

# **Wireshark програм хэрэглэгчдийн гарын авлагын**

Wireshark хувилбар 1.99

Nasantogtokh Amarsaikhan <nasantogtokh.am[AT]gmail.com>

Улаанбаатар хот

2015.11.12

*Wireshark* – Компьютерийн сүлжээгээр дамжиж буй өгөгдлийг цуглуулах, хадгалах, задлан шинжлэх үйл ажиллагаа хийдэг програм хангамж.

## **Агуулга**

ОРШИЛ.....	12
Өмнөх үг.....	12
Энэхүү гарын авлага хэнд зориулагдсан бэ?.....	12
БҮЛЭГ I.....	13
1. ВАЙРШАРК (WIRESHARK) ПРОГРАМЫН ТАНИЛЦУУЛГА.....	13
1.1. Вайршарк (Wireshark) гэж юу вэ?.....	14
1.1.1. Үүрэг зориулалт.....	14
1.1.2. Вайршарк (wireshark)-ын ажиллагааны онцлог.....	14
1.1.3. Олон төрлийн сүлжээний орчинд дамжиж буй сүлжээний өгөгдөл чагнах.....	15
1.1.4. Пакет (packet) өгөгдлүүдийг импорт хийж оруулах.....	15
1.1.5. Бусад програмд дэмжигдэхүйц файл болгон экспорт хийх.....	16
1.1.6. Протокол задалж уншигч.....	16
1.1.7. Нээлттэй эхийн програм.....	16
1.1.8. Вайршарк (wireshark) програм дараах зүйлсийг хийхгүй.....	16
1.2. Системийн үзүүлэлт.....	16
1.2.1. Майкрософт Виндовс (Microsoft Windows).....	17
1.2.2. Юникс болон Линукс (Unix/Linux).....	18
1.3. Вайршарк (Wireshark) програмыг хаанаас татаж авах вэ?.....	18
1.4. Вайршарк (Wireshark)-ын товч түүх.....	18
1.5. Вайршарк (wireshark) программын хөгжүүлэлт болон засан сайжруулалт.....	19
1.6. Алдаа мэдээллэх, туслалцаа авах.....	19
1.6.1. Вебсайт.....	19
1.6.2. Вики хуудас.....	20
1.6.3. Асуулт хариултын сайт.....	20
1.6.4. Түгээмэл асуугддаг асуултууд FAQ.....	20
1.6.5. Мэйлийн жагсаалт (mailing lists).....	20
1.6.6. Асуудал тулгарсан гэдгээ тайлагнах, мэдээллэх.....	21
1.6.7. Линукс/Юникс (Linux/Unix) платформ дээр эвдрэл мэдээллэх.....	21
1.6.8. Виндовс (Windows) платформ дээр эвдрэл мэдээллэх.....	22
БҮЛЭГ II.....	23
2. ВАЙРШАРК (WIRESHARK) ПРОГРАМЫГ СУУЛГАХ.....	23

2.1.	Танилцуулга.....	24
2.2.	Эх код (source) болон бинари тархацуудыш (binary distributions)-ыг татаж авах.....	24
2.3.	Виндовс (Windows) орчинд Вайршарк (wireshark) суулгах.....	24
2.3.1.	Суулгацын бүрэлдэхүүн хэсгүүд.....	25
2.3.2.	Нэмэлт сонголтууд.....	26
2.3.3.	Суулгах байрлал.....	26
2.3.4.	WinPcap суулгах.....	26
2.3.5.	Windows installer –ын команд мөрийн сонголтууд.....	26
2.3.6.	WinPcap-ыг гар аргаар суулгах нь (вайршаркаас салангид байдлаар).....	27
2.3.7.	Вайршарк (wireshark)-г шинэчлэх (Update).....	27
2.3.8.	WinPcap програмыг шинэчлэх.....	27
2.3.9.	Вайршарк (wireshark) програмыг устгах.....	28
2.3.10.	WinPcap програмыг устгах.....	28
2.4.	Мак Θү Эс Х (Mac OS X) орчинд вайршарк (Wireshark) програм суулгах.....	28
2.5.	Юникс (Unix) орчинд вайршаркыг эх (source) кодоос тохируулан суулгах нь.....	28
2.6.	Юникс (Unix) орчинд бинари (binaries) ашиглан вайршарк (wireshark)-г суулгах нь.....	29
2.6.1.	Red Hat болон түүнтэй төстэй үйлдлийн систем дээр RPM-ийг ашиглан суулгах нь	29
2.6.2.	Debian, Ubuntu болон бусад Debian-aas салаалж гарсан үйлдлийн системүүдийн орчинд DEB-ийг ашиглан суулгах нь.....	30
2.6.3.	Gentoo Linux үйлдлийн системд portage-г ашиглан суулгах нь.....	30
2.6.4.	FreeBSD үйлдлийн системд package-г ашиглан суулгах нь.....	30
2.7.	Юникс орчинд суулгах үед үүссэн алдааг засах (Troubleshooting during the install on Unix)	
	30	
2.8.	Виндовс (Windows) орчинд эх код (source code)-оос нь вайршарк програмыг суулгах нь	31
	БҮЛЭГ III.....	32
3.	ХЭРЭГЛЭГЧИЙН ИНТЕРФЭЙС.....	32
3.1.	Танилцуулга.....	33
3.2.	Вайршарк (wireshark) програмыг ачааллах (эхлүүлэх).....	33
3.3.	Үндсэн цонх (Main window).....	33
3.3.1.	Үндсэн цонхыг ашиглах нь.....	35
3.4.	Цэс (Menu).....	36
3.5.	File цэс.....	37

3.6.	Edit цэс.....	40
3.7.	View цэс.....	42
3.8.	Go цэс.....	45
3.9.	Capture цэс.....	46
3.10.	Analyze цэс.....	47
3.11.	Statistics цэс.....	49
3.12.	Telephony цэс.....	52
3.13.	Tools цэс.....	53
3.14.	Internals цэс.....	53
3.15.	Help цэс.....	54
3.16.	Үндсэн товчлуурууд (Main Toolbar).....	55
3.17.	Шүүлтүүрийн товчлуур (Filter toolbar).....	57
3.18.	Пакетыг жагсаан харуулах самбар (Packet list pane).....	59
3.19.	Пакетын дэлгэрэнгүй мэдээллийг харуулах самбар (Packet Details pane).....	60
3.20.	Пакетын мэдээллийг байтаар харах самбар (Packet Bytes pane).....	61
3.21.	Статусбар (Statusbar).....	62
	<b>БҮЛЭГ IV.....</b>	<b>64</b>
4.	<b>СУЛЖЭЭН ДЭЭГҮҮР ДАМЖИЖ БҮЙ ӨГӨГДЛИЙГ ШУУД ЧАГНАХ.....</b>	<b>64</b>
4.1.	Танилцуулга.....	65
4.2.	Урьдач нөхцөл (Prerequisite).....	65
4.3.	Чагнах функцийг эхлүүлэх.....	65
4.4.	Интерфэйсүүд чагнах (Capture Interfaces).....	66
4.5.	Чагнах сонголтууд (Capture Options).....	68
4.5.1.	Чагнах фрэйм (Capture frame).....	69
4.5.2.	Файл чагнах фрэйм (Capture File(s) frame).....	71
4.5.3.	Чагнах процессийг зогсоох фрэйм (Stop Capture ... frame).....	72
4.5.4.	Дэлгэцэнд харуулах сонголтуудын фрэйм (Display Options frame).....	72
4.5.5.	Нэрийн хөрвүүлэлтийн фрэйм (Name Resolution frame).....	73
4.5.6.	Товчлуурууд (Buttons).....	73
4.6.	Интерфэйсийн тохиргоог засварлах цонх (Edit Interface Settings).....	73
4.7.	Хөрвүүлэлтийн үр дүн цонх (Compile Results dialog box).....	77
4.8.	Шинэ Интерфэйс нэмэх (Add New Interfaces).....	77

4.8.1.	Шинэ хоолой (rīpe) нэмэх эсвэл устгах (Add or remove pipeps).....	78
4.8.2.	Локал интерфэйсүүдийг нэмэх эсвэл нуух (Add or hide local interfaces).....	79
4.8.3.	Алсын зайд байгаа интерфэйсийг нэмэх эсвэл нуух.....	80
4.9.	Алсын зайны интерфэйсийг чагнах (Remote Capture Interfaces).....	80
4.9.1.	Алсын зайнаас чагнах интерфэйсүүд (Remote Capture Interfaces).....	81
4.9.2.	Алсын зайнаас чагнах үйлдлийн тохиргоо (Remote Capture Settings).....	82
4.10.	Интерфэйсийн дэлгэрэнгүй (Interface Details).....	84
4.11.	Чагнасан файлууд болон файлын горимууд (Capture files and file modes).....	85
4.12.	Линк түвшний толгойн төрөл (Link-layer header type).....	87
4.13.	Чагнаж байх үедээ шүүлтүүр ашиглах (Filtering while capturing).....	87
4.13.1.	Алсын зай дахь урсгалын автомат шүүлтүүр (Automatic Remote Traffic Filtering)....	90
4.14.	Чагнах процесс ажиллаж байх үед (While capture is running).....	90
4.14.1.	Чагнах процесийг зогсоох.....	92
4.14.2.	Чагнах процесийг дахин эхлүүлэх.....	92
	<b>БҮЛЭГ V.....</b>	<b>93</b>
5.	<b>ФАЙЛЫН ОРОЛТ, ГАРАЛТ, ХЭВЛЭХ ҮЙЛДЭЛ.....</b>	<b>93</b>
5.1.	Танилцуулга.....	94
5.2.	Чагнасан файлыг нээх (Open capture files).....	94
5.2.1.	Чагнасан файл нээх (Open Capture File).....	94
5.2.2.	Оролтын файлын форматууд (Input File Formats).....	97
5.3.	Цуглувансан пакет өгөгдлийг хадгалах (Saving captured packets).....	99
5.3.1.	Цуглувансан файлыг хадгалах (Save Capture File As) цонх.....	99
5.3.2.	Гаралтын файлын форматууд (Output File Formats).....	102
5.4.	Цуглувансан файлуудыг нэгтгэх (Merging capture files).....	103
5.4.1.	“Чагнах файл нэгтгэх (Merge with Capture File)”.....	103
5.5.	Хекс өгөгдөл импорт хийж оруулах (Import hex dump).....	105
5.5.1.	Хекс өгөгдлөөс импорт хийх цонх (Import from Hex Dump).....	106
5.6.	Файлын багц (File sets).....	109
5.6.1.	Файлын жагсаалт (List Files) цонх.....	110
5.7.	Файл экспорт хийх.....	111
5.7.1.	Текст файл хэлбэрээр экспорт хийх (Export as Plain Text File).....	111
5.7.2.	ПостСкрипт файлаар экспорт хийх (Export as PostScript File) цонх.....	113

5.7.3.	CSV файлаар экспорт хийх (Export as Comma separated Values File) цонх.....	113
5.7.4.	Си массив файлаар (пакетын байт мэдээлэл) экспорт хийх цонх (Export as C arrays file)	114
5.7.5.	PSML файл руу экспорт хийх цонх (Export as PSML File).....	114
5.7.6.	PDML файл руу экспорт хийх цонх (Export as PDML File).....	115
5.7.7.	Пакетын идэвхижсэн байтуудыг экспорт хийх цонх (Export selected packet bytes)..	116
5.7.8.	Объектуудыг экспорт хийх цонх (Export Objects).....	117
5.8.	Пакет хэвлэх (Printing packets).....	118
5.8.1.	The “Print” dialog box.....	118
5.9.	Пакетын завсрал фрэйм (Packet Range frame).....	120
5.10.	Пакетын формат фрэйм (Packet Format frame).....	121
	<b>БҮЛЭГ VI.....</b>	<b>123</b>
6.	<b>ЧАГНАСАН ФАЙЛТАЙ АЖИЛЛАХ.....</b>	<b>123</b>
6.1.	Чагнаж цуглуулсан пакетуудаа харах (viewing packets you have captured).....	124
6.2.	Дэлгэгдэн гарч ирдэг цэс (Pop up menu).....	125
6.2.1.	Пакетыг жагсаан харуулах хэсгийн баганы толгой дээр гарч ирэх цэс (Pop-up menu of the Packet List column header).....	126
6.2.2.	Пакетыг жагсаан харуулах самбарын хэсэгт гарч ирэх цэс (Pop-up menu of the Packet List pane).....	127
6.2.3.	Пакетын мэдээллийг дэлгэрэнгүй үзүүлэх самбарт гарч ирэх цэс (Pop-up menu of the Packet Details pane).....	129
6.3.	Пакет үзэх үйлдэл хийх үедээ пакетуудад шүүлтүүр хийх (Filtering packets while viewing)	132
6.4.	Дэлгэцийн шүүлтүүрийн илэрхийллийг үүсгэх (Building display filter expressions).....	134
6.4.1.	Дэлгэцийн шүүлтүүрийн талбарууд (Display filter fields).....	134
6.4.2.	Утгуудыг харьцуулах (Comparing values).....	135
6.4.3.	Илэрхийлгүүдийг хослуулан хамтад нь хэрэглэх (Combining expressions).....	136
6.4.4.	Нийтлэг алдаа (A common mistake).....	137
6.5.	Шүүлтүүрийн илэрхийлэл цонх (The Filter Expression).....	138
6.6.	Шүүлтүүрийг үүсгэж, хадгалах (Defining and saving filters).....	140
6.7.	Шүүлтүүрийн макро тодорхойлох, хадгалах (Defining and saving filter macros).....	142
6.8.	Пакет хайж олох (Finding packets).....	142
6.8.1.	Пакет хайх цонх (Find Packet).....	143

6.8.2.	Дараагийнхийг хайх комманд (Find Next).....	144
6.8.3.	Өмнөхийг хайх комманд (Find Previous).....	144
6.9.	Тодорхой нэг пакет дээр очих (Go to a specific packet).....	144
6.9.1.	Буцаж очих комманд (Go Back).....	144
6.9.2.	Урагшилах комманд (Go Forward).....	144
6.9.3.	Пакет руу очих цонх (Go to Packet).....	144
6.9.4.	Харгалзан тохирч буй пакет руу очих комманд (Go to Corresponding Packet).....	145
6.9.5.	Эхний пакет руу шилжих комманд (Go to First Packet).....	145
6.9.6.	Сүүлийн пакет руу шилжих комманд (Go to Last Packet).....	145
6.10.	Пакетыг тэмдэглэх (Marking packets).....	145
6.11.	Пакетыг үл ойшоор (Ignoring packets).....	145
6.12.	Цаг харуулах форман мөн цагийн тэмдэглэгээ (Time display formats and time references)	
	146	
6.12.1.	Пакетын цагийн лавлагаа (Packet time referencing).....	147
БҮЛЭГ VII.....		149
АХИСАН ТҮВШНИЙ СЭДЭВ.....		149
7.1.	Танилцуулга.....	150
7.2.	TCP урсгал дагах (Following TCP streams).....	150
7.2.1.	TCP урсгал дагах цонх (Follow TCP Stream dialog box).....	151
7.3.	Эксперт мэдээлэл (Expert Information).....	152
7.3.1.	Эксперт мэдээллийн талбарууд (Expert Info Entries).....	153
7.3.2.	Эксперт мэдээлэл цонх (Expert Info dialog).....	154
7.3.3.	Өнгөөр ялгагдсан протоколын мэдээллийг дэлгэрэнгүй харуулах мод хэлбэрийн бүтэц (Colorized Protocol Details Tree).....	155
7.3.4.	Пакетыг жагсаан харуулах хэсэгт дэх Эксперт багана (Expert Packet List Column (optional)).....	156
7.4.	Цагийн тамга (Time Stamps).....	156
7.4.1.	Вайршарк интернал (Wireshark internals).....	157
7.4.2.	Цуглувансан файлын форматууд (Capture file formats).....	157
7.4.3.	Нарийвчлал (Accuracy).....	158
7.5.	Цагийн бүс (Time Zones).....	158
7.5.1.	Компьютерийн цагийг зөв тохируулах хэрэгтэй (Set your computer's time correctly)	
	158	

7.5.2.	Вайршарк програм болон цагийн бүс (Wireshark and Time Zones).....	158
7.6.	Пакет нэгтгэн угсрах (Packet Reassembly).....	160
7.6.1.	Пакет нэгтгэн угсрах гэж юу вэ? (What is reassemble).....	160
7.6.2.	Вайршарк програм үүнийг хэрхэн зохицуулдаг вэ? (How Wireshark handles it).....	160
7.7.	Нэрийн хөрвүүлэлт (Name Resolution).....	162
7.7.1.	Нэрийн хөрвүүлэлтийн сүл тал (Name Resolution drawbacks).....	162
7.7.2.	Этернэт нэрийн хөрвүүлэлт (Ethernet name resolution (MAC layer)).....	162
7.7.3.	IP нэрийн хөрвүүэллт (IP name resolution (network layer)).....	163
7.7.4.	TCP/UDP порт нэрийн хөрвүүлэлт (TCP/UDP port name resolution (transport layer))	164
7.8.	Шалгах нийлбэр (Checksums).....	164
7.8.1.	Вайршарк шалгах нийлбэрийн шалгах (Wireshark checksum validation).....	165
7.8.2.	Шалгах нийлбэрийг оффлоадинг хийх (Checksum offloading).....	165
	<b>БҮЛЭГ VIII.....</b>	<b>167</b>
8.	<b>СТАТИСТИКУУД.....</b>	<b>167</b>
8.1.	Танилцуулга.....	168
8.2.	Товч дүгнэлтийн цонх (The Summary window).....	168
8.3.	Протоколын шаталсан бүтэц цонх (Protocol Hierarchy window).....	170
8.4.	Харилцан мэдээлэл солилцоо (Conversations).....	171
8.4.1.	Харилцан мэдээлэл солилцооны цонх (Conversations)” window.....	171
8.5.	Төгсгөлийн цэгүүд (Endpoints).....	173
8.5.1.	Төгсгөлийн цэгүүд цонх (Endpoints window).....	174
8.6.	IO график цонх (IO Graphs window).....	175
8.7.	Сервисийн хариулах цаг (Service Response Time).....	176
8.7.1.	DCE-RPC сервисийн хариулах цаг цонх (Service Response Time DCE-RPC window)	
	177	
8.8.	Хоёр пакет файл харьцуулах.....	178
8.9.	WLAN Траффикин статистик.....	180
8.10.	Тодорхой протоколын статистик цонх.....	181
	<b>БҮЛЭГ IX.....</b>	<b>183</b>
9.	<b>УТСАН ХАРИЛЦАА.....</b>	<b>183</b>
9.1.	Танилцуулга.....	184
9.2.	RTP Анализ.....	184

9.3.	VoIP Дуудлага.....	186
9.4.	LTE MAC Траффикин статистик.....	186
9.5.	LTE RLC Траффикин статистик.....	187
9.6.	Тодорхой зааж өгсөн протоколын статистикин цонх.....	189
	<b>БҮЛЭГ Х.....</b>	<b>190</b>
10.	<b>ВАЙРШАРК ПРОГРАМЫГ ӨӨРТӨӨ ТОХИРУУЛАН ӨӨРЧЛӨХ.....</b>	<b>190</b>
10.1.	Танилцуулга.....	191
10.2.	Вайршарк програмыг команд мөрөөс эхлүүлэх.....	191
10.3.	Пакет өнгөр ялгах.....	201
10.4.	Протоколын задаргааг удирдах.....	204
10.4.1.	Идэвхижүүлсэн Протоколууд цонх (Enabled Protocols).....	205
10.4.2.	Хэрэглэгчийн тодорхойлж өгсөн задаргаа (User Specified Decodes).....	207
10.4.3.	Хэрэглэгчийн тодорхойлж өгсөн задаргааг харах (Show User Specified Decodes)....	208
10.5.	Тохиргоо (Preferences).....	208
10.5.1.	Интерфэйсийн сонголтууд (Interface Options).....	209
10.6.	Профайл тохируулах (Configuration Profiles).....	210
10.7.	Хэрэглэгчийн хүснэгт (User Table).....	213
10.8.	Дэлгэцийн шүүлтүүрийн макро (Display Filter Macros).....	213
10.9.	ESS Категори Атрибут (ESS Category Attributes).....	214
10.10.	GeoIP өгөгдлийн баазын зам (GeoIP Database Paths).....	214
10.11.	IKEv2 декрипт хүснэгт (IKEv2 decryption table).....	214
10.12.	Объект ялгагч (Object Identifiers).....	216
10.13.	PRES Users Context List.....	216
10.14.	SCCP хэрэглэгчийн хүснэгт (SCCP users Table).....	217
10.15.	SMI (MIB болон PIB) модулууд (SMI (MIB and PIB) Modules).....	217
10.16.	SMI (MIB болон PIB) зам (SMI (MIB and PIB) Paths).....	217
10.17.	SNMP Enterprise Specific Trap Types.....	218
10.18.	SNMP хэрэглэгчийн хүснэгт (SNMP users Table).....	218
10.19.	Tektronix K12xx/15 RF5протоколын хүснэгт (Tektronix K12xx/15 RF5 protocols Table) 219	
10.20.	Хэрэглэгчийн DLT протоколын хүснэгт (User DLTs protocol table).....	219
	<b>Appendix A. Wireshark Messages.....</b>	<b>221</b>

A.1. Packet List Messages.....	221
A.1.1. [Malformed Packet].....	221
A.1.2. [Packet size limited during capture].....	221
A.2. Packet Details Messages.....	221
A.2.1. [Response in frame: 123].....	221
A.2.2. [Request in frame: 123].....	221
A.2.3. [Time from request: 0.123 seconds].....	221
A.2.4. [Stream setup by PROTOCOL (frame 123)].....	222
Appendix B. Files and Folders.....	222
B.1. Capture Files.....	222
B.1.1. Libpcap File Contents.....	223
B.1.2. Not Saved in the Capture File.....	223
B.2. Configuration Files and Folders.....	223
B.2.1. Protocol help configuration.....	230
B.3. Windows folders.....	232
B.3.1. Windows profiles.....	232
B.3.2. Windows roaming profiles.....	233
B.3.3. Windows temporary folder.....	233
Appendix C. Protocols and Protocol Fields.....	234
Appendix D. Related command line tools.....	235
D.1. Introduction.....	235
D.2. tshark: Terminal-based Wireshark.....	235
D.3. tcpdump: Capturing with tcpdump for viewing with Wireshark.....	238
D.4. dumpcap: Capturing with dumpcap for viewing with Wireshark.....	238
D.5. capinfos: Print information about capture files.....	240
D.6. rawshark: Dump and analyze network traffic.....	241
D.7. editcap: Edit capture files.....	242
D.8. mergecap: Merging multiple capture files into one.....	249
D.9. text2pcap: Converting ASCII hexdumps to network captures.....	250
D.10. reordercap: Reorder a capture file.....	254

## ОРШИЛ

### Өмнөх үг

Өнөө үед бидний өдөр тутмын амьдралыг интернэтийн сүлжээнд холбогдсон төхөөрөмжгүйгээр төсөөлөгдөхийн аргагүй болоод байна. Интернэтийн сүлжээг хэрэглэгчдийн тоо, интернэт дээгүүр дамжигдаж буй мэдээллийн хэмжээ өдрөөс өдөрт өсөн нэмэгдсээр байгаа нь өнөө үеийн залуус биднийг интернэт орчны мэдлэг, чадвартай байхыг шууд бусаар шаардах болсон байна. Тийм ч учраас компьютерийн шинжлэх ухаан, компьютерийн сүлжээг сонирхон судлах залуусын тоо эрс өсөж байгаа нь сайшаалтай юм.

Компьютерийн шинжлэх ухааныг судлах залуусын тоо хэдий нэмэгдэж байгаа ч гэсэн эдгээр залууст хэрэгтэй сайн гарын авлага, сурах материал нь Монгол хэл дээр төдийлөн олддоггүй асуудал одоо ч гэсэн байсаар л байна. Энэ нь компьютерт сонирхолтой залуусын сурах процесийг удаашруулах шалтгаан болж байгаа нь илт харагдаж байна.

Тийм учраас wireshark програмыг хэрэглэж буй Монгол залуусд тус нэмэр болох үүднээс энэхүү гарын авлагыг боловсруулан гаргаж байна.

### Энэхүү гарын авлага хэнд зориулагдсан бэ?

Энэ гарын авлагын агуулгад wireshark програмыг интернэтээс татах авах, install хийж суулгах, мөн суулгасны дараа хэрхэн ашиглах талаар аль болох өргөн хүрээний мэдээллийг хамруулахыг хичээллээ. Та компьютерийн сүлжээг анхлан суралцагч уу эсвэл системийн админ уу гэдгээс үл хамааран хэрэгтэй мэдээллээ олно гэдэгт итгэлтэй байна. Хэдийгээр энэхүү гарын авлагыг системийн админ, сүлжээний админы хэрэглээнд нийцэхүйц байлгахыг хичээсэн боловч Wireshark програм нь өөрөө их том хэмжээтэй нээлттэй эхийн програм хангамж учраас зарим нэгэн агуулгыг хамарч чадалгүй орхигдуулсан боломжтой юм..

Энэхүү гарын авлагад компьютерийн сүлжээгээр дамжиж буй packet өгөгдлийг хэрхэн анализ талаар ерөнхийд нь тайлбарласан болно.

*Сүлжээний протоколын талаар тайлбарыг энэ гарын авлага агуулаагүй.*

Энд дурдагдсан агуулгын хүрээнд илүү дэлгэргүүлэн судлахыг хүсвэл <http://wiki.wireshark.org/> веб хуудас руу хандах орно уу.

## **БҮЛЭГ I.**

### **1. ВАЙРШАРК (WIRESHARK) ПРОГРАМЫН ТАНИЛЦУУЛГА**

## **1.1. Вайршарк (Wireshark) гэж юу вэ?**

Вайршарк (wireshark) нь сүлжээний пакет (packet)-д дүн шинжилгээ хийх зориулалт бүхий програм юм. Сүлжээний пакет (packet)-д дүн шинжилгээ хийхдээ энэхүү програм нь сүлжээн дээгүүр дамжигдаж буй пакет (packet)-уудыг чагнаж, цуглуулаад тэдгээр пакет өгөгдөл (packet data)-ийг боломжит хамгийн дэлгэрэнгүй байдлаар задлан харуулдаг.

Сүлжээний пакет анализар (packet analyzer) нь сүлжээний кабел дээгүүр дамжигдаж буй дээд түвшинд харуулах, хэмжих зориулалттай багаж мэтээр ойлгогдож болно.

Хөгжлийнхөө эхэн үед ийм төрлийн програм хангамж нь маш үнэтэй эсвэл оюуны өмчөөр хамгаалагдсан байдаг байсан юм. Гэвч вайршарк (wireshark) програм нь нээлттэй эхийн програм хэлбэрээр хөгжиж эхэлсэн үеэс энэхүү байдал өөрчлөгдсөн. Түүнчлэн вайршарк (wireshark) нь сүлжээний пакет анализар (packet analyzer) програмуудын дундаас шилдэг програмуудынх нь нэгд зүй ёсоор багтдаг юм.

### **1.1.1. Үүрэг зориулалт**

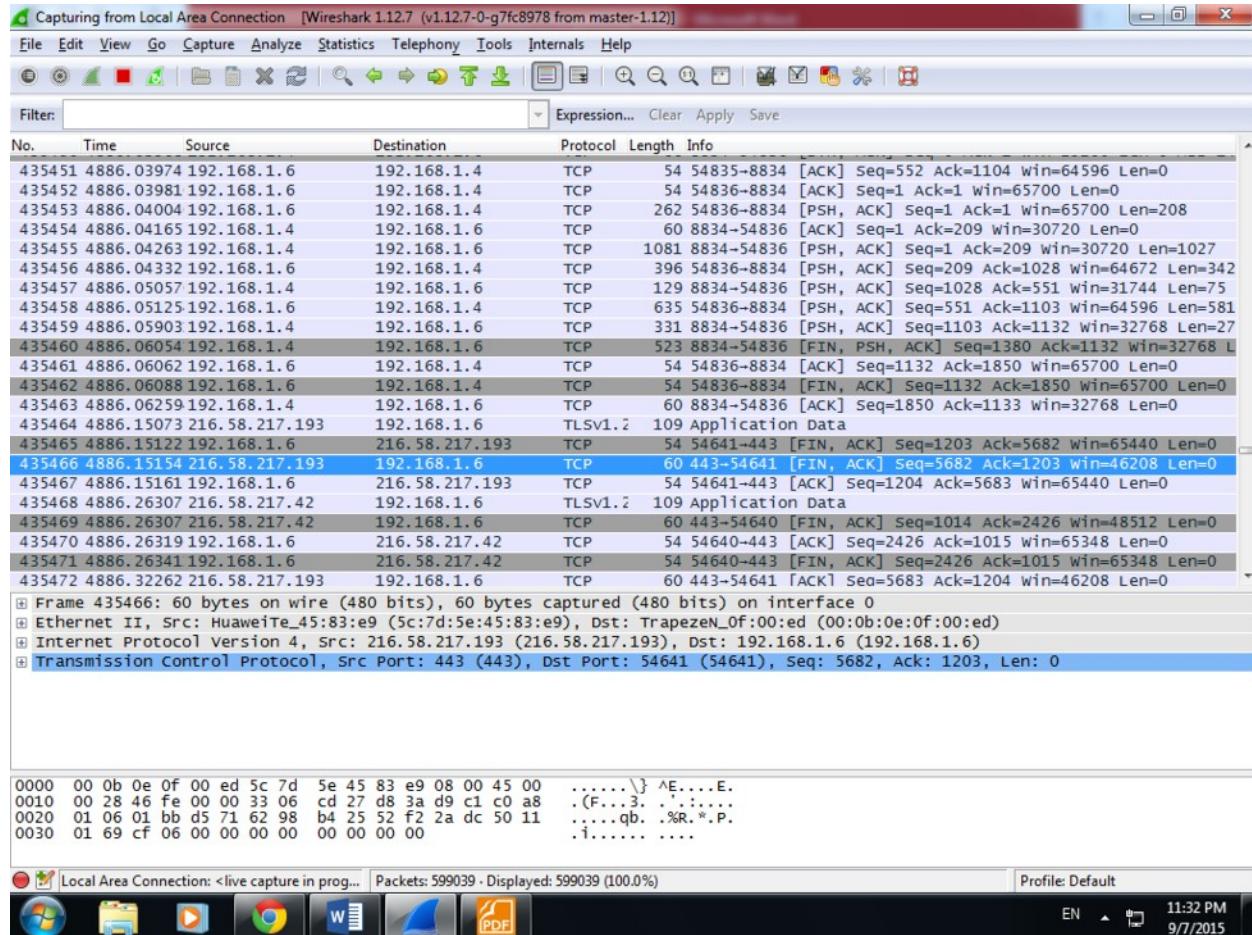
Вайршарк (wireshark) программын зарим түгээмэл хэрэглээг дурдлаа

- Сүлжээнд үүссэн асуудлыг оношлох, тодруулахад
- Сүлжээний аюулгүй байдалтай холбоотой асуудлыг хянах, илрүүлэхэд
- Хөгжүүлэгчид шинэ протокол хөгжүүлэх, хэрэгжүүлэх явцдаа шалгах зориулалтаар
- Компьютерийн сүлжээг хэрхэн ажилладаг талаар суралцаж буй хүмүүс сургалтын зориулалтаар гэх мэт.

### **1.1.2. Вайршарк (wireshark)-ын ажиллагааны онцлог**

- Windows болон Unix үйлдлийн системүүд дээр ажиллана.
- Сүлжээний интерфэйс картууд (Network Interface Card - NIC) дээгүүр дамжигдаж буй packet өгөгдлийг чагнана (capture), цуглуулж авна.
- Вайршарк (Wireshark) програмтай ижил үйлдэл хийдэг tcpdump/WinDump гэх мэт сүлжээний өгөгдөлд анализ хийх програмуудын цуглуулсан packet өгөгдлүүдийг нээнэ, анализ хийнэ.
- Пакет (Packet) өгөгдлийн 16тын тооллын системээр илэрхийлэгдсэн (hex) файлаас вайршарк (wireshark) програм руу импорт хийнэ.
- Пакет (Packet) өгөгдлийг ашиглагдаж буй протоколоор нь дэлгэрэнгүйгээр харуулна.
- Цуглуулж авсан пакет (packet) өгөгдлийг хадгална.
- Цуглуулсан пакет (packet) өгөгдлөө хэсэгчлэн эсвэл бүтнээр нь олон төрлийн файлын төрлийн (file format) сонголттойгоор экспорт хийнэ
- Олон төрлийн шалгуур үзүүлэлт, параметр ашиглан пакет (packet) өгөгдлөөс шүүлт (filter) хийнэ.
- Олон төрлийн шалгуур үзүүлэлт, параметр ашиглан пакт (packet) өгөгдлөөс хайлт хийнэ.

- Шүүлтүүр (filter) хийсэн пакет (packet) өгөгдлийн үр дүнг өнгөөр ялгаж харуулна.
- Төрөл бүрийн статистик үзүүлэлтүүдийг автоматаар үүсгэнэ гэх мэт олон үйлдлүүдийг нэг доор хийх боломжтой.



Зураг 1.1. Вайршарк (Wireshark) програм сүлжээгээр дамжигдаж буй пакет (packet) өгөгдлийггээ дэлгэцэнд харуулж буй байдал.

### 1.1.3. Олон төрлийн сүлжээний орчинд дамжиж буй сүлжээний өгөгдөл чагнах

Вайршарк (Wireshark) програм нь маш олон төрлийн сүлжээний орчинг дэмжин ажилладаг. Гэхдээ вайршарк (Wireshark) програм ямар ямар сүлжээний орчин дэмжин ажиллах нөхцөл нь та ямар үйлдлийн систем ашиглан вайршарк (wireshark) программыг ажиллуулж буйгаас хамаардаг. Тиймээс таны ашиглаж буй үйлдлийн систем дээр вайршарк (wireshark) програм ямар ямар сүлжээний орчинг дэмжин ажиллах эсэхийг нь харахыг хүсвэл <https://wiki.wireshark.org/CaptureSetup/NetworkMedia> веб хуудас руу хандах орно уу.

### 1.1.4. Пакет (packet) өгөгдлүүдийг импорт хийж оруулах

Сүлжээн дээр дамжиж буй өгөгдөл чагнаж цуглуулах зориулалт бүхий бусад програм ашиглан цуглуулсан файлыг Вайршарк (Wireshark) програмруу импорт хийж оруулах

боломжтой. Энэ талаар дэлгэрэнгүйгээр **5.2.2 “Оролтын файлын хэлбэрүүд (Input File Formats)**” хэсгээс харах боломжтой.

#### **1.1.5. Бусад програмд дэмжигдэхүйц файл болгон экспорт хийх**

Вайршарк (Wireshark) програм нь сүлжээний орчноос чагнан, цуглуулж авсан пакет (packet) өгөгдлүүдээ төрөл бүрийн файлын төрөл (file format)-р хадгалах боломжийг олгодог. Ямар төрлийн өгөгдлийн төрөл (file format)-р экспорт хийх боломжтойг **5.3.2 “Гаралтын файлын төрлүүд (Output file formats)**” хэсгээс харах боломжтой.

#### **1.1.6. Протокол задалж уншигч**

Вайршарк (Wireshark) програм төрөл бүрийн сүлжээний протоколуудыг бүтцийнх нь дагуу бүрэлдэхүүн хэсэг бүрээр нь задалж харуулдаг. Дэлгэрэнгүйг **Хавсралт С “Протокол, протоколын талбарууд”**-хэсгээс үзнэ үү.

#### **1.1.7. Нээлттэй эхийн програм**

Вайршарк (Wireshark) програм нь (GNU General Public License - GPL) нээлттэй эхийн програм хангамж юм. Тиймээс вайршарк (wireshark) программыг ашиглахдаа ямар нэгэн төлбөр, лиценз гэх мэт зүйлсэд санаа зовохгүй хэрэглэж болно. Түүнчлэн нээлттэй эхийн програм хангамж учраас вайршарк (wireshark) програмд шинээр протокол нэмж оруулах (залгаас хэлбэрээр /plug-in/ эсвэл үндсэн бүрэлдэхүүнд нь /built-in/) процесс хурдан шуурхай хийгддэг, хэрэв хүсвэл та ч гэсэн вайршарк (wireshark) программыг хөгжүүлж болно.

#### **1.1.8. Вайршарк (wireshark) програм дараах зүйлсийг хийхгүй.**

- Халдлага илрүүлэхгүй – Сүлжээн дээгүүр сэжигтэй, эсвэл илтэд харагдах халдлагын мэдээлэл дамжигдаж байгааг вайршарк (wireshark) програм танихгүй. Мөн хэрэглэгчид ямар нэгэн анхааруулга өгөх чадваргүй. Хэрэглэгч өөрөө л эдгээр сэжигтэй пакет (packet) өгөгдлүүдийг хянах, анализ хийх үйлдлээ гар аргаар хийнэ. Энэ процессд вайршарк (wireshark) програм сүлжээний өгөгдлийг маш дэлгэрэнгүй задалж харуулах тул таны ажил маш ихээр хөнгөвчлөгднө.
- Вайршарк (Wireshark) програм нь пакет (packet) өгөгдөл үүсгэхгүй мөн сүлжээгээр ямар нэгэн өгөгдөл дамжуулдаггүй. Сүлжээ рүү чиглэсэн ямар нэгэн идэвхитэй үйлдлийг хийдэггүй.

### **1.2. Системийн үзүүлэлт**

Вайршарк (Wireshark) программыг суулгаж ажиллуулахад ямар үзүүлэлттэй систем шаардлагдах вэ гэдэг нөхцөл нь сүлжээний ачааллаас хамаарна. Доор үзүүлсэн системийн өрөнхий шаардлага нь хэдэн зуун MB-аар хэмжигдэх дунд зэргийн файл анализ хийхэд хангалттай үзүүлэлт юм. Илүү том хэмжээтэй пакет (packet) өгөгдөл дээр ажиллах шаардлагатай бол танд илүү их хэмжээний шуурхай санах ой (RAM) болон хатуу дискний (hard disk storage) эзлэхүүн шаардлагатай болно.

Сүлжээний орчин ачаалал ихтэй байвал энэ сүлжээн дээгүүр дамжигдаж буй өгөгдөл их хэмжээтэй байна гэсэн үг.

Gbps эсвэл хэдэн зуун Mbps сүлжээний урсгал дээрх сүлжээний өгөгдлийг чагнах (capture), цуглуулах үйлдэл хийвэл богино хугацаанд хэдэн зуун MB хэмжээтэй файл үүсдэг. Им тохиолдолд илүү хурдтай процессор, илүү их санах ой (RAM) мөн хатуу дискний багтаамж (hard disk storage) хэрэгтэй болно.

Вайршарк (Wireshark) програмыг ашиглах үед санах ой хүрэлцэхгүй болвол (runs out of memory) вайршарк (wireshark) эвдэрч ажиллахаа болино. Үүнтэй холбоотой мэдээллийг <https://wiki.wireshark.org/KnownBugs/OutOfMemory> гэсэн хуудаснаас илүү дэлгэрүүлж үзэх боломжтой.

Вайршарк (Wireshark) програм пакет (packet) цуглуулах үйлдлийг хийхдээ олон процесс (multi thread) үүсгэж ажилладаг боловч сүлжээний интерфэйсийг чагнах процесс нь ганц процесс (single thread) дээр ажилладаг юм. Тиймээс таны ашиглаж буй компьютер олон цөмтэй систем байлаа ч гэсэн илүү хурдан ажиллахгүй зөхвөн олон цөмд хэрэглэгдэж буй нэг цөмийн хурдаар ажилладаг.

### 1.2.1. Майкрософт Виндовс (Microsoft Windows)

- Вайршарк (Wireshark) 1.12.7 хувилбар нь Виндовс (Windows)-ын бүх хувилбар дээр ажиллана.
- AMD64/x86-64 битийн процессор байх хэрэгтэй.
- Хамгийн багадаа 200 MB хэмжээтэй шуурхай санах ой (RAM) хэрэгтэй.
- Хамгийн багадаа 75 MB хэмжээтэй хатуу дискний багтаамж (HDD) хэрэгтэй.
- 1024x768 болон түүнээс дээш нягтаршилтай байх ба хамгийн багадаа 16 бит өнгө ялгах дэлгэц дээр бүрэн чадлаараа ажиллана. 8 битийн дэлгэц дээр ажиллах боломжтой хэдий ч бүрэн чадлаараа ажиллахгүй.
- Вайршарк (Wireshark) програм дэмжин ажиллах сүлжээний карт байх хэрэгтэй.
- Сүлжээг чагнах процесс дэмжин ажиллах сүлжээний картууд
  - Итернет (Ethernet): Виндовс (Windows) үйлдлийн систем дэмжиж байгаа сүлжээний картууд вайршарк (wireshark) програмтай хэвийн ажиллана.
  - 802.11 буюу утасгүй интернетийн сүлжээний картын хувьд **Wireshark wiki** хуудсыг үзнэ үү.

Виндовс (Windows)-оос хөгжүүлэлтийг нь зогсоосон хуучин хувилбарууд дээр вайршарк (wireshark) програмын шинэ хувилбарууд нь бүрэн хүчин чадлаараа ажиллахгүй байх магадлалтай.

### **1.2.2. Юникс болон Линукс (Unix/Linux)**

Вайршарк (Wireshark) програм нь ихэнх Юникс (Unix) платформ дээр ажиллана. Системийн шаардлага нь дээр дурдсан Виндовс (Windows) үйлдлийн системийн шаардлагатай ижил байна.

Вайршарк (Wireshark) **Binary Packages** нь дараах төрлийн платформууд дээр ажиллана.

- Apple Mac OS X
- Debian GNU/Linux
- FreeBSD
- Gentoo Linux
- HP-UX
- Mandriva Linux
- NetBSD
- OpenPKG
- Red Hat Enterprise/Fedora Linux
- Sun Solaris/i386
- Sun Solaris/SPARC
- Canonical Ubuntu

Хэрвээ таны системд тохирох **Binary Package** байхгүй бол та Эх код (Source Code) – ийг нь татан аваад **compile** хийх замаар **install** –даж суулгах боломжтой.

### **1.3. Вайршарк (Wireshark) програмыг хаанаас татаж авах вэ?**

<https://www.wireshark.org/download.html> веб хуудаснаас вайршарк (wireshark) программын хамгийн сүүлийн хувилбарыг татаж авах боломжтой. Татаж авах хуудас нь автоматаар таны үйлдлийн системийг таних ба тохирох файлыг танд хамгийн ойрын толин серверээс санал болгодог.

Вайршарк (wireshark) програм нь ихэвчлэн нэгээс хоёр сарын хугацаанд шинэчлэгддэг. Мөн та вайршарк (wireshark) программын шинэчлэлтэй холбоотой мэдээллийг цаг алдалгүй авч байхыг хүсвэл вайршарк (wireshark) программын мэйлийн жагсаалтад (mailing list) бүртгүүлэх хэрэгтэй.

### **1.4. Вайршарк (Wireshark)-ын товч түүх**

1997 онд Жералд Комбс сүлжээнд үүссэн асуудлыг хянах шаардлага үүссэн бөгөөд тэрээр өөрийн хэрэгцээг хангахын тулд Ethereal (анхны вайршарк) хэмээх программыг эхлүүлсэн.

Эхэндээ энэхүү программын хөгжүүлэлт нь удаан байсан бөгөөд 1998 оны 7 сар хүртэл хэд хэдэн удаа дундаа үйл ажиллагаагаа зогсоож байсан. Түүнээс хойши нөхөөс, алдаа зэргийг олон нийтээс мэдээллэж эхэлсний дараа амжилттай хэрэгжих замдаа орсон байна.

Үүний дараахан Гилберт Рамирез энэхүү төслийн ирээдүйн боломжийг олж харан доод түвшний задлан харуулах хэсэг дээр өөрийн хувь нэмрийг оруулсан.

1998 оны 10 сард Гай Харрис tcpview програмаас илүү дээр зүйл хайж байсан бөгөөд улмаар энэхүү төсөлд нөхөөс болон задалж харуулах хэсгүүд дээр өөрийн дэмжлэгийг үзүүлж эхэлсэн. 1998 оны сүүлээр TCP/IP-гийн хичээл орж байсан Ричард Шарпе энэхүү төслийн боломжийг өөрийн хичээлд ашиглах боломжийг олж харсан бөгөөд түүний хүсч буй протоколыг энэхүү програм дэмжиж байгаа эсэхийг хайж үзсэн. Гэтэл энэхүү програмд шинэ нөхөөс, задлагч хэсгүүд тийм ч хялбархан нэмэгдэх боломжгүй байсан юм. Тиймээс тэрээр нөхөөсүүд болон задлах хэсэг дээр өөрийн хувь нэмрийг оруулах болсон. Үүнээс хойш үүнийг дэмжин хөгжүүлэх хүмүүсийн тоо маш ихээр нэмэгдсэн. Эдгээр хүмүүс нь өөрт хэрэгтэй байгаа протоколыг задлах хэсэг дээр ажиллаж хөгжүүлж эхэлсэн.

2006 онд энэхүү байршилаа сольж вайршарк (wireshark) нэрээр гарах болсон.

2008 онд буюу хөгжүүлэлт эхэлснээс 10 жилийн дараа вайршарк (wireshark) 1.0 хувилбар гарсан. Энэ хувилбар нь хамгийн анхны бүрэн хувилбар байсан юм. Гэхдээ тухайн үед энэхүү хувилбарт маш цөөн тооны функцүүд ажиллаж байсан. Вайршарк (wireshark) программын энэхүү хувилбар гарах үед вайршарк хөгжүүлэгчдийн болон хэрэглэгчдийн анхны хурал болох Шаркфест (sharkfest) олж байсан.

### **1.5. Вайршарк (wireshark) программын хөгжүүлэлт болон засан сайжруулалт**

Вайршарк (Wireshark) программын хөгжүүлэлтийг Жералд Комбс эхлүүлсэн юм. Явцын дундын хөгжүүлэлт болон засвар үйлчилгээг вайршаркын баг хийдэг байсан. Энэхүү баг гэдэг нь шинэ функцийг хөгжүүлж алдааг засаж байсан хувь хүмүүс юм.

Вайршарк (wireshark) программын протокол задлагч функцүүдэд өөрийн хувь нэмрээ оруулж буй маш олон хүн байгаа бөгөөд цаашдаа ч энэ хүмүүсийн тоо улам нэмэгдэх хандлагатай байна. Эдгээр хүмүүсийн тухай мэдээллийг вайршарк (wireshark)-ыг веб хуудасны зохиогчид хэсгээс олж үзэх боломжтой.

Вайршарк (Wireshark) програм нь нээлттэй эхийн програм юм. Тийм учраас хэрэв таны хүссэн функц эсвэл протокол энэ програмд байхгүй байвал та өөрөө вайршарк (wireshark) програмд нэмж програмчилж өгч болно. Ингэснээр вайршарк (wireshark) программын дараа дараагийн хувилбаруудад таны нэмж оруулсан функц шинээр нэмэгдэх ба шинэчлэгдэж явах боломжтой.

### **1.6. Алдаа мэдээллэх, туслалцаа авах**

#### **1.6.1. Вебсайт**

Хамгийн эхэнд санал болгох зүйл нь вайршарк (wireshark)-ын веб хуудас юм. Энэ хуудаснаас шинэлэг үнэн зөв мэдээллийг авах боломжтой. <https://www.wireshark.org/>

### **1.6.2. Вики хуудас**

Вики хуудас нь <https://wiki.wireshark.org/> хаяг дээр байрлах бөгөөд эндээс та вайршарк (wireshark) програм мөн пакет (packet) чагнахтай холбоотой маш өргөн хүрээний мэдээллийг олж авна. Та энэхүү хуудаснаас гарын авлага дээрээс олж авч чадахааргүй мэдээллүүдийг ч олж авах болно. Жишээлбэл свитчэд сүлжээг хэрхэн чагнах талаарх тайлбар, протокол хөгжүүлж байгаа процесс гэх мэт.

Түүнээс гадна энэхүү хуудас дээрх сэдвүүд дээр таны сайн мэддэг сэдэв байвал та өөрийн энэхүү сэдэв дээр өөрийн хувь нэмрийг оруулах, мэдлэгээ бусдад түгээх боломжтой.

### **1.6.3. Асуулт хариултын сайт**

<https://ask.wireshark.org/> хаяг дээр байрлах асуулт хариултын сайт нь асуулт болон хариултыг хамтад нь олж болох газар юм. Та ямар асуулт асуугдсаныг болон түүнд хүмүүсийн өгсөн хариултыг хайж олох боломжтой. Хариултууд нь үнэлэгдэх боломжтой тиймээс та хамгийн сайн хариултыг нь олж хялбархан олж авах боломжтой. Хэрэв таны хайж буй асуулт асуугдаагүй байвал та өөрийн асуултыг асуух боломжтой.

### **1.6.4. Түгээмэл асуугддаг асуултууд FAQ**

Энэ нь маш түгээмэл тааралдах асуултуудыг нэгтгэн хариулттай нь санал болгодог. Тиймээс хэрэв ямар нэгэн асуудалтай холбоотойгоор мэйл илгээхээр шийдсэн бол мэйлээ илгээхээсээ өмнө түгээмэл асуугддаг асуултуудыг хянаж үзэх нь зүйтэй юм. Ингэснээр та өөрийн болон бусдын цагийг хэмнэж өгнө. Мэйл илгээж байгаа тохиолдолд та мэйлийн жагсаалт (mailing list)-д маш олон хүн бүртгүүлсэн байгаа гэдгийг тооцож үзэх хэрэгтэй. Өөрөөр хэлбэл маш их хугацаа зарцуулна гэсэн үг.

Түгээмэл асуугддаг асуултыг та Вайршарк (wireshark) програм дотроос Help/Content-г сонгож эндээс нээгдсэн цонх дээрээс FAQ хэсгийг сонгож нээх боломжтой.

Онлайн байдлаар FAQ асуулт хариулт нь <https://www.wireshark.org.faq.html> хаяг дээр байрлана. Онлайн хувилбар нь шинэчлэгдсэн байх магадлал ихтэй бөгөөд уншихад илүү хялбар байж болох юм. Тиймээс боломжтой бол онлайн хувилбарыг нь сонирхож үзэх нь зүйтэй юм.

### **1.6.5. Мэйлийн жагсаалт (mailing lists)**

Вайршаркын (wireshark) тодорхой сэдвүүдийн хүрээнд хэд хэдэн мэйлийн жагсаалтууд байдаг.

*Wireshark-announce* Энэ мэйлийн жагсаалт нь ихэвчлэн 4-8 долоо хоногийн хугацаатайгаар танд вайршарк (wireshark) програмын шинэ хувилбар гарч байгаа талаарх мэдээллийг өгнө.

*Wireshark-users* Энэ нь хэрэглэгчдийн мэйлийн жагсаалт юм. Хүмүүс вайршарк (wireshark)-г суулгах ашиглахтай холбоотой асуултаа асууж бусад нь

хариулах зарчмаар ажилладаг.

Энэ нь хөгжүүлэгчдийн мэйлийн жагсаалт. Та вайршаркийг хөгжүүлэх хүсэлтэй байгаа бол энэ жагсаалтад нэгдэх боломжтой.

<https://www.wireshark.org/lists/> хаяг руу хандаж та эдгээр мэйлийн жагсаалтад бүртгүүлэх боломжтой. Мэйлийн жагсаалтаас мэдээлэл хүлээн авахын тулд тухайн мэйлийн жагсаалттай хамаарах хэсэгт нь `Subscribe/Unsubscribe/Options` хэсгийг ашиглана. Энэ хуудас дээр мөн эдгээр мэйлийн жагсаалтийн архивуудыг үзэх холбоос байдаг. Архиваас та өөрийн хүссэн мэдээллээ цаг алдалгүй олох боломж мөн байгаа юм.

#### 1.6.6. Асуудал тулгарсан гэдгээ тайлагнах, мэдээллэх

Алдааны тухай мэдээлэл илгээхээсээ өмнө вайршарк (wireshark) програмын хамгийн сүүлийн хувилбарыг суулгасан эсэхээ хянаж үзэх хэрэгтэй.

Вайршарк (wireshark)-ын алдааг мэдээллэхдээ дараах мэдээллүүдийг хавсаргаж байх хэрэгтэй.

1. Вайршарк (wireshark)-ын хувилбар мөн түүнтэй хамааралтай сангүүд (dependent libraries) болох Qt эсвэл GLib зэргийн талаар мэдээлэл. Та эдгээр мэдээллийг Вайршарк (wireshark) програмын `about` хэсгээс эсвэл коммандын `Wireshark -v` гэсэн командыг бичиж өгч авах боломжтой.
2. Таны хэрэглэж буй платформ. Өөрөөр хэлбэл вайршарк (wireshark) програм ажиллаж буй платформ.
3. Танд үүссэн асуудлын талаар дэлгэрэнгүй тодорхойлолт
4. Хэрэв та алдаа эсвэл анхааруулах мессэж (error/warning message) хүлээн авсан бол энэ мессеж (мөн энэхүү мессежийн өмнөх болон дараагийн хэд хэдэн мөр) зэргийг явуулах хэрэгтэй.

Хэтэрхий том файл илгээх нь зохимжгүй юм. Ихэвчлэн 500KB-аас бага хэмжээний файл илгээх нь зохистой бөгөөд танд туслах гэсэн хүн илүү дэлгэрэнгүй мэдээлэл хүсвэл илүү том файл явуулах хэрэгтэй юм.

Мөн нууцлалтай холбоотой мэдээлэл илгээж байгаа эсэхээ хянаж үзээрэй. Хэрэв сүлжээнээс чагнасан пакет (packet) өгөгдөл илгээх бол энэхүү өгөгдөл дунд тань нууцлалтай холбоотой мэдээлэл байгаа эсэхийг хянах хэрэгтэй.

#### 1.6.7. Линукс/Юникс (Linux/Unix) платформ дээр эвдрэл мэдээллэх

Вайршарк (wireshark)-тай холбоотой эвдрэл мэдээллэхдээ буцааж хөөх мэдээллийг (traceback) илгээх нь зүйтэй юм.

Юникс/Линукс (Unix/Linux) үйлдлийн систем дээр та буцаан хөөх (traceback) мэдээллийг гарган авахдаа дараах командыг ашиглана.

```
$ gdb `whereis wireshark | cut -f2 -d: | cut -d' ' -f2` core >& backtrace.txt  
backtrace  
^D
```

Хэрэв та gdb-г хэрэглэх боломжгүй бол та өөрийн үйлдлийн системийн дебаггэр (debugger)-ийг шалгаж үзэх хэрэгтэй. Ингээд үүссэн backtrace.txt файлаа [wireshark-dev@wireshark.org](mailto:wireshark-dev@wireshark.org) хуудас руу илгээнэ.

#### **1.6.8. Виндовс (Windows) платформ дээр эвдрэл мэдээллэх**

Виндовс (windows) тархацуудад .pdb симбол файлууд (symbol files) байдаггүй. Яагаад гэвэл эдгээр нь хэтэрхий том байdag юм. Та эдгээрийг <https://www.wireshark.org/download/win32/all-versions> мөн <https://www.wireshark.org/download/win64/all-versions> хуудсуудаас тусад нь татаж авах боломжтой.

## **БҮЛЭГ II.**

### **2. ВАЙРШАРК (WIRESHARK) ПРОГРАМЫГ СУУЛГАХ**

## **2.1. Танилцуулга**

Вайршарк (Wireshark) програмыг хэрэглэхийн тулд вайршарк (wireshark) програмаа өөрийн системд суулгасан байх шаардлагатай. Виндовс (Windows) болон Мак ΘҮЭс (Mac OS) үйлдлийн системүүд дээр ажиллаж байгаа тохиолдолд <https://www.wireshark.org/download.html> веб хуудаснаас өөрийн системд тохирох файлыг татан авч шууд суулгах ба энэ бүлгийн үлдсэн хэсгийг уншилгүй алгасаж болно.

Линукс (Linux) эсвэл ФрийБиЭсДи (FreeBSD) гэх мэт үйлдлийн системүүд дээр вайршарк (wireshark) програмыг суулгахдаа эх код (source code)-оос нь инсталл (install) хийж суулгах боломжтой. Ихэнх Линукс (Linux) тархац дээр вайршарк (wireshark) программын package суулгац байдаг боловч эдгээр хувилбар нь хуучин байх магадлал өндөр байдаг. Тиймээс Линукс (Linux) тархац болон ФрийБиЭсДи (FreeBSD) гэх мэт үйлдлийн системүүд дээр вайршарк (wireshark) програмыг суулгахдаа хаанаас нь эхэлж, хэрхэн суулгахаа мэддэг байх хэрэгтэй юм.

Энэхүү бүлэг **Binary Package** болон **source code**-г хэрхэн татан авч суулгах талаарх ойлголтыг хамарна. Ийнхүү суулгахдаа та дараах алхмуудыг хийх хэрэгтэй.

1. Өөрт хэрэгтэй package-г татаж авах. Жишээлбэл эх код (source code) эсвэл бинари тархац (binary distribution)
2. Шаардлагатай тохиолдолд эх кодын (source) бинари (binary)-руу компайл (complie) хийх. Энэ процессыг хийхийн тулд өөр бусад шаардлагатай package-уудыг суулгах (install/build) шаардлагатай болж магадгүй.
3. Бинари (binaries)-уудыг тэдгээрийн эцсийн суух ёстой хавтас (final destination) руу хуулах.

## **2.2. Эх код (source) болон бинари тархацуудыш (binary distributions)-ыг татаж авах**

Та эх код (source) мөн бинари тархацуудыг (binary distributions) вайршарк (wireshark)-ын веб хуудаснаас / <https://www.wireshark.org> / татаж авах боломжтой. Татаж авах холбоосоор ороод өөрт хэрэгтэй бинари (binary) эсвэл эх пакеж (source package)-г сонгоно.

Хэрэв та вайршарк (wireshark)-г эх код (source)-оос нь суулгах (build) гэж байгаа бол ингэхээсээ өмнө хэд хэдэн эх пакеж (source package)-уудыг татаж суулгах хэрэгтэй болдог. Хэрэв та өмнө нь вайршарк (wireshark) программыг суулгаж байсан бол заавал ингэх шаардлагагүй байж болно.

## **2.3. Виндовс (Windows) орчинд Вайршарк (wireshark) суулгах**

Вайршарк (Wireshark) програмын Виндовс (windows) орчинд суух **Windows installer** файл нь үйлдлийн системийн платформ болон хувилбарыг өөрийн нэрэндээ агуулдаг. Жишээлбэл: Wireshark-win32-1.12.7.exe гэх мэт. Вайршарк (Wireshark) программын суулгац нь өөрийн багцдаа ВинПкап (WinPcap) программыг агуулдаг бөгөөд

Вайршарк програм энэхүү WinPcap-ийг ашиглан сүлжээн дэх пакет (packet) өгөгдлийг чагнах, цуглуулах үйлдлийг хийдэг.

**Windows Installer** файлыг <https://www.wireshark.org/download.html> веб хуудаснаас татаж аваад windows installer буюу .exe өргөтгөлтэй файлыг ажиллуулахад автомаар бүрэн суудаг. Эдгээр файлууд нь **Вайршарк сан (Wireshark Foundation)**-гоос баталгаажсан байдаг.

Өөрийн шаардлагаас хамааран вайршарк (wireshark)-ын бүрэлдэхүүн хэсгүүдээс сонгон зөвхөн өөрт хэрэгтэйгээ суулгах боломжтой.

### 2.3.1. Суулгацын бүрэлдэхүүн хэсгүүд

Суулгацын бүрэлдэхүүн хэсгүүдийг сонгох (*Choose Components*) хэсгээс та дараах бүрэлдэхүүнүүдээс сонгож суулгах боломжтой.

- **Wireshark** – Сүлжээний пакет (packet) өгөгдөл анализ хийх програм (GUI)
- **TShark** – Команд интерфэйс горимтой (Command line interface) сүлжээний пакет (packet) анализар програм.
- **Wireshark 1 Legacy** – Хуучин GTK+ хэрэглэгчийн интерфэйс
- **Plugins & Extensions** – Wireshark болон Tshark програмуудад зориулсан протоколыг хэсэгчлэн задлах зориулалт бүхий залгах хэсэг(plug-in)-үүд
  - **Dissector Plugins** – Протоколыг задлан шинжлэх функцийг өргөтгөж өгдөг нэмэлт залгах хэсэг (plug-in)-үүд
  - **Tree Statistics Plugins** – Статистикин функцийг өргөтгөж өгөх зориулалттай нэмэлт залгах хэсэг (plug-in)-үүд.
  - **Mate - Meta Analysis and Tracing Engine** – Хэрэглэгч өөрөө тохируулж болох өргөтгөл. Энэ нь дэлгэцийн шүүлтийн (display filter) функцийг өргөтгөдөг.
  - **SNMP MIBs** – SNMP протоколыг илүү дэлгэрэнгүй задалж харуулахад хэрэглэгддэг.
- **Tools** – Цуглуулсан пакет (packet) файл дээр ажиллах боломжтой нэмэлт текст горимын хэрэглүүрүүр
  - **Editcap** – Цуглуулсан пакет (packet) файлыг унших мөн тэдгээрийн хэсэгчлэн эсвэл бүгдийг нь өөр файл руу бичих
  - **Text2Pcap** – ASCII хекс (hex) файлаас пакет (packet)-ийг уншиж түүнийгээ .pcap файл руу бичнэ.
  - **Reordercap** – Цуглуулж авсан пакет (packet)-уудыг хугацаанаас (timestamp) нь хамааруулан ангилана.
  - **Mergecap** – Хадгалж авсан олон пакет (packet) өгөгдөлтэй файлуудыг нэг файл болгон нэгтгэж хадгална.
  - **Capinfos** – Цуглуулж авсан пакет (packet) файлын мэдээллийг харуулна.

- **Rawshark** – Raw packet-ын шүүлтүүр (filter).
- **User's Guide** – Ашиглах заавар. Хэрэв ашиглах зааврыг локал хэлбэрээр суулгаагүй бол ашиглах зааврыг үзэхийн тулд заавал интернэтэд холбох хэрэгтэй болдог.

### 2.3.2. Нэмэлт сонголтууд

- **Start Menu Shortcuts** – Windows-ын start menu-рүү shortcut – ийг нэмж оруулах.
- **Desktop Icon** – Wireshark icon-г дэлгэц рүү нэмэх
- **Quick Launch Icon** – Windows-ын хурдан хандах файлын тоноглолд wireshark icon нэмэх
- **Associate file extensions to Wireshark** – Сүлжээний өгөгдлүүдийг вайршарк (wireshark) програм дээр нээж байх тохиргоог хийх.

### 2.3.3. Суулгах байрлал

Өгөгдмөл (default) тохиргоогоор wireshark нь 32 битийн Windows үйлдлийн систем дээр %ProgramFiles%\Wireshark санд харин 64 битийн Windows үйлдлийн систем дээр %ProgramFiles64%\Wireshark санд тус тус байрлана. Энэ нь ихэнх систем дээр C:\Program Files\Wireshark сан байдаг.

### 2.3.4. WinPcap суулгах

Вайршарк (wireshark) программын installer нь WinPcap программын сүүлийн хувилбарыг өөртөө агуулдаг.

Хэрэв таны систем дээр WinPcap програм суугаагүй бол та сүлжээний орчингоор дамжигдаж буй пакет (packet) өгөгдлийг чагнах, цуглуулах үйлдлийг хийж чадахгүй. Гэвч WinPcap байхгүй байх нь өмнө нь хадгалж авсан пакет (packet) өгөгдлийг нээж үзэхэд ямар нэгэн саад болохгүй. Өгөгдмөл (default) тохиргоогоор вайршарк (wireshark)-ыг суулгах үед WinPcap –ийн хамгийн сүүлийн хувилбар нь хамт суудаг. Хэрэв та WinPcap программыг суулгахыг хүсэхгүй байвал эсвэл дахин суулгахыг хүсвэл *Install WinPcap* гэсэн сонголтыг идэвхижүүлэх эсвэл идэвхигүй (Checkbox) болгох замаар хүссэн үр дүндээ хүрэх боломжтой.

WinPcap-ийн талаар дэлгэрүүлэн судлахыг хүсвэл <https://www.winpcap.org/> <https://wiki.wireshark.org/WinPcap> гэсэн веб хуудсууд руу зочилно уу.

### 2.3.5. Windows installer –ын команд мөрийн сонголтууд

Командын горимоос дараах параметруудыг өгөх боломжтой.

- /S - энэ параметр нь инсталлерийг өгөгдмөл тохиргоотойгоор ажиллуулна. Энэ нь WinPcap –ийг суулгахгүй

- /desktopicon - нь дэлгэцийн айкон (icon)-ийг суулгана (=yes – дэлгэцийн айкон (icon) суулгана, =no – дэлгэцийн айкон (icon) суулгахгүй, эсрэг тохиолдолд өгөгдмөл тохиргоотойг авна.)
- /quicklaunchicon - энэ нь вайршарк (wireshark)-ыг хурдан нээх quick icon-г суулгах тохиргоог хийнэ (=yes – хурдан нээх айкон (icon) суулгана, =no – хурдан нээх айкон (icon)-г суулгахгүй, эсрэг тохиолдолд өгөгдмөл тохиргоог авна)
- /D - энэ параметр нь *InstallDir* болон *InstallDirRegKey*-гийн утгыг дарж бичсэнээр инсталл хийх санг (\$INSTDIR) зааж өгнө. Энэхүү параметр нь команд мөрийн хамгийн сүүлийн параметр байх ёстой бөгөөд ямар нэгэн хаалт эсвэл цэг таслал гэх мэт тэмдэгт хэрэглэхгүй.
- /NCRC – нь CRC –ийг шалгах үйлдлийг хаадаг. Энэхүү флагийг хэрэглэхгүй байхыг зөвлөж байна.

Жишээ нь:

```
>Wireshark-win64-wireshark-2.0.5.exe /NCRC /S /desktopicon=yes
/quicklaunchicon=no /D=C:\Program Files\Foo
```

Installer-ийг ямар нэгэн параметргүй ажиллуулвал энгийн интерактив хэлбэрээр ажиллана.

### **2.3.6. WinPcap-ыг гар аргаар суулгах нь (вайршаркаас салангид байдлаар)**

Энд дурдсан суулгах процессыг та вайршарк (wireshark) програмын хэрэглэж буй WinPcap –ын хувилбараас өөр хувилбарын WinPcap-ийг ашиглах үед хэрэглэнэ. Жишээлбэл WinPcap-н шинэ хувилбар гарсан үед.

Ийм тохиолдолд Виндовс (Windows) үйлдлийн системд дэмжигдэх WinPcap програмын installer-ийг <https://www.winpcap.org/> веб хуудаснаас татаж аваад суулгана.

### **2.3.7. Вайршарк (wireshark)-г шинэчлэх (Update)**

Өгөгдмөл (default) тохиргооны дагуу Виндовс (Windows) програмын багц нь шинэ хувилбар гарсан эсэхийг шалгаад хэрэглэгчид шинэ хувилбар гарсан гэдгийг мэдэгддэг. Хэрэв та вайршарк (wireshark) програмыг шинэчлэл шалгах үйлдлийг хаасан эсвэл интернэтэд холбоогүй систем дээр вайршарк (wireshark)-ыг ажиллуулж байгаа бол вайршарк (wireshark)-н мэйлийн жагсаалт (mailing list)-д бүртгүүлэх хэрэгтэй.

Вайршарк (wireshark) програмын шинэ хувилбар нь ихэвчлэн 4-өөс 6 сарын хугацаатай гарах бөгөөд шинэчлэл хийх нь суулгах процесстий ижилхэн бөгөөд *installer.exe* файлыг татаж аваад ажиллуулахад л хангалттай. Компьютерийг дахин ачааллах шаардлагагүй.

### **2.3.8. WinPcap програмыг шинэчлэх**

WinPcap програмын шинэчлэл нь тийм ч хурдан гардаггүй юм. Та WinPcap-ын шинэчлэлийг хэрхэн хийх талаарх мэдээллийг <https://www.winpcap.org/> хаягнаас олж

унших боломжтой. Суулгасныхаа дараа үйлдлийн системийг дахин ачааллах шаардлагатай.

### **2.3.9. Вайршарк (wireshark) програмыг устгах**

Вайршарк (Wireshark) програмыг устгахдаа **Programs and Features** -aac **Wireshark**-ийг сонгож **uninstall** процесийг эхлүүлнэ.

Вайршарк (Wireshark)-ыг устгахад танд бусад бүрэлдэхүүн хэсгүүдийг устгах хэд хэдэн сонголтыг санал болгодог. Өгөгдмөл (default) тохиргоогоор вайршарк (wireshark)-ыг устгах процессд хэрэглэгчийн хувийн тохиргоог хадгалж үлдэх мөн WinPcap программыг устгалгүй хадгалж үлдэх тохиргоотой байдаг.

### **2.3.10. WinPcap программыг устгах**

WinPcap программыг устгахдаа **Programs and Features** -aac **WinPcap**-ийг сонгож **uninstall** процесийг эхлүүлнэ. WinPcap програм байхгүй бол та сүлжээн дээгүүр дамжигдаж буй пакет (packet) өгөгдлийг чагнах боломжгүй болно гэдгийг анхаарах хэрэгтэй.

## **2.4. Мак Өү Эс Х (Mac OS X) орчинд вайршарк (Wireshark) програм суулгах**

Вайршарк (Wireshark) программын Mac OS X дээр суух бэлдэц файл нь *.dmg* буюу disk image файл байх бөгөөд энэ файл нь дотроо вайршарк (wireshark)-ыг Mac OS дээр суулгах зүйлсийг багцаар нь агуулж байдаг. Суулгахын тулд *.dmg* файлыг нээж инсталлер (installer) хэсгийг ажиллуулна.

Инсталлер (installer) нь вайршарк (wireshark) болон түүнтэй холбоотой команд мөрийн програмуудыг мөн өөртөө агуулахаас гадна систем эхлэх үед вайршарк (wireshark)-аар сүлжээг чагнах эрх (permission)-г тохируулах программыг (daemon)-г мөн агуулж байдаг. Илүү дэлгэрэнгүй мэдээллийн Mac OS системд суух вайршарк (wireshark) программын *Read me first* хэсгээс уншина уу.

## **2.5. Юникс (Unix) орчинд вайршаркыг эх (source) кодоос тохируулан суулгах нь**

Вайршарк (Wireshark) программыг эх код (source code)-оос нь суулгахад вайршарк (wireshark)-д ашиглах хөрвүүлэгч (compiler) мөн түүнийг дэмжин ажиллах бусад бүх сангидыг суусан байх шаардлагатай. Дэлгэрэнгүй мэдээллийг <https://www.wireshark.org/docs/> Wireshark программыг хөгжүүлэгчдийн гарын авлагаас үзнэ үү.

Линукс/Юникс (Linux/Unix) үйлдлийн систем дээр вайршарк (Wireshark) программыг суулгахдаа дараах дарааллаар суулгадаг.

1. Шахаж хадгалсан *.tar* файлыг задална. Хэрэв таны хэрэглэж буй Линукс/Юникс (Unix/Linux) системд GNU *tar* програм байгаа бол дараах командаар задална.

```
$ tar xaf wireshark-2.0.5.tar.bz2  
Бусад тохиолдолд  
$ bzip2 -d wireshark-2.0.5.tar.bz2  
$ tar xf wireshark-2.0.5.tar командыг ашиглана.
```

2. Вайршарк (Wireshark) программын эх код (source code) байгаа сан руу шилжих.  
\$ cd wireshark-2.0.5
3. Эх кодоо (source code) хэрэглэж буй системдээ тохируулах хэрэгтэй. Үүнийг дараах командаар хийнэ.  
\$ ./configure  
Хэрэв энэ алхмыг хийх үед алдаа үүсвэл та энэхүү алдааг засссаны дараа дахин  
../configure командыг ажиллуулах хэрэгтэй. Алдааг оношлох, засахтай  
холбоотой мэдээллийг **2.7.”Юникс орчинд суулгах үед үүссэн алдааг оношлох (Troubleshooting during the install in Unix)”** хэсгээс уншина уу.
4. Эх код (source code)-ыг хөрвүүлэх (compile) хийх  
\$ make
5. Програмыг ажиллах сан руу хуулах  
\$ make install

Дээрх алхмуудыг амжилттай хийж програмаа суулгасны дараа та wireshark гэсэн командаар терминалаас вайршарк (wireshark) программыг эхлүүлнэ.

## **2.6. Юникс (Unix) орчинд бинари (binaries) ашиглан вайршарк (wireshark)-г суулгах нь**

Бинари (binary) ашиглан Юникс (Unix) орчинд вайршарк (wireshark)-ыг суулгах үед тухайн Юникс (Unix) үйлдлийн системийн хувилбараас нь хамаараад өөр өөр арга замаар суулгадаг. Жишээлбэл AIX системийн орчинд smit –ийг ашиглан суулгаж байхад Tru64 Unix систем дээр set1d-ыг ашигладаг.

### **2.6.1. Red Hat болон түүнтэй төстэй үйлдлийн систем дээр RPM-ийг ашиглан суулгах нь**

Вайршарк (Wireshark) программын веб хуудаснаас татаж авсан файлаа (.rpm) суулгахдаа дараах командыг ашиглана.

```
rpm -ivh wireshark-2.0.5.i386.rpm
```

Энэхүү командыг биелүүлэх явцад вайршарк (wireshark) програмг дэмжин ажиллах зайлшгүй программуудаас (dependency) болж алдаа гарвал тухайн суулгах ёстой программыг суулгасны дараа дахин вайршарк (wireshark) програмаа суулгах хэрэгтэй.

### **2.6.2. Debian, Ubuntu болон бусад Debian-aac салаалж гарсан үйлдлийн системүүдийн орчинд DEB-ийг ашиглан суулгах нь**

Хэрэв та Repository ашиглан суулгах боломжтой байвал дараах командыг ашиглан суулгана.

```
$ aptitude install wireshark
```

Aptitude команд нь өөрөө вайршарк (wireshark) програмыг дэмжин ажиллахын тулд шаардлагатай байдаг програмуудыг автоматаар суулгадаг.

Хэрэв веб хуудаснаас өөрийн системд тохирох .deb файлыг татаж авсан бол дараах командаар суулгана.

```
$ dpkg -i wireshark-common_2.0.5.0-1_i386.deb  
wireshark-wireshark-2.0.5.0-1_i386.deb
```

dpkg нь вайршарк (wireshark) програмыг дэмжин ажиллахад шаардагдах программууд (dependency)-ыг автоматаар суулгахгүй боловч чухам ямар програм суулгах шаардлагатай байгааг тодорхой хэлж өгдөг.

**Сүлжээ чагнах эрх:** Вайршарк програмыг суулгасны дараа root эрхгүй хэрэглэгчид сүлжээн дээгүүрх өгөгдлийг чагнах эрхгүй байдаг. root эрхгүй хэрэглэгчдэд сүлжээг чагнах эрх олгохын тулд README.Debian файлыг нээж унших хэрэгтэй.

### 2.6.3. Gentoo Linux үйлдлийн системд portage-г ашиглан суулгах нь

Дараах командыг ашиглан вайршарк (wireshark) програмыг суулгана.

```
$ USE="adns gtk ipv6 portaudio snmp ssl kerberos threads selinux"  
emerge wireshark
```

### 2.6.4. FreeBSD үйлдлийн системд package-г ашиглан суулгах нь

Дараах командыг ашиглан суулгана.

```
$ pkg_add -r wireshark
```

pkg\_add команд нь вайршарк (wireshark)-ыг дэмжин ажиллах (dependency) бүх программууд болон сангруудыг автоматаар суулгадаг.

## 2.7. Юникс орчинд суулгах үед үүссэн алдааг засах (Troubleshooting during the install on Unix)

Суулгах процессын үед төрөл бүрийн алдаа гарах боломжтой бөгөөд тэдгээрийг бүгдийг нь энд авч үзэх боломжгүй юм. Гэвч вайршарк (wireshark) програмыг суулгах үед үүсдэг түгээмэл алдааг хэрхэн оношилж, засварлах талаар мэдээллийг дараах хэсэгт тайлбарлалаа.

Хэрэв таныг configure хийж байх үед алдаа үүсвэл эх код (source code) агуулагдах сан дотор байрлах config.log файлд алдааны мэдээлэл байх бөгөөд үүний хамгийн сүүлийн мөрүүдэд алдааны дэлгэрэнгүй мэдээлэл байрладаг.

Түгээмэл тулгардаг алдаануудад систем дээр шаардлагатай хөгжүүлэлтийн багц (development package) байхгүй байх эсвэл хөгжүүлэлтийн багц (development package) нь шинэ хувилбар луугаа шинэчлэгдэж амжаагүй байгаа зэрэр асуудлуудыг хамардаг. Вайршарк (wireshark) програм суухын тулд санггуудын багц (Library package)-аас гадна хөгжүүлэлтийн багц (development package)-ийг суулгасан байх шаардлагатай байдаг. Мөн түүнчлэн Libpcap суугаагүй шалтгаанаас болон `configure` хийх үед алдаа үүсч болно.

Чухам ямар алдаа үүссэнийг тодорхойлж чадахгүй байвал вайршарк (wireshark) программын хөгжүүлэгчдийн мэйлийн жагсаалт (wireshark-dev mailing list) рүү өөрт тулгарсан асуудлаа товч тодорхой тайлбарлан илгээх боломжтой. Ингэхдээ үүссэн алдаатай хамааралтай байж болзошгүй гэж үзэж буй мэдээллээ мэйлдээ хавсаргах хэрэгтэй бөгөөд түүнээс гадна `config.log` файлын гаралтыг заавал хавсаргасан байх хэрэгтэй байдаг.

## **2.8. Виндовс (Windows) орчинд эх код (source code)-оос нь вайршарк программыг суулгах нь**

Та хэрэв вайршарк программыг хөгжүүлэх зорилготой биш бол вайршарк (wireshark) программыг суулгахдаа бэлэн бинари (binary) файлыг ашиглахыг зөвлөж байна.

Хэрэв та вайршарк (wireshark) программыг виндовс орчинд хөгжүүлэхээр шийдсэн бол дараах 2 хаяг дээр мэдээллээс илүү дэлгэрэнгүй мэдээллийг авна уу.

Хөгжүүлэгчдийн гарын авлага: <https://www.wireshark.org/docs/>

Хөгжүүлэгчдийн вики хуудас: <https://wiki.wireshark.org/development>

## **БҮЛЭГ III**

### **3. ХЭРЭГЛЭГЧИЙН ИНТЕРФЭЙС**

#### **3.1. Танилцуулга**

Эндээс цаашхи хэсэгт уншигч таныг өөрийн систем дээр вайршарк (wireshark) програмыг амжилттай суулгачихсан гэж үзэх ба вайршарк (wireshark) программын хэрхэн ашиглах талаар тайлбарлана.

Энэ бүлэгт дараах ойлголтуудыг авч үзнэ. Эдгээрт:

- Вайршарк (Wireshark) програмын хэрэглэгчийн интерфэйс хэрхэн ажилладаг талаар
- Вайршарк (Wireshark) програм дээр пакет (packet) өгөгдөлтэй хэрхэн ажиглах талаар
- Вайршарк (Wireshark) програм дээр пакет (packet) өгөгдлийг хэрхэн харах талаар
- Цуглуулсан пакет (packet) өгөгдлийг хэрхэн шүүж, ангилж харах талаар гэх мэт

### **3.2. Вайршарк (wireshark) програмыг ачааллах (эхлүүлэх)**

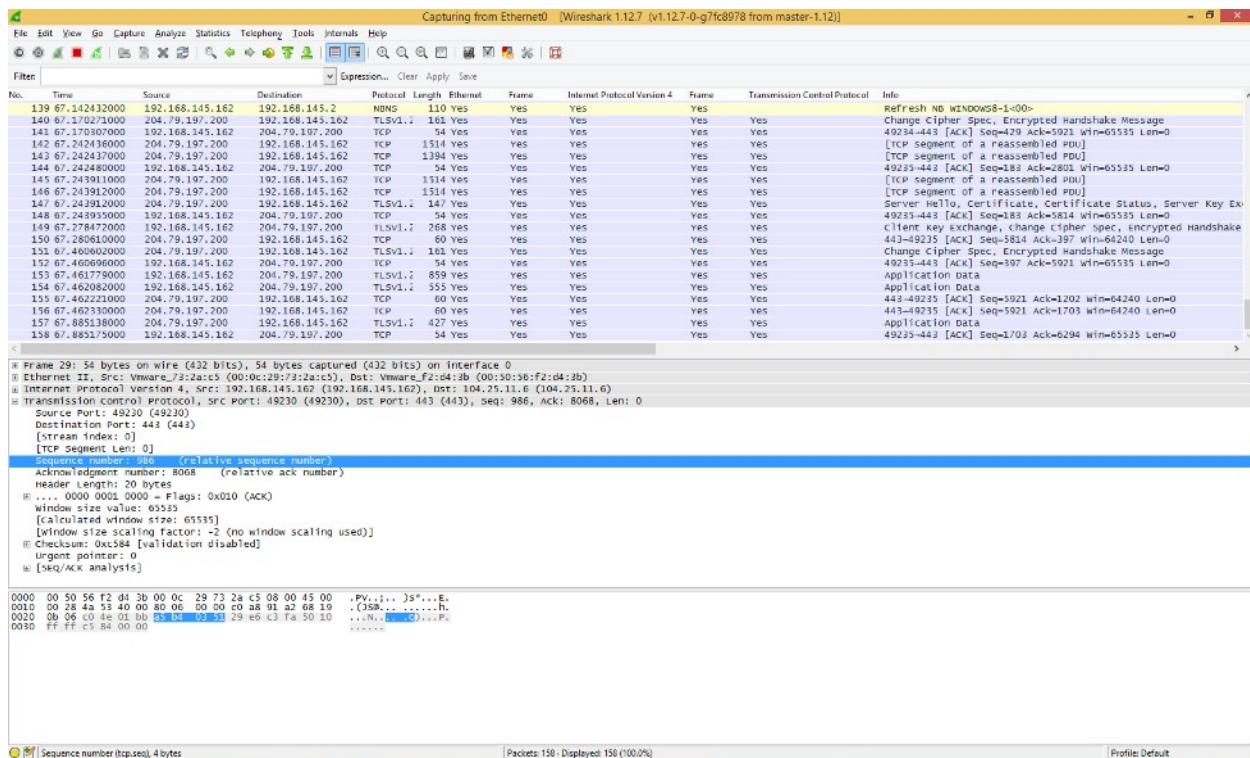
Вайршарк (Wireshark) програмыг график айкон (icon)-ыг ашиглан эсвэл команд горимоос команд ашиглан эхлүүлэх гэсэн 2 аргаар эхлүүлэх боломжтой.

Командын горимоос вайршарк (wireshark) програмыг ажиллуулахдаа хэд хэдэн тохииргооны зүйлсийг хийх боломжтой байдаг бөгөөд энэ талаарх дэлгэрэнгүй мэдээллийг **10.2. “Вайршарк програмыг команд горимоос эхлүүлэх (Start wireshark from the command line)”** хэсгээс уншина уу.

Энэ бүлэгт Виндовс (Windows) орчинд суулгасан вайршарк (wireshark) програмыг жишээ болгон авсан болно. Таны хэрэглэж буй үйлдлийн системийн төрлөөс хамаараад график интерфэйс бага зэрэг өөр харагдаж болох хэдий ч функцууд болон тэдгээрийн ерөнхий байрлалын хувьд ямар нэгэн ялгаатай зүйл байхгүй болно.

### **3.3. Үндсэн цонх (Main window)**

Үндсэн цонх гэдэг нь вайршарк (wireshark) програм ажиллаж байх үеийн дэлгэцэнд харагдах хэсгийг ерөнхийд нь хэлдэг.



Зураг 3.1. Үндсэн цонх

Вайршарк (Wireshark) програмын үндсэн цонх (Main window) нь бусад программын график горимын хэрэглэгчийн цонхтой ерөнхийдөө ижилхэн.

- Цэс (Menu)** нь вайршарк (wireshark) програм дээр үйлдэл хийх, функц эхлүүлэхэд хэрэглэгддэг. (3.4. “Цэс (Menu)” хэсгээс дэлгэрүүлэн уншина уу. )
- Үндсэн товчлуурууд (Main toolbar)** нь байнга хэрэглэгддэг хэрэглүүр, функцүүдээ хялбархан ашиглаг боломжийг олгодог. ( 3.16. “Үндсэн товчлуур (Main toolbar)” хэсгээс дэлгэрүүлэн уншина уу. )
- Шүүлтүүрийн товчлуурууд (Filter toolbar)** нь дэлгэцэнд харагдаж буй пакет (packet) өгөгдлүүдийг шүүлтүүрээр хялбархан оруулах, шүүлтүүрийн дагуу ангилж харах боломжийг олгодог. (3.17. “Шүүлтүүрийн товчлуурууд (Filter toolbar)” мөн 6.3. “Пакет (packet) –ыг үзж байхдаа шүүлтүүрийг ашиглах (Filtering packets while viewing)” хэсгүүдээс дэлгэрүүлэн уншина уу.)
- Пакетыг жагсаан харуулах самбар (Packet list pane)-ын хэсэгт цуглуулсан пакет (packet)-уудыг жагсаалт (list) хэлбэрээр харуулах ба энэхүү цонхонд пакет (packet) бүрийн товч мэдээллийг харуулдаг. Энд байрлах пакет (packet)-ыг хулганы заагчийг ашиглан идэвхижүүлснээр та тухайн пакет (packet)-ийн дэлгэрэнгүй мэдээлэл болон түүний байт (byte)-аар илэрхийлэгдэх хэсгүүдийг дэлгээцийн доод хэсэгт харах болно. (3.18. “Пакетыг жагсааж харуулах самбар (Packet list pane)” хэсгээс дэлгэрүүлэн уншина уу.)**

5. **Пакетын дэлгэрэнгүй мэдээллийг харуулах самбар (Packet details pane)** нь дэлгэцийн төв хэсэгт байрлах пакетыг жагсаан харуулах самбарын хэсэг (packet list pane)-д идэвхижсэн байгаа пакет (packet) –ын тухай мэдээллийг дэлгэрэнгүй хэлбэрээр харуулдаг. (3.19. “Пакетын дэлгэрэнгүй мэдээллийг харуулах самбар (Packet Details pane)” хэсгээс дэлгэрүүлэн уншина уу.)
6. **Пакетын мэдээллийг байтаар харуулах самбар (Packet bytes pane)** нь пакетыг жагсаан харуулах самбар (packet list pane)-д идэвхитэй байгаа пакет (packet)-ын өгөгдлийг байтаар харуулдаг. Ингэхдээ пакетын дэлгэрэнгүй мэдээллийг харуулах самбарын хэсэгт (packet details pane) сонгогдсон байгаа хэсгийг байгаа хэсгийг өнгөөр ялган тодруулж харуулдаг. (3.20 “Пакетын мэдээллийг байтаар харуулах самбар (Packet Bytes Pane)” хэсгээс дэлгэрүүлэн уншина уу.)
7. **Статусбар (Status bar)** нь програмын болон цуглуулсан пакет (packet) өгөгдлийн төлөвийн талаар мэдээллийг хэрэглэгчид өгдөг. (3.21. “Статусбар (status bar)” хэсгээс дэлгэрүүлэн уншина уу)

Үндсэн цонхны бүтэц, зохион байгуулалтыг вайршарк (wireshark) программын тохиргоог (*Edit->Preferences...*) ашиглан өөрчлөх боломжтой. Дэлгэрүүлэн уншихыг хүсвэл 10.5 “Тохируулга (Preferences)” хэсгийг үзнэ үү.

### 3.3.1. Үндсэн цонхыг ашиглах нь

Пакетын жагсаалтаар харах (Packet list) мөн Пакетын мэдээллийг дэлгэрэнгүй харах (packet details) зэрэг үйлдлүүдийг компьютерийн гарын товчлууруудын (keyboard) хослол ашиглан удирдах боломжтой.

*Хүснэгт 3.1 Вайршарк (Wireshark) программыг компьютерийн гар ашиглан удирдах*

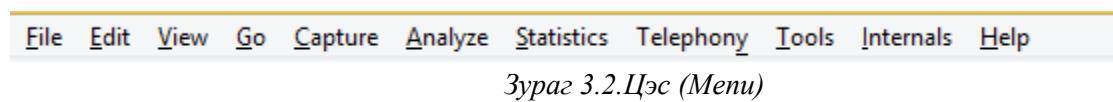
Гарын товчлуурын хослол	Тайлбар
Tab, Shift+Tab	Дэлгэцийн элементүүдийн хооронд шилжинэ. Жишээ нь: Пакетыг дэлгэрэнгүй харуулах самбар (Packet details pane) Пакетын мэдээллийг байтаар харуулах (Packet Bytes Pane) самбар руу шилжих гэх мэт
Down	Дараагийн пакет (packet) руу эсвэл Пакетын мэдээллийг дэлгэрэнгүй харуулах самбар (Packet details pane)-т үзүүлж буй мэдээллийн дараагийнх хэсэг руу шилжих
Up	Өмнөх пакет (packet) руу эсвэл Пакетын мэдээллийг дэлгэрэнгүй харуулах самбар (Packet details pane)-т үзүүлж буй мэдээллийн өмнөх мэдээллийн хэсэг руу шилжих
Ctrl+Down, F8	Пакетыг жагсаан харуулах самбар (Packet list pane) хэсэгт пакет идэвхижээгүй байсан ч үл харгалзан хамааран Пакетыг жагсаан харуулах самбар дахь (packet list pane) дахь дараагийн пакет (packet) руу шилжинэ.
Ctrl+Up, F7	Пакетыг жагсаан харуулах самбар (Packet list pane) хэсэгт пакет идэвхижээгүй байсан ч үл харгалзан хамааран Пакетыг жагсаан харуулах самбар дахь (packet list pane) дахь өмнөх пакет (packet) руу шилжинэ.
Ctrl+.	TCP, UDP, IP протоколуудыг ашиглан холбогдож байгаа 2 хостын үүсгэсэн холболтыг ашиглан илгээсэн өгөгдлийн (conversation)

	дараагийн пакет (packet) руу шилжих
Ctrl+,	TCP, UDP, IP протоколуудыг ашиглан холбогдох байгаа 2 хостын үүсгэсэн холболтыг ашиглан илгээсэн өгөгдлийн (conversation) өмнөх пакет (packet) руу шилжих
Left	Пакетыг дэлгэрэнгүй харуулах самбар (Paket detail) хэсэг дэх мод (tree) хэлбэрийн бүтэцтэй мэдээллийг хаана. Хаалттай байгаа тохиолдолд өмнөх хэсгийн мэдээлэл руу шилжинэ.
Right	Пакетыг дэлгэрэнгүй харуулах самбар (Paket detail) хэсэг дэх мод (tree) хэлбэрийн бүтэцтэй мэдээллийг задалж нээнэ.
Shift+Right	Пакетыг дэлгэрэнгүй харуулах самбар (Packet details pane) хэсгийн мод (tree) хэлбэрийн бүтцэд багтах идэвхижсэн мод (tree) бүтцийн бүх дэд хэсгүүдийг мэдээллийг бүгдийг нь нээж задална.
Ctrl+Right	Пакетын мэдээллийг дэлгэрэнгүй харуулах самбар (Packet Details pane) дээрх мод (tree) хэлбэрийн мэдээллийн дэд хэсгүүдийг бүгдийг нь нээж задална.
Ctrl+Left	Пакетын мэдээллийг дэлгэрэнгүй харуулах самбар (Packet Details pane) хэсгийнмод (tree) хэлбэрийн бүтцийн дэх дэд хэсгүүдийг бүгдийг нь хаана.
Backspace	Пакетын мэдээллийг дэлгэрэнгүй харах самбар (Packet Details pane) хэсэг дэх мод (tree) хэлбэрийн бүтэц дэх мэдээллийн дээд (parent) хэсэг руу үсэрнэ.
Return, Enter	Пакетын мэдээллийг дэлгэрэнгүй харуулах самбар (Packet Details Pane) хэгийн мод (tree) хэлбэрийн бүтцийг нээж, хаах үйлдлийг хийдэг.
Дэлгэцийн аль хэсэг идэвхижиснээс үл хамааран үндсэн цонхон дээр бичсэн тэмдэгтүүд шүүлтүүрийн (filter) хэсэгт бичигддэг.	

### 3.4. Цэс (Menu)

Вайршарк (wireshark) програмын үндсэн цэс (menu) нь үндсэн цонхны (Main window) дээд хэсэгт (Windows, Linux) эсвэл дэлгэцийн дээд хэсэгт (Mac OS) байрладаг.

Хэрэгжих боломжгүй байгаа функц үйлдлүүдийг заах цэс (menu) нь саарал байх бөгөөд идэвхижихгүй. Ямар үед идэвхигүй байх вэ гэвэл жишээлбэл та аль хэдийнэ хадгалчихсан файлаа ямар нэгэн өөрчлөлт оруулалгүйгээр хадгалах гэх мэт.



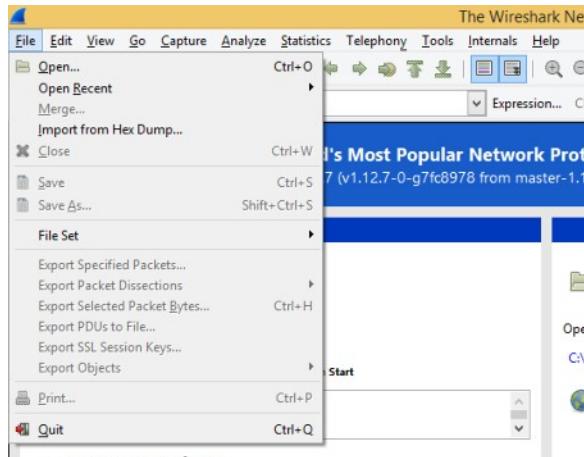
Вайршарк (wireshark) програмын цэс (menu)-д дараах дараах зүйлс багтдаг.

File	File цэс нь цуглувансан файлуудыг нэгтгэх, нээх, хадгалах, хэвлэх, экспорт хийх эсвэл вайршарк (wireshark) програмаас гарах гэсэн үйлдлүүдийг хийдэг. <b>3.5. “File цэс”</b> хэсгээс илүү дэлгэрүүлэн уншина уу
Edit	Edit цэсийг ашиглан пакет (packet) хайх, цагийн лавлагаа харах эсвэл пакетуудыг идэвхижүүлэх (mark), профайлын тохиргоо хийх, өөрийн тохиргоог хийх (preferences) зэрэг үйлдлүүдийг хийх боломжтой. <b>3.6.</b>

	<b>“Edit цэс”</b> хэсгээс дэлгэрүүлэн уншина уу
View	Энэ цэсийг ашиглан цуглуулсан пакет (packet)-уудыг өнгөөр ялгах, дэлгэцийн үсгийн фонт өөрлөх, пакет (packet)-ыг тусдаа шинэ цонхонд харуулах пакетын мэдээллийг дэлгэрэнгүй харах хэсгийн мод (tree) мэдээллийг задалж дэлгэх, хумих гэх мэт дэлгэцэнд мэдээллийг ямар байдлаар харуулж болох бүхий л тохииргоог хийх боломжтой байдаг. <b>3.7 “View цэс”</b> хэсгээс дэлгэрүүлэн уншина уу.
Go	Энэ цэс тодорхой нэг пакет (packet) руу очих, хянах боломжтой болдог. <b>3.8. “Go цэс”</b> хэсгээс дэлгэрүүлэн уншина уу
Capture	Энэ цэс нь сүлжээгээр дамжиж буй пакет (packet) өгөгдлийг чагнах, чагнах процессыг зогсоох, чагнах явцын шүүлтүүрийг засварлах боломж олгодог. <b>3.9. “Capture цэс”</b> хэсгээс дэлгэрүүлэн уншина уу
Analyze	Analyze цэс дэлгэцийн шүүлтүүрийг тохируулан идэвхижүүлэх, протоколын задлах хэсгүүдийг идэвхижүүлэх, болиулах, хэрэглэгчийн тодорхойлж өгсөн байдлаар сүлжээний пакет (packet) өгөгдлийг задлах мөн TCP урсгал (stream)-ыг дагах гэх мэт үйлдлүүдийг хийдэг. <b>3.10. “Analyze цэс”</b> хэсгээс дэлгэрэнгүй мэдээллийг уншина уу
Statistics	Энэ цэс нь нийт пакет (packet)-уудын хураангуйлсан статистик мэдээллийг харахмөн протоколын шаталсан хэлбэрийн статистикиг харах гэх мэт үйлдлийг хийх боломжийг хэрэглэгчид олгодог. <b>3.11. “Statistics цэс”</b> хэсгээс дэлгэрэнгүй мэдээллийг уншина уу.
Telephony	Энэ цэс нь мэдия анализ, урсгалын диаграм, протоколын шаталсан статистик гэх мэт утсан холбоотой хамааралтай статистик мэдээллийг харах боломжоор хэрэглэгчийг хангадаг. <b>3.12. “Telephony цэс”</b> хэсгээс дэлгэрүүлэн уншина уу.
Tools	Tools цэс нь Firewall ACL Rules үүсгэх гэх мэт вайршарк (wireshark) програм дээр хэрэгжүүлэх боломжтой байдаг хэрэглүүрүүдийг (tools) ашиглах боломж олгодог. <b>3.13. “Tools цэс”</b> хэсгээс дэлгэрүүлэн уншина уу.
Internals	Энэ цэс нь вайршарк (wireshark) програмын дотоод мэдээллүүдийг харуулах үүрэгтэй. Жишээлбэл таны ашиглаж буй wireshark програм ямар ямар протоколыг дэмжиж ажиллаж байгаа эсэх гэх мэт. <b>3.14. “Internals цэс”</b> хэсгээс дэлгэрүүлэн уншина уу
Help	Энэ цэс нь хэрэглэгчид туслах зарим нэгэн энгийн туслах командууд, текст горимоос өгөх командуудын тайлбар мөн хэрэгцээтэй веб хандалт ашиглан авах боломжтой заавар зэргийг үзэх боломжоор хэрэглэгчийг хангадаг. <b>3.15. “Help цэс”</b> хэсгээс дэлгэрүүлэн унших боломжтой.

Дээрх хүснэгтэд үзүүлсэн цэс (menu)-уудыг дараагийн хэсгүүдэд задалж дэлгэрэнгүй үзүүллээ.

### 3.5. File цэс



Зураг 3.3 File цэс

File цэсний дэлгэрэнгүй тайлбарыг дараах хүсгэнтээр харууллаа.

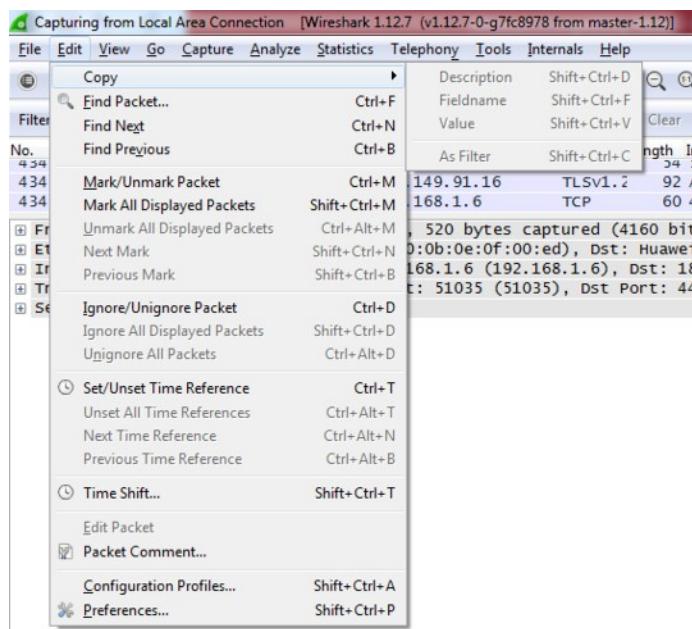
Хүснэгт 3.2 File цэсний команд

Цэс	Гарын товчлуурын хослол	Тайлбар
<b>Open...</b>	Ctrl+O	Энэ цэс нь цуглуулсан сүлжээнийг өгөгдлийг вайршарк дээр нээх үйлдлийг хийхэд тань таныг хөтөлнө. <b>5.2.1. “Цуглуулсан пакет файл нээх (Open Capture File dialog box)</b> ” хэсгээс дэлгэрүүлэн уншина уу.
<b>Open Recent</b>		Энэ цэс нь сүүлд нээсэн файлуудыг файлуудыг танд дэд командын сонголт хэлбэрээр харуулдаг. Ингэснээр та эдгээр дэд сонголтоос сонгох замаар сүүлд нээж үзсэн файлуудыг шууд нээх боломжтой.
<b>Merge...</b>		Энэ цэс нь вайршарк дээр нээлттэй байгаа пакет (packet) файл дээр нэмж өөр пакет (packet)-ын файлыг нэгтгэдэг. <b>5.4. “Файлуудыг нэгтгэх (Merging capture files)</b> ” хэсгээс дэлгэрүүлэн уншина уу.
<b>Import from Hex Dump...</b>		Энэ цэс нь хекс (hex) утгыг нь агуулсан текст файлыг импорт хийх цонхыг нээж өгнө. <b>5.5. “Хекс өгөгдлийг импорт хийх (Import hex dump)</b> ” хэсгээс дэлгэрүүлэн уншаарай
<b>Close</b>	Ctrl+W	Энэ цэс нь цуглуулсан пакет (packet) өгөгдлийг хаадаг. Гэхдээ хэрэв тухайн хаах гэж буй файл хадгалагдаагүй байвал түүнийг хадгалах эсэхийг лавлаж асуудаг. Түүнээс гадна үүний тохиргоог өөрийн хүссэнээр (preference) өөрчлөх боломжтой юм.
<b>Save</b>	Ctrl+S	Энэ цэс нь цуглуулсан файлыг хадгалаад. Өгөгдмөл байдлаар хадгалах файлын нэрийг тохируулж өгөөгүй бол тухайн файлыг хадгалах үйлдлийг хөтлөх цонх (Save Capture file as dialog box) гарч ирнэ. Энэ талаар <b>5.3.1. “Файл хадгалах цонх (Save Capture File as dialog box)</b> ” хэсэгт дэлгэрүүлэн авч үзсэн байгаа.  Файлыг аль хэдийн хадгалчихсан байвал энэ цэс нь саарал өнгөтэй байх ба биелэхгүй.  Сүлжээн дээрх өгөгдлийг бодит байдлаар чагнаж байгаа файлыг хадгалж авдаггүй учраас эхлээд пакет чагнах ажиллагааг зогсоосон байх хэрэгтэй.
<b>Save As...</b>	Shift+Ctrl+	Энэ цэс нь цуглуулсан байгаа пакет файлаа өөрийн хүссэнээр өөрчлөн

	S	хадгалах боломжийг хэрэглэгчид олгоно. Энэ үйлдлийг хийх үед <i>Save Capture File As</i> цонхыг ашиглан гэртээ харих боломжтой болно. <b>5.3.1. “Файл хадгалах цонх (Save Capture File as dialog box)”</b> хэсэгт энэ тухай дэлгэрүүлэн авч үзсэн.
<b>File Set &gt; List Files</b>		Энэ цэс нь файлын багц (file set) дотор орших файлуудын жагсаалтыг үзүүлдэг. Энэ цэс нь Вайршаркын файлын багцийн жагсаалт цонхыг нээх ба түүгээр дамжуулан дээр дурдсан үүргээ биелүүлдэг. <b>5.6. “Файлын багц File sets”</b> хэсэгт дэлгэрэнгүй тайлбарласан байгаа.
<b>File Set &gt; Next File</b>		Одоогоор ачааллагдсан байгаа файл нь файлын багц (file set) –ын нэг хэсэг байвал энэ команд нь файлын багц (file set)-ийн дараагийн файл руу шилжүүлнэ. Ачааллагдсан байгаа файл файлын багц (file set)-д хамаарахгүй эсвэл файлын багцын хамгийн сүүлийн файл байвал саарал өнгөтэй байх ба биелэх боломжгүй байна.
<b>File Set &gt; Previous File</b>		Одоогоор ачааллагдсан байгаа файл нь файлын багц (file set) –ын нэг хэсэг байвал энэ команд нь файлын багц (file set)-ийн өмнөх файл руу шилжүүлнэ. Ачааллагдсан байгаа файл файлын багц (file set)-д хамаарахгүй эсвэл файлын багцын хамгийн эхний файл байвал саарал өнгөтэй байх ба биелэх боломжгүй байна.
<b>Export &gt; File...</b>		Энэ цэс нь одоо дэлгэцэнд харуулж буй чагнаж, цуглуулсан пакет (packet) өгөгдлийг бүгдийг нь (эсвэл хэсэгчилсэн байдлаар) файл болгон экспорт хийдэг. Ингэхдээ вайршарк экспорт хийх цонхыг ашигладаг. Дэлгэрүүлэн уншихыг хүсвэл <b>5.7. “Файл Экспортлох (Exporting data)”</b> хэсигийг уншина уу.
<b>Export &gt; Selected Packet Bytes...</b>	Ctrl+H	Энэ цэс нь пакетын мэдээллийг байтаар харуулах самбарт (packet bytes pane) идэвхижүүлсэн байгаа байтуудыг бинари (binary) файл руу экспорт хийж гаргадаг. Энэ хэсэг нь мөн л вайршарк экспорт хийх цонхоор дамжин хийгдэнэ. Дэлгэрүүлэн уншихыг хүсвэл <b>5.7.7. “Идэвхижүүлсэн байтыг экспорт хийх (Export selected packet bytes)”</b> хэсгийг уншина уу
<b>Export &gt; Objects &gt; HTTP</b>		Энэ цэс нь чагнаж цуглуулсан HTTP объектуудыг бүгдийг нь (эсвэл хэсэгчлэн) локал файл руу экспорт хийнэ. Энэ цэс нь Вайршарк HTTP объектын жагсаалт (Wireshark HTTP object list)-ыг харуулдаг. <b>5.7.8. “Объектуудыг экспорт хийх (Export objects)”</b> хэсгээс дэлгэрүүлэн уншина уу
<b>Export &gt; Objects &gt; DICOM</b>		Энэ цэс нь чагнаж цуглуулсан DICOM объектуудыг бүгдийг нь (эсвэл хэсэгчлэн) локал файл руу экспорт хийнэ. Энэ цэс нь Вайршарк DICOM объектын жагсаалт (Wireshark DICOM object list)-ыг харуулдаг. <b>5.7.8. “Объектуудыг экспорт хийх (Export objects)”</b> хэсгээс дэлгэрүүлэн уншина уу
<b>Export &gt; Objects &gt; SMB</b>		Энэ цэс нь чагнаж цуглуулсан SMB объектуудыг бүгдийг нь (эсвэл хэсэгчлэн) локал файл руу экспорт хийнэ. Энэ цэс нь Вайршарк SMB объектын жагсаалт (Wireshark SMB object list)-ыг харуулдаг. <b>5.7.8. “Объектуудыг экспорт хийх (Export objects)”</b> хэсгээс дэлгэрүүлэн уншина уу
<b>Print...</b>	Ctrl+P	Цуглуулсан пакет (packet) файлуудыг бүгдийг нь (эсвэл хэсэгчлэн) хэвлэх үйлдэл хийнэ. Энэ цэс нь Вайршарк хэвлэх (wireshark print) цонхыг дэлгэцэнд харуулдаг. Дэлгэрүүлэн уншихыг хүсвэл <b>5.8. “Пакетуудыг хэвлэх (Printing packets)”</b> хэсгийг уншина уу.
<b>Quit</b>	Ctrl+Q	Энэ цэс нь таныг вайршарк програмаас гаргана (Вайршарк програмыг хаана). Хэрэв чагнаж цуглуулсан файлаа хадгалаагүй бол хадгалах

		эсэхийг тань асуудаг. Гэхдээ энэ тохиргоог та өөрөө асуухгүй болгон тохируулж болно. Ингэхдээ Preference гэсэн тохиргооны хэсгийг ашиглана.
--	--	---

### 3.6. Edit цэс



Зураг 3.4. Edit команд

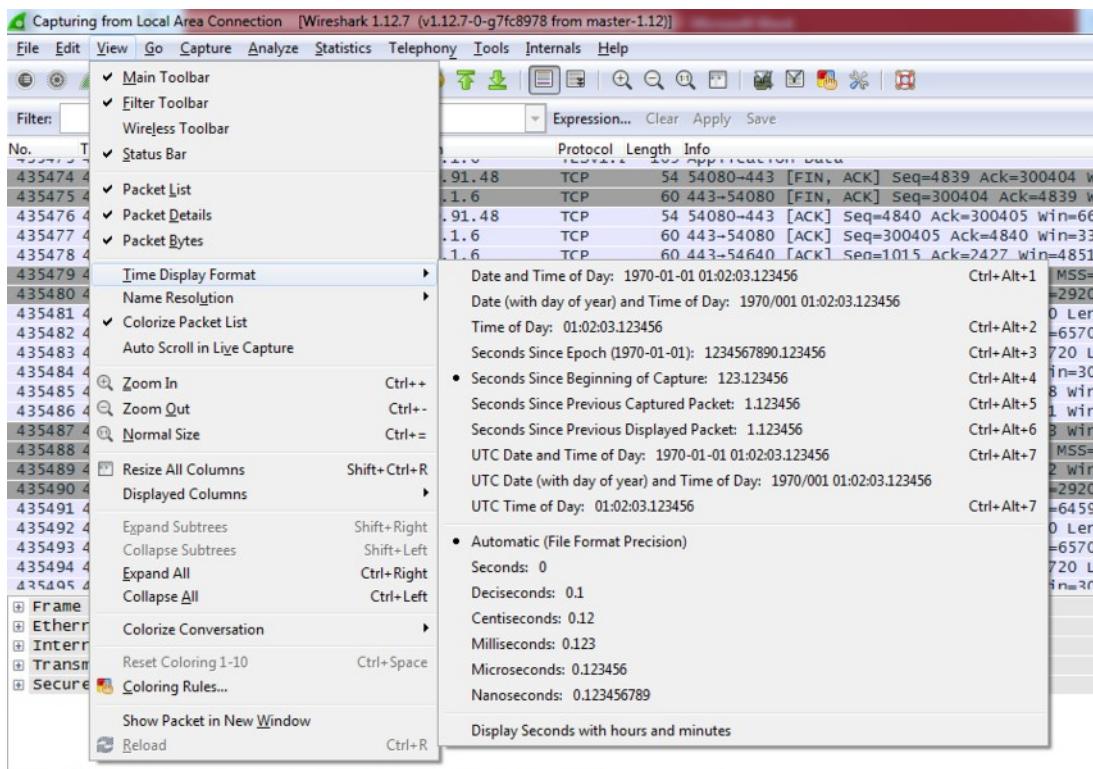
Edit цэсийг дараах хүснэгтээр дэлгэрэнгүй тайлбарлалаа.

Хүснэгт 3.3. Edit цэсний команд

Цэс	Гарын товчлуурын хослол	Тайлбар
<b>Copy &gt; Description</b>	Shift+Ctrl+D	Энэ цэс нь дэлгэрэнгүй мэдээллийг нь харуулах самбар (detailed view)-д идэвхижүүлсэн байгаа өгөгдлийн тодорхойлолтыг санах ой руу (clipboard) хуулдаг.
<b>Copy &gt; Fieldname</b>	Shift+Ctrl+F	Энэ цэс нь дэлгэрэнгүй мэдээллийг нь харуулах самбар (detailed view)-д идэвхижүүлсэн байгаа өгөгдлийн талбарын нэрийг (fieldname) санах ой руу (clipboard) хуулдаг.
<b>Copy &gt; Value</b>	Shift+Ctrl+V	Энэ цэс нь дэлгэрэнгүй мэдээллийг нь харуулах самбар (detailed view)-д идэвхижүүлсэн байгаа өгөгдлийн утгыг (value) санах ой руу (clipboard) хуулдаг.
<b>Copy &gt; As Filter</b>	Shift+Ctrl+C	Энэ цэс нь дэлгэрэнгүй мэдээллийг нь харуулах самбар (detailed view)-д идэвхижүүлсэн байгаа өгөгдлийг дэлгэцийн пакетуудыг шүүх хэсэгт ашигладаг. Энэхүү дэлгэцийн шүүлтүүр нь тэгээд санах ой руу (clipboard) руу хуулагддаг.
<b>Find Packet...</b>	Ctrl+F	Энэ цэс нь төрөл бүрийн шалгуур ашиглан өөрт хэрэгтэй пакетаа хайж олох цонхыг танд харуулдаг. <b>6.8. “Пакет хайх (Finding packets)”</b> хэсгээс дэлгэрүүлэн уншина уу.
<b>Find Next</b>	Ctrl+N	Таны хайж буй шалгуурт тохирсон дараагийн пакетыг танд олж өгнө.
<b>Find Previous</b>	Ctrl+B	Таны хайж буй шалгуурт тохирсон өмнөх пакетыг танд олж өгнө.

<b>Mark/Unmark Packet</b>	Ctrl+M	Идэвхитэй байгаа пакет (packet)-ыг тэмдэглэнэ/тэмдэглэгээг арилгана (mark/unmark). <b>6.10. “Пакетыг тэмдэглэх (Marking packets)”</b> хэсгээс дэлгэрүүлэн уншина уу.
<b>Toggle Marking Of All Displayed Packets</b>	Shift+Ctrl+Alt+M	Дэлгэцэнд байгаа бүх пакет (packet)-уудыг тэмдэглэх/тэмдэглэгээг байхгүй болгох (mark/unmark).
<b>Mark All Displayed Packets</b>	Shift+Ctrl+M	Дэлгэцэнд байгаа бүх пакет (packet)-ыг тэмдэглэнэ (mark).
<b>Unmark All Displayed Packets</b>	Ctrl+Alt+M	Дэлгэцэнд байгаа бүх пакет (packet)-уудын тэмдэглэгээг байхгүй (unmark) болгох.
<b>Find Next Mark</b>	Shift+Ctrl+N	Тэмдэглэгдсэн пакет (marked packet)-уудаас дараагийн тэмдэглэгээтэй пакет (marked packet)-г олно.
<b>Find Previous Mark</b>	Shift+Ctrl+B	Тэмдэглэгдсэн пакет (marked packet)-уудаас өмнөх тэмдэглэгээтэй пакет (marked packet) олно.
<b>Ignore Packet (toggle)</b>	Ctrl+D	Идэвхитэй байгаа пакетад (packet) үл ойшоосон (ignore) тэмдэглэгээ тавина. Дэлгэрүүлэн уншихыг хүсвэл <b>6.11. “Пакетыг үл ойшоох (Ignoring packets)”</b> хэсгийг уншина уу
<b>Ignore All Displayed Packets (toggle)</b>	Shift+Ctrl+D	Дэлгэцэнд байгаа бүх пакетуудыг үл ойшоосон/үл ойшоогоогүй (ignore/unignore) гэсэн тэмдэглэгээгээр тэмдэглэнэ.
<b>UnIgnore All Packets</b>	Ctrl+Alt+D	Бүх пакетуудыг (packet) үл ойшоогоогүй (UnIgnored) гэсэн тэмдэглэгээгээр тэмдэглэнэ.
<b>Set Time Reference (toggle)</b>	Ctrl+T	Энэ цэс нь идэвхитэй байгаа пакетад цагийн лавлагааг тохируулж өгдөг. Ингэснээр цагийн лавлагаа тохируулсан (time reference) пакет (packet)-аас хойш сүлжээгээр дамжсан пакет (packet)-уудыг өмнөх пакет (packet)-ын ирсэн хугацаанаас хойш ямар хугацаанд ирснийг харах боломжтой. Дэлгэрүүлэн уншихыг хүсвэл <b>6.12.1. “Пакетын цагийн лавлагаа (Packet time referencing)”</b> хэсгийг үзнэ уу.
<b>Un-Time Reference All Packets</b>	Ctrl+Alt+T	Пакет (Packet)-уудын дээрх цагийн лавлагaa (time reference) байхгүй болгоно.
<b>Find Next Time Reference</b>	Ctrl+Alt+N	Энэ цэс нь цагийн лавлагaa (time reference) болон тохируулагдсан пакет (packet)-уудаас дараагийн цагийн лавлагaa (time reference) болж буй пакет (packet)-ыг хайж олно.
<b>Find Previous Time Reference</b>	Ctrl+Alt+B	Энэ цэс нь цагийн лавлагaa (time reference) болон тохируулагдсан пакет (packet)-уудаас өмнөх цагийн лавлагaa (time reference) болж буй пакет (packet)-ыг хайж олно.
<b>Configuration Profiles...</b>	Shift+Ctrl+A	Энэ цэс нь профайл тохиргоо хийх цонх руу хөтөлдөг. Илүү дэлгэрүүлэн уншихыг хүсвэл <b>10.6 “Профайл тохиргоо (Configuration Profiles)”</b> хэсгийг үзнэ уу.
<b>Preferences...</b>	Shift+Ctrl+P	Энэ цэс нь вайршарк (wireshark) програмыг удирддаг параметруудыг тохируулах боломжийг олгодог. Энд тохируулсан тохиргоогоо хадгалах, дараа нь вайршарк (wireshark) програмыг эхлүүлэх үед өмнөх тохиргоотойгоор ажиллуулах гэх мэт зүйлсийг хийх боломжтой. Дэлгэрэнгүй уншихыг хүсвэл <b>10.5. “Тохиргоо (Preferences)”</b> хэсгийг үзнэ уу. <a href="mk:@MSITStore:C:\Program%20Files\Wireshark\user-guide.chm::/wsug_chm/ChCustPreferencesSection.html">mk:@MSITStore:C:\Program%20Files\Wireshark\user-guide.chm::/wsug_chm/ChCustPreferencesSection.html</a>

### 3.7. View цэс



Зураг 3.5. View команд

View цэсний командуудыг дараах хүснэгтээр тайлбарлалаа.

1. Пакетыг жагсаан харуулах самбар (Packet list pane)
2. Пакетын дэлгэрэнгүй мэдээллийг харуулах самбар (Packet details pane)
3. Пакетын мэдээллийг байтаар харуулах самбар (Packet bytes pane)
4. Статусбар (Status bar)

Хүснэгт 3.4. View цэсний команда

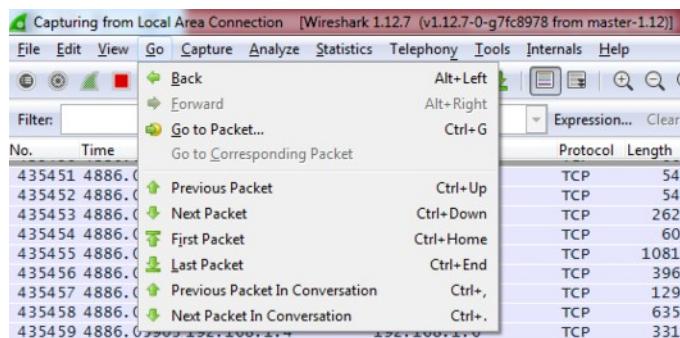
Цэс	Гарын товчлуурын хослол	Тайлбар
Main Toolbar		Энэ цэс нь үндсэн товчлуурууд (main toolbar)-ын хэсгийг үндсэн цонхонд (main windows) харуулах, дэлгэнээс алга болгох үйлдлийг хийдэг. <b>3.16. “Үндсэн товчлуурууд (Main toolbar)”</b> хэсгийг үзнэ үү.
Filter Toolbar		Энэ цэс нь шүүлтүүрийн товчлууруудыг (filter toolbar) үндсэн цонхонд харуулах эсвэл алга болгох үйлдлийг хийнэ. <b>3.17. “Шүүлтүүрийн товчлуурууд (Filter toolbar)”</b> хэсгийг үзнэ үү.
Wireless Toolbar (Windows only)		Энэ цэс нь утасгүй сүлжээний товчлуурууд (wireless toolbar)-ыг үндсэн цонхонд (main window) харуулах эсвэл үндсэн цонхноос алга болгох үйлдлийг хийнэ.
Statusbar		Энэ цэс нь статусбар (status bar) хэсгийг үндсэн цонхонд харуулах эсвэл алга болгох үйлдлийг хийнэ. <b>3.21. “Статусбар (Status bar)”</b> хэсгийг үзнэ үү
Packet List		Энэ цэс нь пакетыг жагсаалт хэлбэрээр харуулах самбарыг (packet list pane) үндсэн цонхонд харуулах эсвэл үндсэн цонхноос алга

		болгох үйлдэл хийнэ. <b>3.18. “Пакетыг жагсаан харуулах самбар (Packet list pane)”</b> хэсгийг үзнэ үү
<b>Packet Details</b>		Энэ цэс нь пакетын мэдээллийг дэлгэрэнгүй харуулах самбарыг (packet details pane) үндсэн цонхонд харуулах эсвэл үндсэн цонхноос алга болгох үйлдэл хийнэ. <b>3.19. “Пакетын мэдээллийг дэлгэрэнгүй харуулах самбар (Packet details pane)”</b> хэсгийг үзнэ үү
<b>Packet Bytes</b>		Энэ цэс нь пакетын мэдээллийг байтаар харуулах самбарыг (packet bytes pane) үндсэн цонхонд харуулах эсвэл үндсэн цонхноос алга болгох үйлдэл хийнэ. <b>3.20. “Пакетын мэдээллийг байтаар харуулах самбар (Packet bytes pane)”</b> хэсгийг үзнэ үү
<b>Time Display Format &gt; Date and Time of Day: 1970-01-01 01:02:03.123456</b>		Энэ хэсгийг сонгосноор вайршарк (Wireshark) програм сүлжээнээс барьж авсан пакет (packet)-уудын ирсэн цагийг мэдээллийг он, сар, өдөр, цаг гэсэн бүтэцтэйгээр харуулдаг. <b>6.12. “Цагийн мэдээллийн бүтэц, тохиргоо (Time display formats and time references)”</b> хэсгээс дэлгэрүүлэн уншина уу.  <b>“Time of Day”, “Date and Time of Day”, “Seconds Since Beginning of Capture”, “Seconds Since Previous Captured Packet”, “Seconds Since Previous Displayed Packet”</b> гэсэн сонголтууд нь нэгэн зэрэг сонгогдох боломжгүй бөгөөд нэг удаад зөвхөн аль нэгийг нь л сонгох боломжтой.
<b>Time Display Format &gt; Time of Day: 01:02:03.123456</b>		Энэ хэсгийг сонгосноор вайршарк (Wireshark) програм пакет (packet)-ын цагийн мэдээллийг тухайн өдрийн цагаар гаргана. <b>6.12. “Цагийн мэдээллийн бүтэц, тохиргоо (Time display formats and time references)”</b> хэсгээс дэлгэрүүлэн уншина уу.
<b>Time Display Format &gt; Seconds Since Epoch (1970-01-01): 1234567890.123456</b>		Энэ хэсэг нь пакет (packet)-ын цагийн мэдээллийг 1970-01-01 00:00:00 эхлэн тоолсон секундын хэмжигдэхүүнээр харуулна. <b>6.12. “Цагийн мэдээллийн бүтэц, тохиргоо (Time display formats and time references)”</b> хэсгээс дэлгэрүүлэн уншина уу.
<b>Time Display Format &gt; Seconds Since Beginning of Capture: 123.123456</b>		Энэ хэсгийг сонгосноор вайршарк (Wireshark) програм пакетын (packet)-ын цагийн мэдээллийг харуулахдаа пакет (packet) цуглуулж эхэлсэн хугацаанаас хойшхи секундээр хэмжин харуулдаг. <b>6.12. “Цагийн мэдээллийн бүтэц, тохиргоо (Time display formats and time references)”</b> хэсгээс дэлгэрүүлэн уншина уу.
<b>Time Display Format &gt; Seconds Since Previous Captured Packet: 1.123456</b>		Энэ сонголтыг идэвхижүүлснээр пакет (packet)-ын цагийн мэдээллийг өмнө нь хүлээн авсан пакет (packet)-аас хойш хэдэн секундын дараа ирж байгаа байдлаар нь харуулна. <b>6.12. “Цагийн мэдээллийн бүтэц, тохиргоо (Time display formats and time references)”</b> хэсгээс дэлгэрүүлэн уншина уу.
<b>Time Display Format &gt; Seconds Since Previous Displayed Packet: 1.123456</b>		Энэ сонголтыг идэвхижүүлснээр пакет (packet)-ын цагийн мэдээллийг өмнөх пакетыг дэлгэцэнд харуулснаас хойш хэдэн секундын дараа дэлгэцэнд харуулж байгаа секундээр хэмждэг. <b>6.12. “Цагийн мэдээллийн бүтэц, тохиргоо (Time display formats and time references)”</b> хэсгээс дэлгэрүүлэн уншина уу.
<b>Time Display Format &gt; Automatic (File Format Precision)</b>		Энэ хэсгийг сонгосноор пакет (packet)-ын цагийн мэдээллийг цуглуулсан файлын форматад тодорхойлсон нарийвчлалаар харуулна. <b>6.12. “Цагийн мэдээллийн бүтэц, тохиргоо (Time display formats and time references)”</b> хэсгээс дэлгэрүүлэн уншина уу. “Automatic”, “Seconds”, “... seconds” гэсэн сонголтуудыг зэрэг сонгох боломжгүй

<b>Time Display Format &gt; Seconds: 0</b>		Энэ сонголтыг сонгосноор вайршарк (wireshark) програм пакет (packet)-ын цагийн мэдээллийг секундын нарийвчлалтайгаар харуулна. <b>6.12. “Цагийн мэдээллийн бүтэц, тохиргоо (Time display formats and time references)”</b> хэсгээс дэлгэрүүлэн уншина уу.
<b>Time Display Format &gt; ...seconds: 0....</b>		Энэ хэсгийг сонгосноор вайршарк (wireshark) програм пакет (packet)-ын цагийн мэдээллийг секунд, 1/10 сек, 1/100 сек, 1/1000сек гэх мэт нарийвчлалтай харуулдаг. <b>6.12. “Цагийн мэдээллийн бүтэц, тохиргоо (Time display formats and time references)”</b> хэсгээс дэлгэрүүлэн уншина уу.
<b>Time Display Format &gt; Display Seconds with hours and minutes</b>		Энэ хэсгийг сонгосноор вайршарк (wireshark) програм пакетын цагийн мэдээллийг цаг минутын хамтаар секундын нарийвчлалтайгаар харуулдаг.
<b>Name Resolution &gt; Resolve Name</b>		Энэ сонголт нь идэвхитэй байгаа пакет (packet)-ын нэрийн хөрвүүлэлтийг хийдэг. <b>7.7. “Нэрийн хөрвүүлэлт (Name Resolution)”</b> хэсгээс дэлгэрүүлэн уншина уу.
<b>Name Resolution &gt; Enable for MAC Layer</b>		Энэ сонголт нь вайршарк (wireshark) програм МАС хаягийг нэр лүү хөрвүүлэх эсэхийг удирддаг. <b>7.7. “Нэрийн хөрвүүлэлт (Name Resolution)”</b> хэсгээс дэлгэрүүлэн уншина уу.
<b>Name Resolution &gt; Enable for Network Layer</b>		Энэ хэсэг нь вайршарк (wireshark) програм сүлжээний хаягуудийг нэрийн хөрвүүлэлт рүү хөрвүүлэх эсэхийг удирддаг. <b>7.7. “Нэрийн хөрвүүлэлт (Name Resolution)”</b> хэсгээс дэлгэрүүлэн уншина уу.
<b>Name Resolution &gt; Enable for Transport Layer</b>		Энэ хэсэг нь вайршарк (wireshark) програм <i>transport</i> түвшний хаягийг нэрийн хөрвүүлэлт рүү хөрвүүлэх эсэхийг удирддаг. <b>7.7. “Нэрийн хөрвүүлэлт (Name Resolution)”</b> хэсгээс дэлгэрүүлэн уншина уу.
<b>Colorize Packet List</b>		Энэ хэсэг нь пакетын жагсаалт (packet list)-ыг өнгөөр ялгах эсэхийг удирдана. Өнгөөр ялгах нь чагнах, цуглуулсан пакет (packet)-ыг дэлгэцэнд хэвлэх үйлдлийг удаан болгодог.
<b>Auto Scroll in Live Capture</b>		Энэ хэсэг нь пакетыг жагсаан харуулах самбарт (packet list pane) шинэ пакет (packet) нэмэгдэхэд дэлгэцийг автоматаар доош нь гүйлгэдэг.. Хэрэв энэ хэсэгт тэр тохиргоог хийж өгөхгүй бол шинээр пакет цуглуулахад ирж байгаа пакетууд нь дэлгэцэнд харагдахгүйгээр доол талд нь нэмэгдэж явна.
<b>Zoom In</b>	Ctrl++	Үсгийн фонтыг томруулна
<b>Zoom Out</b>	Ctrl+-	Үсгийн фонтыг багасгана.
<b>Normal Size</b>	Ctrl+=	Үсгийн фонтын хэмжээг хэвийн болгоно.
<b>Resize All Columns</b>	Shift+Ctrl+R	Багана бүрийн өргөнийг өгөгдлийнх уртад тааруулан өөрчлөх. Их хэмжээний өгөгдлөтэй байгаа үед баганын хэмжээг тааруулах нь илүү их хугацаа зарцуулах магадлалтай
<b>Displayed Columns</b>		Энэ хэсэг нь дэлгэцэнд харуулахаар тохируулсан багануудыг нэгтгэн удирдана. Эдгээр тохиргоогоор пакетын жагсаан харуулах самбар (packet list pane) харуулж байгаа багануудыг дэлгэцэнд харуулах эсвэл дэлгэцэнд харуулахгүй байх тохируулгыг хийнэ.
<b>Expand Subtrees</b>	Shift+Right	Энэ сонголт нь пакетын мэдээллийг дэлгэрэнгүй харуулах самбар (packet details pane)-т байрлах мод (tree) хэлбэрийн бүтцийн мэдээллийг задалж харуулна.
<b>Collapse Subtrees</b>	Shift+Left	Энэ сонголт нь пакетын мэдээллийг дэлгэрэнгүй харуулах самбар (packet details pane)-т байрлах мод (tree) хэлбэрийн бүтцийн мэдээллийг хумиж хаана.

<b>Expand All</b>	Ctrl+Right	Пакетын мэдээллийг дэлгэрэнгүй харуулах самбар (packet details pane) дахь мод (tree) хэлбэрийн бүтэцтэй мэдээллийг бүгдийг нь задална.
<b>Collapse All</b>	Ctrl+Left	Пакетын мэдээллийг дэлгэрэнгүй харуулах самбар (packet details pane) дахь мод (tree) хэлбэрийн бүтэцтэй мэдээллийг бүгдийг нь хумиж хаана.
<b>Colorize Conversation</b>		Энэ сонголт нь пакетын жагсаалт хэлбэрээр харуулах самбар (packet list pane)-т идэвхитэй байгаа пакетын IP хаяг дээр суурилан тухайн пакет (packet)-уудыг өнгөөр ялгадаг. Ингэснээр мэдээлэл солилцож буй 2 хостын пакет (packet) өгөгдлийг ялган хараад хялбар болно. <b>10.3. “Пакетыг өнгөөр ялгах (Packet colorization)”</b> хэсгээс дэлгэрүүлэн уншина уу.
<b>Colorize Conversation &gt; Color 1-10</b>		Энэ сонголт нь идэвхитэй байгаа пакет (packet)-ын IP хаяг (source, destination) дээр суурилан өнгөөр ялгана. Ингэхдээ түр зуур ялгах 10 өнгийг санал болгодог.
<b>Colorize Conversation &gt; Reset coloring</b>		Энэ сонголт нь өнгөөр ялгасан пакет (packet)-уудын өнгийг алга болгоно.
<b>Colorize Conversation &gt; New Coloring Rule...</b>		Энэ сонголт нь идэвхижсэн байгаа пакетын IP хаяг (source, destination) дээр суурилан өнгөөр ялгах шинэ дүрэм байх дүрэм үүсгэх боломж олгоно.
<b>Coloring Rules...</b>		Энэ сонголт нь пакетыг жагсаан хараа самбар (packet list pane)-т байгаа пакет (packet)-уудыг өөрийн сонгосон шүүлтүүрийг ашиглан өөр өнгөөр ялган хараа тохиргоог хийх боломжийг олгодог. Энэ тохиргоо нь тодорхой төрлийн пакет (packet)-уудыг ялгаж хараад маш их хэрэгтэй байдаг. <b>10.3. “Пакетыг өнгөөр ялгах (Packet colorization)”</b> хэсгээс дэлгэрүүлэн уншина уу.
<b>Show Packet in New Window</b>		Энэ сонголт нь сонгож авсан пакет (packet)-ыг тусдаа цонхонд нээж хараа боломжийг олгодог. Тусдаа нээгдсэн цонхонд зөвхөн мод (tree) хэлбэрийн бүтцээр мэдээллийг нь дэлгэрэнгүй хараа мөн байтаар хараа самбарын мэдээллүүд л агуулагддаг..
<b>Reload</b>	Ctrl+R	Энэ сонголт нь одоогийн цуглуулсан байгаа пакет (packet) файлыг дахин ачаалладаг.

### 3.8. Go цэс



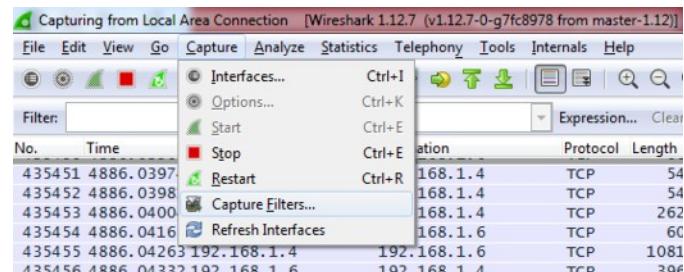
Зураг 3.6. Go команд

Го цэсний командуудын тайлбарын доор үзүүлсэн хүснэгтэд харууллаа.

### Хүснэгт 3.5. Go цэсний команд

Цэс	Гарын товчлуурын хослол	Тайлбар
<b>Back</b>	Alt+Left	Пакетын түүх (Packet history) хэсэгт хадгалагсан байгаа пакет (packet)-уудын дарааллын дагуу хамгийн сүүлд хандсан пакет (packet) руу очно.
<b>Forward</b>	Alt+Right	Пакетын түүх (Packet history) хэсэгт хадгалагсан байгаа пакет (packet)-уудын дарааллын дагуу тухайн пакетын өмнө хандсан пакет (packet) руу очно. <b>Back</b> цэсний эсрэг үйлдэл.
<b>Go to Packet...</b>	Ctrl+G	Пакет (Packet)-ын дугаарыг нь зааж өгснөөр тухайн (packet) руу очно. <b>6.9. “Заасан пакет руу үсрэх (Go to a specific packet)”</b> хэсгээс дэлгэрүүлэн уншина уу
<b>Go to Corresponding Packet</b>		Протокол талбар дээр идэвхижсэн байгаа протоколын талбартай нийцэж байгаа пакет (packet) руу очно. Хэрэв сонгогдсон байгаа протоколын талбарт ямар нэгэн пакет (packet) харгалзахгүй байвал энэ команд нь саарал өнгөтэй болох ба биелэгдэхгүй.
<b>Previous Packet</b>	Ctrl+Up	Пакетыг жагсаан харуулах самбарт (Packet list pane) байгаа пакет (packet)-ын өмнөх пакет (packet) руу очно. Энэ команд нь пакетыг жагсаан харуулах сабмар (packet list pane) хэсэгт компьютерийн гар идэвхижээгүй байсан ч гэсэн өмнөх пакет (packet) руу нь шилжүүлдэг.
<b>Next Packet</b>	Ctrl+Down	Пакетыг жагсаан харуулах самбарт (Packet list pane) байгаа пакет (packet)-ын дараагийн пакет (packet) руу очно. Энэ команд нь пакетыг жагсаан харуулах сабмар (packet list pane) хэсэгт компьютерийн гар идэвхижээгүй байсан ч гэсэн өмнөх пакет (packet) руу нь шилжүүлдэг.
<b>First Packet</b>	Ctrl+Home	Пакет жагсаан харуулах самбарт (Packet list pane) дахь хамгийн эхний пакет (packet) дээр очно
<b>Last Packet</b>	Ctrl+End	Пакет жагсаан харуулах самбарт (Packet list pane) дахь хамгийн суулийн пакет (packet) дээр очно
<b>Previous Packet In Conversation</b>	Ctrl+,	Одоогийн пакетын (packet) харилцан мэдээлэл (conversation) дамжуулалтын өмнөх пакет руу аваачдаг.
<b>Next Packet In Conversation</b>	Ctrl+.	Одоогийн пакетын (packet) харилцан мэдээлэл (conversation) дамжуулалтын дараагийн пакет руу аваачдаг.

### 3.9. Capture цэс



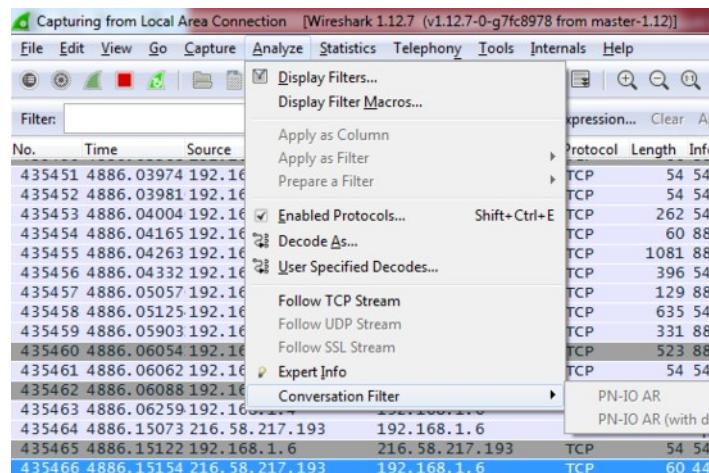
Зураг 3.7 Capture цэс команд

Capture цэсний тайлбарыг доор хүснэгтэд тайлбарлан үзүүллээ.

Хүснэгт 3.6 Capture цэсний команд

Цэс	Гарын товчлуурын хослол	Тайлбар
Interfaces...	Ctrl+I	Энэ сонголт нь сүлжээний интерфэйсүүд дээр ямар ачаалтай мэдээлэл дамжигдаж буй мэдээллийг харуулдаг цонх руу хөтөлнө. <b>4.4. “Интерфэйс чагнах (Capture Interfaces)”</b> хэсгээс дэлгэрүүлэн уншина уу
Options...	Ctrl+K	Энэ сонголт нь сүлжээг чагнахдаа ямар тохиргоотойгоор чагнах тохиргоог хийх цонх руу хөтөлдөг. Мөн эндээс чагнах үйлдлийг эхлүүлж болдог. <b>4.5. “Чагнах процесст хийх тохиргоо (Capture Options)”</b> хэсгээс дэлгэрүүлэн уншина уу
Start	Ctrl+E	Өмнө нь хэрэглэж байсан пакет чагнах тохиргоог ашиглан пакет (packet)-ыг чагнах үйлдлийг эхлүүлнэ.
Stop	Ctrl+E	Одоо ажиллаж буй пакет чагнах процессыг зогсоно. <b>4.14.1. “Ажиллаж буй чагнах үйлдлийг зогсоох (Stop the running capture)</b> ” хэсгээс дэлгэрүүлэн уншина уу
Restart	Ctrl+R	Пакет чагнах үйлдлийг дахин эхлүүлдэг. Ингэхдээ өмнө нь хэрэглэж байсан тохиргоог ашигладаг.
Capture Filters...		Энэ сонголт нь сүлжээний интерфэйс дээгүүрх пакет өгөгдлийг чагнахдаа шүүлтүүр тохируулж чагнах боломж олгох мөн түүнчлэн шүүлтүүрийн тохиргоог шинээр үүсгэх түүндээ нэр өгч дараа нь ашиглахад бэлэн болгох боломжтой. <b>6.6. “Шүүлтүүрийг тодорхойлдог мөн шүүлтүүрийг хадгалах (Defining and saving filter)</b> ” хэсгээс дэлгүүлэн уншина уу

### 3.10. Analyze цэс



Зураг 3.8. “Analyze” команд

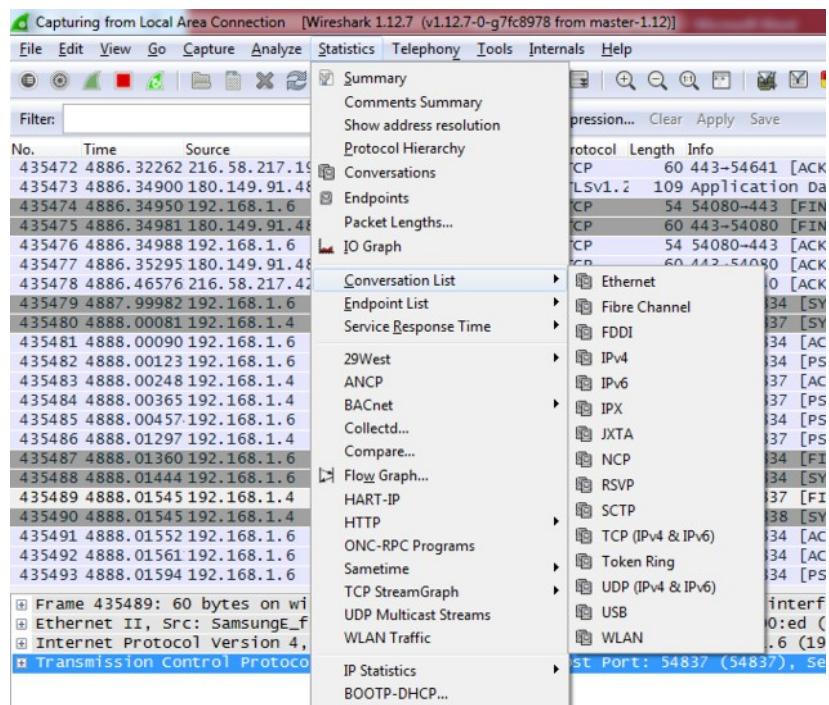
Analyze команда нь тайлбарыг хүснэгтэд үзүүллээ.

Хүснэгт 3.7. Analyze цэсний команд

Цэс	Гарын товчлуурын хослол	Тайлбар
Display Filters...		Энэ цэс нь дэлгэцэнд харуулж байгаа (packet)-уудыг шүүлтүүрээр оруулах, шүүтүүрийг шинээр үүсгэх, түүндээ нэр өгч хадгалах зэрэг үйлдлийг хийх цонх руу хэрэглэгчийг хөтөлнө. Дэлгэрүүлэн уншихын тулд <b>6.6. “Шүүтүүрийг тодорхойлох мөн хадгалах (Defining and saving filters)”</b> хэсгийг үзнэ уу
Display Filter Macros...		Энэ цэс нь дэлгэцийн шүүлтүүрийн макро үүсгэх цонх руу хөтөлнө. Энэ цонхыг ашиглан макро үүсгэх, үүсгэсэн макрогог засварлах гэх мэт үйлдлүүдийг хийх цонхыг нээдэг. Эдгээр макродоо нэр өгөх хадгалар, дараа ашиглахаар тохируулж болно. Дэлгэрүүлж уншихыг хүсвэл <b>6.7. “Макрогог тодорхойлох, хадгалах (defining and saving filter macros)”</b> хэсгээс харна уу
Apply as Column		Энэ цэс нь пакетын протоколын хэсэгт идэвхижсэн байгаа талбарыг нь пакетыг жагсаан харуулах самбарт (packet list pane) шинэ багана болгон нэмж харуулдаг.
Apply as Filter > ...		Эдгээр сонголт нь дэлгэцийн шүүлтүүрийн (display filter) тохиргоог өөрчлөх ба өөрчлөгдсөн тохиргоог нэн дариу идэвхижүүлдэг. Сонгосон сонголтоос хамаарч шүүлтүүрийн тэмдэгт нь пакетыг дэлгэрэнгүй харуулах самбарт (packet details pane) сонгосон байгаа протоколын хэсгээр шууд солигдоно эсвэл одоо байгаа түлхүүр үг дээр нэмэгдэж давхар орох (And, Or логик холбоосуудаар холбогдоно) сонголтууд байдаг.
Prepare a Filter > ...		Эдгээр сонголтууд нь одоо идэвхитэй байгаа шүүлтүүрийг өөрчлөх хэдий ч тэдгээрийг одоо идэвхитэй байгаа дэлгэцэнийн шүүлтүүр болгон идэвхижүүлэхгүй. Сонгосон сонголтоос хамаарч шүүлтүүрийн тэмдэгт нь пакетыг дэлгэрэнгүй харуулах самбарт (packet details pane) сонгосон байгаа протоколын хэсгээр шууд солигдоно эсвэл одоо байгаа түлхүүр үг дээр нэмэгдэж давхар орох (And, Or логик холбоосуудаар холбогдоно) сонголтууд байдаг.
Enabled Protocols...	Shift+Ctrl+E	Энэ команд нь протоколыг задлан харуулах хэсгийг (dissector) идэвхижүүлэх/идэвхигүй болгох үйлдлийг хийдэг. Илүү дэлгэргүүлэн уншихын хүсвэл <b>10.4.1. “Идэвхижүүлсэн протоколууд (Enabled Protocols)”</b> хэсгийг үзнэ уу
Decode As...		Энэ цэс нь тодорхой пакет (packet)-уудыг заагдсан (хэрэглэгч өөрөө тодорхойлж өгсөн протокол байж болно) протоколын дагуу задалдаг. <b>10.4.2. “Хэрэглэгчийн тодорхойлсон задлагч (User Specified Decodes)”</b> хэсгээс дэлгэрүүлэн уншина уу
User Specified Decodes...		Энэ сонголт нь өөрийн зааж өгсөн протоколын дагуу пакет (packet)-уудыг задлан харуулдаг. <b>10.4.3. “Хэрэглэгчийн тодорхойлсон задлагчуудыг харах (Show User Specified Decodes)”</b> хэсгээс дэлгэрүүлэн уншина уу
Follow TCP Stream		Энэ цэс нь сонгогдсон байгаа TCP пакет (packet)-тай ижилхэн холболт ашиглаж байгаа бүх TCP сегментүүдийг тусад нь дэлгэцэнд харуулдаг. <b>7.2. “TCP урсгалыг хөөх (Following TCP streams)”</b> хэсгээс дэлгэрүүлэн үзнэ уу.
Follow UDP Stream		Өмнөх командтай ижилхэн үйлдэл хийнэ гэхдээ UDP пакет (packet)-ын хувьд энэхүү үйлдлийг хийдэг.
Follow SSL Stream		Өмнөх командтай ижилхэн үйлдэл хийнэ гэхдээ SSL пакет (packet)-ын хувьд энэхүү үйлдлийг хийдэг. XXX – SSL түлхүүрүүдийг хэрхэн хангах

		вэ?
<b>Expert Info</b>		Энэ хэсэг нь цуглувалсан пакет (packet)-уудын талаар ахисан түвшинд хэрэглэгдэх мэдээллийг харуулна. Эдгээр мэдээллийн хэмжээ нь протоколуудаас хамаардаг бөгөөд түүнчлэн эдгээр мэдээлүүд нь маш дэлгэрэнгүй харуулдаг. XXX – шинэ хэсэг нэмэх, эндээс холболт үүсгэх (link from here)
<b>Conversation Filter &gt; ...</b>		Энэ хэсэгт харилцан мэдээлэл солилцож буй холболтыг шүүж харах шүүлтүүр олно. (conversation filter)

### 3.11. Statistics цэс



Зураг 3.9. "Statistics" команд

Statistics цэсний дэлгэрэнгүй тайлбарыг доорхи хүснэгтээр харууллаа.

Энэ цэсний бүх сонголтууд нь статистикийн тухай мэдээллийг агуулсан шинэ цонх нээдэг.

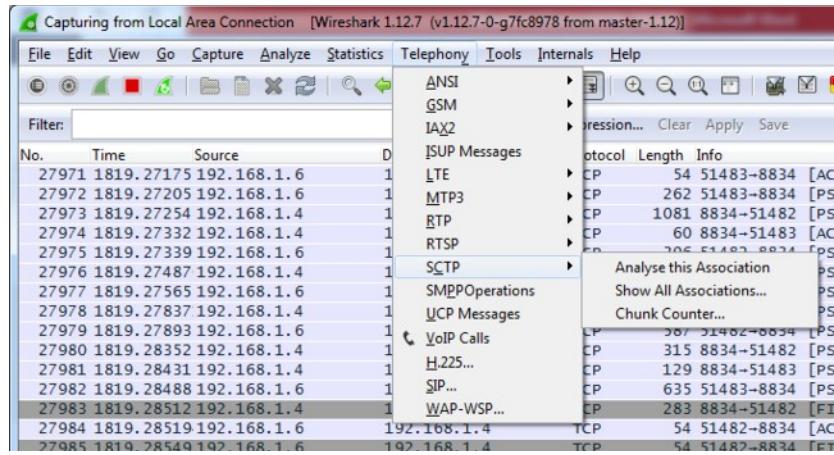
Хүснэгт 3.8. "Statistics" команд

Цэс	Гарын товчлуурын хослол	Тайлбар
<b>Summary</b>		Цуглувалж авсан өгөгдлийн талаарх мэдээллийг харуулна. <b>8.2. "Товч дүгнэлт (Summary" window)" хэсгээс</b>

		дэлгэрүүлэн үзнэ үү.
<b>Protocol Hierarchy</b>		Протоколын статистик мэдээллийн шаталсан бүтцийг мод (tree) хэлбэрээр харуулна. <b>8.3. “Протоколын шаталсан бүтэц (Protocol Hierarchy window)</b> хэсгээс дэлгэрүүлэн үзнэ үү.
<b>Conversations</b>		Харилцан мэдээлэл дамжуулсан 2 төгсгөлийн цэгүүдийн талаарх статистик мэдээллийг харуулна. <b>8.4.1. “Харилцан мэдээлэл солилцсон холболт (Conversations window)</b> ” хэсгээс дэлгэрүүлэн үзнэ үү.
<b>Endpoints</b>		Өгөгдөл дамжуулж буй эсвэл хүлээн авч буй төгсгөлийн цэгүүдийг (хаягийг) харуулдаг. <b>8.5.1. “Төгсгөлийн цэгүүд( Endpoints window)</b> ” хэсгээс дэлгэрүүлэн үзнэ үү.
<b>Packet Lengths...</b>		<b>8.10. “Тухайлан тодорхойлсон статистик (Protocol specified statistic)”</b> хэсгээс харна уу.
<b>IO Graphs</b>		Хэрэглэгчийн заасан дүрмийн дагуу график байгуулна. (жиш: Пакетын тоогоор). <b>8.6. “IO График (IO Graphs)”</b> хэсгийг харна уу.
<b>Conversation List</b>		Харилцан мэдээлэл солилцож байгаа мэдээллийн статистикийг харуулна. <b>8.4.3. “Протоколд харгалзуулсан тухайлан тодорхойлсон холболтыг жагсаан харуулах (Protocol specific Conversation List)</b> ” хэсгийг харна уу.
<b>Endpoint List</b>		Төгсгөлийн цэгүүдийг жагсаан харуулна. <b>8.5.3 “Протоколд харгалзуулсан тухайлан тодорхойлсон төгсгөлийн цэгүүдийг жагсаан харуулах (Protocol specific Endpoint List)</b> ” хэсгийг харна уу.
<b>Service Response Time</b>		Илгээж буй хүсэлт(request), түүний хариуд ирж байгаа хариу(response) 2-ын дунд хэр их хугацаа зарцуулагдаж байгааг харуулна. <b>8.7. “Үйлчилгээний хугацаа (Service Response Time)</b> ” хэсгийг харна уу.
<b>ANCP...</b>		<b>8.10. “Протоколд суурилан тодорхойлсон статистик (The protocol specific statistics windows)”</b> хэсгийг харна уу.
<b>BOOTP-DHCP...</b>		<b>8.10. “Протоколд суурилан тодорхойлсон статистик (The protocol specific statistics windows)”</b> хэсгийг харна уу.
<b>Collectedd...</b>		<b>8.10. “Протоколд суурилан тодорхойлсон статистик (The protocol specific statistics windows)”</b> хэсгийг харна уу.

Compare...		<b>8.10. “Протоколд суурилан тодорхойлсон статистик (The protocol specific statistics windows)”</b> хэсгийг харна уу.
Flow Graph...		<b>8.10. “Протоколд суурилан тодорхойлсон статистик (The protocol specific statistics windows)”</b> хэсгийг харна уу.
HTTP		HTTP хүлэлт/хариу (request/response)-ын статистик <b>8.10. “Протоколд суурилан тодорхойлсон статистик (The protocol specific statistics windows)”</b> хэсгийг харна уу.
IP Addresses...		<b>8.10. “Протоколд суурилан тодорхойлсон статистик (The protocol specific statistics windows)”</b> хэсгийг харна уу.
IP Destinations...		<b>8.10. “Протоколд суурилан тодорхойлсон статистик (The protocol specific statistics windows)”</b> хэсгийг харна уу.
IP Protocol Types...		<b>8.10. “Протоколд суурилан тодорхойлсон статистик (The protocol specific statistics windows)”</b> хэсгийг харна уу.
ONC-RPC Programs		<b>8.10. “Протоколд суурилан тодорхойлсон статистик (The protocol specific statistics windows)”</b> хэсгийг харна уу.
Sametime		<b>8.10. “Протоколд суурилан тодорхойлсон статистик (The protocol specific statistics windows)”</b> хэсгийг харна уу.
TCP Stream Graph		<b>8.10. “Протоколд суурилан тодорхойлсон статистик (The protocol specific statistics windows)”</b> хэсгийг харна уу.
UDP Multicast Streams		<b>8.10. “Протоколд суурилан тодорхойлсон статистик (The protocol specific statistics windows)”</b> хэсгийг харна уу.
WLAN Traffic		<b>8.9. “WLAN ургалын статистик (WLAN Traffic Statistics)”</b> хэсгийг харна уу
BOOTP-DHCP		<b>8.10. “Протоколд суурилан тодорхойлсон статистик (The protocol specific statistics windows)”</b> хэсгийг харна уу.

### 3.12. Telephony цэс



Зураг 3.10. "Telephony" команд

Telephony цэсийн тайлбарыг доорхи хүснэгтэд үзүүллээ.

Эдгээр командууд нь утсан харилцаа (telephony)-тай холбоотой статистикин мэдээллүүдийг тусдаа цонхонд харуулна.

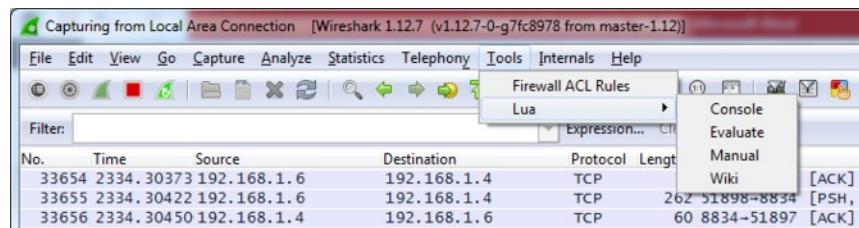
Хүснэгт 3.9. Telephony команд

Цэс	Гарын товчлуурын хослол	Тайлбар
IAX2		9.6. “Протоколд суурилсан статистик (Protocol specific statistics windows)” хэсгийг харна уу.
SMPP Operations..		9.6. “Протоколд суурилсан статистик (Protocol specific statistics windows)” хэсгийг харна уу.
SCTP		9.6. “Протоколд суурилсан статистик (Protocol specific statistics windows)” хэсгийг харна уу.
ANSI		9.6. “Протоколд суурилсан статистик (Protocol specific statistics windows)” хэсгийг харна уу.
GSM		9.6. “Протоколд суурилсан статистик (Protocol specific statistics windows)” хэсгийг харна уу.
H.225...		9.6. “Протоколд суурилсан статистик (Protocol specific statistics windows)” хэсгийг харна уу.
ISUP Messages...		9.6. “Протоколд суурилсан статистик (Protocol specific statistics windows)” хэсгийг харна уу.
LTE		9.4. “LTE MAC сүлжээний ургалын статистик (LTE MAC Traffic Statistics)” хэсгийг харна уу
MTP3		9.6. “Протоколд суурилсан статистик (Protocol specific statistics windows)” хэсгийг харна уу.
RTP		9.2. “RTP шинжилгээ (RTP Analysis)” хэсгийг харна уу
SIP...		9.6. “Протоколд суурилсан статистик (Protocol specific statistics windows)” хэсгийг харна уу.
UCP Messages...		9.6. “Протоколд суурилсан статистик (Protocol specific statistics windows)” хэсгийг харна уу.
VoIP Calls...		9.3. “VoIP дуудлага (VoIP Calls)” хэсгийг харна уу
WAP-		9.6. “Протоколд суурилсан статистик (Protocol specific statistics windows)” хэсгийг харна уу.

WSP...

windows)" хэсгийг харна уу.

### 3.13. Tools цэс

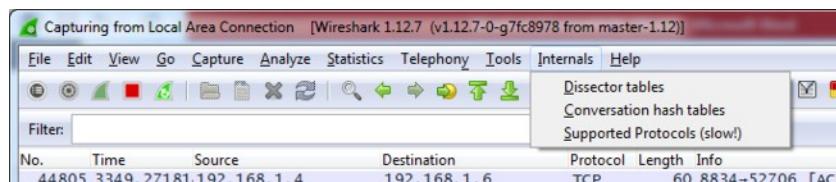


Зураг 3.11. Tools команд

Дараах хүснэгтэд tools цэсний тайлбарыг үзүүллээ.

Цэс	Гарын товчлуурын хослол	Тайлбар
Firewall ACL Rules		Энэ хэсгийг ашиглан Cisco IOS, Linux Netfilter (iptables), OpenBSD pf мөн Windows Firewall (via netsh) гэх мэт олон галт ханын (firewall) төхөөрөмжүүдэд текст хэрэглэгчийн горимоос (command line) ACL-н дүрмүүдийг үүсгэдэг. MAC хаяг, IPv4 хаяг, TCP болон UDP порт, мөн IPv4+порт гэх мэт зүйлсийг ашиглан дүрэм бичих боломжтой. Вайршарк (Wireshark) програм эдгээр дүрмүүдийг гадаад интерфэйс дээр биелнэ гэж үздэг.
Lua		Lua хөрвүүлэгч (Lua interpreter)-ийг вайршарк (wireshark) –д ашиглахад үүнийг хэрэглэнэ. Хэрэв дэлгэрүүлэн судлахыг хүсвэл хөгжүүлэгчдийн гарын авлага дээрээс “Lua Support in Wireshark” хэсгийг үзнэ үү.

### 3.14. Internals цэс



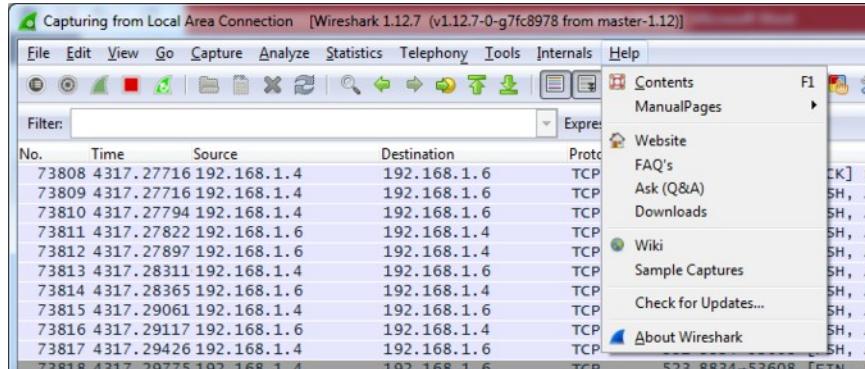
Зураг 3.12. Internals команд

Дараах хүснэгтээр Internals цэсийг тайлбарлалаа.

Цэс	Гарын товчлуурын хослол	Тайлбар
Dissector tables		Энэ цэс нь дэд задаргааны хоорондын хамаарлыг агуулсан хүснэгтийг харуулдаг.
Supported Protocols		Энэ цэс нь вайршарк (wireshark) програмын дэмжиж буй протоколууд тэдгээрийн талбаруудын талаарх мэдээллийг харуулдаг.

(slow!)

### 3.15. Help цэс



Зураг 3.13.

Дараах хүснэгтэд Help цэсний тайлбарлан үзүүллээ.

Цэс	Гарын товчлуурын хослол	Тайлбар
Contents	F1	Энгийн хэрэглээний туламжийн мэдээллийг харуулна.
Manual Pages > ...		Энэ хэсэг нь хэрэглэх зааврыг веб броузер ашиглан харуулна. (Локал дээр суусан байгаа хэрэглэх заавар (user guide)).
Website		Энэ цэс нь <a href="https://www.wireshark.org/">https://www.wireshark.org/</a> веб хуудсыг нээнэ.
FAQ's		FAQ асуултуудыг веб броузер дээр харуулна.
Downloads		Энэ цэс нь <a href="https://www.wireshark.org/">https://www.wireshark.org/</a> веб хуудсыг нээнэ.
Wiki		Энэ цэс нь <a href="https://wiki.wireshark.org/">https://wiki.wireshark.org/</a> веб хуудсыг нээнэ.
Sample Captures		Энэ хэсэг нь веб хуудас нээх ба энэ хуудас дээр жишээ болгон хэрэглэж болох сүлжээний пакет(packet) өгөгдлүүд байна. Энэ цэс нь <a href="https://wiki.wireshark.org/">https://wiki.wireshark.org/</a> веб хуудсыг нээнэ.
About Wireshark		Энэ сонголт нь вайршарк (wireshark) програмын талаар мэдээллийг дэлгэрэнгүйгээр өгнө. Жишээлбэл: Вайршарк (wireshark)-г хэрхэн суулгасан (build), ямар ямар нэмэлт залгаасууд (plug-ins) ачааллагдсан байгаа гэх мэт ...

Веб броузер нээх үйлдэл нь таны хэрэглэж буй вайршарк (wireshark) дээр дэмжигдээгүй байвал харгалзах хэсэг нь харагдахгүй болсон байна. Эсвэл сонгож болж байгаа хэдий ч веб броузер тань хариу үйлдэл үзүүлэхгүй байвал та веб броузерийнхээ тохиргоог харна уу.

### 3.16. Үндсэн товчлуурууд (Main Toolbar)

Үндсэн товчлуурууд (Main toolbar) нь хэрэглэгчдийн байнга хэрэглэдэг функцийг товчлуур болгон агуулсан байдаг ба эдгээр нь байнга хэрэглэдэг функциудаа хурдан сонгох боломжийг олгоно. Энэхүү товчлууруудыг (toolbar) хэрэглэгч өөрийн хүсснээр өөрчлөх боломжгүй хэдий ч **View** цэсний тохиргоог ашиглан дэлгэцэнд харагдахгүй болгон тохируулж болно.

Цэсний сонголтууд (Menu options)-ийн адил програмын одоогийн төлөвт биелэх боломжтой товчлуурууд нь дарагдах ба бусад нь саарал болсон байх ба биелүүлэгдэх боломжгүй байна. (Жишээлбэл: Пакет (packet) өгөгдөл чагнаж цуглуулах процесс хийгээгүй бол хадгалар товчлуур саарал өнгөтэй байна.)



Зураг 3.14. Үндсэн toolbar-г харуулсан байдал

Товчлуур	Товчлуурын нэр	Харгалзах цэсний сонголт	Тайлбар
	Interfaces...	Capture/Interfaces...	Энэ товчлуур нь Сүлжээний орчинд чагнах боломжтой байгаа интерфэйсүүдийг жагсаан харуулна. <b>4.3. “Чагнах процесс эхлүүлэх (Start Capturing)”</b> хэсгийг үзнэ үү.
	Options...	Capture/Options...	Энэ хэсэг нь сүлжээг чагнах сонголтуудыг харуулна. <b>4.3. “Чагнах процесс эхлүүлэх (Start Capturing)”</b> хэсгийг үзнэ үү. Энэ хэсгээс та пакет (packet) чагнах үйлдлийг эхлүүлэх боломжтой
	Start	Capture/Start	Энэ хэсэг нь хамгийн сүүлд өгсөн тохиргоог ашиглан пакет (packet) чагнах процессыг эхлүүлнэ.
	Stop	Capture/Stop	Сүлжээг чагнаж буй үйлдлийг зогсоно.
	Restart	Capture/Restart	Энэ сонголт нь сүлжээг чагнах процессыг зогсоож дахин эхлүүлнэ.
	Open...	File/Open...	Файл нээх үйлдлийг хийх цонхыг нээнэ. Үүнийг ашиглан өмнө нь хадгалсан файлуудаа нээж үзэх боломжтой. <b>5.2.1. “Цуглуулсан файл нээх (Open Capture File)”</b> хэсгийг үзнэ үү
	Save As...	File/Save As...	Одоо ачааллагдсан байгаа пакет (packet) өгөгдлийг өөрийн хүссэн файлын өргөтгөлтэйгээр хадгалах боломжийг олгоно. Энэ товчлуур нь Цуглуулсан Файлыг хадгалах цонхыг нээдэг. <b>5.3.1. “Цуглуулсан файлыг хадгалах (Save Capture File)”</b> хэсгийг үзнэ үү.
	Close	File/Close	Нээлттэй байгаа цуглуулсан пакет (packet)-уудыг хаана. Хэрэв хадгалж амжаагүй бол

			хадгалах эсэхийг асуусан цонхыг харуулна.
	<b>Reload</b>	View/Reload	Дэлгэцэнд харж буй ачааллагдсан пакет (packet) өгөгдлийг дахин ачааллана.
	<b>Find Packet...</b>	Edit/Find Packet...	Пакет (packet) хайх цонхыг нээнэ. <b>6.8. “Пакет хайх (Finding packets)”</b> хэсгийг үзнэ үү
	<b>Go Back</b>	Go/Go Back	Пакетын түүх хуудас (packet history)-д бичигдсэн байгаа өмнөх пакет (packet) дээр очно.
	<b>Go Forward</b>	Go/Go Forward	Пакетын түүх хуудас (packet history)-д бичигдсэн байгаа дараагийн пакет (packet) дээр очно.
	<b>Go to Packet...</b>	Go/Go to Packet...	Пакет (packet)-ын дугаараар тухайн пакет (packet) дээр очно.
	<b>Go To First Packet</b>	Go/First Packet	Цуглувансан пакет (packet)-уудын хамгийн эхний пакет (packet) дээр очно.
	<b>Go To Last Packet</b>	Go/Last Packet	Цуглувансан пакет (packet)-уудын хамгийн сүүлийн пакет (packet) дээр очно.
	<b>Colorize</b>	View/Colorize	Пакет (packet)-уудыг өнгөөр ялгах/өнгөөр ялгахыг болиулах үйлдлийг хийнэ.
	<b>Auto Scroll in Live Capture</b>	View/Auto Scroll in Live Capture	Сүлжээг чагнаж байх үед пакетуудыг жагсаан харуулах самбар (packet list pane)-т байгаа пакетуудын хамгийн сүүлийн packet-ийг дэлгэцэнд багтаан харуулах.
	<b>Zoom In</b>	View/Zoom In	Үсгийн фонт томруулах
	<b>Zoom Out</b>	View/Zoom Out	Үсгийн фонт жижигрүүлэх
	<b>Normal Size</b>	View/Normal Size	Үсгийн фонт хэвийн хэмжээтэй болгох
	<b>Resize Columns</b>	View/Resize Columns	Багануудын хэмжээг дахин өөрчлөх, ингэснээр багануудын агуулга нь баганад яг таарна
	<b>Capture Filters...</b>	Capture/Capture Filters...	Сүлжээний интерфэйсийг чагнах үед шүүлтүүр ажиллуулах цонхыг нээнэ. Эндээс та шинэ шүүлтүүрийн дүрэм үүсгэх, түүндээ нэр өгөх, хадгалах үйлдлүүдийг хийх боломжтой. <b>6.6. “Шүүлтүүрийг тодорхойлох, хадгалах (Defining and saving filters)”</b> хэсгээс дэлгэрүүлэн үзнэ үү.
	<b>Display Filters...</b>	Analyze/Display Filters...	Энэ товчлуур нь дэлгэцэнд харуулах пакет (packet)-уудыг шүүлтүүрээр оруулах цонхыг харуулна. Мөн та шинэ шүүлтүүрийн дүрэм үүсгэх түүндээ нэр өгөн хадгалах боломжтой. <b>6.6. “Шүүлтүүрийг тодорхойлох, хадгалах (Defining and saving filters)”</b> хэсгээс

			дэлгэрүүлэн үзнэ үү.
	<b>Coloring Rules...</b>	View/Coloring Rules...	Энэ товчлуур нь хэрэглэгчийн сонгосон шүүлтүүрийн дагуу пакет (packet)-уудыг өнгөөр ялгах үйлдлийг хийдэг. Эндээс та шинээр өнгөөр ялгах дүрэм бичих, хуучин дүрмийг өөрчлөх гэх мэт үйлдлүүдийг хийх боломжтой. Олон пакет (packet) өгөгдөл байгаа үед ингэж өнгөөр ялгаж харах нь ажлыг маш ихээр хөнгөвчилдэг. 10.3. “Пакет өнгөөр ялгах (Packet colorization)” хэсгээс дэлгэрүүлэн үзнэ үү.
	<b>Preferences..</b>	Edit/Preferences	Энэ товчлуур нь вайршарк (wireshark) программыг удирдах параметрүүдийг тохируулах боломжийг олгоно. Өөрийн хүссэн тохиргоог хийх, түүнийгээ хадгалах гэх мэт үйлдлүүдийг хийх боломжтой. <b>10.5. “Тохиргоо (Preferences)”</b> хэсгээс дэлгэрүүлэн үзнэ үү.
	<b>Help</b>	Help/Contents	<b>Help</b> цэсэнд байрлах хэрэглэгчид туслах зориулалттай вайршарк (wireshark)-ыг хэрхэн хэрэглэх талаарх мэдээллийг үзүүлнэ.

### 3.17. Шүүлтүүрийн товчлуур (Filter toolbar)

Шүүлтүүрийн товчлуур (Filter toolbar)-ыг ашиглан пакетуудыг жагсаан харуулах самбар (Packet List Pane)-т байх пакет (packet) өгөгдлүүдийг тодорхой түлхүүр үгүүд, дүрмүүдэд тохируулах шүүн харах боложмтой юм. Энэ хэсгийг дэлгэцэнд харуулснаар хэрэглэгчид шүүлтүүрийг ашиглахын тулд **Analyze→Filter** хэсэг рүү хандаж цаг алдалгүй хурдан хугацаанд шууд үндсэн дэлгэцэн дээрээс шүүлтүүрийн түлхүүр үгийг өөрчлөх, идэвхижүүлэх боломжийг олгодог. **6.3. “Пакетыг шүүн харах (Filtering packets while viewing)”** хэсгээс дэлгэрэгүйгээр харах боломжтой.



Зураг 3.15. Filter toolbar

Хүснэгт. Шүүлтүүрийн товчлуурууд

Товчлуур	Товчлуурын нэр	Тайлбар
----------	----------------	---------

	Filter:	Шүүлтүүрийн бүтцийн цонхыг дэлгэцэнд харуулна. Цонхыг Зураг 6.8-д үзүүллээ.
	Filter input	<p>Дэлгэцэнд харуулж буй пакет (packet) өгөгдлүүдийг шүүж харах шүүлтүүрийн түлхүүр үгийг оруулах, өөрчлөх, засварлах хэсэг. Таны оруулсан шүүлтүүрийн түлхүүр үг буруу эсвэл дутуу байгаа тодхиолдолд энэ хэсгийн арын суурь өнгө улаан болно. Харин түлхүүр үг, шүүлтүүрийн дүрмээ зөв, бүрэн оруулахад энэ хэсгийн арын суурь өнгө ногоон болно. Баруун гар талд байрлах доошоо заасан сумны дүрс нь өмнө нь хэрэглэсэн шүүлтүүрүүд (recent)-ийн түлхүүр үгсийг танд санал болгодог.</p> <p><b>6.4. “Дэлгэцийн шүүлтүүрийг үүсгэх “Building display filter expression” хэсгээс илүү дэлгэрэнгүй харна уу.</b></p> <p>Дэлгэцэнд байгаа пакет (packet) өгөгдлийг шүүхэд хэрэглэгдэж буй дүрэм мөн энэхүү талбар дээр харагддаг.</p> <p>Энэ хэсэгт өөрчлөлт оруулсны дараа Apply товчыг дарах эсвэл Enter гарын товчийг дарж тухайн шүүлтүүрээ идэвхижүүлэх хэрэгтэй.</p>
	Expression. ..	<p>Энэ хэсэг нь төрөл бүрийн протоколуудын талбариудыг жагсааж харуулдаг. Эдгээр талбариудыг та өөрийн шүүлтүүрийн түлхүүр үгээр сонгон дэлгэцэнд байгаа пакет (packet) өгөгдлүүдийг шүүн харах боломжтой.</p> <p><b>6.5. “Шүүлтүүрийн түлхүүр үгс (Filter expression)” хэсгээс дэлгэрэлүүлэн уншина уу.</b></p>

	Clear	Идэвхитэй байгаа шүүлтүүрийн тохиргоог байхгүй болгох, шүүлтүүрийн түлхүүр үг оруулах хэсгийг цэвэрлэнэ. Түүнээс гадна дэлгэцэнд байгаа пакет (packet) өгөгдлүүдийг ямар нэгэн шүүлтүүргүйгээр харуулна.
	Apply	Шүүлтүүрийн түлхүүр үг оруулах хэсэгт оруулсан байгаа дүрмийг идэвхижүүлнэ.
	Save	Энэ товчлуурыг ашиглан одоо хэрэглэж буй шүүлтүүрийн дүрэмд нэр өгч хадгалдаг.

### 3.18. Пакетыг жагсаан харуулах самбар (Packet list pane)

Ачааллагдсан байгаа пакет (packet) өгөгдлийн бүх пакетыг жагсаалт (list) хэлбэрээр харуулдаг цонхыг пакетыг жагсаан харуулах самбар (Packet List Pane) гэдэг. Өөрөөр хэлбэл хэрэв пакет өгөгдлөтэй файл нээсэн бол тухайн файлд байгаа пакетуудыг, эсвэл сүлжээний интерфэйсээс пакет чагнаж байгаа бол цуглуулсан бүх пакетуудыг энэ цонх тоймлон жагсаалт хэлбэрээр харуулдаг гэсэн үг.

No.	Time	Source	Destination	Protocol	Length	Ethernet	Frame	Internet Protocol Version 4	Frame	Transmission Control Protocol	Info
1297	1:485,344219000	192.168.1.3	173.192.82.194	TCP	72	Yes	Yes	Yes	Yes	49442-80 [PSH, ACK] Seq=889 Ack=297 Win=4089 Len=6 tsval=909	
1298	1:494,557095000	52.7.49.61	192.168.1.4	TCP	60	Yes	Yes	Yes	Yes	80-49204 [FIN, ACK] Seq=222 Ack=4118 Win=27520 Len=0	
1299	1:494,558095000	192.168.1.4	52.7.49.61	TCP	34	Yes	Yes	Yes	Yes	49204-80 [ACK] Seq=4118 Ack=223 Win=261888 Len=0	
1300	1:494,558095000	192.168.1.3	173.192.82.194	TCP	60	Yes	Yes	Yes	Yes	49442-80 [PSH, ACK] Seq=4119 Ack=298 Win=4088 Len=6 tsval=909	
1301	1:494,558095000	192.168.1.3	173.192.82.194	TCP	72	Yes	Yes	Yes	Yes	13442-80 [PSH, ACK] Seq=885 Ack=299 Win=4088 Len=6 tsval=909	
1302	1:504,380197000	192.168.1.3	173.192.82.213	TCP	188	Yes	Yes	Yes	Yes	[TCP Retransmission 49008-512.2 [FIN, PSH, ACK] Seq=4019 Ack=	
1304	1:505,310210000	192.168.1.3	173.192.82.194	TCP	66	Yes	Yes	Yes	Yes	49442-80 [ACK] Seq=901 Ack=301 Win=4088 Len=0 Tsvval=00912928	
1305	1:505,311152000	192.168.1.3	173.192.82.194	TCP	72	Yes	Yes	Yes	Yes	49442-80 [PSH, ACK] Seq=901 Ack=301 Win=4088 Len=6 tsval=909	
1306	1:509,884589000	192.168.1.4	202.70.32.11	DNS	120	Yes	Yes	Yes	Yes	standard query 0x2a23 SRV _ldap._tcp.Default-FIRST-SITE-NAM	
1307	1:510,225915000	192.168.1.4	173.192.82.194	TCP	12	Yes	Yes	Yes	Yes	Standard query response 0x2a23	
1308	1:510,225915000	192.168.1.4	173.192.82.194	TLSv1.2	323	Yes	Yes	Yes	Yes	Encrypted Alert	
1309	1:510,225915000	192.168.1.4	173.192.82.194	TLSv1.2	123	Yes	Yes	Yes	Yes	Encrypted Alert	
1310	1:510,225915000	54.85.156.219	192.168.1.4	TLSv1.2	123	Yes	Yes	Yes	Yes	Encrypted Alert	
1311	1:510,226099000	192.168.1.4	54.85.156.219	TCP	34	Yes	Yes	Yes	Yes	49201-443 [ACK] Seq=884 Ack=15591 Win=280608 Len=0	
1312	1:510,226235000	192.168.1.4	54.85.156.219	TCP	34	Yes	Yes	Yes	Yes	49202-443 [ACK] Seq=884 Ack=15599 Win=261888 Len=0	
1313	1:510,2263516000	192.168.1.4	54.85.156.219	TCP	34	Yes	Yes	Yes	Yes	49200-443 [ACK] Seq=884 Ack=15575 Win=261888 Len=0	
1314	1:510,227283000	192.168.1.4	202.70.32.11	DNS	60	Yes	Yes	Yes	Yes	Standard query response 0x2a23 SRV _ldap._tcp.dc._msdcs.test.com	
1315	1:510,580770000	202.70.32.11	192.168.1.4	DNS	148	Yes	Yes	Yes	Yes	Standard query response 0x2a23 SRV _ldap._tcp.dc._msdcs.test.com	
1316	1:510,540038000	192.168.1.4	202.70.32.11	DNS	131	Yes	Yes	Yes	Yes	Standard query response 0x2a23 SRV _ldap._tcp.f09ade06-2302-4139-87b	
1317	1:510,8422638000	202.70.32.11	192.168.1.4	DNS	190	Yes	Yes	Yes	Yes	Standard query response 0x51da	

Зураг 3.16. Пакетуудыг жагсаан харуулах самбар (Packet List Pane цонх)

Энэ хэсэгт харагдаж буй пакетууд дундаас та аль нэгийг нь сонговол Пакетыг дэлгэрэнгүй харуулах самбар (Packet Details) мөн Пакетын мэдээллийг байтаар харуулах самбар (Packet Bytes) хэсгүүдэд тухайн сонгосон пакетын мэдээллийг дэлгэрэнгүйгээр харуулдаг.

Энэ хэсэгт пакет доторх өгөгдлийг задлан харуулахдаа протоколуудын задаргааны талбаруудын мэдээллийг ашигладаг. Гэхдээ дээд түвшний протоколууд нь өөрсдийн мэдээллийг бичихдээ харгалзах доод түвшний протоколуудын мэдээллийг дарж бичдэг. Тиймээс энэ хэсгийн багануудын мэдээлэл нь ихэвчлэн дээд түвшний протоколууд байна.

Жишээлбэл: TCP Packet –ын дотор IP Packet. Харин IP Packet Дотор Ethernet Packet байна. Ethernet протоколыг задалж буй хэсэг нь Ethernet протоколын өгөгдлийг (Ethernet address)

бичиж байхад, IP Packet -ын түвшинд эдгээр хэсгийг IP Packet-ын задаргааны хэсгүүдэд (IP address) хуваан дарж бичнэ. Үүнээс дээшлээд TCP packet –ын түвшинд задлах хэсэг нь TCP packet-ын өгөгдлөөр задлах гэх мэтчилэн дарааллуулан задалдаг.

Пакетыг жагсаан харуулах самбар (Packet List Pane)-т маш олон багануудыг харах боломжтой. Ямар ямар багануудыг харах вэ гэдгээ тохиргоо өөрчлөх (Preference Settings) хэсгээнс хийнэ. Тохиргооны талаар дэлгэрэнгүй мэдэхийг хүсвэл 10.55 “Тохиргоо (Preferences)” хэсгээс харна уу.

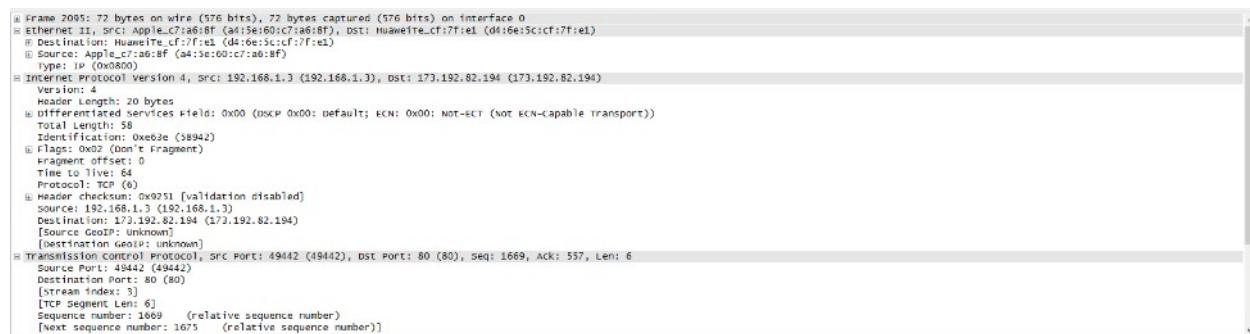
Өгөгдмөл тохиргоогоор харуулж буй багануудын тайлбарыг дор үзүүллээ.

- **No:** Цуглуванс пакет өгөгдлүүдийн дугаарлалт. Эдгээр дугаарлалт нь өөрчлөлгддэггүй. Шүүлтүүрийн тохиргоо хийж дэлгэцэнд байгаа бүх пакетуудыг шүүж харуулсан ч гэсэн өмнөх дугаарлалтаар хэдээр дугаарлагдсан тэр дугаарыг харуулдаг.
- **Time:** Пакетын цагийн мэдээлэл. Пакетын цагийн мэдээллийг төрөл бүрийн форматаар харах боломжтой. Энэхүү тохиргоог хэрхэн тохируулахыг **6.12 .“Цагийг харуулах формат болон цагийн тохируулга (Time display formats and time references)** хэсгээсээс харна уу.
- **Source:** Пакетыг илгээгч талын хаяг.
- **Destination:** Пакетыг хүлээн авч буй талын хаяг.
- **Protocol:** Протоколын нэр, хувилбарын мэдээлэл.
- **Info:** Пакетын бүтцийн талаарх нэмэлт дэлгэрэнгүй мэдээлэл.

Баганууд дээр хулганы заагчийг аваачин баруун товчийг дарснаар багана дотор агуулагдах мэдээллийг өөрчлөх, тохируулах үйлдлүүдийг хийж болдог. **6.4. “Пакетыг жагсаан харуулах хэсэгт ил гарах цэс (Pop-up menu of the Packet list pane)** хэсгээс ямар ямар тохиргоог хийх боломжтойг харна уу

### 3.19. Пакетын дэлгэрэнгүй мэдээллийг харуулах самбар (Packet Details pane)

Энэ самбар нь пакетыг жагсаан харуулах самбарт (Packet List Pane) идэвхижсэн байгаа пакетын мэдээллийг илүү дэлгэрэнгүйгээр харуулдаг.



Зураг 3.17. Пакетын мэдээллийг дэлгэрэнгүй харуулах самбар (Packet Details Pane)

Энэ хэсэгт Вайршарк програм нь Пакетыг жагсаан харуулах самбар (Packet List Pane) цонхонд идэвхижсэн байгаа пакетын протокол, протоколын талбаруудын мэдээллийг мод (tree) хэлбэрийн бүтэцтэй байдлаар харуулна.

Энэ самбарт байх мэдээлэл дээр хулганы заагчийг аваачин баруун товчийг дарснаар доторх мэдээллийг ашиглах, мөн програмыг тохируулахдаа эдгээр мэдээллийг ашиглах зэрэг нэмэлт үйлдлүүдийг хийж болдог.

Зарим протоколын талбаруудыг тусгайлан харуулдаг.

- Үүсгэсэн талбарууд (Generated fields):** Хаалтаар тусгаарлагдсан талбарыг Вайршарк програм үүсгэдэг. Энэхүү талбар доторх мэдээлэл нь пакет өгөгдөл доторх мэдээллээс ялган авсан мэдээлэл байдаг. Жишээлбэл: Вайршарк програм нь TCP Packet өгөгдлүүдийн sequence/acknowledge analysis мэдээллийг TCP протоколын [SEQ/ACK analysis] талбарт харуулдаг.
- Холбоосууд (Links):** Вайршарк програм тухайн пакетыг өөр пакеттай холбогдож байгааг илрүүлвэл тухайн холбогдож буй пакет руу очих холбоосыг үүсгэнэ. Холбоос нь ийм хэлбэртэй байх ба тухайн пакет руу очихын тулд холбоос дээр 2 удаа дарах хэрэгтэй.

### 3.20. Пакетын мэдээллийг байтаар харах самбар (Packet Bytes pane)

Энэ цонх нь Пакетыг жагсаан харуулах самбарт идэвхижсэн байгаа пакетын өгөгдлийг хекс (hex) буюу 16-тын тоогоор харуулдаг.

0000	00	50	56	f2	d4	3b	00	0c	29	73	2a	c5	08	00	45	00	.PV..;... )s*...E.
0010	00	28	3f	81	40	00	80	06	00	00	c0	a8	91	a2	c0	e5	.(?.@... .....:
0020	91	c8	c0	3d	00	50	07	91	c1	0b	87	fe	d2	d2	50	10	...=.P.. .....P.
0030	fa	f0	a5	13	00	00											.....

Зураг 3.18. Packet Bytes Pane

Энэ цонхны хамгийн зүүн талд нь оффсет (offset) хаяг нь дунд хэсэгт пакетын өгөгдөл хекс (hex) хэлбэрээр харин баруун талд нь тухайн хекс (hex)-д харгалзах ASCII тэмдэгтийг харуулдаг.

Пакет өгөгдлийн хэмжээнээс хамаараад энэ хэсэг нь олон хуудас мэдээллээс бүрдэх тохиолдол байдаг. Жишээлбэл Packet Reassembly буюу пакетуудын өгөгдлийг нэгтгэн нэг өгөгдөл болгох гэх мэт. Энэ тохиолдолд энэхүү самбарын доод талд нь нэмэлт сонгох хэсэг (tab) гарч ирэх ба та энэ хэсгээс өөрийн харахыг хүсч буй хуудсаа харах сонгон харах боломжтой юм. Нэмэлт хуудсуудад агуулагдах мэдээллүүд нь олон пакетуудын өгөгдлүүдийг агуулсан байх магадлалтай.

Frame (114 bytes)	Reassembled TCP (56120 bytes)	De-chunked entity body (55483 bytes)
-------------------	-------------------------------	--------------------------------------

Зураг 3.19. Олон хуудас пакет өгөгдлийг харуулах нэмэлт самбар (additional tab)

Хулганы баруун товчийг дарах үед гарч ирэх цэс байх бөгөөд эдгээр нь боломжит бүх хуудсуудыг жагсаан харуулдаг. Хэрэв энэхүү талбарын хэмжээ нь бүх хуудсуудыг харуулах боломжгүй жижигхэн байгаа бол энэхүү сонголтыг хийж бүх хуудсыг харах боломжтой юм.

### 3.21. Статусбар (Statusbar)

Төлөв байдлын самбар нь хэрэглэгчид төлөв байдлыг мэдээллэдэг.

Ерөнхийдөө зүүн талын самбар нь агуулгатай холбоотой мэдээллийг, дунд хэсэгт пакетын тоог харин баруун талын хэсэгт идэвхитэй байгаа профайл тохиргооны талаарх мэдээллийг тус тус өгдөг.



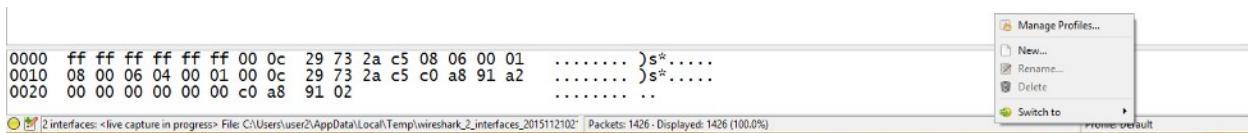
Зураг 3.20. Програмыг эхлүүлэх уеийн төлөвийн самбар



Зураг 3.21. Програмд пакет ачаалласан уеийн төлөвийн самбар

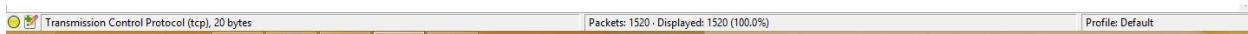
- Өнгөт бөмбөлөг (Colorized bullet):** Зүүн талын өнгөтэй бөмбөлөг нь одоогийн цуглуулагдсан файлд олсон хамгийн өндөр мэргэжлийн түвшний (expert info level) мэдээллийг харуулдаг. Энэ бөмбөлөгийн дүрс дээр хулганы заагчийг аваачсанаар мэргэжлийн түвшний мэдээллийн тодорхойлолтыг харуулдаг бөгөөд энэ бөмбөлөгийн дүрс дээр дарснаар энэ нь мэргэжлийн мэдээллийн (Expert Infos dialog) цонхыг гаргаж ирдэг. Дэлгэрүүлэн уншихыг хүсвэл 7.3. “Мэргэжлийн мэдээлэл (Expert Information)” хэсгийг үзнэ үү.
- Зүүн хэсэг (Left side):** Энэ хэсэг нь чагнасаж цуглуулсан файлын талаарх мэдээллийг, файлын нэр, файлын хэмжээ цуглуулж эхэлснээс хойш хэр их хугцаа өнгөрсөн зэрэг мэдээллийг харуулна.
- Дунд талын хэсэг (Middle part):** Энэ хэсэг нь цуглуулсан файлд байгаа пакетын тоог харуулдаг. Дараах утгуудыг харуулдаг.
  - Пакет:** Чагнасан файлын тоо
  - Дэлгэцэнд харуулсан (Displayed):** Энэ хэсэг нь одоогоор дэлгэцэнд харуулж буй пакетуудын тоо
  - Тэмдэглэсэн (Marked):** Тэмдэглэгээ хийсэн пакетын тоо
  - Гээгдүүлсэн (Dropped):** Гээгдүүлсэн пакетын тоо (Вайршарк програм бүх пакетыг барьж чадахгүй байгаа тохиолдолд харуулдаг)

- **Үл ойшоосон (Ignored):** Үл ойшоосон пакетын тоо (Вайршарк програм дээр ямар нэгэн пакетыг үл ойшоосон тохиолдолд харуулдаг)
- **Баруун тал (Right side):** Тохируулагдсан байгаа профайлын нэрийг харуулдаг. Энэ хэсэг дээр дарснаар статусбар нь профайл тохируулах цэсийг гаргаж ирэх ба энэхүү гарч ирсэн жагсаалтаас сонгох замаар профайлын тохиргоог солих боломжтой.



*Зураг 3.22. Профайл тохиргоог харуулсан статусбар*

Профайл тохиргооны тодорхойлолтын талаарх дэлгэрэнгүй мэдээллийг **10.6. “Профайл тохиргоо (Configuration Profiles)”** хэсгээс үзнэ үү.



*Зураг 3.23. Протоколын талбарыг идэвхижүүлсэн үеийн статусбар*

Зураг 3.23 хэсэгт үзүүлсэн статусын мэдээлэл нь зөвхөн Пакетын мэдээллийг дэлгэрэнгүй үзүүлэх самбар (Packet Details pane) –т ямар нэгэн протоколын талбарыг идэвхижүүлсэн үед харагдана.

Хаалтанд байгаа утга (жишээлбэл дээрх зурагны tcp)-ыг дэлгэцийн пакетуудыг шүүн харах түлхүүр үг болгон ашиглаж болно.



*Зураг 3.24. Дэлгэцийн пакетуудыг шүүх шүүлтүүрийг идэвхижүүлсний дараах статусбарын харагдах байдал*

Энэ мэдээлэл нь дэлгэцийн түлхүүр үг нь таны хүсээгүй үр дүнг өгч болзошгүй байгаа үед гарч ирдэг. Дэлгэрэнгүй мэдээлэл үзэхийг хүсвэл **6.4.4. “Нийтлэг алдаанууд (Common mistake)”** хэсгийг үзнэ үү

## **БҮЛЭГ IV**

### **4. СҮЛЖЭЭН ДЭЭГҮҮР ДАМЖИЖ БУЙ ӨГӨГДЛИЙГ ШУУД ЧАГНАХ**

#### **4.1. Танилцуулга**

Сүлжээний интерфэйс дээр одоо дамжиж байгаа өгөгдлийг шууд чагнах нь вайршарк програмын функцүүдийн үндсэн функцүүдийн нэг юм.

Вайршарк програмын пакет чагнах функц дараах зүйлсийг хийх хүчин чадалтай:

- Этернет (Ethernet) эсвэл 802.11 гэх мэт өөр өөр сүлжээний техник хангамжаас сүлжээг чагнана.
- Өөр өөр хүчин зүйлээс хамааруулан чагнах үйлдлийг зогсоно. (Эдгээр хүчин зүйлд цутгуулсан файлын хэмжээ, сүлжээг чагнасан цаг эсвэл пакетын тоо гэх мэт)
- Вайршарк програм пакет чагнаж байх үед нэгэн зэрэг пакетуудыг задалж харуулдаг.
- Чагнах пакетуудыг шүүлтүүрээр оруулна. Ингэснээр нийт чагнах пакетын хэмжээг багасгана. **4.13. “Чагнах үед шүүлтүүр хэрэглэх (Filtering while capturing)”** хэсгээс дэлгэрүүлэн үзнэ үү.
- Удаан хугацаанд пакет чагнах үед пакетуудыг өөр олон файлаар эргэлдэх байдлаар явж болдог. **4.11. “Файл чагнах мөн файлын төрлүүд (Capture files and file modes)”** хэсгээс дэлгэрүүлэн үзнэ үү.
- Олон интерфэйсээс нэгэн зэрэг пакет чагнах

Пакет чагнах функц нь дараах үйлдлийг хийхгүй:

- Чагнасан өгөгдөл дээр суурилан чагнах процессыг зогсоох (эсвэл өөр үйлдэл хийх).

#### **4.2. Урьдач нөхцөл (Prerequisite)**

Вайршарк програмыг ашиглан анх удаа пакет чагнах үед танд эргэлзээтэй асуудлууд үүсэх магадлалтай юм. Хэрхэн чагнах үйлдлийг тохируулах, эхлүүлэх талаар дэлгэрэнгүй зааврыг <https://wiki.wireshark.org/CaptureSetup> хэсгээс үзнэ үү.

Нийтлэг тулгардаг зарим асуудлыг дор харууллаа.

- Сүлжээг чагнахын тулд танд тусгай эрх шаардлагатай болж магадгүй (Special privilege)
- Сүлжээний пакетыг чагнахдаа зөв интерфэйсээ сонгосон байх шаардлагатай
- Сүлжээний урсгалыг харахын тулд сүлжээний зохион байгуулалтын хувьд зөв байрлалд суусан байх шаардлагатай болдог.

Хэрэв эдгээр тохиргоотой холбоотой асуудал үүссэн гэж үзэж байвал дээр дурдсан зааврыг үзнэ.

#### **4.3. Чагнах функцийг эхлүүлэх**

Дараах аргуудыг ашиглан вайршарк програмаар пакет чагнах үйлдлийг эхлүүлж болдог.

- Үндсэн цонх дээр харагдах интерфэйс дээр хулганыг 2 удаа дарах
- Чагнах боломжтой интерфэйсүүдийн талаарх мэдээллийг харах боломжтой. Ингэхдээ (**Capture → Options**) –ийг ашиглана. Зураг 4.1. –д Виндовс орчинд Интерфэйс чагнах үйлдэл хэрхэн эхлүүлэхийг, Зураг 4.2.-т Линукс/Юникс орчинд Интерфэйс чагнах үйлдэл эхлүүлэхийг тус тус харуулсан. Та энэхүү зурагт үзүүлсэн хэсэгт байрлах **Эхлүүлэх (Start)** товчлуурыг дарж чагнах процессийг эхлүүлж болно.
- Одоогоор идэвхитэй байгаа тохиргооны дагуу чагнах бол та **Capture → Start** эсвэл эхний товчлуур (first toolbar)-г дарж шууд чагнах процессийг эхлүүлж болно.
- Хэрэв чагнах интерфэйсийнхээ нэрийг мэдэж байгаа бол командын горимоос дараах командыг ашиглан чагнах процессийг эхлүүлж болно.

```
$ wireshark -I eth0 -k
```

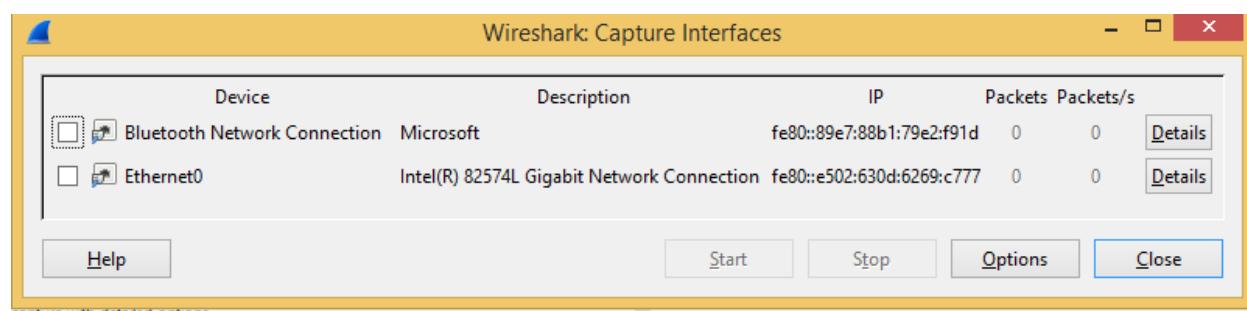
Энэ команд нь вайршарк програмын чагнах процессийг **eth0** интерфэйс дээр эхлүүлнэ. Дэлгэрүүлэн уншихыг хүсвэл **10.2. “Вайршарк програмыг командын горимоос эхлүүлэх (Start Wireshark from the command line)”** хэсгийг үзнэ үү.

#### 4.4. Интерфэйсүүд чагнах (**Capture Interfaces**)

Вайршарк програмын үндсэн цэсний хэсгээс **Capture → Options** –г сонгох үед танд **Чагнах интерфэйсүүд (Capture Interfaces)** цонх харагдана. Энэ цонхны зургийг Виндовс орчинд бол зураг 4.1.-ээс Линукс/Юникс орчинд бол 4.2.-оос тус тус харж болно.

Хэрэглэгч өөрөө эсвэл хэрэглэгчийн үйлдлийн систем нь интерфэйсийг харагдуулахгүй болгон нууж болдог. Дээрх цонх нь Вайршарк програм хандах боломжтой дотоод интерфэйс (Local Interfaces)-үүдийг л харуулдаг. Энэ хэсэг нь мөн **10.5.1. “Интерфэйсийн сонголтууд (Interface Options)”** хэсэгт нуугдсан (hidden) гэж тэмдэглэгдсэн интерфэйсүүдийг нуудаг. Түүнчлэн Вайршарк програм бүх дотоод интерфэйсүүдийг илрүүлж харж чадахгүй байх боломжтой бөгөөд алсын зайд (remote) байгаа хэдий ч чагнах боломжтой интерфэйсүүдийг илрүүлж чадахгүй.

Нэгээс олон интерфэйс сонгож бүгдийг нь зэрэг чагнах боломжтой.



Зураг 4.1. Виндовс орчинд Интерфэйсүүдийг чагнах цонх



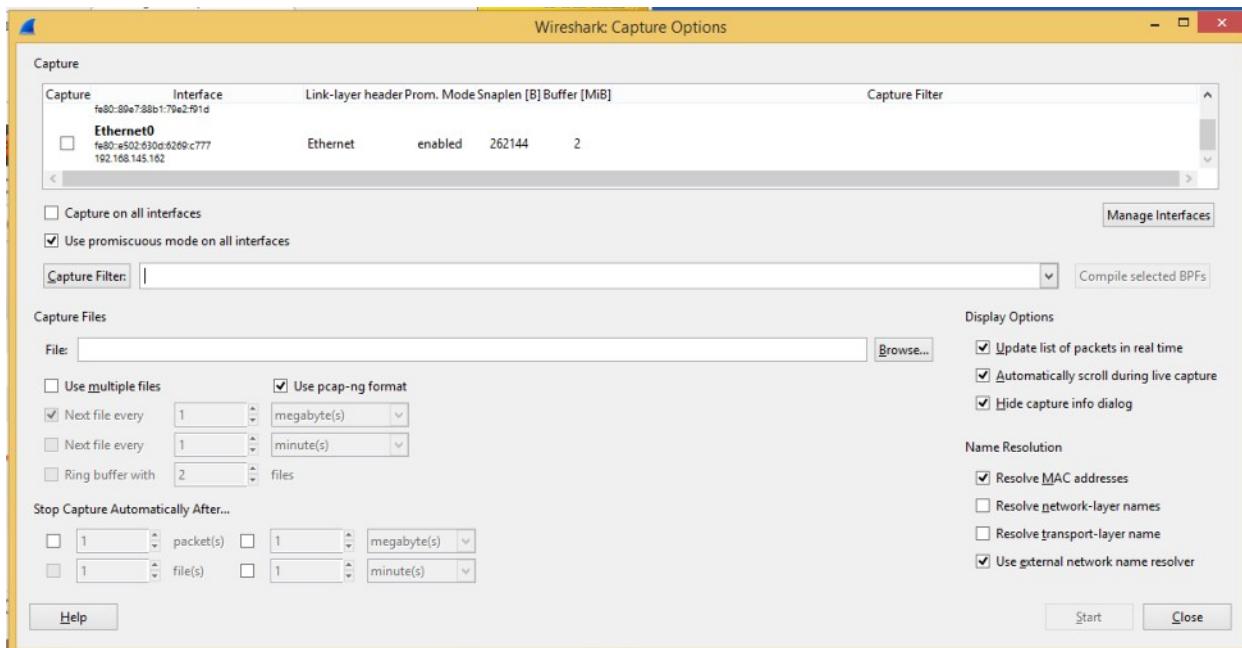
Зураг 4.2. Линукс/Юникс орчинд Интерфэйсүүдийг чагнах цонх

<i>Device</i> (Төхөөрөмж – зөвхөн - Unix/Linux)	Интерфэйс төхөөрөмжийн нэр
<i>Description</i> (Тодорхойлолт)	Үйлдлийн системийн тодорхойслноор интерфэйсийн тухай тодорхойлолт эсвэл <b>10.5.1. “Интерфэйсийн сонголтууд (Interface Options)”</b> хэсэгт нэмж тайлбар байдлаар хэрэглэгчийн оруулсан тодорхойлолт
<i>IP</i> (Интернэт протокол хаяг)	Вайршарк програмын илрүүлсэн энэ интерфэйс дээрх IP хаяг. Энэхүү интерфэйст олгогдсон бусад хаяг руу циклдэхийн тулд энэхүү хаяг дээр дараахад хангалттай. Гэхдээ өөр хаяг олдохгүй бол “none” гэсэн мэдээллийг харуулна.
<i>Packets</i> (Пакетууд)	Энэхүү цонх нээгдсэнээс хойш тухайн интерфэйс дээр чагнагдсан пакетын тоо. Ямар ч пакет орж ирж чагнагдаагүй байвал саарал байна.
<i>Packets/s</i> (Пакетууд)	Сүүлийн секундэд чагнагдсан пакетын тоо. Сүүлийн секундэд пакет чагнаагүй бол саарал өнгөтэй байна.
<i>Stop</i> (Зогсоох)	Одоогийн ажиллаж буй чагнах процесийг зогсоох

<i>Start</i> (Эхлүүлэх)	Сонгосон бүх интерфэйсүүд дээр чагнах үйлдлийг эхлүүлнэ. Ингэхдээ хэрэв ямар нэгэн тохиргоо хийгдээгүй бол өмнө нь хэрэглэсэн эсвэл өгөгдмөл (default) тохирготойгоор эхлүүдэг.
<i>Options</i> (Сонголтууд)	Сонгож тэмдэглэсэн интерфэйсүүдтэй чагнах сонголтууд (Capture Options)-ын цонхыг нээнэ. <b>4.5. “Чагнах сонголтууд (Capture Options)”</b> хэсгийг ҮЗНЭ ҮҮ.
<i>Details</i> (Дэлгэрэнгүй - Зөвхөн Microsoft Windows)	Интерфэйсийн талаарх дэлгэрэнгүй мэдээллийг агуулсан цонхыг нээнэ. <b>4.10. “Интерфэйсийн дэлгэрэнгүй мэдээлэл (Interface Details)”</b> хэсгийг ҮЗНЭ ҮҮ.
<i>Help</i> (Туслах)	Туслах хуудсыг нээнэ
<i>Close</i> (Хаах)	Энэ хэсгийг хаана.

#### 4.5. Чагнах сонголтууд (Capture Options)

**Capture → Options ...** хэсгийг сонгосноор (Эсвэл үндсэн товчлуурууд (main toolbar)) дээрээс харгалзах товчлуурыг дарснаар Вайршарк програм танд тухайн цэсд харгалзах цонхыг харуулна. Энэхүү цонхыг Зураг 4.3.-д харууллаа.



Зураг 4.3. Чагнах сонголтууд (Capture Options)

Хэрэв та ямар сонголтыг сонгохoo мэдэхгүй байвал өгөгдмөл (default) тохиргоогоор нь ашиглана уу. Өгөгдмөл хэлбэрээр ашиглах зөвхөн энэ тохиолдолд ч бус өөр олон тохиолдолд хангалттай хэмжээнд ажиллана.

#### 4.5.1. Чагнах фрэйм (Capture frame)

Хүснэгт нь боломжит бүх интерфэйсүүд дээрх тохиргоонуудыг харуулна.

Лүүпбак (loopback) интерфэйс нь виндовс үйлдлийн систем дээр боломжгүй байдаг

- Интерфэйсийн нэр болон IP хаяг. Хэрэв хаяг нь хөрвүүлэгдэх боломжгүй байвал түүнийг “none” гэсэн тэмдэглэгээгээр харуулна.
- Линк түвшний толгойны төрөл (Link-Layer header type)
- Холимог горим (Promiscuous mode) идэвхижисэн эсвэл идэвхижээгүй талаарх мэдээлэл
- Пакет бүр дээр чагнагдах хамгийн их өгөгдлийн хэмжээ. Өгөгдмөл утга нь 65535 байт хэмжээтэй байдаг.
- Чагнасан пакетыг хадгалж байх зориулалтаар нөөцлөгдсөн кернелийн буфферийн хэмжээ
- Пакетуудыг ажиглалтын горим (Monitor mode)-д чагнах эсэх мэдээлэл (Зөвхөн Юникс/Линукс)
- Сонгосон пакетын шүүлтүүр

Эхний багана дахь хэрээст талбар (checkbox)-г хэрээслэж тэмдэглэснээр тухайн интерфэйсээс чагнахаар сонгож байна гэсэн үг. Интерфэйс дээр хулганы товчийг 2 удаа дарснаар Интерфэйсийн тохиргоог засварлах (Edit Interface Settings) –г гаргаж ирнэ. (Зураг 4.4. Интерфэйсийн тохиргоог засварлах (Edit Interface Settings) цонхыг харуулна)

*Capture on all interfaces (Бүх интерфэйс дээр чагнах)*

Вайршарк програм олон интерфэйсийг чагнах боломжтой учраас боломжит бүх интерфэйсийг сонгож болдог.

*Capture all packets in promiscuous mode (Бүх пакетыг холимог горимоор чагнах)*

Энэ хэрээст талбар нь вайршарк програмд бүх интерфэйсийг чагнах үедээ бүгдийг нь холимог горимд (promiscuous mode) чагнах болгох тохиргоог хийнэ.

*Capture Filter (Чагнах үеийн шүүлтүүр)*

Энэ талбар нь сонгосон байгаа интерфэйсүүд дээр пакет чагнах үеийн шүүлтүүр тодорхойлж өгөх боломжийг олгодог. Энэ хэсэгт түлхүүр үгийг оруулсан тохиолдолд шинээр нэмж сонгосон интерфэйсүүд мөн энэхүү тохиргоог өвлөн авдаг. Чагнах үеийн шүүлтүүрийг 4.13. “Чагнах үеийн

**шүүлтүүр (Filtering while capturing)**” хэсэгт дэлгэргүй авч үзнэ. Өгөгдмөл тохиргоогоор (default) ямар нэгэн шүүлтүүр байдаггүй.

Түүнчлэн та чагнах шүүлтүүр товчуур дээр дарах боломжтой бөгөөд Вайршарк Чагнах үеийн шүүлтүүр (Capture Filters) цонхыг гаргана. Энэ цонхноос та шүүлтүүрийг үүсгэх эсвэл шүүлтүүр сонгох үйлдлүүдийг хийж болно. 6.6. “Шүүлтүүр тодорхойлох мөн хадгалах (Defining and saving filters)” хэсгийг үзнэ үү.

#### *Compile selected BPFs*

Энэ товч нь чагнах үеийн шүүлтүүрийг BPF рүү хөрвүүлж эмхэтгэх (compile) боломжоор хангана мөн псевдо кодтой цонхыг харуулна. Энэ нь өөрийн үүсгэсэн чагнах үеийн шүүлтүүртэй ажиллах процесийг ойлгоход тус дэмтэй байна. BPF-үүд рүү хөрвүүлж, эмхэтгэх (compile) нь таныг **Зураг 4.5. “Хөрвүүлэлтийн үр дүн (Compile Results)**” дээр харуулж байгаа руу хөтөлнө.

#### **Зөвлөгөө (Линукс хэрэглэгчдэд)**

BPF-үүдийн биелүүлэлт нь нь Линукс дээр дараах командыг ажиллуулснаар BPF ЛТ-ийг ачааллаж маш хурдан хийгдэх боломжтой болдог.

```
$ echo 1 >/proc/sys/net/core/bpf_jit_enable
```

Энэхүү өөрчлөлтөө байнгын болгохын тулд та sysfsutils-г ашиглаж болно.

#### *Manage Interfaces (Интерфэйсүүдийг удирдах)*

Интерфэйсийг удирдах (Manage Interfaces) товч нь **Зураг 4.6. “Шинэ интерфэйс нэмэх (Add New Interfaces)**” цонхыг нээдэг. Энэхүү цонх дээр хоолойнуудыг (pipes) тодорхойлх, локал интерфэйсүүдийг хайх эсвэл нуух (hide)эсвэл алсын зайд (remote) байгаа интерфэйсүүдийг нэмж (зөвхөн windows орчинд) өгч болно

The Manage Interfaces button opens the Figure 4.6, “The “Add New Interfaces” dialog box” where pipes can be defined, local interfaces scanned or hidden, or remote

interfaces added (Windows only).

#### 4.5.2. Файл чагнах фрэйм (Capture File(s) frame)

Файл чагнах үйлдлийн хэрэглээний талаарх тайлбарыг 4.11. “Файл чагнах мөн Файлын горимууд (Capture files and file modes)” хэсгээс үзнэ үү.

*File (файл)*

Энэ талбар нь танд чагнах файлд хэрэглэгдэх файлын нэрийг тодорхойлох боломжийг өгдөг. Өгөгдмөл (default) утгаараа энэ талбар нь хоосон байдаг. Хэрэв энэ талбар нь хоосон байвал чагнаж буй файл нь түр зуурын (temporary) файлд хадгалагдана. 4.11. “Чагнах файл мөн файлын горимууд (Capture files and file modes)” хэсгийг үзнэ үү

Та файлын системийг үзэхийг хүсвэл энэ талбарын барын хэсэг дэх товчлуурыг дарах хэрэгтэй.

*Use multiple files (Олон файл хэрэглэх)*

Ганц файлтай ажиллахын оронд вайршарк програм нь тодорхой нөхцөл биелэгдэх үед шинэ файл руу шилждэг.

*Use pcap-ng format (pcap-ng формат хэрэглэх)*

Энэ хэрэест талбарыг (checkbox) хэрээслэнээр чагнасан пакетуудаа pcap-ng форматаар хадгалдаг. Дараагийн үеийн чагнах файлын формат нь одоогоор хөгжүүлэлтэнд явж байна. Хэрэв нэгээс олон интерфэйс чагнахаар сонгогдсон байвал энэ хэсэг нь өгөгдмөл тохиргоогоороо хэрээслэгдсэн байдаг.

Дэлгэрүүлэн [уншихыг](https://wiki.wireshark.org/development/pcapng) хүсвэл <https://wiki.wireshark.org/development/pcapng> хэсгийг үзнэ үү

*Next file every n megabyte(s) (n мегабайт бүрт дараагийн файл)*

Олон файлтай ажиллах үед хэрэглэнэ. Чагнаж буй пакетын хэмжээ тодорой MB, KB, GB хэмжээнд хүрэх үед дараагийн файл руу шилжинэ.

*Next file every n minute(s) (n минут бүрт дараагийн файл)*

Олон файлтай ажиллах үед хэрэглэнэ. Тодорхой хугацаа өнгөрсөн нөхцөлд дараагийн файл руу шилжинэ.

<i>Ring buffer with n files (n файлтай ринг буфер)</i>	Олон файлтай ажиллах үед хэрэглэнэ. Тодорхойлж өгсөн файлын тоотойгоор чагнах файлын ринг буферийг үүсгэнэ.
<i>Stop capture after n file(s) (n файлын дараа чагнах үйлдлийг зогсоох)</i>	Олон файлтай ажиллах үед хэрэглэнэ. Дараагийн файл руу тодорхой тоотойгоор шилжсэний дараа чагнах процесийг зогсооно.

#### 4.5.3. Чагнах процесийг зогсоох фрэйм (Stop Capture ... frame)

<i>... after n packet(s) (n тооны пакетын дараа)</i>	Тодорхой тооны пакет чагнасан тохиолдолд чагнах үйлдлийг зогсооно.
<i>... after n megabytes(s) (n тооны мегабайтын дараа)</i>	Чагнасан файлын хэмжээ тодорхой хэмжээнд (byte(s)/kilobyte(s)/ megabyte(s)/gigabyte(s)) хүрсний дараа чагнах үйлдлийг зогсооно. Хэрэв олон файлтай ажиллаж байгаа бол энэ сонголт хэрэглэгдэх боломжгүй.
<i>... after n minute(s) (n тооны минутын дараа)</i>	Тодорхой хугацаа (second(s)/minutes(s)/ hours(s)/days(s)) өнгөрсний дараа чагнах үйлдлийг зогсооно.

#### 4.5.4. Дэлгэцэнд харуулах сонголтуудын фрэйм (Display Options frame)

<i>Update list of packets in real time (Пакетын жагсаалтыг бодит хугацаанд шинэчлэх)</i>	Энэ сонголт нь вайршарк програмын пакет орж ирэх үед пакетыг жагсаан харуулах самбарыг доош нь гүйлгэх тохиргоог хийнэ. Ийм байдлаар хэрэглэгч хамгийн сүүлд ирсэн пакетыг байнга храж байх боломжтой болно. Энэ тохиргоог хийхгүй бол вайршарк програм шинээр ирж буй
<i>Automatic scrolling in live capture (Шуул чагнаж байгаа өгөгдлийг автоматаар дооши нь гүйлгэх)</i>	

пакетуудаа жагсаан харуулах самбарт нэмэх хэдий ч түүнийг жагсаалтын хамгийн сүүлд нэмэх ба хэрэглэгч түүнийг харах боломжгүй байдаг. Хэрэв пакетыг жагсаалтыг бодит хугацаанд тохиргоо хийгдээгүй бол энэ тохиргоо хийгдэх боломжгүй байх агаад саарал өнгөтэй болсон байдаг.

*Hide capture info dialog*  
(Чагнах мэдээллийн цонхыг нуух)

Хэрэв энэ сонголт хэрээслэгдсэн байвал **4.14 “чагнаж байх үед (while a capture is running ...)”** хэсэгт тодорхойлсон цонх нуугддаг (hidden)

#### 4.5.5. Нэрийн хөрвүүлэлтийн фрэйм (Name Resolution frame)

*Enable MAC name resolution*  
(MAC нэрийн хөрвүүлэлт идэвхижүүлэх)

Энэ сонголт нь Вайршарк програм MAC хаягийг нэр лүү хөрвүүлэх эсэхийг удирддаг. **7.7. “Нэрийн хөрвүүлэлт (Name Resolution)”** хэсгийг үзнэ үү

*Enable network name resolution*  
(Сүлжээний нэрийн хөрвүүлэлт идэвхижүүлэх)

Энэ сонголт нь Вайршарк програм сүлжээний хаягуудийг нэр лүү нь хөрвүүлэх эсэхийг удирддаг. **7.7. “Нэрийн хөрвүүлэлт (Name Resolution)”** хэсгийг үзнэ үү

*Enable transport name resolution*  
(Дамжуулалтын нэрийн хөрвүүлэлт идэвхижүүлэх)

Энэ сонголт нь Вайршарк програм дамжуулалтын түвшний (transport) хаягийг протокол руу хөрвүүлэх эсэхийг удирддаг. **7.7. “Нэрийн хөрвүүлэлт (Name Resolution)”** хэсгийг үзнэ үү

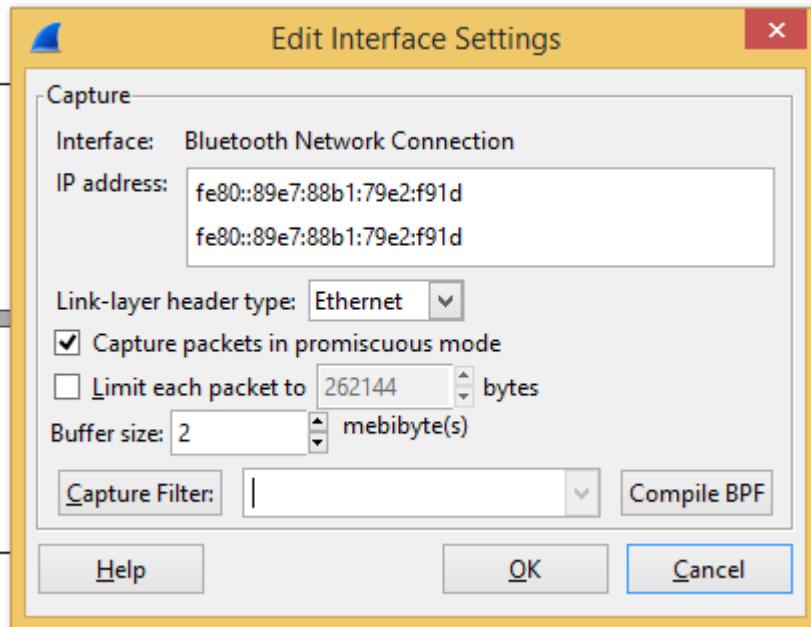
#### 4.5.6. Товчлуурууд (Buttons)

Өөрийн хүссэн тохиргоог хийсэн бол та **Start** товчлуур дээр дарж чагнах үйлдлийг эхлүүлэх эсвэл **Cancel** товчлуурыг дарж чагнах үйлдлийг цуцална.

Хэрэв та чагнах үйлдлийг эхлүүлсэн бол та хангалттай пакет өгөгдөл цуглувалж авсныхаа дараа чагнах үйлдлийг зогсоох боломжтой. Дэлгэрүүлэн судлахыг хүсвэл **4.14 “чагнаж байх үед (while a capture is running ...)”** хэсгийг үзнэ үү.

#### 4.6. Интерфэйсийн тохиргоог засварлах цонх (Edit Interface Settings)

Хэрэв та зураг 4.3. “Чагнах сонголтууд” цонхлнд харуулсан интерфэйс дээр хулганыг 2 удаа дарсан бол дараах цонх гарч ирнэ.



Зураг 4.4. Интерфэйсийн тохиргоог засварлах

Энэхүү цонхноос та дараах талбаруудыг тохируулж болно:

*IP address (IP хаяг)*

Сонгогдсон интерфэйсийн IP хаяг (хаягууд). Хэрэв хаягууд нь системээс хөрвүүлэгдэх боломжгүй байвал “none” гэсэн үгийг харуулна.

*Link-layer header type (Линк түвшний толгойн төрөл)*

Ховор нөхцөлд энэхүү тохиргоог өөрчлөх шаардлагатай болдог тиймээс энэ тохиргоог өгөгдмөл тохиргоогоор нь орхисон нь дээр байдаг. Гэхдээ дэлгэрүүлэн судлахыг хүсвэл **4.12. “Линк түвшний толгойн төрөл (Link-layer header type)”** хэсгийг уншина уу

*Wireless settings (Утасгүй сүлжээн тохиргоо – Зөвхөн Виндовс)*

Эндээс AirPCap адаптерийг ашиглан утасгүй сүлжээний өгөгдлийг чагнах тохиргоог хийдэг. Дэлгэрэнгүй судлахыг хүсвэл AirPCap хэрэглэгчдийн гарын авлагыг уншина уу.

*Remote settings (Алсын тохиргоо – Зөвхөн Виндовс)*

Энд та алсын зайнаас (remote) чагнах тохиргоог хийх боломжтой. Дэлгэрүүлэн судлахыг хүсвэл **4.9. “Алсын зайнаас интерфэйс чагнах (The Remote Capture Interfaces)**” хэсгийг уншина уу.

*Capture packets in promiscuous mode (Холимог горимд пакет чагнах)*

Энэ хэрэest талбар (checkbox) нь вайршарк програм интерфэйсийг чагнах процесс хийхдээ тухайн интерфэйсийг холимог горим (**promiscuous mode**)-д оруулах тохиргоог хийдэг.

Хэрэв та энэ тохиргоог тодорхойлж өгөхгүй бол вайршарк нь зөвхөн таны таны компьютерт ирж байгаа эсвэл таны компьютерээс гарч буй пакет өгөгдлүүдийг л чагнана. (Дотоод сүлжээнд байгаа бүх пакет өгөгдлийг биш)

## Тэмдэглэл

Хэрэв бусад процесс тухайн интерфэйсийг холимог горим (Promiscuous mode)-д оруулсан байвал та энд холимог горимын тохиргоог хаасан байсан хэдий ч холимог горимоор чагнаж байх боломжтой.

Холимог горим (promiscuous mode)-д байгаа ч та дотоод сүлжээний бүх пакетыг харах шаардлагагүй. Вайршарк программын түгээмэл асуугддаг асуултын хэсгээс дэлгэрэнгүй мэдээлэл үзнэ үү.

*Limit each packet to n bytes  
(Пакетуудыг n байтаар хязгаарлах)*

Энэ талбар нь чагнах пакетын хамгийн их хэмжээг тодорхойлох боломжийг олгодог мөн заримдаа снаплен (snaplen) гэж нэрлэгдэх нь ч байдаг. Хэрэв энэ тохиргоог идэвхигүй болговол хамгийн их утга нь 65535 болон тохицуулагдах ба энэ нь ихэнх протоколд хангалттай хэмжээ юм. Зарим үндсэн зарчим:

- Хэрэв итгэлтэй бус байгаа бол өгөгдмөл утгаар нь үлдээх
- Хэрэв танд пакетад байгаа бүр өгөгдөл шаардлагагүй бол (Жишээлбэл танд зөвхөн линк түвшин (Link layer), IP, мөн TCP толгой (headers) хэрэгтэй байгаа бол танд бага снапшот (snapshot) хэмжээ хэрэгтэй байж болно. Ингэснээр пакетыг хуулахад CPU бага цаг зарцуулах, буферийн хэмжээ бага байх ингэснээр пакет гээгдэх магадлал багасах гэх мэт ач холбогдолтой)
- Хэрэв та бүх өгөгдлийг чагнаагүй бол таны үзэхийг хүсч буй пакет өгөгдөл гээгдсэн пакет

дотор эсвэл дахин дамжуулах шаардлагатай болсон байх магадлалтай юм.

*Buffer size: n megabyte(s)*  
*(Буферын хэмжээ н мегабайт)*

Чагнах үйлдэлд хэрэглэгдэх буферийн хэмжээг оруулах. Энэ нь чагнасан пакетуудаа диск рүү бичтэлээ хадгалж байх кернелийн буферийн хэмжээ юм. Хэрэв пакет гээгдэх тохиолдол их байвал энэ утгыг ихэсгээд үзэх хэрэгтэй.

*Capture packets in monitor mode*  
*(Хяналтын горимд пакет чагнах - Зөвхөн Unix/Linux)*

Энэ хэрэest талбар нь утасгүй сүлжээний интерфэйсийг хүлээн авч чадах бүх урсгалаа хүлээн авах тохиргоог хийдэг. Ингэхдээ дан ганцхан түүнтэй холбоотой BSS дээрх ургалаар хязгаарлагдагүй юм. Энэ нь мөн холимог горим (promiscuous mode)-н үед ч гэсэн ажилладаг. Түүнчлэн IEEE 802.11 толгой (header) мөн радио мэдээллийг (radio information)-г харахын тулд энэ сонголтыг ажиллуулсан байх ёстой.

## Тэмдэглэл

Хяналтын горимд адаптер нь өөрийгөө (өөрийнхөө хамааралтай) сүлжээнээсээ тусгаарлан ялгах магадлалтай.

*Capture Filter (Чагнах үеийн шүүлтүүр)*

Энэ талбар нь танд чагнах үеийн шүүлтүүрийг тодорхойлох боломжийг олгоно. **4.13. “Чагнах үедээ шүүлтүүр ашиглах (Filtering while capturing)”** хэсгээс дэлгэрэнгүй тайлбарыг уншина уу. Өгөгдмөл тохиргоогоороо энэ нь хоосон байдаг.

Мөн түүнчлэн та Чагнах шүүлтүүр (Capture Filter) товчдуу дээр дарж болох ба ингэснээр вайршарк **Чагнах шүүлтүүр (Capture Filter)** цонхыг харуулна. Энэ цонхыг ашиглан та шүүлтүүр үүсгэх эсвэл шүүлтүүрээс сонгох боломжтой байда. **6.6. “Шүүлтүүр тодорхойлох, хадгалах(Defining and saving filters)”** хэсгээс дэлгэрүүлэн уншина уу

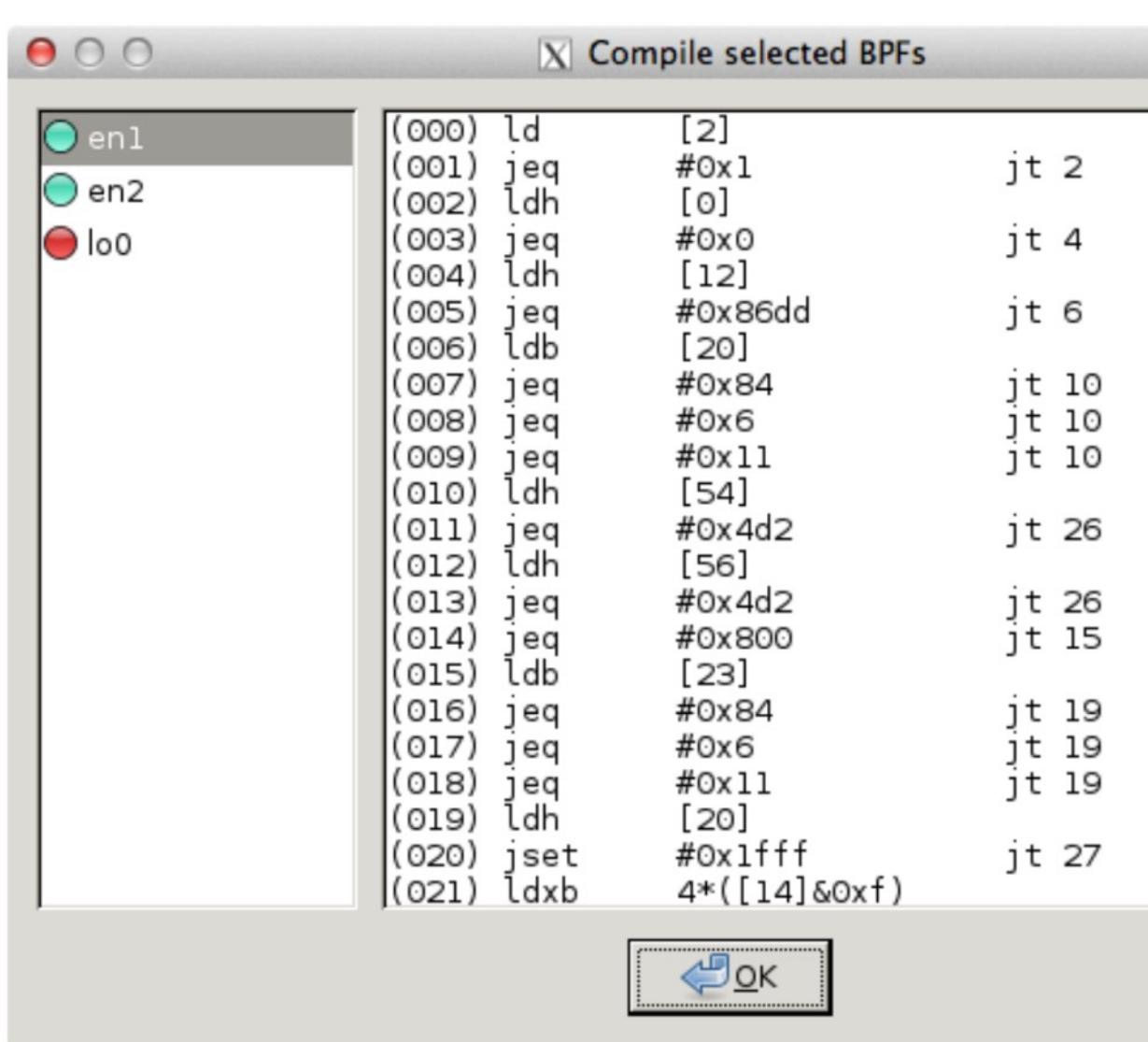
*Compile BPF (BPF хөрвүүлэлт, эмхэтгэл)*

Энэ товчлуур нь танд чагнах үеийн шүүлтүүрийг BPF код руу хөрвүүлэх боломжийг олгоно. Ингэснээр вайршарк танд псевдо код агуулсан цонхыг харуулна: Энэ нь өөрийн үүсгэсэн чагнах үеийн шүүлтүүр дээр

ажиллах үйлдлээ ойлгоход тань тус дэм болно.

#### 4.7. Хөрвүүлэлтийн үр дүн цонх (Compile Results dialog box)

Энэ зурагт сонгосон интерфэйсүүдийг хөрвүүлсэн хөрвүүлэлтийн үр дүнг харууллаа

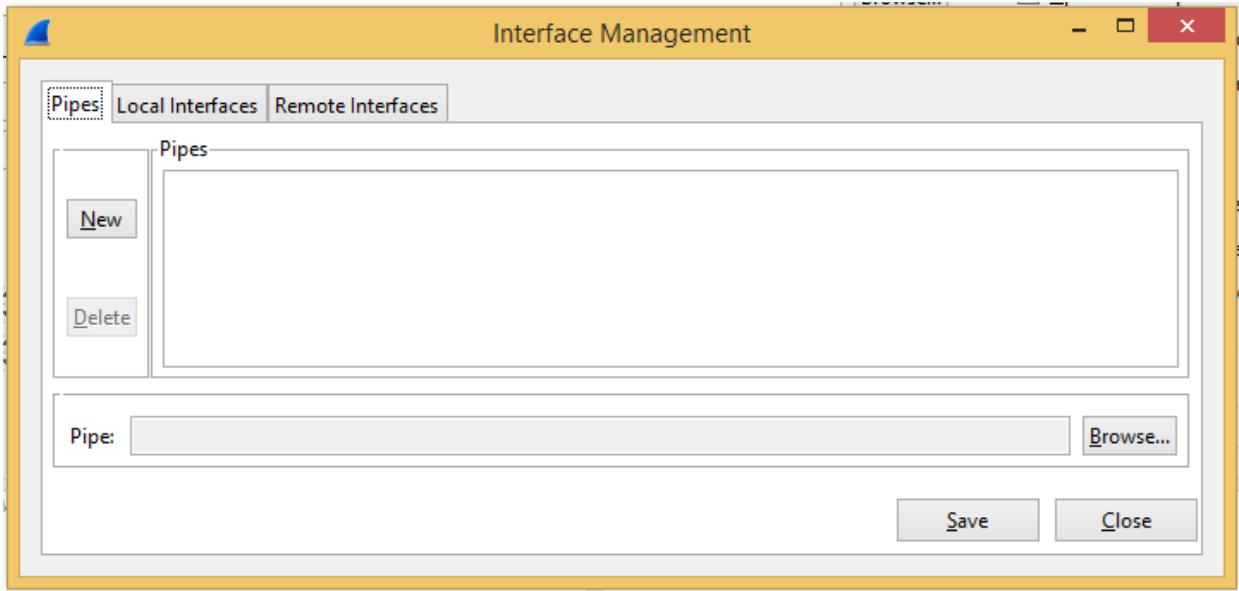


Зураг 4.5.Хөрвүүлэлтийн үр дүн цонх

Зүүн цонхонд интерфэйсийн нэрс жагсаалт хэлбэрээр харагдаж байна. Тухайн нэг интерфэйсийн үр дүн тухайн интерфэйсийн сонгосон үед баруун талын цонхонд харагдаж байна.

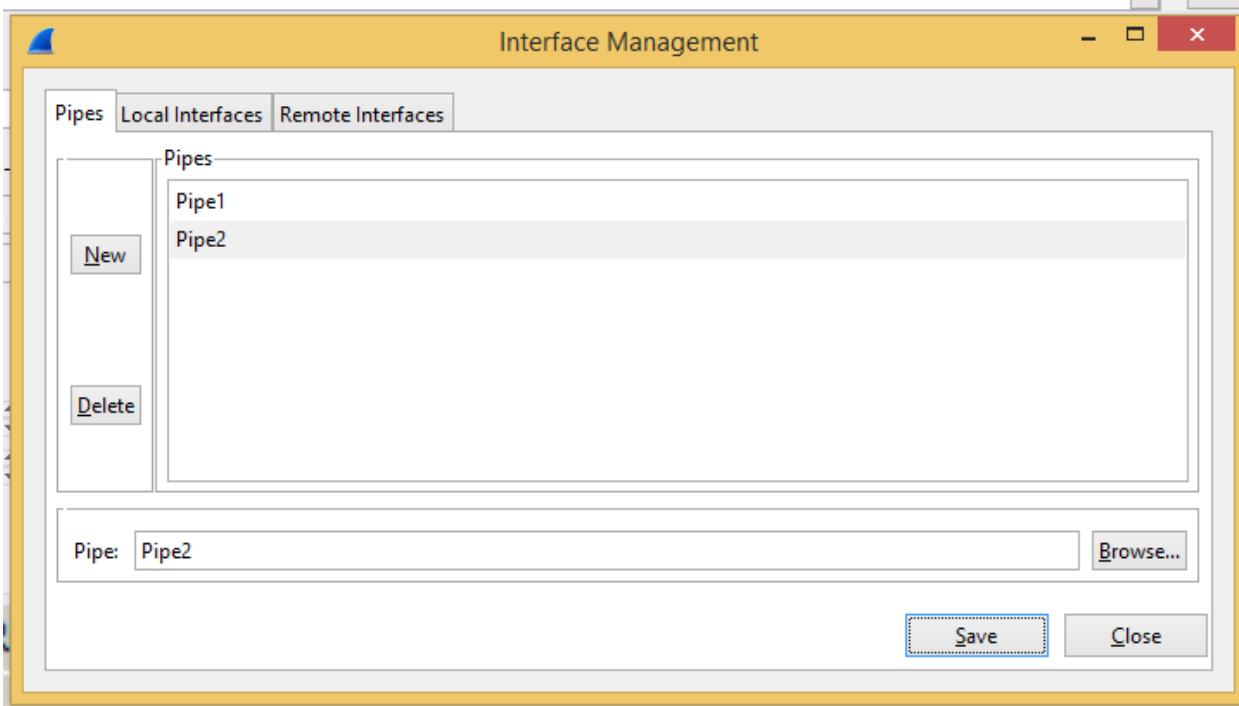
#### 4.8. Шинэ Интерфэйс нэмэх (Add New Interfaces)

Интерфэйсүүдийг удирдах төв цэг болохынхoo хувьд энэ цонх нь 3 хэсгээс бүрдэх ба эдгээр нь шинэ интерфэйс нэмэх эсвэл интерфэйсийг устгах үүрэгтэй.



Зураг 4.6. Шинэ интерфэйс нэмэх цонх

#### 4.8.1. Шинэ хоолой (pipe) нэмэх эсвэл устгах (Add or remove pipes)



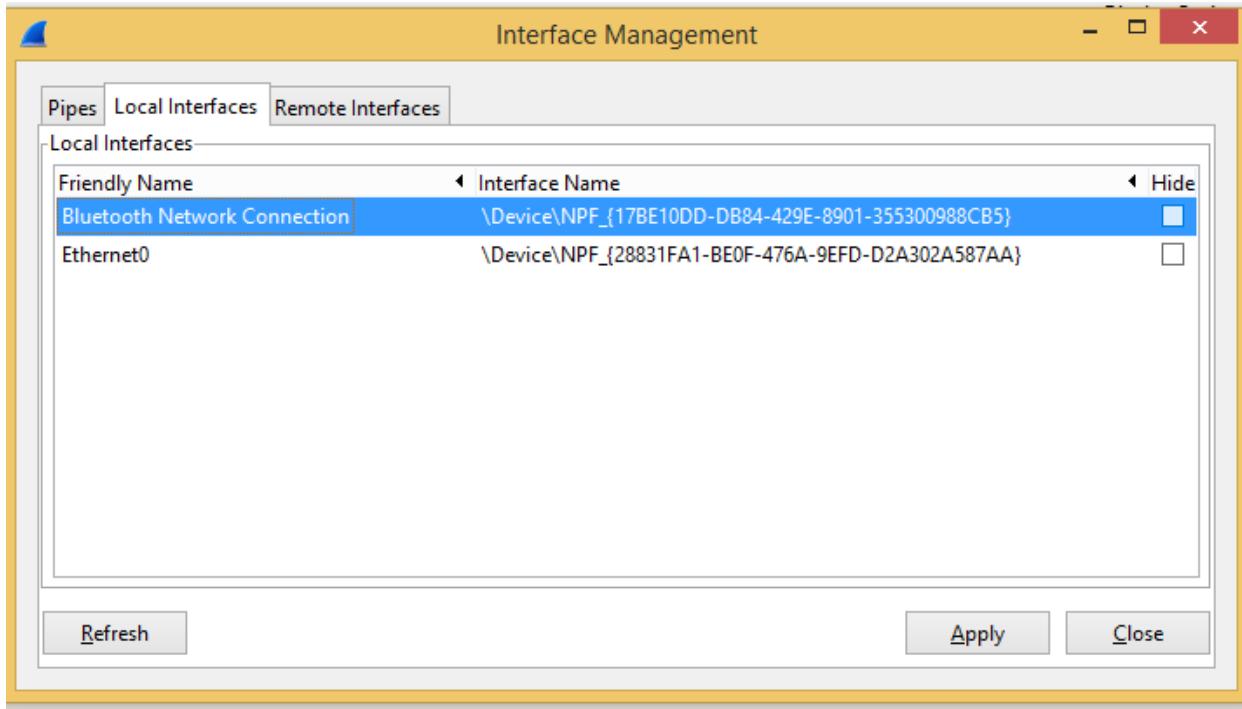
Зураг 4.7. Шинэ интерфэйс – хоолой (pipe) нэмэх цонх

Хоолой (pipe) шинээр амжилттай нэмэхийн тулд эхлээд энэ хоолойг үүсгэсэн байх шаардлагатай. New товчлуур дээр дараах ба дараа нь хоолой (pipe)-н нэрийг замтай (path) нь хамтад нь оруулна. Өөр нэгэн сонголт нь **Browse** товчлуур дээр хоолой (pipe)-н байгаа газрыг зааж өгөх боломжтой юм. Үүний дараа **Save** товчлуурыг дарснаар энэхүү хоолой

(pipe) нь боломжит интерфэйсийн жагсаалт руу нэмэгдсэн байна. Дараа нь өөр хоолой (pipe) нэмж болно.

Хоолойг интерфэйсийн жагсаалтаас хасахын тулд эхлээд сонгох хэрэгтэй бөгөөд дараа нь **Delete** товчлуур дээр дарна.

#### 4.8.2. Локал интерфэйсүүдийг нэмэх эсвэл нуух (Add or hide local interfaces)



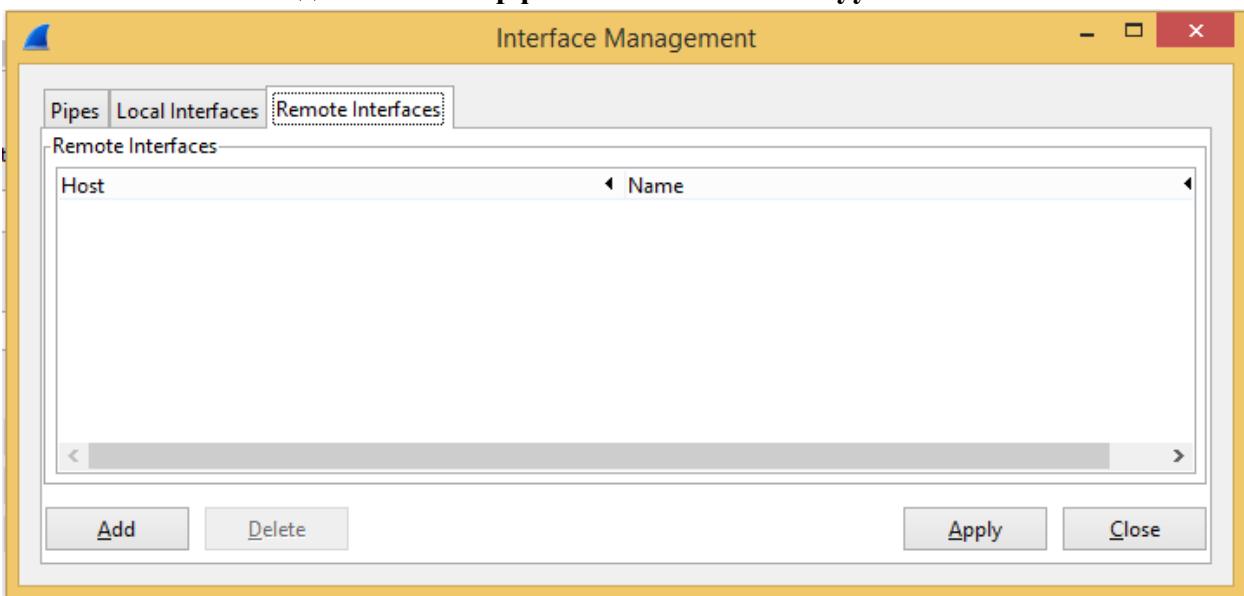
Зураг 4.8. Шинэ интерфэйс нэмэх – Локал интерфэйс

Дотоод Интерфэйсүүд (Local Interfaces) хэсэг (tab) нь локал интерфэйсүүдийг жагсаан харуулна. Ингэхдээ нуугдсан бусад жагсаалтад харагдахгүй нуугдсан (hidden) интерфэйсүүдийг ч гэсэн харуулдаг.

Хэрэв шинэ локал интерфэйс нэмэгдвэл (жиш. Wireless Interface идэвхитэй болвол) энэ хэсэг нь интерфэйсийг хийх процесс удаан үргэлжилэх асуудлаас сэргийлэн өөрийн энэхүү жагсаалт руу автоматаар нэмдэг. Энэхүү жагсаалтыг шинэчлэхийн тулд дахин хайлт хийх үйлдлийг хийж болно.

Интерфэйсийг нуух (hide) аргуудын нэг нь интерфэйсийн тохиргоо (preferences)-г өөрчөх юм. Хэрэв **Hide** (нуух) хэрээст талбар хэрээслэгдсэн бөгөөд **Apply** (идэвхижүүлэх) товчлуурыг дарсан байвал тухайн интерфэйс нь **Capture Interfaces** (Чагнах Интерфэйсүүд) хэсэгт харагдахгүй. Эдгээр тохиргоо нь мөн **preferences file** (Тохиргооны файл)-д хадгалагддаг.

#### 4.8.3. Алсын зайд байгаа интерфэйсийг нэмэх эсвэл нуух



Зураг 4.9. Шинэ Интерфэйс нэмэх – Алсын Интерфэйс (Add New Interfaces - Remote Interfaces)

Энэ хэсэг даар алсын зайд байгаа хостын интерфэйсийг нэмж болно. Эдгээр интерфэйсүүдийг нуух боломжтой. Локал интерфэйсүүдээс ялгаатай нь эдгээр интерфэйсийн тохиргоо нь preference file (тохиргооны файл) дээр хадгалагддагтүй.

Алсын хостыг бүх интерфэйстэй нь энэхүү жагсаалтаас устгахын тулд тухайн хостоо сонгоод Delete (Устгах) товчлуурыг дарах хэрэгтэй.

Дэлгэрүүлэн уншихыг хүсвэл **4.9. Алсын зайны интерфэйсийг чагнах (Remote Capture Interfaces)** хэсгийг үзнэ үү.

#### 4.9. Алсын зайны интерфэйсийг чагнах (Remote Capture Interfaces)

Зөвхөн локал интерфэйсийг чагнах үйлдэл хийхээс гадна Вайршарк програм нь чагнах даемон (capture daemon) эсвэл сервисийн процессыг (service process) ашиглан сүлжээн дээрх алсын хостын хүлээн авч буй өгөгдлийг чагнах боломжтой.

##### Зөвхөн Виндовс орчинд ажиллана

Энэ хэсэг нь зөвхөн Виндовс орчинд л ажиллана. Линук/Юникс орчинд үүнтэй ижилхэн үйлдэл хийхийг хүсвэл SSH туннелийг ашиглах хэрэгтэй.

Вайршарк програмтай холбогдохын тулд алсын зайны хост дээр эхлээд Алсын Пакет Чагнах Протокол Сервис ажллаж байх ёстой. Үүнийг хийх хамгийн хялбар арга нь

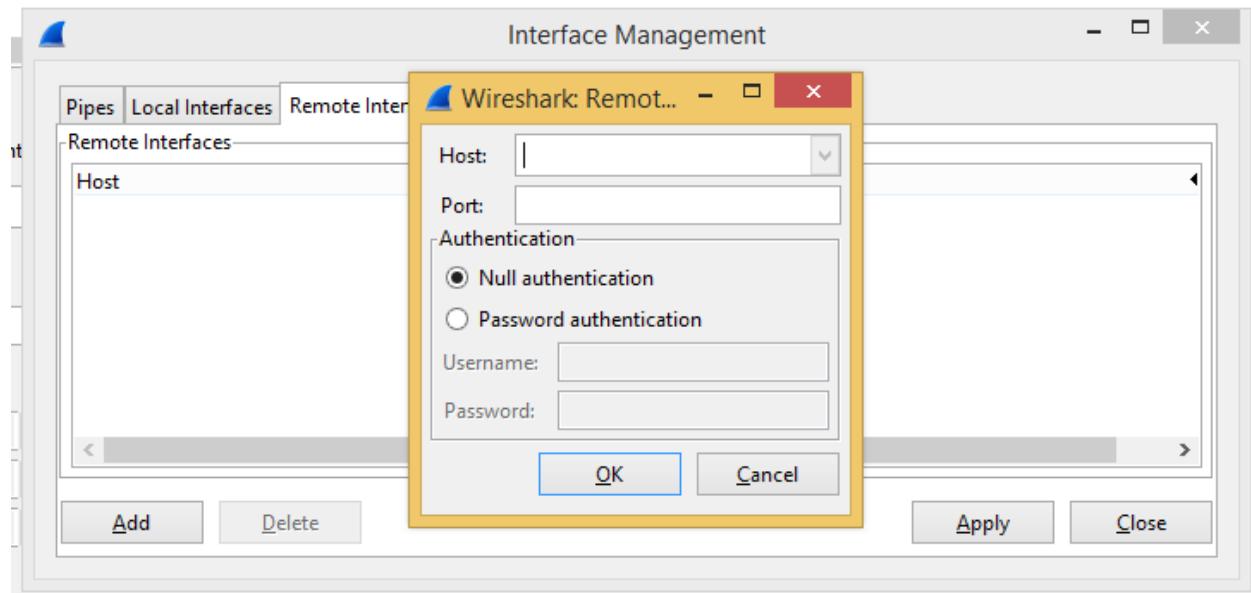
WinPcap программыг <https://www.winpcap.org/install/> хаягаас татан зорилтот хост (on target host) дээрээ суулгах юм. Амжилттай суулгасны дараа Сервис хянах самбар (Service control panel) дээрээс Алсын Пакет Чагнах Протокол сервис (Remote Packet Capture Protocol service)-ийг хайж олоод түүнийгээ идэвхижүүлэх хэрэгтэй.

### Мэдэгдэл

Зорилтот (target) хост дээр гадагшаа хандах 2002 порт нээлттэй байх ёстойг анхаарна уу. Энэ порт нь Алсын Пакет Чагнах Протокол сервис (Remote Packet Capture Protocol service) өгөгдмөл (default) тохиргоогоороо холболтоо хийхэд ашигладаг порт юм.

Алсын зайнаас чагнах интерфэйс (Remote Capture Interfaces) руу хандахын тулд Шинээр Интерфэйс нэмэх (Add New Interfaces-Remote-ийг ашиглана. Зураг 4.9. дээрх цонхыг үзнэ үү. Энэ цонхонд хүрсний дараа Add (нэмэх) товчлуурыг дарна уу.

#### 4.9.1. Алсын зайнаас чагнах интерфэйсүүд (Remote Capture Interfaces)



Зураг 4.10. Алсын зайнаас чагнах интерфэйсүүд (Remote Capture Interfaces)

Дараах цонхонд та дараах параметруудийг тохируулах шаардлагатай болно.

##### Host (Хост)

Алсын зайнаас пакет чагнах протокол сервис (Remote Packet Capture Protocol service) чагнаж байгаа хостын IP хаяг эсвэл нэрийг оруулна. Доошоо заасан сум нь өмнө нь амжилттай холбогдож байсан хостуудыг харуулна.

##### Port (Порт)

Алсын зайнаас пакет чагнах протокол сервис (Remote Packet

Capture Protocol service) чагнаж байгаа портын дугаарыг оруул. Өгөгдмөл 2002 портыг ашиглах бол энэ тохиргоог хоосон орхино уу.

*Null authentication  
(Хоосон  
баталгаажуулалт)*

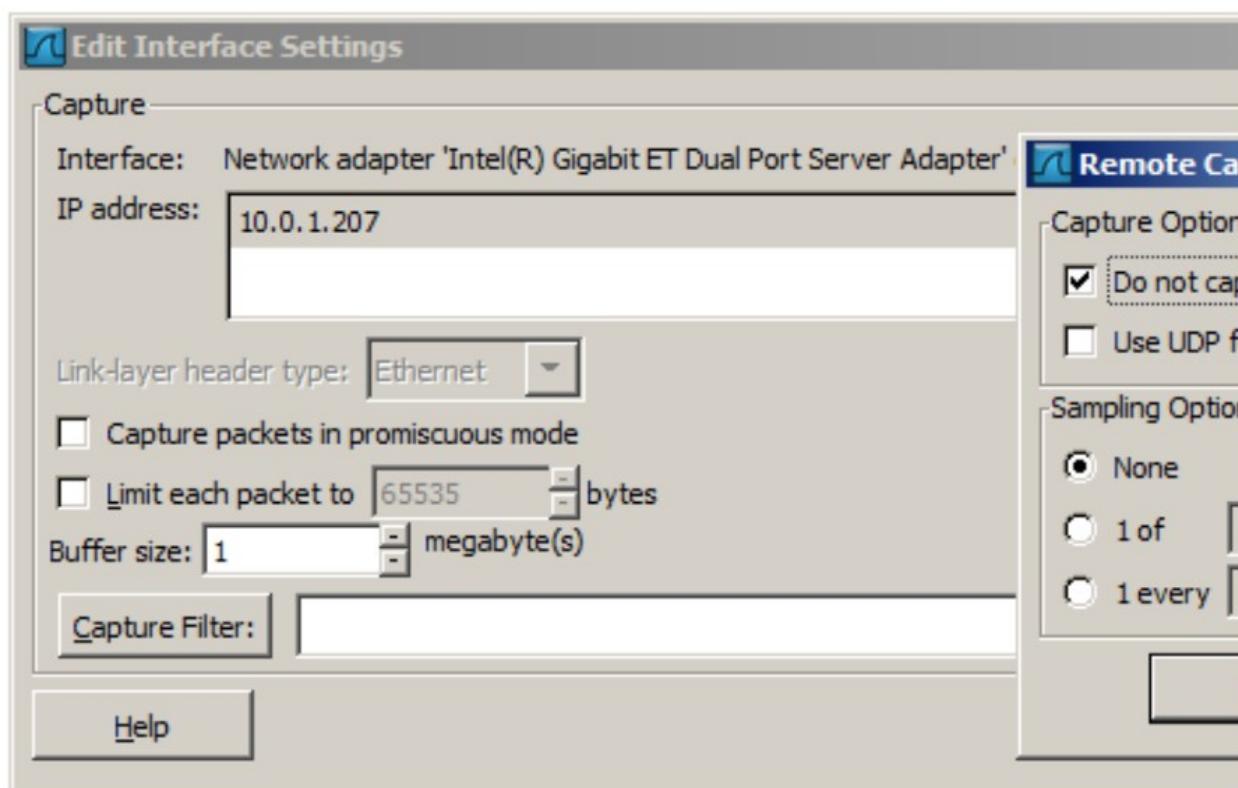
Хэрэв алсын хостын интерфэйсийг чагнах процессийг эхлүүлэхэд тань баталгаажуулалт хэрэггүй бол энэ тохиргоог сонгоно. Ийнхүү тохируулах нь аюулгүй байдлын үүднээс илүү эрсдэлтэй байдаг.

*Password authentication  
(Нууц үзээр  
баталгаажуулах)*

Энэ тохиргоо нь зорилтот (target) хосттой холбогдох энгийн арга юм. Нууц үг, нэрийг холболт хийх үедээ тохируулж өгөх хэрэгтэй.

#### 4.9.2. Алсын зайнас чагнаас үйлдлийн тохиргоо (Remote Capture Settings)

Алсын зайнас чагнаас үйлдэл (remote capture) нь таны нөхцөлөөс хамааран тохируулагдах боломжтой. Зураг “4.4. Интерфэйсийн тохиргоог засварлах” цонх дээрх Алсын зайны тохиргоо (Remote Settings) товчлуур танд дараах сонголтыг хийх боломжийг олгоно. Энэ нь Зураг 4.11.-т үзүүлсэн цонхыг харуулна.



Зураг 4.11. Алсын зайнас чагнаас тохиргоо (Remote Capture Settings)

Энэхүү цонхноос та дараах параметрүүдийг тохируулах боломжтой.

*Do not capture own RPCAP traffic  
(Өөрийн RPCAP файлыг чагнахгүй байх)*

Энэ сонголт нь Алсын зайнаас пакет чагнах протокол (Remote Packet Capture Protocol) сервисийн дамжуулж байгаа болон мөн түүний хүлээн авч байгаа пакетуудыг чагнахгүй байх шүүлтүүрийг идэвхижүүлдэг.

Энэхүү рекурс нь линк (link)-ийг давхардсан (duplicate) пакеттай болгодог.

Интерфэйсийг буцааж вайршарк руу холбогдох үйлдэл хийж түүнийгээ чагнах гэж байгаагаас бусад үед энэ тохиргоог хаах хэрэгтэй.

*Use UDP for data transfer (Өгөгдөл дамжуулалтai UDP ашиглах)*

Алсаас чагналтын удирдлага мөн өгөгдлийн өгөгдлийн урсгал нь TCP протоколыг ашигладаг. Харин сонголт энэхүү протоколын тохиргоог UDP болгодог.

*Sampling option None (Түүвэрлэлтийн тохиргоо : None)*

Энэ сонголт нь Алсын зайнаас пакет чагнах протокол (Remote Packet Capture Protocol) сервисийг чагнах үеийн шүүлтүүрээр дамжсан бүх пакетаа буцаан илгээх тохиргоо юм. Хангалттай шугамын өргөнтэй байгаа үед энэ нь тийм ч хүндрэлтэй асуудал биш юм.

*Sampling option 1 of x packets  
(Түүвэрлэлтийн тохиргоо : x пакетад 1)*

Энэ сонголт нь Алсын зайнаас пакет чагнах протокол (Remote Packet Capture Protocol) сервисийг зөхөн дэд түүвэрлэлийн өгөгдлөө дамжуулах тохиргоог хийдэг. Ингэхдээ пакетын тоонд суурилна. Энэ тохиргоо нь шугамын өргөн нь хангалттай биш үед өөрийн шугамын өргөнөөс илүү хэмжээтэй шугамын өргөнтэй сүлжээг чагнах боломжийг олгодог.

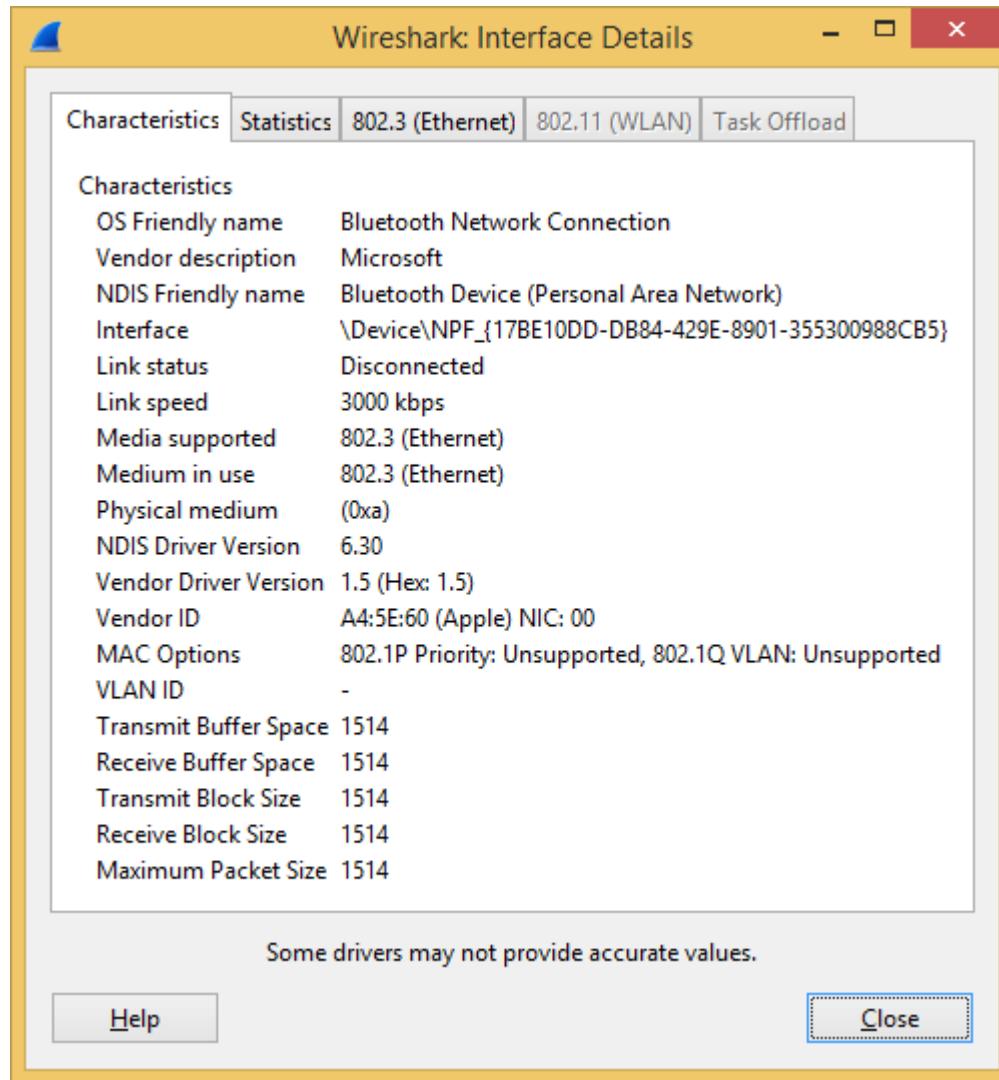
*Sampling option 1 every x milliseconds  
(Түүвэрлэлтийн тохиргоо : x миллисекунд бүрт 1 пакет)*

Энэ тохиргоо нь Алсын зайнаас пакет чагнах протокол (Remote Packet Capture Protocol) сервисийг хугацаанаас хамааруулан түүврээс дэд хэсгийг өгөгдлийг дамжуулах тохиргоог хийдэг. Энэ тохиргоо нь шугамын өргөн нь хангалттай биш үед өөрийн шугамын өргөнөөс илүү хэмжээтэй шугамын өргөнтэй сүлжээг чагнах

боломжийг олгодог.

#### 4.10. Интерфэйсийн дэлгэрэнгүй (Interface Details)

*Capture (Чагнах) → Interface (Интерфэйс) цохны Details (Дэлгэрэнгүй) хэсгийг сонгоход вайршарк програм танд Wireshark Interface Details (вайршарк интерфэйсийн дэлгэрэнгүй) цонхыг дэлгэцэнд харуулна. Энэ цонх нь танд тухайн сонгон авсан интерфэйсийн шинж чанар, статистикийг харуулдаг.*



Зураг 4.12. Интерфэйсийн дэлгэрэнгүй (Interface Details)

Энэ цонх нь зөвхөн Виндовс орчинд боломжтой.

#### 4.11. Чагнасан файлууд болон файлын горимууд (Capture files and file modes)

Чагнах процесс ажиллахад *либкап чагнах хэрэглүүр* (*libpcap capturing engine*) ажиллаж пакетуудыг сүлжээний картнаас цуглувалж авах ба түүнийгээ харьцангуй жижигхэн кернел буферт (kernel buffer)-т хадгалдаг. Энэхүү буфер дэх өгөгдлийг вайршарк програм уншиж түүнийгээ хэрэглэгчийн тодорхойлж өгсөн чагнах файл руу бичиж хадгалдаг.

Дээрх буфер дэх өгөгдлийг чагнах файл руу хадгалахад өөр өөр горимоор (mode) хадгалах боломжтой.

##### Зөвлөмж

Их хэмжээний өгөгдлөтэй ажиллах үед (хэдэн зуун МВ) эсвэл ачаалалтай сүлжээний интерфэйсээс чагнах үедээ чагнасан файлыг олон файл руу хадгалах (*Multiple files*) горимоор хадгалах нь зүйтэй юм. Ингэснээр их файлтай ажиллахад систем удах магадлалаас зайлсхийгээд зогсохгүй дараа нь чагнаж бичсэн файлтайгаа ажиллахад ч гэсэн таатай болдог.

*Олон файлд хадгалах горим* (*Multiple files*) ашиглах сүлжээний агуулгатай холбоотой мэдээллийг 2 өөр файлд хуваан хадгалах магадлалтай. Вайршарк ачаалласан пакет өгөгдлийн агуулгын талаарх мэдээллийг хадгалж байдаг учраас вайршарк програм энэ үед агуулгатай холбоотой алдааг өгч магадгүй мөн агуулгатай холбоотой протоколын мэдээллийг ч гэсэн хадгалж байдаг. (Жишээлбэл: *холболт тогтоох ye* (*establishing phase*)-ийн мэдээлэл солилцож байгаа үед дараагийн пакетад харгалзах агуулгатай байдаг). Вайршарк нь ачааллагдсан файлын агуулгын талаарх мэдээллийг агуулдаг учраас олон файлыг хэрэглэх горим (*multiple file modes*) нь агуулгыг нь хуваадаг. Хэрэв холболт тогтоох (*establishing phase*) үе нь нэг файл руу хадгалагдсан бөгөөд бусад мэдээлэл нь өөр файлд байгаа бол та тухайн файлд байхгүй хэсгийг нь харж чадахгүй. Өөрөөр хэлбэл та тухайн холболттой хамааралтай чухал мэдээллүүдийг харж чадахгүй байх магадлалтай.

**Хавсралт В Files and Folders** –тээс олон файлд хэрэглэгдэх файлууд, фолдеруудын талаарх мэдээллийг үзнэ үү.

*Хүснэгт 4.1. Чагнах үеийн горимууд (Capture file mode selected by capture options)*

Файл (file) сонголт	Олон файл хэрэглэх (Use multiple files) сонголт	N ширхэг файлтай ринг буфер (Ring buffer with n files) сонголт	Горим (Mode)	Үр дүнд нь үүсэх файлын нэрс

-	-	-	<i>Ганц ширхэг түр зуурын файл (Single temporary file)</i>	wiresharkXXXXXX (XXXXXX нь дахин давтагдахгүй тоо байна)
foo.cap	-	-	<i>Ганц файл (нэр нь тодорхой) (Single named file)</i>	foo.cap
foo.cap	x	-	<i>Үргэлжилсэн олон файл (Multiple files, continuous)</i>	foo_00001_20100205110102.cap, foo_00002_20100205110318.cap, ...
foo.cap	x	x	<i>Ринг буфер дэх олон файл (Multiple files, ring buffer)</i>	foo_00001_20100205110102.cap, foo_00002_20100205110318.cap, ...

#### *Ганц ширхэг түр зуурын файл (Single temporary file)*

Өгөгдмөл тохиргоогоор түр зуурын (temporary) файл үүсгэж хэрэглэдэг. Чагнах процесс зогссоны дараа тухайн файлыг өөрийн хүссэн нэрийг өгч хадгалах боломжтой.

#### *Ганц файл (нэр нь тодорхой) (Single named file)*

Ганц файл хэрэглэгдэнэ. Хэрэв шинэ чагнах файлыг өөрийн зааж өгсөн фолдер дотор хадгалахыг хүсч байвал энэ горимыг сонгоно.

#### *Үргэлжилсэн олон файл (Multiple files, continuous)*

Дээр дурдсан ганц файлд хадгалахтай ижилхэн хадгална. Гэхдээ тодорхой нөхцөл биелмэгц дахин шинээр нэг файл үүсгэн олон файлд хадгалдаг.

#### *Ринг буфер дэх олон файл (Multiple files, ring buffer)*

Дээр дурдсан үргэлжилсэн олон файлын тохиргоотой төстэй. Өөрөөр хэлбэл тодорхой нэгэн нөхцөл биелмэгц өөр файл шинээр нээж хадгалдаг. Энэ тохиргоо нь n файлтай ринг буфериин хэмжээ (ring buffer with n files) –нд хүрээгүй байвал шинээр файл үүсгэнэ. Харин энэхүү буфериин хэмжээ дүүрсэн бол хуучин хадгалсан файлыг дарж хадгалах зарчмаар хадгалагддаг (Тиймээс ринг буфер гэж нэрлэгддэг).

Энэ горим нь их хэмжээний өгөгдөл хадгалж байгаа тохиолдолд дискний хэмжээг хэт их ашиглах эрсдэл үүсэхээс сэргийлдэг.

#### **4.12. Линк түвшний толгойн төрөл (Link-layer header type)**

Дараах цөөн тохиолдлуудаас бусад тохиолдолд танд линк түвшний толгойн төрлийг (Link-layer header type) тодорхойлох шаардлага гарагчдаг.

Этернет (ethernet) төхөөрөмжөөс чагнах үйлдэл хийж байгаа үед “Ethernet” эсвэл “DOCSIS” гэсэн 2 сонголтоос сонгох хэрэгтэй болно. Хэрэв та DOCSIS урсгалыг Ethernet рүү чагнахаар оруулдаг *Циско Кабел Терминашин Систем* (*Cisco Cable Modem Termination System*) хэрэглэж байгаа бол “DOCSIS”-г сонгох хэрэгтэй. Бусад тохиолдолд “Ethernet”-г сонгоно.

Хэрэв та зарим BSD систем дээрээс 802.11 төхөөрөмжийг чагнаж байвал “Ethernet” эсвэл “802.11” гэсэн 2 сонголтоос сонгох шаардлагатай болно. “Ethernet” нь чагнасан пакетуудыг хуурамч (cooked) Этернет (Ethernet) толгойтой (header) болгоно. “802.11” нь тэдгээрийг IEEE 802.11 бүтцийн бүрэн толгойтой (header) болгоно. Тийм учраас хэрэв чагнах процесс тань 802.11 толгойг унших шаардлагатай байвал та “802.11”-г сонгох шаардлагатай.

Хэрэв та синхрон сериал шугамтай холбогдсон Endace DAG карт дээр чагнаж байгаа бол танд “PPP over serial” эсвэл “Cisco HDLC” гэсэн сонголт гарч ирнэ. Хэрэв тухайн сериал шугам дээрх протокол нь PPP бол “PPP over serial” гэсэн сонголтыг сонгоно харин тухайн сериал шугам дээрх протокол нь Cisco HDLC бол “Cisco HDLC”-г сонгоно.

Хэрэв та ATM сүлжээнд холбогдсон байгаа Endace DAG карт дээр пакет чагнах шаардлагатай болсон бол танд “RFC 1483 IP-over-ATM” эсвэл “Sun raw ATM” гэсэн сонголт гарч ирнэ. Хэрэв сүлжээний чагнаж буй урсгал нь зөвхөн RFC 1483 LLC-encapsulated IP байвал эсвэл чагнасан файлыг ашиглах шаардлагад тань SunATM толгой (SunATM headers) шаардлагагүй бол “RFC 1483 IP-over-ATM”-г сонгох хэрэгтэй. Эсрэг тохиолдолд “Sun raw ATM”-г сонгоно.

#### **4.13. Чагнаж байх үедээ шүүлтүүр ашиглах (Filtering while capturing)**

Вайршарк програм нь либпкап шүүлтүүрийн хэл (libpcap filter language)-ийг чагнах үеийн шүүлтүүрээр ашигладаг. Түлхүүр үгсийн товч тайлбарыг танилцууллаа. Үүний талаар бүрэн документ (documentation) нь pcap-filter man хуудсанд байдаг. Мөн чагнах үеийн шүүлтүүрийн жишээг <https://wiki.wireshark.org/CaptureFilters> хуудаснаас олж үзэх боломжтой.

Зураг 4.3. –т үзүүлсэн чагнах үед хийх сонголтуудын *шүүлтүүр* (*filter*) талбарт чагнах үеийн шүүлтүүрийн түлхүүр үгийг оруулна.

Чагнах үеийн шүүлтүүр нь холбоосууд (and/or)-аар холбогдсон энгийн цуваа хэлбэрээр түлхүүр үгээ авдаг бөгөөд эдгээрийн өмнө нь мөн үгүйсгэл (not) түлхүүр үгийг хэрэглэх боломжтой

```
[not] шүүлт [and|or [not] шүүлт ...]
```

**Жишээ 4.1.** Энд тодорхой нэг хостын telnet –ийг шүүн чагнах үйлдэл хийж байна.

```
tcp port 23 and host 10.0.0.5
```

Энэ жишээ нь 10.0.0.5 хост руу илгээж байгаа мөн тухайн хостоос ирж байгаа телнет (telnet) өгөгдлийг чагнаж байна. Та дээрх жишээнээс хэрхэн шүүлтүүрийн энгийн түлхүүр үг (“tcp port”, “host”) -ийг ашиглах мөн тэдгээрийг хэрхэн (and) холбоосоор холбож байгааг харах боломжтой.

**Жишээ 4.2.** Энд 10.0.0.5 хостоос бусад бүх telnet өгөгдлийг чагнах үйлдлийг хэрхэн хийхийг харуулж байна.

```
10.0.0.5 хостоос бусад telnet өгөгдлийг шүүн чагнах үйлдэл хийж байна.
```

```
tcp port 23 and not src host 10.0.0.5
```

Шүүлтийн түрхүүр үгс

```
[src|dst] host <host>
```

Энэ түлхүүр үг нь хостын IP хаяг эсвэл нэрээр нь шүүх боломжийг олгодог.

Мөн түүнчлэн та энэ түлхүүр үгийн өмнө нь илгээгч болон хүлээн авагчийг нь тодорхойлох *src|dst* түлхүүр үгийг хэрэглэх боломжтой. Хэрэв өмнө нь *src|dst* түлхүүр үг байхгүй байвал илгээгч болог хүлээн авагч 2 талаас хамааралгүй бүх пакетыг чагнана.

```
ether [src|dst] host <ehost>
```

Энэ түлхүүр үг нь танд Этернет (Ethernet) хостын хаягийг тодорхойлох боломж олгоно. Та *ether host* гэсэн 2 түлхүүр үгийн дунд нь *src|dst* гэсэн түлхүүр үгийг нэмж өгөх замаар зөвхөн өөрийн харахыг хүсч буй илгээгч эсвэл хүлээн авагч талыг нь харах боломжтой. Хэрэв *src|dst* түлхүүр үг байхгүй байвал 2 талаас илгээж эсвэл хүлээн авч

	байгаа бүх пакетыг чагнана.
<i>gateway host &lt;host&gt;</i>	Энэ шүүлтүүр нь танд гарц (gateway)-аар ашиглагдаж байгаа хостын пакетыг шүүх боломжийг олгоно.
	Энд Этернет (Ethernet) илгээгч эсвэл хүлээн авагч хаяг нь хост байх ба илгээгч эсвэл хүлээн авагч IP хаяг нь хост гэсэн үг биш юм.
<i>[src dst] net &lt;net&gt; [{mask &lt;mask&gt;} {len &lt;len&gt;}]</i>	Энэ шүүлтийн түлхүүр үг нь сүлжээний хаяг дээр шүүлт хийх боломж олгоно. Энэ түлхүүр үгийн өмнө <i>src dst</i> үгийг оруулснаар илгээгч эсвэл хүлээн авагчийн аль хэсгийг нь сонирхож байгаагаа ялгаж харах боломжтой юм. Хэрэв энэхүү <i>src dst</i> түлхүүр үгийг урд нь нэмж оруулаагүй бол илгээгч хүлээн авагч 2 талыг 2-ууланг нь чагнана. Сүлжээний хаягийн маск (Subnet mask) бичихдээ netmask эсвэл CIDR хэлбэрээр алинаар нь ч бичсэн болно.
<i>[tcp udp] [src dst] port &lt;port&gt;</i>	Энэ түлхүүр үг нь TCP, UDP портын дугаараар шүүнэ. Энэхүү түлхүүр үгийн өмнө нь <i>src dst</i> түлхүүр үгийг <i>tcp udp</i> –тэй оруулж өгснөөр илгээгч эсвэл хүлээн авагч талын аль хэсгийн алийг нь харахыг хүсэж байгаагаа тодорхойлох боломжтой. <i>tcp udp</i> түлхүүр үгсийн аль нэг нь <i>src dst</i> –ийн өмнө байх ёстой. Хэрэв энэ түлхүүр үг байхгүй бол шүүлтүүр нь TCP болон UDP протоколуудыг 2-ууланг нь харуулах болно.
<i>less greater &lt;length&gt;</i>	Энэ түлхүүр үг нь танд тухайн пакетын хэмжээнээс хамааруулан шүүлтүүр хийх боломж олгоно. Ингэхдээ тухайн зааж өгсөн хэмжээнээс их, тэнцүү эсвэл бага гэсэн 3-н сонголтоос сонгож тохиргоогоо оруулна.
<i>ip ether proto &lt;protocol&gt;</i>	Энэ түлхүүр үг нь танд Ethernet эсвэл IP (layer) түвшинд шүүлтүүр хийх боломжийг олгоно.
<i>ether ip broadcast multicast</i>	Энэ түлхүүр үг нь танд Ethernet эсвэл IP broadcast эсвэл multicast хаягаар шүүх боломж олгоно.
<i>&lt;expr&gt; relop &lt;expr&gt;</i>	Энэ түлхүүр үг нь танд бүрэн шүүлтүүрийг үүсгэх боломж олгоно. Энэ сонголтоор пакетын байтууд

эсвэл пакетын байтуудын завсар гэх мэт зүйлсийг тодорхойлж болдог. Pcap-filter man хуудаснаас <http://www.tcpdump.org/manpages/pcap-filter.7.html> дэлгэрүүлэн үзнэ үү.

#### **4.13.1. Алсын зайд дахь урсгалын автомат шүүлтүүр (Automatic Remote Traffic Filtering)**

Хэрэв вайршарк програм алсын зайнаас ажиллаж байвал (Remotely – SSH, Exported X11 window, terminal server гэх мэт зүйлсийг ашиглан холбогдоно) алсын зайд байгаа сүлжээний агуулга (content) нь сүлжээн дээгүүр дамжигдах ёстой. Энэ нь яг сонирхож байгаа мэдээллээс гадна өөр чухал бус маш их урсгалыг сүлжээн дээгүүр нэмж дамжуулдаг.

Үүнээс сэргийлэхийн тулд хэрэв тухайн чагнах процесс маань алсын зайд байвал түүнийг автоматаар шүүх шүүлтүүрийг үүсгэдэг. Ингэхдээ орчны хувьсагч ашиглан шүүдэг.

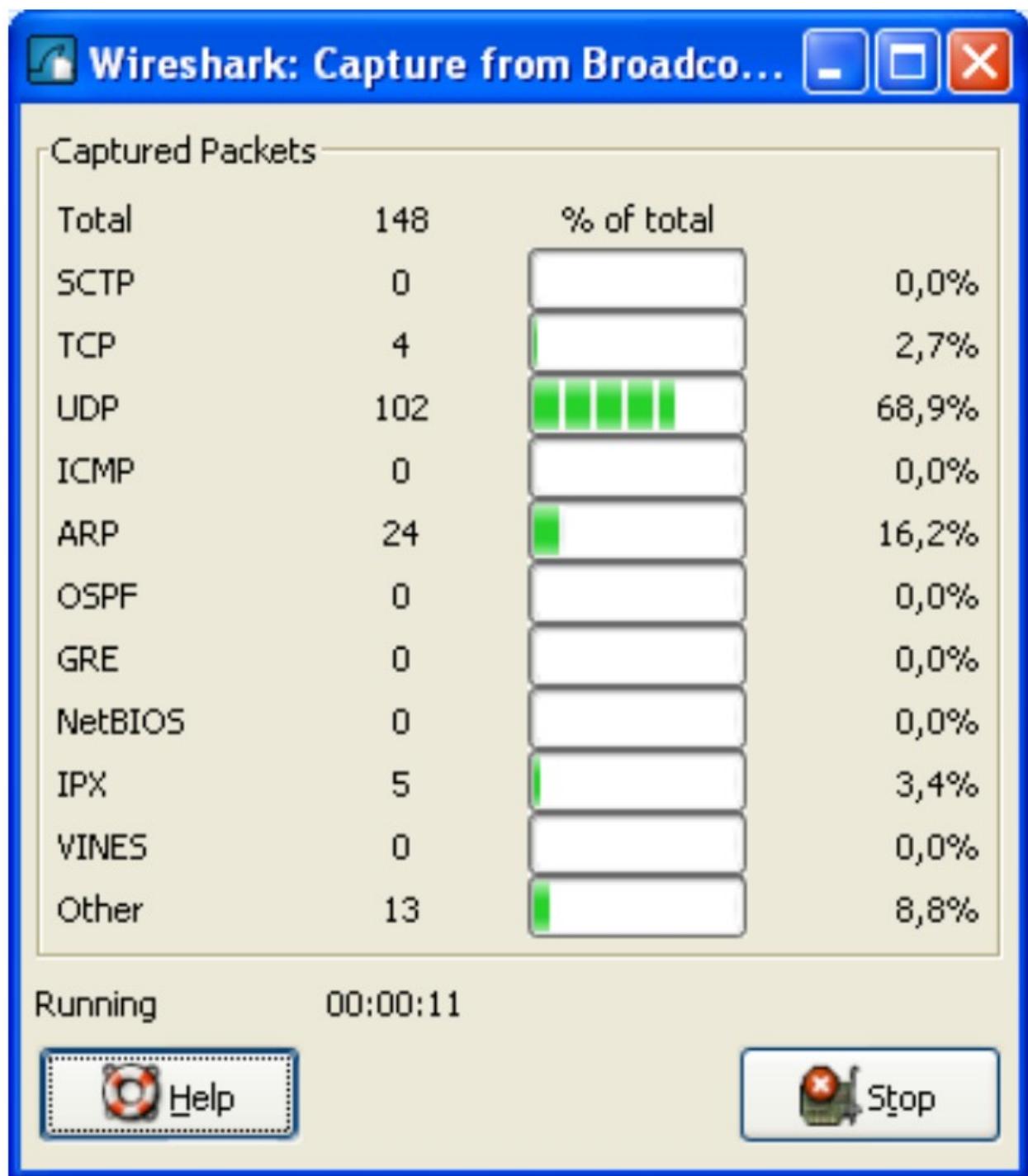
Дараах орчны хувьсагчид ашиглагдана.

<i>SSH_CONNECTION</i> (ssh)	<remote IP> <remote port> <local IP> <local port>
<i>SSH_CLIENT</i> (ssh)	<remote IP> <remote port> <local port>
<i>REMOTEHOST</i> (tcsh, others?)	<remote name>
<i>DISPLAY</i> (x11)	[remote name]:<display num>
<i>SESSIONNAME</i> (terminal server)	<remote name>

Виндовс орчинд Remote Desktop Services-г ашиглаж байгаа бол вайршарк програм үйлдлийн системийн хувилбарыг асуудаг.

#### **4.14. Чагнах процесс ажиллаж байх үед (While capture is running)**

Чагнах процесс ажиллаж байх үед дараах цонх харагдана.



Зураг 4.13. Чагнах процесийн мэдээлэл (Capture info)

Энэ цонх нь хэрэглэгчид чагнах процесс эхэлснээс хойш хэр их пакет чагнагдсан болохыг харуулна:

Энэхүү цонхыг **Capture → Options** хэсгийн “**Hide capture info dialog**” гэсэн сонголтыг ашиглан алга болгож болно.

#### **4.14.1. Чагнах процесийг зогсоох**

Чагнах процесийг дараах арга замуудыг ашиглан зогсоно.

- ❖ Capture info цонхны [Stop] товчийг дарах
- ❖ Capture → Stop сонголтыг ашиглан
- ❖ Үндсэн товчлуурын (toolbar) Stop товчлуурыг дарж
- ❖ **Ctrl+E** дарж
- ❖ Зогсоох нөхцөлүүдийн аль нэг нь биелсэн тохиолдолд автоматаар зогсоно.  
(Жишээлбэл: Өгөгдлийн дамжуулах хамгийн их хэмжээ болсон тохиолдолд)

#### **4.14.2. Чагнах процесийг дахин эхлүүлэх**

Чагнах процесийн холболт нь өмнөхтэй ижилхэн байдлаар дахин эхлүүлэгдэнэ. Бид эхлээд цуглуулсан бүх пакетуудыг хасна. Хэрэв хэрэгцээтэй пакетууд цуглуулагдаагүй бол тэдгээрийг устгасан дээр байдаг.

Дахин эхлүүлэх нь Чагнах процесийг зогсоогоод буцаан эхлүүлж буйтай ижилхэн үйлдэл хийдэг энгийн функц юм. Дахин эхлүүлэх үйлдлийг дараах аргуудаар хийж болно.

- ❖ Capture → Restart сонголтыг сонгох
- ❖ Үндсэн товчлуурын (toolbar) Restart товчийг дарах

## **БҮЛЭГ V**

### **5. ФАЙЛЫН ОРОЛТ, ГАРАЛТ, ХЭВЛЭХ ҮЙЛДЭЛ**

## **5.1. Танилцуулга**

Энэ бүлэгт бид цуглуулсан файлын оролт гаралтын талаар авч үзнэ.

- Олон төрлийн файлын формат дээрх файлыг нээх
- Цуглуулсан файлуудыг олон төрлөөр хадгалах, экспорт хийх
- Цуглуулсан файлуудыг нийлүүлэх
- Пакетын хекс (hex dump) өгөгдлийг агуулсан текст файлыг импорт хийх
- Хэвлэх

## **5.2. Чагнасан файлыг нээх (Open capture files)**

Вайршарк програм өөрийн өмнө нь чагнаж хадгалсан файлуудаа уншдаг. Өмнө нь хадгалсан файлуудыг унших үйлдлийг хийхдээ **File → Open** эсвэл үндсэн товчлуурууд (toolbar)-ын **нээх** товчийг дараах сонголтыг сонгоно. Вайршарк програм **File Open** цонхыг дэлгэцэнд харуулах бөгөөд энэ цонхны талаар дэлгэрэнгүйгээр 5.2.1 хэсэгт авч үзнэ.

Хулганыг ашиглан чирч оруулах нь илүү хялбархан юм. (Drag and drop)

Өөрийн файл менежер дээр байгаа файлыг хулганы курсорыг ашиглан чирэх замаар вайршарк програмын үндсэн цонхонд оруулах боломжтой. Гэхдээ энэхүү чирэх үйлдэл нь бүх үйлдлийн систем дээр дэмжигдэхгүй байх магадлалтай.

Хэрэв та одоогийн чагнаж буй файлаа хадгалаагүй бол танаас хадгалах эсэхийг тань асуудаг. Энэ нь өгөгдөл устахаас сэргийлсэн үйлдэл юм. Гэхдээ энэ тохиргоог өөрчлөн анхааруулга, асуух үйлдэл хийхгүй болгох боломжтой. Үүнийг тохиргоо (preference) хэсгийг ашиглан хийнэ.

Түүнчлэн вайршарк програмын үндсэн файлын төрөл нь (pcapng) боловч вайршарк програм нь өөр сүлжээний орчин чагнах програмуудын үүсгэсэн олон төрлийн файлуудыг унших чадвартай. 5.2.2. хэсэгт вайршарк програм ямар ямар файлын төрлүүдийг унших боломжтой талаар дурдсан.

### **5.2.1. Чагнасан файл нээх (Open Capture File)**

Энэ цонх нь танд өмнө нь хадгалсан пакет өгөгдлөө хайх улмаар түүнийгээ вайршарк програмын үндсэн цонхонд нээх боломжоор хангана. Дараах хэсгүүдэд вайршарк програмын “Open File” цонхны ажиллагааг жишээ болгон харууллаа. Энэ цонх хэрхэн харагдах нь системээс шалтгаалах хэдий ч функционал үүргийн хувьд ялгаатай зүйл байхгүй.

Бүх үйлдлийн системийн хувьд нийтлэг шинж чанарууд:

- Файл болон фолдер сонгох
- Өөрийн сонгосон файлаа нээхийн тулд **Open** эсвэл **OK** товчийг дараах

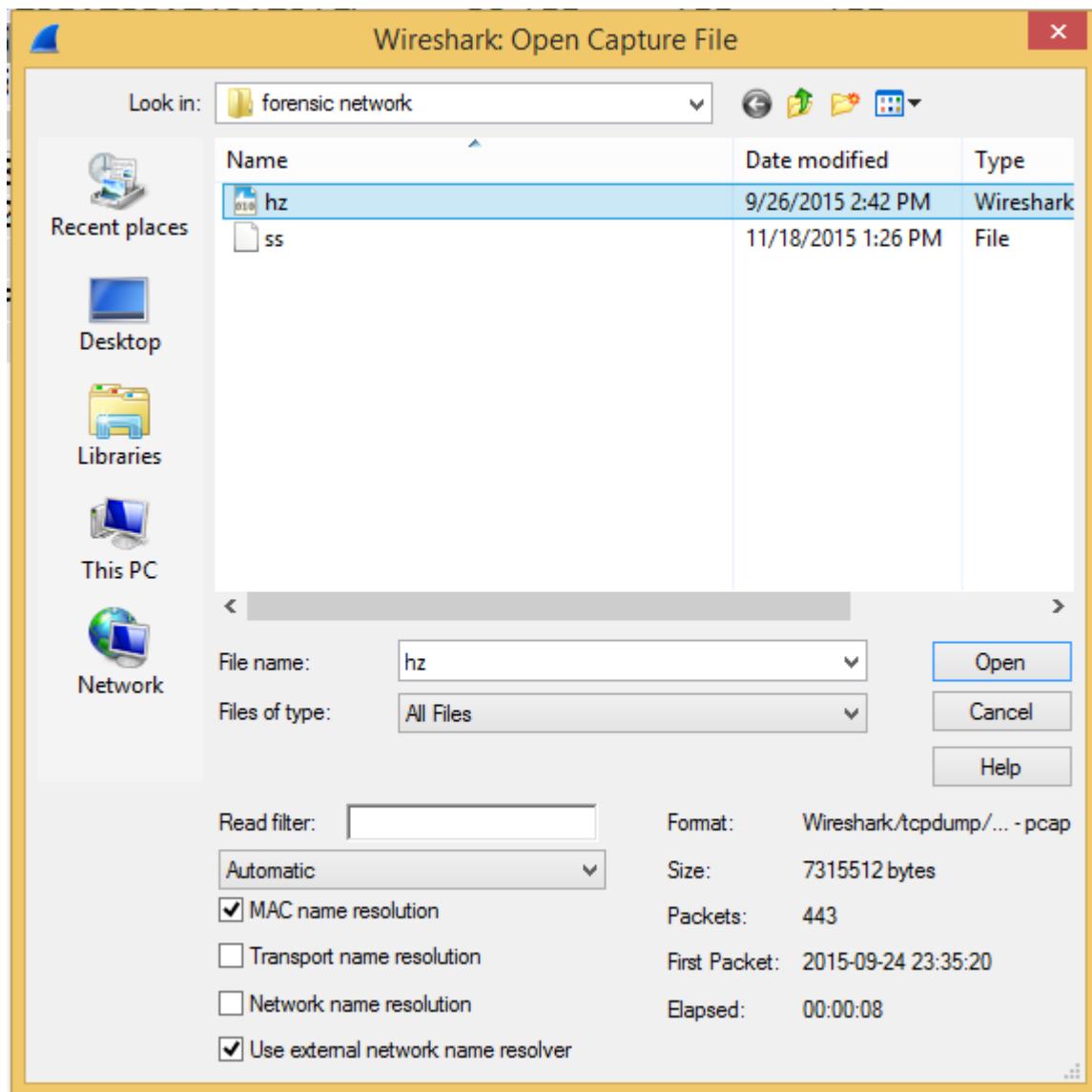
- Вайршарк програм руу буцах (ямар нэгэн файл нээж ачааллахаа болих) бол **Cancel** товчлуурыг дарах

Энэхүү цонхны стандарт шинж чанар дахь вайршарк програмын нэмэлт өргөтгөл:

- Файлын хэмжээ, тухайн файлд байгаа пакетын тоо гэх мэт мэдээллийг харах
- Filter товчлуур болон шүүлтүүрийн талбар (filter field)-р дэлгэцийн шүүлтүүрийг тодорхойлох. Энэ шүүлтүүр нь шинэ файл нээх үед хэрэглэгдэнэ. Filter товчлуур дээр дарснаар вайршарк програм танд *Шүүлтүүр (Filter)* цонхыг харуулна. (Шүүлтүүрийн талаар 6.3. “**Пакетыг дэлгэцэнд харах үеийн шүүлтүүр (Filtering packets while viewing)**” хэсгээс дэлгэрүүлэн уншина уу)
- Нэрийн хөрвүүлэлтийн ямар төрлийг ашиглах вэ гэдгээ “... name resolution”-ын хэрээст талбарыг ашиглан сонгоно. Илүү дэлгэрэнгүй уншихыг хүсвэл 7.7. “**Нэрийн хөрвүүлэлт (Name resolution)**” хэсгийг үзнэ үү.

#### **Их хэмжээний пакет файл ачааллахдаа цаг хугацаа хэмнэх**

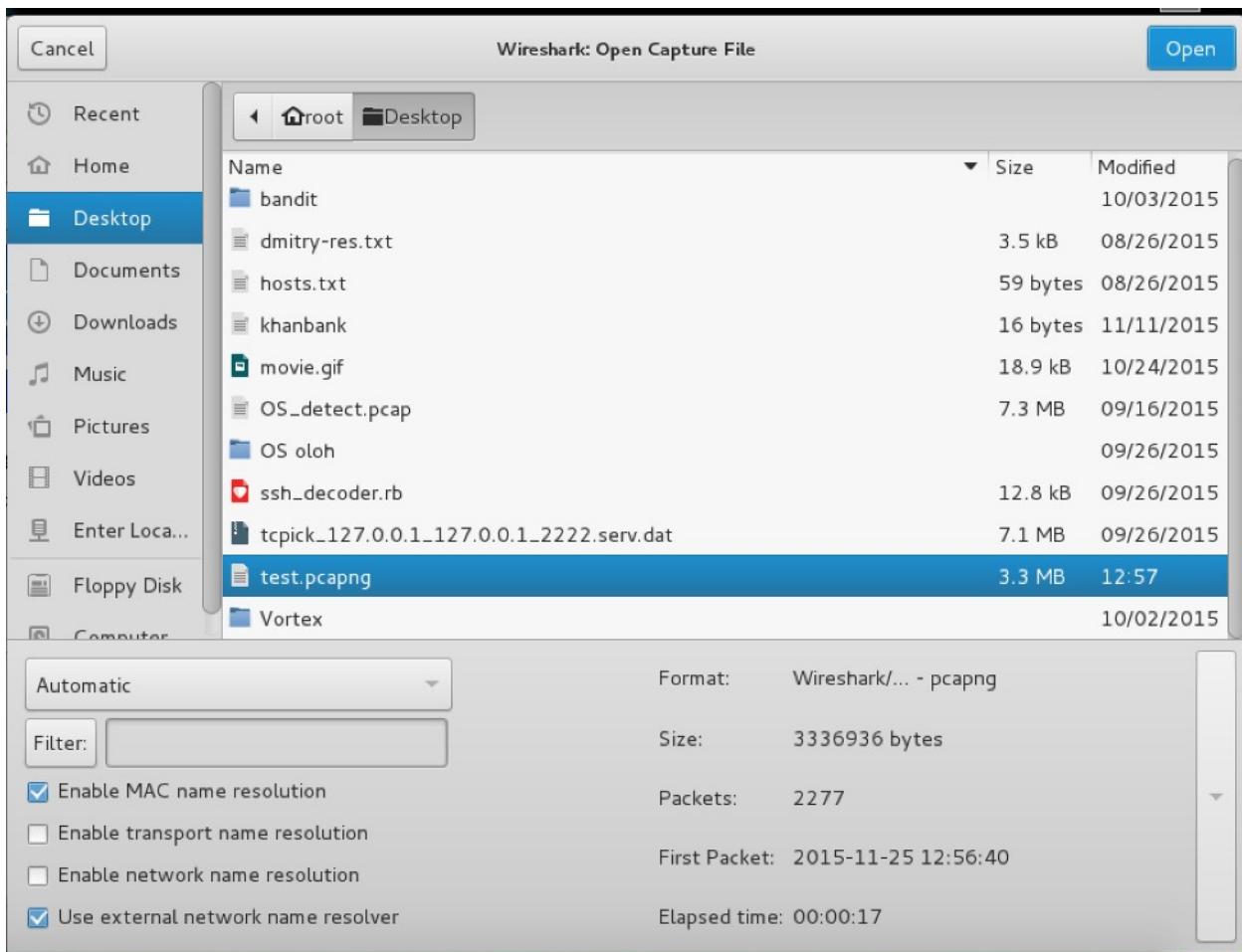
Их хэмжээний пакет өгөгдлийг бүгдийг нь дэлгэцэнд нээснийхээ дараа нь эдгээр шүүлтүүрийг идэвхижүүлэх боломжтой. Гэхдээ эдгээр шүүлтүүрийн тохиргоог нээхээсээ өмнө хийж өгснөөр их хэмжээний файлыг санах ой руу ачааллаж нэмэлт цаг алдахгүй байх давуу талтай юм.



Зураг 5.1. Виндовс орчин дэх Нээх (Open) цонх

Энэ цонх нь виндовс үйлдлийн системүүд дээр өрөнхийдөө ижилхэн байдаг.

- Help товчлуур нь таныг хэрэглэгчийн ашиглах заавар рүү (user guide) хөтөлнө.



Зураг 5.2. Линукс болон Юникс орчин дахь Нээх (Open) цонх

- Хэрэв вайршарк програм таны сонгосон файлыг танихгүй байвал Нээх (Open) товчлуур нь саарал өнгөтэй болсон байх ба дарагдахгүй.

### 5.2.2. Оролтын файлын форматууд (Input File Formats)

Сүлжээний өгөгдлийг чагнах програмууд дээр цуглувлагдсан дараах төрлийн файлуудыг вайршарк програм нээх чадвартай.

- pcapng. Уян хатан, өргөтгөж болдог файлын төрөл бөгөөд энэ нь libpcap форматын үргэлжлэл болон гарч ирсэн. Вайршарк 1.8 болон түүний дараачийн хувилбарууд pcapng файлаар файлаа хадгалдаг. Өмнөх хувилбарууд нь libpcap форматаар хадгалдаг байсан.
- libpcap. Libpcap capture library-гийн ашигладаг (default) файлын төрөл. Энэ файлын төрлийг tcpdump, \_Snort, Nmap, Ntop гэх мэт олон програмууд ашигладаг.
- Oracle (өмнө нь Sun) snoop болон atmsnoop
- Finisar (өмнө нь Shomiti) Surveyor captures
- Microsoft Network Monitor captures

- Novell LANalyzer captures
- AIX iptrace captures
- Cinco Networks NetXray captures
- Network Associates Windows-based Sniffer мөн Sniffer Pro captures
- Network General/Network Associates DOS-based Sniffer (шахсэн эсвэл шахаагүй) captures
- AG Group/WildPackets/Savvius EtherPeek/TokenPeek/AiroPeek/EtherHelp/PacketGrabber captures
- RADCOM's WAN/LAN Analyzer captures
- Network Instruments Observer version 9 captures
- Lucent/Ascend рөүтэрийн debug гаралт
- HP-UX's nettle
- Toshiba's ISDN рөүтэрийн dump гаралт
- ISDN4BSD i4btrace utility
- traces from the EyeSDN USB S0
- IPLog format from the Cisco Secure Intrusion Detection System
- pppd logs (pppdump format)
- the output from VMS's TCPIPtrace/TCPtrace/UCX\$TRACE utilities
- the text output from the DBS Etherwatch VMS utility
- Visual Networks' Visual UpTime traffic capture
- the output from CoSine L2 debug
- the output from Accelgent's 5Views LAN agents
- Endace Measurement Systems' ERF format captures
- Linux Bluez Bluetooth stack hcidump -w traces
- Catapult DCT2000 .out files
- Gammu generated text output from Nokia DCT3 phones in Netmonitor mode
- IBM Series (OS/400) Comm traces (ASCII & UNICODE)
- Juniper Netscreen snoop captures
- Symbian OS btsnoop captures
- Tamosoft CommView captures
- Textronix K12xx 32bit .rf5 format captures
- Textronix K12 text file format captures
- Apple PacketLogger captures
- Captures from Aethra Telecommunications' PC108 software for their test instruments

Шинэ файлын форматууд үе үе нэмэгдэж орж байдаг.

Зарим пакетын төрөл болон түүний бүтцээс хамаараад вайршарк програм унших боломжгүй байх боломжтой. Ethernet цуглуулсан пакет нь ихэнх файлын форматаар дэмжигддэг хэдий ч PPP эсвэл IEEE 802.11 зэрэг пакетийн төрлүүд бүх файлын форматаас уншигдахгүй байх магадлалтай.

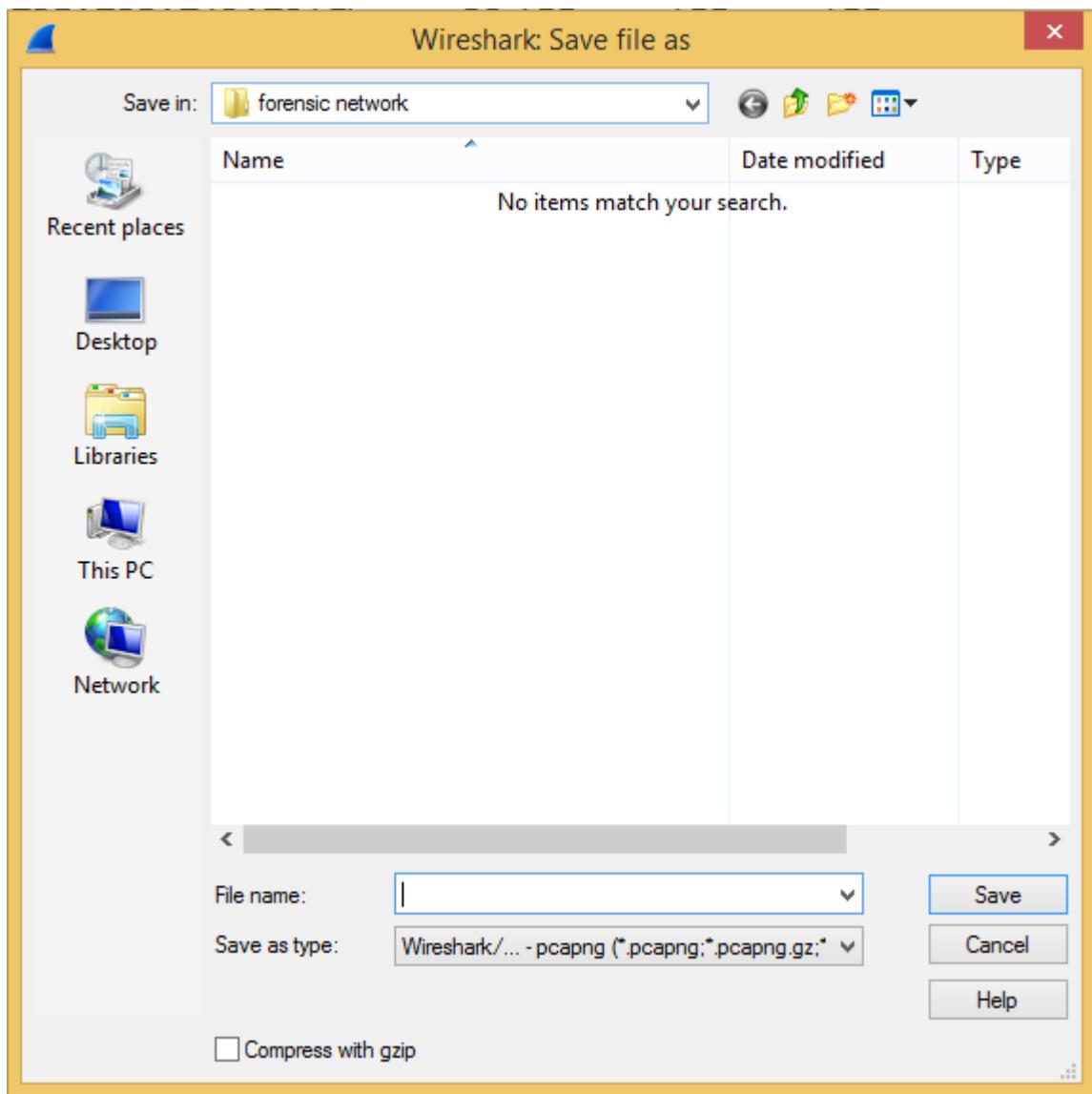
### **5.3. Цуглуулсан пакет өгөгдлийг хадгалах (Saving captured packets)**

Та цуглуулсан пакетуудаа **File → Save As...** сонголтыг ашиглан хадгалах боломжтой. Ингэхдээ та аль пакетуудыг хадгалах ямар файлын формат ашиглахыг өөрөө тодорхойлж өгөх боломжтой.

Хадгалах үед тухайн цуглуулсан пакет өгөгдлийн бүх мэдээлэл хадгалагдаггүй. Жишээлбэл: ихэнх файлын форматууд хэр их пакет гээгдсэн (dropped) болохыг бичиж авдаггүй. **B.1. “Цуглуулсан файлууд (Capture Files)”** хэсгийг үзнэ үү.

#### **5.3.1. Цуглуулсан файлыг хадгалах (Save Capture File As) цонх**

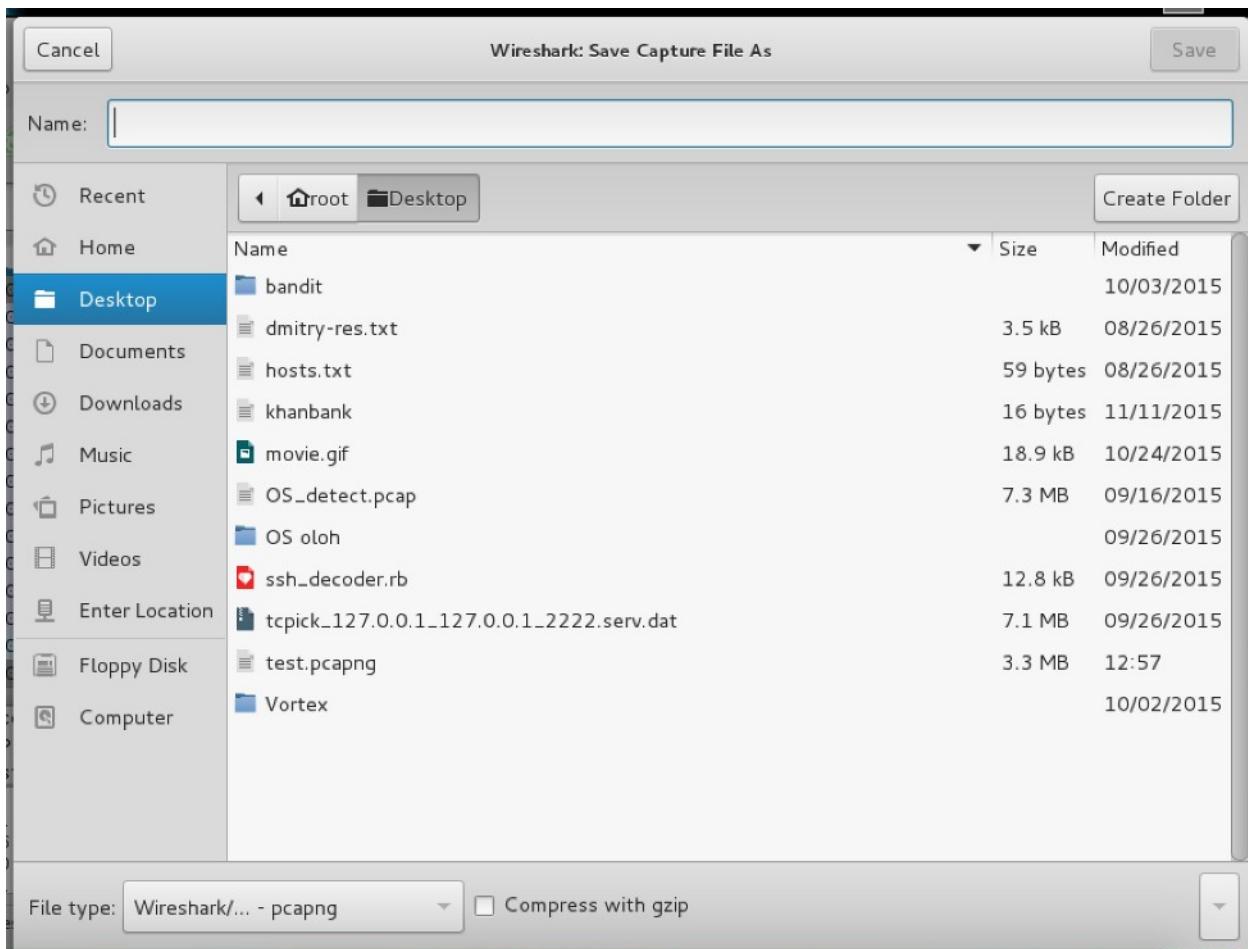
Цуглуулсан файлыг хадгалах (Save Capture File As) цонх нь танд одоогийн чагнасан байгаа пакет өгөгдлөө файл руу хадгалах боломж олгоно. Дараах хэсгүүдэд энэ цонхны жишээг үзүүллээ. Энэхүү цонхны харагдах байдал нь системээсээ хамаарах хэдий ч үндсэн фунц үйлдлүүд нь ижилхэн юм.



Зураг 5.3. Виндовс орчин дахь хадгалах (Save) цонх

Энэ цонх нь дараах зүйлсийг хийнэ.

- **Help** товчлуур нь хэрэглэх заавар луу хэрэглэгчийг хөтөлнө
- Хэрэв файлын өргөтгөлийг (.pcap) тодорхойлож өгөөгүй бол вайршарк өөрийн стандарт файлын өргөтгөлөөр файлыг хадгалдаг.



Зураг 5.4. Линукс болон Юникс систем дээрх хадгалах (Save) цонх

Энэ цонхыг ашиглан дараах үйлдлүүдийг хийх боломжтой.

1. Өөрийн файлыг хадгалахыг хүсч буй нэрийг оруулах
2. Өөрийн файлыг хадгалах фолдерийг сонгох
3. Хадгалах файлынхаа форматыг өөрчлөх. Дэлгэрэлүүлэн уншихыг хүсвэл 5.3.2. “Гаралтын файлын төрлүүд (Output File Formats)” хэсгийг уншина уу
4. Пакет өгөгдлийг шахах

Пакетын төрлөөсөө хамаараад зарим файлын төрлүүдээр хадгалах боломжгүй байх магадлалтай.

Вайршарк програм нь файлын форматын хөрвүүлэлт хийдэг.

Вайршарк програм дээр нэг файлын төрлөөр файлыг уншаад өөр файлын төрөл рүү хадгалах замаар файлуудыг хооронд нь хөрвүүлж болно.

1. Save эсвэл OK товчлуур дээр дарж өөрийн сонгосон файлыг халгална. Хэрэв хадгалах үед алдаа үүсвэл дэлгэцэнд алдаа өгдөг. Энэхүү алдааны мэдээлэл дээрх OK товчийг дарсны дараа та дахин хадгалахаар оролдох боломжтой.
2. Пакет өгөгдлийг хадгалахгүйгээр вайршарк програм руу буцахыг хүсвэл Cancel товчлуурыг дарна уу.

### **5.3.2. Гаралтын файлын форматууд (Output File Formats)**

Вайршарк програм өөрийн үндсэн файлын төрөл болох (pcapng) формат гадна бусад пакет өгөгдлөтэй ажиллах программууд унших боломжтой олон форматаар файлыг хадгалдаг.

**Файлын формат нь өөр байвал цагийн нарийвчлалийн тэмдэглэгээ нь өөр өөр байна.**

Одоо хэрэглэж буй файлын форматаас өөр файлын формат руу өөрчлөн хадгалах нь цагийн тэмдэглэгээний нарийвчлал бууруулдаг. 7.4. “Цагийн тэмдэглэгээ (Time Stamps)” хэсгээс дэлгэрүүлэн уншина уу.

Вайршарк програм нь дараах форматуудаар файлыг хадгалах боломжтой:

- pcapng (\*.pcapng). Уян хатан, өргөтгөж болдог файлын төрөл бөгөөд энэ нь libpcap форматын үргэлжлэл болон гарч ирсэн. Вайршарк 1.8 болон түүний дараачийн хувилбарууд pcapng файлын форматаар файлаа хадгалдаг. Өмнөх хувилбарууд нь libpcap форматаар хадгалдаг байсан.
- libpcap, tcpdump and various other tools using tcpdump's capture format (\*.pcap, \*.cap, \*.dmp)
- Accelgent 5Views (\*.5vw)
- HP-UX's nettl (\*.TRC0, \*.TRC1)
- Microsoft Network Monitor - NetMon (\*.cap)
- Network Associates Sniffer - DOS (\*.cap, \*.enc, \*.trc, \*.fdc, \*.syc)
- Network Associates Sniffer - Windows (\*.cap)
- Network Instruments Observer version 9 (\*.bfr)
- Novell LANalyzer (\*.tr1)
- Oracle (өмнө нь Sun) snoop (\*.snoop, \*.cap)
- Visual Networks Visual UpTime traffic (\*.\*)

Үе үе шинэ файлын форматууд нэмэгдэж байдаг.

Бусад протокол анализаруудад тодорхой төрлийн файлын өргөтгөлүүд шаардагдах магадлалтай.

Вайршарк програм тухайн файлын төрлийг тодорхойлохын тулд түүний агуулгыг нь шалгаж үздэг. Бусад протокол анализар програмуудын зарим нь зөвхөн файлын нэрний өргөлийг шалгадаг. Жишээлбэл. Та Sniffer дээр файлыг нээхийн тулд .cap өргөтгөлтэй афл хэрэгтэй болж болох юм.

## **5.4. Цуглүулсан файлуудыг нэгтгэх (Merging capture files)**

Зарим тохиолдолд хэрэглэгчдэд хэд хэдэн пакет файлуудыг нэг файл болгон нэгтгэх шаардлага гарч болно. Жишээлбэл хэрэв та олон интерфэйс дээр зэрэг чагнах процесс хийсэн бол тэдгээрийгээ нэгтгэх шаардлага гарч болох юм.

Вайршарк програм дээр файлуудыг нэгтгэх 3 арга байдаг.

- File → Merge цэсийг ашиглах. 5.4.1. “Чагнах файлыг нэгтгэх (Merge with Capture File)”-хэсгийг үзнэ үү. Хэрэв та вайршарк програм руу файл ачааллаагүй бол энэ цэс идэвхижихгүй.
- Үндсэн цонх (main window) руу олон файлыг хулганы курсороор чирч оруулах (drag and drop). Вайршарк програм энэ файлын пакетуудыг хугацааны дарааллын дагуу нэгтгэдэг. Хэрэв зөвхөн ганцхан файл үндсэн цонх руу чирч оруулвал одоо ачааллагдсан файлын оронд шинэ файлыг сольж ачаалладаг.
- Mergecap tool-ийг ашиглах. Энэ нь командын мөрөөс хэрэгждэг файлыг нэгтгэх хэрэглүүр юм. Энэ хэрэглүүрийг ашиглан файл нэгтгэх функцуудийн ихэнхийг нь хийх чадвартай. D.8 “mergecap: Олон файлыг нэг файл руу нэгтгэх (Merging multiple files into one)” хэсгээс дэлгэрүүлэн үзнэ үү.

### **5.4.1. “Чагнах файл нэгтгэх (Merge with Capture File)”**

Энэ цонх нь танд одоо ачааллагдсан байгаа файл дээр нэмж файл нэгтгэх боломжийг олгоно. Хэрэв одоогийн ачаалласан файлаа хадгалаагүй байвал түүнийг эхлээд хадгалах эсэхийг тань вайршарк програм эхлээд асууна.

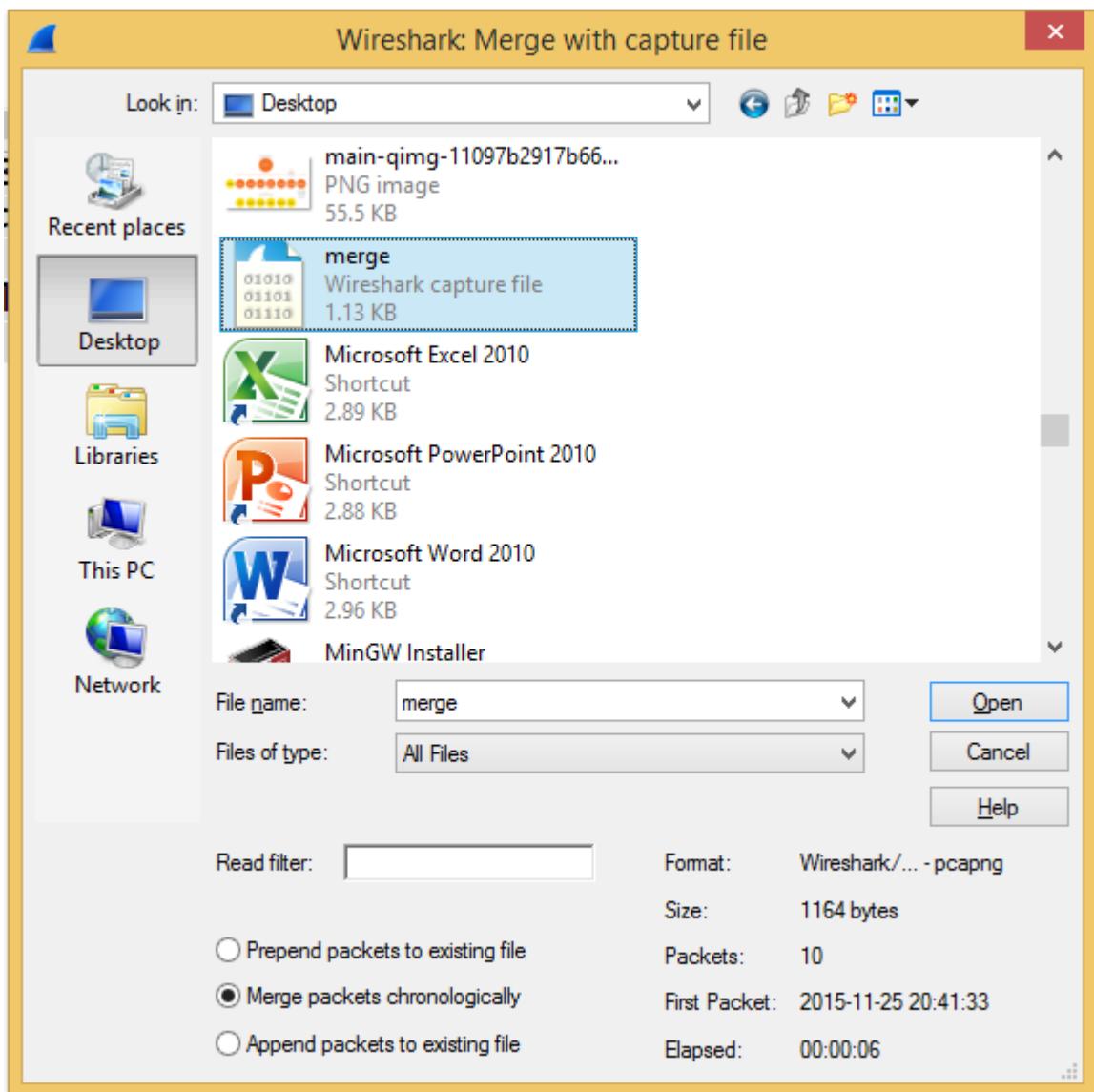
Энэ цонхны удирдлагын хэсгүүд нь 5.2.1. “Чагнасан файл нээх (Open Capture File)” хэсэг дэх цонхтой ижилхэн ажиллана.

Файл нэгтгэхтэй холбоотой удирдлагын хэсгүүд нь дараах үйлдлүүдийг хийдэг.

*Prepend packets to existing file*      Одоо ачааллагдсан байгаа файлын пакетын өмнө нь энэхүү цонхоор сонгосон файлыг нэмж хавсаргах

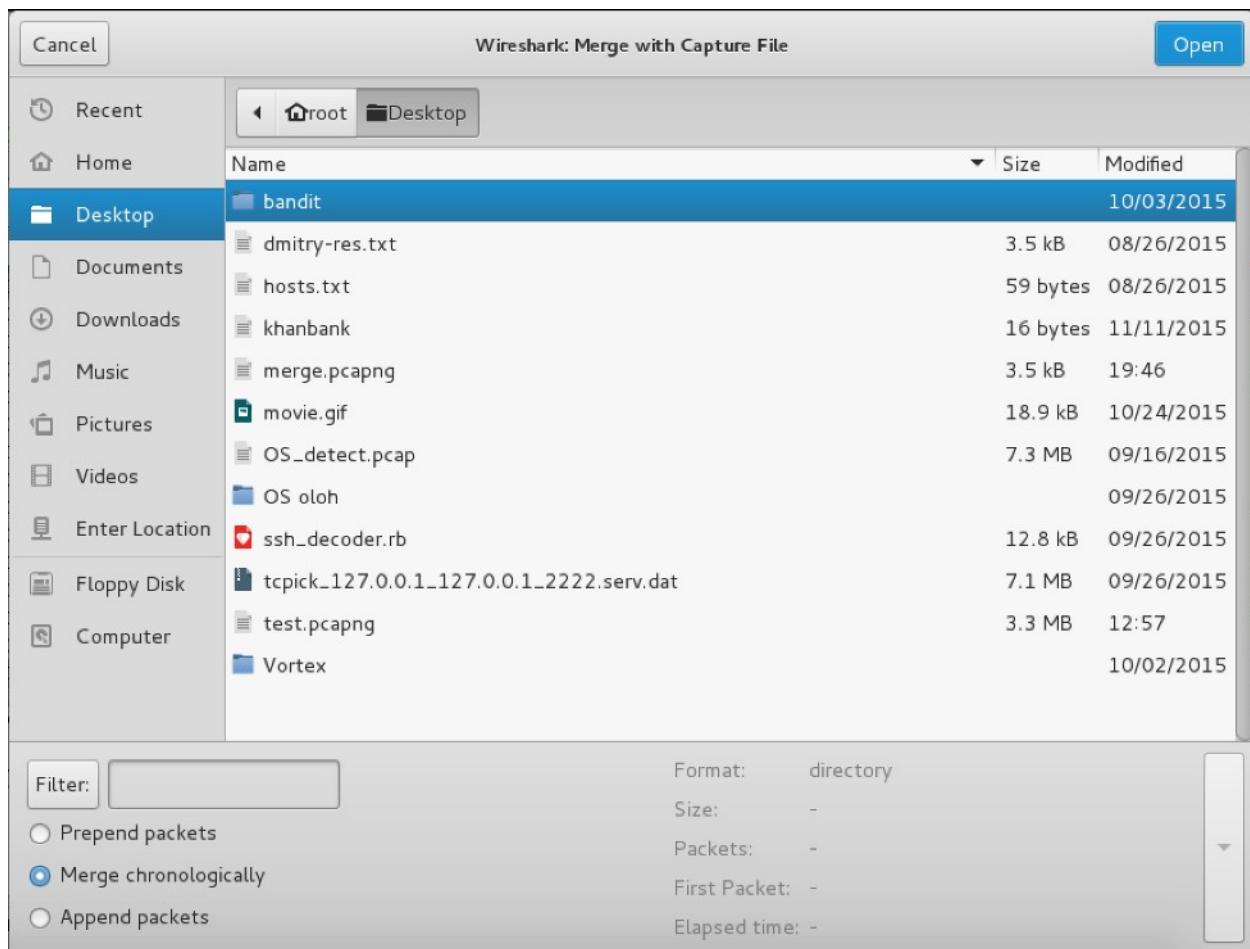
*Merge packets chronologically*      Одоо ачааллагдсан байгаа файл болон энэхүү цонхыг ашиглан файлуудыг хугацааны дарааллын дагуу нэгтгэх

*Append packets to existing file*      Одоо ачааллагдсан байгаа пакет файлын араас нь энэхүү цонхыг ашиглан сонгосон пакет файлыг нэгтгэх.



Зураг 5.5. Виндовс орчин дахь “Нэгтгэх (Merge)” цонх

Виндовс орчинд энэ цонх нь нийтлэг ижил төстэй байдаг.



Зураг 5.6. Линукс болон Юникс систем дээрх “Нэгтгэх (Merge)” цонх

Энэ цонх нь Gimp/GNOME график интерфэйсүүд дээр нийтлэг төстэй байдаг.

### 5.5. Хекс өгөгдөл импорт хийж оруулах (Import hex dump)

Вайршарк програм нь ASCII хекс өгөгдлийг уншиж чадвартай бөгөөд түүнчлэн үүнийг libpcap түр зуурын файл руу бичдэг. Дотроо олон пакет өгөгдөлтэй хекс өгөгдлийг (hex dump) унших ба улмаар олон пакеттай чагнасан файлыг (Capture File) бий үүсгэх боломжтой. Аппликэшн (Application) түвшний хекс өгөдөл (hex dump)-ийг бүрэн боловсруулагдах пакетын өгөгдөл (packet dump) үүсгэхийн тулд энэ функц нь дамми (dummy) Ethernet, IP мөн UDP, TCP, эсвэл SCTP толгой (header) файлуудыг үүсгэх чадвартай.

од –Ax –tx1 –v –ын үүсгэсэн хекс дамп (hex dump) өгөгдлийг вайршарк програм ойлгож уншдаг. Өөрөөр хэлбэл байт бүрийг тус тусад нь хоосон зайгаар тусгаарлан дэлгэцэнд харуулдаг. Мөр бүр файлын байрлалыг заах оффсет хаягаар эхэлдэг. Оффсет хаяг нь хекс тоо (octal or decimal) байдаг. Дараах хэсэгт импорт хийгдэх боломжтой хекс өгөгдлийн (hex dump) жишээг үзүүллээ.

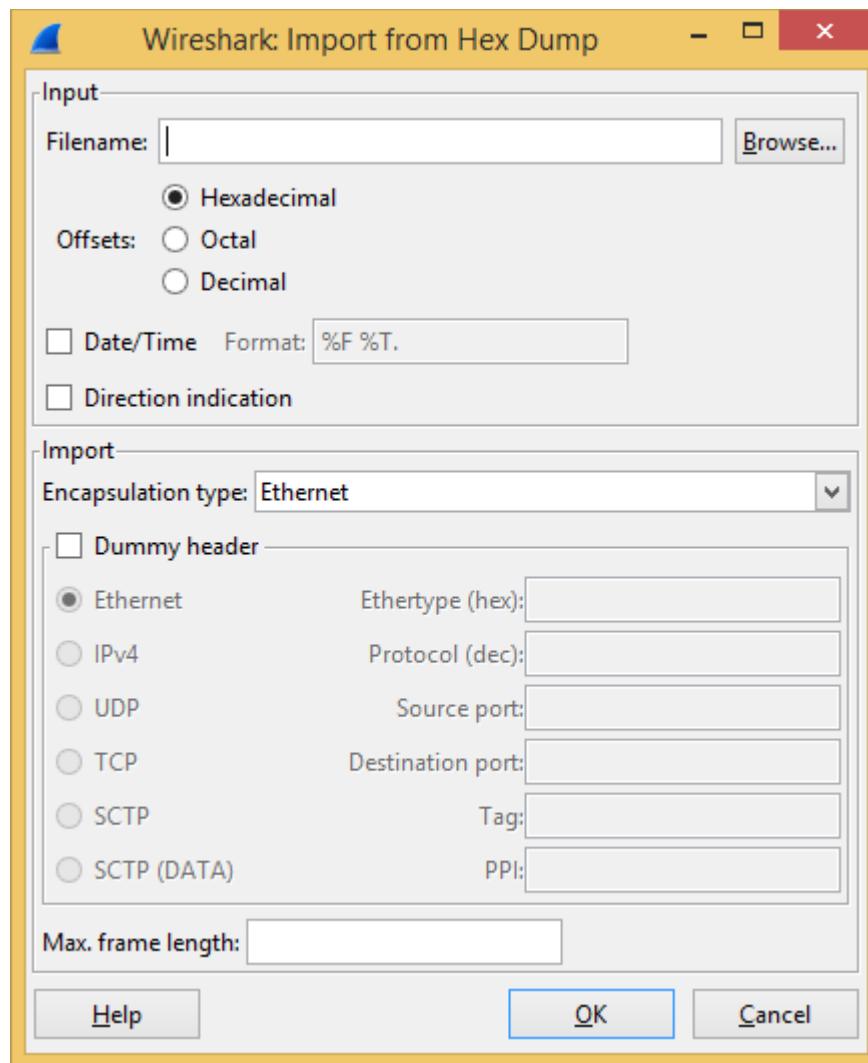
```
000000 00 e0 1e a7 05 6f 00 10 .....
000008 5a a0 b9 12 08 00 46 00 .....
000010 03 68 00 00 00 00 0a 2e .....
000018 ee 33 0f 19 08 7f 0f 19 .....
000020 03 80 94 04 00 00 10 01 .....
000028 16 a2 0a 00 03 50 00 0c .....
000030 01 01 0f 19 03 80 11 01 .....
```

Энд байт мөрийн өргөн эсвэл байтын тоон дээр хязгаар байхгүй. Мөн хекс өгөгдлийн (hex dump)-ын төгсгөлийн мөр нь гээгддэг (ignored). Байт болон хекс тоо (hex number) нь том үсгээр эсвэл жижиг үсгээр аль нь ч байсан болдог. Оффсетийн өмнөх текстийг алгасан орхидог (ignored). Байтстринг (bytestring) мөрүүдийн дундах текст мөрүүдийг орхигдуулан алгасдаг (ignored). Оффсет нь байтуудыг мөшгөх, байрлалыг тогтоох зорилгоор хэрэглэгддэг учраас оффсет хаяг нь үнэн зөв байх ёстой. Оффсет хаягтгүй эхэлж байгаа мөрүүдийг гээгдүүлэн орхидог. Оффсет хаяг нь 2 тэмдэгтээс илүү олон хекс тоо (hex number) байгаа гэдгээрээ ялгагдан танигддаг. Байтуудын (bytes) дараах текст өгөгдлийг алгасан орхидог (ignored). Тэг оффсет нь шинэ пакет эхэлж байна гэдэг мэдээллийг илэрхийлдэг тиймээс хекс өгөгдлийг (hex dump) агуулсан ганц файл нь олон пакет агуулсан пакет өгөгдөл рүү хөрвүүлэгдэх боломжтой. Пакетууд нь цагийн мэдээллээр эхэлж болдог. Эдгээр файл нь өгөгдсөн форматын дагуу задлагдан уншигддаг. Хэрэв эхний пакет нь одоогийн цагны мэдээллийг агуулаагүй байдлаар импорт хийгдвэл импорт хийгдсэн олон пакетуудын цагийн мэдээлэл нь 1 микросекундээр ялгаатай байдаг. Ерөнхийдөө маш цөөн тооны хязгаарлалтыг эс тооцвол вайршарк програм нь хекс өгөгдөл (hex dump)-ийг уншихдаа маш их өргөн хүрээтэй чөлөөт байдлаар уншиж чаддаг. Үүнийг маш олон нөхцөлд туршиж үзсэн (Эдгээр туршиж үзсэн нөхцөл байдлуудад мэйлээр хэд хэдэн удаа дамжуулсан, багцалсан мөрүүдтэй файлуудыг гэх мэт нөхцөлүүдэд туршиж үзсэн)

Үүнээс өөр хэд хэдэн дурдах шаардлагатай функцууд байгаа юм. Энхний мөр нь хоосон мөр биш #-аар эхэлсэн мөр нь тайлбар гэж үзэгдэж алгасагдан орхигддог. #TEXT2PCAP мөрөөр эхэлсэн мөр нь удирдамж заалт бөгөөд өөр сонголтууд нь энэ командын араас нэмэгдэж орж болно. Одоогоор өөр удирдамж чиглүүлэлт байхгүй байна. Гэсэн хэдий ч ирээдүйд энэхүү командыг хекс өгөгдлийг удирдахад илүү ихээр ашиглах бололцоотой юм. Жишээлбэл: цагийн мэдээлэл (timestamps), encapsulation type гэх мэт. Вайршарк програмын хэрэглэгчид dummy L2, L3, L4 толгойг пакет бүрийн өмнө нэмж өгснөөр аппликэши түвшний (application layer) өгөгдлийг өгөгдлийг унших боломжтой. Хэрэглэгч пакет бүрийн өмнө Ethernet headers, Ethernet болон IP эсвэл Ethernet, IP мөн UDP, TCP, SCTP headers-ийг пакет бүрийн өмнө нэмж өгөх боломжтой. Энэ нь вайршаркыг эсвэл бусад пакет задлашч програмуудад dump өгөгдлийг задалж унших боломжийг олгодог.

### 5.5.1. Хекс өгөгдлөөс импорт хийх цонх (Import from Hex Dump)

Энэ цонх нь танд хекс өгөгдлийг (hex dump) агуулсан текст файлыг сонгож импорт хийх мөн импорт хийх параметрүүдийг тохируулах боломжийг олгодог.



Зураг 5.7. Хекс өгөгдлөөс импорт хийх (Import from Hex dump)

Импортын удирдах хэсэг нь 2 хэсэгт хуваагддаг.

*Оролт (Input):* Ямар файлыг импорт хийх мөн түүнийг хэрхэн тайлж уншихыг тодорхойлдог

*Импорт (Import):* Өгөгдөл хэрхэн импорт хийгдэх вэ гэдгийг тодорхойлно.

Оролтын параметрүүд нь дараах утгыг агуулна:

*Filename / Browse* Импорт хийх файлын нэрийг оруулна. Мөн хэрэглэгч *browse* гэсэн товчийг ашиглан фолдерууд руу графикаар хандаж текст файл руугаа хандах боломжтой.

<i>Offsets</i>	Импорт хийх текст файлын оффсетийн төрлийг сонгоно. Энэ нь ихэвчлэн хекс (hex) байдаг. Гэхдээ аравт болон наймтын тоолын системээр оффсетийг өгөх боломжтой.
<i>Date/Time</i>	Таны импорт хийх текст файлын фрэймд цагийн мэдээлэл байгаа бол үүнийг хэрээслэнэ. Хэрэв тийм мэдээлэл байхагүй бол одоо байгаа цагийн мэдээллийг таны фрэймийн цагийн мэдээллээр харуулдаг.
<i>Format</i>	Энэ хэсэг нь импорт хийх текст файлын хугацааны мэдээллийн форматыг тодорхойлж өгөх хэсэг. %H нь цаг, %M нь минут, %S нь секундийг илэрхийлэх ба эдгээрийг ашиглан цагийн форматыг нь тодорхойлж өгдөг. %T нь хялбархан цагийн формат бөгөөд энэ нь HH:MM:SS гэсэн энгийн формат юм. Дэлгэрүүлэн уншихыг хүсвэл strftime(3) –г үзнэ үү

Импорт хэсгийн параметрууд:

<i>Encapsulation type</i>	Энд та ямар төрлийн фрэйм импорт хийх гэж байгаагаа зааж өгнө. Энд зааж өгөх төрөл нь тухайн <i>dump</i> өгөгдлийг ямар төрлийн орчинд цуглуулсан гэдгээс хамаарна. Энэхүү сонголтонд вайршарк програм уншиж чадах бүх төрлийг агуулдаг учраас тухайн файлдаа тохирсон зөв задлах хэсгийг тохируулах хэрэгтэй.
<i>Dummy header</i>	<i>Ethernet encapsulation</i> –ийг сонгосон тохиолдолд та импорт хийх фрэймийнхээ өмнө нь dummy header нэмж өгөх боломжтой. Эдгээр толгой файлууд (header) нь хиймэл Ethernet, IP, UDP, TCP эсвэл SCTP толгой файлыг (headers) мөн SCTP өгөгдлийн хэсэг (data chunks) нэмэх боломжийг олгодог. Dummy header сонгох үед тохируулж болох талбарууд (entries) нь идэвхитэй болдог бөгөөд бусад нь саарал өнгөтэй байх ба өгөгдмөл утгуудаа (default value) авдаг.
<i>Maximum frame length</i>	Та текст файлын фрэймүүдийг бүгдийг нь бүтнээр сонирхоогүй зөвхөн эхний хэсгийг нь л сонирхож байх тохиолдол гарч болох юм. Эндээс та фрэймийн эхлэлээс

хэр их өгөгдлийг нь импорт хийх вэ гэдгээ тохируулах боломжтой. Хэрэв хоосон орхивол хамгийн их хэмжээ болох 65535 байтаар тохируулагддаг.

Оролтын болон импортын бүр параметрүүдээ тохируулсныхаа дараа **OK** гэсэн товчийг дарж импорт үйлдлийг хийнэ. Хэрэв үндсэн дэлгэцэнд ачаалласан пакет өгөгдлөө хадгалаагүй байсан бол танаас энэхүү файлаа хадгалах эсэхийг тань асууна.

Үүний дараа текст файлаас импорт хийж оруулсан шинэ фрэймүүд (пакет өгөгдөл)-ийг вайршарк програм руу ачаалладаг.

### 5.6. Файлын багц (File sets)

Олон файл (Multiple Files) тохиргоогоор чагнах үйлдэл хийж байгаа үед (4.11. “Чагнасан файлууд болон файлын төрлүүд (Capture files and file modes)” хэсгийг үзнэ үү.) чагнасан файл маань хэд хэдэн файлуудад хуваагдан тарж хадгалагддаг ба эдгээр файлуудыг файлын багц гэдэг (File set).

Файлын багцтай гараараа ажиллах нь залхуутай ажил бөгөөд үүнийг хялбарчлах функцийн вайршарк програмд байдаг.

#### Вайршарк програм файлын багцийг хэрхэн таньдаг вэ?

Файлын багцад байгаа файлын нэрс дараах хэлбэртэй байдаг. Угтвар\_Dугаар\_ОнCapЗалгавар жишээлбэл test\_00001\_20060420183910.rcap. Нэг багцад байгаа файлууд бүгд ижил угтвар (өмнөх жишээн дээрх “test”) ижил залгавартай байна (өмнөх жишээн дээрх “.rcap”) байдаг ба дунд хэсэг нь өөр өөр байдаг.

Файлын багцийн файлуудыг олохын тулд вайршарк зааж өгсөн санд байгаа бүх файлуудын нэрийг шалгадаг ингэхдээ програмд ачааллагдсан байгаа файлтай ижихэн угтвар, дагавартай (prefix, suffix) файлуудыг хайж олдог.

Энэ энгийн механизм нь ихэнх тохиолдолд хэвийн ажилладаг хэдий ч зарим сул талуудтай. Жишээлбэл: Хэрэв хэд хэдэн файлын багцийг ижил угтвар, ижил төгсгөлтэйгээр хадгалсан байвал програм тэдгээрийг бүгдийг нь нийлүүлэн нэг файлын багц хэмээн таньдаг. Мөн түүнчлэн хэрэв аль нэг файлынх нь нэрийг нь сольчихсон эсвэл аль нэг файлыг нь өөр фолдерт хуулсан байвал тухайн файлыг файлын багцад хамруулан таньж чаддаггүй.

File → File Set гэсэн цэсэн дэх дараас сонголтууд таныг файлын багцтай хялбар ажиллах боломжийг бүрдүүлдэг

- “List Files” энэ цонх нь одоогийн файлын багцад хамаарах бүх файлуудыг жагсаан харуулна.

- “Next File” програмд одоо ачааллагдсан байгаа файлыг хааж файлын багцад байгаа түүний дараагийн файлыг нээнэ.
- “Previous File” програмд одоо ачааллагдсан байгаа файлыг хааж файлын багцад байгаа түүний өмнөх файлыг нээнэ

#### 5.6.1. Файлын жагсаалт (List Files) цонх

**Wireshark: 17 Files in Set**

Filename	Created	Last Modified	S
<input checked="" type="radio"/> test1_00001_20050819181503.pcap	2005.08.19 18:15:03	2005.08.19 18:15:05	1067
<input type="radio"/> test1_00002_20050819181505.pcap	2005.08.19 18:15:05	2005.08.19 18:15:05	1108
<input type="radio"/> test1_00003_20050819181505.pcap	2005.08.19 18:15:05	2005.08.19 18:15:06	1093
<input type="radio"/> test1_00004_20050819181506.pcap	2005.08.19 18:15:06	2005.08.19 18:15:07	1031
<input type="radio"/> test1_00005_20050819181507.pcap	2005.08.19 18:15:07	2005.08.19 18:15:07	1070
<input type="radio"/> test1_00006_20050819181507.pcap	2005.08.19 18:15:07	2005.08.19 18:15:08	1126
<input type="radio"/> test1_00007_20050819181508.pcap	2005.08.19 18:15:08	2005.08.19 18:15:09	1074
<input type="radio"/> test1_00008_20050819181509.pcap	2005.08.19 18:15:09	2005.08.19 18:15:10	1037
<input type="radio"/> test1_00009_20050819181510.pcap	2005.08.19 18:15:10	2005.08.19 18:15:12	1060
<input type="radio"/> test1_00010_20050819181512.pcap	2005.08.19 18:15:12	2005.08.19 18:15:13	1079
<input type="radio"/> test1_00011_20050819181513.pcap	2005.08.19 18:15:13	2005.08.19 18:15:14	1029
<input type="radio"/> test1_00012_20050819181514.pcap	2005.08.19 18:15:14	2005.08.19 18:15:16	1119
<input type="radio"/> test1_00013_20050819181516.pcap	2005.08.19 18:15:16	2005.08.19 18:15:17	1029
<input type="radio"/> test1_00014_20050819181517.pcap	2005.08.19 18:15:17	2005.08.19 18:15:18	1085
<input type="radio"/> test1_00015_20050819181518.pcap	2005.08.19 18:15:18	2005.08.19 18:15:18	1083
<input type="radio"/> test1_00016_20050819181518.pcap	2005.08.19 18:15:18	2005.08.19 18:15:18	1058
<input type="radio"/> test1_00017_20050819181518.pcap	2005.08.19 18:15:18	2005.08.19 18:15:18	1386

... in directory: D:/fileset

 Help  Close

Зураг 5.8. Файлын жагсаалт (List Files) цонх

Мөр бүр файлын багцад байгаа тухайн нэг файлын мэдээллийг агуулна.

- *Filename* – файлын нэр. Хэрэв та файлын нэр дээр дарвал (эсвэл түүний зүүн талын бөөрөнхий сонгох цэсийг сонговол) одоо нээлттэй байгаа файлыг хааж таны сонгосон файлыг нээнэ.
- *Created* – Файлыг үүсгэсэн хугацаа
- *Last Modified* – Хамгийн сүүлд өөрчлөлт оруулсан хугацаа
- *Size* - Файлын хэмжээ

Сүүлийн мөрөнд эдгээр файлын багц байрлаж буй фолдериин мэдээллийг агуулдаг.

Файл нээх/хаах бүрт энэхүү цонхны мэдээлэлд шинэчлэл хийгдэж байдаг.

**Close** товч нь энэ цонхыг хаана.

### 5.7. Файл экспорт хийх

Вайршарк програмыг ашиглан пакет өгөгдлийг хэд хэдэн арга замаар хэд хэдэн файлын форматаар экспорт хийж болдог. Энэ хэсэгт вайршарк програмыг ашиглан файл экспорт хийх энгийн арга замуудыг авч үзнэ.

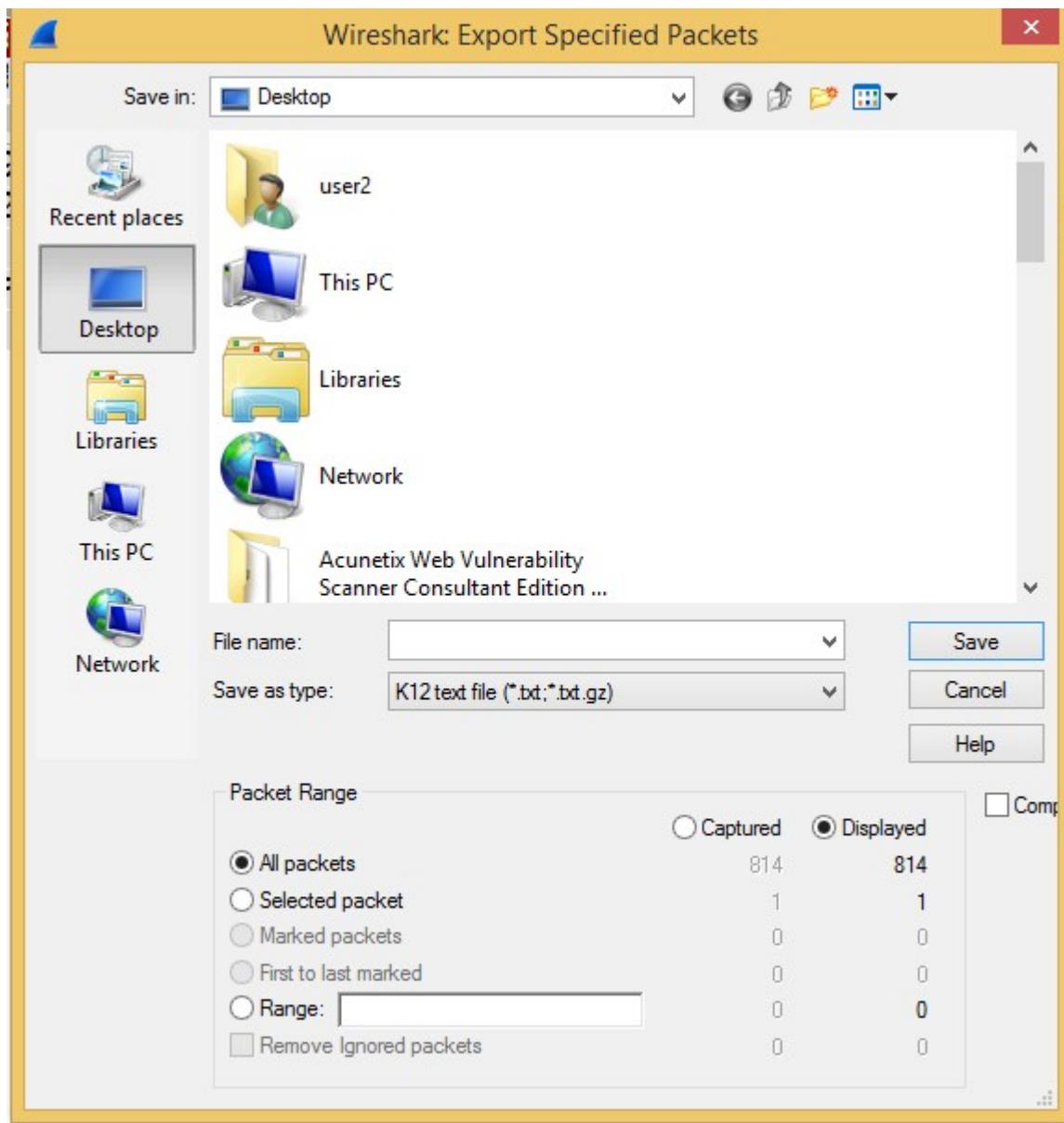
#### 5.7.1. Текст файл хэлбэрээр экспорт хийх (Export as Plain Text File)

Файлыг энгийн ASCII текст файл байдлаар экспорт хийх. Энэ үйлдэл нь пакет хэвлэх үйлдэлтэй төстэй бөгөөд хэвлэхэд хэрэглэдэг файлын форматаар экспорт хийж байна гэсэн үг.

#### Зөвлөгөө

Хэрэв та өмнө нь экспорт хийсэн пакет энгийн текст файлаасаа буцаан импорт хийх боломжтой байлгахыг хүсч байвал дараах зүйлсийг хийхийг зөвлөж байна.

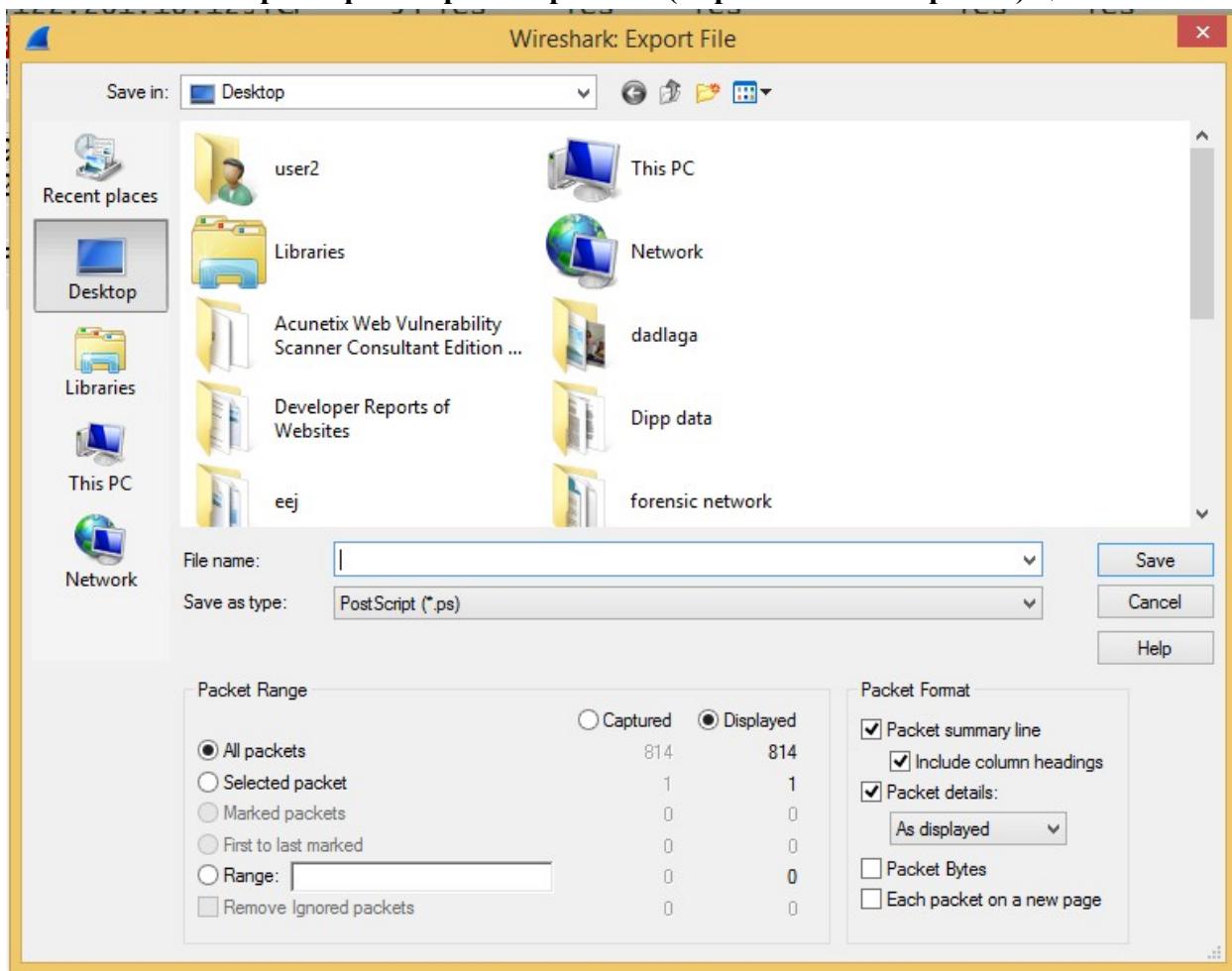
- “Үнэмлэхүй он сар цагийн мэдээлэл (Absolute date and time)” багана нэмэх
- Бусад багануудыг түр хугацаагаар нуух (hide)
- Edit → Preferences → Protocols → Data “Show not dissected data on new Packet Bytes pane” хэсгийн тохиргоог идэвхигүй болгох. Дэлгэрүүлэн уншихыг хүсвэл 10.5. Тохиргоо (Preferences) хэсгийг үзнэ үү.
- Пакетын нэгтгэн дүгнэсэн мөрийг (summary) нэмэх
- Баганын толгойны хэсгийг хасах
- Пакетын дэлгэрэнгүй хэсгийг хасах
- Пакетын байтын хэсгийг оруулах



Зураг 5.9. “Текст файл болгон экспорт хийх (Export as Plain Text File) үонх”

- Файл руу Экспорт хийх (Export to file): Фрэйм пакетын өгөгдлийг экспорт хийх файлыг сонгодог.
- Пакетын завсар (Packet Range): Энэ хэсгийг **5.9. “Пакетийн завсар фрэйм (Packet Range frame)”** хэсгээс үзнэ үү.
- Пакетын Дэлгэрэнгүй мэдээлэл (Packet Details): Энэ хэсгийг **5.10. “Пакет формат фрэйм (Packet Format frame)”** хэсгээс үзнэ үү.

### 5.7.2. ПостСкрипт файлаар экспорт хийх (Export as PostScript File) цонх



Зураг 5.10. “Пост Скрипт файлаар экспорт хийх (Export as PostScript File) цонх”

- Файл руу Экспорт хийх (Export to file): Фрэйм пакетын өгөгдлийг экспорт хийх файлыг сонгодог.
- Пакетын завсар (Packet Range): Энэ хэсгийг 5.9. “Пакетийн завсар фрэйм (Packet Range frame)” хэсгээс үзнэ үү.
- Пакетын Дэлгэрэнгүй мэдээлэл (Packet Details): Энэ хэсгийг 5.10. “Пакет формат фрэйм (Packet Format frame)” хэсгээс үзнэ үү.

### 5.7.3. CSV файлаар экспорт хийх (Export as Comma separated Values File) цонх

Пакетын товч дүгнэлтийг CSV файл руу экспорт хийснээр хүснэгт ашигладаг програмууд руу импорт хийх, экспорт хийх боломжтой болдог.

- Файл руу Экспорт хийх (Export to file): Фрэйм пакетын өгөгдлийг экспорт хийх файлыг сонгодог.
- Пакетын завсар (Packet Range): Энэ хэсгийг 5.9. “Пакетийн завсар фрэйм (Packet Range frame)” хэсгээс үзнэ үү.

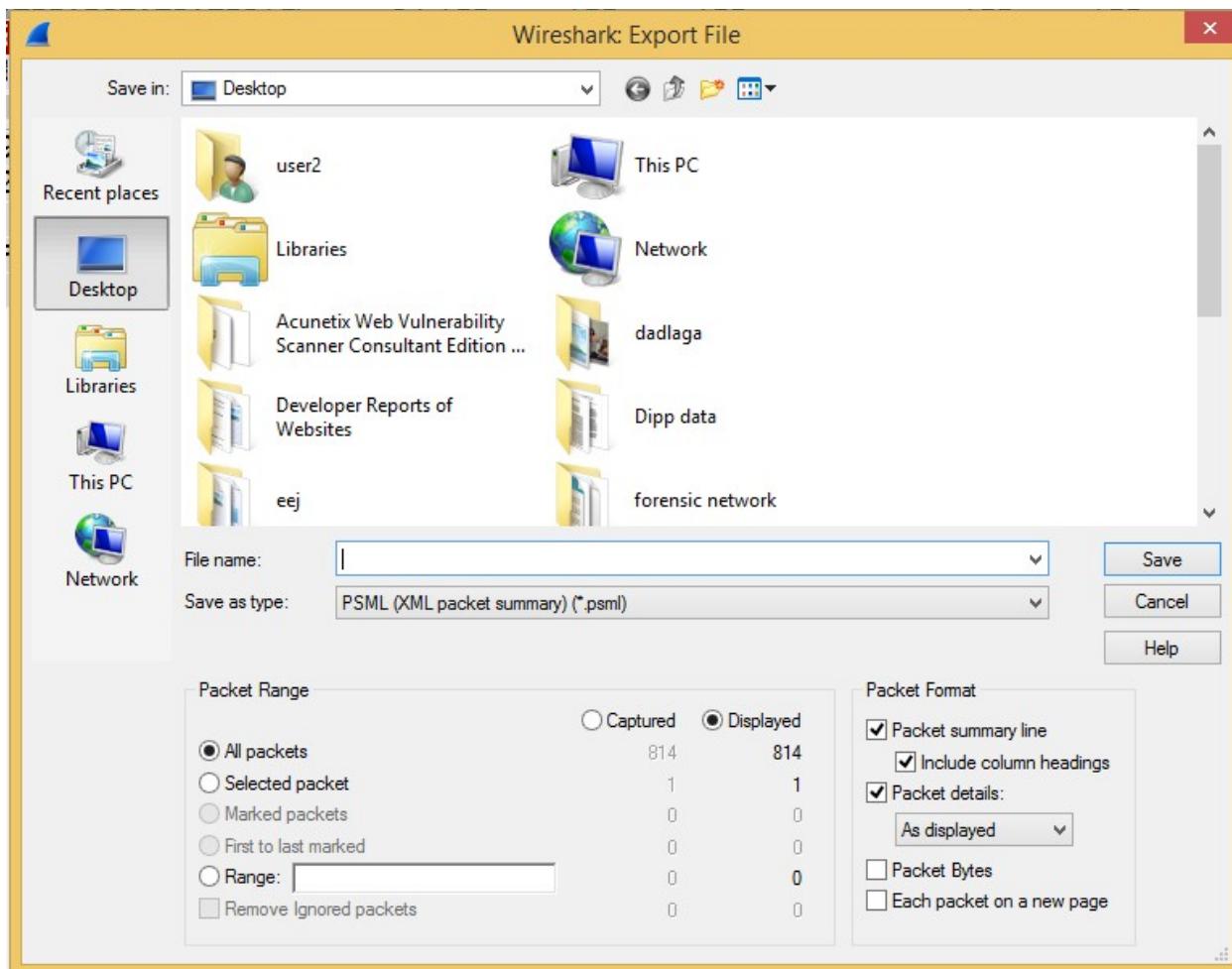
#### 5.7.4. Си массив файлаар (пакетын байт мэдээлэл) экспорт хийх цонх (Export as C arrays file)

Пакетын байтуудыг Си програмын массив руу экспорт хийх ба ингэснээр та энэхүү массиваа дараа нь өөрийн Си програм руу импорт хийж оруулах боломжтой болдог.

- Файл руу Экспорт хийх (Export to file): Фрэйм пакетын өгөгдлийг экспорт хийх файлыг сонгодог.
- Пакетын завсрал (Packet Range): Энэ хэсгийг 5.9. “Пакетийн завсрал фрэйм (Packet Range frame)” хэсгээс үзнэ үү.

#### 5.7.5. PSML файл руу экспорт хийх цонх (Export as PSML File)

Пакетын өгөгдлийг PSML файл руу экспорт хийх. Энэ нь зөвхөн пакетын хураангуй дүгнэлтийг агуулах XML дээр суурилсан формат юм. PSML файлын тодорхойлолтыг [http://www.nbee.org/doku.php?id=netpdl:psml\\_specification](http://www.nbee.org/doku.php?id=netpdl:psml_specification) хаягаас үзнэ үү.

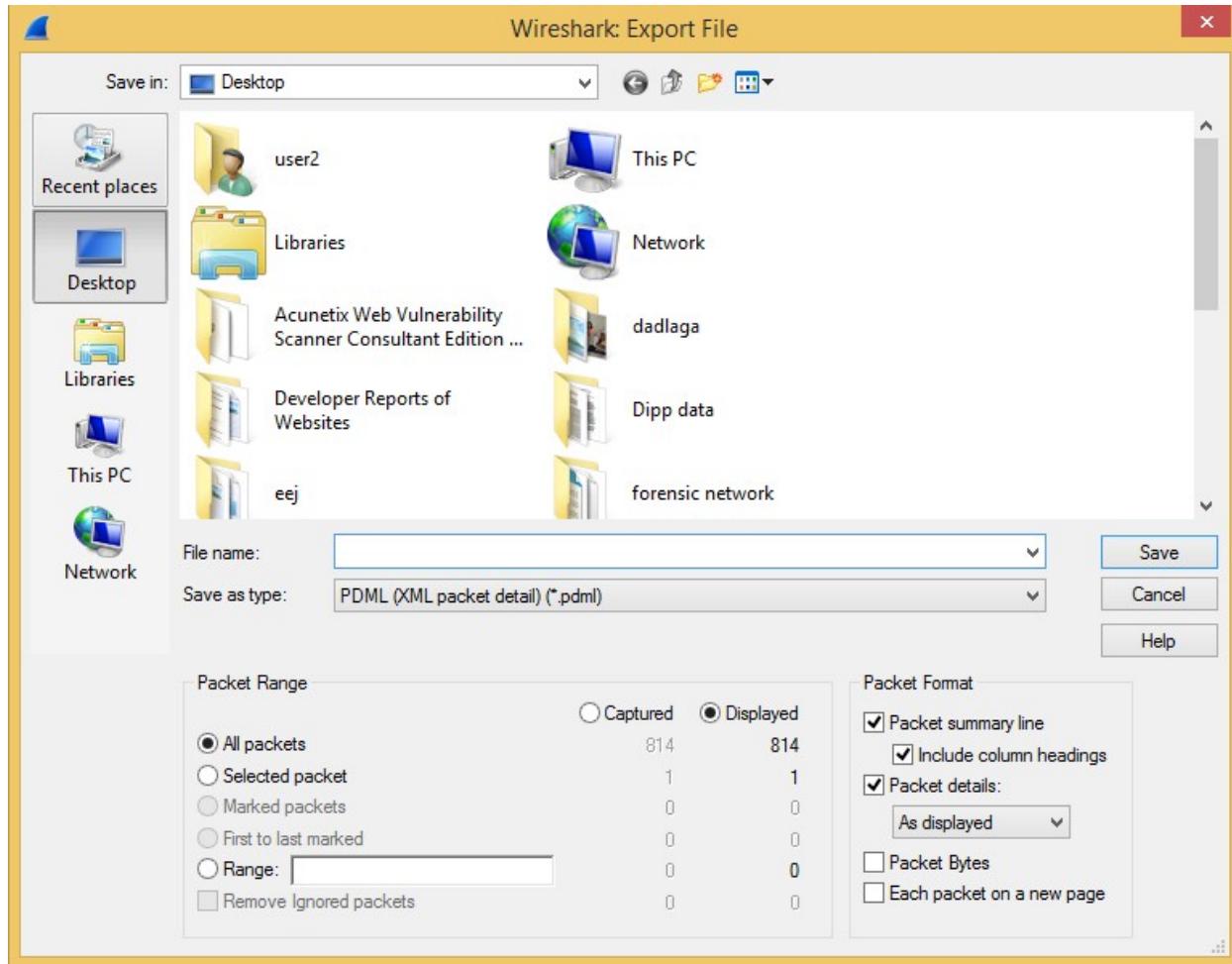


Зураг 5.11. “PSML файл руу экспорт хийх цонх (Export as PSML File)”

- Файл руу Экспорт хийх (Export to file): Фрэйм пакетын өгөгдлийг экспорт хийх файлыг сонгодог.
- Пакетын завсар (Packet Range): Энэ хэсгийг 5.9. “Пакетийн завсар фрэйм (Packet Range frame)” хэсгээс үзнэ үү.

#### 5.7.6. PDML файл руу экспорт хийх цонх (Export as PDML File)

Пакетын өгөгдлийг PDML файл руу экспорт хийдэг. Энэ файл нь пакетын дэлгэрэнгүй мэдээллийг агуулдаг файл бөгөөд XML дээр сууринсан формат юм. PDML файлын тодорхойлолтыг [http://www.nbee.org/doku.php?id=netndl:pdml\\_specification](http://www.nbee.org/doku.php?id=netndl:pdml_specification) хаяг руу орж үзэх боломжтой.



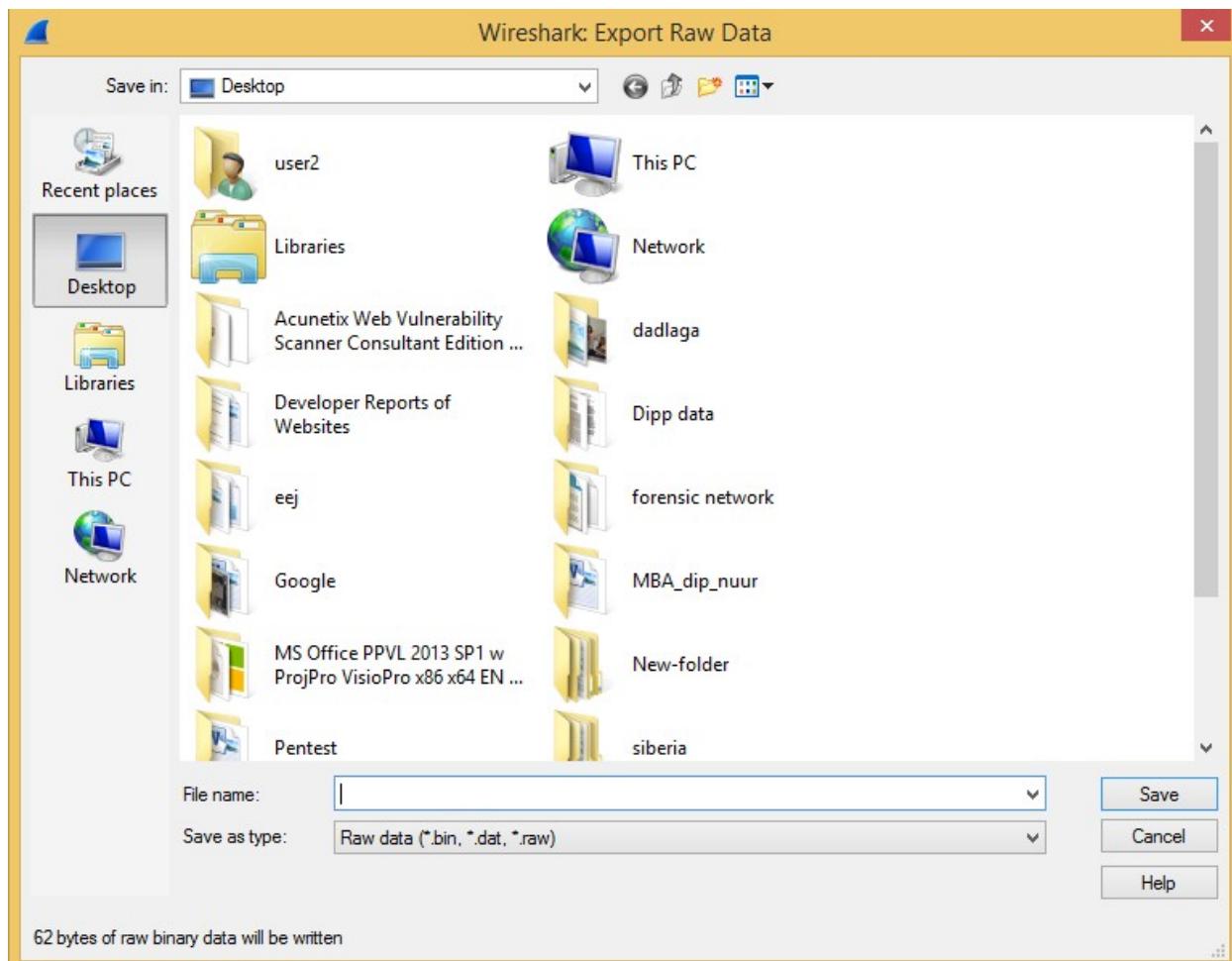
Зураг 5.12. “PDML файл руу экспорт хийх цонх (Export as PDML File)”

- Файл руу Экспорт хийх (Export to file): Фрэйм пакетын өгөгдлийг экспорт хийх файлыг сонгодог.
- Пакетын завсар (Packet Range): Энэ хэсгийг 5.9. “Пакетийн завсар фрэйм (Packet Range frame)” хэсгээс үзнэ үү.

PDML экспортэд зориулагдсан пакетын мэдээллийг дэлгэрэнгүй харуулах фрэйм байхгүй бөгөөд пакетын формат нь PDML-ын бүтцээр тодорхойлогддог.

#### 5.7.7. Пакетын идэвхижсэн байтуудыг экспорт хийх цонх (Export selected packet bytes)

Энэ цонх нь пакетын мэдээллийг байтаар харуулах самбарт идэвхижсэн байгаа байтуудыг рав бинари файл (raw binary file) руу экспорт хийдэг.



Зураг 5.13. Пакетын идэвхижсэн байтуудыг экспорт хийх (Export Selected Packet Bytes) цонх

- Name: Пакет өгөгдлийг экспорт хийх файлын нэр.
- The Save in folder: Энэ талбар нь файлаа хадгалах фолдерээ зааж өгөгх боломжийг олгодог.
- Илүү уян хатан байдлаар (график интерфэйсээс) фолдерээ сонгох боломжтой.

### 5.7.8. Объектуудыг экспорт хийх цонх (Export Objects)

Энэ функц нь HTML документууд, зургийн файлууд, биелэх боломжтой файлууд (executables) гэх мэт HTTP протоколоор дамжих боломжтой объектуудыг одоогийн нээлттэй байгаа цуглуулсан файл, эсвэл одоогийн чагнаж байгаа файл болон дахин угсарсан (reassembled) объектуудын HTTP урсгалаас хайж олоод тэдгээрийгээ диск рүү хадгалдаг. Хэрэв таны чагнах процесс ажиллаж байгаа бол энд харагдах объектийн жагсаалт нь шинэ объектуудаар шинэчлэгдэж байдаг. Хадгалсан объектууд нь дараа нь зохистой програмаараа нээгдэх, ажиллах боломжтой (executable файлын хувьд). Энэ функц нь GTK2 хэрэглэж буй 2.4-өөс доош хувилбарууд дээр ажиллахгүй.

Packet num	Hostname	Content Type	Size	Filename
1571	google.com	text/html	258 bytes	\
1581	www.google.mn	text/html	274 bytes	?gfe_rd=cr&ei=ey9XVuusLuOS8Qej_oCICg
7322	vignette2.wikia nocookie.net	image/png	109 kB	latest?cb=20121222015443
7703	forums.terraria.org	image/png	415 kB	halo-logo.png.26672
8167	forums.terraria.org	image/png	415 kB	halo-logo.png.26672
8264	en-US.appex-rf.msn.com	application/xml	964 bytes	Today.xml
8267	finance.services.appex.bing.com	application/xml	1200 bytes	AppTileV2?symbols=&contentType=-1&tileType=0&locale=en-
8272	en-US.appex-rf.msn.com	application/xml	943 bytes	Today.xml?cgversion=v6
8275	en-US.appex-rf.msn.com	application/xml	967 bytes	Home.xml?cgversion=v6

Зураг 5.14. Объект экспорт хийх (Export Objects) цонх

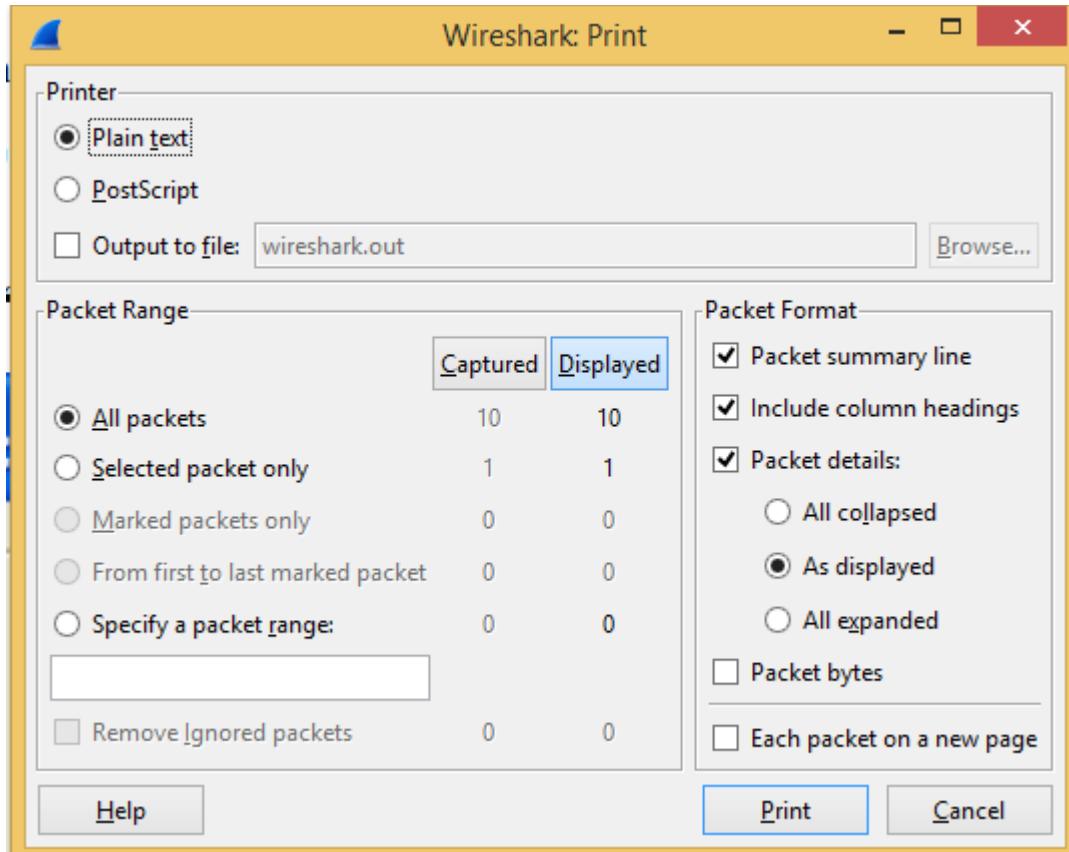
- *Packet num*: Объект илэрсэн пакетын дугаар. Зарим тохиолдолд нэг пакетад хэд хэдэн объект байж болдог.
- *Hostname*: HTTP хүсэлтэд хариу өгч буй серверийн хостын нэр
- *Content Type*: Энэ объектийн HTTP контентийн төрөл.
- *Size*: Энэ объектийн хэмжээг байтаар харуулна.

- *Filename*: Сүүлийн слашийн дараах URI –ын сүүлчийн хэсэг. Энэ нь ихэвчлэн файлын нэр байдаг. Гэхдээ энэ нь HTTP POST хүсэлтийн хариуд ирсэн файлыг илэрхийлэх маш урт тэмдэгт мөр байх магадлалтай.
- *Help*: Хэрэглэх зааврыг нээнэ.
- *Close*: Энэ цонхыг хаадаг.
- *Save As*: Одоо сонгогдсон байгаа объектийг таны зааж өгсөн нэрээр хадгална. Өгөгдмөл тохиргоогоор (default) өгөх файлын нэр нь объект жагсаалтын “*Filename*” хэсэгт байгаа файлын нэрийг авна.
- *Save All*: Энэ объектын жагсаалтад байгаа файлуудыг бүгдийг нь *Filename* баганад байгаа нэrsийг ашиглан хадгалдаг. Танаас аль сан/фолдерт хадгалахыг асууна. Хэрэв файлын нэр вайршарк ажиллаж байгаа үйлдлийн ситсемд тохирогчийн байвал эсвэл таны файлын системд тохирогчийн байвал алдааны мессеж өгөх ба объект файл хадгалагдахгүй. (Гэхдээ алдаа заагаагүй бусад объектууд нь зүгээр хадгалагдана)

## 5.8. Пакет хэвлэх (Printing packets)

Пакетуудыг хэвлэхийн тулд **File → Print** сонголтыг сонгоно. Энэ сонголтыг сонгосноор вайршарк програм танд хэвлэх цонхыг харуулна.

### 5.8.1. The “Print” dialog box



Зураг 5.15. Хэвлэх (Print) цонх

Хэвлэх (Print) цонхыг ашиглан та дараах тохиргоог хийх боломжтой.

#### *Printer*

*Plain Text:* нь пакетыг энгийн текст хэлбэрээр хэвлэх тохиргоог заана

*PostScript:* Хэвлэхдээ PostScript-г үүсгэж хэвлэх тохиргоог зааж өгдөг

*Output to file:* Файл руу хэвлэх үйлдлийг хийх тохиргоог хийдэг. Энд байгаа файлын нэр оруулах хэсэгт файлынхаа нэрийг тодорхойлж өгдөг.

Хэрэв та файл руу хэвлэх (Print to file) сонголтыг хийсэн бол энэ хэсэгт та хэвлэх файлынхаа нэрийг оруулж өгөх хэсэг юм. Хэрэв файл руу хэвлэх (Print to file) хэсгийг сонгоогүй бол энэ хэсэг идэвхижихгүй.

*Print command* хэсэг нь хэвлэх үед хэрэглэгдэх командуудыг агуулдаг.

Эдгээр *Print command* нь Виндовс систем дээр хэрэгжих боломжгүй.

Хэвлэх команд нь ихэвчлэн lpr байдаг бөгөөд та өөрийн хүссэнээр хэвлэхийн тулд та энэхүү дарааллыг өөрөө өөрчлөн тохируулж өгөх боломжтой. Жишээлбэл:

```
$ lpr -Pmypostscript
```

Хэрэв файл руу гаргах (*Output to file*) хэсгийг идэвхижиүүлсэн бол энэхүү командын хэсэгт команд оруулах боломжгүй.

#### *Packet Range*

Пакетыг хэвлэхдээ тодорхой пакетын завсарыг хэвлэх бол энэ хэсгийг сонгоно. **5.9. Пакетын завсар фрэйм (Packet Range Frame)** хэсгийг үзнэ үү

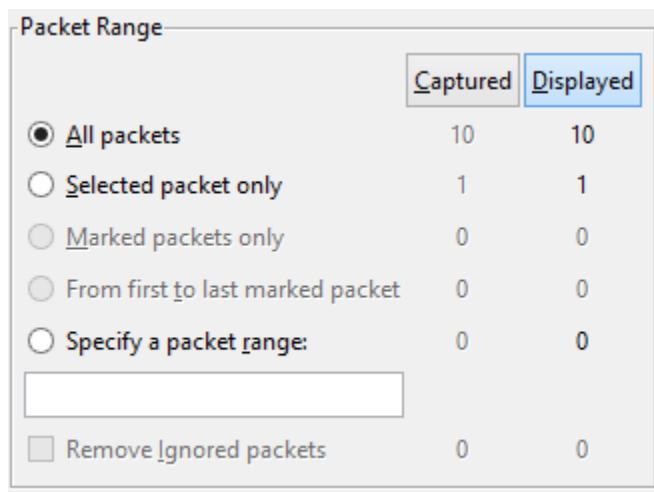
#### *Packet Format*

Пакетын гаралтын форматыг сонгох боломжтой. Энэ хэсгийг ашиглан пакетуудыг яг ямар байдлаар хэвлэх вэ гэдгээ зааж өгч болдог. **5.17. Пакетын формат фрэйм (Packet Format Frame)** зургийг үзнэ үү

Пакет бүрийг хэрхэн хэвлэгдэхийг сонгож болдог. Зураг 5.17-г үзнэ үү

### **5.9. Пакетын завсар фрэйм (Packet Range frame)**

Пакетын завсарын фрэймийг ашиглан хэрэглэгч гаралтын функцээр ямар ямар пакет орж боловсруулагдахыг тодорхойлж өгдөг.



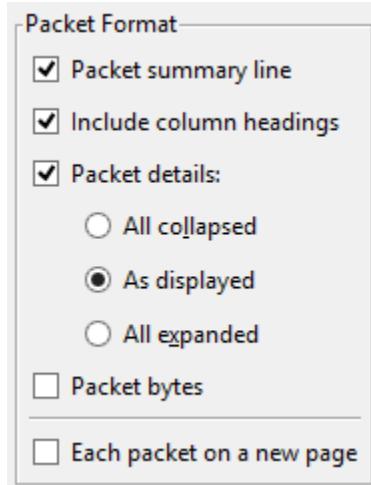
5.16 Пакетын завсар фрэйм (Packet Range frame)

Хэрэв **Captured** товчлуур сонгогдсон (өгөгдмөл тохиргоогоор сонгогдсон байдал) байвал энэ хэсэгт сонгох дүрэм бүх пакетуудад ажиллана. Хэрэв **Displayed** товчлуур сонгогдсон байвал зөвхөн дэлгэцэнд харуулж буй пакетуудад л энэ хэсгээр сонгосон дүрмүүд хэрэгжинэ.

- *All packets*: Бүх пакетуудыг боловсруулдаг.
- *Selected packet only*: Зөвхөн сонгож идэвхижүүлсэн пакетуудыг боловсруулна.
- *Marked packets only*: Зөвхөн тэмдэглэсэн (marked) пакетуудад боловсруулалт хийдэг.
- *From first to last marked packet*: Хамгийн эхний пакетаас эхлээд хамгийн сүүлийн тэмдэглэгдсэн (marked) пакет хүртэл бүх пакетыг боловсруулна.
- *Specify a packet range*: Хэрэглэгчийн зааж өгсөн завсарт харьялагдах пакетуудад боловсруулалт хийнэ. Жишиэлбэл 5,10-15,20- хэмээн тодорхойлж өгсөн байвал 5 дугаар дээрх пакет, 10-аас 15 хүртэл (15 –ыг оруулаад) пакетууд мөн 20-оос хойш дуустал бүх пакетуудад боловсруулалтыг хийнэ.

### 5.10. Пакетын формат фрэйм (Packet Format frame)

Энэ нь гаралттай холбоотой тохиргоог хийж өгөх хэсэг юм. Энд байгаа тохиргоог ашиглан та пакетын аль хэсэг нь гаралтын функц руу дамжуулагдахыг тохируулна.



Зураг 5.17. Пакетын формат фрэйм (Packet Format frame)

- *Packet summary line* хэсэг нь пакетын товч дүгнэлтийн хэсгийг идэвхижүүлдэг. (Пакетыг жагсаан харуулах самбар шиг)
- *Include column headings* хэсэг пакетын толгой хэсгийн баганыг идэвхижүүлнэ.
- *Packet details* хэсэг нь пакетын мэдээллийг дэлгэрэнгүй үзүүлдэг мод хэлбэрийн гаралтыг идэвхижүүлдэг
- *All collapsed* Пакетын мэдээллийг дэлгэрэнгүй харуулах самбарын мэдээллийг бүгдийг нь хумисан байдлаар хэвлэх

- *As displayed* Пакетын мэдээллийг дэлгэрэнгүй харуулах самбарын мэдээллийг яг одоо байгаа байдлаар нь хэвлэх
- *All expanded* Пакетын мэдээллийг дэлгэрэнгүй харуулах самбарын мэдээллийг бүгдийг нь задалсан байдлаар нь хэвлэх
- *Packet bytes* Пакетын байтуудыг гаралтанд идэвхижүүлдэг (Пакетын байтыг харуулах самбар шиг)
- *Each packet on a new page* Пакет бүрийг шинэ хуудсанд хэвлэнэ. (Жишээлбэл текст файл руу хэвлэх, хадгалах үйлдлийг хийж байгаа бол энэ тохиргоо нь пакетуудын хооронд тодорхой форматтай ялгах тэмдэглэгээ авна).

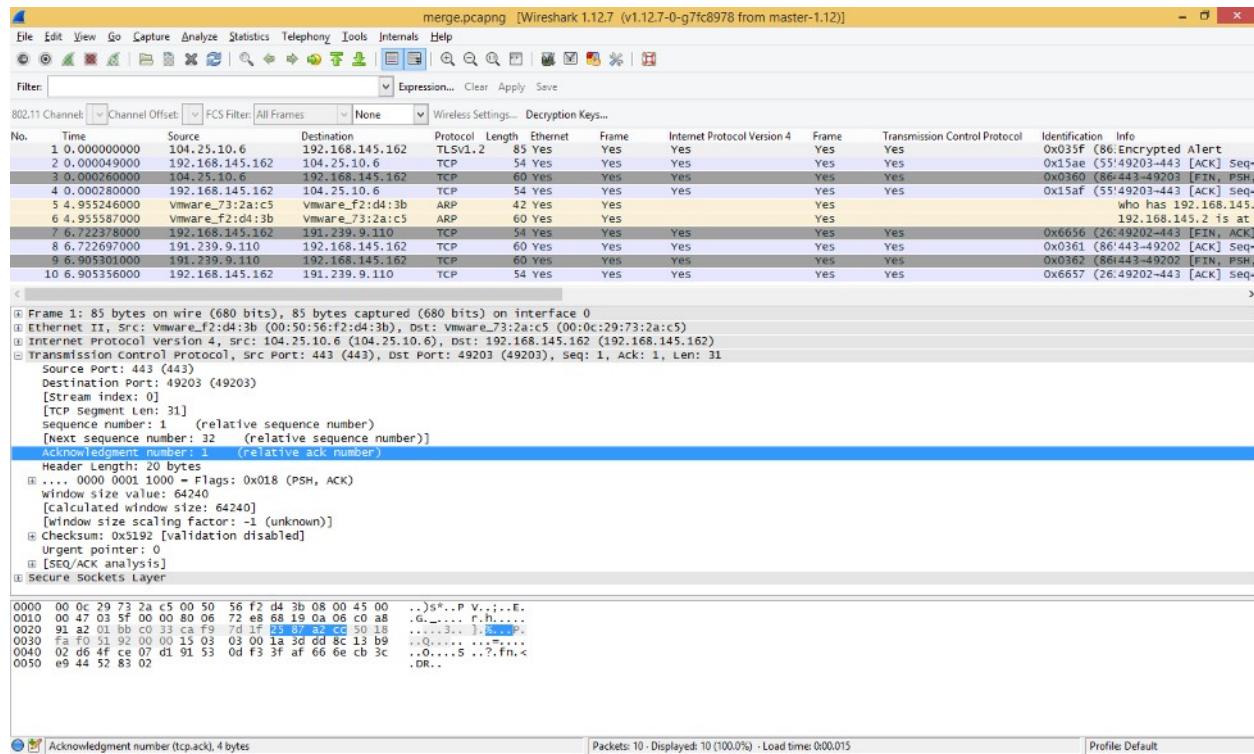
## **БҮЛЭГ VI**

### **6. ЧАГНАСАН ФАЙЛТАЙ АЖИЛЛАХ**

## 6.1. Чагнаж цуглүулсан пакетуудаа харах (viewing packets you have captured)

Пакет чагнасан эсвэл өмнө нь цуглүулж авсан пакетаа вайршарк дээр нээсэн бол та тухайн пакетуудаа пакетыг жагсаан харуулах самбар (Packet list pane) дээрээс сонгож дээр нь дарах замаар цааш нь дэлгэрүүлэн харах (Packet Details pane) самбар мөн пакетын мэдээллийн байтаар харуулах (Packet Bytes Pane) хэсэг зэрэгт задалж харах боломжтой.

Улмаар та пакетын дэлгэрэнгүй мэдээллийн мод хэлбэрийн бүтэцтэй мэдээллийг задалж пакет бүр дээр протоколыг нь задлан харах боломжтой. Мод хэлбэрийн бүтэцтэй мэдээлэл дээр хулганы заагчийг дарж идэвхижүүлснээр тухайн хэсэгтэй харгалзах хэсгийг пакетын байтын хэсэг (packet bytes pane) дээр тодруулж харуулна. Жишээлбэл TCP пакетыг сонгосон байдлын зургийг зураг 6.1.-д үзүүллээ. Энэ хэсэгт мөн TCP толгой хэсгийн (header) Acknowledgement –ийн дугаарыг сонгосон байгаа бөгөөд энэхүү хэсэг нь пакетын байтын хэсэгт тодруулагдан харагдаж байна.

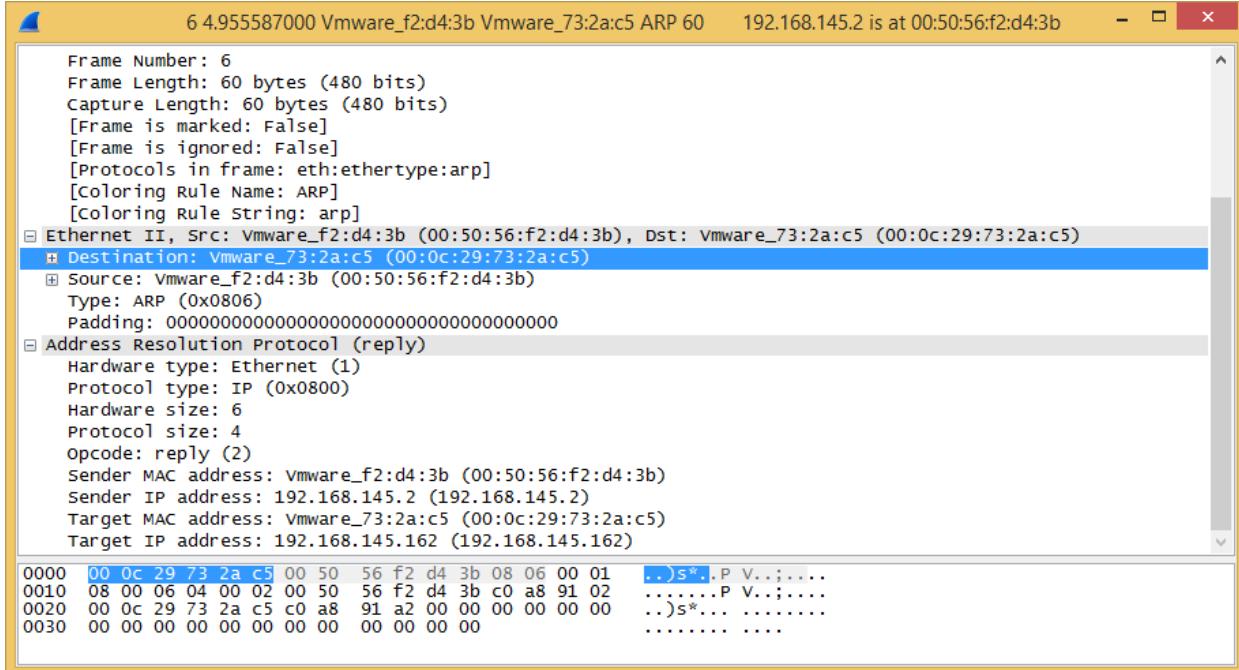


Зураг 6.1. Вайршарк програмд TCP пакетыг харах

Вайршарк програм пакет чагнаж байх үед (while capturing) ч гэсэн яг энэ аргаар хүссэн пакетаа харах боломжтой. Хэрэв пакет чагнаж дэлгэцэнд харуулж байгаа бол та “Capture Preferences (Чагнах тохиргоо)” хэсгээс пакетыг жагсаан харуулах самбарыг бодит хугацааны эгшинд шинэчилж байх тохиргоог хийж болдог. Ингэснээр шинээр чагнагдсан пакетууд пакетыг жагсаан харуулах самбарыг шинэчилж, нэмэгдэж байдаг.

Мөн түүнчлэн пакет бүрийг зураг 6.2.-т харуулсан шиг тусад нь цонхонд харах боломжтой. Ингэж харахын тулд пакетыг жагсаан харуулах самбар (packet list pane)

дээрээс харахыг хүссэн пакет дээр хулганаар 2 удаа дарах эсвэл тухайн пакетаа идэвхижүүлээд **View → Show Packet in New Window** гэсэн сонголтыг сонгох хэрэгтэй. Ийм байдлаар та 2 болон түүнээс олон пакетыг (тус тусдаа файлд байсан ч хамаагүй) хооронд нь харьцуулж харах боломжтой болно.



*Зураг 6.2. Пакетыг тусдаа цонхонд харж байна*

Пакетыг жагсаан харуулах хэсэгт хулганыг 2 удаа дарах мөн үндсэн цэсний сонголтуудыг ашиглан шинэ пакетын цонх үүсгэн олон арга байдаг.

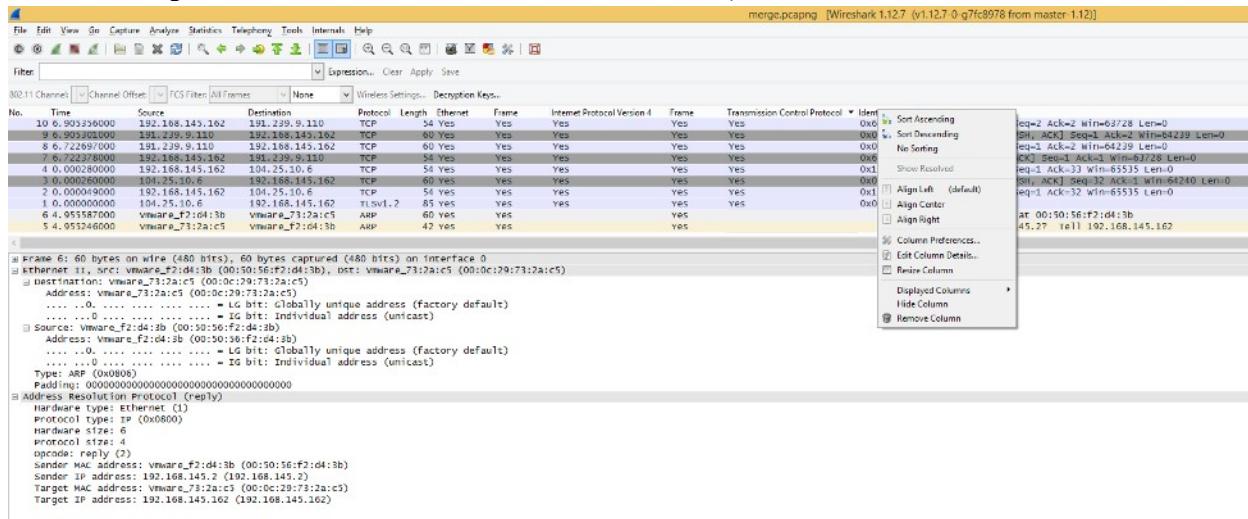
Along with double-clicking the packet list and using the main menu there are a number of other ways to open a new packet window:

- Shift товчийг дарангaa пакетыг дэлгэрэнгүй харуулах хэсгийн фрэймийн линк дээр хулганыг 2 удаа дарах
  - Хүснэгт 6.2. “Пакетыг жагсаан харуулах самбарын цэс”-ээс харна уу
  - Хүснэгт 6.3. “Пакетын мэдээллийг дэлгэрэнгүй харуулах самбарын цэс”-ээс харна уу

## 6.2. Дэлгэгдэн гарч ирдэг цэс (Pop up menu)

“Пакетыг жагсаан харуулах самбар (Packet list pane)” эсвэл “Пакетын мэдээллийг дэлгэрэнгүй харуулах самбар (packet details pane)”-үүд дээр дэлгэгдэн гарч ирдэг цэсийг (Pop-up Menu) гаргахын тулд тухайн самбартай харгалзах хэсэгт хулганы баруун товчийг дараах хэрэгтэй.

### 6.2.1. Пакетыг жагсаан харуулах хэсгийн баганы толгой дээр гарч ирэх цэс (Pop-up menu of the Packet List column header)



Зураг 6.3. Пакетыг жагсаан харуулах хэсгийн баганын толгой дээр гарч ирэх цэс (Pop-up menu of the "Packet List" column header)

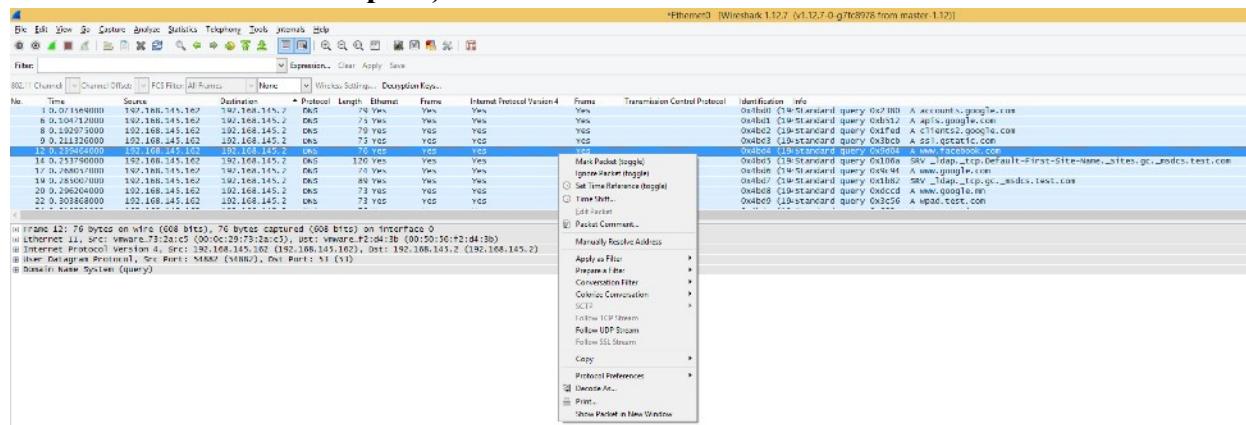
Дараах хүснэгтээр энэхүү цэснүүдийн функцуудийг товч тайлбарыг мөн эдгээр цэсийг үндсэн цэс (main menu)-ний хаанаас хайж олох боломжтойг харууллаа.

Хүснэгт 6.1. Пакетыг жагсаан харуулах самбар хэсгийн баганын толгой хэсгийн цэс (The menu items of the Packet List column header pop-up menu)

Цэс	Энэ цэстэй дүйцэх үндсэн цэс	Тайлбар
Sort Ascending		Тухайн баганын утгаас харгалзуулан багаас нь өсөх дарааллаар ангилана.
Sort Descending		Тухайн баганын утгаас харгалзуулан ихээс нь бага руу буурах дарааллаар ангилана.
No Sort		Тухайн баганын утгаар ангилсан ангилалыг арилгана.
Align Left		Энэ багана дахь утгуудыг зүүн тийш нь мөр тэнцүүлэх тохируулга хийнэ
Align Center		Энэ багана дахь утгуудыг төв хэсэгт нь мөр тэнцүүлэх тохируулга хийнэ
Align Right		Энэ багана дахь утгуудыг баруун тийш нь мөр тэнцүүлэх тохируулга хийнэ
Column Preferences...		Баганын тохиргооны хэсгийг шинэ цонхонд нээнэ (preferences)
Resize Column		Тухайн баганын уртыг энэхүү баганад харуулах утгын хэмжээнд тааруулан өөрчилнэ.
Rename Column Title		Баганын толгой хэсгийн гарчигийг өөрчлөх боломж

		олгоно.
Displayed Column	View	Энэ цэс бүх тохируулагдсан байгаа бүх багануудыг хумих хаах боломжийг олгодог. Өөрөөр хэлбэл энэ цэснээс та тухайн баганыг пакетыг жагсаан харуулах самбарт ил харуулах уу эсвэл харагдуулахгүй нуух уу гэдэг тохиргоог хийх боломжтой юм.
Hide Column		Тухайн баганыг пакетын жагсаан харуулах самбарт харуулахгүй болгоно.
Remove Column		Тухайн баганыг пакетыг жагсаан харуулах самбараас хасна

### 6.2.2. Пакетыг жагсаан харуулах самбарын хэсэгт гарч ирэх цэс (Pop-up menu of the Packet List pane)



Зураг 6.4. Пакетыг жагсаан харуулах самбарын хэсэгт гарч ирэх цэс (Pop-up menu of the Packet List pane)

Дараах хүснэгтэд эдгээр цэснүүдийг ашиглан юуг хийх боломжтой, тэдгээрийн үндсэн цэсний хаанаас олох боломжтойг оруулсан. Мөн түүнчлэн эдгээр цэснүүдийн товч тайлбарыг бас оруулсан байгаа.

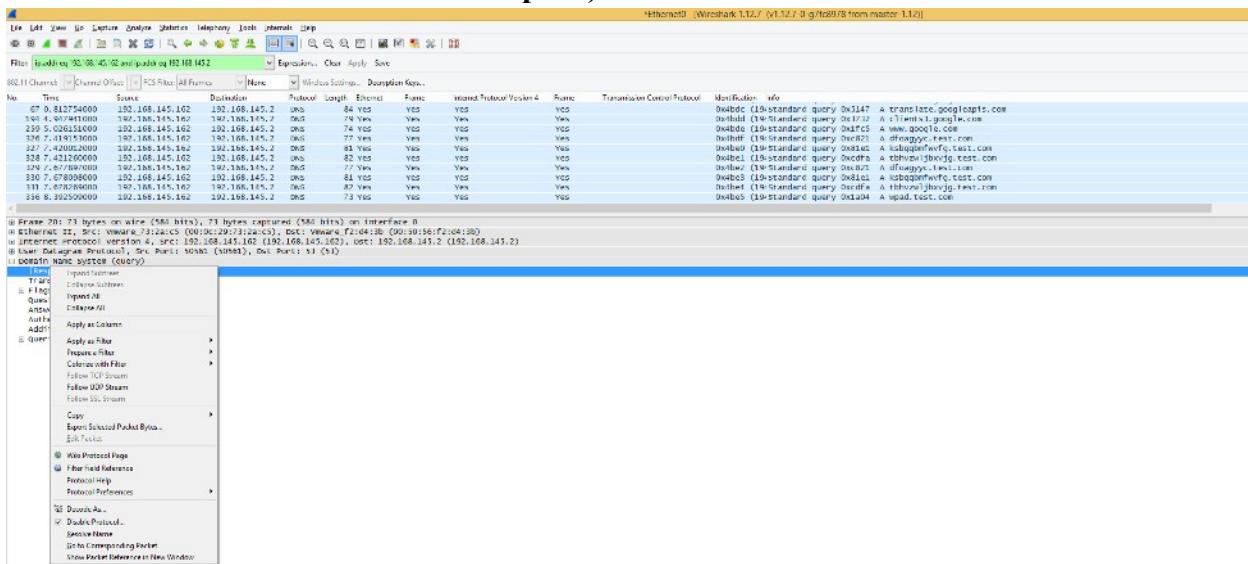
Хүснэгт 6.2. Пакетыг жагсаан харуулах самбарт гарч ирэх цэс (Menu items of the Packet List pop-up menu)

Цэс	Энэ цэстэй дүйцэх үндсэн цэс	Тайлбар
Mark Packet (toggle)	Edit	Пакетад тэмдэглэгээ хийх/тэмдэглэгээг болиулах (mark/unmark)
Ignore Packet (toggle)	Edit	Цуглувансан файлыг задалж үзэх явцдаа тухайн пакетыг үл ойшоох эсвэл хянаж шалгана
Set Time Reference (toggle)	Edit	Цагийн лавлагаа тохируулах/хэвэнд нь оруулах.

Manually Resolve Address		Идэвхижүүлсэн хаягад харгалзан хөрвүүлэх нэрийг оруулах боломжийг өгнө.
Apply as Filter	Analyze	Сонгосон байгаа хэсэг дээр суурилсан шүүлтүүрийг бэлдэж түүнийгээ идэвхижүүлэх
Prepare a Filter	Analyze	Сонгосон байгаа хэсэг дээр суурилсан дэлгэцийн шүүлтүүрийг бэлдэх
Conversation Filter		Энэ цэс нь сонгосон байгаа пакетын хаягийн мэдээллээр дэлгэцэнд байгаа пакетуудыг шүүдэг. Жишээлбэл IP хаягийг сонгон энэ хэсгийг идэвхижүүлбэл тухайн 2 IP хаягуудын траффикийг харуулна.
Colorize Conversation		Энэ цэс нь өнгөөр ялгах шинэ дүрэм үүсгэхийн тулд одоо сонгосон байгаа пакетын хаягийн мэдээлэл болон дэлгэцийн шүүлтүүрийн хэсгийг хэрэглэдэг.
SCTP		Энэ хэсэг нь хэрэглэгчид SCTP холболтын шүүлтүүрийг бэлдэх, анализ хийх боломжийг олгоно.
Follow TCP Stream	Analyze	2 цэгийн хоорондох бүх TCP урсгалын өгөгдлийг харуулна.
Follow UDP Stream	Analyze	2 цэгийн хоорондох бүх UDP урсгалын өгөгдлийг харуулна.
Follow SSL Stream	Analyze	2 SSL холболттой цэгийн хоорондох бүх SSL урсгалын мэдээллийг харуулна.
Copy/ Summary (Text)		Товч дүгнэлтийн талбар (summary field)-ийг дэлгэцэнд харагдаж байгаа байдлаар нь санах ой руу (clipboard) хуулна. Ингэхдээ tab-separated текст хэлбэрээр хуулдаг.
Copy/ Summary (CSV)		Comma-separated текст хэлбэрээр товч дүгнэлтийн талбар (summary field)-ийг санах ой руу (clipboard) хуулна.
Copy/ As Filter		Одоо идэвхижсэн байгаа хэсгээр шүүлтүүрийг бэлдэх бөгөөд энэхүү сонгогдсон хэсгээ санах ой (clipboard) руу хуулдаг.
Copy/ Bytes (Offset Hex Text)		Пакетын мэдээллийг байт хэлбэрээр санах ой (clipboard) руу хуулна. Ингэхдээ hexdump шиг форматаар хуулах бөгөөд текстийн хэсгийг нь хуулахгүй
Copy/ Bytes (Offset Hex)		Пакетын мэдээллийг байт хэлбэрээр санах ой руу (clipboard) хуулна. Ингэхдээ hexdump шиг форматаар хуулах бөгөөд текстийн хэсгийг нь хуулахгүй
Copy/ Bytes (Printable Text Only)		Хэвлэгдэх боломжгүй текстүүдийг нь хассан байдлаар пакетын байт мэдээллийг ASCII текст форматаар санах ой руу (clipboard) хуулдаг
Copy/ Bytes (Hex Stream)		Пакетын байт мэдээллийг санах ой (clipboard) руу хуулдаг. Ингэхдээ цэг таслалгүй хекс тооны жагсаалт байдлаар хуулдаг.

Copy/ Bytes (Binary Stream)		Рав бинари (raw binary) хэлбэрээр пакет байт өгөгдлийг санах ой (clipboard) руу хуулдаг. Санах ойд (clipboard) хуулагдсан өгөгдөл нь MIME-төрлийн “application/octet-stream” байдаг
Decode As...	Analyze	2 задлагч хэсгийн хоорондын шинэ хамаарлыг идэвхижүүлэх эсвэл өөрчилдөг.
Print...	File	Пакетыг хэвлэнэ.
Show Packet in New Window	View	Идэвхижсэн пакетыг шинэ цонхонд хэвлэнэ.

### 6.2.3. Пакетын мэдээллийг дэлгэрэнгүй үзүүлэх самбарт гарч ирэх цэс (Pop-up menu of the Packet Details pane)



Зураг 6.5. Пакетын мэдээллийг дэлгэрэнгүй харуулах хэсэгт гарч ирэх цэс (Pop-up menu of the Packet Details pane)

Дараах хүснэгтээр энэ хэсэгт хэрэгжүүлэх боломжтой функцуудийг тэдний тайлбар мөн эдгээр функцуудийн үндсэн цэсэнд харгалзах хэсэг зэргийг харууллаа.

Хүснэгт 6.3. Пакетын мэдээллийг дэлгэрэнгүй харах самбарт гарч ирэх цэс (The menu items of the Packet Details pop-up menu)

Цэс	Энэ цэстэй дүйцэх үндсэн цэс	Тайлбар
Expand Subtrees	View	Идэвхитэй байгаа хэсгийн дэд мод хэлбэрийн (subtree) мэдээлүүдийг задлах
Collapse Subtrees	View	Идэвхитэй байгаа хэсгийн дэд мод хэлбэрийн мэдээллийг хумих
Expand All	View	Пакет файлд байгаа бүх пакетын дэд мод

		хэлбэрийн мэдээллүүдийг задлах
Collapse All	View	Пакет файлд байгаа бүх пакетын дэд мод хэлбэрийн мэдээллүүдийг хумиж хаана.
Apply as Column		Идэвхитэй байгаа протоколын хэсгийг ашиглан пакетыг жагсаан харуулах хэсэгт багана нэмэрх.
Apply as Filter	Analyze	Идэвхитэй байгаа хэсгийг ашиглан дэлгэцийн шүүлтүүр үүсгэн түүнийгээ идэвхижүүлэх.
Prepare a Filter	Analyze	Идэвхитэй байгаа хэсгийг ашиглан дэлгэцийн шүүлтүүрийн хэсгийг бэлдэх.
Colorize with Filter		Энэ цэс нь идэвхитэй байгаа протоколын хэсэг болон дэлгэцийн шүүлтүүрийн хэсгийг ашиглан өнгөөр ялгах шинэ дүрэм үүсгэдэг.
Follow TCP Stream	Analyze	2 төгсгөлийн цэгийн хооронд дамжиж буй TCP өгөгдлийг харуулна.
Follow UDP Stream	Analyze	2 төгсгөлийн цэгийн хооронд дамжиж буй UDP өгөгдлийг харуулна.
Follow SSL Stream	Analyze	2 төгсгөлийн цэгийн хооронд дамжиж буй SSL өгөгдлийг харуулна.
Copy/ Description	Edit	Идэвхижсэн байгаа талбарын дэлгэцэнд харагдаж байгаа текст өгөгдлийг санах ой (clipboard) руу хуулна
Copy/ Fieldname	Edit	Идэвхитэй байгаа талбарын нэрийг санах ой руу (clipboard) хуулна.
Copy/ Value	Edit	Идэвхитэй байгаа талбарын утгыг санах ой (clipboard) руу хуулна.
Copy/ As Filter	Edit	Идэвхитэй байгаа хэсгийг ашиглан дэлгэцийн шүүлтүүрийг бэлдэх ба энэ хэсгийн өгөгдлийг санах ой (clipboard) руу хуулна.
Copy/ Bytes (Offset Hex Text)		Пакетын байт мэдээллийг санах ой (clipboard) руу hexdump-тай төстэй форматаар хуулна. Пакетыг жагсаан харуулах самбарын командтай ерөнхийдөө ижилхэн боловч энэ команд нь зөвхөн пакетын байт хэсэгт идэвхитэй байгаа хэсэгт хамааралтай байт өгөгдлийг хуулдаг.
Copy/ Bytes (Offset Hex)		Пакетын байт мэдээллийг санах ой (clipboard) руу hexdump-тай төстэй форматаар хуулна. Гэхдээ текстийн хэсгийг хуулахгүй. Пакетыг жагсаан

		харуулах самбарын командтай ерөнхийдөө ижилхэн боловч энэ команд нь зөвхөн пакетын байт хэсэгт идэвхитэй байгаа хэсэгт хамааралтай байт өгөгдлийг хуулдаг.
Copy/ Bytes (Printable Text Only)		Пакетын байт мэдээллийг санах ой (clipboard) руу ASCII тэмдэгт (хэвлэгдэх боломжгүй тэмдэгтүүдийг хасдаг) хэлбэрээр хуулна. Пакетыг жагсаан харуулах самбарын командтай ерөнхийдөө ижилхэн боловч энэ команд нь зөвхөн пакетын байт хэсэгт идэвхитэй байгаа хэсэгт хамааралтай байт өгөгдлийг хуулдаг.
Copy/ Bytes (Hex Stream)		Пакетын байт мэдээллийг санах ой (clipboard) руу цэг таслалгүй хекс тоон лист форматаар хуулна. Пакетыг жагсаан харуулах самбарын командтай ерөнхийдөө ижилхэн боловч энэ команд нь зөвхөн пакетын байт хэсэгт идэвхитэй байгаа хэсэгт хамааралтай байт өгөгдлийг хуулдаг.
Copy/ Bytes (Binary Stream)		Пакетын байт мэдээллийг санах ой (clipboard) руу рав бинари (raw binary) форматаар хуулна. Пакетыг жагсаан харуулах самбарын командтай ерөнхийдөө ижилхэн боловч энэ команд нь зөвхөн пакетын байт хэсэгт идэвхитэй байгаа хэсэгт хамааралтай байт өгөгдлийг хуулдаг. Өгөгдөл нь санах ойд (clipboard) MIME-төрлийн “application/octet-stream” хэлбэрээр хадгалагддаг.
Export Selected Packet Bytes...	File	Энэ цэс нь File цэсний ийм цэстэй ижилхэн үйлдэл хийдэг. Өөрөөр хэлбэл энэ цэс нь рав пакет байтуудыг (raw packet bytes) бинари файл (binary file) руу экспорт хийдэг
Wiki Protocol Page		Идэвхитэй байгаа протоколын хэсэгтэй холбоотой вики хуудсыг таны веб хөтөч дээр нээнэ .
Filter Field Reference		Идэвхижсэн байгаа протоколын талбартай харгалзуулан шүүлгүүр хийж болох тохиргооны сонголтуудыг таны веб хөтөч дээр харуулна.

Protocol Preferences...		Энэ цэс нь таныг төлөв байдлыг (properties) харуулах цонх руу хөтөлдөг. Ингэхдээ хэрэв идэвхижүүлсэн талбарт хамаарах төлөв байдлын хуудсыг сонгодог. Илүү дэлгэрүүлэн уншихыг хүсвэл Зураг 10.7. Тохииргооны цонх (Preferences dialog)-г үзнэ үү
Decode As...	Analyze	Хоёр задлагч (dissector) хэсгийн дундын шинэ хамаарлыг идэвхижүүлэх эсвэл өөрчлөх
Disable Protocol		Албан ёсны протокол задлагчийг хааж байж болзошгүй протокол задлагчийг (dissector) түр хаана.
Resolve Name	View	Идэвхитэй байгаа пакетад нэрийн хөрвүүлэлтийг хийдэг. (Бүх пакетад биш зөвхөн тухайн сонгосон пакетад л нэрийн хөрвүүлэлт хийгдэнэ)
Go to Corresponding Packet	Go	Хэрэв идэвхижсэн байгаа талбарт харгалзах пакет байгаа бол тухайн пакет руу очно. Харгалзах пакет нь ихэвчлэн request/response пакетын хос эсвэл үүнтэй төстэй пакетууд байдаг.

### 6.3. Пакет үзэх үйлдэл хийх үедээ пакетуудад шүүлтүүр хийх (Filtering packets while viewing)

Вайршарк програм шүүлтүүрийн 2 хэлтэй. Нэг нь чагнах процесийн үед шүүлтүүр хийдэг бол нөгөөх нь пакетыг дэлгэцэнд харуулах үед шүүлтүүр хийдэг. Энэ хэсэгт бид 2 дахь тохиолдолыг авч үзэх юм. Өөрөөр хэлбэл энэ хэсэг нь дэлгэцийн шүүлтүүр юм. Эхний хэсгийн талаар бид 4.13. “Чагнах процесийн үед шүүлтүүр хийх” хэсэгт авч үзсэн байгаа.

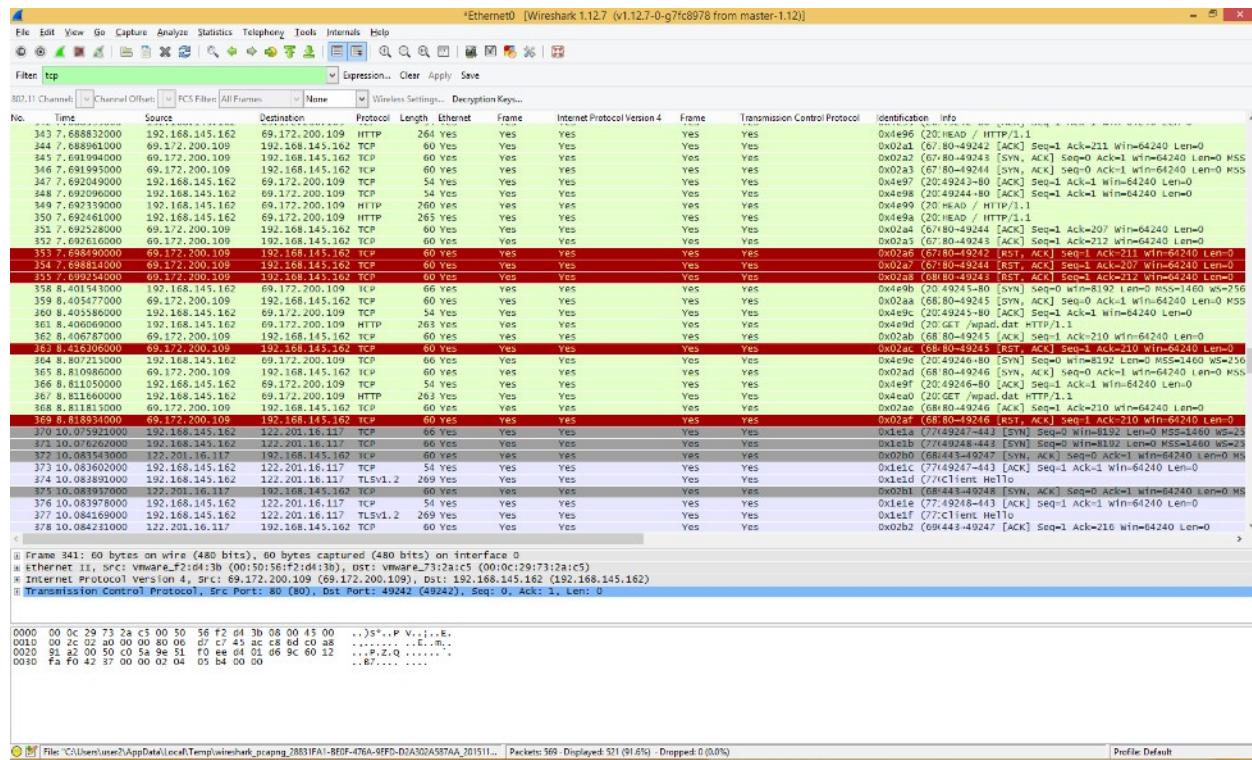
Дэлгэцийн шүүлтүүр нь өөрийн сонирхсон пакетуудаа ялгаж зөвхөн тэдэн дээрээ анхаарах боломжийг олгоно. Таны сонирхлыг татахгүй байгаа пакетуудыг дэлгэцэнд харагдуулахгүй болгон нуудаг. Дэлгэцийн шүүлтүүр нь дараах зүйлсийг ашиглан шүүлт хийх боломжтой.

- Протокол (Protocol)
  - Протоколын талбар (The presence of a field)
  - Талбарын утга (The values of fields)
  - Талбаруудыг хооронд нь харьцуулсан харьцуулалт (A comparison between fields)
- ГЭХ МЭТ

Протоколын төрөл дээр тулгуурлан пакетуудыг сонгохын тулд Вайршарк програмын шүүлтүүрийн товчлууруудын хэсэгт хэсэгт өөрийн сонирхож буй протоколын төрлийг бичиж **Enter** дараахад л хангалттай. Зураг 6.6. “TCP протоколоор шүүлт хийж байна” зурагт шүүлтүүрийн хэсэгт **tcp** –г оруулвал юу болж байгааг дүрслэн үзүүлсэн байна.

## Мэдэгдэл

Протоколын нэрүүд болон талбарын нэрүүдийг шүүлтүүрийн хэсэгт дандаа жижиг үсгээр оруулна. Мөн энэ хэсэгт түлхүүр үгээ оруулсны дараа **Enter** дарж байж л энэхүү шүүлтүүр идэвхижих ёстойг анхаарна уу.



Зураг 6.6. “TCP протоколоор шүүлт хийж байна (Filtering on the TCP protocol)”

Одоо дэлгэцэнд зөвхөн TCP протоколын пакетуудыг харуулж байгааг анхаарч харна уу.

## Мэдэгдэл

Дэлгэцний шүүлтүүрээр пакетыг шүүх үед вайршарк програм зөвхөн пакетыг дэлгэцэнд харуулахдаа л ялгаж харуулах бөгөөд энэхүү пакетууд байгаа пакет файлд ямар нэгэн өөрчлөлт орохгүй.

Та вайршарк програм уншиж чадах бүх протоколоор шүүлт хийж болно. Мөн түүнчлэн мод хэлбэрийн бүтцэд нэмэгдэж байгаа талбар бүрээр шүүлт хийж болно. Гэхдээ ингэхийн

тuld эдгээр задлагч (dissector) талбар нь үсгийн товчлолтой байх ёстой. Эдгээр талбаруудыг жагсаалт хэлбэрээр харахын тулд вайршарк програмын *Add Expression...* хэсгийг үзэх хэрэгтэй. Илүү дэлгэрүүлэн уншихыг хүсвэл **6.5. “Шүүлтүүрийн илэрхийлэл (Filter Expression)”** хэсгийг уншина уу

Пакетыг жагсаалт хэлбэрээр харуулах самбарт байгаа пакетууд дундаас зөвхөн нэг IP хаяг (192.168.0.1.) руу илгээж байгаа эсвэл тухайн IP хаягнаас (192.168.0.1.) ирж буй пакетуудыг ялган авч сонирхохыг хүсвэл дараах шүүлтүүрийн илэрхийллийг хэрэглэнэ .

ip.addr==192.168.0.1

#### Мэдэгдэл

Шүүлтүүрийг болиулахын тулд шүүлтүүрийн илэрхийлэл оруулах талбарын баруун талд байрлах Clear товчлуурыг дарна.

### 6.4. Дэлгэцийн шүүлтүүрийн илэрхийллийг үүсгэх (Building display filter expressions)

Вайршарк програмын шүүлтүүрийн хэл нь энгийн хэрнээ хүчирхэг шүүлтүүрийн илэрхийллийг оруулах боломжоор хэрэглэгчийг хангадаг. Та пакет доторх утгуудыг харьцуулахаас гадна илүү нарийвчилсан илэрхийлэл бичихийн тулд илэрхийллүүдийг хамтад нь хослуулан хэрэглэж болдог. Дараах хэсгүүдэд эдгээр илэрхийллийг хэрхэн бичихийг дэлгэрүүлэн үзүүллээ.

#### Зөвлөгөө

Вайршарк програмын дэлгэцийн шүүлтүүрийн жишээнүүдийг wireshark-wiki-display-filter:[wireshark-wiki-display-filter:[]] дээрх Вайршарк Вики Дэлгэцийн Шүүлтүүрийн хуудаснаас харах боломжтой.

#### 6.4.1. Дэлгэцийн шүүлтүүрийн талбарууд (Display filter fields)

Пакетын мэдээллийг дэлгэрэнгүй харуулах самбарын бүх талбарууд (field) шүүлтүүрийн тэмдэгт мөрөөр ашиглагдах боломжтой. Энэхүү шүүлтүүрийн үр дүнд зөвхөн эдгээр талбарууд (field) оршин байгаа пакетуудыг л дэлгэцэнд харуулна. Жишээлбэл: tcp гэсэн тэмдэгт мөрөөр шүүлтүүр хийвэл зөвхөн tcp протоколыг агуулсан пакетууд л харагдана.

Вайршарк програм дэмжих боломжтой бүх шүүлтүүрийн талбаруудыг **Help → Supported Protocols** цонхны “*Supported Protocols*” хэсгээс харах боломжтой.

#### 6.4.2. Утгуудыг харьцуулах (Comparing values)

Төрөл бүрийн харьцуулалтын операторуудыг ашиглан талбарын утгуудыг харьцуулах шүүлтүүрийн илэрхийллүүдийг бичдэг. Хүснэгт 6.4. “Дэлгэцийн шүүлтүүрийн харьцуулах операторууд”-д эдгээр операторуудыг харууллаа.

#### Зөвлөгөө

Та Англи болон Си хэлний хувилбаруудын алийг нь ч ашиглаж болно.

*Хүснэгт 6.4. Дэлгэцийн шүүлтүүрийн харьцуулах операторууд*

Англи	Си төст хувилбар	Тайлбар, Жишээ
eq	==	Тэнцүү, ip.src==10.0.0.5
ne	!=	Тэнцүү биш, ip.src!= =10.0.0.5
gt	>	Их, frame.len > 10
lt	<	Бага, frame.len < 128
ge	>=	Их буюу тэнцүү, frame.len ge 0x100
le	<=	Бага буюу тэнцүү, frame.len <= 0x20

Түүнчлэн протоколын талбар бүр төрөлтэй. Хүснэгт 6.5. “Дэлгэцийн шүүлтүүр талбарын төрлүүд”-д эдгээр төрлүүдийг харуулсан бөгөөд эдгээр төрлүүдийг хэрхэн ашиглахыг харуулсан жишээг орууллаа.

*Хүснэгт 6.5. Дэлгэцийн шүүлтүүр талбарын төрлүүд*

Төрөл	Жишээ
Unsigned integer (8-bit, 16-bit, 24-bit, 32-bit)	Бүхэл тоог илэрхийлэхдээ аравт, наймт, арван зургаатын тооллын системийн алинаар нь ч бичигдэж болно. Жишээлбэл эдгээр шүүлтүүрийн илэрхийллүүд бүгд ижилхэн юм ---- ip.len le 1500 ip.len le 02734 ip.len le 0x436 ----
Signed integer (8-bit, 16-bit, 24-bit, 32-bit)	
Boolean	Бүүлийн утга нь зөвхөн протоколыг задлах үед тухайн талбарын утга үнэн байх тохиолдолд ашиглагддаг. Жишээлбэл tcp.flags.syn илэрхийлэл хэзээ үнэн байх вэ гэхээр TCP сегментийн толгой (header) дотор SYN flag байх үед юм.  Иймд tcp.flags.syn нь зөвхөн tcp syn flag байгаа пакетуудыг ялган харуулна.
Ethernet address (6 bytes)	Тусгаарлагч тэмдэг нь (:), (.), (-) зэрэг байх бөгөөд эдгээр тусгаарлагчдийн дунд нэг эсвэл хоёр байт байдаг. Жишээлбэл ---- eth.dst ==

	ff:ff:ff:ff:ff:ff eth.dst == ff-ff-ff-ff-ff-ff eth.dst == ffff.ffff.ffff ----
IPv4 address	ip.addr == 192.168.0.1  Хэрэв IPv4 хаяг тодорхой subnet-д байгаа эсэхийг шалгахын тулд CIDR –г хэрэглэх боломжтой. Жишээлбэл Дараах шүүлтүүр нь 129.111 Class-B хаягтай холбоотой бүх пакетуудыг ялган харуулна.
	ip.addr == 192.111.0.0/16
IPv6 address	ipv6.addr == ::1

**6.4.3. Илэрхийлүүдийг хослуулан хамтад нь хэрэглэх (Combining expressions)**  
Хүснэгт 6.6-д үзүүлсэн логик операторуудыг ашиглан шүүлтүүрийн илэрхийлүүдийг хослуулан хэрэглэх боломжтой.

*Хүснэгт 6.6 Дэлгээцийн шүүлтүүрийн логик операторууд*

Англи	Си төст	Тайлбар, жишээ
and	&&	Логик AND ip.src==10.0.0.5 tcp.flags.fin and
or		Логик OR ip.scr == 10.0.0.5 ip.src == 192.1.1.1 or
xor	^^	Логик XOR tr.dst[0:3]==0.6.29 tr.src[0:3]==0.6.29 xor
not	!	Логик NOT not llc
[...]		Дэд текст (substring) оператор. Вайршарк програм танд нарийвчлан заахын оронд үргэлжилсэн цуваа хэлбэрээр сонгох боломжийг олгодог. Хаягжуулсны дараа 2 хос та тодорхой завсар дахь утгыг (таслалаар тусгаарлан) агуулсан хос хаалт [] нэмж байрлуулна. --- eth.src[0:3] == 00:00:83 ---- Энэ жишээнд n:m форматтайгаар ганцхан завсарыг тодорхойлж өгсөн байна. Энэ тохиолдолд n нь оффсетийн эхлэл бөгөөд m нь энэхүү завсарыг тодорхойлж буй уртын хэмжээ юм. ---- eth.src[1-2]== 00:83 ---- Энэ жишээнд n-m форматыг ашиглан ганцхан завсарыг илэрхийлсэн байна. Энэ тохиолдолд n нь

	<p>оффсетийн эхлэл харин т нь оффсетийн төгсгөл юм.</p> <p>---- eth.src[:4] == 00:00:83:00 ---- Энэ жишээнд :t форматыг ашигласан бөгөөд энэ нь оффсетийн эхлэлээс т оффсет хүртэлх бүх утгийг агуулна. Энэ нь өөрөөр бол 0:t гэсэн завсртай ижилхэн.</p> <p>---- eth.src[4:] == 20:20 ---- Энэ жишээ нь p: форматыг ашигласан байгаа нь харагдаж байна. Энэ нь p дэх оффсетээс хойши бүх оффсетийн завсрыйг агуулна.</p> <p>---- eth.src[2] == 83 ---- Энэ жишээнд p форматыг ашиглан ганицан завсрыйг тодорхойлж өгч байна. Энэ тохиолдолд цуваа хэлбэрийн дотор байгаа p оффсет дээрх элементийг сонгодог. Энэ нь p:1 гэсэн илэрхийлэлтэй ижилхэн юм.</p> <p>----eth.src[0:3,1-2,:4,4:,2] == 00:00:83:00:83:00:00:83:00:20:20:83---- Олон хосолсон завсрыйг бий болгохын тулд та вайршарк програм дээр завсруудыг таслааар тусгаарлан бичиж өгөхөд хангалттай.</p>
--	---

#### 6.4.4. Нийтлэг алдаа (A common mistake)

!= операторыг ашиглан eth.addr, ip.addr, tcp.port, udp.port талбаруудыг ашиглан хосолсон илэрхийлэл бичих үед таны хүлээж байгаа шиг ажиллахгүй байх магадлалтай.

Хүмүүс ихэнхдээ 1.2.3.4 ip хаягийг агуулсан бүх пакетуудыг дэлгэцэнд харуулахын тулд ip.addr == 1.2.3.4. Харин 1.2.3.4 ip хаягийг агуулаагүй пакетуудыг шүүн харахын тулд ip.addr != 1.2.3.4 илэрхийллийг хэрэглэдэг. Гэхдээ энэ илэрхийлэл таны хүссэн үйлдлийг хийдэггүй.

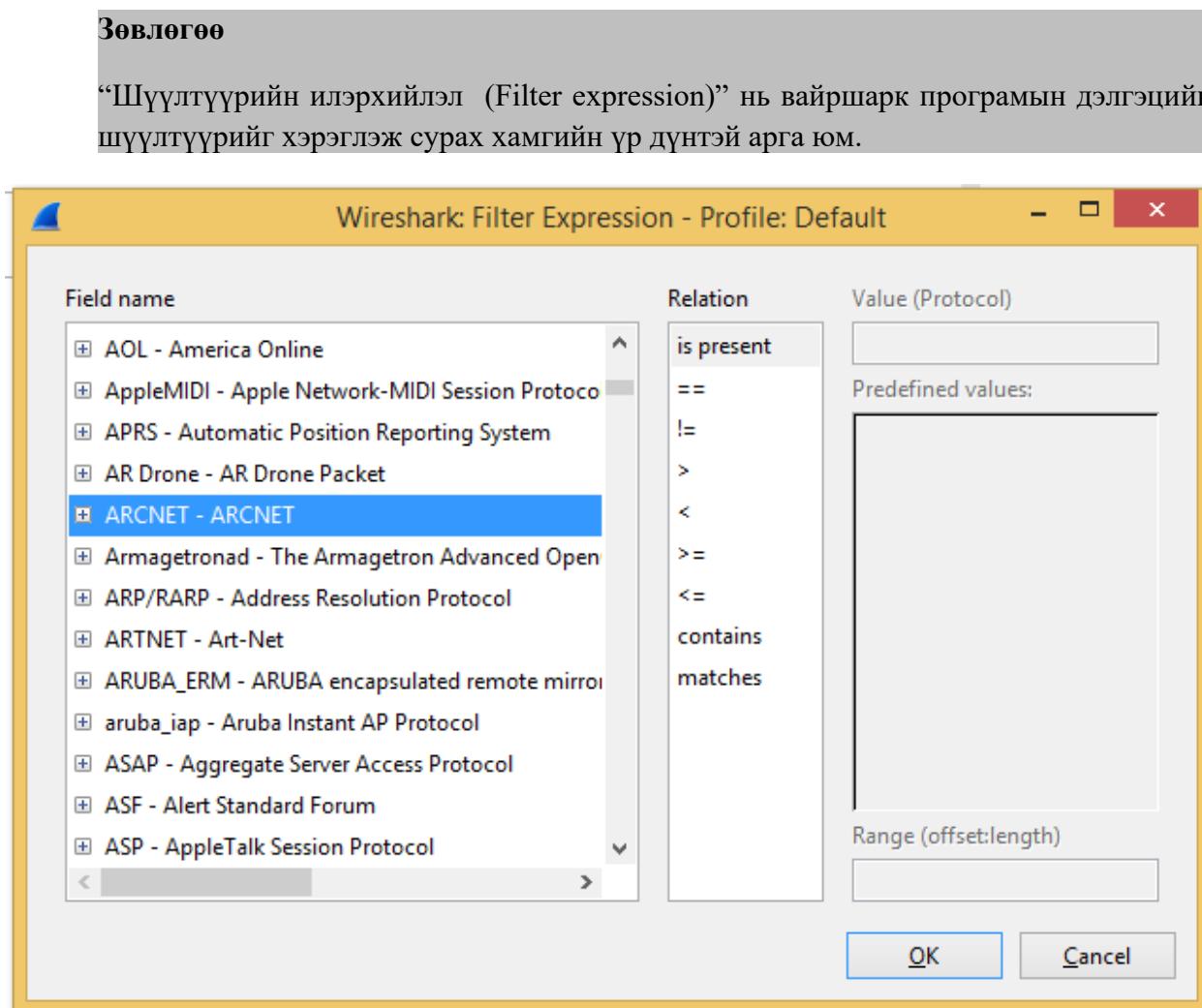
Энэ илэрхийлэл нь 1.2.3.4 гэсэн ip хаягыг агуулсан пакетуудыг харуулдаг. Үүний шалтгаан нь ip.addr != 1.2.3.4 илэрхийлэл нь уншигдахдаа ip.addr талбар нь 1.2.3.4 гэсэн утгаас ялгаатай байх ёстой гэж уншигддаг. IP datagram нь илгээгч болон хүлээн авагч (source, destination) агуулдаг учраас энэ илэрхийлэл нь энэ илэрхийлэл нь энэ 2 талбарын аль нэг хаяг л 1.2.3.4 утгаас өөр байгаа эсэхийг үнэлдэг.

Хэрэв та 1.2.3.4 хаягаас ирж байгаа эсвэл энэ хаягийн хүлээн авч буй пакетуудыг ялгаж хасахыг хүсч байвал шүүлтүүрийн илэрхийллээ !(ip.addr == 1.2.3.4) ийм болгон өөрчлөх хэрэгтэй энэ нь ip.addr гэсэн талбар нь 1.2.3.4 гэсэн хаягтай байгаа пакетуудыг ялгаж аваад дараа нь үгүйсгэл хийж байна.

#### 6.5. Шүүлтүүрийн илэрхийлэл цонх (The Filter Expression)

Вайршарк програмын шүүлтүүрийн системийг хэрэглэж сурсан хүнд хэзээ ямар түлхүүр үг ашиглан шүүлтүүр хийх вэ гэдгээ хялбархан гараар бичиж оруулчихаж болохуйц маш хялбархан, энгийн зүйл юм. Гэвч хэрэв та вайршарк програм дээр ажиллаж байгаагүй эсвэл сүлжээний протоколыг ашиглан шүүлтүүр хийж байсан туршлага байхгүй бол

шүүлтүүрийн процесс маш эргэлзээтэй мэт санагдаж болно. Шүүлтүүрийн илэрхийлэл (filter expression) хэсэг нь танд эдгээр эргэлзээг багасгаж өгөх зорилготой юм.



Зураг 6.7 Шүүлтүүрийн илэрхийлэл (Filter Expression)

Шүүлтүүрийн илэрхийлэл (Filter Expression) цонхыг нээгээд та гурван хэсэг талбарыг харах бөгөөд эдгээр хэсгүүд нь протоколын талбар болон тэдгээртэй холбоотой хэсгүүдийг агуулдаг.

#### Талбарын нэр (Field Name)

Протоколын талбар мод хэлбэрийн (Protocol field tree) хэсгээс протоколын талбарыг сонгоно. Дээд түвшинд шүүж болох бүхий л протоколын талбарууд энд байгаа. (протоколын талбарыг хайхын тулд тухайн талбарын эхний хэдэн үсгийг оруулах хэрэгтэй). Протоколын нэрийг доош нь задалснаар та тухай протоколын хувьд

шүүн харж болох талбаруудыг харна.

*Хамаарал (Relation)*

Хамаарлыг соонгох хэсгээс хэрхэн хамааруулж болох вэ гэдгээ сонгоно. Энэ хэсэг нь унар оператор буюу хэрэв тухайн талбар нь пакетад байгаа эсэхийг шалгадаг нэг байт оператортой.

Энэхүү унар оператороос бусад нь операторууд нь бүгд бинари хамаарал буюу нэмэлт өгөгдөл шаарддаг операторууд юм. (Жишээлбэл: Жишиж үзэх утга)

Та талбарын нэр хэсгээс талбараа сонгоод улмаар хамаарлын (relation) хэсгээс бинари оператор сонгосон тохиолдолд (жишээлбэл тэнцүү эсэх хамаарлыг шалгах == оператор сонгосон бол) танд утга оруулах (value) хэсэг идэвхижих бөгөөд энэ хэсэгт тодорхой завсарт байх утга оруулж ч болох тохиолдол бий.

*Утга (Value)*

Утга оруулах хэсэгт та тухайн талбарын хэсэгт тохирох утгыг оруулах боломжтой. Энэхүү Утга нь тухайн талбарын нэрийн төрлийг илэрхийлдэг. Жишээлбэл тэмдэгт мөр байх гэх мэт

*Үрьдчилан тодорхойлсон утгууд (Predefined values)*

Зарим протоколын талбарууд нь Си хэлэн дэх enum шиг үрьдчилан тодорхойлсон утгуудтай байдаг. Хэрэв таны сонгосон протоколын талбарт хэрэглэх боломжтой үрьдчилан тодорхойлсон талбарын утга байвал та энэ хэсгээс сонгох боломжтой.

*Завсар (Range)*

Тоон утгын завсар эсвэл завсаруудыг агуулсан хэд хэдэн завсарууд байж болно. Жишээлбэл 1-12 эсвэл 39-42, 98-2000

*OK*

Өөрийн хүссэн шүүлтүүрээ оруулж дууссан бол OK товчийг дарах хэрэгтэй. Ингэснээр таны шүүлтүүрийн түлхүүр үг бэлэн болно.

*Цуцлах (Cancel)*

Шүүлтүүрт ямар нэгэн өөрчлөлт оруулахгүйгээр энэхүү цонхыг хаана.

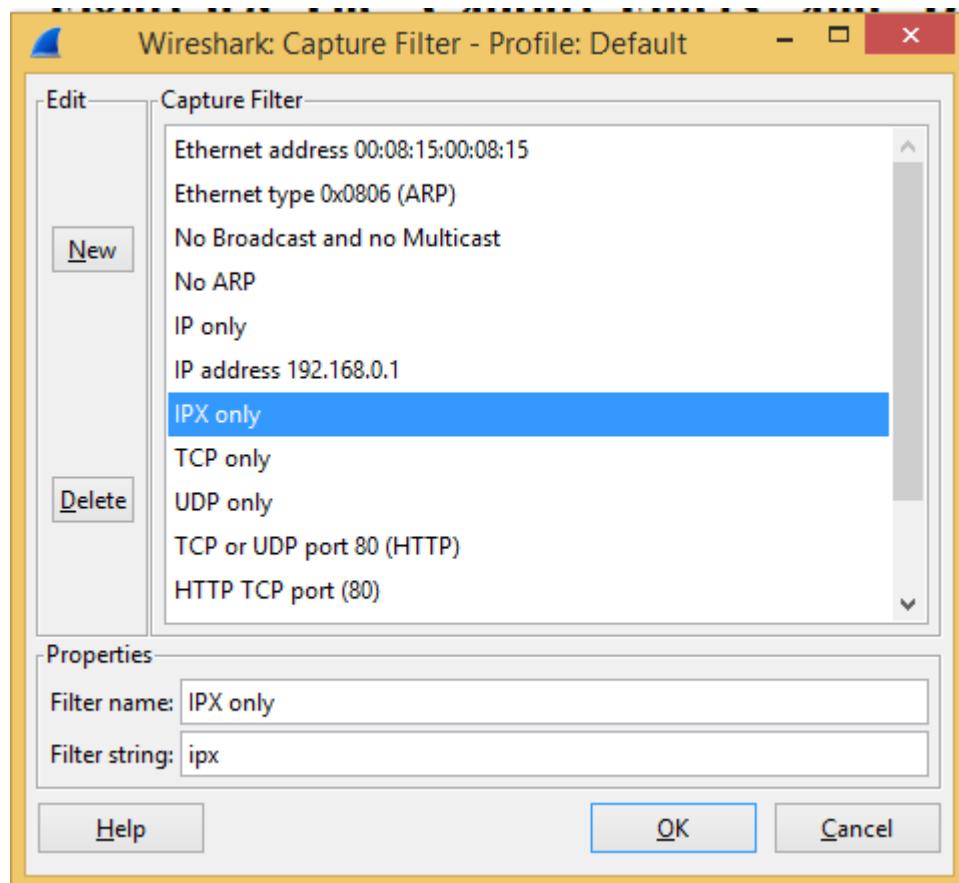
## 6.6. Шүүлтүүрийг үүсгэж, хадгалах (Defining and saving filters)

Та өөрийн хэрэгцээнд нийцсэн шүүлтүүрийн илэрхийллийг үүсгэж түүндээ нэр өгөх боломжтой юм. Улмаар эдгээр шүүлтүүрийн илэрхийллээ дараа нь ашиглах боломжтой.

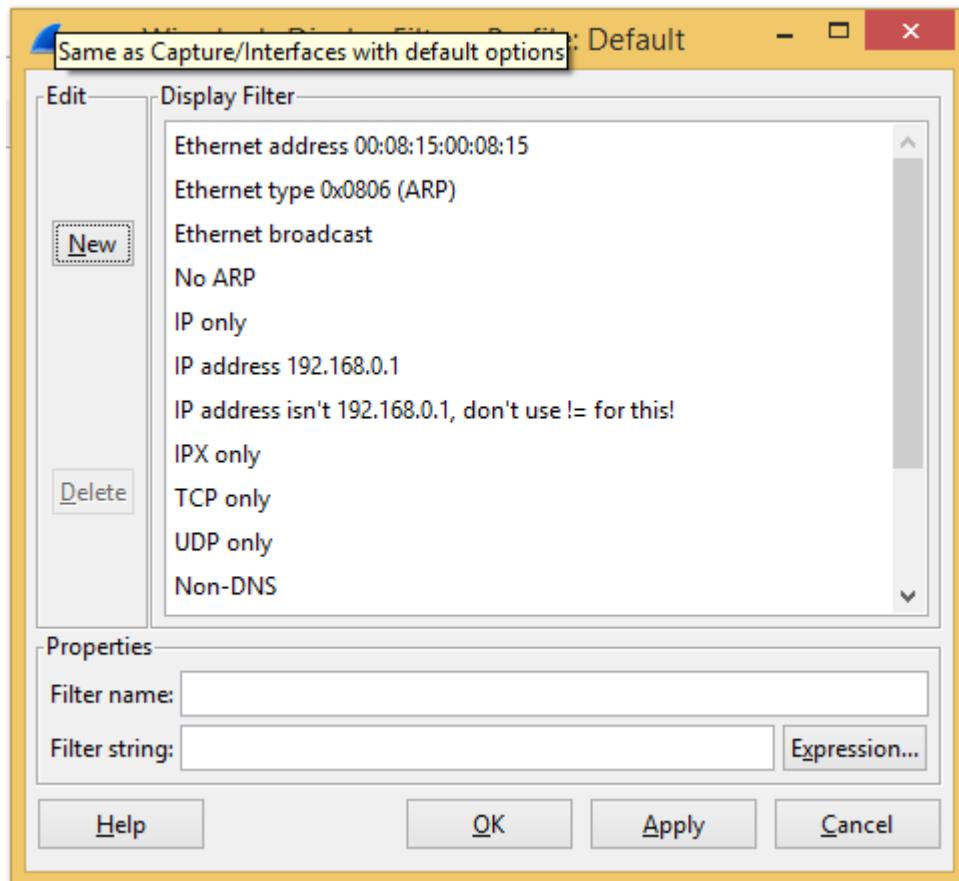
Энэ нь танд маш урт эсвэл дахин дахин бичихэд төвөгтэй байж болох шүүлтүүрийн илэрхийллийг хэрэглэх үед таны цагийг хэмнэж, үйлдлийг тань хялбарчилсж өгдөг.

Шинэ шүүлтүүрийн илэрхийллийг үүсгэх эсвэл өмнө нь үүсгэсэн шүүлтүүрийн илэрхийллээ засварлахын тулд Capture → Capture Filters хэсгийг сонгож пакет чагнах үеийн шүүлтүүрийг харин Analyze → Display Filters хэсгийг сонгож дэлгэцийн шүүлтүүрийг дэлгэцэнд гаргаж ирнэ. Ингэснээр вайршарк програм танд **Зураг 6.8** болон **Зураг 6.9-д** үзүүлсэн зургуудийг харуулна.

Дэлгэцийн шүүлтүүр (display filter) болон пакет чагнах үеийн шүүлтүүрийг (Capture Filter) үүсгэх, хадгалах нь бараг л яг ижилхэн бөгөөд эдгээр ойлголтуудыг нэгтгэн энэ хэсэгт авч үзсэн болно. Гэхдээ тэдгээрийн зарим жижигхэн ялгааг тухай бүрт нь дурдсан байгаа.



Зураг 6.8 Пакет чагнах үеийн шүүлтүүр үонх (Capture Filters)



Зураг 6.9 Дэлгээцийн шүүлтүүр үонх (Display Filters)

- |  |   |
|--|---|
| <i>Шинэ (New)</i>                            | Энэ товчлуур нь шүүлтүүрийн жагсаалтанд шинэ шүүлтүүрийн илэрхийлэл нэмнэ. Шүүлтүүрийн нэр (Filter name), Шүүлтүүрийн тэмдэгт мөр (Filter string) хэсгүүдэд оруулсан байгаа утгууд нь энэхүү шинэ шүүлтүүрийн илэрхийллийг тодорхойлно. |
| <i>Устгах<br/>(Delete)</i>                   | Энэ товчлуур нь баруун хэсэгт байрлах шүүлтүүрүүдээс сонгогдсон байгаа шүүлтүүрийг устгадаг.  |
| <i>Шүүлтүүр<br/>(Filter)</i>                 | Энэ хэсгээс та шүүлтүүрийг сонгох боломжтой. Эдгээрийг сонгосноор тухайн шүүлтүүрийн нэр нь шүүлтүүрийн нэр (Filter name) хэсэгт харин шүүлтүүрийн илэрхийлэл (Filter string) талбарт тус тус харагдана.                                |
| <i>Шүүлтүүрийн<br/>нэр (Filter<br/>name)</i> | Шинээр хадгалах шүүлтүүрийн илэрхийллийн нэрийг оруулах эсвэл сонгогдсон байгаа шүүдтүүрийн нэрийг өөрчлөн засварлахдаа энэ талбарыг ашигладаг.   |
|  | Шүүлтүүрийн нэр нь танд тухайн шүүлтүүрээ танихад тань л хэрэглэгдэх бөгөөд өөр ямар нэгэн газар ашиглагддаггүй. Та олон өөр өөр шүүлтүүрийг нэг ижил нэрээр хадгалсан ч болдог. Гэхдээ энэ нь тийм ч үр ашигтай                        |

байхгүй нь ойлгомжтой юм.

<i>Шүүлтүүрийн тэмдэгт мөр (Filter String)</i>	Одоо идэвхижсан байгаа шүүлтүүрийн илэрхийллийг та энэ хэсгээс өөрчилж болно.
<i>Илэрхийлэл (Expression...)</i>	Зөвхөн дэлгэцийн шүүлтүүр хэсэгт: Энэ товчлуур нь шүүлтүүрийн илэрхийлэл нэмэх үйлдлийг дэмжих цонхыг харуулдаг. Дэлгэрүүлэн уншихыг хүсвэл 6.5. Шүүлтүүрийн илэрхийлэл цонх (Filter Expression dialog box) хэсгийг үзнэ үү.
<i>Хэрэглэх (Apply)</i>	Зөвхөн дэлгэцийн шүүлтүүр хэсэгт: Энэ товчлуур нь дэлгэцэнд байгаа пакетуудад энд идэвхитэй байгаа шүүлтүүрийг идэвхижүүлдэг бөгөөд энэхүү цонхыг хаахгүй дэлгэцэнд харуулсан хэвээр байдаг.
<i>OK</i>	Пакет чагнах процесийн шүүлтүүрийн хувьд тухайн шүүлтүүрийг нэмэх эсвэл засварлах үйлдлийг хийнэ харин дэлгэцийн шүүлтүүрийн хувьд дэлгэцийн шүүлтүүр нэмж хадгалах үйлдэл хийхээс гадна тухайн идэвхитэй байгаа шүүлтүүрийг дэлгэцийн шүүлтүүр болгон идэвхижүүлж энэхүү цонхыг хаадаг.
<i>Цуцлах (Cancel)</i>	Ямар нэгэн өөрчлөлт хийлгүйгээр энэхүү цонхыг хаана. Хадгалаагүй өөрчлөлтүүдийг цуцалдаг.

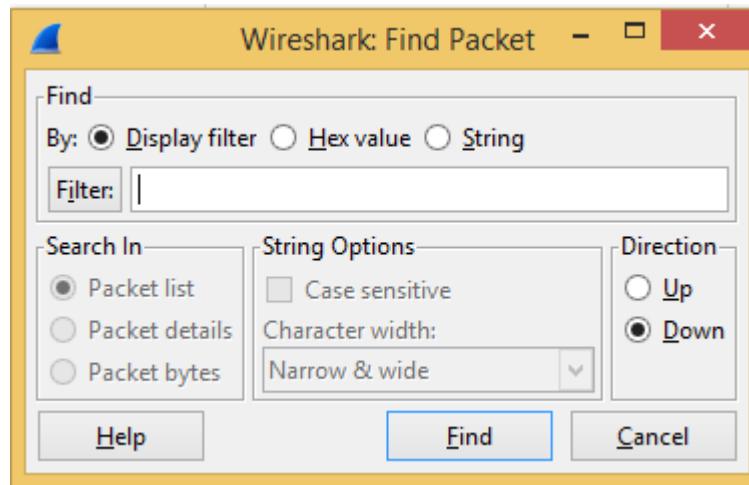
## 6.7. Шүүлтүүрийн макро тодорхойлох, хадгалах (Defining and saving filter macros)

Вайршарк програмыг ашиглан шүүлтүүрийн макро (Filter Macro)-г үүсгэж тэдгээртээ нэр өгч, дараа нь ашиглаж болдог. Ингэснээр дахин бичихэд төвөгтэй урт шүүлтүүрүүдээ хялбархан хэрэглэж, цаг хугацаа хэмнэх боломжийг олгодог.

## 6.8. Пакет хайж олох (Finding packets)

Өмнө нь цуглуулсан файлыг вайршарк дээр нээсэн эсвэл та өөрөө вайршарк програмыг ашиглан пакет цуглуулсан тохиолдолд пакет хайх үйлдэл нь хялбархан юм. Edit → Find Packet хэсгийг сонгож пакет хайх цонхыг гаргаж ирнэ. Дараах зурагт пакет хайх цонхыг үзүүллээ.

### 6.8.1. Пакет хайх цонх (Find Packet)



Зураг 6.10 Пакет хайх цонх (Find Packet)

Та эхлээд хайх төрлөө сонгох хэрэгтэй:

- Дэлгэцийн шүүлтүүр (Display filter)

Энэ хэсгийг сонгосон бол Filter (шүүлтүүр) хэсэгт дэлгэцийн шүүлтүүр хэсэгт хэрэглэдэг тэмдэгт мөрийг оруулаад дараа нь хайх чиглэлээ Up (дээшээ) эсвэл Down (доошоо) хэсгээс сонгож Find товчлуурыг дарна.

Жишээлбэл: 192.168.0.1 хаяг дээрх 3 чиглэлт холболт тогтоох процесс (three way handshake) –г олохыг хүсвэл дараах тэмдэгт мөрийг ашиглана.

```
ip.src==192.168.0.1 and tcp.flags.syn==1
```

Илүү дэлгэрүүлэн судлахыг хүсвэл **6.3. Пакетыг харах үедээ шүүх хэсгийг үзнэ үү.**

- Хекс утга (Hex Value)

Пакетын өгөгдөл байгаа байтуудыг тодорхой дарааллын дагуу хайна.

Жишээлбэл: Пакет дундаас 00:00 гэсэн дараалласан байтыг олохын тулд энэхүү тэмдэгт мөрийг оруулна.

- Тэмдэгт мөр (String)

Пакет дахь тэмдэгт мөрийг төрөл бүрийн сонголттойгоор хайна.

Тэмдэгт мөрийн энэхүү хэсэгт бичих үед вайршарк програм таны тэмдэгт мөр пакетуудад байгаа эсэхийг шалгах ба хэрэв ийм мэдээлэл пакетууд дотор олдвол энэ хэсэг нь ногоон өнгөтэй болно эсрэг тохиолдолд улаан өнгөтэй болно.

Хайх чиглэлээ тодорхойлж өгөх боломжтой.

- *Дээшиээ (Up)*

Пакетыг жагсаан харуулах самбарт байгаа пакетуудаас дээшээ чиглэлд хайна. (Пакетын дугаарыг бууруулна)

- *Доошоо (Down)*

Пакетыг жагсаан харуулах самбарт байгаа пакетуудаас доошоо чиглэлд хайна. (Пакетын дугаарыг ихэсгэнэ)

#### **6.8.2. Дараагийнхийг хайх команд (Find Next)**

Дараагийнхийг хайх (Find Next) команд нь өмнө нь хайсан хайлтын тохиргоогоор үргэлжүүлэлн дараагийн пакетыг хайна.

#### **6.8.3. Өмнөхийг хайх команд (Find Previous)**

Өмнөхийг хайх (Find Previous) команд нь дараагийн пакетыг хайх үйлдэлтэй ижил үйлдлийг түүний эсрэг чиглэлд хийдэг.

### **6.9. Тодорхой нэг пакет дээр очих (Go to a specific packet)**

**Очих (Go)** цэсэн дэх сонголтуудыг ашиглан та тодорхой пакет руу хялбархан үсэрч очих боломжтой.

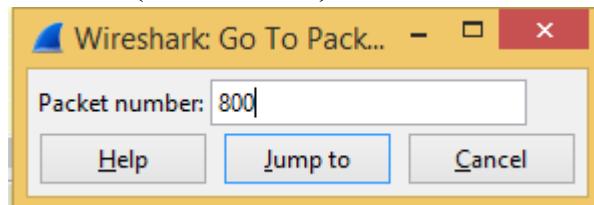
#### **6.9.1. Буцаж очих команд (Go Back)**

Пакетын түүх хэсэгт байгаа өмнөх пакет руу **Буцаж очих (go back)** команд нь веб хөтөчийн түүхийг хадгалдаг хуудас шиг ажилладаг.

#### **6.9.2. Урагшилах команд (Go Forward)**

Пакетын түүх хэсэгт байгаа урагшилах команд нь веб хөтөчийн түүхийг хадгалдаг хуудас шиг ажилладаг.

#### **6.9.3. Пакет руу очих цонх (Go to Packet)**



Зураг 6.11. Пакет руу очих цонх

Энэ цонх нь танд пакетын дугаарыг оруулах замаар тухайн пакет дээр очих боломжийг олгодог.

#### **6.9.4. Харгалзан тохирч буй пакет руу очих комманд (Go to Corresponding Packet)**

Хэрэв өөр пакетын протокол дахь талбартай нь нийцэж байгаа эсвэл тохирч байгаа пакетын протоколыг сонгосон байгаа бол энэ командаар тухайн харгалзах пакет руу нь шууд шилждэг.

Эдгээр протоколын талбариуд нь одоо веб хуудас дээрх холбоос шиг (link) ажилладаг болсон бөгөөд тухайн протоколын талбар дээр хулганыг 2 удаа товшсоноор харгалзах талбар луу нь шилжинэ.

#### **6.9.5. Эхний пакет руу шилжих комманд (Go to First Packet)**

Энэ комманд нь дэлгэцэнд харуулж буй пакетуудын хамгийн эхний пакет руу шилжинэ.

#### **6.9.6. Сүүлийн пакет руу шилжих комманд (Go to Last Packet)**

Энэ комманд нь дэлгэцэнд харуулж буй пакетуудын хамгийн сүүлийн пакет руу шилжинэ.

### **6.10. Пакетыг тэмдэглэх (Marking packets)**

Та пакетыг жагсаан харуулах хэсэгт байгаа пакетуудыг тэмдэглэх боломжтой. Эдгээр тэмдэглэгдсэн пакетууд нь өнгөөр ялгах дүрмээс хамаарахгүйгээр хар суурь өнгөтэй болдог. Пакетыг тэмдэглэснээр их хэмжээний пакет өгөгдөлтэй ажиллаж пакет анализ хийж байгаа үед түүнийгээ эргэж олоход хялбар байдал үүсгэдэг.

Пакетын тэмдэглээ нь хадгалагдаггүй бөгөөд та тухайн пакет файлыг хаах үед пакетын тэмдэглэгээ устан алга болдог.

Пакетыг халгалах, экспорт хийх, хэвлэхдээ тэдгээрийн гаралтыг удирдах үйлдэлдээ пакетыг тэмдэглэх аргыг хэрэглэж болно. 5.9. Пакетын завсар фрэйм хэсгээс дэлгэрүүлэн үзнэ үү.

Пакетын тэмдэглэх төлөвийг удирдах дараах 3 төрлийн фундаменталын байдал.

- *Mark packet (toggle)* – Ганц пакетын төлөвийг тэмдэглэх, тэмдэглэгээг арилгах үйлдэл хийнэ.
- *Mark all displayed packets* - Дэлгэцэнд харуулж буй бүх пакетын багцийг тэмдэглэгдсэн төлөвтэй болгоно.
- *Unmark all packets* – Дэлгэцэнд байгаа бүх пакетын тэмдэглэгээг арилгана.

Эдгээр функцийг **Edit** цэснээс сонгох боломжтой мөн түүнчлэн Пакетыг жагсаан харуулах самбарт гарч ирэх цэснээс *Mark packet (toggle)* хэмээх цэсийг сонгох боломжтой юм.

### **6.11. Пакетыг үл ойшоор (Ignoring packets)**

Пакетыг жагсаан харуулах хэсэгт байгаа пакетуудыг үл ойшоох (*ignore*) боломжтой. Ингэснээр вайршарк програм энэхүү пакетыг пакет файлд байхгүй мэтээр авч үздэг. Үл

оийшоогдсон пакет өнгөөр ялгах дүрмээс үл хамааран цагаан суурь өнгө, саарал үсгийн фонттой байдаг.

Үл оийшоогдсон пакетуудын тэмдэглэгээг хадгалдаггүй бөгөөд үл оийшоогдсон тэмдэглэгээ нь тухайн пакет файлыг хаах үед алга болдог.

Пакетыг үл ойгоох гурван төрлийн функц байдаг:

- *Ignore packet (toggle)* - Ганц пакетыг үл ойшоох тэмдэглэгээг тавих эсвэл энэ тэмдэглээг алга болгох үйлдлийг хийдэг
- *Ignore all displayed packets* – Дэлгэцэнд харуулж буй бүх пакетыг үл оийшоогдсон төлөвт оруулдаг.
- *Un-Ignore all packets* – Үл оийшоогдсон байгаа пакетын төлөвийг буцаана.

Эдгээр сонголтууд нь Edit цэсэнд байрлах ба түүнчлэн пакетыг жагсаан харуулах самбарт гарч ирэх цэсэнд Ignore packet (toggle) функц байрладаг.

### **6.12. Цаг харуулах форман мөн цагийн тэмдэглэгээ (Time display formats and time references)**

Пакетыг чагнаж цуглуулахын зэрэгцээ пакет бүрт цагийн мэдээллийг оруулж өгдөг. Эдгээр цаг хугацааны тамга нь чагнасан пакет файлд хадгалагддаг учраас дараа нь дахин нээх үед харах боломжтой.

Цаг хугацааны тамга, түүнтэй холбоотой мэдээлэл мөн цагийн бүс түүнтэй төстэй мэдээллийг дэлгэрэнгүй үзэхийг хүсвэл 7.4. Цаг хугацааны тамга (Time Stamps ) хэсгийг үзнэ үү.

Цаг хугацааны тамгыг үзүүлэх формат болон цаг хугацааны тамгын нарийвчлалыг View цэсийг ашиглан сонгох боломжтой. **Зураг 3.5-аас** үзнэ үү

Одоогоор вайршарк програмд ашиглах боломжтой цагийн форматууд:

- *Date and Time of Day: 1970-01-01 01:02:03.123456* Пакетыг чагнасан он, сар, өдөр, цаг, минут, секунд
- *Time of Day: 01:02:03.123456* Пакетыг чагнасан өдрийн цаг, минут, секунд
- *Seconds Since Beginning of Capture: 123.123456* Пакет чагнаж эхэлсэн үеэс хойшхи тухайн пакетаас өмнөх цагийн лавлагaa (Time Reference) болж буй пакетаас хойшхий хугацаа (6.12.1 Пакетын цагийн лавлагaa (Packet time referencing))
- *Seconds Since Previous Captured Packet: 1.123456* Өмнөх пакетыг хүлээн авснаас хойшхи хугацаа
- *Seconds Since Previous Displayed Packet: 1.123456* Өмнөх пакетыг дэлгэцэнд харуулснаас хойшхи хугацаа

- *Seconds Since Epoch (1970-01-01): 1234567890.123456* Epoch (UTC гийн 1970 оны 1 сарын 1-ний шөнө дунд) – оос хойшхи хугацаа

Хугацааг ямар нарийвлчлалаар харах боломжтой вэ:

- *Automatic* Ачааллагдсан пакет файлын нарийвчлал хэрэглэгдэнэ.
- *Seconds, Deciseconds, Centiseconds, Milliseconds, Microseconds or Nanoseconds* Цагийн тамгыг эдгээр нарийвлчлалаас тохируулагдан харагдана. Хэрэв бодит боломжит нарийвчлал нь жижигхэн бол тэг хавсаргагддаг. Хэрэв нарийвчлал нь их бол үлдэж буй бутархай хэсгийг гээдэг.

Нарийвлчлалын жишээ: Хэрэв та “Seconds Since Previous Packet” тохиргоотойгоор цагийн тамгыг харж байгаа бол цагийн утга нь 1.123456 утгатай ойролцоо утгатай байх магадлалтай өндөр юм. Энэ нь libpcap файлын тохиргооны “Automatic” тохиргоогоор дэлгэцэнд харагдана (Энэ нь микросекунд). Хэрэв та Seconds тохиргоог хэрэглэвэд та зөвхөн 1-ийг харна харин Nanoseconds тохиргоог хэрэглэвэл 1.123456000 гэсэн утгыг харна.

### **6.12.1. Пакетын цагийн лавлагаа (Packet time referencing)**

Хэрэглэгч пакетыг цагийн лавлагаа болгон тохируулах боломжтой. Цагийн лавлагаа гэдэг нь түүнээс хойшхи пакетуудын цагийг тооцоолоход тухайн пакет эхлэлийн цэг нь болдог гэсэн үг юм. Хэрэв та тодорохой нэг пакетаас харгалзуулан хугацааг нь харахыг хүсвэл энэ тохиргоо нь маш хэрэгтэй тохиргоо юм. Жишээлбэл та шинэ хүсэлт илгээнээс хойшхи хугацааг харахыг хүсч болох юм. Нэг пакет файлд хэд хэдэн пакетыг цагийн лавлагаа болгон тохируулах боломжтой.

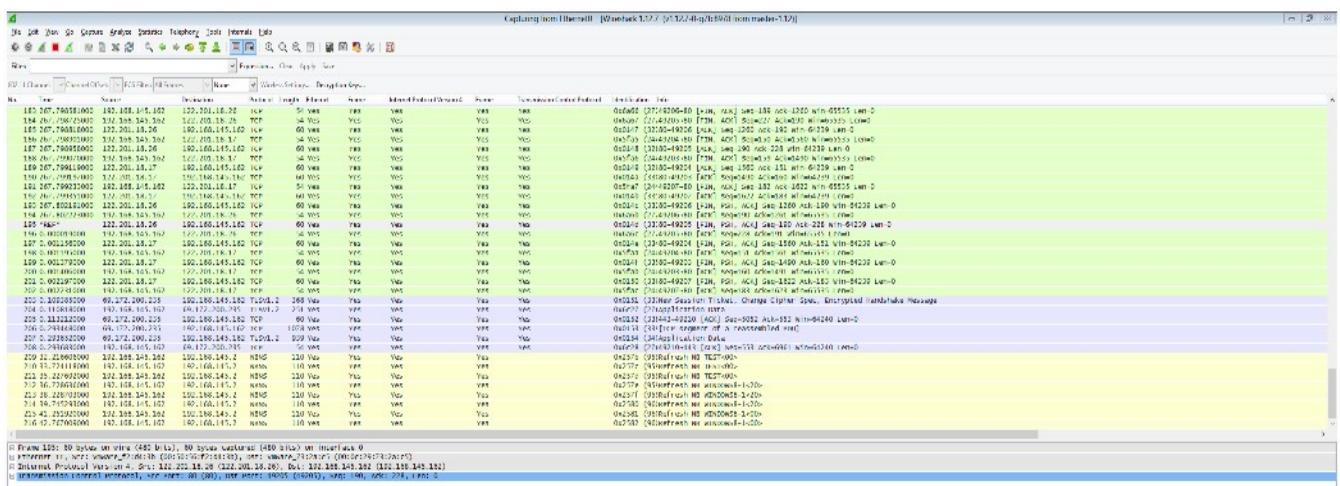
Цагийн лавлагаа нь хадгалагддаггүй бөгөөд пакет файлыг хаах үед устгагддаг.

Цагийн лавлагааг “Seconds Since Beginning of Capture” тохиргоотой хэрэглэх нь хамгийн тохиромжтой юм. Хэрэв та цагийн бүтцийг өөр форматаар харуулах тохиргоог сонгосон бол цагийн лавлагаа тохируулж өгсөн хэдий ч ямар нэгэн нөлөө байхгүй эсвэл ойлгогдохгүй мэдээлэл харуулдаг.

Цагийн лавлагаатай ажиллахын тулд Edit цэсэн дэх Цагийн лавлагааны цэснүүдээс сонгох эсвэл Пакетыг жагсаан харуулах самбарт гарч ирэх цэснээс сонгон хэрэглэж боломжтой.

#### **3.6. Edit цэс хэсгийг үзнэ үү.**

- *Set Time Reference (toggle)* Идэвхижүүлсэн байгаа пакетыг цагийн лавлагаа болгол, тухайн пакетнаас цагийн лавлагааны тохиргоог болиулах үйлдлийг хийнэ.
- *Find Next* Пакетыг жагсаан харуулах самбарт байгаа пакетуудаас цагийн лавлагаа болсон дараагийн пакетыг олно.
- *Find Previous* Пакетыг жагсаан харуулах самбарт байгаа пакетуудаас цагийн лавлагаа болсон өмнөх пакетыг олно.



Зураг 6.12. Вайршарк програм цагийн лавлагаа болсон пакетыг харуулж байна.

Цагийн лавлагаа болсон пакет цаг харуулах багананд \*REF\* тэмдэгт мөрөөр тэмдэглэгдсэн байдаг (195 дугаартай пакетыг харна уу). Түүнээс хойшхи пакетуудын цаг нь цагийн лавлагаанаас хойшхи цагаар харагдаж байна.

**БҮЛЭГ VII**

**АХИСАН ТҮВШНИЙ СЭДЭВ**

## **7.1. Танилцуулга**

Энэ бүлэгт вайршарк програмыг хэрэглэх ахисан түвшний функцүүд, агуулгыг авч үзнэ.

## **7.2. TCP урсгал дагах (Following TCP streams)**

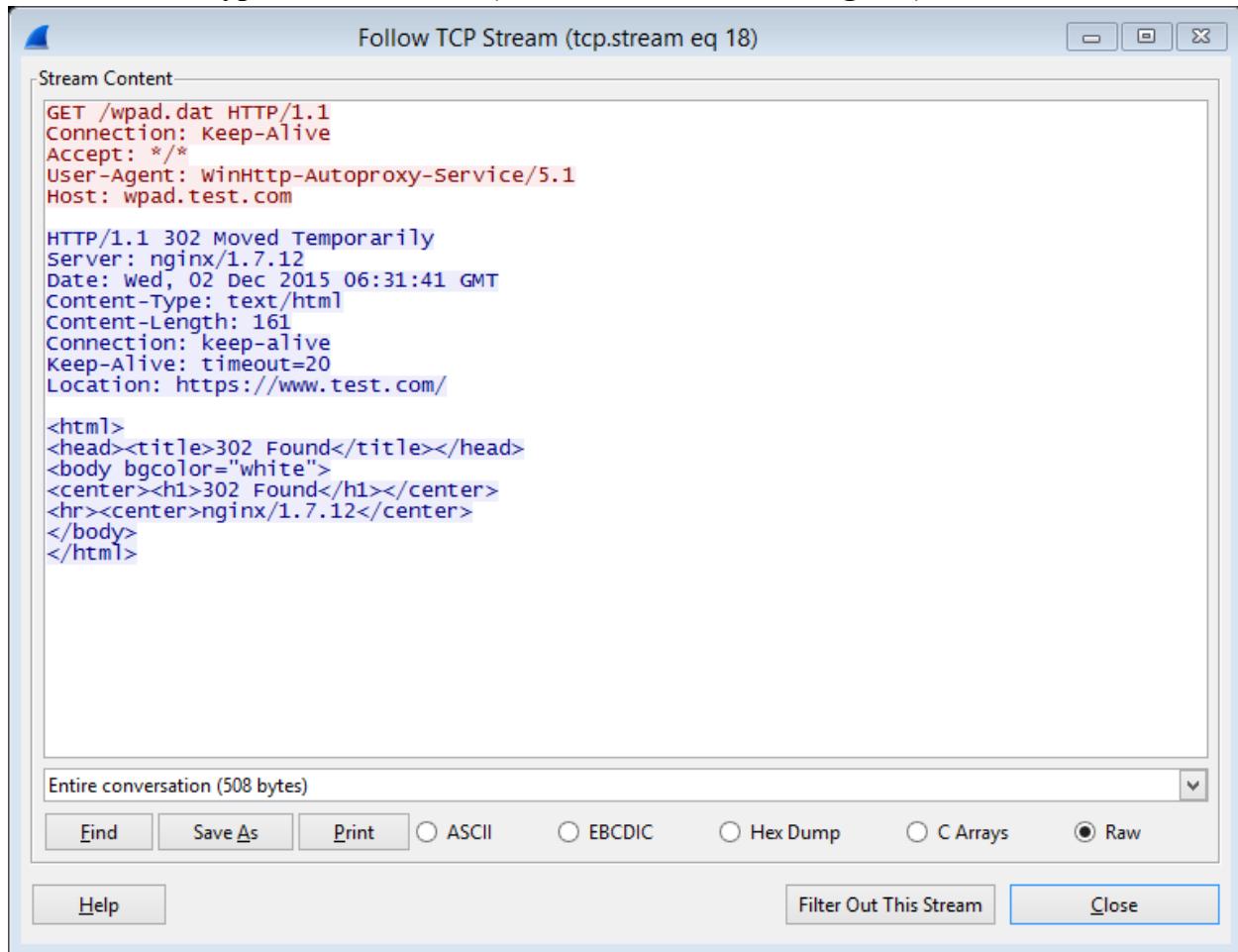
Та TCP дээр суурилсан протоколтой ажиллаж байгаа бол аппликація (application) түвшинд TCP урсгалын өгөгдлийг харах нь маш хэрэгтэй зүйл юм. Магадгүй та Telnet урсгалын нууц үгийг хайж байгаа эсвэл өгөгдлийн урсгалын (data stream) ямар өгөгдөл явж байгааг нь тайлж унших гэж байгаа бол эсвэл TCP урсгалын пакетуудыг дэлгэцийн шүүлтүүрээр оруулан харахыг хүсвэл Вайршарк програмын TCP урсгалыг дагах (Follow TCP stream) функц танд энэ үйлдлийг хийж өгнө.

Өөрийн сонирхож буй урсгалын (холболтын) TCP пакетыг (пакетыг жагсаан харуулах самбарын хэсгээс) сонгоод *Analyze* → *Follow TCP Stream* цэсийг сонгоно. Вайршарк програм дэлгэцийн шүүлтүүрийн хэсэгт тухайн холболтыг шүүн харуулах шүүлтүүрийн илэрхийллийг оруулах бөгөөд бүх өгөгдлийг дарааллан харуулсан цонхыг дэлгэцэнд харуулдаг. Зураг 7.1. –д TCP урсгалыг дагах цонхыг харууллаа.

Тэмдэглэл

TCP урсгал дагах функцийг идэвхижүүлснээр таны сонгосон TCP урсгалын бүх пакетыг дэлгэцэнд ялган харуулах дэлгэцийн шүүлтүүрийн илэрхийллэл идэвхиждэг.

### 7.2.1. TCP урсгал дагах цонх (Follow TCP Stream dialog box)



Зураг 7.1. TCP урсгалыг дагах цонх ("Follow TCP Stream" dialog box)

Урсгалын агуулгад байгаа мэдээлэл нь сүлжээн дээр дамжигдаж байгаа дараалалтайгаа ижил дарааллаар дэлгэцэнд харагддаг. А хэсгээс В рүү чиглэж байгаа траффик улаан өнгөөр харагддаг харин В хэсгээс А руу дамжих байгаа нь цэнхэр өнгөөр харагддаг.

Хэвлэгдэх боломжгүй тэмдэгтүүдийг цэгээр дүрсэлдэг.

Та чагнах процессоо хийж байгаа үед энэхүү цонх автоматаар урсгалын агуулгыг шинэчлэхгүй. Шинээр цуглуулж байгаа пакетын мэдээллийг харахын тулд та энэхүү цонхыг хаагаад нээх хэрэгтэй.

Дараах үйлдлүүдийг энэ цонхыг ашиглан хийх боломжтой.

1. *Save As*: Энэ цонхонд сонгогдсон байгаа форматаар урсгалын өгөгдлийг хадгална.
2. *Print*: Сонгогдсон байгаа форматын дагуу урсгалын мэдээллийг хэвлэнэ.
3. *Direction*: Урсгалын мэдээллийг дэлгэцэнд харуулах чиглэлийг сонгоно. ("Entire conversation", "data from A to B only" эсвэл "data from B to A only").

4. *Filter out this stream:* Дэлгэцэнд ялган харуулсан байгаа пакетуудаас бусад пакетыг дэлгэцэнд харуулах дэлгэцийн шүүлтүүрийг идэвхижүүлнэ. Өөрөөр хэлбэл тухайн холболтыг хасаж бусад бүх пакетыг харах тохиргоо юм.
5. *Close:* Энэ цонхыг хаана. Гэхдээ дэлгэцийн шүүлтүүр хэсэгт байгаа илэрхийлэл тэр хэвээрээ үлддэг.

Өгөгдлийг дараах форматуудаар харах боломжтой:

1. *ASCII:* Энэ сонголтыг идэвхижүүлснээр та 2 талаас ирж буй өгөгдлийг ASCII тэмдэгтээр харна. HTTP гэх мэт ASCII дээр суурисан протоколуудад хамгийн тохиromжтой юм.
2. *EBCDIC:* For the big-iron freaks out there.
3. *HEX Dump:* Энэ хэсэг нь танд бүх өгөгдлийг харах боломжийг олгоно. Дэлгэцнээс маш их зайд шаарддаг бөгөөд бинари протоколтой ашиглагдах нь илүү зохистой байдаг.
4. *C Arrays:* Энэ хэсэг нь ургалын өгөгдлийг өөрийн Си програм руу импорт хийж оруулах боломжийг олгодог.
5. *Raw:* Энэ хэсэг нь үргэлжлүүлэн шалгах шаардлагатай үед танд ургалын мэдээллийг өөрчлөгдөөгүй байдлаар ачааллах боломжийг олгодог. Дэлгэцэнд харгдах хэсэг нь ASCII тохиргоотой ижил байх хэдий ч Save As товчлуурыг дарж хадгалах үед бинари файл (binary file) болгон хадгалдаг.

### **7.3. Эксперт мэдээлэл (Expert Information)**

Эксперт мэдээлэл нь вайршарк пакет файлаас олдсон хэвийн бус мэдээллийн лог мэдээллийн төрөл юм.

Энэ хэсгийн ард байх ерөнхий агуулга нь хэвийн бус (uncommon) эсвэл зүгээр л сүлжээний төлөв байдлыг илүү дээр байдлаар дэлгэцэнд харуулдаг юм. Ийм байдлаар хэрэглэгчид сүлжээнд үүссэн асуудлуудыг гараараа бүх пакетыг шүүж байж илрүүлэхээс хамаагүй хурдан илрүүлэх боломжтой болдог.

Эксперт мэдээлэл нь зөвхөн сануулга дохио юм

Эксперт мэдээлэл (expert info) хэсгийг зөвхөн ороод шалгачихад илүүдэхгүй сануулга мэтээр л ойлгох хэрэгтэй. Жишээлбэл эксперт мэдээлэл байхгүй байх нь бүх зүйл асуудалгүй ажиллаж байгаа гэсэн баталгаа болохгүй юм.

Эксперт мэдээллийн хэмжээ нь хэрэглэж буй протоколоос хамаардаг. TCP/IP гэх мэт нийтлэг хэрэглэгдэг протоколын хувьд эксперт мэдээлэл нь маш дэлгэрэнгүй мэдээллийг өгдөг байхад бусад протоколууд дээр эксперт мэдээлэл байхгүй байх ч магадлалтай юм.

Дараах хэсгүүд нь эхлээд эксперт мэдээлэлд агуулагдах зүйлсийг тайлбарлах бөгөөд дараа нь Хэрэглэгчийн интерфэйсийг (User interface) тайлбарлана

### 7.3.1. Эксперт мэдээллийн талбарууд (Expert Info Entries)

Эксперт мэдээллийн хэсэг нь дараах хүснэгтэд дэлгэрэнгүй үзүүлсэн хэсгүүдийг агуулсан байдаг.

*Хүснэгт 7.1. Эксперт мэдээллийн зарим жисийн*

Packet # (Пакетын дугаар)	Severity (Ноцтой байдал)	Group (Групп)	Protocol (Протокол)	Summary (Хураангуй)
1	Note	Sequence	TCP	Duplicate ACK (#1)
2	Chat	Sequence	TCP	Connection reset (RST)
8	Note	Sequence	TCP	Keep-Alive
9	Warn	Sequence	TCP	Fast retransmission (suspected)

#### 7.3.1.1. Ноцтой байдал (Severity)

Эксперт мэдээлэл бүр ноцтой байдлын түвшинтэй байдаг. Дор ноцтой байдлын түвшингүүдийг үзүүллээ. Хаалтанд байгаа өнгө нь хэрэглэгчид тэмдэглэгдэн харагдах өнгө нь юм.

- Chat (саарал): Энгийн урсгал дамжиж буй мэдээлэл, Жишээлбэл SYN flag нь бүхий TCP пакет
- Note (Цэнхэр ногоон өнгө): Анхаарч харвал зохистой зүйлс, Жишээлбэл Аппликэшн (application) энгийн алдааны код болох HTTP 404 алдааг өгсөн гэх мэт
- Warn (шар): Анхааруулга, Жишээлбэл Аппликэшн (application) хэвийн бус код бүхий алдаа өгсөн. Магадгүй холболтын асуудалтай холбоотой алдаа гэх мэт
- Error (улаан): Ноцтой асуудал жишээлбэл [хэлбэрийн хувьд буруу хэлбэртэй пакет]

#### 7.3.1.2. Групп (Group)

Эксперт мэдээлэлд хэрэглэгддэг нийтлэг хэд хэдэн групп байлаг. Дараах группуудийг одоогоор хэрэглэж байна.

- *Checksum*: checksum мэдээлэл нь хүчин төгөлдөр бус
- *Sequence*: протоколын дараалал сэжигтэй жишээлбэл дараалал нь үргэлжилсэн биш эсвэл дахин дамжуулалт хийсэн гэх мэт
- *Response Code*: Аппликэшн (application) хариу илгээж буй код нь алдаатай. Жишээлбэл HTTP 404 хуудас олдсонгүй хэмээх алдаа
- *Request Code*: ихэвчлэн чатын түвшин (chat level) дэх Аппликэшн хүсэлт (жишээлбэл File Handle == x)
- *Undecoded*: Задлагч хэсэг бүрэн ажиллаагүй эсвэл өгөгдөл нь задлахад ямар нэгэн асуудал үүссэн.

- *Reassemble*: Нэгтгэн угсрах үед алдаа үүссэн. Жишээлбэл угсрах бүх хэсгүүд (fragments) бүрэн биш эсвэл нэгтгэн угсрах үед өөр алдаа үүссэн.
- *Protocol*: Протокол дахь хэсгүүдэд зөрчил илэрсэн (жишээлбэл. Талбарын утга хүчин төгөлдөр биш эсвэл урт нь нь буруу байх)
- *Malformed*: Буруу бүтэцтэй пакет (malformed packets) эсвэл задлагч хэсэг нь алдаатай байх.
- *Debug*: Дебаг (debugging) (release хувилбар дээр энэ групп байдаггүй)

Цаашдаа өөр олон групп нэмэгдэх боломжтой юм.

#### **7.3.1.3. Протокол (Protocol)**

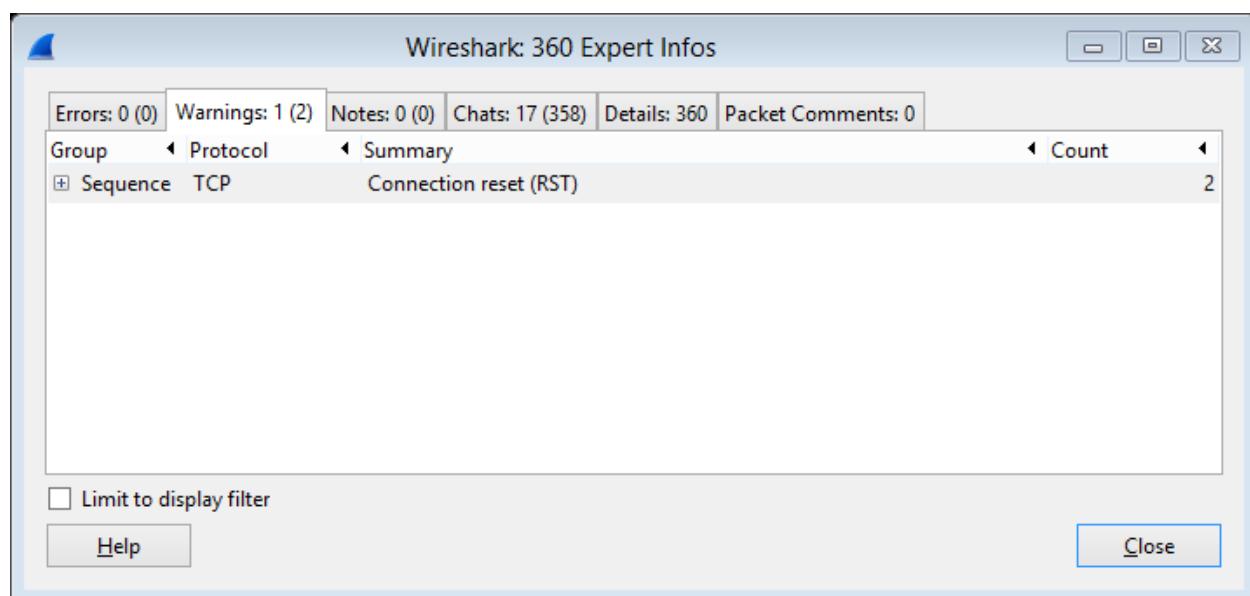
Эксперт мэдээллийг үүсгэсэн протокол

#### **7.3.1.4. Хураангуй (Summary)**

Эксперт мэдээлэл бүрт товчхон тайлбарласан хураангуй хэлбэрийн богино мэдээлэл байдаг.

#### **7.3.2. Эксперт мэдээлэл цонх (Expert Info dialog)**

Эксперт мэдээллийн цонхыг Analyze → Expert Info цэсийг ашиглан нээнэ.



Зураг 7.2. Эксперт мэдээлэл цонх

#### **7.3.2.1. Errors / Warnings / Notes / Chats хэсгүүд (tabs)**

Дэлгэрэнгүй мэдээллийг (Details) харахгүйгээр өөрийн сонирхсон мэдээллийг харахыг үүссэн хүнд Errors/Warnings/Notes/Chats гэсэн ноцтой байдлын түвшингүүдийг сонирхож үзэх юм. Эдгээр хэсгүүд нь тухайн хэсэгт хичнээн талбар байгааг харуулдаг бөгөөд түүнээс гадна эдгээр хэсгүүд (tab)-ийг ашиглан хамгийн чухал гэсэн талбарыг хялбархан олж анализ хийх боломжтой юм.

Яг адилхан Эксперт мэдээлэл бүхий хэд хэдэн өөр пакет байх боломжтой бөгөөд эдгээр адилхан мэдээллийг вайршарк програм ганцхан мөрөнд нэгтгэн харуулах бөгөөд хамгийн баруун талын тоо (count) багананд хэдэн пакетан яг ижилхэн эксперт мэдээлэлтэй байгааг нь итлгэдэг. Эдгээр пакетуудын дугаарыг нь харахын туол зүүн талд байрлах нэмэх (+) тэмдэг дээр дарж задалснаар пакет бүрийн дугаарыг харах боломжтой.

### 7.3.2.2. Details хэсэг (tab)

Энэ хэсэг нь эксперт мэдээллийг лог шиг хэлбэрээр харуулах бөгөөд хэсэг бүрийг нэг мөрөнд харуулдаг (Пакетыг жагсаан харуулах самбартай мөн төстэй). Цуглуулсан пакетын тоо ихсэх үед сонирхсон мэдээллээ хайхад хүндрэл үүсдэг. Харин энэ хэсэг нь тэдгээр талбаруудыг ирсэн дарааллаар нь харуулдаг бөгөөд энэ хэсгийг ашиглан асуудлын учир шалтгааныг олох тохиолдол процессыг хөнгөвчилж болдог.

### 7.3.3. Өнгөөр ялгагдсан протоколын мэдээллийг дэлгэрэнгүй харуулах мод хэлбэрийн бүтэц (Colorized Protocol Details Tree)

```
* Frame 15 (96 bytes on wire, 96 bytes captured)
* Ethernet II, Src: RichardH_00:09:ba (00:80:63:00:09:ba)
  □ Internet Protocol, Src: 192.168.2.6 (192.168.2.6)
    Version: 4
    Header length: 20 bytes
    * Differentiated Services Field: 0x00 (DSCP 0x00)
      Total Length: 82
      Identification: 0x459f (17823)
    * Flags: 0x00
      Fragment offset: 0
    Time to live: 1
    Protocol: UDP (0x11)
    * Header checksum: 0xd0e2 [correct]
      Source: 192.168.2.6 (192.168.2.6)
      Destination: 224.0.0.107 (224.0.0.107)
  * User Datagram Protocol, Src Port: ptp-event (319)
  * Precision Time Protocol (IEEE1588)
```

Зураг 7.3. Өнгөөр ялгагдсан протоколын мэдээллийг дэлгэрэнгүй харуулах хэсэг

Эксперт мэдээллийн хэсэгт ордог протоколын талбарууд өнгөөр ялгагддаг. Жишээлбэл ноцтой байдлын түвшин нь тийм ч ноцтой биш хэсгийг цэнхэр ногоон өнгөөр харуулдаг. Энэ өнгө нь протоколын мэдээллийн мод хэлбэрийн мэдээллийн дээд түвшинд ч гэсэн дамжуулагдан өнгөөр ялгагддаг. Тиймээс эксперт мэдээллийг үүсгэж байгаа тэр хэсгийг олоход хялбархан байдаг.

Дээрх зурганд үзүүлсэнчлэн IP протоколын Time ti live хэсгийн утга нь маш бага (зөвхөн 1) байна, тиймээс түүнтэй харгалзах протоколын хэсэг нь цэнхэр ногоон өнгөөр тэмдэглэгдсэн байна. Энэ хэсгийг хялбархан олох боломжоор хангахын тулд энэ хэсгийг дээд талын түвшин болон IP протоколын хэсэг мөн цэнхэр ногоон өнгөөр ялгагдсан байна.

#### 7.3.4. Пакетыг жагсаан харуулах хэсэгт дэх Эксперт багана (Expert Packet List Column (optional))

Source	Destination	Expert
205.196.219.244	192.168.0.2	
205.196.219.244	192.168.0.2	
192.168.0.2	205.196.219.244	
205.196.219.244	192.168.0.2	
205.196.219.244	192.168.0.2	
192.168.0.2	205.196.219.244	
205.196.219.244	192.168.0.2	
205.196.219.244	192.168.0.2	Warn
192.168.0.2	205.196.219.244	
205.196.219.244	192.168.0.2	
192.168.0.2	205.196.219.244	Note
205.196.219.244	192.168.0.2	
192.168.0.2	205.196.219.244	Note
205.196.219.244	192.168.0.2	
192.168.0.2	205.196.219.244	Note
205.196.219.244	192.168.0.2	Chat
192.168.0.2	205.196.219.244	
192.168.0.2	205.196.219.244	Chat
205.196.219.244	192.168.0.2	Chat
192.168.0.2	205.196.219.244	

Зураг 7.4. Эксперт багана

Эксперт мэдээллийн ноцтой байдлын түвшинг та пакетыг жагсаан харуулах хэсэгт нэмэлт багана байдлаар харах боломжтой. Хэрэв энэ хэсэгт хоосон байвал Вайршарк програм энэ пакетад ямар нэгэн асуудалгүй байна хэмээн үзэж байна гэсэн үг юм. Энэ багана өгөгдмөл тохиргоогоор харагддаггүй бөгөөд та өөрөө нэмж оруулах шаардлагатай. Ингэхийн тулд **10.5. Тохиргоо (Preferences)** хэсэг дэх Багануудын тохиргоо (Preferences Columns) хуудсыг үзнэ үү.

#### 7.4. Цагийн тамга (Time Stamps)

Цагийн тамга, түүний нарийвчлал зэрэг нь нэлээн ээдрээтэй мэт санагдаж болох юм. Энэ хэсэг цагийн тамга тавьж буй процесс хийгдэж буй мэдээллээр таныг хангана.

Пакетыг чагнан цуглуулж байх үед буюу пакетыг орж ирэхэд нь вайршарк програм түүнд цагийн тамгын мэдээллийг тавьж өгдөг. Эдгээр цагийн тамгын мэдээлэл нь пакет файлд хадгалагддаг ба сүүлд дахин нээх үед өмнөх цагийн тохиргоог харах, түүн дээр анализ хийх боломжтой гэсэн үг.

Эдгээр цагийн тамга хаанаас гарч ирээд байна вэ? Чагнаж байх үед вайршарк програм libpcap (winpcap) сангаас цагийн тамгыг хүлээн авдаг. Харин libpcap (winpcap) сан нь энэхүү цагийн мэдээллэ үйлдлийн системийн кернелээс хүлээн авдаг. Хэрэв вайршарк програм өмнө нь хадгалсан байсан файлыг ачааллаж байгаа бол энэхүү цагийн мэдээллийг тухайн файлаасаа хүлээн авдаг.

#### **7.4.1. Вайршарк интернал (Wireshark internals)**

Вайршарк программын цагийн мэдээллийг хадгалж буй потоод форматад он сар өдөр (1970 оны 1 сарын 1 нээс хойши), тухайн өдрийн цаг(шөнө дундаас хойши наносекундээр) гэсэн зүйлс багтдаг. Вайршарк програм цагийн тамгын мэдээллийг хэрхэн дэлгэцэнд харуулахыг тохируулж болдог. Энэхүү тохиргоог хэрхэн хийхийг 3.7. View цэсний Цагийг дэлгэцэнд харуулах формат (Time Display Format) хэсгээс харна уу.

Пакет файл уншихад эсвэл бичихдээ вайршарк програм цагийн тамгын мэдээллийг дотоод форматаас пакет файлын формат руу эсвэл эсрэг байдлаар хөрвүүлдэг.

Чагнах үедээ вайршарк програм миросекундын хөрвүүлэлт дэмждэг libpcap (winpcap) library-г ашигладаг. Хэрэв та тусгай зориулалтын эсвэл илүү мэргэжлийн техник хангамж дээр ажиллаагүй бол энэ хөрвүүлэлт таны шаардлагад хангалттай юм.

#### **7.4.2. Цуглуулсан файлын форматууд (Capture file formats)**

Вайршарк программын ашигладаг цуглуулсан пакет файлын форматууд бүгд цагийн тамгыг дэмжиж ажилладаг. Зарим нэгэн пакет файлын формат “0” секундээс “0.123456789” наносекундээр зөрдөг. Ихэнх пакет файлууд цагийн тамгыг тодорхой тогтмол нарийвчлалаар хадгалдаг (жишээлбэл микросекунд), харин зарим файлын формат нь цагийн тамгын нарийвчлалыг өөрөө сонгон хадгалах боломжтой байдаг

Нийтлэг хэрэглэгддэг libpcap чагнаж, цуглуулсан файлын формат ихэвчлэн хэрэглэгддэг (бусад програмууд ч гэсэн энэ файлын форматыг хэрэглэдэг) бөгөөд энэ файлын формат нь зөвхөн тогтмол урттай микросекундын нарийвчлал дэмжих ба “0.123456”-н хөрвүүлэлт хийдэг.

Өгөгдлийг пакет файл руу бичих нь бодит нарийвчлалыг байнга хадгалж байна гэсэн баталгаа болдоггүй. Жишээлбэл. Хэрэв та наносекунд хөрвүүлэлттэй файлыг libpcap файл руу ачааллавал вайршарк програм таны наносекунд нарийвчлалыг буулгаж микросекунд нарийвчлал болгоно.

### **7.4.3. Нарийвчлал (Accuracy)**

Хүмүүс ихэвчлэн вайршарк програм цагийн тамгыг үзүүлэхдээ ямар нарийвчлалаар үзүүлдэг вэ хэмээн асуудаг. Ер нь бол вайршарк програм ямар нэгэн цагийн тамгыг үүсгэдэггүй бөгөөд эдгээр цагийн тамгуудыг өөр ямар нэгэн газраас хүлээн авдаг бөгөөд тэдгээрийгээ дэлгэцэнд харуулдаг юм. Тиймээс нарийвчлал нь пакетыг чагнаж буй системээс (үйлдлийн систем, гүйцэтгэл гэх мэт) хамаардаг. Тийм учраас дээр дурдсан асуултанд ганц хариулт өгөхөд түвэгтэй болж байгаа юм.

#### **Тэмдэглэл**

USB-гээр холбогдсон сүлжээний карт нь ихэвчлэн маш муу нарийвчлал өгдөг. Яагаад гэвэд USB сүлжээний картаар дамжиж буй мэдээлэл USB кабел дээгүүр дамжаа кернелд хүртлээ урт хугацаа зарцуулдаг. Тиймээс тухайн пакетыг кернелд очиж боловсруулагдан цагийн тамга авч байгаа учраас яг бодит ирсэн цагаасаа нэлээн нарийвчлал муутай цагийн тамга болох магадлалтай байдаг.

Тийм учраас хэрэв танд цагийн нарийвчлал чухал байгаа бол USB сүлжээний NIC карт хэрэглэхгүй байхыг зөвлөж байна.

### **7.5. Цагийн бүс (Time Zones)**

Цагийн бүсээс хамаар таны толгой эргэх магадлалтай юм.

Магадгүй танд цагийн бүсийн талаар мэдэх бүр огтхон ч шаардлагагүй ч байж болох юм.

Жишээлбэл: Та зөвхөн пакетын цагийн ялгааг нь л харахыг хүсч байгаа бөгөөд тухайн пакетын цагийн он сар өдөр нь танд огтхон ч сонин биш байж болно. Эсвэл та цагийн бүс өөрчлөгдөх газар очдоггүй зөвхөн өөрийн цагийн бүсэд л сүлжээний өгөгдөл цуглуулдаг бол цагийн бүсийн талаар санаа зовоод байх зүйл байхгүй юм.

#### **7.5.1. Компьютерийн цагийг зөв тохируулах хэрэгтэй (Set your computer's time correctly)**

Компьютерийнхээ цагийг болон цагийн бүсээ зөв дараалалтайгаар тохируулах хэрэгтэй.

1. Цагийн бүсээ одоо байгаа байрлалтайгаа нийцүүлэн тааруулна.
2. Компьютерийн цагийг өөрийн локал цаг болгон тохируулна.

Ийм байдлаар компьютерийн локал цаг болон UTC оффсет цагийг тохируулдаг.

Интернэтэд байгаа NTP цагийн серверээс синхрон хийх замаар өөрийн компьютерийн цагийг тохируулах боложмтой. NTP клиент програм бүх үйлдлийн систем дээр байдаг. Илүү дэлгэрүүлэн үзэхийг хүсвэл <http://www.ntp.org> хуудас руу хандана уу

#### **7.5.2. Вайршарк програм болон цагийн бүс (Wireshark and Time Zones)**

Вайршарк програмын үндсэн файлын формат (libpcap format) мөн бусад файлын форматууд болох windows sniffer, EtherPeek, AiroPeek, Sun snoop гэх мэт форматууд пакет

ирсэн цагийг UTC утгаар хадгалдаг. Unix болон Windows NT суурьтай системүүд дотоод цаг (time internally)-гаа UTC хэлбэрээр хадгалдаг. Вайршарк програм пакет чагнах процесс хийж байх үед ямар нэгэн хөрвүүлэлт хийх шаардлага байдаггүй. Гэхдээ хэрэв системийн цагийн бүс зөв таараагүй байвал тухайн систем локал цагаа зөв зааж байсан ч хамаагүй байвал системийн UTC цаг буруу байж болно. Чагнах процесс хийгдэх үед пакетыг вайршарк руу илгээхийн өмнө WinPcap цагийг UTC рүү хөрвүүлэх шаардлагатай байдаг. Хэрэв системийн цагийн бүс зөв тохируулагдаагүй байвал хөрвүүлэлт зөв хийгдэггүй.

Microsoft Network Monitor, DOS-based Sniffer, Network Instruments Observer гэх мэт бусад пакет файлын форматууд нь пакетын ирсэн цагийг локал цагийн утгаар хадгалдаг.

Вайршарк програм нь дотор цагийн тамгыг UTC дээр дүрсэлдэг. Энэ нь хэрэв цагийн тамга нь локал дээр хадгалагдсан пакет өгөгдлийг вайршарк програмаар ачааллах хэрэгтэй болвол тухайн локал цагийн мэдээллийг вайршарк UTC утга руу хөрвүүлэх ёстой гэсэн уг юм.

Гэхдээ вайршарк програм цагийн тамгыг дэлгэцэнд харуулахдаа локал цагаар харуулдаг. Цагийн тамгыг харуулж буй компьютер UTC цагаас локал цаг руу хөрвүүлж харуулдаг юм. Пакет файлын ирсэн цагийг нь UTC утгаар хадгалснаар пакет ирсэн цаг таны систем дээр таны локал цагаар харагдах бөгөөд энэхүү харагдаж байгаа цаг нь пакетыг цуглуулсан цагийн бүсийн цаг биш аиж болно. Пакетын цаг нь локал цагаар байгаа хадгалсан пакет файлын хувьд UTC рүү хөрвүүлэх хөрвүүлэлт нь таны цагийн бүсийн UTC оффсет болон DST дүрмийг ашиглан хөрвүүлдэг. Тиймээс хөрвүүлэлт дээр алдаа үүсэх магадлалтай бөгөөд UTC утгаас буцааж локал цаг руу хөрвүүлэхэд мөн алдаа үүсэх магадлал байдаг.

*Хүснэгт 7.2. UTC пакет ирэх цагийн бүсийн жишээ (DST байхгүй)*

	<b>Los Angeles</b>	<b>New York</b>	<b>Madrid</b>	<b>London</b>	<b>Berlin</b>	<b>Tokyo</b>
<b>Capture File (UTC)</b>	10:00	10:00	10:00	10:00	10:00	10:00
<b>Local Offset to UTC</b>	-8	-5	-1	0	+1	+9
<b>Displayed time (Local time)</b>	02:00	05:00	09:00	10:00	11:00	19:00

Жишээлбэл Лос Анжелес хотод байгаа нэг хүн вайршарк програмыг ашиглан яг локал цагаар яг 2 цагт пакет цуглуулсан бөгөөд тэр файлаа тан руу илшээсэн гэж төсөөлье. Пакетын цагийн тамга нь UTC 10 цагаар илэрхийлэгдэнэ. Хэрэв та Берлинд энэ файлыг нээж харвал таны дэлгэцэнд 11 цагийг харуулна.

Ингээд хэрэв та тухайн пакет файлтай холбоотой асуудлаар хүнтэй утсаар ярих эсвэл видео хурал, интернэт уулзалт хийгээд дэлгэц рүүгээ хараад Лос Анжелесд байгаа нь 2 цагийг харах боловч Берлинд байгаа нь 11 цагийг гэсэн үр дүн харна. Ийм байдлаар вайршарк програмын дэлгэц дээр яг ижил цаг хугацаанл тухайн бүсийн локал цагийг нь харуулдаг гэсэн үг юм.

Дүгнэлт: Хэрэв цагийн мэдээлэл тань таны хүлээж буй үр дүнг өгч л байвал танд цагийн талаар санаа зовоод байх шалтгаан байхгүй байж болох юм. Гэхдээ хэрэв та өөр цагийн бүсээс эсвэл DST өөрчөлттэй цагийн зөрүүтэй нөхцөлд пакет файл хүлээн авбал та цагийн бүс болон DST-н зөрүүг олох хэрэгтэй болох бөгөөд цагийн мэдээллээ тохиуулах шаардлагатай болно. Эцэст нь ямар ч тохиолдолд компьютерийн цагийн бүсийн мэдээлэл зөв байгаа эсэхийг шалгаж үзэж байхад илүүдэхгүй юм.

## 7.6. Пакет нэгтгэн угсрах (Packet Reassembly)

### 7.6.1. Пакет нэгтгэн угсрах гэж юу вэ? (What is reassemble)

Сүлжээний протоколоор том хэмжээтэй өгөгдлийг дамжуулах хэрэг гардаг. Жишээлбэл файл дамжуулж байгаа үед тухайн файл дамжуулалтын суурь болж буй үр дүнг өгч туслахад тухайн файлыг тэр чигт бүгдийг нь нэг дор явуулж чадахгүй байх магадлалтай юм. (Жишээлбэл сүлжээний пакетын хэмжээнээс шалтгаалаад) эсвэл бүр TCP Шиг урсгал дээр суурилсан (stream based) протоколууд нь өгөгдлийн хэсэг (data chunk)-г таньдаггүй юм.

Ийм тохиолдолд сүлжээний протокол өөрөө өгөгдлийн хэмжээг удирдах хэрэгтэй болдог ба хэрэв шаардлагатай болвол өгөгдлийг хэд хэдэн пакетад хуваан байрлуулдаг. Ийм тохиолдолд мөн тухайн хуваан илгээсэн өгөгдлийг хүлээн авагч талд ямар байдлаар нэгтгэх вэ гэдгийг тодорхойлох механизм хэрэгтэй болдог.

Энэ механизмыг вайршарк програм нэгтгэн угсрах (reassemble) гэж нэрлэдэг. Гэхдээ тухайлсан протоколын хувьд энэ нэр томьёо өөр байдаг (жишээлбэл Desegmentation, Defragmentation гэх мэт)

### 7.6.2. Вайршарк програм үүнийг хэрхэн зохицуулдаг вэ? (How Wireshark handles it)

Зарим сүлжээний протоколуудын хувьд вайршарк програм хэрхэн тухайн хэсэглэн хуваасан файлуудыг унших вэ гэдгээ мэддэг. Өөрөөр хэлбэл тухайн хэсэглэн хуваахад хэрэглэсэн механизмыг вайршарк програм өөрөө тодорхойлох чадвартай байдаг гэсэн үг юм. Вайршарк програм тухайн хэсэгтэй харгалзах өгөгдлийг олохыг хичээх ба улмаар нэгтгэсэн өгөгдлийг пакетын мэдээллийг байтаар харуулах самбар (Packet Bytes Pane) дэх нэмэлт хуудсанд харуулдаг. (Пакетын мэдээллийг байтаар харуулах самбарын талаар дэлгэрэнгүй мэдээлэл уншихыг хүсвэл 3.20. хэсгийг үзнэ үү)

0000	08	00	06	ab	04	53	08	00	06	6b	7f	bd	08	00	45	00	.....S.. .
0010	01	48	33	c7	00	00	1e	11	dd	51	bc	a8	08	0a	bc	a8	.H3..... .
0020	09	32	41	af	07	04	01	34	00	b4	04	00	2e	00	10	00	.2A.....4 .
0030	00	00	00	00	a0	de	97	6c	d1	11	82	71	00	57	80	f0	.....1 .

Frame (342 bytes) Reassembled DCE/RPC (1604 bytes)

Зураг 7.5. Нэгтгэсэн хэсгийг пакетын мэдээллийг байтаар харуулах самбарт харуулж байна (The “Packet Bytes” pane with a reassembled tab)

Нэгтгэх (reassembly) нь протоколын хэд хэдэн түвшинд хийгдэх боломжтой учраас Пакетын мэдээллийг байтаар харуулах самбарт хэд хэдэн нэмэлт хуудас байх боломжтой юм.

### Тэмдэглэл

Нэгтгэсэн өгөгдлийг та пакетыг хуваасан хэсгүүдийн хамгийн сүүлийн хэсгээс харах боломжтой.

Жишээлбэл: HTTP GET –ийн хариу дотор тухайн хэрэглэгчийн хүссэн өгөгдөл (жишээлбэл HTML хуудас) илгээгддэг. Вайршарк програм нь өгөгдлийн хекс өгөгдлийг (hex dump of data) пакетын мэдээллийг байтаар харуулах самбарт “Uncompressed entity body” гэсэн шинэ хуудсанд харуулдаг.

Нэгтгэх функц нь өгөгдмөл тохиргоогоор идэвхитэй байдаг. Гэхдээ хэрэв хэрэглэгч хүсвэл тухайлсан протоколын хувьд нэгтгэх функцийг нь идэвхигүй болгох боломжтой юм. Ингэхдээ тохиргоо (preferences)-г ашиглаж энэхүү үйлдлийг хийнэ. Протоколын хувьд нэгтгэх функцийг идэвхижүүлэх, идэвхигүй болгохын тулд дараах 2 зүйл хэрэгтэй.

- Доод түвшний протоколууд (жишээлбэл TCP) нэгтгэх (reassembly) үйлдлийг дэмжин ажилладаг байх ёстой. Энэхүү нэгтгэх үйлдлиг нь идэвхижүүлэх, идэвхигүй болгоходоо ихэчвлэн протоколын тохиргоо (protocol preferences) хэсгийг ашигладаг.
- Илүү дээд түвшний протокол (жишээлбэл HTTP) нь хуваагдсан өгөгдлүүдийг нэгтгэх механизм хэрэглэх шаардлагатай байдаг. Гэхдээ энэ механизмыг мөн протоколын тохиргоо (protocol preferences) хэсгийг ашиглан идэвхигүй болгох, идэвхижүүлэх боломжтой.

Дээд түвшний протоколын тохиргооны түүлтип (tooltip) нэгтгэгчийг идэвхижүүлэх эсвэл болих эсэхийг мөн доод түвшний протоколын тохиргооноос алийг нь анхаарч үзэх шаардлагатай вэ гэдгийг танд мэдэгддэг.

## 7.7. Нэрийн хөрвүүлэлт (Name Resolution)

Нэрийн хөрвүүлэлт нь тоон хаягийг хүн унших боломжтой формат руу хөрвүүлэх оролдлого хийдэг. Хөрвүүлэлт хэрхэн хийгдэхээс шалтгаалсан 2 төрлийн хөрвүүлэлтийн арга байдаг. Эхнийх нь систем/сүлжээний сервисийг (gethostname() функц шиг гэсэн үг) дудаах харин дараагийнх нь вайршаркын тусгай тохиргооны файлуудаас хөрвүүлэх юм. Нэрийн хөрвүүлэлт болон түүнтэй төстэй функцэд хэрэглэдэг тохиргооны файлуудын талаар илүү дэлгэрэнгүй мэдээллийг хавсралт В файлууд болон фолдерууд гэсэн хэсгээс үзнэ үү.

Дараах протоколын түвшин (layer) нэрийн хөрвүүлэлтийг дангаар нь идэвхижүүлэх боломжтой.

### 7.7.1. Нэрийн хөрвүүлэлтийн сул тал (Name Resolution drawbacks)

Вайршарк програмтай ажиллаж байх үед нэрийн хөрвүүлэлт хийх нь маш их үнэ цэнийг хэрэглэгчид бий болгодог бөгөөд түүгээр ч зогсохгүй таны ажлын цагийг хэмнэдэг. Гэхдээ харамсалтай нь нэрийн хөрвүүлэлтэд дараах сул талууд байдаг.

- Нэрийн хөрвүүлэлт бүтэлгүй болох тохиолдол байдаг. Нэрийн сервер нь тухайн асуусан нэрийг мэдэхгүй байж болно эсвэл серверүүд нь ажиллахгүй байх тохиолдол байх ба тухайн нэр нь вайршаркын тохиргооны файл дотроос ч олдохгүй байж болно.
- Хөрвүүлэгдсэн нэрс нь пакет файлд эсвэл өөр ямар нэгэн газар хадгалагдаггүй. Тиймээс хөрвүүлсэн нэр нь файлыг хаагаад нээх үед байхгүй болсон байна. Та пакет файлыг вайршарк дээр нээж ачааллах бүрд тань тухайн хөрвүүлэлт бага зэрэг өөр байж болно (яагаад гэвэл өмнө нь холбогдсон сервертэйгээ холбогдоогүй өөр сервер лүү холбогдон тухайн хөрвүүлэлтийг хийсэн байх магадлалтай)
- DNS нь таны пакет файлд пакет нэмэх магадлалтай. Өөрөөр хэлбэл нэрийн хөрвүүлэлт хийж буй пакетууд таны пакет файлд чагнагдах боломжтой.
- Хөрвүүлэгдсэн DNS нэрс нь вайршарк програмын кэш (cache) ойд санагддаг. Гэхдээ энэ нь системээс нөөц шаарддаг. Түүнээс гадна хэрэв вайршарк програм ажиллаж байх үед нэрийн хөрвүүлэлтийн мэдээлэл өөрчлөгдөх хэрэгтэй байгаа бол (жишээлбэл DHCP lease болвол) вайршарк програм энэхүү өөрчлөлтийг мэдэхгүй.

Пакетын жагсаалтанд байгаа нэрийн хөрвүүлэлт нь жагсаалд дүүрэн байгаа үед хийгддэг. Хэрэв пакетыг жагсаалт рүү нэмсний дараа нэрийн хөрвүүлэлтийг хийх боломжтой байвал түүний өмнөх бичилтэд өөрчлөлт орохгүй. Нэрийн хөрвүүлэлт кэш ойд санагдсан байгаа бол та View → Reload-г ашиглан пакетын жагсаалтыг хөрвүүлсэн нэrtэй нь дахин ачааллаж болдог.

### 7.7.2. Этернэт нэрийн хөрвүүлэлт (Ethernet name resolution (MAC layer))

Вайршарк нь Ethernet MAC хаяг (жиш 00:09:5b:01:02:03) –г хөрвүүлэх гэж оролддог.

*ARP name resolution (system service):* Вайршарк програм үйлдлийн системээс Ethernet хаягийг харгалзах IP хаяг руу нь хөрвүүлж өгөхийг хүсдэг (00:09:5b:01:02:03 → 192.168.0.1)

*Ethernet codes (ether file):* Хэрэв ARP хөрвүүлэлт амжилтгүй болвол вайршарк програм Ethernet хаягийг хэрэглэгч өөрөө ether file –г ашиглан олгож өгсөн төхөөрөмжийн нэр лүү хөрвүүлэх оролдлого хийдэг. (00:09:5b:01:02:03 → homerouter)

*Ethernet manufacturer codes (manuf file):* Хэрэв ARP болон ethers 2-н үр дүн амжилтгүй байвал вайршарк програм тухайн хаягийн эхний 3 байтыг үйлдвэрлэгчийн нэрний эхний 3 үсэгний товчлолоор хөрвүүлэх гэж оролддог. Эдгээр нэрсийг IEEE –ээс олгодог. (Жишээлбэл 00:09:5b:01:02:03 → Netgear\_01:02:03)

### 7.7.3. IP нэрийн хөрвүүлэлт (IP name resolution (network layer))

IP хаягийг хөрвүүлэх гэж оролддог. (жиш: 216.239.37.99)

*DNS/concurrent DNS name resolution (system/library service):* Вайршарк програм үйлдлийн системээс (эсвэл concurrent DNS library-aac) IP хаягийг түүнтэй хамаарах хостын нэрээр хөрвүүлэх хүсэлт гаргадаг. (жишээлбэл 216.239.37.99 → [www.1.google.com](http://www.1.google.com)). DNS сервис нь DNS сервер лүү синхрон дуудлага (synchronous calls) хэрэглэдэг. Тиймээс вайршарк програм нь DNS хүсэлтийн хариу иртэл хариу урвал үзүүлдэггүй. Хэрэв боломжтой бол Concurrent DNS library-г хэрэглэх нь зүйтэй юм. Яагаад гэвэл энэ нь серверээс хариу ирэхийг хүлээдэггүй.

#### Анхааруулга

Нэрийн сервер ажиллахгүй байгаа үед вайршарк нэрийн хөрвүүлэлт програмыг маш удаан болгодог. Яагаад гэвэл вайршарк програм нэрийн сервер лүү хүсэлтээ илгээчихээд хүсэлтийн хугацаа дуустал (request time out) хүлээдэг. Concurrent DNS хөрвүүлэлтийг хэрэглэж байх нь зүйтэй.

*DNS vs. concurrent DNS:* Энд жижигхэн харьцуулалтыг харууллаа. Энэ 2 механизм нь хоёулаа IP хаягийг хүн унших боломжтой домэйн нэр лүү хөрвүүлдэг. Энгийн DNS call gethostname() нь хаягийг нэр лүү хөрвүүлэх оролдлого хийнэ. Үүнийг хийхийн тулд эхлээд системээс хост файлд (жишээлбэл /etc/hosts) тохирч буй бичилт байгаа эсэхийг шалгана. Хэрэв энэ процесс амжилтгүй болвол тохиргоон дээр байгаа DNS сервер лүү хүсэлт тухайн IP хаягт харгалзах домэйн нэрийг хүссэн хүсэлт илгээдэг.

Тиймээс DNS болон concurrent DNS-ийн ялгаа нь хүлээх хугацаан дээр гарч байгаа юм. gethostname() system call нь тухайн нэр хөрвүүлэгдтэл эсвэл ямар нэгэн алдаа үүстэл хүлээдэг. Хэрэв DNS сервер хариу өгөх боломжгүй байвал хэдэн секунд хүртэл хугацаагаар хүлээх магадлалтай.

Concurrent DNS сервис нь бага зэрэг өөр байдлаар ажилладаг. Энэ нь DNS серверээс нэрийн хөрвүүлэлтийн хүсэлт илгээж домэйн нэр асуудаг боловч энэ механизм нь хариу ирэхийг нь хүлээдэггүй. Mash бага хугацаанд буцаад вайршарк програм руу ирдэг. Бодит хаягийн талбар нь DNS –ээс хариу иртэл тухайн нэрийг харуулдаггүй. Дээр дурдсанчлан эдгээр утгууд нь кэш ойд ордог бөгөөд эдгээрийг харахын тулд View → Reload-г дарж мэдээллийг шинэчилж харах хэрэгтэй юм.

*hosts name resolution (hosts file):* Хэрэв DNS хөрвүүлэлт амжилтгүй болвол вайршарк програм хэрэглэгчийн бичиж өгсөн hosts файлыг ашиглан тухайн IP хаягийг харгалзах нэр лүү нь хөрвүүлэх оролдлого хийдэг. (жишээлбэл 216.239.37.99 → www.google.com)

#### 7.7.4. TCP/UDP порт нэрийн хөрвүүлэлт (TCP/UDP port name resolution (transport layer))

TCP/UDP портыг хөрвүүлэх оролдлого хийдэг. (жишээлбэл 80)

*TCP/UDP port conversion (system service):* Вайршарк програм үйлдлийн системээс TCP эсвэл UDP портыг түүний олонд танигдсан түгээмэл нэрлүү нь хөрвүүлэх хүсэлт тавьдаг (жишээлбэл 80 → http)

### 7.8. Шалгах нийлбэр (Checksums)

Хэд хэдэн сүлжээний протоколууд шалгах нийлбэр (checksums) ашиглан өгөгдөл бүрэн бүтэн байгааг баталгаажуулдаг. Шалгах нийлбэрийг хэрхэн хэрэглэх талаар энэ хэсэгт дурдлаа. Энэ хэсгийг мөн нэмэлт шалгах (redundancy checking) гэж нэрлэх тохиолдол ч байдаг.

#### Шалгах нийлбэрийг юунд ашиглах вэ?

Шалгах нийлэр нь өгөгдөл дамжуулалт эсвэл хадгалалтын үед тухайн өгөгдлийн бүрэн бүтэн байдлыг хангах зорилгоор хэрэглэгддэг.

Сүлжээний дамжуулалтад алдаа үүсэх тохиолдол цөөнгүй байдаг. Жишээлбэл бит зөрөх, бит дутах, давхардах гэх мэт. Улмаар хүлээн авсан өгөгдөл нь дамжуулсан өгөгдөлтэй ижилхэн биш болдог.

Дамжуулалтын алдаанаас үүдээд эдгээр алдаа үүссэн эсэхийг шалгахын тулд сүлжээний протоколууд шалгах нийлбэрийг ашиглах нь түгээмэл байдаг. Дамжуулж буй тал нь шалгах нийлбэрийг тухайн өгөгдөл дээрээ тооцоолох бөгөөд тухайн өгөгдөлөө шалгах нийлбэртэй нь хамтад нь дамжуулдаг. Хүлээн авч буй тал нь хүлээн авсан өгөгдөл дээрээ дамжуулагч талтай ижилхэн алгоритм ашиглан шалгах нийлбэрийг тооцоолдог. Ингээд хэрэв шалгах нийлбэр нь тохирогчийн байвал алдаа үүссэн байна хэмээн үздэг байна.

Шалгах нийлбэр тооцоолдог зарим алгоритмууд энгийн алдаануудыг хаана алдаа үүссэнээс нь хөөх замаар засах чадвартай байдаг.

## Хэрэв

Алдааг засах боломжгүй байвал хүлээн авагч тал тухайн пакетыг хаядаг. Тухайн өгөгдлийн алдааг шуух үл ойшоох уу эсвэл илгээгч тал руу мэдэгдэж дахин дамжуулах уу гэдэг нь сүлжээний протоколоос хамаардаг.

Шалгах нийлбэр ашиглах нь дамжуулалтын үед үүсч буй илрэхгүй байгаа алдааны тоог маш их хэмжээгээр бууруулдаг. Гэхдээ л шалгах нийлбэрийн алгоритм нь алдаа илрүүлэлтийг 100% баталгаатай хийж чаддаггүй. Mash бага хэмжээний дамжуулалтын алдаа байсаар байдаг.

Хэд хэдэн төрлийн шалгах нийлбэрийн алгоритмууд байдаг. Хамгийн түгээмэл хэрэглэгддэг шалгах нийлбэрийн алгоримт бол CRC32 юм. Шалгах нийлбэрийн алгоритмыг сонгох процесс нь дамжуулалтад хүлээгдэж буй алдааны түвшин, алдаа илрүүлэлт нь хэр чухал эсэх, тооцоолол хийх процессорын гүйцэтгэх, бусад функцэд шаардлагатай гүйцэтгэл, түүний нөөц зэрэгээс хамаардаг.

Дэлгэрүүлэн уншихыг хүсвэл <https://en.wikipedia.org/wiki/checksum> хуудсанд зочилно уу.

### 7.8.1. Вайршарк шалгах нийлбэрийн шалгах (Wireshark checksum validation)

Вайршарк програм IP, TCP, UDP гэх мэт олон протокол дээр шалгах нийлбэрийг бататган шалгадаг.

Энэ нь энгийн хүлээн авагчтай ижил үйлдэл хийдэг. Шалгах нийлбэр (checksum) талбар дахь утгыг пакетын дэлгэрэнгүй мэдээллийн хэсгээс хараад [correct], [invalid, must be 0x12345678] гэсэн тайлбаруудыг хийдэг.

Төрөл бүрийн протокол дээр шалгах нийлбэрийн батагалаажуулалтыг вайршарк протокол тохиргоо (protocol preference) хэсгийг ашиглан унтраах боломжтой (гүйцэтгэлийг маш бага хэмжээгээр нэмэгдүүлэхийн тулд үүнийг хийдэг)

Хэрэв шалгах нийлбэрийн баталгаажуулалт нь нээлттэй тэгээд шалгах нийлбэр нь тохирохгүй байвал пакет нэгтгэх (packet reassembly) гэх мэт үйлдлүүд хийгдэхгүй. Ингэснээр дотоод өгөгдлийн баазыг холболтыг буруу мэдээлэл төөрөгдүүлэхээс сэргийлдэг.

### 7.8.2. Шалгах нийлбэрийг оффлоадинг хийх (Checksum offloading)

Шалгах нийлбэрийг тооцоолох үйлдлийг сүлжээний драйвер, протоколын драйвер эсвэл бүр техник хангамж хийх боломжтой байдаг.

Жишээлбэл: Ethernet дамжуулалтын техник хангамж Ethernet CRC32 шалгах нийлбэрийг тооцоолдог бөгөөд хүлээн авагч талын техник хангамж нь шалгах үйлдлийг нь хийдэг. Хэрэв шалгах нийлбэр буруу байвал вайршарк програм дээр пакет ирэхгүй бөгөөд Ethernet техник хангамж тэндээ пакетыг хаях үйлдэл хийдэг.

Дээд түвшний шалгах нийлбэрүүд нь уламжлалт байдлаар протокол дээр хийгддэг бөгөөд бүрэн болсон пакетыг дараа нь техник хангамж руу өгдөг.

Сүүлийн үеийн сүлжээний техник хангамжууд IP шалгах нийлбэр гэх мэт тооцооллыг хийх чадвартай болсон бөгөөд үүнийг шалгах нийлбэрийг оффлоадинг хийх гэж нэрлэдэг. Сүлжээний драйвер өөрөө шалгах нийлбэрийг тооцоолохгүй хэдий ч энэ хэсэг нь техник хангамжийн талбар луу хоосон (zero or garbage) шалгах нийлбэрийн талбарыг өгдөг

### Тэмдэглэл

Шалгах нийлбэр оффлоадинг нь сүлжээний пакетуудыг түүний шалгах нийлбэр нь бүрэн тооцоологдоогүй байх үед нь вайршарк програм руу өгдөг бөгөөд вайршарк програм хоосон шалгах нийлбэрийн хэсгийг авдаг бөгөөд хэдийгээр эдгээр пакет нь техник хангамжаас гарах үедээ хүчин төгөлдөр шалгах нийлбэрээ агуулж байх боловч вайршарк програм эдгээрийг хүчин төгөлдөр бус хэмээн үздэг.

Шалгах нийлбэр оффлоадинг нь эргэлзээ төрүүлэхээр мөн маш олон [invalid] гэсэн мессэжийг дэлгэцэн дээр гаргаж ирэх ба энэ нь залхмаар санагдаж болох юм. Дээр дурдсанчлан шалгах нийлбэр нь хүчин төгөлдөр бус байх нь пакетуудыг дахин нэгтгэх үйлдлийг хийхгүй байх үндэслэл болдог. Энэ нь пакет өгөгдөл дээр анализ хийх үйлдлийг түвэгтэй болгодог.

Та шалгах нийлбэрийн оффлоадингийн асуудлаас сэргийлэхийн тулд 2 зүйлийг хийх боломжтой.

- Хэрэв сүлжээний драйвер дээр оффлоадинг асаалттай байвал түүнийг унтраах
- Вайршарк тохиргооны (preference) хэсэг дээрээс тодорхой хэд хэдэн протоколын шалгах нийлбэрийг баталгаажуулж буй хэсгийг хаах. Модемийн техник хангамжийн болон үйлдлийн системүүдийн оффлоадингийн тархалт их байгаагаас үүдэн вайршарк програм сүүлийн үеийн хувилбарууд дээрээ өгөгдмөл тохиргоогоороо шалгах нийлбэрийн баталгаажуулалтаа хаадаг болсон байна.

## **БҮЛЭГ VIII**

### **8. СТАТИСТИКУУД**

## 8.1. Танилцуулга

Statistics цэсийг ашиглан та төрөл бүрийн сүлжээний статистикийг харах боломжтой.

Эдгээр статистикууд нь ерөнхий мэдээллээс (цуглуулагдсан пакетын тоо гэх мэт) эхлээд тодорхой протокол (жишээлбэл http хүсэлт болон хариу түүний тоо гэх мэт) руу чиглэсэн статиститыг хүртэл гаргах чадвартай

- Ерөнхий статистик:
  - **(Summary)** Пакет цуглуулсан файлын ерөнхий хураангуй.
  - **Protocol Hierarchy** чагнасан пакетуудын протоколын шаталсан бүтэц
  - **Conversations** Харилцан мэдээлэл солилцсон байдал Жишээлбэл тодорхой IP хаягуудын хоорондын траффик
  - **Endpoints** Төгсгөлийн цэгүүд. жишээлбэл IP хаягууд рүү ирж байгаа болон тухайн хаягаас гарч буй траффик
  - **IO Graphs** Пакетын тоог (эсвэл түүнтэй төстэй өгөгдлийг) цагаас хамааруулан график зурна.
- Протоколын тодорхой статистик:
  - **Service Response Time** Зарим пакетын хүсэлт болон түүний хариу хоёрын хоорондын хугацаа.

### Тэмдэглэл

Протоколын тодорхой статистик нь тухайн протоколынхоо талаар дэлгэрэнгүй мэдлэгтэй байхыг шаарддаг. Хэрэв та протоколоо сайн мэдэхгүй бол статистикиг ойлгоход маш хүндрэлтэй байдал үүснэ.

## 8.2. Товч дүгнэлтийн цонх (The Summary window)

Цуглуулсан байгаа пакет файлын ерөнхий статистик

**Wireshark: Summary**

**File**

Name: C:\Users\user2\AppData\Local\Temp\wireshark\_pcapan\_28831FA1-BE0F-476A-9EFD-D2A302A587AA\_20151204051609\_a03084  
Length: 72378 bytes  
Format: Wireshark/... - pcapng  
Encapsulation: Ethernet

**Time**

First packet: 2015-12-04 05:16:18  
Last packet: 2015-12-04 05:25:30  
Elapsed: 00:09:12

**Capture**

OS: 32-bit Windows 8.1, build 9600  
Capture application: Dumpcap 1.12.7 (v1.12.7-0-g7fc8978 from master-1.)

**Capture file comments**

**Interface**

Interface	Dropped Packets	Capture Filter	Link Layer
\Device\NPF_{28831FA1-BE0F-476A-9EFD-D2A302A587AA}	unknown	none	Ethernet

**Display**

Display filter: none  
Ignored packets: 0 (0.000%)

Traffic	Captured	Displayed	Displayed %	Marked	Marked %
Packets	298	298	100.000%	0	0.000%
Between first and last packet	552.089 sec				
Avg. packets/sec	0.540				
Avg. packet size	209 bytes				
Bytes	62177	62177	100.000%	0	0.000%
Avg. bytes/sec	112.621				
Avg. MBit/sec	0.001				

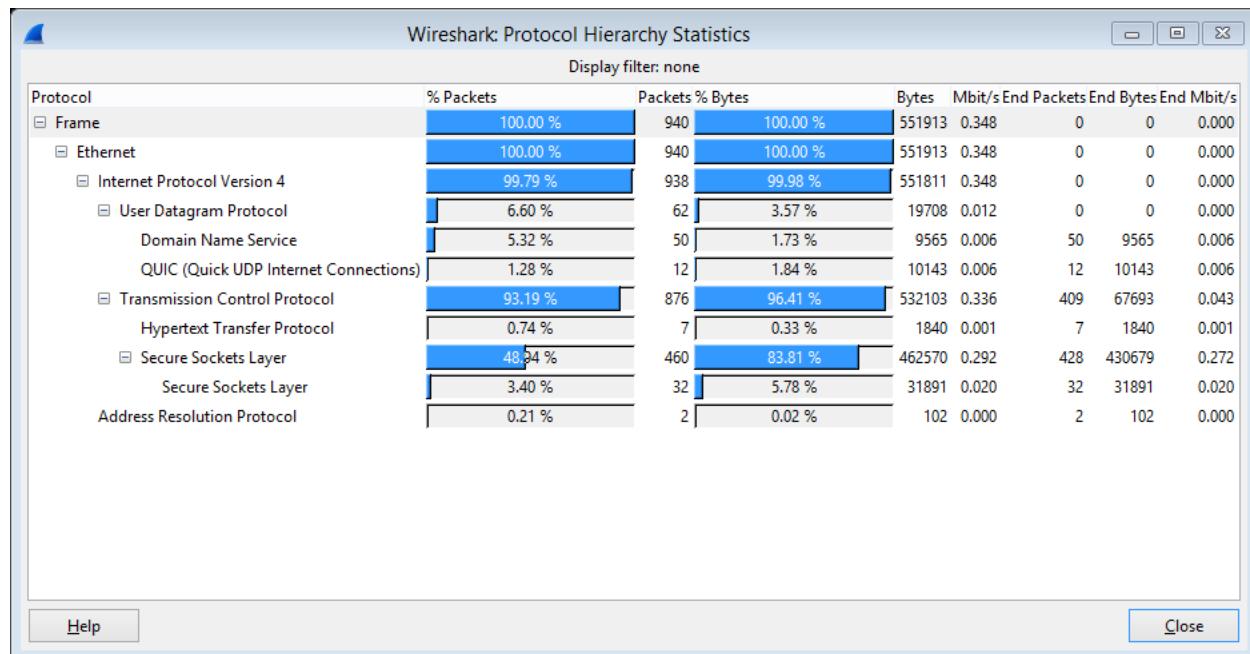
Зураг 8.1. Төвч дүгнэлтийн цонх (Summary)

- *File*: Пакет файлын талаарх өрөнхий мэдээлэл.

- *Time*: Эхний болон сүүлийн пакетын цагийн тамга, мөн энэ хоёр пакетын хооронд өнгөрсөн хугацаа
  - *Capture*: Пакет чагнахдаа ямар үйлдлийн систем дээр ямар програм (application) ашиглан пакет цуглуулсан мөн аль интерфэйс дээр чагнах үйлдэл хийсэн зэрэг мэдээллийг өгнө.
  - *Display*: Пакетуудыг дэлгэцэнд харуулахтай холбоотой зарим мэдээллүүд
  - *Traffic*: Сүлжээний траффикийн статистикийн мэдээллүүд. Харин Marked пакет байгаа бол та Marked багананд тэмдэглэгдсэн пакетуудын утгыг харна. Captured багана дахь утга хэвээр хадгалагдах бөгөөд Displayed багана нь дэлгэцэнд харуулж буй пакетын тооноос хамаарч өөрчлөгддөг бол харин marked багананд байгаа утга нь тэмдэгдсэн пакетын тооноос хамаарч утгаа өөрчилинө.

### 8.3. Протоколын шаталсан бүтэц цонх (Protocol Hierarchy window)

## Цуглуулсан пакетуудын протоколын шаталсан бүтэц



Зураг 8.2. Протоколын шаталсан бүтэц цонх (Protocol Hierarchy)

Энэ нь тухайн пакет файлд байгаа бүх протоколын мод хэлбэрийн бүтэц. Мөр бүр тухайлсан 1 протоколын статистик мэдээллийг агуулдаг. 2 багана нь (Percent Packets болон Percent Bytes) график үзүүлдэг. Хэрэв дэлгэцийн шүүлтүүр байвал дээд хэсэгт нь харагддаг.

### Протоколын шаталсан бүтцийн баганууд (Protocol hierarchy columns)

Protocol

## Протоколын нэр

<i>Percent Packets</i>	Цуглуулсан бүх пакеттай харьцангуй байдлаар тухайн протокол хэр их хувийг эзэлж байгааг харуулна.
<i>Packets</i>	Тухайн протоколын пакетын нийт тоо
<i>Percent Bytes</i>	Цуглуулсан файлын нийт байтад тухайн пакетын хэдэн байтыг нь эзэлж байгааг хувиар харуулна.
<i>Bytes</i>	Тухайн протоколын нийт байтын тоо
<i>Bits/s</i>	Цуглуулсан цагтай харьцангуйгаар тухайн протоколын шугамын өргөний хэмжээ (bandwidth)

Пакетад ихэвчлэн олон протокол агуулагддаг. Тиймээс пакет бүр лээр нэгээс олон протокол тоологдох боломжтой. Жишээлбэл дээрх зурганд үзүүлсэн IP пакетын хувь нь 99 харин TCP нь 93 хувьтай байна (Хэрэв нийлүүлэн тооцвол 100% аас хол давсан утга гарч ирнэ)

Протоколын түвшингүүд нв дээд түвшний протокол агуулаагүй пакетаас бүрдэж болно. Тиймээс дээд түвшний бүх пакетуудын нийлбэр нь нийт пакетын тоотой тэнцэхгүй байх боломжтой юм. Жишээлбэл TCP 93% байгаа хэдий ч түүний дэд протоколууд болох SSL, HTTP зэрэг нь үүнээс бага байна гэсэн үг юм.

Нэг пакетад ижилхэн протоколыг нэгээс олон удаа өөртөө агуулах тохиолдол байж болдог: Энэ тохиолдолд тухайн протоколыг тухайн протокол байгаа хэлбэрээр нь тоолдог. Жишээлбэл ICMP хариу пакет болог туннелийн протоколууд нэгээс олон IP header агуулдаг.

#### **8.4. Харилцан мэдээлэл солилцоо (Conversations)**

Сүлжээний харилцан мэдээлэл солилцоо нь 2 төгсгөлийн цэгийн хооронд дамжигдаж байгаа траффик юм. Жишээлбэл IP харилцан мэдээлэл солилцоо нь 2 IP хаягын хоорогд дамжиж буй траффик байна гэсэн үг. Төгсгөлийн цэгүүд, тэдгээрийн төрөлийн талаарх мэдээлэл **8.5. Төгсгөлийн цэгүүд (endpoints)** хэсэгт бий.

##### **8.4.1. Харилцан мэдээлэл солилцооны цонх (Conversations)" window**

Харилцан мэдээлэл солилцооны цонх нь төгсгөлийн цэгийн цонхтой төстэй. 8.5.1. Төгсгөлийн цэгийн цонх (Endpoints window) хэсгээс нийтлэг функцүүд болон тэдгээрийн тодорхойлолтыг харах боломжтой. Хаягууд, Пакет тоологч, байт тоологч гэх мэт зүйлстэй нийлээд харилцан мэдээлэл солилцооны цонхонд 4 багана нэмэгддэг. Мөн чагнаж эхэлсэн хугацаа болон харилцан мэдээлэл солилцож эхэлсэн хугацааны хооронд өнгөрсөн хугацааг секундээр (“Rel Start”), харилцан мэдээлэл солилцсон хугацааг секундээр, чиглэл бүрт дамжуулагдаж байгаа өгөгдлийг бит/секундээр (байт биш) тус тус харуулдаг.

Conversations: 2 interfaces															
Ethernet: 4	Fibre Channel	FDDI	IPv4: 19	IPv6: 1	IPX	JXTA	NCP	RSVP	SCTP	TCP: 40	Token Ring	UDP: 49	USB	WLAN	
IPv4 Conversations															
Address A	Address B	Packets	Bytes	Packets A→B	Bytes A→B	Packets A←B	Bytes A←B	Packets A→B	Bytes A→B	Rel Start	Duration	bps A→B	bps A←B		
192.168.145.2	192.168.145.162	151	22 492	44	12 126	107	10 366	0.000000000	791.1705	122.61		104.82			
69.172.200.109	192.168.145.162	82	7 857	41	3 156	41	4 701	0.949019000	633.1401	39.88		59.40			
122.201.16.249	192.168.145.162	327	166 340	195	151 633	132	14 707	0.961493000	310.1070	3911.76		379.40			
122.201.16.185	192.168.145.162	173	123 210	116	118 976	57	4 234	0.992053000	299.2691	3180.44		113.18			
192.168.145.162	216.58.216.138	44	8 746	20	1 883	24	6 863	1.029057000	240.9307	62.52		227.88			
192.168.145.162	216.58.216.45	97	47 544	37	7 673	60	39 871	5.268447000	245.5969	249.94		1298.75			
122.201.16.230	192.168.145.162	43	8 859	23	6 156	20	2 703	6.495401000	240.4216	204.84		89.94			
122.201.16.177	192.168.145.162	147	88 130	93	83 135	54	4 995	9.500263000	241.1225	2758.27		165.72			
122.201.16.216	192.168.145.162	365	195 646	225	181 479	140	14 167	10.029064000	591.5420	2454.32		191.59			
122.201.16.165	192.168.145.162	90	54 790	56	51 823	34	2 967	12.686999000	240.4273	1724.36		98.72			
69.172.200.235	192.168.145.162	46	17 604	26	15 396	20	2 208	32.964770000	662.0523	186.04		26.68			
192.168.145.161	204.79.197.200	2	120	0	0	2	120	34.184482000	0.9222	N/A		1040.96			
122.201.18.17	192.168.145.162	8	456	4	240	4	216	47.267573000	0.0182	105639.61		95075.65			
122.201.18.26	192.168.145.162	4	228	2	120	2	108	47.268061000	0.0209	45840.89		41256.80			
122.201.16.212	192.168.145.162	632	552 935	440	515 470	192	37 465	61.207991000	242.1852	17027.30		1237.57			
131.253.14.153	192.168.145.162	13	4 082	7	1 074	6	3 008	274.503062000	0.5677	15134.81		42388.73			
122.201.16.219	192.168.145.162	15	4 482	8	3 812	7	670	361.232205000	70.0960	435.06		76.47			
192.168.145.162	207.204.40.133	15	1 423	9	861	6	562	575.503703000	35.6198	193.38		126.22			
192.168.145.162	207.204.21.133	12	1 006	6	444	6	562	610.997962000	0.6362	5582.84		7066.57			

Зураг 8.3. Харилцан мэдээлэл солилцох цонх (Conversations)

Энэхүү жагсаалт дахь мөр бүр зөвхөн ганцхан харилцан мэдээлэл солилцож байгаатай холбоотой статистикиг харуулдаг.

Хэрэв энэ цонхонд байх *Name resolution*-г идэвхижүүлсэн байвал эсвэл тодорхой протоколын түвшинд нэрийн хөрвүүлэлт идэвхитэй (MAC layer for the selected Ethernet endpoints) байвал нэрийн хөрвүүлэлт хийгдсэн байна. *Limit to display filter* –г идэвхижүүлснээр дэлгэцийн шүүлтүүр хэсэгтэй тохирч буй харилцан мэдээлэл солилцсон хэсгийг л харуулдаг.

Сору товчуур нь эдгээр утгуудыг CSV (Comma Separated Values) эсвэл YAML форматаар санах ой руу (clipboard) хуулдаг. Follow Stream товчуур нь урсгалаар дамжиж буй мэдээллийг 7.1 зурагт үзүүлсэн хэлбэрээр харуулдаг. Graph Товчуур нь графикиг 8.6 хэсэгт дүрсэлсэн хэлбэрээр харуулдаг.

Харилцан мэдээлэл солилцооны төрлүүд нь танд ямар төрлийн траффикиг харах вэ гэдгээ сонгох боломжийг олгодог. 8.5. “Төгсгөлийн цэгүүд” хэсгээс төгсгөлийн цэгийн төрлүүдийг харна уу. Идэвхижүүлсэн төрлүүд нь таны профайл тохиргоонд хадгалагдсан байдаг.

### Зөвлөгөө

Энэ цонх нь тодорхой давтамжтайгаар шинэчлэгддэг учраас энэ цонхыг сүлжээнээс чагнах үйлдэл хийж байхдаа ч гэсэн хэрэглэхэд асуудал үүсдэггүй.

## 8.5. Төгсгөлийн цэгүүд (Endpoints)

Сүлжээний төгсгөлийн цэг нь тодорхой протоколын түвшний траффикин логик төгсгөлийн цэг юм. Вайршарк програмын төгсгөлийн цэгийн статистик нь дараах төгсгөлийн цэгүүдийг тооцож үздэг.

### Зөвлөгөө

Хэрэв та бусад сүлжээний програмууд дээр байдаг hostlist хэмээх функцийг хайж байгаа бол та эрэлээ эндээс олно. Ихэнхдээ List of Ethernet эсвэл IP endpoints нь таны хайж байгаа зүйл байдаг.

### Төгсгөлийн цэгүүдийн төрлүүд мөн харилцан мэдээлэл солилцох төрлүүд

<i>Bluetooth</i>	Ethernet-тэй төстэй 48 бит MAC хаяг
<i>Ethernet</i>	Ethernet төхөөрөмжийн MAC-48 ялгагдах нэр
<i>Fibre Channel</i>	Ethernet-тэй төстэй MAC-48 хаяг
<i>IEEE 802.11</i>	Ethernet-тэй төстэй MAC-48 хаяг
<i>FDDI</i>	FDDI MAC-48 хаягтай ижилхэн
<i>IPv4</i>	32 бит IPv4 хаягтай ижилхэн
<i>IPv6</i>	128 бит IPv6 хаягтай ижилхэн
<i>IPX</i>	32 бит сүлжээний дугаар болон 48 бит node хаягийн нийлбэр. Θгөгдмэл тохиргоогоор Ethernet интерфэйсийн MAC-48 хаяг
<i>JXTA</i>	160 бит SHA-1 URN
<i>NCP</i>	IPX тэй төстэй
<i>RSVP</i>	Төрөл бүрийн RSVP сэши болон IPv4 хаягуудын хослол
<i>SCTP</i>	IP хаягууд болон хэрэглэгдэжбуй SCTP портын хослол. Ижил IP хаяг дээр байгаа өөр SCTP Порт нь өөр төгсгөлийн цэг болно. Гэхдээ өөр IP хаяг дээр байгаа ижил SCTP порт нь ижил төгсгөлийн цэг болдог.
<i>TCP</i>	IP хаяг болон TCP портын хослол. Нэг ижил хаяг дээр байгаа өөр TCP портын дугаар нь өөр өөр TCP төгсгөлийн цэг үүсгэдэг.
<i>Token Ring</i>	Token Ring MAC-48 хаягтай ижилхэн

*UDP*

IP хаяг болон UDP портын хослол. Нэг ижил хаяг дээр байгаа өөр TCP портын дугаар нь өөр өөр UDP төгсгөлийн цэг үүсгэдэг.

*USB*

7 бит USB хаягтай ижилхэн

## Broadcast болон multicast төгсгөлийн цэгүүд

Broadcast болон multicast траффик нь нэмэлт төгсгөлийн цэгээр харагддаг. Мэдээж хэрэг эдгээр нь физик төгсгөлийн цэгүүд биш учраас unicast төгсгөлийн цэгийн жагсаалтанд байгаа төгсгөлийн цэгүүд бодит траффикиг хүлээн авдаг.

### 8.5.1. Төгсгөлийн цэгүүд цонх (Endpoints window)

Энэ цонх нь төгсгөлийн цэгүүдтэй холбоотой статистикиг харуулдаг.

Endpoints: 2 interfaces											
Ethernet: 4	Fibre Channel	FDDI	IPv4: 20	IPv6: 2	IPX	JXTA	NCP	RSVP	SCTP	TCP: 56	Token Ring
IPv4 Endpoints											
Address											
192.168.145.162	2 266	1 305 950	888	113 376	1 378	1 192 574	-	-	-	-	-
192.168.145.2	151	22 492	44	12 126	107	10 366	-	-	-	-	-
69.172.200.109	82	7 857	41	3 156	41	4 701	-	-	-	-	-
122.201.16.249	327	166 340	195	151 633	132	14 707	-	-	-	-	-
122.201.16.185	173	123 210	116	118 976	57	4 234	-	-	-	-	-
216.58.216.138	44	8 746	24	6 863	20	1 883	-	-	-	-	-
216.58.216.45	97	47 544	60	39 871	37	7 673	-	-	-	-	-
122.201.16.230	43	8 859	23	6 156	20	2 703	-	-	-	-	-
122.201.16.177	147	88 130	93	83 135	54	4 995	-	-	-	-	-
122.201.16.216	365	195 646	225	181 479	140	14 167	-	-	-	-	-
122.201.16.165	90	54 790	56	51 823	34	2 967	-	-	-	-	-
69.172.200.235	46	17 604	26	15 396	20	2 208	-	-	-	-	-
204.79.197.200	2	120	2	120	0	0	-	-	-	-	-
122.201.18.17	8	456	4	240	4	216	-	-	-	-	-
122.201.18.26	4	228	2	120	2	108	-	-	-	-	-
122.201.16.212	632	552 935	440	515 470	192	37 465	-	-	-	-	-
131.253.14.153	13	4 082	7	1 074	6	3 008	-	-	-	-	-
122.201.16.219	15	4 482	8	3 812	7	670	-	-	-	-	-
207.204.40.133	15	1 423	6	562	9	861	-	-	-	-	-
207.204.21.133	12	1 006	6	562	6	444	-	-	-	-	-

Зураг 8.4. Төгсгөлийн цэгүүд цонх

Дэмжигдэж буй протокол бүр нь энэ цонхонд харагддаг (tab хэлбэрээр). Тухайн цонх бүр (tab) нь тухайн протоколыг ашиглаж буй төгсгөлийн цэгүүдийн тоог харуулдаг. (Жишээлбэл Ethernet 4 нь 4 ethernet төгсгөлийн цэг байна гэдгийг хэлж өгч байна). Хэрэв тухайн протокол дээр төгсгөлийн цэг байхгүй байвал тухайн цонх саарал өнгөтэй байна. Гэхдээ тухайн цонхыг сонгож харах боломжтой байдаг.

Жагсаалтад байгаа мөр бүр нь тухайлсан нэг төгсгөлийн цэгийн утгатай холбоотой статистикуудыг агуулдаг.

Энэхүү цонхонд нэрийн хөрвүүлэлтийг (*name resolution*) идэвхижүүлсэн тохиолдолд эсвэл нэрийн хөрвүүлэлт нь аль нэг протоколын түвшинд идэвхитэй байвал (MAC layer for the selected Ethernet endpoints page) нэрийн хөрвүүлэлтийг хийдэг. *Limit to display filter* нь дэлгэцийн шүүлтүүрт тохирох харилцан мэдээлэл солилцох хэсгийг л харуулдаг.

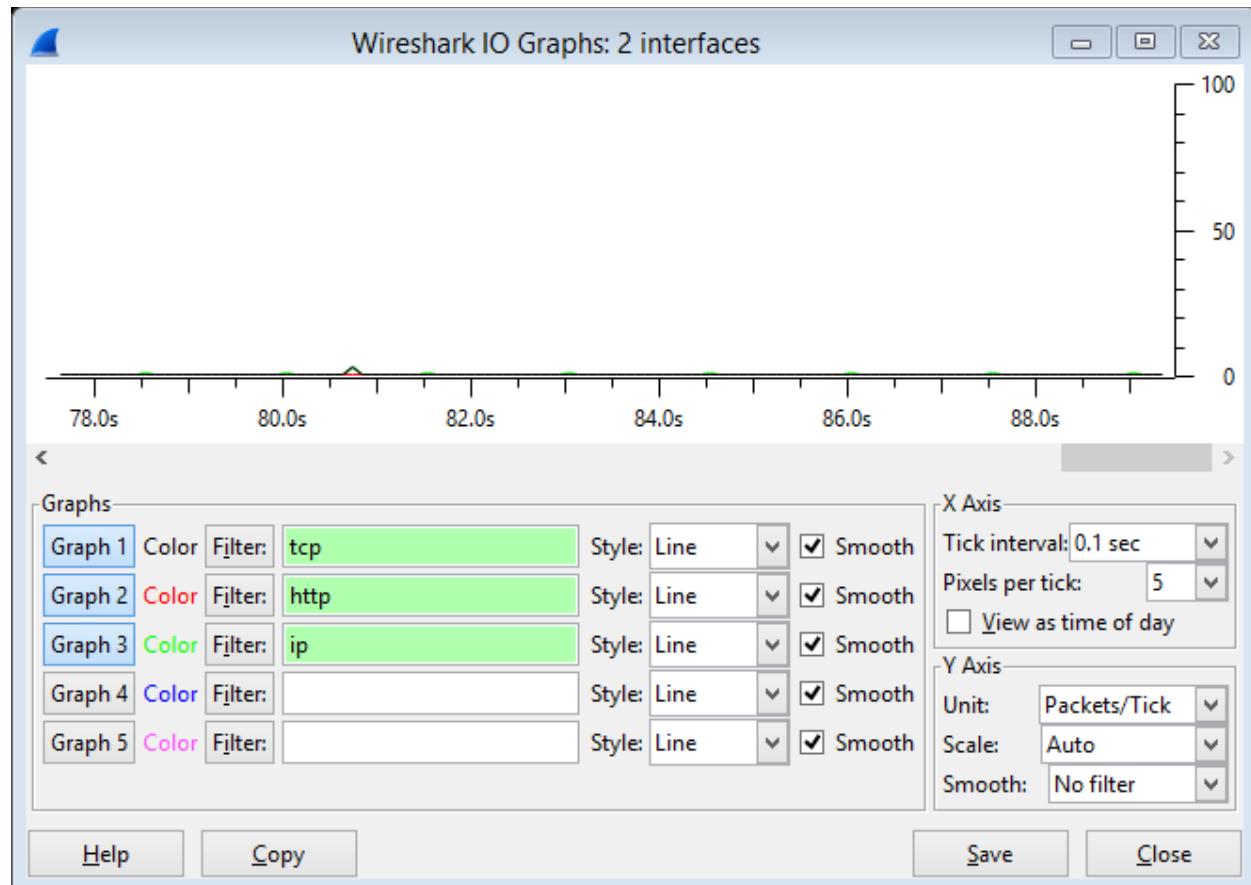
*Copy* товчлуур нь жагсаалтын утгыг санах ой руу (clipboard) CSV (Comma Separated Values) эсвэл YAML форматаар хуулдаг. *Map* товчлуур нь төгсгөлийн цэгүүдийг веб хөтөч дээр зурагласан байдлаар харуулдаг.

Төгсгөлийн цэгийн төрлүүд нь танд ямар траффикин төрлүүдийг цонхонд (tab) харуулах эсэхээ сонгох боломж олгодог. 8.5. “Төгсгөлийн цэгүүд” хэсгээс төгсгөлийн цэгийн төрлүүдийг харна уу. Идэвхижүүлсэн төрлүүд нь таны профайл дээр хадгалагддаг.

## 8.6. IO график цонх (IO Graphs window)

Сүлжээнээс цуглуулсан пакетуудын харуулдаг хэрэглэгч өөрөө тохируулж болдог графикууд.

Та хамгийн ихдээ 5 хүртэлх өөр өнгийн график тодорхойлж өгч болно.



Зураг 8.5. IO график цонх

Хэрэглэгч дараах зүйлсийг тохируулах боломжтой:

- *Graphs*
  - *Graph 1-5*: 1-5 хүртэлх графикуудыг идэвхижүүлдэг (зөвхөн 1 график нь өгөгдмөл тохиргоогоороо идэвхитэй байдаг.)
  - *Color*: Графикин өнгийг заах бөгөөд өөрчилж болдоггүй.
  - *Filter*: Графикт зориулагдсан дэлгэцийн шүүлтүүр (Энэхүү шүүлтүүрт орж буй пакетууд л графикт дүрслэгдэнэ)
  - *Style*: Графикин загвар (Line/Impulse/FBar/Dot)
- X Axis
  - *Tick interval*: х чиглэлд байгаа интервалын утга (10/1 минут эсвэл 10/1/0.1/0.01/0.001 секундээр)
  - *Pixels per tick*: 10/5/2/1 гэсэн пикселийн интервалыг хэрэглэдэг.
  - *View as time of day*: х тэнхлэгийг секунд эсвэл минутаар тэмдэглэхгүй пакет чагнаж эхэлсэн үеэс хойшхий өдөр цагийн тэмдэглэгээгээр тэмдэглэх тохиргоо
- Y Axis
  - *Unit*: у тэнхлэгийн нэгж (Packets/Tick, Bytes/Tick, Bits/Tick,)
  - *Scale*: у нэгжийн шкаал (Logarithmic,Auto,10,20,50,100,200,500,...)

Save товчуур нь дэлгэцэнд байгаа графикиг төрөл бүрийн файлын форматаар хадгалдаг. Сору товчуур нь сонгогдсон байгаа графикиг CSV форматаар санах ой руу хуулдаг (CSV).

#### Зөвлөгөө

Өөрийн сонгосон интервал дахь эхний пакеж (package)-г сонгохын тулд график дээрээ дарна уу.

### 8.7. Сервисийн хариулах цаг (Service Response Time)

Сервисийн хариулах цаг нь хүсэлт болон түүнд харгалзах хариу хоёрын хооронд өгөрч буй цаг юм. Энэ мэдээллийг маш олон протоколын хувьд харуулах боломжтой байдаг.

Дараах протоколууд дээр сервисийн хариу илгээх хүсэлтийн статистик цагийг харуулах боложмтой:

- *DCE-RPC*
- *Fibre Channel*
- *H.225 RAS*
- *LDAP*
- *LTE MAC*
- *MGCP*
- *ONC-RPC*

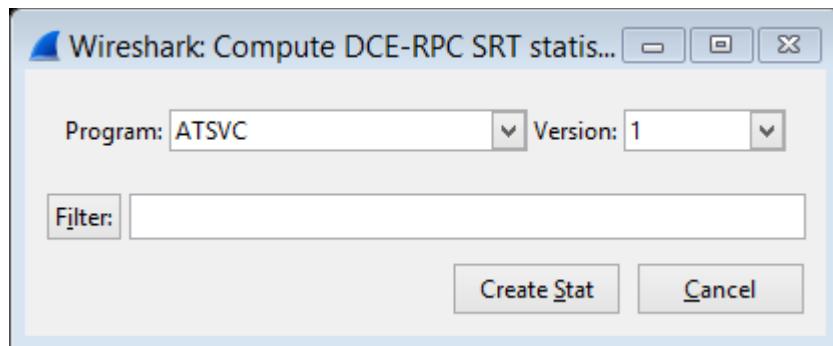
- *SMB*

Жишээлбэл DCE-RPC хүсэлтийн хариу мэдээлэл маш дэлгэрэнгүй дүрслэгддэг.

#### **8.7.1. DCE-RPC сервисийн хариулах цаг цонх (Service Response Time DCE-RPC window)**

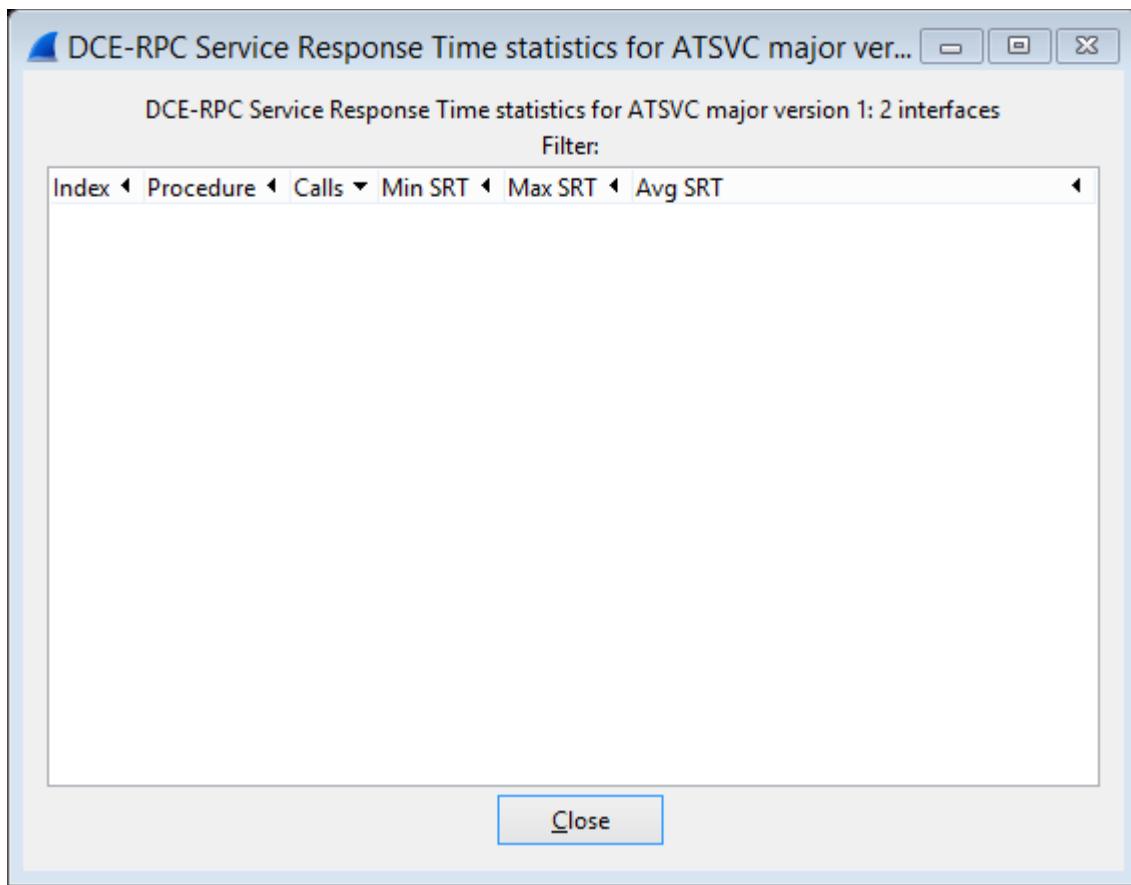
DCE-RPC-гийн сервисийн хариулах цаг гэдэг нь хүсэлт болон түүний хариу хоёрын хоорондын цагийн зөрүү юм

Эхлээд та DCE-RPC интерфэйс сонгох шаардлагатай болдог.



*Зураг 8.6. DCE-RPC тооцоолох статистикийн цонх (Compute DCE-RPC statistics window)*

Пакетын тоог цөөрүүлэх зорилгоор дэлгэцийн шүүлтүүрийг хэрэгжүүлж болно.



*Зураг 8.7. DCE-RPC статистик цонх*

Мэр бүр нь сонгогдсон интерфэйсийн аргатай харгалздаг. Calls хэсгийн аргууд мөн SRT хугацаа тооцоологддог.

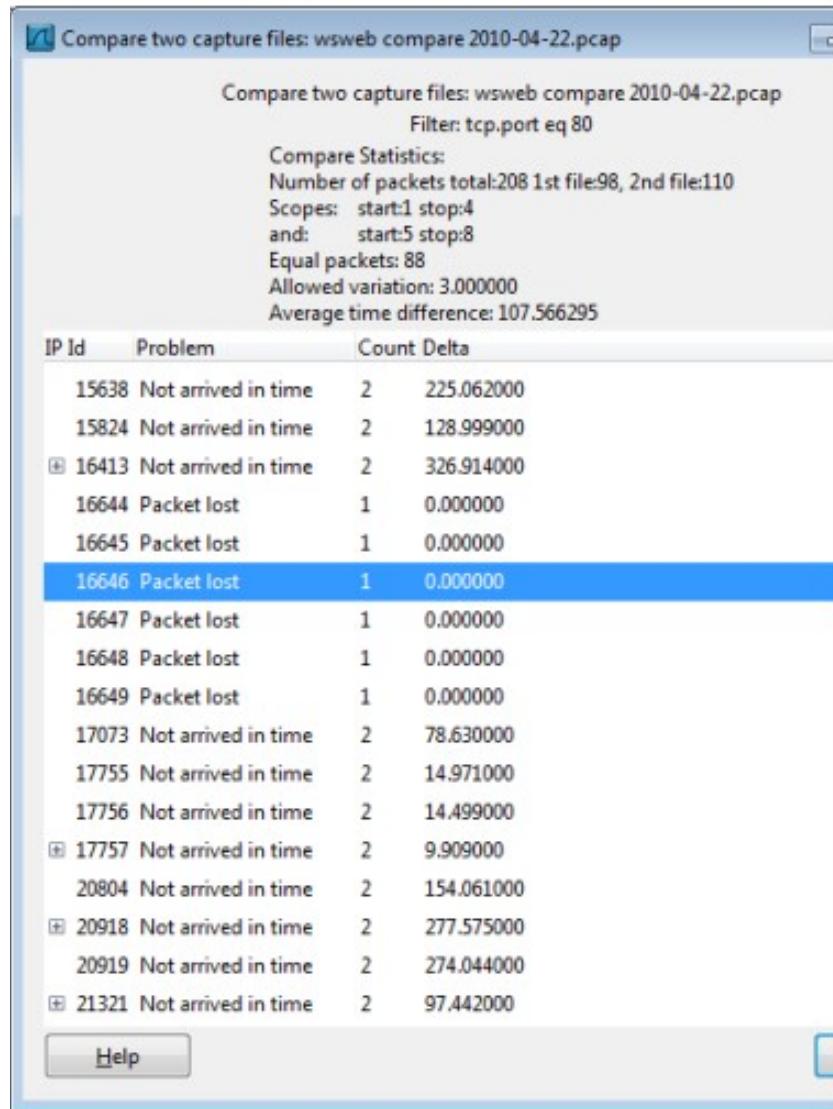
### **8.8.       Хоёр пакет файл харьцуулах**

Цуглусан 2 пакет файлыг харьцуулах

Энэ функц клиент/сервер холболтоос авсан пакет файлуудаа хугацааны дараалтайгаар нэгтгэсэн үед хамгийн сайн ажилладаг.

Нэгтгэгдсэн пакет файлаас пакет дутсан эсэхийг шалгадаг. Хэрэв холболт байгаа нь илэрвэл тухайн пакетуудаас дараах зүйлсийг шалгадаг.

- IP пакетын толгой хэсэг дэх шалгах нийлбэр (IP header checksums)
- Хугацааны хэт их saat (Excessive delay) (Хугацааны хазайлт буюу “Time Variance” тохиргоонд тохируулагддаг)
- Пакетын дараалал (Packet order)



Зураг 8.8. Харьцуулах цонх

Та дараах зүйлсийг тохируулах боложмтой:

- *Харьцуулалтыг эхлүүлэх (Start compare)*: IP ID-нуул нь тохирч байвал харьцуулалтыг эхлүүлдэг. Тэг утга (zero value) харьцуулалтыг нэн дариу эхлүүлдэг.
- *Харьцуулалтыг зогсоох (Stop compare)*: IP ID-нууд тохирохoo болимогц харьцуулалтыг зогсоодог. Тэг утга байнга харьцуулагдана.
- *Төгсгөлийн цэгүүдийн ялгаа (Endpoint distinction)*: Холболтын төгсгөлийн цэгүүдийг тодорхойлохын тулд MAC хаяг эсвэл IP time-to-live утгуудыг хэрэглэдэг. .

- *Дараалал шалгах* (*Check order*): Төгсгөл бүр дээр IP ID мөн тэдний өмнөх IP ID хоорондоо тохирч байгаа эсэхийг шалгадаг.
- *Хугацааны хазайлт* (*Time variance*): Хэрэв пакет дундаж хугацаанаас удаан хугацааны дараа ирвэл алдаа заадаг.
- *Шүүлтүүр* (*Filter*): Харьцуулах пакетуудыг дэлгэцийн шүүлтүүрт тохируулан хязгаарладаг.

Info багана нь шинэ дугаарлалтыг агуулах бөгөөд ингэснээр ижилхэн пакетуудыг параллел байдлаар харуулдаг.

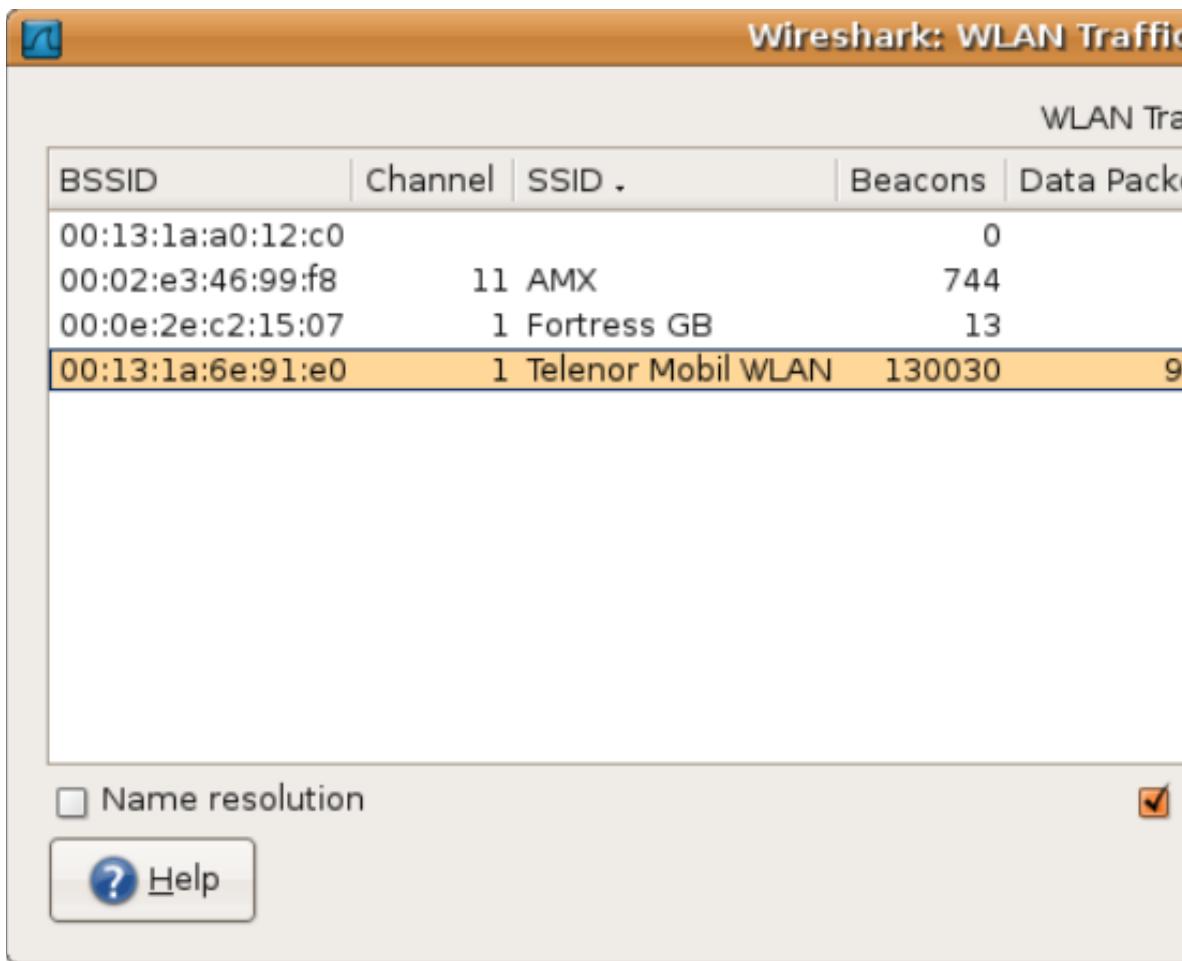
Өнгө шүүлтүүр нь 2 файлыг нэг нэгээс нь ялгадаг. Хэрэв Info багана нь эрэмбэлэгдсэн бол “zebra” нөлөө үүсгэгддэг.

#### Зөвлөмж

Хэрэв та алдааны мэдээллийг жагсаан харуулах хэсэг дээр дарвал үндсэн цонх дээр байх харгалзах пакет руу шилждэг.

#### 8.9. WLAN Трафикийн статистик

WLAN траффикаас чагнасан пакетын статистик. Энэ цонх нь пакет файлаас олдсон бүх утасгүй сүлжээний трафикийг тоймлон дүгнэдэг. Хэрэв SSID тохирч байвал проб хүсэлт (probe requests)-үүд нь одоо байгаа сүлжээ рүү нэгтгэгддэг.



Зураг 8.9. WLAN траффикиг статистик цонх

Мөр бүрт аль нэг утасгүй сүлжээний статистик утгыг харуулдаг.

*Name resolution* хэсгийг сонгосон байвал эсвэл нэрийн хөрвүүлэлтийг MAC түвшинд идэвхижүүлсэн байвал нэрийн хөрвүүлэлт хийгддэг.

*Only show existing networks* хэсэг нь сүлжээг жагсаан харуулах хэсэгтэй тохирогчийг байгаа SSID-тай проб хүсэлтүүдийг хасна.

*Copy* товчлуур нь энэхүү хэсэгт байгаа утгуудыг санах ой руу (clipboard) CSV форматаар хуулдаг.

### Зөвлөмж

Энэ цонх нь богино хугацаанд шинэчлэгдэж байдаг учраас энэ цонхыг нээсний дараа дахин ачааллах шаардлагагүйгээр шинээр ирж буй мэдээлэл харагддаг.

## 8.10. Тодорхой протоколын статистик цонх

Энэ хэсэг нь таны зааж өгсөн протоколын статистикийг дэлгэрэнгүйгээр харуулдаг.

Зарим статистикуудийн талаар <https://wiki.wireshark.org/Statistics> хуудсанд дурдсан бөгөөд энэ хуудаснаас уншина уу.

## **БҮЛЭГ IX**

### **9. УТСАН ХАРИЛЦАА**

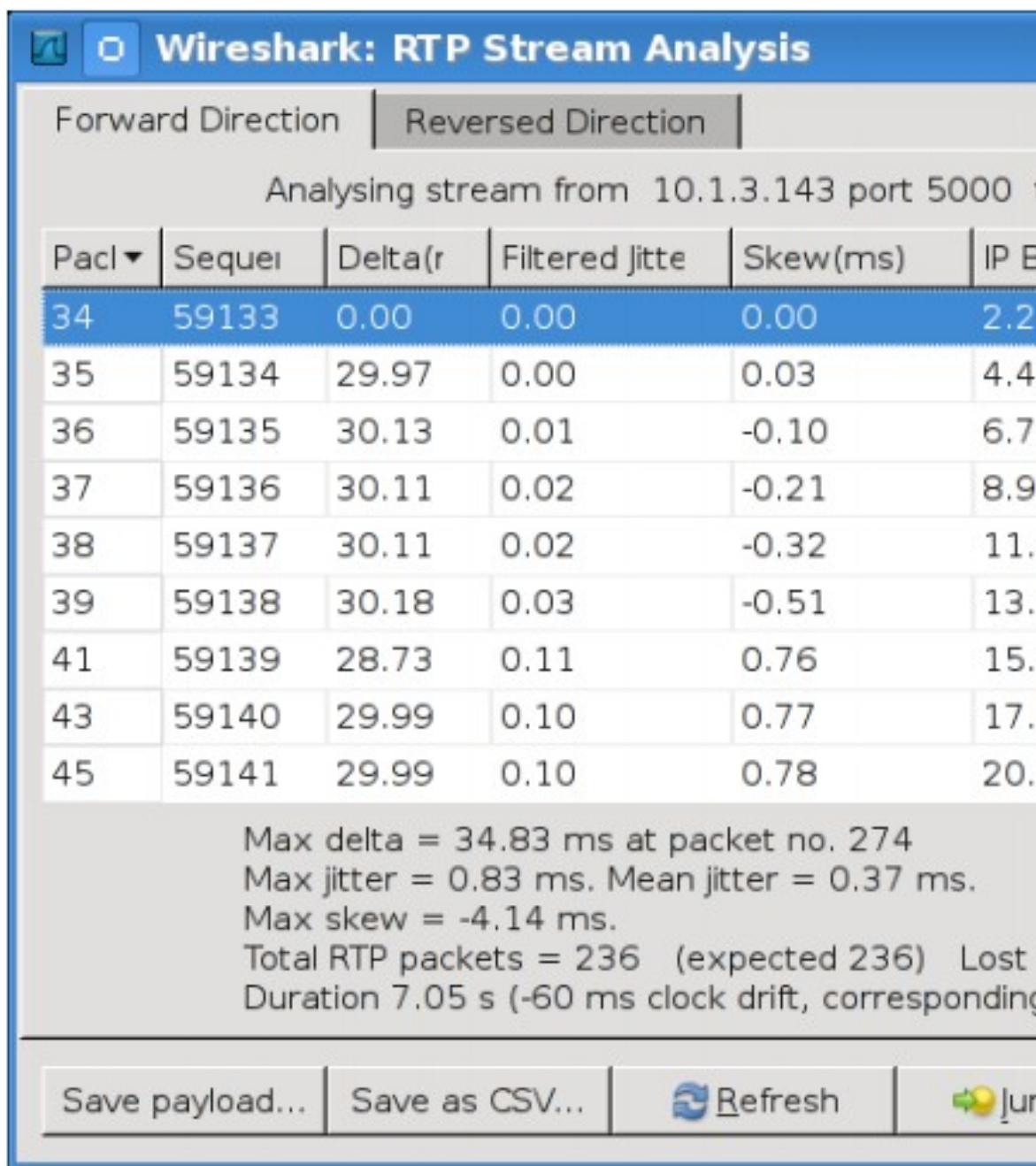
### **9.1. Танилцуулга**

Telephony цэсийг ашиглан та утсан холбоотой хамааралтай сүлжээний статистикуудыг гарган авах боломжтой.

Эдгээр нь сигналийн протоколоос эхлээд, сигнал болон медиа урсгалыг анализ хийх зэрэг хүртэл маш олон статистикийн гаргадаг. Хэрэв медиа урсгалын шифрлэлттэй нийцтэй байдлаар шифрлэгдсэн байвал медиа урсгалыг тоглуулж болдог.

### **9.2. RTP Анализ**

RTP анализ функц нь сонгогдсон RTP урсгал (хэрэв боломжтой бол урсгалыг урвуу болгодог) дээр статистикуудыг үүсгэдэг.



Зураг 9.1. RTP урсгалын анализ цонх

Пакетын дугаар, sequence дугаар цаашлаад ирсэн цаг, хоцрогдол, гажилт (jitter), пакетын хэмжээ гэх мэт статистик мэдээллүүдийг үүсгэдэг.

Пакет бүрийн статикаас гадна доод хэсэгт байрлах хэсэг нь хамгийн бага болон хамгийн их дельта (delta), гажилт (jitter), цагийн гажуудал (skew) гэх мэт нийт статистикийг харуулдаг. Түүнчлэн гээгдсэн пакетуудын мэдээлэл нэгтгэгдсэн байдаг.

RTP урсгалын анализ цонх нь RTP өгөгдлийг хадгалах сонголтыг өгдөг. Ингэхдээ хэрэв RTP өгөгдөл нь PCM encoding мөн Audio файл байвал raw data хэлбэрээр хадгална. Мөн экспорт хийх, мөн RTP урсглын статистикуудыг зурах сонголтууд бас байдаг.

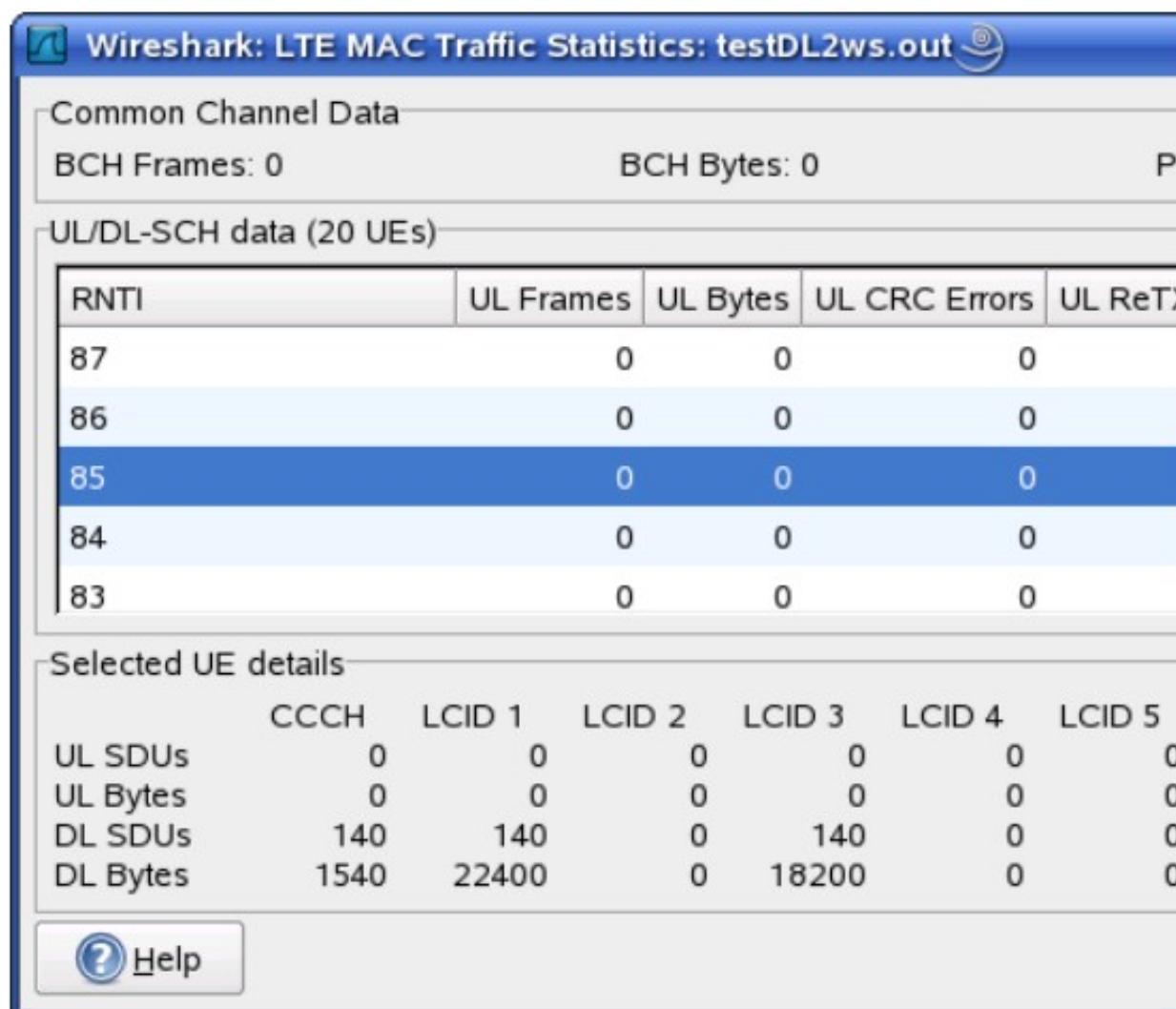
### 9.3. VoIP Дуудлага

VoIP дуудлага цонх нь цуглувсан пакет файл дотроос илэрсэн бүх VoIP дуудлагуудыг харуулдаг. Вайршарк програм эдгээр дуудлагуудыг сигналынх нь тусламжтайгаар ялгаж олдог.

Илүү дэлгэрэнгүй мэдээллийг [https://wiki.wireshark.org/VoIP\\_calls](https://wiki.wireshark.org/VoIP_calls) page хуудаснаас үзнэ үү.

### 9.4. LTE MAC Траффикин статистик

Пакет файл дахь LTE MAC траффикин статистик. Энэ цонх нь пакет файлаас илэрсэн LTE MAC урсгалын тойм мэдээллийг үзүүлдэг.



Зураг 9.2. LTE MAC Траффикин статистик цонх

Энэ цонхны дээд хэсэгт нийтлэг шугамуудын (common channels) статистикиг харуулдаг. Дунд хэсэгт нь яг нэг UE/C-RNTI-гийн статистикиг идэвхижүүлэн, тодотгон харуулдаг. Доод хэсэгт нь та өөрийн сонгосон UE/C-RNTI –г шугам бүрээр нь задлан траффикиг нь харах боломжтой.

#### **9.5. LTE RLC Траффикин статистик**

Энэ цонх нь пакет файлд байгаа LTE RLC траффикиг тоймлон дүгнэж харуулдаг.

Wireshark: LTE RLC Traffic Statistics: test04\_multi\_ue.out (2 UEs, 2)

Show RLC PDUs found inside logged MAC frames

2 UEs

UEId	UL F
1	
2	

Channels of selected UE

	Mode	UL Frames	UL Bytes	UL ACKs	UL NACKs	DL F
CCCH	TM	1	6	0	0	
SRB-1	AM	4	41	2	0	

Filter on selected channel

 Help

Зураг 9.3. LTE RLC траффикин статистик цонх

Дээд хэсэгт байрлах хэрээслэх сонголт нь MAC PDU дотроос илэрсэн RLC PDУ-г энэ цонхонд нэмж оруулах уу эс оруулах уу гэдгийг тодорхойлдог. Энэ нь PDU-н тоо болон үүсгэгдсэн дэлгэцийн шүүлтүүрийн хэсэгт нөлөөлдөг.

Дээд талд нь байрлах мэдээллийг жагсаан харуулах хэсэг нь идэвхитэй байгаа UE бүрийг тоймлон дүгнэдэг. Доод талд байрлах мэдээллийг жагсаан харуулах хэсэг нь тухан сонгогдсон UE доторх шугам бүрийн статистикийн мэдээллийг харуулдаг.

Энэ цонхны доод хэсэг нь дэлгэцийн шүүлтүүр үүсгэх мөн шугам сонгох боломжийг олгодог. Хэрэв Acknowledged Mode channels дээр нэг чигэлтэй байхаар тохируулсан бол үүсгэгдэх шүүлтүүр нь өгөгдлийг тухайн чиглэлд мөн control PDU-г эсрэг чиглэлд харуулдаг болохыг анхаарна уу.

#### **9.6. Тодорхой зааж өгсөн протоколын статистикийн цонх**

Энэ цонх нь таны зааж өгсөн протоколын дэлгэрэнгүй мэдээллийн статистикиг харуулдаг.

Зарим статистикийн мэдээлэл <https://wiki.wireshark.org/Statistics> хаяг дээрх хуудас дээр бичигдсэн байгаа учир энэ хуудас руу зочилно уу.

## **БҮЛЭГ X**

### **10. ВАЙРШАРК ПРОГРАМЫГ ӨӨРТӨӨ ТОХИРУУЛАН ӨӨРЧЛӨХ**

## 10.1. Танилцуулга

Вайршарк програмын өгөгдмөл тохиргоо нь таны хэрэгцээнд нийцэх нь дамжиггүй юм. Гэсэн хэдий ч та вайршарк програмтай ажиллаж сурснаар та энэ программыг өөрийн хэрэгцээнд тохируулан төрөл бүрээр өөрчлөх боломжтой гэдгийг мэдэх гарцаагүй шаардлагатай болно. Энэ бүлэгт дараах агуулгуудыг авч үзнэ:

- Вайршарк програмыг командын мөрний параметрүүдийг ашиглан хэрхэн эхлүүлэх вэ?
  - Пакетыг жагсаан харуулах хэсгийг хэрхэн өнгөөр ялгах вэ?
  - Протокол задлах хэсгийг хэрхэн удирдах вэ?
  - Вайршарк програмын тохиргоог хэрхэн өөрчлөх вэ?.

## **10.2. Вайршарк програмыг команд мөрөөс эхлүүлэх**

Вайршарк програмыг график интерфэйсээс эхлүүж болох хэдий ч мөн командын мөрөөс эхлүүлэх боломжтой байдаг. Энэ хэсэгт командын мөрнөөс хэрхэн вайршаркыг ачааллах, удирдах зэргийг авч үзнэ.

Команд мөрнөөс вайршарк програм руу маш олон параметрийг оруулах боломжтой байдаг. Эдгээр нь чухам ямар параметрүүд болохыг харахыг хүсвэл вайршаркын команд мөрийн хэсэгт `-h` гэсэн үгийг бичих ба энэ нь туслах зориулалт бүхий тайлбарын мэдээллийг дэлгэцэнд хэвдэдэг. Бид дараах жишээгээр энэхүү командын мөрөнд оруулах параметрүүдийн тайлбарыг орууллаа.

Жишээ 10.1. Вайршарк програмын туслах мэдээлэл

Wireshark 1.12.1 (Git Rev Unknown from unknown) Interactively dump and analyze network traffic. See <https://www.wireshark.org> for more information.

Copyright 1998-2014 Gerald Combs <gerald@wireshark.org> and  
contributors. This is free software; see the source for copying  
conditions. There is NO warranty; not even for MERCHANTABILITY or  
FITNESS FOR A PARTICULAR PURPOSE.

Usage: wireshark [options] ... [<infile>]

Capture interface (интерфэйс дээр чагнах үйлдэл хийх):

`-i <interface>` Интерфэйсийн нэр эсвэл `idx` (`def: first non-`

	loopback)
-f <capture filter>	Libpcap шүүлтүүр дэх пакет шүүлтүүрийн хэсэг
-s <snaplen>	Пакетын урт (def: 65535)
-p	Холимог горим (promiscuous) дээр чагнах процесс хийхгүй
-k	Нэн дариу чагнах процесс эхлүүлэх (def: do nothing)
-S	Шинэ пакет ирэх уед дэлгэцэнд байгаа пакет мэдээллүүдийг шинэчлэх
-l	-S -г хэрэлэгж байх уед автоматаар дэлгэц доошоо гуйх тохиргоог идэвхижүүлэх
-I	Чагнах процессыг монитор горимоор ажиллуулах (хэрэв боломжтой бол)
-B <buffer size>	Кернел буфферийн хэмжээ (def: 2MB)
-y <link type>	link layer төрөл (def: first appropriate)
-D	Интерфэйсүүдийг жагсаан хэвлээд гарна
-L	Интерфэйсийн link-layer төрлүүдийг жагсаан хэвлээд гарна

Capture stop conditions (чагнах үйлдлийг зогсоох нөхцөлүүд) :

-c <packet count>	N пакет хүлээн авсаны дараа зогсоох (def: infinite)
-a <autostop cond.> ...	Ургэлжлэх хугацаа:TOO – TOO сек өнгөрсөний дараа зогсоох Файлын хэмжээ:TOO – энэ файлын хэмжээ TOO KB болсон тохиолдолд зогсоох Файлууд:TOO – TOO файл үүссэний дараа зогсоно

Capture output (гаралт) :

-b <ringbuffer opt.> ...	Ургэлжлэх хугацаа:TOO – TOO сек-н өнгөрсний дараа дараагийн файл руу шилжинэ Файлын хэмжээ:TOO – TOO KB болсны дараа дараагийн файл руу шилжинэ
--------------------------	--

Файлнууд: ТОО - ringbuffer: ТОО файл үүссэний дараа эхнээс нь дарж бичнэ

Input file (оролт):

-r <infile> Унших файлын нэрийг зааж өгнө (no pipes or stdin)

Processing (боловсруулалт):

-R <read filter> Вайршарк програмын дэлгэцийн шүүлтүүр дэх пакет шүүлтүүр

-n Бүх нэрийн хөрвүүлэлтүүдийг идэвхигүй болгох (def: all enabled)

-N <name resolve flags> Тодорхой нэрийн хөрвүүлэлтүүдийг идэвхижүүлэх: "mnNtCd"

--disable-protocol <proto\_name> proto\_name -ийн задаргаа идэвхигүй болгох  
Протокол бүр дээр сонголтыг давтах

--enable-heuristic <short\_name> Хьюристик протоколыг задаргаа идэвхижүүлэх  
Протокол бүр дээр сонголтыг давтах

--disable-heuristic <short\_name> Хьюристик протоколыг задаргаа идэвхигүй болгох

Протокол бүр дээр сонголтыг давтах

User interface:

-C <config profile> Тохируулж өгсөн профайл тохиргоотой эхлүүлэх

-Y <display filter> Өгөгдсөн дэлгэцийн шүүлтүүртэйгээр эхлүүлэх

-g <packet number> "-r" -ын дараа тодорхой дугаар дээрх пакет руу очих

-J <jump filter> Дэлгэцийн шүүлтүүртэй тохирч буй эхний пакет руу очих

-j "-J" -ын дараа тохирч буй пакетуудыг урвуу чиглэлтэй хайх

-m <font> Текстэд ашиглагдах фонтын нэр тохируулах

-t a|ad|d|dd|e|r|u|ud Цагийн тамгын формат (def: r: rel. to first)

-u s hms	Секундын гаралтын формат (def: s: seconds)
-X <key>:<value>	Өргөлийн (eXtentions) сонголтууд <b>man</b> хуудаснаас дэлгэрэнгүй мэдээллийг нь үзнэ үү
-z <statistics>	Төрөл бүрийн статистикийн мэдээллүүдийг харуулна. <b>man</b> хуудаснаас дэлгэрэнгүй мэдээллийг нь үзнэ үү
Output (гаралт) :	
-w <outfile ->	Гаралтын файлын нэр (эсвэл '-' for stdout)
Miscellaneous (бусад) :	
-h	Энэ хэсэгт байгаа туслах зориулалт бүхий мэтээддийг хэвлэнэ тэгээд гарна
-v	Хувилбарын талаарх мэдээллийг хэвлээд гарна
-P <key>:<path>	persconf:path -хувийн тохиргооны файлууд persdata:path - хувийн өгөгдлийн файлууд
-o <name>:<value> ...	Toхиргоог дарж бичих
-K <keytab>	Керberosийн задлах үйлдэлд хэрэглэх keytab файл
--display=DISPLAY	Хэрэглэх X дэлгэц

Командын мөрөөс өгч буй сонголтуудыг задалж авч үзье.

Хамгийн эхэнд анхаарал зүйл нь wireshark гэсэн командаар вайршарк програмыг дууддаг. Вайршарк програмыг ийнхүү дуудан ажиллуулахдаа та хэдэн ч параметрүүдийг өгөх боломжой. Параметрүүдийн тайлбарууд (цагаан толгойн дарааллаар):

-a <capture autostop condition>	Чагнаж буй пакетуудыг цуглуулж буй пакет файл руу бичих процессийг зогсоо шалгуурууд.
duration:value	Үргэлжлэх хугацаа: утга Энд зааж өгсөн утга бүхий секунд өнгөрсөний дараа пакет файл руу бичилт хийхийг зогсоодог.
filesize:value	Файлын хэмжээ: утга Файлын хэмжээ нь энд зааж өгсөн утга бүхий файлын хэмжээ (KB) хүрэхэд файл руу бичих үйлдлийг зогсоодог.

Хэрэв энэ сонголт нь **-b** сонголттой хамт хэрэглэгдвэл вайршарк програм тухайн файлыг хааж дараагийн файл руу шилждэг.

Файлууд: утга

files:value

Энд зааж өгсөн утга бүхий файлууд бичигдсэн тохиолдолд пакет файл руу бичилт хийхээ зогсоодог.

**-b <capture ring buffer option>** Пакет файлын хэмжээ хамгийн ихдээ ямар хэмжээтэй байхыг зааж өгсөн бол энэ параметр вайршарк програмыг “ring buffer” горим руу оруулдаг. Энэ горимд вайршарк хэд хэдэн файл руу бичилт хийдэг. Файлуудын нэрс файлын дугаар болон тухайн файлыг үүсгэсэн он сар өдөр дээр суурилдаг.

Хамгийн анхны пакет файлын хэмжээ дүүрэх үед вайршарк програм дараагийн файл руу шилжин орж бичиж эхэлдэг бөгөөд энэ зарчмаар ажилладаг. <command>файлууд</ command> сонголоор мөн “ring buffer” үүсгэх боломжтой байдаг. Энэ тохиргоо нь тодорхой тооны файлуудыг шинэ файлаар дүүргэх ба энэхүү тоо нь гүйцсэн үед эхнээс нь өмнөх бичсэн файлуудаа дарж шинэ файлуудаа бичдэг.

Хэрэв <command>үргэлжлэх хугацаа</command> сонголтыг хийвэл вайршарк програм тодорхой тооны секунд өнгөрвөл дараагийн файл руу шилжих ба файлуудыг дүүргэх гэж оролддоггүй.

Үргэлжлэх хугацаа </command>: Тухайн файл дүүрсэн эсэхээс нь үл хамааран тодорхой хугацаа өнгөрөх үед дараагийн файл руу шилжинэ.  
утга  
duration</command>:value

Файлын хэмжээ </command>: утга  
filesize</command>:value

Файлын хэмжээ нь тодорхой KB болох үед дараагийн файл руу шилждэг.

Файлууд </command>: утга  
files</command>:value

Бүх файлуудад бичилт хийгээд дууссан тохиолдолд эхний файлаасаа дахин эхлээд

бичих үйлдлийг хийнэ.  
(ring buffer үүсгэж байна)

- B <capture buffer size>** Чагнах үйлдлийн буфферийн хэмжээг тодорхойлж өгөх. (Өгөгдмөлөөрөө 1 МВ байдаг). Үүнийг чагнах үйлдлийн драйвер буфферлэгдсэн пакет өрөгдөл ашиглагддаг. Хэрэв танд пакетын алдагдал мэдэгдвэл энэ хэмжээг нэмэгдүүлж үзэх хэрэгтэй. Зарим платформ дээр хэрэгжих боломжгүй.
- c <capture packet count>** Энэ сонголт нь пакет чагнан файл руу буулгаж байх үед хэдэн пакет цагнах тоог зааж өгдөг. Энэ тохиргоо нь -k тохиргоотой холбоотой байдаг.
- D** Вайршарк програм чагнах боломжтой интерфэйсүүдийг хэвлэх ба дараа нь вайршарк програмаас гарна. Интерфэйс бүр дээр интерфэйсийн дугаар мөн нэр магадгүй текст хэлбэрийн тодорхойлолт ч хэвлэгддэг. -i флаг ашиглан араас нь интерфэйсийн нэр эсвэл дугаарыг зааж өгснөөр тухайн интерфэйсийг чагнадаг.
- Энэ нь интерфэйсийн листээ үүсгэдэггүй системүүдэд маш хэрэгтэй байдаг. (Жишээлбэл ifconfig -a команд байхгүй системүүд). Интерфэйсийн нэр нь GUID байгаа Виндовс систем дээр интерфэйсийн дугаар ашиглахад таатай байдаг.
- Энэ параметр нь вайршарк програм чагнах боломжтой интерфэйсүүдийг л харуулдаг. Хэрэв таны ажиллаж буй платформ дээр пакет чагнахын тулд тусгай өөр хэрэглэгчийн эрх шаарддаг (жиш: root) бөгөөд таны одоо байгаа хэрэглэгчийн эрх чинь энэ эрхтэй бич бол -D танд ямар ч интерфэйс харуулахгүй.
- f <capture filter>** Пакет чагнахад хэрэглэгдэх пакетын шүүлтүүрийг тохируулна.
- g <packet number>** -r флаг ашиглан пакет файл ачааллаж уншсаны дараа тодорхой дугаар дээр байгаа пакет дээр очих үйлдлийг хийнэ.
- h** -h флаг нь вайршаркын хувилбар болон хэрэглэх заавар хэвлэх ба дараа нь програмаас гарна.
- i <capture interface>** Чагнах үйлдэл хийх сүлжээний интерфэйсийн нэр эсвэл rpipe тохируулна.
- Сүлжээний интерфэйсийн нэр нь wireshark -D командын үр дүнд байсан интерфэйсүүдийн нэг нь байх хэрэгтэй.

Хэрэв интерфэйсийн нэрийг зааж өгөөгүй бол вайршарк програм өөрөө хайлт хийх бөгөөд хамгийн эхний non-loopback интерэйсийг сонгоно. Хэрэв non-loopback интерфэйс байхгүй байвал хамгийн эхний loopback интерфэйсийг сонгодог. Сонгох ямар ч интерфэйс байхгүй байвал алдаа заах ба эхлэхгүй.

Pipe нэр нь FIFO pipe нэр эсвэл стандарт оролтоос өгөгдөл унших бол “-” байна. Pipe-aac уншиж буй өгөгдөл нь стандарт libpcap форматтай байх ёстой.

**-J <jump filter>**

-r флаг ашиглан пакет файл уншсаны дараа тохируулж өгсөн шүүлтүүртэй таарч буй хамгийн эхний пакет руу очно. Шүүлтүүрийн илэрхийлэл нь дэлгэцийн шүүлтүүрийн илэрхийлэл юм.

**-I**

Утасгүй сүлжээний пакетыг монитор горимоор чагнана (хэрэв ингэх боломжтой бол)

**-j**

Энэ флагыг -J флагын дараа хийх дараалал нь эсрэг талаасаа эхний пакетыг хийх үйлдэлд хэрэглэдэг.

**-k**

-k вайршарк программын пакет чагнах үйлдлийг нэн дариу эхлүүлдэг. Энэ флаг нь -i параметрийг ашиглан интерфэйсийг тохируулж өгсөн байхыг шаарддаг.

**-K <keytab file>**

Керberosыг задалж уншихын тулд тодорхой файлыг ашиглахад хэрэглэнэ.

**-l**

Энэ сонголт нь пакетыг жагсаан харуулах хэсэгт шинэ пакет ирэх үед хамгийн сүүлд шинээр ирсэн пакетыг харуулах (automatic scroll) үйлдлийг идэвхижүүлдэг. (-S флагаар тодорхойлогдсон)

**-L**

Интерфэйс дэмжин ажиллах data link төрлүүдийг харуулах ба дараа нь програмаас гардаг

**-m <font>**

Вайршарк программын ихэнх текстэд хэрэглэгдэх фонтын нэрийг тохируулдаг.

**-n**

Сүлжээний объект нэрийн хөрвүүлэлтийг идэвхигүй болгоно. (жишээлбэл хостын нэр, TCP, UDP портын нэрүүд)

**-N <name resolving flags>**

Тодорхой төрлийн хаяг эсвэл портын дугаарын хувьд нэрийн хөрвүүлэлтийг идэвхижүүлнэ. Аргумент нь тэмдэгт мөр байдаг бөгөөд энд тодорхой үсэг ашиглан ямар хөрвүүлэлт хийхээ шийддэг. **m** MAC хаяг хөрвүүлэлт, **n** сүлжээний хаяг хөрвүүлэлт,

**t** transport түвшний портын дугаар хөрвүүлэлт хийнэ. Энд хэрэв –  
N болон –n гэсэн 2 флаг байвал –n нь л хэрэгждэг.

С конкурент DNS lookups –ийг идэвхижүүлнэ  
d нь DNS пакетаас хөрвүүлэлт хийхийг идэвхижүүлдэг.

**-o <preference or recent settings>**

Тохиргооны хэсэг (preference) эсвэл хамгийн сүүлд хэрэглэгдсэн тохиргооны утгуудыг тохируулдаг. Энэ тохиргоо нь өгөгдмөл тохиргоо, эсвэл өмнө нь таны тохируулсан байсан тохиргоог дарж бичдэг. Флагын аргумент нь тэмдэгт мөр байдаг бөгөөд дараах форматтай байна.

*prefname: value*

*prefname* нь тохиргооны нэр (name of preference) байна.(Энэ нь preference хэсэгт харагдах нэр эсвэл сүүлд ашиглагдсан файлуудын нэртэй ижил байна.)

*value*: Тохируулах утга нь байна.

Нэг командын мөрөнд ` -o <preference settings> ` -г олон удаа бичиж өгөх боломжтой.

Тохиргооны хэсгийг зааж өгч буй жишээ:

wireshark -o mgcp.display\_dissect\_tree:TRUE

мөн –о командын нэг мөрөнд зэрэг олныг бичиж болно.  
Жишээлбэл:

wireshark -o mgcp.display\_dissect\_tree:TRUE -o  
mgcp.udp.callagent\_port:2627

Та хэрэглэх боломжтой тохиргооны тэмдэгт мөрүүдийг preferences хэсгээс үзэх боломжтой. Хавсралт В Files and Folders for details хэсгийг үзнэ үү

Хэрэглэгч хандах хүснэгт (user access table)-ийг “uat”-г ашиглан өөрчлөх боломжтой. Ингэхдээ “uat”-ийн араас UAT файлын нэр эсвэл файлд хэрэглэж болох бичилтүүдийг зааж өгөгх хэрэгтэй:

wireshark -o "uat:user\_dlts:\"User 0  
(DLT=147)\",\"http\",\"0\",\"\",\"0\",\"\""

Дээр үзүүлсэн жишээ нь data link төрөл нь 147 байгаа пакетуудыг HTTP гээр задална. Өөрөөр хэлбэл энэ нь протоколын тохиргооны хэсэгт (protocol preferences) DLT\_USER-г тохируулсан мэт ажиллана.

-p

Интерфэйсийг холимог (promiscuous) горим руу оруулах хэрэггүй. Ямар нэгэн байдлаар интерфэйс нь холимог горимд шилжсэн байх магадлалтайг анхаарч үзэх хэрэгтэй. Тиймээс -p нь тухайн траффик нь зөхвөн вайршарк програм ажиллаж буй машин руу ирж байгаа, энэ машинаас илгээгдэж байгаа эсэхийг мөн энэ машины хүлээн авч буй broadcast болон multicast траффик мөн эсэхийг ялгаж чадахгүй болдог.

-P <path setting>

Автоматаар танигддаг онцгой файлын замыг заах тохиргоо. Энэ нь вайршарк програмыг USB дээрээс тодорхой байрлал дээрээс эхлүүлэхэд гэх мэт тусгай тохиолдлуудад хэрэглэгддэг. Флагын аргумент нь дараах хэлбэртэй байдаг:

persconf:path           Хувиний тохиргооны файлын зам (path)

persdata:path           Хувийн өгөгдлөйн файлын зам. Энэ нь програм эхлэхэд нээгдэх фолдер байдаг.

-Q

Энэ тохиргоог ашигласнаар вайршарк програм чагнах үйлдэл хийж дууссаныхаа дараа програмаас гардаг. Энэ флагыг -c флагтай хамт ашиглах боломжтой. Энэ флаг нь -i болон -w тохиргоонуудтай холбоос байдлаар ашиглагдах ёстай.

-r <infile>

Энэ сонголтыг ашиглан вайршарк програмд пакет файлыг нээдэг. Пакет файл нь вайршарк програм нээх боломжтой форматтай байх ёстай.

-R <read (display)  
filter>

Энэ тохиргоо нь пакет чагнах үед хэрэгжих дэлгэцийн шүүлтүүрийг тодорхойлж өгдөг. 6.3 шүүлтүүрийн талаар авч үзсэн байгаа. Шүүлтүүр тохирохгүй байгаа пакетуудыг дэлгэцэнд харуулдаггүй.

-s <capture snapshot  
length>

Энэ сонголт нь пакет чагнах үед хэрэглэх **snapshot** уртыг тодорхойлж өгдөг. Вайршарк нь пакет бүрийн өгөгдлийн snaplen байтуудыг чагнана.

-S

Энэ сонголт нь вайршарк програм пакет чагнах үйлдэл хиймэгцээ тэдгээрийгээ дэлгэцэнд харуулах эсэхийг тодорхойлно. Пакет чагнах нь нэг процесс дээр харин тэднийг дэлгэцэнд харуулах нь

өөр процесс ашигладаг. Энэ тохиргоо нь Capture Options цонхонд байрла “Update list of packets in real time” тохиргоотой ижилхэн юм.

**-t <time stamp format>** Энэ тохиргоо нь пакетыг жагсаан харуулах хэсэгт байрлах цагийн тамгын ямар форматтай байхыг тохируулдаг. Формат нь дараах хэлбэртэй байж болно:

- r Харьцангуй, Цагийн тамга нь хамгийн эхэнд чагнагдсан пакеттай харьцангуй байдлаар харагдана.
- a Туйлын, Бүх пакет дээр бодит цагийг харуулах тохиргоо
- ad Туйлын + Он, сар, өдөр, Бүх пакет дээр бодит он, сар, өдөр мөн бодит цагийг харуулдаг.
- d Дельта, Пакетын цагийг өмнөх пакеттай нь харьцангуй байдлаар харуулдаг.
- e Эпок(epoch), Пакетын цагийг epoch (Jan 1, 1970 00:00:00) цагаас хойш өнгөрсөн секундээр харуулдаг.

**-u <s | hms>** Цагийн тамгыг секундээр харуулах, (s,өгөгдмөл утга) (h-цаг, m-минут, s-секунд)

**-v** Вайршарк програмын хувилбарын талаарх мэдээллийг хэвлээд програмаас гарна.

**-w <savefile>** Пакет файлыг хадгалах үед хэрэглэгдэх файлын нэрийг тохируулдаг.

**-y <capture link type>** Хэрэв чагнах процесс командын мөрнөөс -k параметртэйгээр эхэлсэн бол пакет чагнахад хэрэглэгдэх data link төрлийг тохируулдаг. -L параметрийн үр дүнд гарч байгаа утгуудаас хэрэглэж болно.

**-X <eXtension option>** Tshark модул руу дамжуулагдах сонголтыг тодорхойлдог. Өргөтгөлийн сонголт нь extension\_key:value бүтэцтэй байдаг

lua\_script:lua\_script\_filename Вайршарк програмд өгөгдмөл Lua script дээр нэмээд өгөгдсөн script-ийг ачааллах ёстойг хэлж өгдөг.

lua\_script[num]:argument Lua\_script командын индекс

хэлбэрийн дарааллыг заах тоогоор ялгагдах Lua script рүү аргумент дамжуулдаг. Жишээлбэл: Хэрэв -X lua\_script:my.lua гэсэн ганцхан скрипт ачааллагдсан байвал -X lua\_script1:foo нь foo гэсэн тэмдэгтийг my.lua script рүү дамжуулна.

- z <statistics-string> Вайршарк програмаас төрөл бүрийн статистикуудыг авах ба эдгээр статистикуудын үр дүнг тусдаа цонхонд харуулдаг.

### 10.3. Пакет өнгөр ялгах

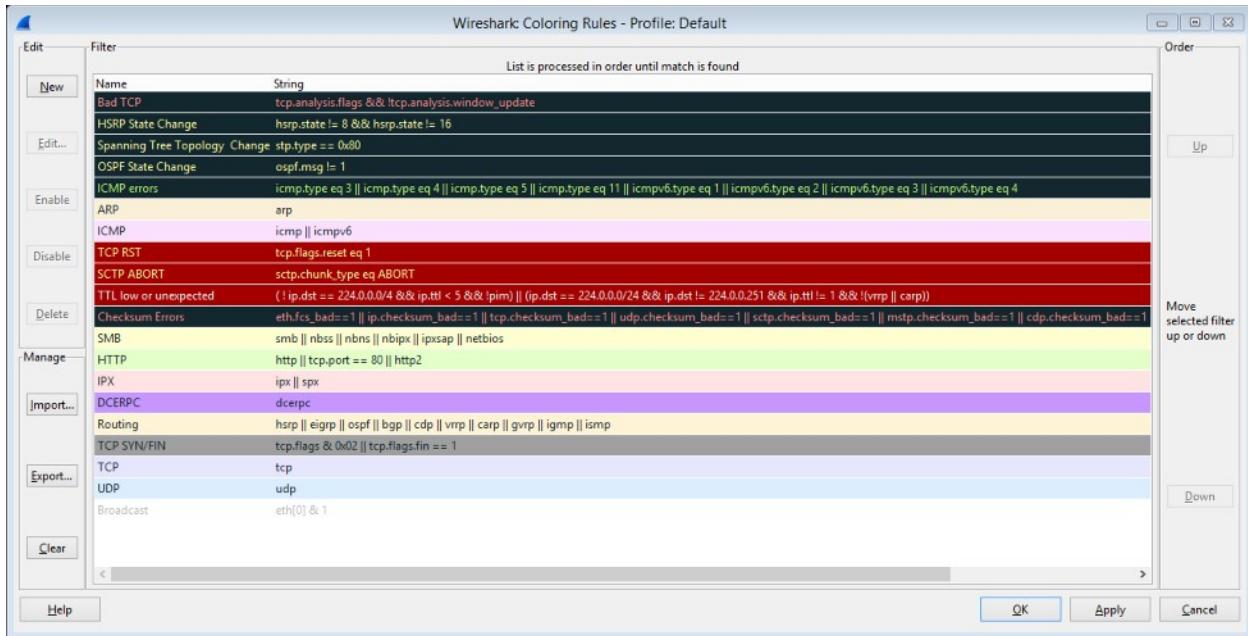
Вайршарк програм дээрх маш хэрэгтэй механизм нь пакетыг өнгөр ялгах юм. Хэрэв та тохируулж өгвөл вайршарк програм дэлгэцийн шүүлтүүрийн дагуу пакетуудыг өнгөр ялгадаг. Ингэснээр өөрийн сонирхож буй пакетаа тодотгон харах боломжтой болдог.

<https://wiki.wireshark.org/ColoringRules> хуудаснаас өнгөр ялгах дүрмүүдийн жишээг харах боломжтой.

Түр зуурын (temporary) болон байнгын (permanent) гэсэн 2 төрлийн өнгөр ялгах дүрэм байдаг. Түр зуурын өнгөр ялгалт нь вайршарк програмыг хаах хүртэл л хэрэглэгддэг харин байнгын өнгөр ялгах дүрэм нь вайршарк програмыг хаагаад дараа нь нээхэд тохиргоон дээр байдаг бөгөөд дахин ашиглах боломжтой байдаг.

Түр зуурын дүрэм нь ямар нэгэн пакетыг сонгоод Ctrl + Any Num (ямар нэгэн тоо) дарснаар идэвхижих бөгөөд энэ нь тухайн пакетаар харилцан мэдээлэл солилцож байгаа тэр пакетууд дээр үндэслэн өнгөр ялгах дүрмийг үүсгэдэг. Энэ тохиргоо нь эхлээд TCP холболт дээр суурисан дараа нь UDP, IP, Ethernet гэсэн дарааллаар тухайн пакетуудын хоорондын мэдээлэл солилцож байгаа пакетуудыг өнгөр ялгах оролдлого хийдэг. Түр зуурын өнгөр ялгах дүрмийг мөн пакетын мэдээллийг дэлгэрэнгүй харуулах хэсэгт хулганы баруун товчийг дарж Colorize with Filter → Color X сонголтыг сонгох замаар тохируулах боломжтой.

Пакетад байнгын өнгөр ялгах дүрэм тохируулахын тулд View → Coloring Rules... сонголтыг сонгох ба энэ нь дэлгэцэнд өнгөр ялгах дүрмүүд (Coloring Rules) цонхыг харуулдаг.



Зураг 10.1. Өнгөөр ялгах дүрмүүд цонх (Coloring Rules)

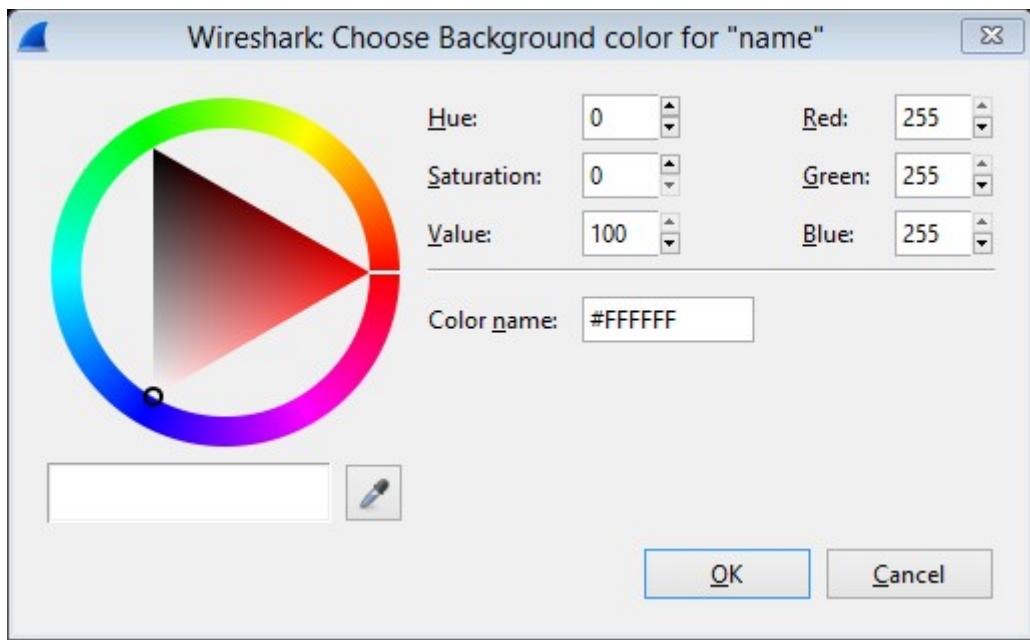
Өнгөөр ялгах дүрмийг анх удаа хэрэглэж байгаа бол энэ цонх нь өгөгдмөл тохиргоотойгоор байх бөгөөд дээрх зурганд харуулсантай ижилхэн цонхыг танд харуулна.

Тохирч буй хамгийн эхний дүрэм хэрэгжинэ.

Илүү тодорхой байх ёстой дүрмүүд нь өрөнхий дүрмүүдээс өмнө байх хэрэгтэй байдаг. Жишээлбэл: Хэрэв танд DNS дүрмийн өмнө UDP-г өнгөөр ялгах дүрэм байвал DNS өнгөөр ялгах дүрэм тань хэрэгжихгүй байх магадлалтай яагаад гэвэл DNS нь ихэвчлэн UDP дээгүүр дамжигддаг бөгөөд UDP дүрэм нь эхлээд хэрэгжих боломжтой болно гэсэн үг.

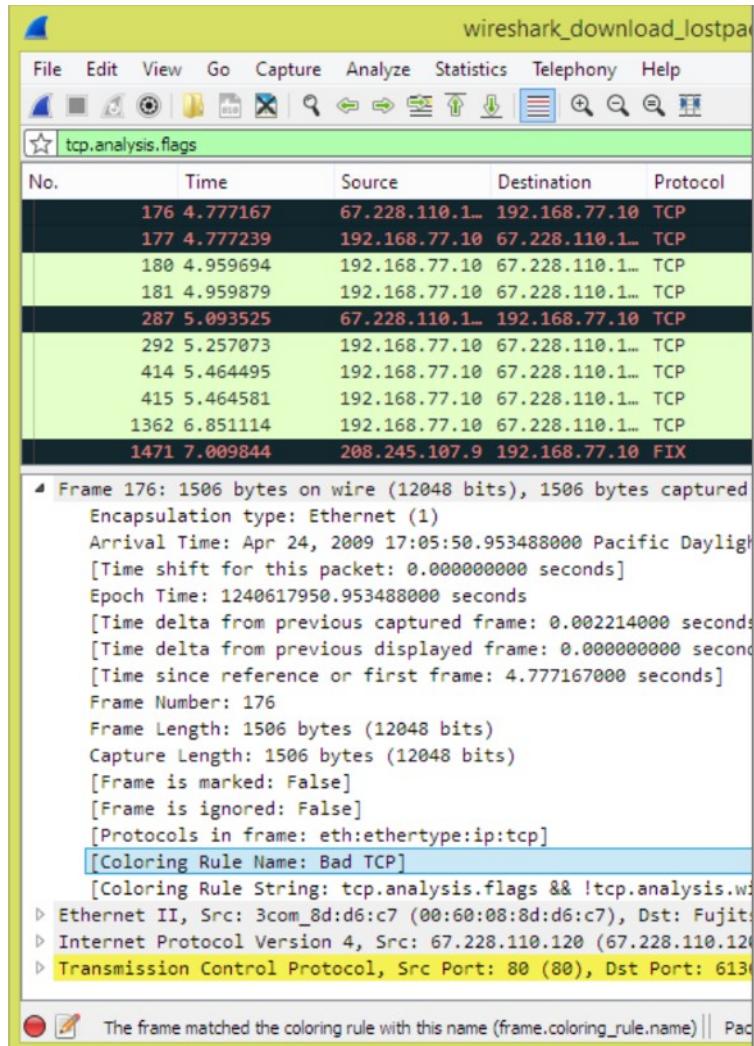
New товчлуурыг дарж шинэ дүрэм үүсгэх мөн тухайн дүрмээ идэвхижүүлээд Delete товчлуурыг дарж устгаж дүрмийг устгаж болно.

Тухайн дүрэм дээр хулганаар 2 удаа дараах эсвэл идэвхижүүлээд Edit товчлуурыг дарах замаар та тухайн дүрмийг тохируулах, өөрчлөх боломжтой. Тухайн дүрмийг засварлах эсвэл шинээр дүрэм үүсгэх үед арын фон эсвэл урд талын фонын өнгийг өөрчлөх тохиргоог хийж болдог. Ингэхдээ Foreground color эсвэл Background color товчлуур дээр 2 удаа дараах хэрэгтэй. Эдгээр товчлуур дээр дарснаар өнгө сонгох цонхыг танд харуулдаг.



Зураг 10.2. Өнгө сонгох цонх

Зураг 10.3.-т Вайршарк програм дээр өнгөөр ялгах шүүлтүүрийг хэрэглэж буй жишээг харууллаа. Фрэймийн дэлгэрэнгүй мэдээллийн хэсэгт тухайн шүүлтүүрийн дагуу “Bad TCP” дүрмийг хэрэгжүүлсэн байгааг харуулж байна.



Зураг 10.3. Вайршарк програм өнгөөр шүүлт хийж байна

#### 10.4. Протоколын задаргааг удирдах

Хэрэглэгч протоколууд хэрхэн задлагдах вэ гэдгийг удирдах боломжтой.

Протол бүр өөрийн задлагчтай тиймээс пакетыг задалж байгаа үйлдэл нь ихэвчлэн хэд хэдэн задлагчийг ашигладаг. Вайршарк програм (статик чиглэл эсвэл хьюристик таах арга ашиглан) зөв задлагчийг олох гэж оролддог гэхдээ вайршарк програм зарим тохиолдолд буруу задлагчийг сонгох магадлал байдаг. Жишээлбэл вайршарк програм таныг түгээмэл бус TCP порт дээр түгээмэл протокол ашиглаж байгаа эсэхийг тань мэдэж чадахгүй. (Стандарт 80 портын оронд TCP 800 портыг HTTP –тэй ашиглах гэх мэт)

Протокол болон түүний задлагч хоёрын хоорондын хамаарлыг удирдах 2 арга байдаг. Эхнийх нь протоколын задлагчийг тэр чигт нь идэвхигүй болгох нөгөөх нь вайршаркын задлагчуудын чиглэлийг түр зуур өөрчлөх юм.

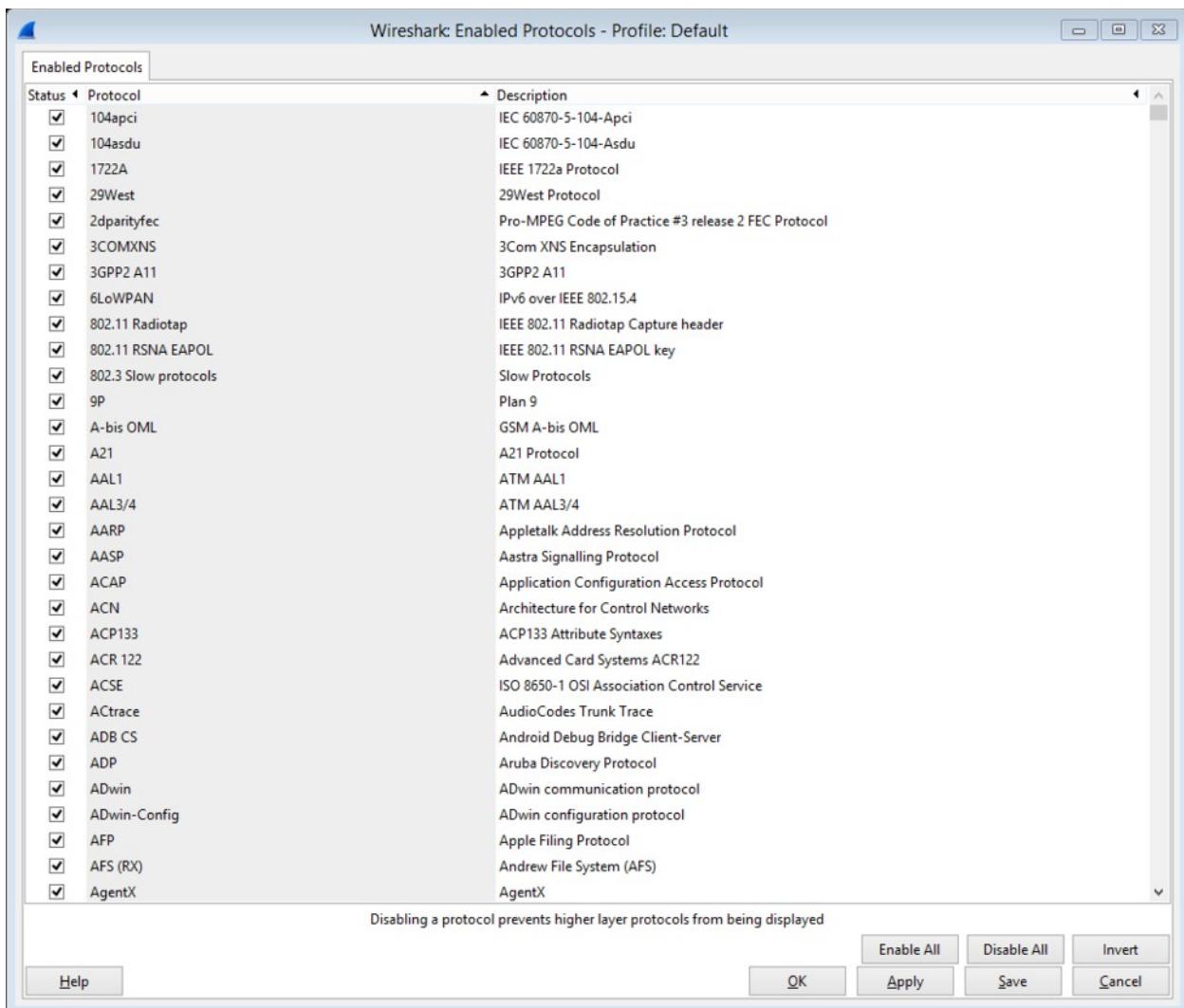
#### **10.4.1. Идэвхижүүлсэн Протоколууд цонх (Enabled Protocols)**

Идэвхижүүлсэн протоколууд цонх нь тодорхой протоколуудыг идэвхижүүлэх эсвэл идэвхигүй болгох боломжийг олгоно. Өгөгдмөл тохиргоогоор бүх протоколууд идэвхитэй байна. Протоколыг идэвхижүүлээгүй байгаа үед вайршарк руу тухайн протокол орж ирвэл програм боловсруулалт хийхээ зогсоодог.

Мэдэгдэл

Протоколыг идэвхигүй болгосон протокол нь дээд түвшний протоколуудыг дэлгэцэнд харагдуулахгүй болгодог. Жишээлбэл хэрэв та IP протоколыг идэвхигүй болгосон бөгөөд HTTP, TCP, IP, Ethernet гэсэн протоколуудыг агуулсан пакетыг сонгон авч харвал вайршарк танд Ethernet-н мэдээллийг харуулах бөгөөд бусад протоколуудын талаарх мэдээллийг харуулахгүй. Өөрөөр хэлбэл та IP протоколын хэсгийг идэвхигүй болгосноор түүнээс дээд түвшний бусад протоколыг харах боломжгүй болж байна гэсэн үг.

Протоколыг идэвхижүүлэх эсвэл идэвхигүй болгохын тулд Analyze → Enabled Protocols...-г сонгоно. Вайршарк програм танд идэвхитэй протоколууд (Enabled Protocols) цонхыг харуулна. (Зураг 10.4.-т үзүүлэв)



*Зураг 10.4. Идэвхижүүлсэн протоколууд цонх (Enabled Protocols)*

Өөрийн хайх гэж буй протоколын эхний үсгийг шууд бичсэнээр энэ цонхноос хайх түр зуурын жижиг хэсэг нээгдэж улмаар таны хайж буй protokolыг танд хялбархан олж өгнө.

Энэ цонхыг ашиглан дараах үйлдлүүдийг хийх боломжтой.

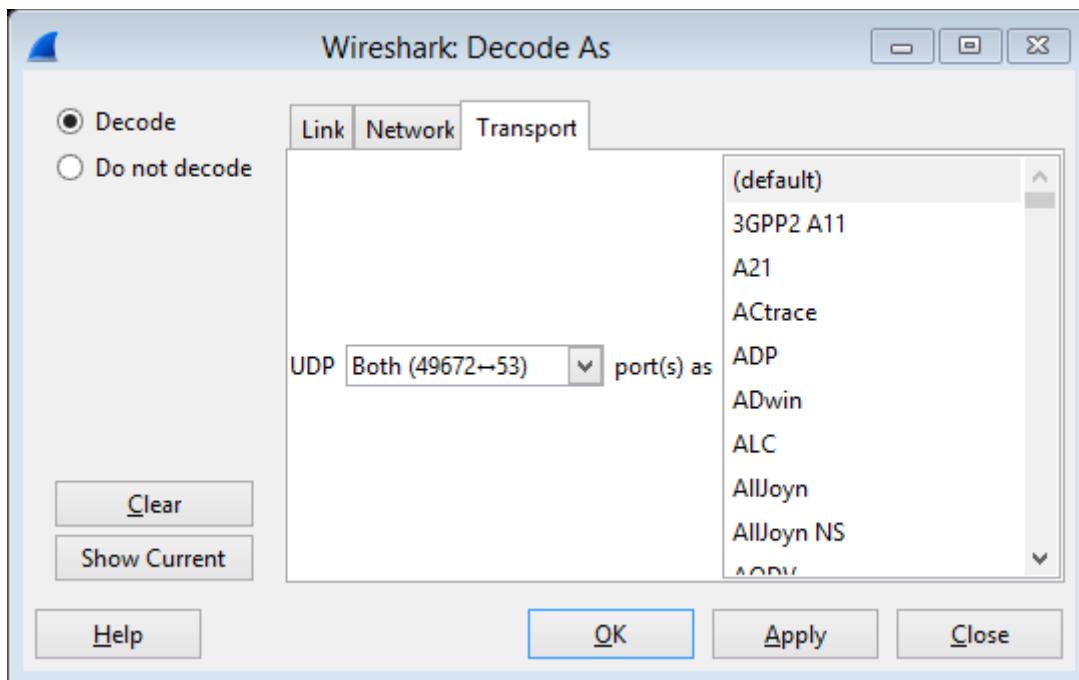
1. *Enable All:* Энэ жагсаалтанд байгаа бүх protokolуудыг идэвхижүүлнэ
2. *Disable All:* Энэ жагсаалтанд байгаа бүх protokolуудыг идэвхигүй болгоно
3. *Invert:* Одоо байгаа төлөвийн яг эсрэг төлөвийг бий болгоно. (идвэхитэй protokolуудыг идэвхигүй болгож, идэвхигүй байгаа protokolуудыг идэвхижүүлдэг)
4. *OK:* Тохиргоог хадгалж цонхыг хаана
5. *Apply:* Тохиргоог идэвхижүүлнэ гэхдээ цонхыг хаахгүй
6. *Save:* Тохиргоог the disabled\_protos хэсэг рүү хадгална. Хавсралт B, Files and Folders for details хэсгээс үзнэ үү.

7. *Cancel*: Тохиргоог түдгэлзүүлж цонхыг хаана.

#### 10.4.2. Хэрэглэгчийн тодорхойлж өгсөн задаргаа (User Specified Decodes)

“Decode As” функц нь танд протоколын задлагчийг түр хугацаагаар идэвхигүй болгох боломжийг олгодог. Хэрэв та өөрийн сүлжээндээ задаргаатай холбоотой туршилт хийж байгаа бол энэ функц танд маш хэрэгтэй функц юм.

Analyze → Decode As... хэсгийг сонгож энэ функцийг ашиглана. Вайршарк програм танд зураг 10.5.-д харуулсан “Decode as” цонхыг харуулна.



Зураг 10.5. “Decode As” цонх

Энэ цонхонд агуулагдах мэдээлэл нь тухайн үед сонгогдсон байсан пакетаас хамаардаг.

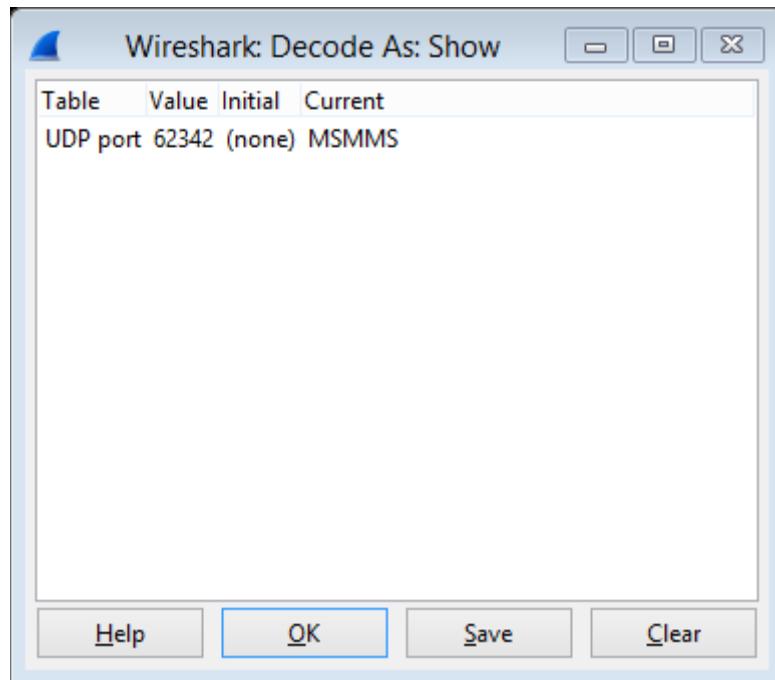
Та эдгээр тохиргоог Хэрэглэгчийн тодорхойлж өгсөн задаргаа (10.4.3. хэсэгт) хэсэгт хадгалж өгөхгүй эдгээр тохиргоо нь вайршаркаас гарах эсвэл профайлыг солих үед устаж алга болдог.

1. *Decode*: Пакетыг сонгосон аргын дагуу задлах.
2. *Do not decode*: Пакетыг сонгосон аргын дагуу задлахгүй байх.
3. *Link/Network/Transport*: Задлах үйлдэл хаана хийгдэх сүлжээний түвшинг тодорхойлж өгөх хэсэг. Тухайн нээгдсэн байгаа хэсэгт энэхүү задаргаа хийгдэнэ.
4. *Show Current*: Хэрэглэгчээс тодорхойлж өгсөн задлагчуудыг тусдаа цонхонд харуулдаг.
5. *OK*: Тохиргоог идэвхижүүлээд цонхыг хаана
6. *Apply*: Тохиргоог идэвхижүүлнэ гэхдээ цонхыг нээлттэй орхино

7. *Cancel*: Өөрчлөл хийсэн бол тухайн өөрчлөлтийг идэвхижүүлэлгүйгээр цонхыг хаана.

#### 10.4.3. Хэрэглэгчийн тодорхойлж өгсөн задаргааг харах (Show User Specified Decodes)

Энэ цонх нь одоо идэвхитэй байгаа хэрэглэгчийн тодорхойлж өгсөн задлагчуудыг харуулдаг. Эдгээр бичилтүүдийг одоогийн хэрэглэж буй профайл руугаа хадгалах боломжтой бөгөөд ингэснээр дараа нь ашиглах боломж бий болдог.

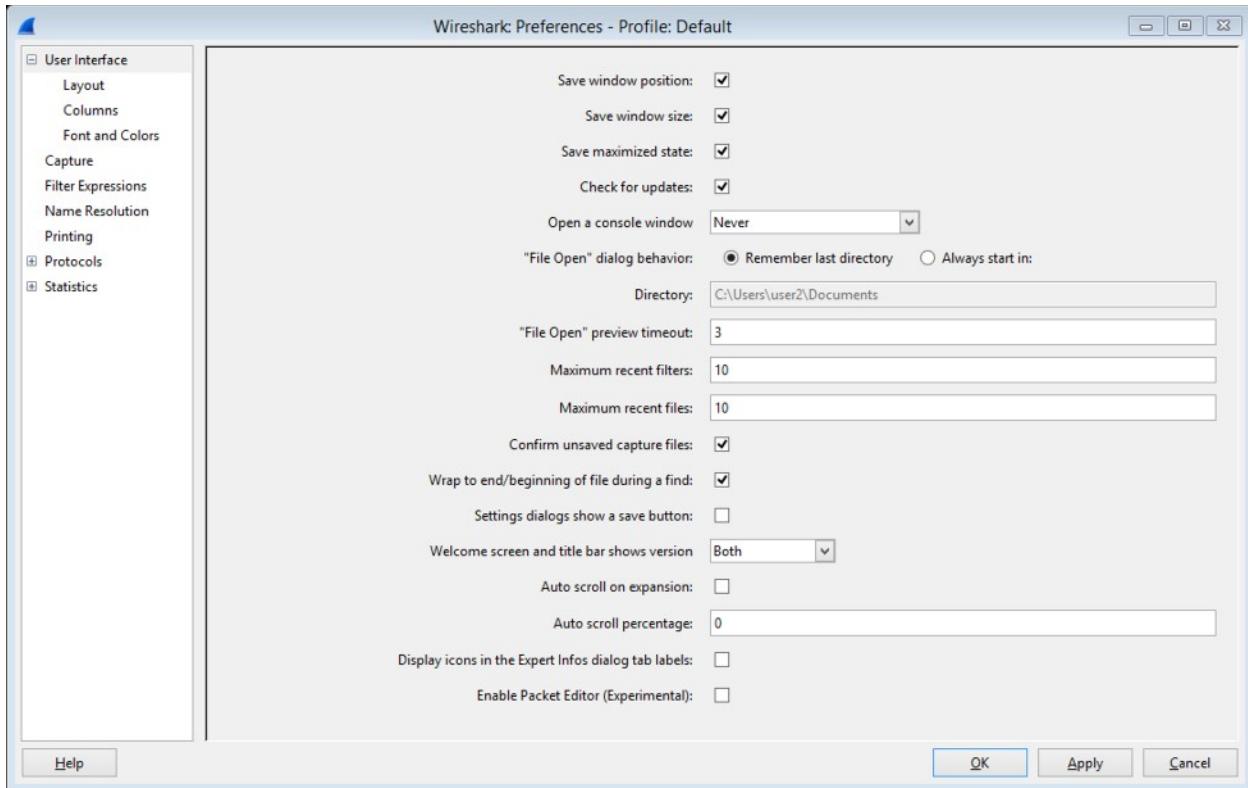


Зураг 10.6. “Decode As: Show” цонх

1. *OK*: Энэ цонхыг хаана
2. *Save*: Одоо хэрэглэж буй профайл руу энэ хүснэгтийн бичилтүүдийг хадгална
3. *Clear*: Хэрэглэгчийн профайлыг өөрчлөлгүйгээр хэрэглэгчийн тодорхойлж өгсөн задаргаануудыг устгадаг.

#### 10.5. Тохиргоо (Preferences)

Хэрэглэгч тохируулах боломжтой хэд хэдэн тохиргоо байдаг. Тохиргооны хэсгийг гаргахын тулд та *Edit → Preferences...* (*Wireshark → Preferences...* Mac OS X дээр)-г сонгох хэрэгтэй. Улмаар вайршарк програм танд Зураг 10.7.-д үзүүлсэн цонхыг гаргаж ирнэ.

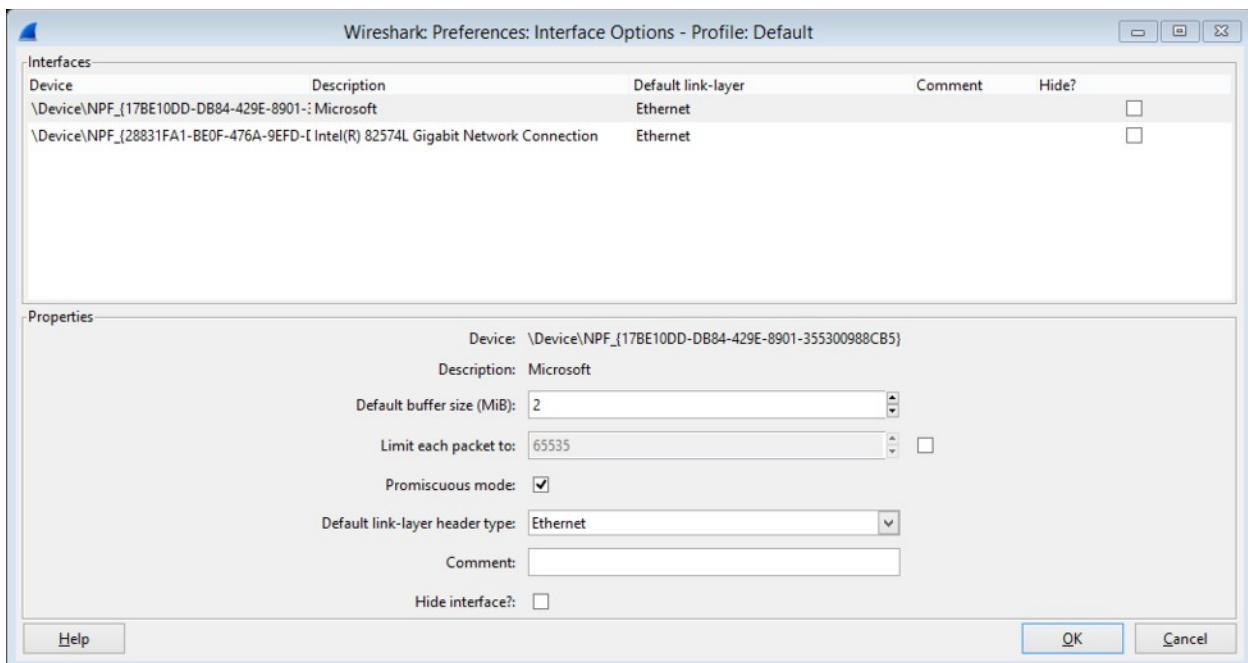


Зураг 10.7. Тохиргооны цонх (Preferences)

- *OK* товчлуур нь тохиргооны хэсэгт хийсэн өөрчлөлтийг идэвхижүүлж цонхыг хаана.
- *Apply* товчлуур нь тохиргоо хэсэгт хийсэн өөрчлөлтийг идэвхижүүлэх боловч цонхыг нээлттэй орхино.
- *Cancel* товчлуур нь тохиргооны хэсэгт хамгийн сүүлд хадгалагдсан төлвийг буцаан сэргээж авч ирэх бөгөөд энэ цонхыг хаана.

### 10.5.1. Интерфэйсийн сонголтууд (Interface Options)

Тохиргооны “Capture” хэсэг дээрээс таны компьютерийн интерфэйсд хэд хэдэн тохиргоог хийх боломжтой байдаг. “Capture” хэсгийг сонгоод Edit товчлуурыг дарах хэрэгтэй. Энэ цонхыг ашиглан интерфэйсийн өгөгдмэл link layer header-ийн төрлийг өөрчлөх, тайлбар нэмэх эсвэл интерфэйсийг програмын бусад хэсгээс нуух тохиргоог хийж болдог.



Зураг 10.8. Интерфэйсийн тохиргоо цонх (interface options)

Мөр бүр таны компьютер дээр байгаа интерфэйсийн тохиргоог агуулдаг.

- *Device*: Үйлдлийн системийн үүсгэж өгч буй төхөөрөмжийн нэр
- *Description*: Үйлдлийн системийн үүсгэж өгч буй тайлбар
- *Default link-layer*: Интерфэйс бүр хэд хэдэн link-layer header төрөлтэй байж болно. Энд сонгогдсон байгаа link-layer нь вайршарк програм ачааллагдахад хэрэглэгддэг төрөл юм. Пакет чагнаж эхлэх үедээ 4.5. хэсэгт үзүүлсэн Чагнах сонголтууд (capture options) цонхыг ашиглан энэ хэсгийг утгыг нь өөрчлөх боломжтой байдаг. Дэлгэрүүлэн судлахыг хүсвэл 4.12 хэсгийг уншина уу
- *Comment*: Хэрэглэгчээс тодорхойлж өгсөн тайлбар. Энэ тайлбар нь Үйлдлийн системийн үүсгэсэн тайлбарын оронд хэрэглэгдэнэ.
- *Hide?*: Програмын бусад хэсэгт интерфэйсийг харагдуулахгүй болгохыг хүсвэл энэ тохиргоог идэвхижүүлдэг.

### 10.6. Профайл тохируулах (Configuration Profiles)

Профайл тохиргоо нь хэд хэдэн тохиргоог ашиглах боломжийг бүрдүүлдэг. Edit → Configuration Profiles хэсгийг сонгосноор вайршарк програм профайл тохиргооны цонхыг хэрэглэгчид харуулдаг. (зураг 10.9.-д үзүүлэв). Статусбар хэсэгт байрлах профайл дээр дараах замаар профайлыг өөрчлөх боломжтой байдаг.

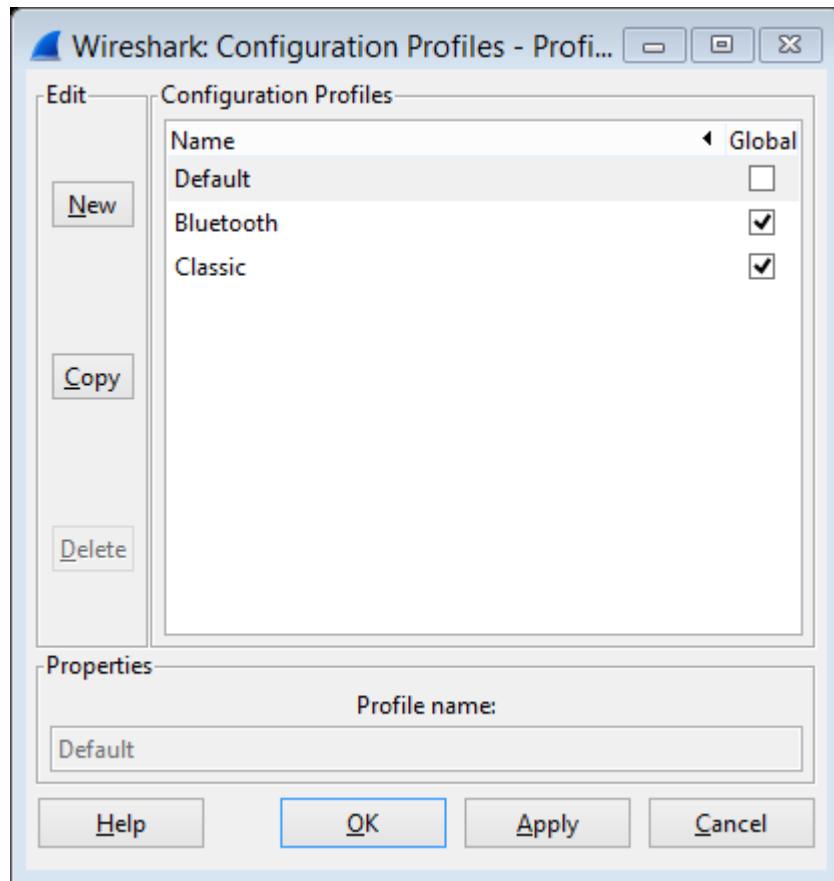
Профайлд дараах тохиргооны файлууд хадгалагддаг:

- Тохиргоо (preferences) (10.5. “Тохиргоо (Preferences)” хэсэг)

- Чагнах үеийн шүүлтүүр (cfilters) (6.6. “Шүүлтүүр тодорхойлох, хадгалах (Defining and saving filters)” хэсэг)
- Дэлгэцийн шүүлтүүр (dfilters) (6.6. “Шүүлтүүр тодорхойлох, хадгалах (Defining and saving filters)” хэсэг)
- Өнгөөр ялгах дүрмүүд (colorfilters) (10.3. “Пакет өнгөөр ялгах (Packet colorization)” хэсэг)
- Идэвхигүй болгосон тохиргоонууд (disabled\_protos) (10.4.1, “Идэвхитэй протоколууд (Enabled Protocols)” хэсэг)
- Хэрэглэгч хандах боломтой хүснэгт (User Accessible Tables):
  - Custom HTTP headers (custom\_http\_header\_fields)
  - Custom IMF headers (imf\_header\_fields)
  - Custom LDAP AttributeValue types (custom\_ldap\_attribute\_types)
  - Display Filter Macros (dfilter\_macros) (10.8. “Дэлгэцийн шүүлтүүрийн макро (Display Filter Macros)” хэсэг)
  - ESS Category Attributes (ess\_category\_attributes) (10.9. “ESS ангиллын атрибутууд (ESS Category Attributes)” хэсэг)
  - GeoIP Database Paths (geoip\_db\_paths) (10.10, “GeoIP өгөгдлийн баазын замууд (GeoIP Database Paths)” хэсэг)
  - K12 Protocols (k12\_protos) (10.19, “Tektronix K12xx/15 RF5 protocols Table” хэсэг)
  - Object Identifier Names and Associated Syntaxes (10.12, “Object Identifiers” хэсэг)
  - PRES Users Context List (pres\_context\_list) (10.13, “PRES Users Context List” хэсэг)
  - SCCP Users Table (scpp\_users) (10.14, “SCCP users Table” хэсэг)
  - SNMP Enterprise Specific Trap Types (snmp\_specific\_traps) (10.17, “SNMP Enterprise Specific Trap Types” хэсэг)
  - SNMP Users (snmp\_users) (10.18, “SNMP users Table” хэсэг)
  - User DLTs Table (user\_dlt) (10.20, “User DLTs protocol table” хэсэг)
  - IKEv2 decryption table (ikev2\_decryption\_table) (10.11, “IKEv2 decryption table” хэсэг)
- Өөрлчлөлт орсон задлагчууд (decode\_as\_entries), Үүнийг (Decode As...) цонхыг шаиглан тохируулах боломжтой (10.4.2, “User Specified Decodes” хэсэг), мөн цаашлаад Хэрэглэгчийн тодорхойлж өгсөн задлагч (User Specified Decodes...) цонход хадгалагддаг (10.4.3, “Show User Specified Decodes” хэсэг).
- Саяханы тохиргоонууд (recent), Жишээлбэл үндсэн цонхны (Main window) хэмжээ (3.3, “The Main window” хэсэг), пакет жагсаан харуулах хэсгийн баганын өргөн (3.18, “The “Packet List” pane” хэсэг), “View” цэсээр харуулж буй бүх хэсгүүд (3.7,

“The “View” menu” хэсэг) мөн файл нээх (file open) цонх хаанаас файлыг нээж байсан фолдерын зам гэх мэт тохиргоонууд

Бусад бүх тохирноо нь хувийн тохиргооны фолдерт хадгалагдаг бөгөөд бусад профайлуудын тохиргоотой ижилхэн байдаг.



Зураг 10.9. Профайл тохиргооны цонх (Configuration profiles)

- |                               |  |
|-------------------------------|--|
| <i>New</i>                    | Энэ товчлуур нь жагсаалт руу шинэ профайл нэмнэ  |
| <i>Copy</i>                   | Энэ товч нь одоо идэвхитэй байгаа профайлын бүх тохиргоог хуулж авсан шинэ профайлыг жагсаалт руу нэмдэг. Шинэ үүссэн профайлын нэр нь хуулбарласан профайлын нэрийн араас “сору” гэсэн үгийг давхар хуулсан байдаг. |
| <i>Delete</i>                 | Сонгосон байгаа профайлыг устгадаг.”Default” профайлыг устгах боломжгүй  |
| <i>Configuration Profiles</i> | Профайлын тохиргоогоо та энэ хэсэгт харагдах жагсаатаас сонгоно.   |
| <i>Profile name</i>           | Сонгогдсон байгаа профайлын нэрийг энэ хэсгийг ашиглан сольдог.  |

Профайлын нэр нь “Personal configurations” фолдер дотор байрлах тохиргооны фолдериин нэр болж өгдөг. Ижил нэртэй олон профайл үүсгэвэл зөвхөн ганцхан профайл л үүссэн байдаг.

Виндовс орчинд нэр нь цэг(.) –ээр эхэлж эсвэл төгсөж болохгүй мөн ‘\’, ‘/’, ‘:’, ‘\*’, ‘?’, ‘‘’, ‘<’, ‘>’, ‘|’, or ‘+’ тэмдэгтүүдийг ашиглах боломжгүй. Харин Юникс орчинд ‘/’ тэмдэгтийг ашиглах боломжгүй.

<i>OK</i>	Энэ товчлуур нь таны оруулсан бүх өөрчлөлтийг хадгалж, идэвхижүүлэх бөгөөд энэ цонхыг хаадаг
<i>Apply</i>	Энэ товчлуур нь таны оруулсан тохиргоог хадгалах бө сонгогдсон байгаа профайлыг идэвхижүүлдэг боловч энд харагдаж буй цонхыг нээлттэй орхидог.
<i>Cancel</i>	Ямар нэгэн өөрчлөлт оруулахгүйгээр энэ цонхыг хаадаг
<i>Help</i>	Энэхүү туслах хуудсыг харуулна

## 10.7. Хэрэглэгчийн хүснэгт (User Table)

Хэрэглэгчийн хүснэгт засварлагч нь вайршарк дээр төрөл бүрийн хүснэгтүүдийг удирдан зохион байгуулахад хэрэглэгддэг. Үндсэн цонх нь 10.3. Пакетыг өнгөөр ялгах хэсэгтэй төстэй ажилладаг.

## 10.8. Дэлгэцийн шүүлтүүрийн макро (Display Filter Macros)

Дэлгэцийн макро нь комплекс шүүлтүүрүүдийн (shortcut) богино замыг үүсгэх механизмын. Жишээлбэл `tcp_conv` нэртэй макрогийн текст нь ( `(ip.src == $1 and ip.dst == $2 and tcp.srcport == $3 and tcp.dstport == $4) or (ip.src == $2 and ip.dst == $1 and tcp.srcport == $4 and tcp.dstport == $3)` ) бол бид энэ шүүлтүүрийг бүгдийг нь бичихийн оронд дараах хэлбэрээр бичиж өгөх боломжтой.  `${tcp_conv:10.1.1.2;10.1.1.3;1200;1400}`

Дэлгэцийн шүүлтүүрийн макро нь 10.7. “Хэрэглэгчийн хүснэгт” хэсгээр буюу Analyze → Display Filter Macros цэсийг сонгох байдлаар удирдагддаг. Хэрэглэгчийн хүснэгтэд дараах талбарууд байдаг.

<i>Name</i>	Макрогийн нэр
<i>Text</i>	Макрогийн орлох текст. Макро нь оролтын аргументээр \$1, \$2, \$3, ... -г авдаг.

### **10.9. ESS Категори Аттрибут (ESS Category Attributes)**

Вайршарк энэ хүснэгтийг ESS Security Category attributes-уудыг текст дүрслэлтэй нь холбохын тулд ашигладаг. Хүснэгтэд байрлах утгууд нь XML SPIF –д байдаг. Харин энэхүү XML SPIF нь security labels тодорхойлоход хэрэглэгддэг.

Энэ хүснэгт нь 10.7. хэсэгт дурдсан хэрэглэгчийн хүснэгтээр удирдагдаг бөгөөд дараах талбаруудтай.

<i>Tag Set</i>	Category Tag Set илэрхийлэх Объект тодорхойлогч
<i>Value</i>	Категорийг илэрхийлэх утга (Label And Cert Value)
<i>Name</i>	Утгын текстэн хэлбэрийн илэрхийлэл

### **10.10. GeoIP өгөгдлийн баазын зам (GeoIP Database Paths)**

Хэрэв таны вайршарк MaxMind’s GeoIP санг дэмждэг бол та тэдний өгөгдлийн баазын IP хаягууд, ASN, ISP гэх мэт мэдээллүүдийг тэдгээрийн улс, хотуудтай нь тохируулах зорилгоор ашиглаж болно.

Зарим өгөгдлийн бааз нь үнэгүй байдаг харин зарим нь лицензийн төлбөр нэхдэг. MaxMind веб хуудаснаас дэлгэрүүлэн үзнэ үү.

Энэ хүснэгтийг мөн хэрэглэгчийн хүснэгт удирдагдаг бөгөөд дараах талбарууд энэ хэсэгт хамаардаг.

<i>Database pathname</i>	Энэ нь GeoIP өгөгдлүүд бүхий файлуудын санг заадаг. Geo –оор эхэлж .dat –аар төгссөн файлууд бүгд автоматаар ачааллагддаг. Нийтдээ 8 файл ачааллагдах боломжтой. Таны файл хаана байрлаж байгаа нь таны тохиргооноос хамаардаг. Гэхдээ ихэнхдээ /usr/share/ GeoIP (Linux), C:\GeoIP (Windows), C:\Program Files \ Wireshark\GeoIP (Windows) байрлалууд дээр хадгалбал зохистой байдаг.
--------------------------	--

### **10.11. IKEv2 декрипт хүснэгт (IKEv2 decryption table)**

Шаардлагатай мэдээллээр нь хангаж өгсөн тохиолдолд вайршарк програм IKEv2 (Internet Key Exchange version 2)-ын шифрлэгдсэн өгөгдлийг задалдаг. Хэрэв IKEv1 пакет эсвэл ESP пакетыг задалж унших бол ISAKMP protocol preference хэсгийн эсвэл ESP protocol preference хэсгийн Log Filename тохиргоог ашиглана.

Энэ хүснэгт нь 10.7 хэсэг дэх хэрэглэгчийн хүснэгтээр зохицуулагдда г бөгөөд дараах талбаруудтай.

<i>Initiator's SPI</i>	IKE_SA-гийн холболт үүсгэгчийн SPI. Энэ талбар нь 16-тын тооллын системд бичигдсэн тоон утгыг 0x гэсэн эхлэлгүйгээр авдаг бөгөөд 16-тын тооллоын системийн 16 ширхэг хекс тэмдэгт урттай байдаг (8 октетийг илэрхийлдэг)
<i>Responder's SPI</i>	IKE_SA-ийн хариу өгч байгаа талын SPI. Энэ талбар нь 16-тын тооллын системд бичигдсэн тоон утгыг 0x гэсэн эхлэлгүйгээр авдаг бөгөөд 16-тын тооллоын системийн 16 ширхэг хекс тэмдэгт урттай байдаг (8 октетийг илэрхийлдэг)
<i>SK_ei</i>	Холболт үүсгэгч талаас хүлээн авагч тал руу илгээж буй IKEv2 пакетуудыг задлахад мөн шифрлэхэд хэрэглэгддэг түлхүүр. Энэ талбар нь “0x” ээр эхлэхгүй ба 16-тын тооллын системийн тэмдэгтүүд байх ба урт нь сонгосон шифрлэлтийн алгоритмын шаардлагад нийцсэн байдал.
<i>SK_er</i>	Холболтол хариу үзүүлж байгаа талд илгээгчээс ирж буй IKEv2 пакетуудыг задлах эсвэл шифрлэх хэрэглэгддэг түлхүүр. Энэ талбар нь “0x” ээр эхлэхгүй ба 16-тын тооллын системийн тэмдэгтүүд байх ба урт нь сонгосон шифрлэлтийн алгоритмын шаардлагад нийцсэн байдал.
<i>Encryption Algorithm</i>	IKE_SA ийн шифрлэлтийн алгоритм
<i>SK_ai</i>	Холболтын хариу үзүүлж буй талаас холболтыг эхлүүлсэн тал руу илгээж буй IKEv2 пакетуудын бүрэн бүтэн байдлыг шалгах нийлбэрийг тооцоолоход хэрэгдэгддэг түлхүүр. Энэ талбар нь 0x ээр эхлээгүй 16-тын тооллын системийн тэмдэгтүүд байх ба урт нь сонгосон бүрэн бүтэн байдлыг шалгадаг алгоритмын шаардлагад нийцсэн байдал.
<i>SK_ar</i>	Холболт эхлүүлсэн талаас холболтод хариу үзүүлж буй тал руу илгээж буй IKEv2 пакетуудын бүрэн бүтэн байдлыг шалгах нийлбэрийг тооцоолоход хэрэгдэгддэг түлхүүр. Энэ талбар нь 0x ээр эхлээгүй 16-тын тооллын системийн тэмдэгтүүд байх ба урт нь сонгосон бүрэн бүтэн байдлыг шалгадаг алгоритмын шаардлагад нийцсэн байдал.
<i>Integrity Algorithm</i>	IKE_SA –гийн бүрэн бүтэн байдал шалгах алгоритм

## **10.12.      Объект ялгагч (Object Identifiers)**

ASN.1 хэрэглэдэг ихэнх протоколууд Объект ялгагч (OIDs – Object Identifier)-ийг мэдээллийн тодорхой хэсгүүдийг онцгой байдлаар ялгахын тулд хэрэглэдэг. Ихэнх тохиолдолд эдгээр нь өргөтгөлийн механизмаар хэрэглэгддэг учраас шинэ объектийн ялгагчуудыг (тэдгээртэй хамааралтай утгууд) тодорхойлоходоо үндсэн стандарттай нийцүүлэх шаардлага байдаггүй.

Вайршарк програм ихэнхи OIDs болон тэдгээрийн бичилттэй хамааралтай утгуудыг мэддэг хэдий ч өргөтгөх байдал гэдэг нь өөр бусад утгууд ч тохиолдох боломжтой гэсэн үг.

Вайршарк энэ хүснэгтийг өөрийн мэдэхгүй байгаа объект ялгагчийн нэр болон түлхүүр үгийг хэрэглэгчээр тодорхойлуулах зорилгоор хэрэглэдэг.(Жишээлбэл: X400 гэгдэх хувийн хэрэглээний өргөтгөл). Түүнчлэн энэ хэсэг нь вайршарк програм өөрийн мэддэг объект ялгагчынхаа нэр, түлхүүр үгийг өөрчлөх, дарж бичих боломжийг олгодог. (ж.нь. “id-at-countryName” нэрийг зөвхөн “с” болгох).

Энэ хүснэгтийг 10.7 хэсгээр зохицуулдаг бөгөөд дараах талбаруудтай.

<i>OID</i>	Объект ялгагчийг тодорхойлдог ялгагчууд. Ж.нь “2.5.4.6”.
<i>Name</i>	Объект ялгагчийг задлах үед дэлгэцэнд харуулах ёстой пакетын нэр. (Ж.нь: с);
<i>Syntax</i>	Объект ялгаатай холбоотой утгуудын түлхүүр үгс (syntax). Эдгээрийг вайршарк програмл мэддэг байх шаардлагатай. (Ж.нь PrintableString)

## **10.13.      PRES Users Context List**

Харилцан мэдээлэл солилцож буй мэдээллийн агуулгын тодорхойлолтыг өөртөө багтаасан PRES пакетууд чагнах үед илрээгүй бол вайршарк програм энэ хүснэгтийг агуулгын ялгагч (presentation context identifier)-ийг өгөгдсөн объектийн ялгагчтай (Object identifier) харьцуулахдаа хэрэглэдэг.

Энэ хүснэгт нь 10.7 хэсэгт үзүүлсэн хэрэглэгийн хүснэгтээр зохицуулагддаг бөгөөд дараах талбаруудтай.

<i>Context Id</i>	Энэ уялдаа холбоо хүчин төгөлдөр байгаа агуулгын ялгагч (context identifier)-г төлөөлөх тоон утга
<i>Syntax Name OID</i>	Хийсвэр өгүүлбэр зүйн нэрийг төлөөлөх объектийн ялгагч. Энэ өгүүлбэр зүйн нэр нь энэ холболт дээгүүр дамжигдаж буй

протоколыг тодорхойлдог.

#### **10.14. SCCP хэрэглэгчийн хүснэгт (SCCP users Table)**

Энэхүү хүснэгтийг вайршарк програм тодорхой протоколуудыг SPPC-д зориулагдсан тодорхой DCP/SSN хослуулд руу холбохын тулд ашигладаг.

Энэ хүснэгтийг 10.7 хэсэгт үзүүлсэн хэрэглэгчийн хүснэгт удирддаг бөгөөд дараах талбаруудтай.

<i>Network Indicator</i>	Энэ холболтод хүчинтэй байгаа сүлжээний индикаторыг илэрхийлэх тоон утга
<i>Called DPCs</i>	Энэ холболтод хүчинтэй байгаа dpcs -г илэрхийлэг тоон утгын завсар
<i>Called SSNs</i>	Энэ холболтод хүчинтэй байгаа ssns-г илэрхийлэх тоон утгын завсар
<i>User protocol</i>	Энэ холболт дээгүүр илгээгдэж буй протокол

#### **10.15. SMI (MIB болон PIB) модулууд (SMI (MIB and PIB) Modules)**

Хэрэв таны вайршарк програм libSMI дэмждэг бол та MIB болон PIB модулуудын жагсаалтыг энд тодорхойлж өгч болно. COPS болон SNMP задлагчууд нь эдгээрийг OID-г хөрвүүлэхийн тулд хэрэглэдэг.

*Module name*      Модулын нэр. Ж.нь: IF-MIB

#### **10.16. SMI (MIB болон PIB) зам (SMI (MIB and PIB) Paths)**

Хэрэв таны вайршарк програм libSMI дэмждэг бол та энд MIB болон PIB модулуудын замуудыг энд тодорхойлж өгч болно.

*Directory name*      Модулын сан. Ж.нь: /usr/local/snmp/mibs. Вайршарк програм стандарт SMI замыг таны үйлдлийн системд тохируулан сонгон хэрэглэдэг. Тиймээс ихэнхдээ энэ хэсэгт нэмэлт зүйл оруулахгүй байх нь дээр байдаг.

#### **10.17. SNMP Enterprise Specific Trap Types**

Энэ хэсгийг вайршарк програм specific trap утгыг Trap PDU хэсэг дэх хэрэглэгчийн зааж өгсөн тайлбартай холбоход хэрэглэдэг. Тайлбар нь пакетын дэлгэрэнгүй specific-trap элементийн хэсэгт харагддаг.

Энэ хүснэгтийг 10.7 хэсэгт үзүүлсэн хэрэглэгчийн хүснэгт удирддаг бөгөөд дараах талбаруудтай.

<i>Enterprise OID</i>	Trap-ийг үүсгэж буй объектийг илэрхийлэх объектийн ялгагч (OID)
<i>Trap Id</i>	Specific-trap кодыг илэрхийлэх тоон утга
<i>Description</i>	Пакетыг дэлгэрэнгүй харуулах хэсэгт харагдах тайлбар

#### **10.18. SNMP хэрэглэгчийн хүснэгт (SNMP users Table)**

Вайршарк програм энэ хүснэгтийг шифрлэгдсэн SNMPv3 пакетуудыг задлах мөн түүний баталгаажуулалтыг шалгах зорилгоор хэрэглэдэг.

Энэ хүснэгтийг 10.7 хэсэгт үзүүлсэн хэрэглэгчийн хүснэгт удирдах бөгөөд дараах талбаруудтай.

<i>Engine ID</i>	Хэрэв энэ талбар өгөгдсөн байвал зөвхөн engine ID нь тохирч байгаа пакетуудад л хэрэглэгддэг. Энэ талбар нь 16 тын тооллын тэмдэгтийг 0102030405 форматаар авдаг.
<i>Username</i>	SNMP engine-ийн хэрэглэгчийн нэр юм.
<i>Authentication model</i>	Баталгаажуулалтын ямар хэлбэрийг сонгохыг тодорхойлдог (“MD5” эсвэл “SHA1”).
<i>Password</i>	Баталгаажуулалтын нууц үг. \xDD –г хэвлэгдэх боломжгүй тэмдэгтээр ашигладаг. 16-тын тооллын системд байгаа нууц үг нь \xDD тэмдэгтийн дарааллаар орсон байх ёстой. Жишээлбэл 010203040506 гэсэн хекс нууц үг нь \x01\x02\x03\x04\x05\x06 хэлбэрээр орох ёстой. \ тэмдэгт нь хэвлэгдэх боломжгүй тэмдэгт гэсэн утгыг илэрхийлэх ёстой.
<i>Privacy protocol</i>	Шифрлэлтийн ямар алгоритм ашиглахыг шийддэг. (“DES” эсвэл “AES”).
<i>Privacy password</i>	Хувийн нууц үг. \xDD –г хэвлэгдэх боломжгүй тэмдэгтээр ашигладаг. 16-тын тооллын системд байгаа нууц үг нь \xDD тэмдэгтийн дарааллаар орсон байх ёстой. Жишээлбэл 010203040506 гэсэн хекс нууц үг нь \x01\x02\x03\x04\x05\x06 хэлбэрээр орох ёстой. \ тэмдэгт нь хэвлэгдэх боломжгүй тэмдэгт гэсэн утгыг илэрхийлэх ёстой.

### **10.19. Tektronix K12xx/15 RF5 протоколын хүснэгт (Tektronix K12xx/15 RF5 protocols Table)**

Тодорхой интерфэйс дээр хэрэглэгдэж буй төрөл бүрийн протоколуудыг тодорхойлохын тулд Tektronix K12xx/15 rf5 файлын формат нь туслагч файлуудыг (\*.stk) хэрэглэдэг. Вайршарк эдгээр stk файлуудыг уншдаггүй бөгөөд аль доод түвшний протоколыг хэрэглэхийг тодорхойлоход туслах хүснэгтийг хэрэглэдэг байна.

Протокол тохируулах Stk файл нь 10.7 хэсэгт үзүүлсэн хэрэглэгчийн хүснэгтээр удирдагдаг бөгөөд дараах талбаруудтай.

<i>Match string</i>	Stk файлын нэрийг хэсэгчилсэн байдлаар тааруулж үздэг тиймээс хэрэв танд тодорхой тохиолдол болон ерөнхий тохиолдол 2 байгаа бол тодорхой тохиолдол нь жагсаалтын эхэнд нь байх нь зүйтэй.
<i>Protocol</i>	Encapsulating protocol-ын нэр(пакет өгөгдлийн хамгийн доод түвшин). Энэ хэсэгт зүгээр л протоколын нэр (ж.нь: mtp2, eth_witoutfcs, sscf-nni) эсвэл encapsulation protocol-ын нэр болон түүн дээр байрлах “application” протокол 2-ыг таслалаар тусгаарлан зааж өгсөн байх боломжтой. (ж.нь: sscop:sscf-nni, sscop:alcap, sscop:nbap, ...)

### **10.20. Хэрэглэгчийн DLT протоколын хүснэгт (User DLTs protocol table)**

Рсар файл хэрэглэгчийн DLT-ийн нэгийг хэрэглэж байгаа бол вайршарк програм DLT хэрэглэгчид аль протоколыг нь ашиглах вэ гэдгээ тодорхойлохын тулд энэ хүснэгтийг хэрэглэдэг.

Энэ хүснэгтийн 10.7 хэсэгт үзүүлсэн хэрэглэгчийн хүснэгт удирдагдаг бөгөөд дараах талбаруудтай.

<i>DLT</i>	Хэрэглэгчийн dlt-гүүдийн нэг
<i>Payload protocol</i>	Payload протоколын нэр (пакет өгөгдөл дэх хамгийн доод түвшин) (ж.нь: Ethernet-д “eth”, IPv4 -д “ip”)
<i>Header size</i>	Хэрэв header protocol байгаа (payload protocol-ын өмнө) бол энэ хэсэг header –н хэмжээг зааж өгдөг. 0 гэсэн утга нь header protocol-г идэвхигүй болгодог.
<i>Header protocol</i>	Хэрэглэгдэх header protocol-ын нэр (өгөгдмөл тохиргоогоор “data”-г хэрэглэдэг)
<i>Trailer size</i>	Trailer протокол (payload protocol-ын дараа) байгаа бол энэ

хэсэг trailer-ийн хэмжээг зааж өгнө. 0 гэсэн утга нь trailer протоколыг идэвхигүй болгодог.

#### *Trailer protocol*

Хэрэглэгдэх trailer protocol-ын нэр (өгөгдмөл тохиргоогоор “data”-г хэрэглэдэг)

#### **Appendix A. Wireshark Messages**

Wireshark provides you with additional information generated out of the plain packet data or it may need to indicate dissection problems. Messages generated by Wireshark are usually placed in square brackets (“[]”).

## A.1. Packet List Messages

These messages might appear in the packet list.

### A.1.1. [Malformed Packet]

Malformed packet means that the protocol dissector can't dissect the contents of the packet any further. There can be various reasons:

- *Wrong dissector*: Wireshark erroneously has chosen the wrong protocol dissector for this packet. This will happen e.g. if you are using a protocol not on its well known TCP or UDP port. You may try Analyze|Decode As to circumvent this problem.
- *Packet not reassembled*: The packet is longer than a single frame and it is not reassembled, see Section 7.6, “Packet Reassembly” for further details.
- *Packet is malformed*: The packet is actually wrong (malformed), meaning that a part of the packet is just not as expected (not following the protocol specifications).
- *Dissector is buggy*: The corresponding protocol dissector is simply buggy or still incomplete.

Any of the above is possible. You'll have to look into the specific situation to determine the reason. You could disable the dissector by disabling the protocol on the Analyze menu and check how Wireshark displays the packet then. You could (if it's TCP) enable reassembly for TCP and the specific dissector (if possible) in the Edit|Preferences menu. You could check the packet contents yourself by reading the packet bytes and comparing it to the protocol specification. This could reveal a dissector bug. Or you could find out that the packet is indeed wrong.

### A.1.2. [Packet size limited during capture]

The packet size was limited during capture, see “Limit each packet to n bytes” at the Section 4.5, “The “Capture Options” dialog box”. While dissecting, the current protocol dissector was simply running out of packet bytes and had to give up. There's nothing else you can do now, except to repeat the whole capture process again with a higher (or no) packet size limitation.

## A.2. Packet Details Messages

These messages might appear in the packet details.

### A.2.1. [Response in frame: 123]

The current packet is the request of a detected request/response pair. You can directly jump to the corresponding response packet just by double clicking on this message.

### A.2.2. [Request in frame: 123]

Same as “Response in frame: 123” above, but the other way round.

### A.2.3. [Time from request: 0.123 seconds]

The time between the request and the response packets.

### A.2.4. [Stream setup by PROTOCOL (frame 123)]

The session control protocol (SDP, H225, etc) message which signaled the creation of this session. You can directly jump to the corresponding packet just by double clicking on this message.

## **Appendix B. Files and Folders**

### **B.1. Capture Files**

To understand which information will remain available after the captured packets are saved to a capture file, it's helpful to know a bit about the capture file contents.

Wireshark uses the pcapng file format as the default format to save captured packets. It is very flexible but other tools may not support it.

Wireshark also supports the libpcap file format. This is a much simpler format and is well established. However, it has some drawbacks: it's not extensible and lacks some information that would be really helpful (e.g. being able to add a comment to a packet such as "the problems start here" would be really nice).

In addition to the libpcap format, Wireshark supports several different capture file formats. However, the problems described above also applies for these formats.

### B.1.1. Libpcap File Contents

At the start of each libpcap capture file some basic information is stored like a magic number to identify the libpcap file format. The most interesting information of this file start is the link layer type (Ethernet, 802.11, MPLS, etc).

The following data is saved for each packet:

- The timestamp with millisecond resolution
- The packet length as it was “on the wire”
- The packet length as it’s saved in the file
- The packet’s raw bytes

A detailed description of the libpcap file format can be found at: <https://wiki.wireshark.org/Development/LibpcapFileFormat>

### B.1.2. Not Saved in the Capture File

You should also know the things that are not saved in capture files:

- Current selections (selected packet, ...)
- Name resolution information. See Section 7.7, “Name Resolution” for details

Pcapng files can optionally save name resolution information. Libpcap files can’t. Other file formats have varying levels of support.

- The number of packets dropped while capturing
- Packet marks set with “Edit/Mark Packet”
- Time references set with “Edit/Time Reference”
- The current display filter

## B.2. Configuration Files and Folders

Wireshark uses a number of files and folders while it is running. Some of these reside in the personal configuration folder and are used to maintain information between runs of Wireshark, while some of them are maintained in system areas.

### Tip

A list of the folders Wireshark actually uses can be found under the Folders tab in the dialog box shown when you select About Wireshark from the Help menu.

The content format of the configuration files is the same on all platforms. However, to match the different policies for Unix and Windows platforms, different folders are used for these files.

Table B.1. Configuration files and folders overview

File/Folder	Description	Unix/Linux folders	Windows folders
-------------	-------------	--------------------	-----------------

preferences	Settings from the Preferences dialog box.	/etc/wireshark.conf, \$HOME/.wireshark/preferences	%WIRESHARK%\wireshark.conf, %APPDATA%\Wireshark\preferences
recent	Recent GUI settings (e.g. recent files lists).	\$HOME/.wireshark/recent	%APPDATA%\Wireshark\recent
cfilters	Capture filters.	\$HOME/.wireshark/cfilters	%WIRESHARK%\cfilters, %APPDATA%\Wireshark\cfilters
dfilters	Display filters.	\$HOME/.wireshark/dfilters	%WIRESHARK%\dfilters, %APPDATA%\Wireshark\dfilters
colorfilters	Coloring rules.	\$HOME/.wireshark/colorfilters	%WIRESHARK%\colorfilters, %APPDATA%\Wireshark\colorfilters
disabled_protos	Disabled protocols.	\$HOME/.wireshark/disabled_protos	%WIRESHARK%\disabled_protos, %APPDATA%\Wireshark\disabled_protos

ethers	Ethernet name resolution.	/etc/ethers, \$HOME/.wireshark/ethers	%WIRESHARK%\ethers, %APPDATA%\Wireshark\ethers
manuf	Ethernet name resolution.	/etc/manuf, \$HOME/.wireshark/manuf	%WIRESHARK%\manuf, %APPDATA%\Wireshark\manuf
hosts	IPv4 and IPv6 name resolution.	/etc/hosts, \$HOME/.wireshark/hosts	%WIRESHARK%\hosts, %APPDATA%\Wireshark\hosts
services	Network services.	/etc/services, \$HOME/.wireshark/services	%WIRESHARK%\services, %APPDATA%\Wireshark\services
subnets	IPv4 subnet name resolution.	/etc/subnets, \$HOME/.wireshark/subnets	%WIRESHARK%\subnets, %APPDATA%\Wireshark\subnets
ipxnets	IPX name resolution.	/etc/ipxnets, \$HOME/.wireshark/ipxnets	%WIRESHARK%\ipxnets, %APPDATA%\Wireshark\ipxnets

plugins	Plugin directories.	/usr/share/wireshark/plugins, /usr/local/share/wireshark/plugins, \$HOME/.wireshark/plugins	%WIRESHARK%\plugins<version>, %APPDATA%\Wireshark\plugins
temp	Temporary files.	Environment: TMPDIR	Environment: TMPDIR or TEMP

## Windows folders

%APPDATA% points to the personal configuration folder, e.g.: C:\Documents and Settings \<username>\Application Data (details can be found at: Section B.3.1, “Windows profiles”),

%WIRESHARK% points to the Wireshark program folder, e.g.: C:\Program Files\Wireshark

## Unix/Linux folders

The /etc folder is the global Wireshark configuration folder. The folder actually used on your system may vary, maybe something like: /usr/local/etc.

\$HOME is usually something like: /home/<username>

## File contents

### preferences/wireshark.conf

This file contains your Wireshark preferences, including defaults for capturing and displaying packets. It is a simple text file containing statements of the form:

```
variable: value
```

The settings from this file are read in at program start and written to disk when you press the Save button in the "Preferences" dialog box.

### recent

This file contains various GUI related settings like the main window position and size, the recent files list and such. It is a simple text file containing statements of the form:

```
variable: value
```

It is read at program start and written at program exit.

#### **cfilters**

This file contains all the capture filters that you have defined and saved. It consists of one or more lines, where each line has the following format:

```
"<filter name>" <filter string>
```

The settings from this file are read in at program start and written to disk when you press the Save button in the "Capture Filters" dialog box.

#### **dfilters**

This file contains all the display filters that you have defined and saved. It consists of one or more lines, where each line has the following format:

```
"<filter name>" <filter string>
```

The settings from this file are read in at program start and written to disk when you press the Save button in the "Display Filters" dialog box.

#### **colorfilters**

This file contains all the color filters that you have defined and saved. It consists of one or more lines, where each line has the following format:

```
@<filter name>@<filter string>@[<bg RGB (16-bit)>] [<fg RGB (16-bit)>]
```

The settings from this file are read in at program start and written to disk when you press the Save button in the "Coloring Rules" dialog box.

#### **disabled\_protos**

Each line in this file specifies a disabled protocol name. The following are some examples:

```
tcp  
udp
```

The settings from this file are read in at program start and written to disk when you press the Save button in the "Enabled Protocols" dialog box.

#### **ethers**

When Wireshark is trying to translate Ethernet hardware addresses to names, it consults the files listed in [Table A.1, “Configuration files and folders overview”](#). If an address is not found in /etc/ethers, Wireshark looks in \$HOME/.wireshark/ethers

Each line in these files consists of one hardware address and name separated by whitespace. The digits of hardware addresses are separated by colons (:), dashes (-) or periods(.). The following are some examples:

```
ff-ff-ff-ff-ff-ff      Broadcast
c0-00-ff-ff-ff-ff      TR_broadcast
00.2b.08.93.4b.a1    Freds_machine
```

The settings from this file are read in at program start and never written by Wireshark.

## **manuf**

Wireshark uses the files listed in [Table A.1, “Configuration files and folders overview”](#) to translate the first three bytes of an Ethernet address into a manufacturers name. This file has the same format as the ethers file, except addresses are three bytes long.

An example is:

```
00:00:01      Xerox          # XEROX CORPORATION
```

The settings from this file are read in at program start and never written by Wireshark.

## **hosts**

Wireshark uses the files listed in [Table A.1, “Configuration files and folders overview”](#) to translate IPv4 and IPv6 addresses into names.

This file has the same format as the usual /etc/hosts file on Unix systems.

An example is:

```
# Comments must be prepended by the # sign!
192.168.0.1 homeserver
```

The settings from this file are read in at program start and never written by Wireshark.

## **services**

Wireshark uses the files listed in [Table A.1, “Configuration files and folders overview”](#) to translate port numbers into names.

An example is:

```
mydns      5045/udp      # My own Domain Name Server  
mydns      5045/tcp      # My own Domain Name Server
```

The settings from this file are read in at program start and never written by Wireshark.

### **subnets**

Wireshark uses the files listed in [Table A.1, “Configuration files and folders overview”](#) to translate an IPv4 address into a subnet name. If no exact match from the hosts file or from DNS is found, Wireshark will attempt a partial match for the subnet of the address.

Each line of this file consists of an IPv4 address, a subnet mask length separated only by a '/' and a name separated by whitespace. While the address must be a full IPv4 address, any values beyond the mask length are subsequently ignored.

An example is:

```
# Comments must be prepended by the # sign!  
192.168.0.0/24 ws_test_network
```

A partially matched name will be printed as "subnet-name.remaining-address". For example, "192.168.0.1" under the subnet above would be printed as "ws\_test\_network.1"; if the mask length above had been 16 rather than 24, the printed address would be "ws\_test\_network.0.1".

The settings from this file are read in at program start and never written by Wireshark.

### **ipxnets**

Wireshark uses the files listed in [Table A.1, “Configuration files and folders overview”](#) to translate IPX network numbers into names.

An example is:

```
C0.A8.2C.00      HR  
c0-a8-1c-00      CEO  
00:00:BE:EF      IT_Server1  
110f             FileServer3
```

The settings from this file are read in at program start and never written by Wireshark.

### **plugins folder**

Wireshark searches for plugins in the directories listed in [Table A.1, “Configuration files and folders overview”](#). They are searched in the order listed.

### **temp folder**

If you start a new capture and don't specify a filename for it, Wireshark uses this directory to store that file; see [Section 4.11, “Capture files and file modes”](#).

### B.2.1. Protocol help configuration

Wireshark can use configuration files to create context-sensitive menu items for protocol detail items which will load help URLs in your web browser.

To create a protocol help file, create a folder named “protocol\_help” in either the personal or global configuration folders. Then create a text file with the extension “.ini” in the “protocol\_help” folder. The file must contain key-value pairs with the following sections:

#### [database]

Mandatory. This contains initialization information for the help file. The following keys must be defined:

source

Source name, e.g. "HyperGlobalMegaMart".

version

Must be "1".

location

General URL for help items. Variables can be substituted using the [location data] section below.

#### [location data]

Optional. Contains keys that will be used for variable substitution in the "location" value. For example, if the database section contains

```
location = http://www.example.com/proto?cookie=${cookie}&path=${PATH}
```

then setting

```
cookie = anonymous-user-1138
```

will result in the URL "http://www.example.com/proto?cookie=anonymous-user-1138&path=\${PATH}". PATH is used for help path substitution, and shouldn't be defined in this section.

#### [map]

Maps Wireshark protocol names to section names below. Each key MUST match a valid protocol name such as "ip". Each value MUST have a matching section defined in the configuration file.

Each protocol section must contain an “\_OVERVIEW” key which will be used as the first menu item for the help source. Subsequent keys must match descriptions will be appended to the location.

Suppose the file C:\Users\sam.clemens\AppData\Roaming\Wireshark\protocol\_help\wikipedia.ini contains the following:

```
# Wikipedia (en) protocol help file.

# Help file initialization # source: The source of the help
information, e.g. ``Inacon'' or ``Wikipedia'' # version: Currently
unused. Must be ``1''. # url_template: Template for generated URLs.
See ``URL Data'' below. [database] source=Wikipedia version=1
url_template=https://${language}.wikipedia.org/wiki/${PATH}

# Substitution data for the location template. # Each occurrence of
the keys below in the location template will be # substituted with
their corresponding values. For example, ``${license}'' # in the URL
template above will be replaced with the value of ``license'' # below.
# # PATH is reserved for the help paths below; do not specify it here.
[location data] language = en

# Maps Wireshark protocol names to section names below. Each key MUST
match # a valid protocol name. Each value MUST have a matching section
below. [map] tcp=TCP

# Mapped protocol sections. # Keys must match protocol detail items
descriptions. [TCP] _OVERVIEW=Transmission_Control_Protocol
Destination port=Transmission_Control_Protocol#TCP_ports Source
port=Transmission_Control_Protocol#TCP_ports
```

Right-clicking on a TCP protocol detail item will display a help menu item that displays the Wikipedia page for TCP. Right-clicking on the TCP destination or source ports will display additional help menu items that take you to the “TCP ports” section of the page.

example, the following configuration is functionally equivalent to the previous configuration:

```
[database] source=Wikipedia version=1
location=https://en.wikipedia.org/wiki/

[map] tcp=TCP

[TCP] _OVERVIEW=Transmission_Control_Protocol Destination
port=Transmission_Control_Protocol#TCP_ports Source
port=Transmission_Control_Protocol#TCP_ports
```

## B.3. Windows folders

Here you will find some details about the folders used in Wireshark on different Windows versions.

As already mentioned, you can find the currently used folders in the About Wireshark dialog.

### B.3.1. Windows profiles

Windows uses some special directories to store user configuration files which define the “user profile”. This can be confusing, as the default directory location changed from Windows version to version and might also be different for English and internationalized versions of Windows.

Note

If you've upgraded to a new Windows version, your profile might be kept in the former location. The defaults mentioned here might not apply.

The following guides you to the right place where to look for Wireshark's profile data.

Windows 7, Windows Vista

C:\Users\<username>\AppData\Roaming\Wireshark

Windows XP

C:\Documents and Settings\<username>\Application Data, "Documents and Settings" and "Application Data" might be internationalized.

Windows 2000 (no longer supported by Wireshark, for historical reference only)

C:\Documents and Settings\<username>\Application Data, "Documents and Settings" and "Application Data" might be internationalized.

Windows NT 4 (no longer supported, for historical reference only)

C:\WINNT\Profiles\<username>\Application Data\Wireshark

Windows ME, Windows 98 with user profiles (no longer supported, for historical reference only)

In Windows ME and 98 you can enable separate user profiles. In that case, something like C:\windows\Profiles\<username>\Application Data\Wireshark is used.

Windows ME, Windows 98 without user profiles (no longer supported, for historical reference only)

Without user profiles enabled the default location for all users is C:\windows\Application Data\Wireshark

Without user profiles enabled the default location for all users was C:\windows\Application Data\Wireshark

### **B.3.2. Windows roaming profiles**

Some larger Windows environments use roaming profiles. If this is the case the configurations of all programs you use won't be saved on your local hard drive. They will be stored on the domain server instead.

Your settings will travel with you from computer to computer with one exception. The "Local Settings" folder in your profile data (typically something like: C:\Documents and Settings\<username>\Local Settings) will not be transferred to the domain server. This is the default for temporary capture files.

### **B.3.3. Windows temporary folder**

Wireshark uses the folder which is set by the TMPDIR or TEMP environment variable. This variable will be set by the Windows installer.

Windows 7, Windows Vista

C:\Users\<username>\AppData\Local\Temp

Windows XP, Windows 2000

C:\Documents and Settings\<username>\Local Settings\Temp

Windows NT

C:\TEMP

## **Appendix C. Protocols and Protocol Fields**

Wireshark distinguishes between protocols (e.g. tcp) and protocol fields (e.g. tcp.port).

A comprehensive list of all protocols and protocol fields can be found in the “Display Filter Reference” at  
<https://www.wireshark.org/docs/deref/>

## Appendix D. Related command line tools

### D.1. Introduction

Along with the main application, Wireshark comes with an array of command line tools which can be helpful for specialized tasks. These tools will be described in this chapter. You can find more information about each command in the Manual Pages.

### D.2. tshark: Terminal-based Wireshark

TShark is a terminal oriented version of Wireshark designed for capturing and displaying packets when an interactive user interface isn't necessary or available. It supports the same options as wireshark. For more information on tshark see the manual pages (man tshark).

**Help information available from tshark.**

```
TShark 1.12.0 (v1.12.0-rc2-59-g7ea0d6c from master-1.12)
Dump and analyze network traffic.
See http://www.wireshark.org for more information.
```

```
Copyright 1998-2014 Gerald Combs <gerald@wireshark.org> and
contributors.
This is free software; see the source for copying conditions. There is
NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR
PURPOSE.
```

Usage: tshark [options] ...

```
Capture interface:
  -i <interface>           name or idx of interface (def: first non-
loopback)
  -f <capture filter>       packet filter in libpcap filter syntax
  -s <snaplen>              packet snapshot length (def: 65535)
  -p                         don't capture in promiscuous mode
  -I                         capture in monitor mode, if available
  -B <buffer size>          size of kernel buffer (def: 1MB)
  -y <link type>            link layer type (def: first appropriate)
  -D                         print list of interfaces and exit
  -L                         print list of link-layer types of iface and
exit

Capture stop conditions:
  -c <packet count>         stop after n packets (def: infinite)
  -a <autostop cond.> ...    duration:NUM - stop after NUM seconds
                             filesize:NUM - stop this file after NUM KB
                             files:NUM - stop after NUM files

Capture output:
  -b <ringbuffer opt.> ...  duration:NUM - switch to next file after
NUM secs
                             filesize:NUM - switch to next file after
NUM KB
```

```

files:NUM - ringbuffer: replace after
NUM files
RPCAP options:
  -A <user>:<password>      use RPCAP password authentication
Input file:
  -r <infile>                 set the filename to read from (no stdin!)

Processing:
  -2                           perform a two-pass analysis
  -R <read filter>           packet Read filter in Wireshark display
filter syntax
  -Y <display filter>        packet display filter in Wireshark display
filter
  -n                           syntax
                                disable all name resolutions (def: all
enabled)
  -N <name resolve flags>    enable specific name resolution(s): "mntC"
  -d <layer_type>==<selector>,<decode_as_protocol> ...
                                "Decode As", see the man page for details
                                Example: tcp.port==8888,http
                                read a list of entries from a hosts file,
                                then be written to a capture file. (Implies

Output:
  -w <outfile|->              write packets to a pcap-format file named
"outfile"
  -C <config profile>
  -F <output file type>

types
  -V                           add output of packet tree          (Packet
Details)
  -O <protocols>              Only show packet details of these
                                protocols, comma
                                separated
                                print packet summary even when writing to a
                                file
  -S <separator>              the line separator to print between packets
                                -x
                                add output of hex and ASCII dump (Packet
Bytes)
  -T pdml|ps|psml|text|fields
                                format of text output (def: text)
                                -e <field>                  field to print if -Tfields selected (e.g.
tcp.port,
                                _ws.col.Info)
                                this option can be repeated to print
multiple fields
  -E<fieldoption>=<value>   set options for output when -Tfields
selected:
  header=y|n                   switch headers on and off

```

```

separator=/t|/s|<char> select tab, space, printable character as
separator
  occurrence=f|l|a      print first, last or all occurrences of
each field
  aggregator=,|/s|<char> select comma, space, printable character
as
  quote=d|s|n
  -t a|ad|d|dd|e|r|u|ud
to first)
  -u s|hms
  -l
  -q
statistics)
  -Q
than -q)
  -g
file(s)
  -W n
supported.

information
  -X <key>:<value>
details
  -z <statistics>
details
--capture-comment <comment>
add a capture comment to the newly created
output file (only for pcapng)

Miscellaneous:
  -h
  -v
  -o <name>:<value> ...
  -K <keytab>
  -G [report]
exit
display this help and exit
display version info and exit
override preference setting
keytab file to use for kerberos decryption
dump one of several available reports and
default report="fields"
use "-G ?" for more help

```

### D.3. tcpdump: Capturing with tcpdump for viewing with Wireshark

It's often more useful to capture packets using tcpdump rather than wireshark. For example, you might want to do a remote capture and either don't have GUI access or don't have Wireshark installed on the remote machine.

Older versions of tcpdump truncate packets to 68 or 96 bytes. If this is the case, use -s to capture full-sized packets:

```
$ tcpdump -i <interface> -s 65535 -w <some-file>
```

You will have to specify the correct interface and the name of a file to save into. In addition, you will have to terminate the capture with ^C when you believe you have captured enough packets.

tcpdump is not part of the Wireshark distribution. You can get it from <http://www.tcpdump.org> or as a standard package in most Linux distributions.

#### D.4. dumpcap: Capturing with dumpcap for viewing with Wireshark

Dumpcap is a network traffic dump tool. It captures packet data from a live network and writes the packets to a file. Dumpcap's native capture file format is libpcap format, which is also the format used by Wireshark, tcpdump and various other tools.

Without any options set it will use the pcap library to capture traffic from the first available network interface and write the received raw packet data, along with the packets' time stamps into a libpcap file.

Packet capturing is performed with the pcap library. The capture filter syntax follows the rules of the pcap library.

#### Example D.2. Help information available from dumpcap

```
Dumpcap 1.12.0 (v1.12.0-rc2-59-g7ea0d6c from master-1.12)
Capture network packets and dump them into a pcapng file.
See http://www.wireshark.org for more information.
```

Usage: dumpcap [options] ...

```
Capture interface:
  -i <interface>           name or idx of interface (def: first non-
                           loopback)
                           or for remote capturing, use one of these
formats:
  -f <capture filter>      rpcap://<host>/<interface>
                           TCP@<host>:<port>
                           packet filter in libpcap filter syntax
  -s <snaplen>             packet snapshot length (def: 65535)
  -p                         don't capture in promiscuous mode
  -I                         capture in monitor mode, if available
  -B <buffer size>          size of kernel buffer in MB (def: 2MB)
  -y <link type>            link layer type (def: first appropriate)
  -D                         print list of interfaces and exit
  -L                         print list of link-layer types of iface and
exit
  -d                         print generated BPF code for capture filter
  -k                         set channel on wifi interface <freq>,
[<type>]
  -S                         print statistics for each interface once
per second
  -M                         for -D, -L, and -S, produce machine-
readable output
```

```

RPCAP options:
  -r                      don't ignore own RPCAP traffic in capture
  -u                      use UDP for RPCAP data transfer
  -A <user>:<password>    use RPCAP password authentication
  -m <sampling type>      use packet sampling
                           count:NUM - capture one packet of every NUM
                           timer:NUM - capture no more than 1 packet

in NUM ms

Stop conditions:
  -c <packet count>      stop after n packets (def: infinite)
  -a <autostop cond.> ... duration:NUM - stop after NUM seconds
                           filesize:NUM - stop this file after NUM KB
                           files:NUM - stop after NUM files

Output (files):
  -w <filename>           name of file to save (def: tempfile)
  -g                       enable group read access on the output
file(s)
  -b <ringbuffer opt.> ... duration:NUM - switch to next file after
NUM secs
                           filesize:NUM - switch to next file after
                           NUM KB
                           files:NUM - ringbuffer: replace after
                           NUM files
  -n                       use pcapng format instead of pcap (default)
  -P                       use libpcap format instead of pcapng
--capture-comment <comment> add a capture comment to the output file
                           (only for pcapng)

Miscellaneous:
  -N <packet_limit>      maximum number of packets buffered within
dumpcap
  -C <byte_limit>         maximum number of bytes used for buffering
packets
                           within dumpcap
  -t                       use a separate thread per interface
  -q                       don't report packet capture counts
  -v                       print version information and exit
  -h                       display this help and exit

```

Example: `dumpcap -i eth0 -a duration:60 -w output.pcapng`  
 "Capture packets from interface eth0 until 60s passed into  
`output.pcapng`"

Use Ctrl-C to stop capturing at any time.

## D.5. capinfos: Print information about capture files

Included with Wireshark is a small utility called **capinfos**, which is a command-line utility to print information about binary capture files.

### **Example D.3. Help information available from capinfos**

```
Capinfos 1.12.0 (v1.12.0-rc2-59-g7ea0d6c from master-1.12)
Prints various information (infos) about capture files.
See http://www.wireshark.org for more information.
```

Usage: capinfos [options] <infile> ...

General infos:

- t display the capture file type
- E display the capture file encapsulation
- H display the SHA1, RMD160, and MD5 hashes of the file
- k display the capture comment

Size infos:

- c display the number of packets
- s display the size of the file (in bytes)
- d display the total length of all packets (in bytes)
- l display the packet size limit (snapshot length)

Time infos:

- u display the capture duration (in seconds)
- a display the capture start time
- e display the capture end time
- o display the capture file chronological status (True/False)
- S display start and end times as seconds

Statistic infos:

- y display average data rate (in bytes/sec)
- i display average data rate (in bits/sec)
- z display average packet size (in bytes)
- x display average packet rate (in packets/sec)

Output format:

- L generate long report (default)
- T generate table report
- M display machine-readable values in long reports

Table report options:

- R generate header record (default)
- r do not generate header record
- B separate infos with TAB character (default)
- m separate infos with comma (,) character
- b separate infos with SPACE character
- N do not quote infos (default)
- q quote infos with single quotes ('')
- Q quote infos with double quotes ("")

Miscellaneous:

```
-h display this help and exit
-C cancel processing if file open fails (default is to continue)
-A generate all infos (default)
```

Options are processed from left to right order with later options superceding or adding to earlier options.

If no options are given the default is to display all infos in long report output format.

## D.6. rawshark: Dump and analyze network traffic.

Rawshark reads a stream of packets from a file or pipe, and prints a line describing its output, followed by a set of matching fields for each packet on stdout.

### Example D.4. Help information available from rawshark

```
Rawshark 1.12.0 (v1.12.0-rc2-59-g7ea0d6c from master-1.12)
Dump and analyze network traffic.
See http://www.wireshark.org for more information.
```

```
Copyright 1998-2014 Gerald Combs <gerald@wireshark.org> and
contributors.
This is free software; see the source for copying conditions. There is
NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR
PURPOSE.
```

Usage: rawshark [options] ...

```
Input file:
-r <infile>           set the pipe or file name to read from

Processing:
-d <encap:linktype>|<proto:protoname>
                         packet encapsulation or protocol
-F <field>             field to display
-n
enabled)                disable all name resolution (def: all
-N <name resolve flags> enable specific name resolution(s): "mntC"
-p
use the system's packet header format
(which may have 64-bit timestamps)
-R <read filter>       packet filter in Wireshark display filter
syntax
-s
skip PCAP header on input

Output:
-l
flush output after each packet
```

```

-S                               format string for fields
                                (%D - name, %S - stringval, %N numval)
-t ad|a|r|d|dd|e               output format of time stamps (def: r: rel.
to first)

Miscellaneous:
-h                               display this help and exit
-o <name>:<value> ...        override preference setting
-v                               display version info and exit

```

## D.7. editcap: Edit capture files

Included with Wireshark is a small utility called **editcap**, which is a command-line utility for working with capture files. Its main function is to remove packets from capture files, but it can also be used to convert capture files from one format to another, as well as to print information about capture files.

### Example D.5. Help information available from editcap

```

Editcap 1.12.0 (v1.12.0-rc2-59-g7ea0d6c from master-1.12)
Edit and/or translate the format of capture files.
See http://www.wireshark.org for more information.

```

```

Usage: editcap [options] ... <infile> <outfile> [ <packet#>[-
<packet#>] ... ]

```

```

<infile> and <outfile> must both be present.
A single packet or a range of packets can be selected.

```

#### Packet selection:

- <b>r</b> delete them. - <b>A</b> <start time> (or equal hh:mm:ss). - <b>B</b> <stop time> the	keep the selected packets; default is to only output packets whose timestamp is after to) the given time (format as YYYY-MM-DD only output packets whose timestamp is before given time (format as YYYY-MM-DD hh:mm:ss).
---	--

#### Duplicate packet removal:

- <b>d</b> - <b>D</b> <dup window> window>  option) is  - <b>w</b> <dup time window> EQUAL TO OR	remove packet if duplicate (window == 5). remove packet if duplicate; configurable <dup Valid <dup window> values are 0 to 1000000. NOTE: A <dup window> of 0 with -v (verbose useful to print MD5 hashes. remove packet if duplicate packet is found
---	--

packet.  
seconds  
LESS THAN <dup time window> prior to current  
A <dup time window> is specified in relative  
(e.g. 0.000001).

with  
expected.  
have the  
NOTE: The use of the 'Duplicate packet removal' options  
other editcap options except -v may not always work as  
Specifically the -r, -t or -S options will very likely NOT  
desired effect if combined with the -d, -D or -w.

#### Packet manipulation:

-s <snaplen> truncate each packet to max. <snaplen> bytes  
of data.  
-C [offset:]<choplen> chop each packet by <choplen> bytes. Positive  
values  
at the  
length,  
that value.  
beginning,  
can use  
chopping  
least 1  
negative.  
-L  
snapping  
-t <time adjustment> adjust the frame length when chopping and/or  
(e.g. -0.5).  
-S <strict adjustment> adjust timestamp of packets if necessary to  
insure  
<strict  
with  
reasonable.  
timestamps so  
value  
adjust the timestamp of each packet;  
<time adjustment> is in relative seconds  
strict chronological increasing order. The  
adjustment> is specified in relative seconds  
values of 0 or 0.000001 being the most  
A negative adjustment value will modify  
that each packet's delta time is the absolute

of the adjustment specified. A value of -0 will set all packets to the timestamp of the first packet.

-E <error probability> set the probability (between 0.0 and 1.0 incl.) that a particular packet byte will be randomly changed.

**Output File(s):**

- c <packets per file> split the packet output to different files based on uniform packet counts with a maximum of <packets per file> each.
- i <seconds per file> split the packet output to different files based on uniform time intervals with a maximum of <seconds per file> each.
- F <capture type> set the output file type; default is pcapng.

An empty "-F" option will list the file types.

-T <encap type> set the output file encapsulation type; default is the same as the input file. An empty "-T" option will list the encapsulation types.

**Miscellaneous:**

- h display this help and exit.
- v verbose output.

Packet Removal' options (-d, -D or -w) then Packet lengths and MD5 hashes are printed to standard-error.

#### Example D.6. Capture file types available from editcap

```
$ editcap -F
editcap: option requires an argument -- 'F'
editcap: The available capture file types for the "-F" flag are:
 5views - InfoVista 5View capture
 btsnoop - Symbian OS btsnoop
 commview - TamoSoft CommView
 dct2000 - Catapult DCT2000 trace (.out format)
 erf - Endace ERF capture
 eyesdn - EyeSDN USB S0/E1 ISDN trace format
 k12text - K12 text file
```

```
lanalyzer - Novell LANalyzer
logcat - Android Logcat Binary format
logcat-brief - Android Logcat Brief text format
logcat-long - Android Logcat Long text format
logcat-process - Android Logcat Process text format
logcat-tag - Android Logcat Tag text format
logcat-thread - Android Logcat Thread text format
logcat-threadtime - Android Logcat Threadtime text format
logcat-time - Android Logcat Time text format
modlibpcap - Modified tcpdump - libpcap
netmon1 - Microsoft NetMon 1.x
netmon2 - Microsoft NetMon 2.x
nettl - HP-UX nettl trace
ngsniffer - Sniffer (DOS)
ngwsniffer_1_1 - NetXray, Sniffer (Windows) 1.1
ngwsniffer_2_0 - Sniffer (Windows) 2.00x
niobserver - Network Instruments Observer
nokialibpcap - Nokia tcpdump - libpcap
nseclibpcap - Wireshark - nanosecond libpcap
nstrace10 - NetScaler Trace (Version 1.0)
nstrace20 - NetScaler Trace (Version 2.0)
nstrace30 - NetScaler Trace (Version 3.0)
pcap - Wireshark/tcpdump/... - pcap
pcapng - Wireshark/... - pcapng
rf5 - Tektronix K12xx 32-bit .rf5 format
rh6_llibpcap - RedHat 6.1 tcpdump - libpcap
snoop - Sun snoop
suse6_3libpcap - SuSE 6.3 tcpdump - libpcap
visual - Visual Networks traffic capture
```

#### **Example D.7. Encapsulation types available from editcap**

```
$ editcap -T
editcap: option requires an argument -- 'T'
editcap: The available encapsulation types for the "-T" flag are:
    ap1394 - Apple IP-over-IEEE 1394
    arcnet - ARCNET
    arcnet_linux - Linux ARCNET
    ascend - Lucent/Ascend access equipment
    atm-pdus - ATM PDUs
    atm-pdus-untruncated - ATM PDUs - untruncated
    atm-rfc1483 - RFC 1483 ATM
    ax25 - Amateur Radio AX.25
    ax25-kiss - AX.25 with KISS header
    bacnet-ms-tp - BACnet MS/TP
    bacnet-ms-tp-with-direction - BACnet MS/TP with Directional Info
```

ber - ASN.1 Basic Encoding Rules  
bluetooth-bredr-bb-rf - Bluetooth BR/EDR Baseband RF  
bluetooth-h4 - Bluetooth H4  
bluetooth-h4-linux - Bluetooth H4 with linux header  
bluetooth-hci - Bluetooth without transport layer  
bluetooth-le-ll - Bluetooth Low Energy Link Layer  
bluetooth-le-ll-rf - Bluetooth Low Energy Link Layer RF  
bluetooth-linux-monitor - Bluetooth Linux Monitor  
can20b - Controller Area Network 2.0B  
chdlc - Cisco HDLC  
chdlc-with-direction - Cisco HDLC with Directional Info  
cosine - CoSine L2 debug log  
dbus - D-Bus  
dct2000 - Catapult DCT2000  
docsis - Data Over Cable Service Interface Specification  
dpnss\_link - Digital Private Signalling System No 1 Link Layer  
dvbcii - DVB-CI (Common Interface)  
enc - OpenBSD enc(4) encapsulating interface  
epon - Ethernet Passive Optical Network  
erf - Extensible Record Format  
ether - Ethernet  
ether-nettl - Ethernet with nettl headers  
fc2 - Fibre Channel FC-2  
fc2sof - Fibre Channel FC-2 With Frame Delimiter  
fddi - FDDI  
fddi-nettl - FDDI with nettl headers  
fddi-swapped - FDDI with bit-swapped MAC addresses  
flexray - FlexRay  
frelay - Frame Relay  
frelay-with-direction - Frame Relay with Directional Info  
gcom-serial - GCOM Serial  
gcom-tie1 - GCOM TIE1  
gprs-llc - GPRS LLC  
gsm\_um - GSM Um Interface  
hhdlc - HiPath HDLC  
i2c - I2C  
ieee-802-11 - IEEE 802.11 Wireless LAN  
ieee-802-11-airopeek - IEEE 802.11 plus AiroPeek radio header  
ieee-802-11-avs - IEEE 802.11 plus AVS radio header  
ieee-802-11-netmon - IEEE 802.11 plus Network Monitor radio header  
ieee-802-11-prism - IEEE 802.11 plus Prism II monitor mode radio  
header  
    ieee-802-11-radio - IEEE 802.11 Wireless LAN with radio  
    information  
        ieee-802-11-radiotap - IEEE 802.11 plus radiotap radio header  
        ieee-802-16-mac-cps - IEEE 802.16 MAC Common Part Sublayer  
        infiniband - InfiniBand  
        ios - Cisco IOS internal  
        ip-over-fc - RFC 2625 IP-over-Fibre Channel  
        ip-over-ib - IP over Infiniband  
        ipfix - IPFIX  
        ipmb - Intelligent Platform Management Bus

ipmi-trace - IPMI Trace Data Collection  
ipnet - Solaris IPNET  
irda - IrDA  
isdn - ISDN  
ixveriwave - IxVeriWave header and stats block  
jfif - JPEG/JFIF  
juniper-atm1 - Juniper ATM1  
juniper-atm2 - Juniper ATM2  
juniper-chdlc - Juniper C-HDLC  
juniper-ether - Juniper Ethernet  
juniper-frelay - Juniper Frame-Relay  
juniper-ggsn - Juniper GGSN  
juniper-mlfr - Juniper MLFR  
juniper-mlPPP - Juniper MLPPP  
juniper-ppp - Juniper PPP  
juniper-pppoe - Juniper PPPoE  
juniper-svcs - Juniper Services  
juniper-vp - Juniper Voice PIC  
k12 - K12 protocol analyzer  
lapb - LAPB  
lapd - LAPD  
layer1-event - EyeSDN Layer 1 event  
lin - Local Interconnect Network  
linux-atm-clip - Linux ATM CLIP  
linux-lapd - LAPD with Linux pseudo-header  
linux-sll - Linux cooked-mode capture  
logcat - Android Logcat Binary format  
logcat\_brief - Android Logcat Brief text format  
logcat\_long - Android Logcat Long text format  
logcat\_process - Android Logcat Process text format  
logcat\_tag - Android Logcat Tag text format  
logcat\_thread - Android Logcat Thread text format  
logcat\_threadtime - Android Logcat Threadtime text format  
logcat\_time - Android Logcat Time text format  
ltalk - Localtalk  
mime - MIME  
most - Media Oriented Systems Transport  
mp2ts - ISO/IEC 13818-1 MPEG2-TS  
mpeg - MPEG  
mtp2 - SS7 MTP2  
mtp2-with-phdr - MTP2 with pseudoheader  
mtp3 - SS7 MTP3  
mux27010 - MUX27010  
netanalyzer - netANALYZER  
netanalyzer-transparent - netANALYZER-Transparent  
netlink - Linux Netlink  
nfc-llcp - NFC LLCP  
nflog - NFLOG  
nstrace10 - NetScaler Encapsulation 1.0 of Ethernet  
nstrace20 - NetScaler Encapsulation 2.0 of Ethernet  
nstrace30 - NetScaler Encapsulation 3.0 of Ethernet  
null - NULL

packetlogger - PacketLogger  
pflog - OpenBSD PF Firewall logs  
pflog-old - OpenBSD PF Firewall logs, pre-3.4  
pktap - Apple PKTAP  
ppi - Per-Packet Information header  
ppp - PPP  
ppp-with-direction - PPP with Directional Info  
pppoes - PPP-over-Ethernet session  
raw-icmp-nettl - Raw ICMP with nettl headers  
raw-icmpv6-nettl - Raw ICMPv6 with nettl headers  
raw-telnet-nettl - Raw telnet with nettl headers  
rawip - Raw IP  
rawip-nettl - Raw IP with nettl headers  
rawip4 - Raw IPv4  
rawip6 - Raw IPv6  
redback - Redback SmartEdge  
rtac-serial - RTAC serial-line  
s4607 - STANAG 4607  
s5066-dpdu - STANAG 5066 Data Transfer Sublayer PDUs (D\_PDU)  
sccp - SS7 SCCP  
sctp - SCTP  
sdh - SDH  
sdlc - SDLC  
sita-wan - SITA WAN packets  
slip - SLIP  
socketcan - SocketCAN  
symantec - Symantec Enterprise Firewall  
tnef - Transport-Neutral Encapsulation Format  
tr - Token Ring  
tr-nettl - Token Ring with nettl headers  
tzsp - Tazmen sniffer protocol  
unknown - Unknown  
unknown-nettl - Unknown link-layer type with nettl headers  
usb - Raw USB packets  
usb-linux - USB packets with Linux header  
usb-linux-mmap - USB packets with Linux header and padding  
usb-usbpcap - USB packets with USBPcap header  
user0 - USER 0  
user1 - USER 1  
user2 - USER 2  
user3 - USER 3  
user4 - USER 4  
user5 - USER 5  
user6 - USER 6  
user7 - USER 7  
user8 - USER 8  
user9 - USER 9  
user10 - USER 10  
user11 - USER 11  
user12 - USER 12  
user13 - USER 13  
user14 - USER 14

```
user15 - USER 15
v5-ef - V5 Envelope Function
whdlc - Wellfleet HDLC
wireshark-upper-pdu - Wireshark Upper PDU export
wpan - IEEE 802.15.4 Wireless PAN
wpan-nofcs - IEEE 802.15.4 Wireless PAN with FCS not present
wpan-nonask-phy - IEEE 802.15.4 Wireless PAN non-ASK PHY
x2e-serial - X2E serial line capture
x2e-xoraya - X2E Xoraya
```

## D.8. mergecap: Merging multiple capture files into one

Mergecap is a program that combines multiple saved capture files into a single output file specified by the -w argument. Mergecap knows how to read libpcap capture files, including those of tcpdump. In addition, Mergecap can read capture files from snoop (including Shomiti) and atmsnoop, LanAlyzer, Sniffer (compressed or uncompressed), Microsoft Network Monitor, AIX's iptrace, NetXray, Sniffer Pro, RADCOM's WAN/LAN analyzer, Lucent/Ascend router debug output, HP-UX's nettl, and the dump output from Toshiba's ISDN routers. There is no need to tell Mergecap what type of file you are reading; it will determine the file type by itself. Mergecap is also capable of reading any of these file formats if they are compressed using gzip. Mergecap recognizes this directly from the file; the '.gz' extension is not required for this purpose.

By default, it writes the capture file in libpcap format, and writes all of the packets in the input capture files to the output file. The -F flag can be used to specify the format in which to write the capture file; it can write the file in libpcap format (standard libpcap format, a modified format used by some patched versions of libpcap, the format used by Red Hat Linux 6.1, or the format used by SuSE Linux 6.3), snoop format, uncompressed Sniffer format, Microsoft Network Monitor 1.x format, and the format used by Windows-based versions of the Sniffer software.

Packets from the input files are merged in chronological order based on each frame's timestamp, unless the -a flag is specified. Mergecap assumes that frames within a single capture file are already stored in chronological order. When the -a flag is specified, packets are copied directly from each input file to the output file, independent of each frame's timestamp.

If the -s flag is used to specify a snapshot length, frames in the input file with more captured data than the specified snapshot length will have only the amount of data specified by the snapshot length written to the output file. This may be useful if the program that is to read the output file cannot handle packets larger than a certain size (for example, the versions of snoop in Solaris 2.5.1 and Solaris 2.6 appear to reject Ethernet frames larger than the standard Ethernet MTU, making them incapable of handling gigabit Ethernet captures if jumbo frames were used).

If the -T flag is used to specify an encapsulation type, the encapsulation type of the output capture file will be forced to the specified type, rather than being the type appropriate to the encapsulation type of the input capture file. Note that this merely forces the encapsulation type of the output file to be the specified type; the packet headers of the packets will not be translated from the encapsulation type of the input capture file to the specified encapsulation type (for example, it will not translate an Ethernet capture to an FDDI capture if an Ethernet capture is read and '-T fddi' is specified).

### **Example D.8. Help information available from mergecap**

```
Mergecap 1.12.0 (v1.12.0-rc2-59-g7ea0d6c from master-1.12)
```

```
Merge two or more capture files into one.
```

```
See http://www.wireshark.org for more information.
```

```
Usage: mergecap [options] -w <outfile>|- <infile> [<infile> ...]
```

#### **Output:**

```
-a          concatenate rather than merge files.  
           default is to merge based on frame timestamps.  
-s <snaplen>  truncate packets to <snaplen> bytes of data.  
-w <outfile>|- set the output filename to <outfile> or '-' for  
stdout.  
-F <capture type> set the output file type; default is pcapng.  
           an empty "-F" option will list the file types.  
-T <encap type>  set the output file encapsulation type;  
           default is the same as the first input file.  
           an empty "-T" option will list the encapsulation  
types.
```

#### **Miscellaneous:**

```
-h          display this help and exit.  
-v          verbose output.
```

A simple example merging `dhcp-capture.libpcap` and `imap-1.libpcap` into `outfile.libpcap` is shown below.

### **Example D.9. Simple example of using mergecap**

```
$ mergecap -w outfile.libpcap dhcp-capture.libpcap imap-1.libpcap
```

## **D.9. text2pcap: Converting ASCII hexdumps to network captures**

There may be some occasions when you wish to convert a hex dump of some network traffic into a libpcap file.

**Text2pcap** is a program that reads in an ASCII hex dump and writes the data described into a libpcap-style capture file. `text2pcap` can read hexdumps with multiple packets in them, and build a capture file of multiple packets. `text2pcap` is also capable of generating dummy Ethernet, IP and UDP headers, in order to build fully processable packet dumps from hexdumps of application-level data only.

`Text2pcap` understands a hexdump of the form generated by `od -A x -t x1`. In other words, each byte is individually displayed and surrounded with a space. Each line begins with an offset describing the position in the file. The offset is a hex number (can also be octal - see `-o`), of more than two hex digits. Here is a sample dump that `text2pcap` can recognize:

```

000000 00 e0 1e a7 05 6f 00 10 .....
000008 5a a0 b9 12 08 00 46 00 .....
000010 03 68 00 00 00 00 0a 2e .....
000018 ee 33 0f 19 08 7f 0f 19 .....
000020 03 80 94 04 00 00 10 01 .....
000028 16 a2 0a 00 03 50 00 0c .....
000030 01 01 0f 19 03 80 11 01 .....

```

There is no limit on the width or number of bytes per line. Also the text dump at the end of the line is ignored. Bytes/hex numbers can be uppercase or lowercase. Any text before the offset is ignored, including email forwarding characters '>'. Any lines of text between the bytestring lines is ignored. The offsets are used to track the bytes, so offsets must be correct. Any line which has only bytes without a leading offset is ignored. An offset is recognized as being a hex number longer than two characters. Any text after the bytes is ignored (e.g. the character dump). Any hex numbers in this text are also ignored. An offset of zero is indicative of starting a new packet, so a single text file with a series of hexdumps can be converted into a packet capture with multiple packets. Multiple packets are read in with timestamps differing by one second each. In general, short of these restrictions, text2pcap is pretty liberal about reading in hexdumps and has been tested with a variety of mangled outputs (including being forwarded through email multiple times, with limited line wrap etc.)

There are a couple of other special features to note. Any line where the first non-whitespace character is '#' will be ignored as a comment. Any line beginning with #TEXT2PCAP is a directive and options can be inserted after this command to be processed by text2pcap. Currently there are no directives implemented; in the future, these may be used to give more fine grained control on the dump and the way it should be processed e.g. timestamps, encapsulation type etc.

Text2pcap also allows the user to read in dumps of application-level data, by inserting dummy L2, L3 and L4 headers before each packet. Possibilities include inserting headers such as Ethernet, Ethernet + IP, Ethernet + IP + UDP, or Ethernet + Ip + TCP before each packet. This allows Wireshark or any other full-packet decoder to handle these dumps.

#### **Example D.10. Help information available from text2pcap**

```

Text2pcap 1.12.0 (v1.12.0-rc2-59-g7ea0d6c from master-1.12)
Generate a capture file from an ASCII hexdump of packets.
See http://www.wireshark.org for more information.

```

```
Usage: text2pcap [options] <infile> <outfile>
```

```
where  <infile> specifies input filename (use - for standard input)
      <outfile> specifies output filename (use - for standard output)
```

Input:

<code>-o hex oct dec</code> <code>-t &lt;timefmt&gt;</code> date/time code;  the sort	parse offsets as (h)ex, (o)ctal or (d)ecimal; default is hex. treat the text before the packet as a the specified argument is a format string of supported by strftime.
---	---

format code

must be

remaining

second.

date/time are

-D  
or an O,

outbound.

PCAP-NG.

-a

identified

looks

not

Output:

-l <typenum>  
(Ethernet). See

list of

complete

wish to

-m <max-packet>

Prepend dummy header:

-e <l3pid>  
specified L3PID

-i <proto>  
protocol

well.

Example: The time "10:15:14.5476" has the

"%H:%M:%S."

NOTE: The subsecond component delimiter, '.',

given, but no pattern is required; the

number is assumed to be fractions of a

NOTE: Date/time fields from the current

used as the default for unspecified fields.  
the text before the packet starts with an I

indicating that the packet is inbound or

This is only stored if the output format is

enable ASCII text dump identification.

The start of the ASCII text dump can be

and excluded from the packet data, even if it

like a HEX dump.

NOTE: Do not enable it if the input file does  
contain the ASCII text dump.

link-layer type number; default is 1

<http://www.tcpdump.org/linktypes.html> for a  
numbers. Use this option if your dump is a  
hex dump of an encapsulated packet and you

specify the exact type of encapsulation.

Example: -l 7 for ARCNet packets.

max packet length in output; default is 65535

prepend dummy Ethernet II header with

(in HEX).

Example: -e 0x806 to specify an ARP packet.

prepend dummy IP header with specified IP

(in DECIMAL).

Automatically prepends Ethernet header as

Example: -i 46

```

-4 <srcip>,<destip>      prepend dummy IPv4 header with specified
                             dest and source address.
                             Example: -4 10.0.0.1,10.0.0.2

-6 <srcip>,<destip>      replace IPv6 header with specified
                             dest and source address.
                             Example: -6
fe80:0:0:0:202:b3ff:fe1e:8329,2001:0db8:85a3:0000:0000:8a2e:0370:7334
-u <srcp>,<destp>        prepend dummy UDP header with specified
                             source and destination ports (in DECIMAL).
                             Automatically prepends Ethernet & IP headers
as well.

Example: -u 1000,69 to make the packets look
like

-T <srcp>,<destp>        TFTP/UDP packets.
                             prepend dummy TCP header with specified
                             source and destination ports (in DECIMAL).
                             Automatically prepends Ethernet & IP headers
as well.

Example: -T 50,60

-s <srcp>,<dstp>,<tag>  prepend dummy SCTP header with specified
                             source/dest ports and verification tag (in
DECIMAL).

Example: -s 30,40,34

-S <srcp>,<dstp>,<ppi>  prepend dummy SCTP header with specified
                             source/dest ports and verification tag 0.
                             Automatically prepends a dummy SCTP DATA
                             chunk header with payload protocol identifier
ppi.

Example: -S 30,40,34

Miscellaneous:
-h                         display this help and exit.
-d                         show detailed debug of parser states.
-q                         generate no output at all (automatically
disables -d).
-n                         use PCAP-NG instead of PCAP as output format.

```

## D.10. reordercap: Reorder a capture file

Reordercap allows to reorder a capture file according to the packets timestamp.

### Example D.11. Help information available from reordercap

```

Reordercap 1.12.0
Reorder timestamps of input file frames into output file.
See http://www.wireshark.org for more information.

```

Usage: reordercap [options] <infile> <outfile>

**Options:**

- n            don't write to output file if the input file is ordered.
- h            display this help and exit.