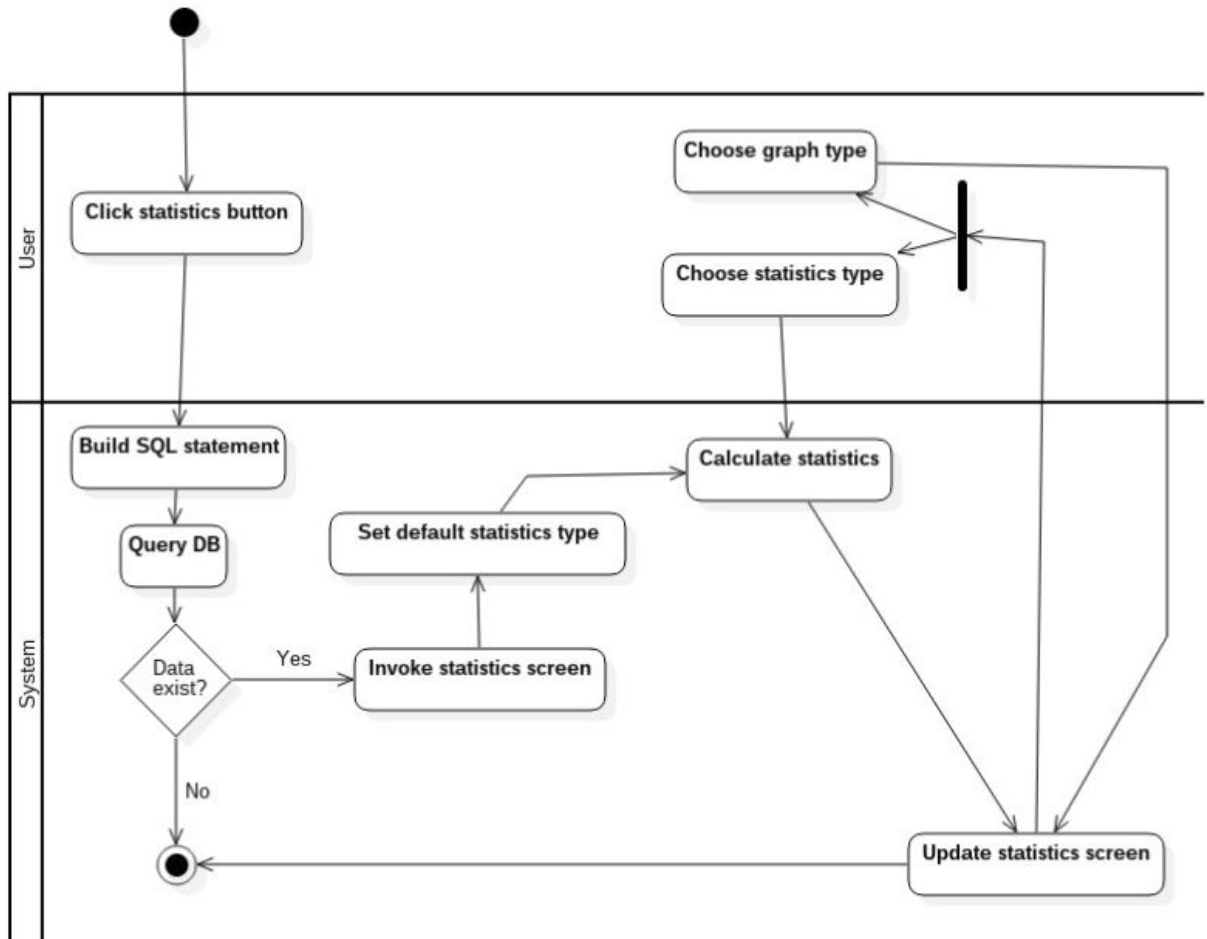| Use Case ID:	UC-15
Use Case Name:	Select Packet
Description:	User can choose a specific packet in the display list.

Actors:	User		
Pre-Conditions:	Capturing packets or filtering packets should be executed and the results should be displayed in the lists.		
Post-Conditions:	Show the chosen packet of the selected protocol on the screen.		
Frequency of Use:	Very Often		
Flow of Events:		Actor Action	System Response
	1	Select a specific packet in the lists	Display protocol layer lists for the selected packet
	2		Display whole contents of the selected packet
Variations:			
Notes and Issues:			
Developer Notes:			

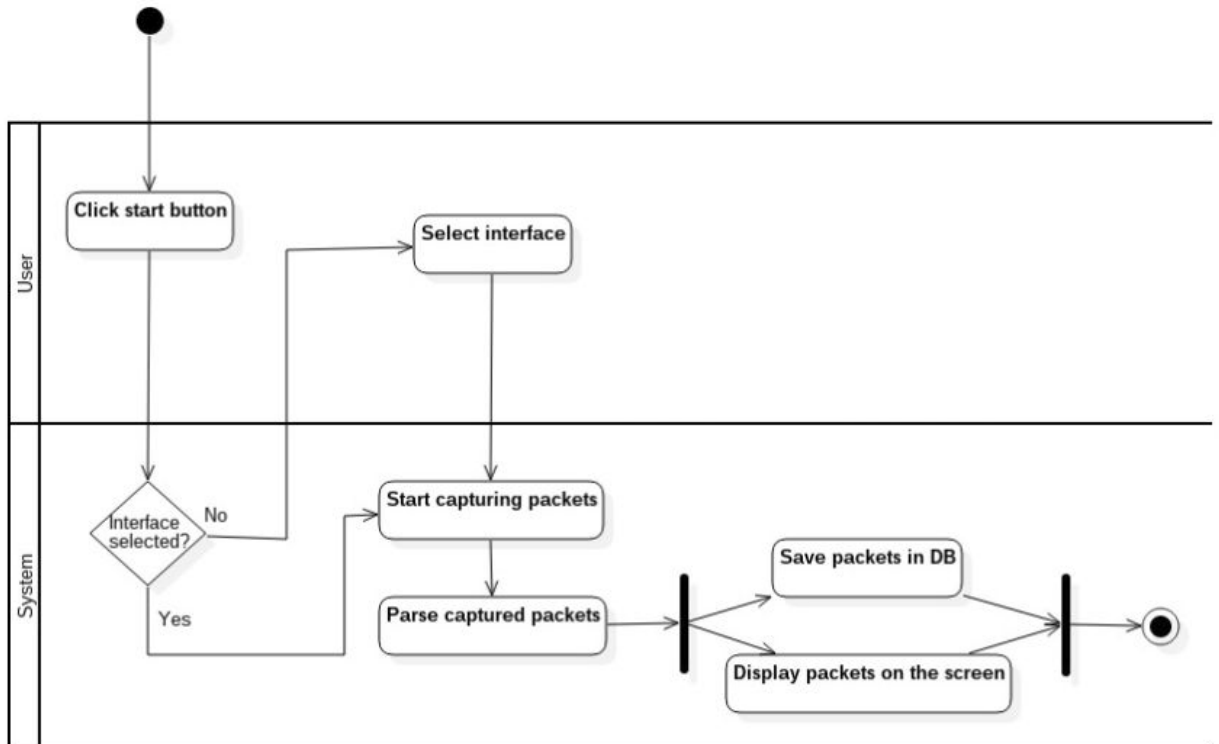| Use Case ID:	UC-16
Use Case Name:	Exit Program
Description:	User can terminate all functions related to packet capturing and release all resources which the program has used.

| Actors:	User		
Pre-Conditions:	All dialog boxes such search, statistics and etc should be closed.		
Post-Conditions:	Terminate the program		
Frequency of Use:	Very rare		
Flow of Events:		Actor Action	System Response
	1	Click "Exit" button or Choose exit menu	Check whether all sub dialog boxes are closed
	2		Terminate the program
Variations:			
Notes and Issues:			
Developer Notes:			

6. Activity Diagram

6.1. Requirement ID:US-09, Use Case ID: UC-07, Use Case Name: Show statistics, Name: Woncheol Song

6.2. **Requirement ID: US-01, Use Case ID: UC-02, Use Case Name: Start capturing, Name: Tae Gu Kim**

6.3. Requirement ID: US-06, Use Case ID: UC-05, Use Case Name: Filter packet, Name: Hui Soon Kim
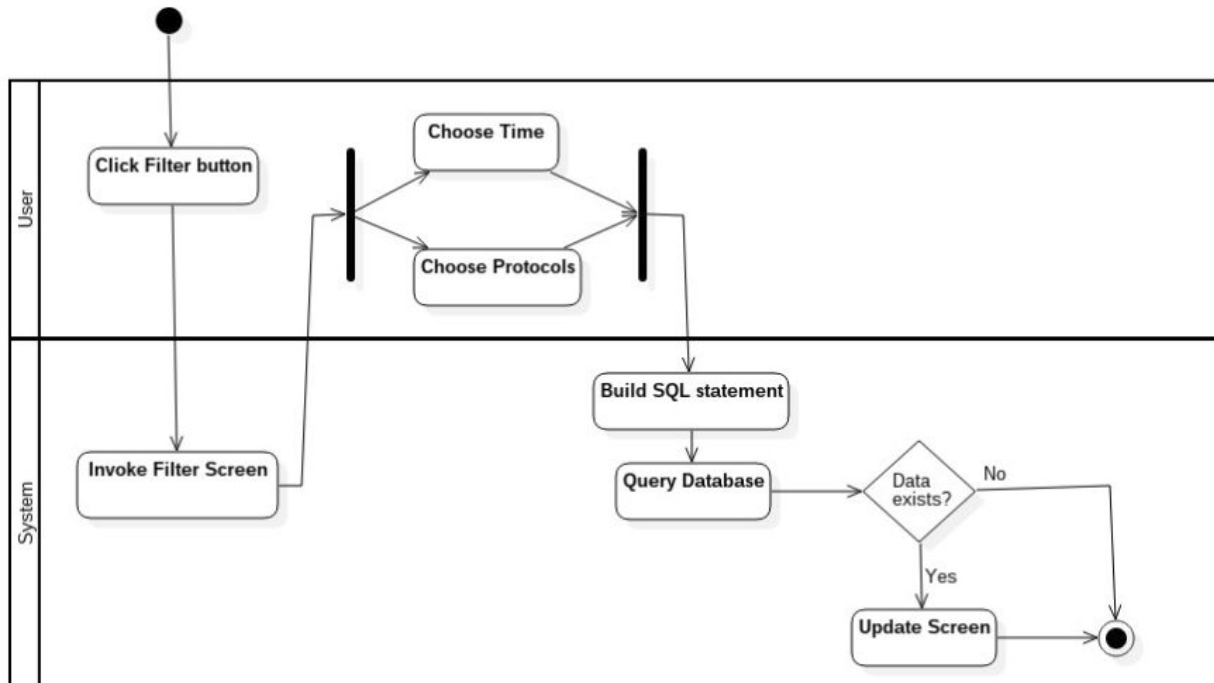

**7. Data Storage**

7.1. Data Storage: SQLite or MySQL

7.2. Classes: OArchive class to store each parsed packet information in DB and to read packets from it. OArchive is a abstract class, and the concrete classes of OArchive: OArchiveSQLite or OArchiveMySQL will be instantiated at run-time according to the type of used database:SQLite or MySQL respectively.

8.   UI Mockups

8.1. Main Screen: The following mockup shows the main screen that users are supposed to see when the "Packet Analyzer" program is executed for the first time. The captured packets are listed in the first lists window displaying packet number, collected time, source IP, destination IP, and application protocol in real time. When user click a specific packet in the lists, the detailed packet information is displayed in the second window and the payload contents of the packet is shown in the third window.
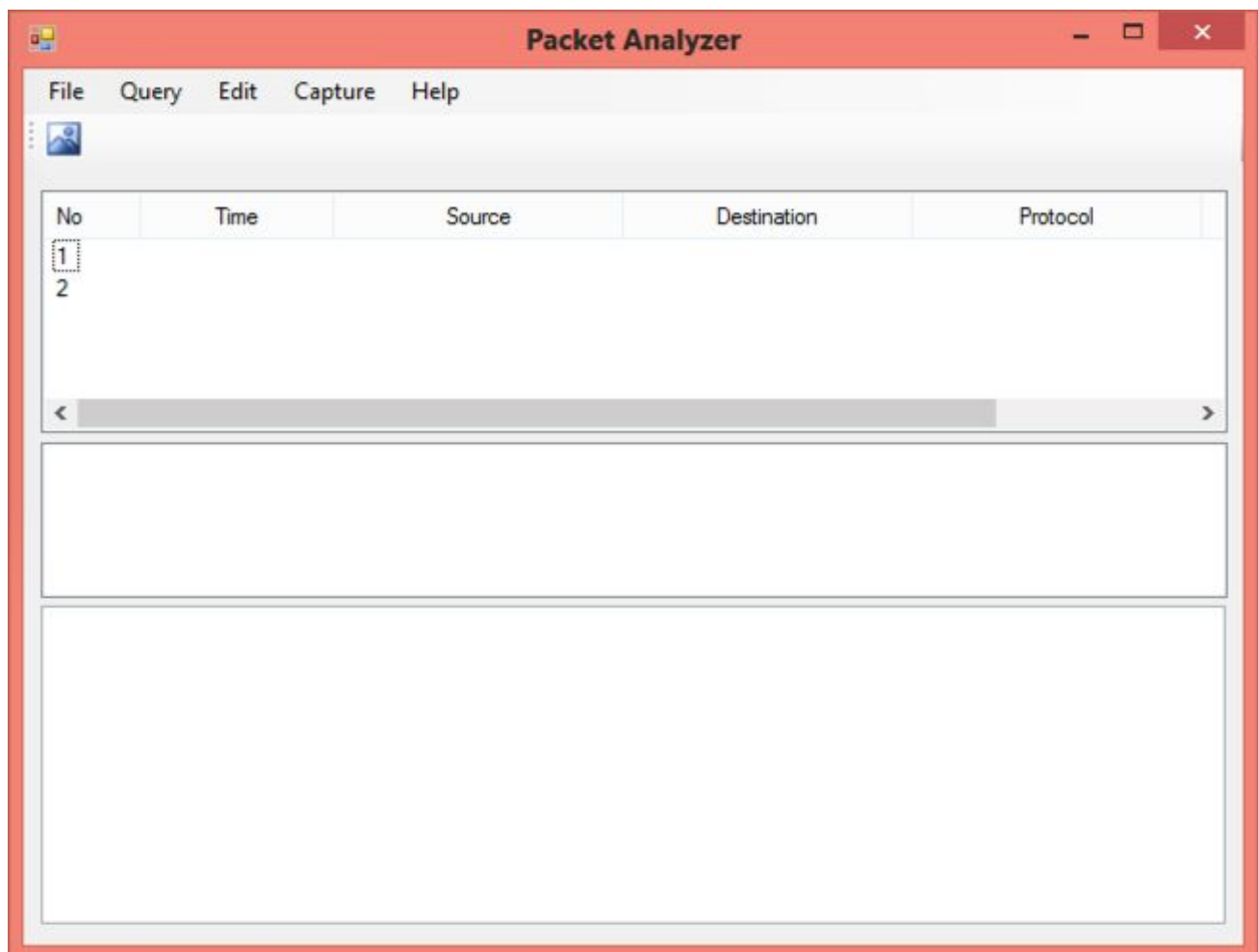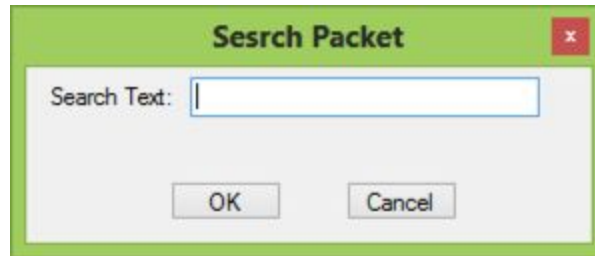
8.2. Packet Filtering Screen: The following mockup pops up when user clicks "Menu->Query -> Filter". Using this window, user can set the time period and protocol types to filter from packets in the current lists of packets of main window. The the results of filtering which are filtered packet lists are displayed on the first list window of the main screen.
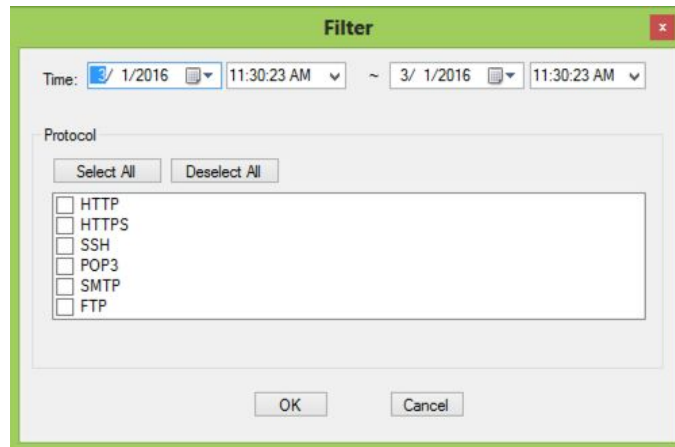
8.4. Statistics Screen: The following mockup pops up when user clicks "Menu->Edit -> Statistics". Using this window, user can set statistics type and graph type and see the statistics graph of packets in the current lists window depending on the setting.
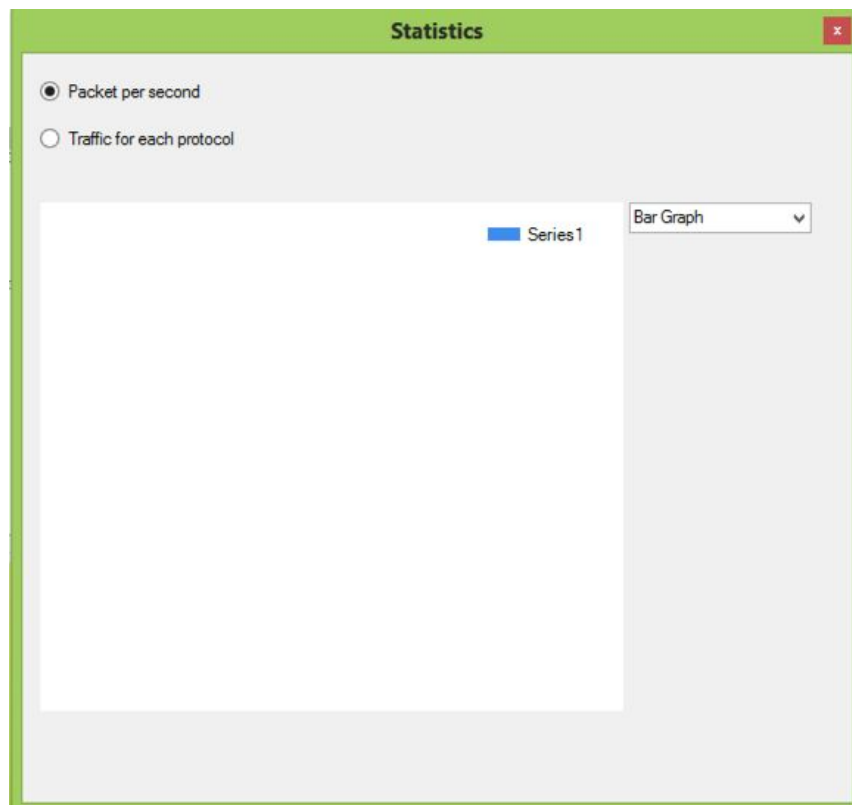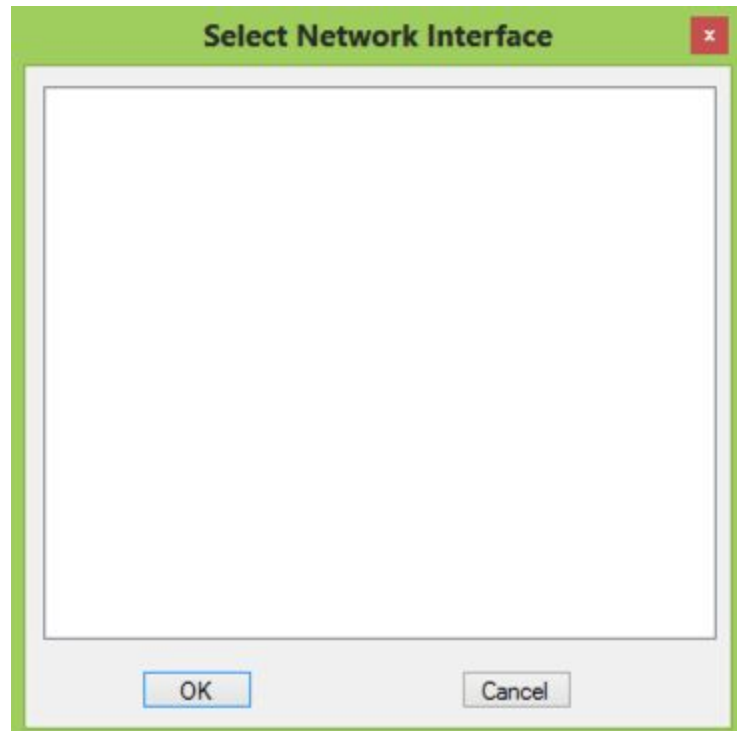
8.3. Search Packet Screen: The following mockup pops up when user clicks "Menu->Edit -> Search packet". Using this window, user can set a string to search in DB.   The the results of search which are packets that are matched with the string in DB are displayed on the first lists window in main screen.

8.5. Select Network Interface Screen: The following mockup pops up when user clicks "Menu->Capture -> Set interface". Using this window, user can choose a specific NIC in the host computer which is used to capture network packets.

9. User Interactions

9.1. Requirement ID: US-09, Use Case ID: UC-07, Use Case Name: Show statistics, Name: Woncheol Song
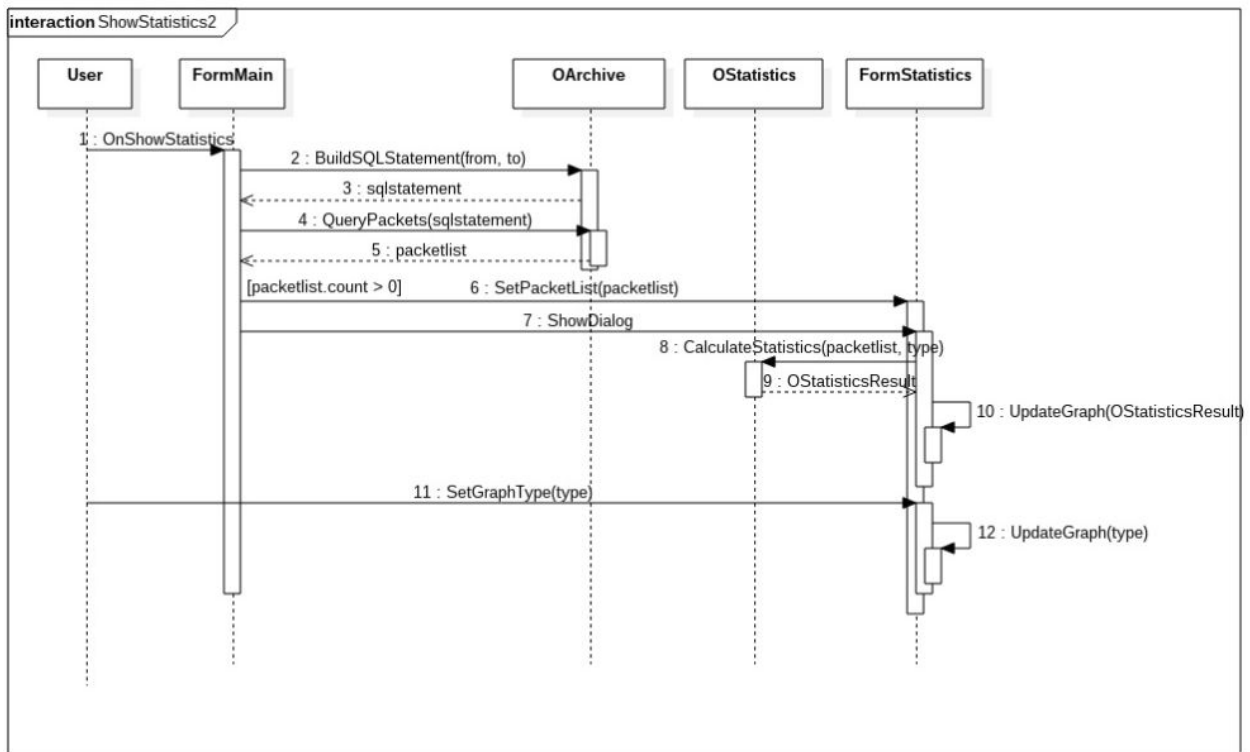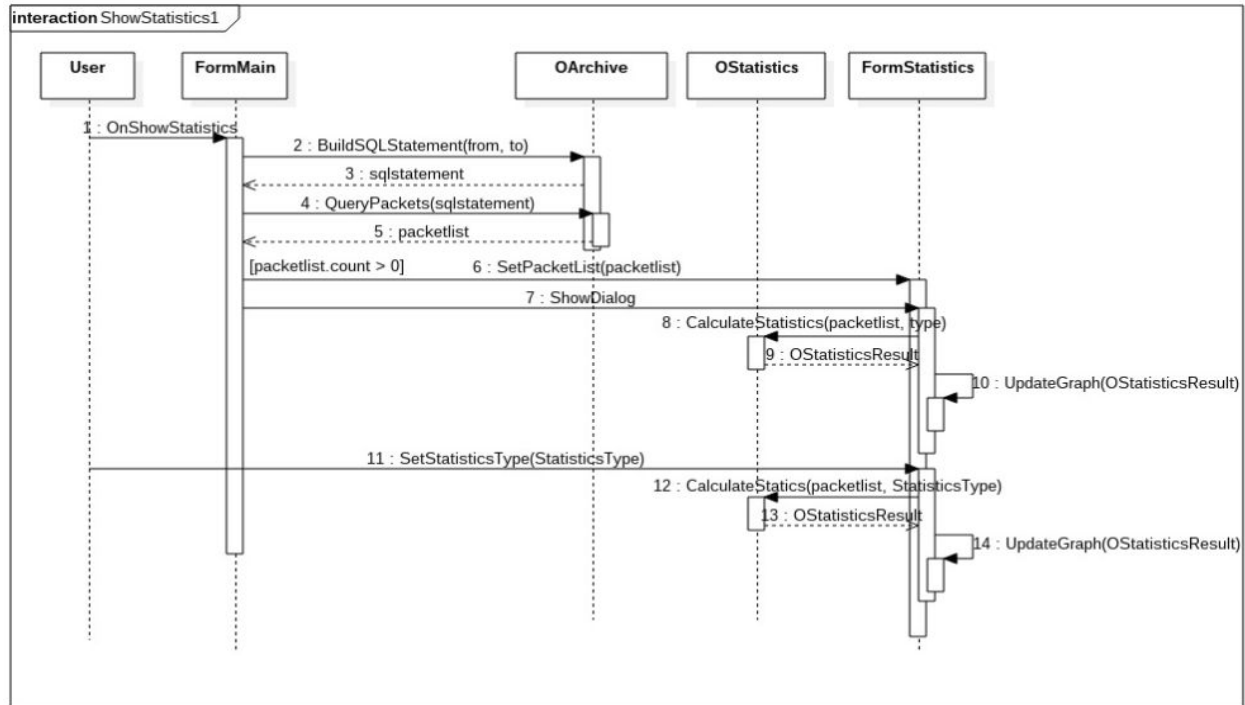
9.2. Requirement ID: US-01, Use Case ID: UC-02, Use Case Name: Start capturing, Name: Tae Gu Kim
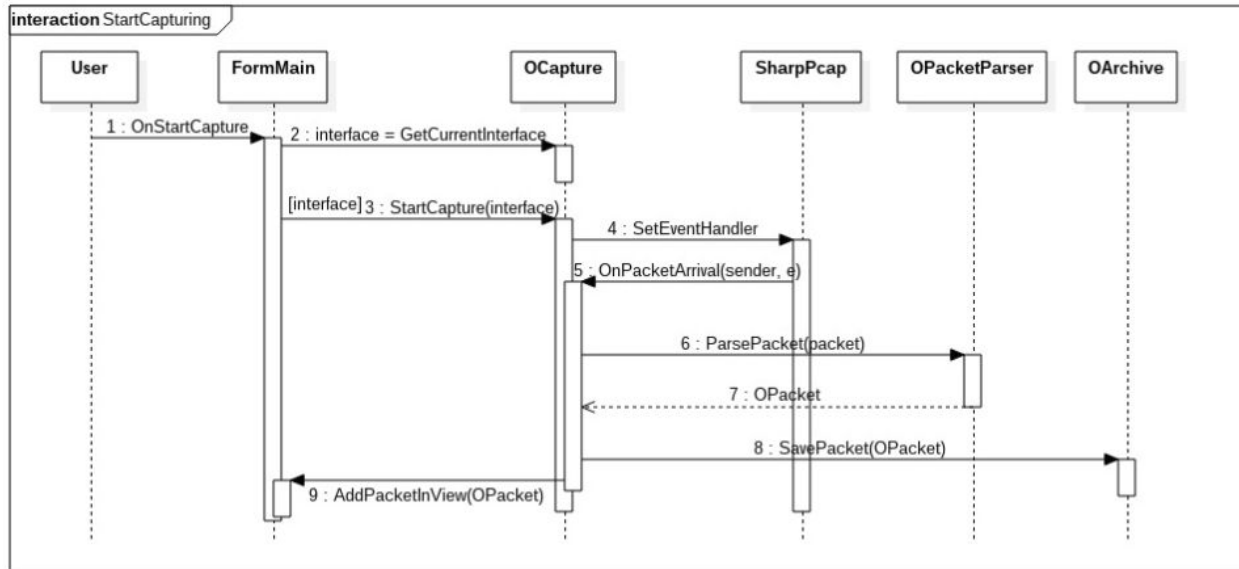
9.3. Requirement ID: US-06, Use Case ID: UC-05, Use Case Name: Filter packet, Name: Hui Soon Kim

10. Class Diagrams

OStatistics

+CalculateStatistics(packet: OCurrentPacketList, type: int): OStatisticsResult
-EnumeratePacket()
-GetNameForPacket(packet: OPacket): String
-IsNameExist(name: String)
-IncrementCountForName(name: String)

OStatisticsResult

-_val: HashTable

+AddStatisticsData(packet: OPacket)
+GetItemCount(): int
+GetName(index: int): String
+GetCount(index: int): int

Template Design Pattern
CalculateStatistics()
{
    EnumeratePacket()
    GetNameForPacket()
    IsNameExist()
    IncrementCountForName()
}

OStatisticsPacketPerProtocol

+GetNameForPacket(packet: OPacket): String

OStatisticsPacketPerTime

+GetNameForPacket(packet: OPacket): String

OCurrentPacketList

-_packets: OPacket[]

+GetCount(): int
+GetAt(i: int): OPacket
+AddPacket(packet OPacket)
+RemoveAt(i: int)

OPacket

-_protocol: int
-_timeCollected: Time
-_rawData: Binary

+SetProtocol(protocol: int)
+GetProtocol(): int
+SetTimeCollected(time: Time)
+GetTimeCollected(): Time
+SetRawData(rawdata: Binary)
+GetRawData(): Binary
+GetRangeOf(protocol_layer: int, start: int, end: int)

OpacketParserEthernet

+ParsetPacket(packet: RawCapture): OPacket

OpacketParserIP

+ParsePacket(packet: RawCapture): OPacket

OPacketParserTransport

+ParsePacket(packet: RawCapture): OPacket

SharpPcap

+SetEventHanler()

OPacketParser

+ParsePacket(packet: RawCapture): OPacket

OCapture

-_device: CaptureDevice[]
-_packetlist: OcurrentPacketList
-_parse: OPacketPaser

+StartCapture(interface: int)
+StopCapture()
+OnPacketArrival(sender: object, e: CaptureEventArg)
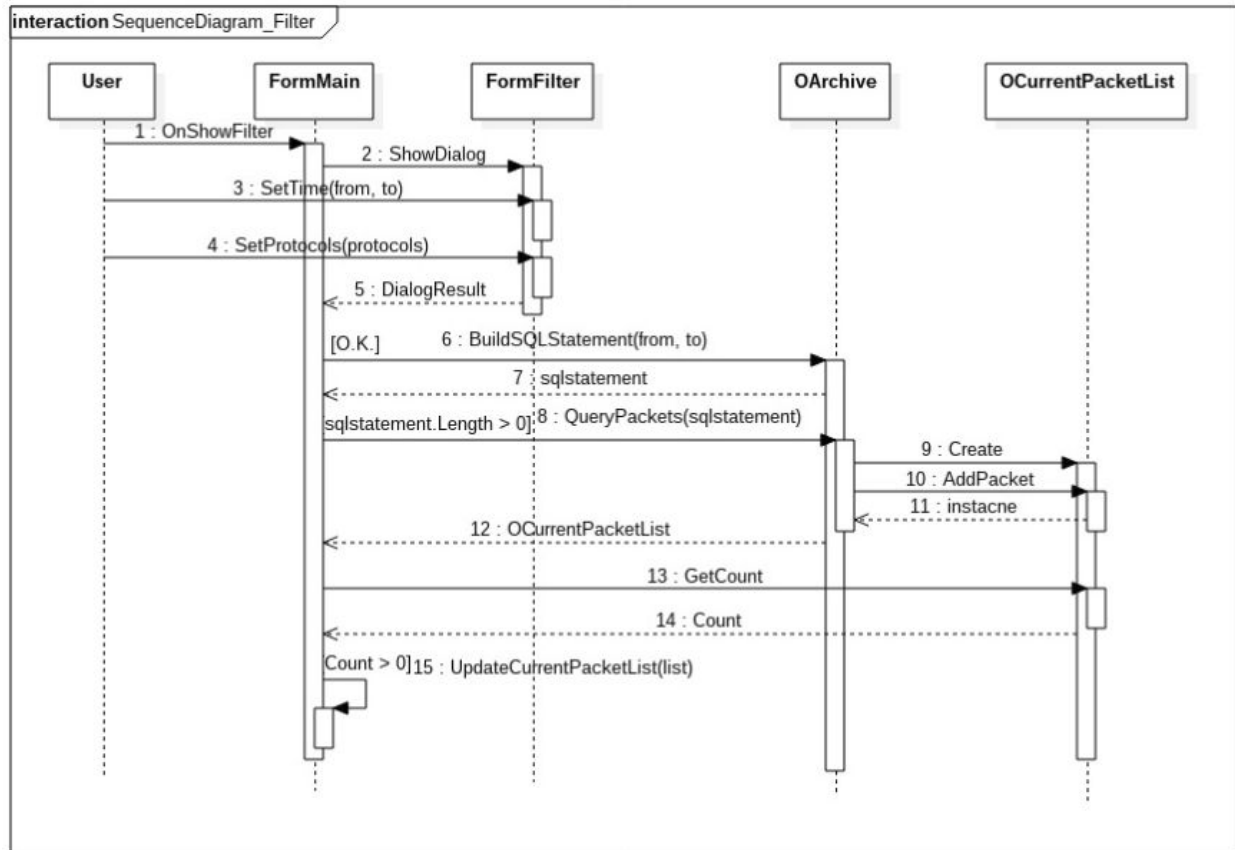+OnCaptureStopped(sender: object, status: CaptureStoppedStatus)
+GetCurrentInterface(): int

OArchiveFactory

+CreateArchive(type: int): OArchive

OArchive

+InitializeDB()
+BuildSQLStatement(from: Time, to: Time): Stirng
+QueryPackets(sqlstatement: String): OCurrentPacketList
+SavePacket(packet: OPacket)

OArchiveSQLite

+InitializeDB()

OArchiveMySQL

+InitializeDB()

FormMain

-_frmStatistics: FormStatistics
-_frmFilter: FormFilter
-_archive: OArchive
-_capture: OCapture

+OnStartCaputre()
+OnStopCapture()
+OnShowFilter()
+OnShowStatistics()
+AddPacketInView(packet: OPacket)
+UpdateCurrentPacketList(list: OCurrentPacketList)

FormStatistics

-_chart: MSChart

+SetPacketList(packetlist: OCurrentPacketList)
+ShowDialog()
+UpdateGraph(res: OStatisticsResult)
+UpdateGraph(type: int)
+SetGraphType(type: int)

FormFilter

-_from: Time
-_to: Time
-_protocols: int[]

+ShowDialog()
+SetTime(from: Time, to: Time)
+SetProtocols(protocols: int[])
+GetTimeFrom(): Time
+GetTimeTo(): Time
+GetProtocols(): int[]