



МОНГОЛ УЛСЫН БОЛОВСРОЛЫН ИХ СУРГУУЛЬ
МАТЕМАТИК, БАЙГАЛИЙН УХААНЫ СУРГУУЛЬ

МЭДЭЭЛЭЛ ЗҮЙН ТЭНХИМ

Энхсайхан ЭНХЖАРГАЛ

WIRESHARK АШИГЛАН СҮЛЖЭЭНИЙ
УРСГАЛД АНАЛИЗ ХИЙХ НЬ

D011401

БАКАЛАВРЫН ДИПЛОМЫН АЖИЛ

УЛААНБААТАР ХОТ

2020 ОН



МОНГОЛ УЛСЫН БОЛОВСРОЛЫН ИХ СУРГУУЛЬ
МАТЕМАТИК, БАЙГАЛИЙН УХААНЫ СУРГУУЛЬ

МЭДЭЭЛЭЛ ЗҮЙН ТЭНХИМ

Хадныхан

Энхсайхан ЭНХЖАРГАЛ

WIRESHARK АШИГЛАН СҮЛЖЭЭНИЙ
УРСГАЛД АНАЛИЗ ХИЙХ НЬ

D011401

БАКАЛАВРЫН ДИПЛОМЫН АЖИЛ

УДИРДАГЧ:

Ц.НЯМСҮРЭН/МАГИСТР/

ШҮҮМЖЛЭГЧ:

С.ЭРХБАЯР/МАГИСТР/

УЛААНБААТАР ХОТ

2020 ОН

ГАРЧИГ

УДИРТГАЛ	1
БҮЛЭГ I. ОНОЛЫН СУДАЛГАА	2
1.1 Wireshark гэж юу вэ?	2
1.2 Wireshark програмын товч түүх	2
1.3 Wireshark програмын гүйцэтгэх үүрэг, онцлог	3
1.4. Wireshark програмыг суулгах заавар	5
1.5. Үндсэн цонхны тайлбар.....	6
1.5.1.Цэс (Menu) Вайршарк (wireshark) програмын үндсэн цэс.....	8
1.5.2.Edit цэс	13
1.5.3.View цэс	16
1.5.4.Go цэс.....	21
1.5.5.Capture цэс.....	23
1.5.6.Analyze цэс	24
1.5.7.Statistics цэс	27
1.5.8.Tools цэс	28
1.5.9. Internals цэс	28
1.5.10. Help цэс	29
1.6.Үндсэн товчлуурууд (Main Toolbar)	30
БҮЛЭГ 2. ТУРШИЛТ СУДАЛГААНЫ ХЭСЭГ	34
2.1 Судалгааны өгөгдөл цуглуулах.....	34
2.1.1. Wireshark програм ашиглан өгөгдөл чагнах алхамчилсан заавар	34
2.1.2. Wireshark програм ашиглан өгөгдөл чагнах видео заавар	35
2.2. Чагнасан файлтай ажиллах	36
2.2.1. HTTP протоколоор шүүлт хийх видео заавар	36
2.2.2. HTTP Протоколоор шүүлт хийх алхамчилсан заавар.....	37
2.2.3. Сүлжээгээр дамжсан зураг болон бусад файлыг задалж харах	37
2.2.4. Чагнасан файлаас зураг ялгаж харах видео заавар	39
ДҮГНЭЛТ	40
АШИГЛАСАН МАТЕРИАЛЫН ЖАГСААЛТ	41

УДИРТГАЛ

Өнөө үед бидний өдөр тутмын амьдрал интернетийн сүлжээнд холбогдсон төхөөрөмжгүйгээр төсөөлөгдөхийн аргагүй болоод байна. Интернетийн сүлжээг хэрэглэгчдийн тоо, интернет дамжиж буй мэдээллийн хэмжээ өдрөөс өдөрт өсөн нэмэгдсээр байгаа нь өнөө үеийн залуус биднийг интернет орчны мэдлэг, чадвартай байхыг шууд бусаар шаардах болсон байна. Энэ асуудал дээр үндэслэн компьютерийн сүлжээгээр дамжиж буй өгөгдлийг цуглуулах, хадгалах, задлан шинжлэх үйл ажиллагаа хийдэг ямар програм хангамж талаар байдаг судлах, мэдэж авах үүднээс энэхүү сэдвийг сонгосон болно.

Зорилго

Wireshark програм ашиглаж сурах, сүлжээгээр дамжиж буй өгөгдлийг чагнах, чагнасан файлтай ажиллах

Зорилт

- Сүлжээ чагнах Wireshark програмыг судлах
- Сүлжээгээр дамжиж буй өргөдлийг чагнах, бичиж авах
 - Компьютерийн лабораторийн 5 өдрийн өгөгдлийг чагнах, бичиж авах
 - Өөрийн компьютерийн 1 өдрийн өгөгдлийг бичиж авах
- Чагнасан файлтай ажиллах
 - Оюутнууд ямар сайтыг түлхүү ашигладгийг илрүүлэх
 - Сүлжээгээр дамжсан зураг болон бусад файлыг задалж харах

БҮЛЭГ I. ОНОЛЫН СУДАЛГАА

1.1 Wireshark гэж юу вэ?¹

Wireshark компьютерийн сүлжээгээр дамжиж буй өгөгдлийг цуглуулах, хадгалах, задлан шинжлэх үйл ажиллагаа хийдэг програм хангамж юм. Сүлжээний пакетад дүн шинжилгээ хийхдээ энэхүү програм нь сүлжээгээр дамжиж буй пакетуудыг чагнаж, цуглуулаад тэдгээр пакет өгөгдлийг боломжит хамгийн дэлгэрэнгүй байдлаар задлан харуулдаг.

1.2 Wireshark програмын товч түүх²

1997 онд Жералд Комбс сүлжээнд үүссэн асуудлыг хянах шаардлага үүссэн бөгөөд тэр бээр өөрийн хэрэгцээг хангахын тулд Ethereal (анхны вайршарк) хэмээх програмыг эхлүүлсэн. Эхэндээ энэхүү програмын хөгжүүлэлт нь удаан байсан бөгөөд 1998 оны 7 сар хүртэл хэд хэдэн удаа дундаа үйл ажиллагаагаа зогсоож байсан. Түүнээс хойших алдаа зэргийг олон нийтээс мэдээлж 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 tcp view програмаас илүү дээр зүйл хайж байсан бөгөөд улмаар 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 хүсэж буй протоколыг энэхүү програм дэмжиж байгаа эсэхийг хайж үзсэн. Гэтэл энэхүү задлагч хэсгүүд тийм ч хялбархан нэмэгдэх боломжгүй байсан юм. Тиймээс тэр бээр 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.

¹ <https://www.academia.edu/41226241/Wireshark>

² <https://www.academia.edu/41226241/Wireshark>

- 2006 онд энэхүү байршлаа 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.
- Wireshark програмын энэхүү хувилбар гарах үед вайршарк хөгжүүлэгчдийн болон хэрэглэгчдийн анхны хурал болох Шаркфест (sharkfest) болж байсан.

1.3 Wireshark програмын гүйцэтгэх үүрэг, онцлог³

Үүрэг зориулалт

- Сүлжээнд үүссэн асуудлыг оношлох, тодруулах
- Сүлжээний аюулгүй байдалтай холбоотой асуудлыг хянах, илрүүлэх
- Хөгжүүлэгчид шинэ протокол хөгжүүлэх, хэрэгжүүлэх явцдаа шалгах
- Компьютерийн сүлжээ хэрхэн ажилладаг талаар суралцаж буй хүмүүст сургалтын зориулалтаар ашиглах гэх мэт олон үүрэг зориулалтаар ашиглаж болно.

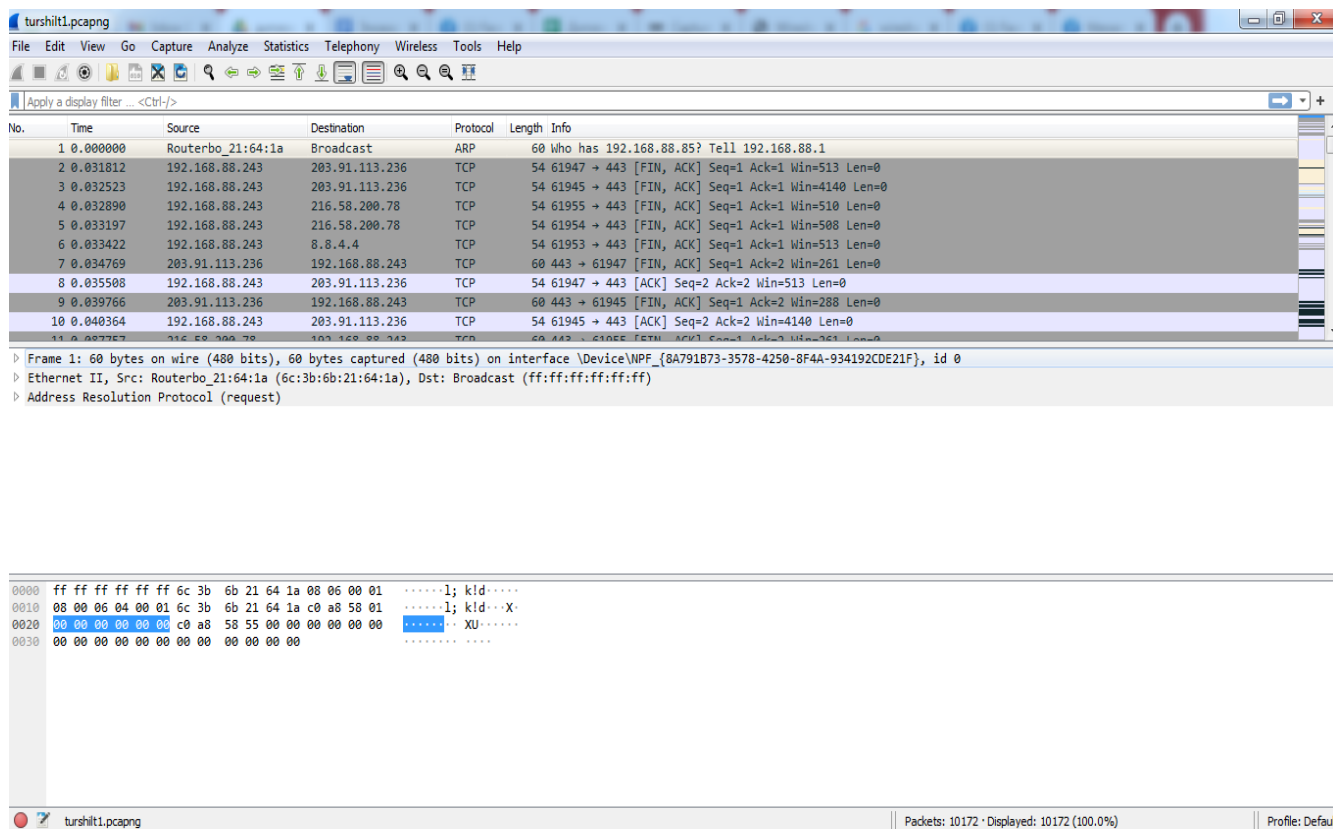
Wireshark-ын ажиллагааны онцлог

- Windows болон Unix үйлдлийн системүүд дээр ажиллана.
- Сүлжээний интерфейс картуудаар (Network Interface Card - NIC) дамжиж буй packet өгөгдлийг чагнан цуглуулж авна.
- Wireshark програмтай ижил үйлдэл хийдэг tcpdump/WinDump гэх мэт сүлжээний өгөгдөлд анализ хийх програмуудын цуглуулсан packet өгөгдлүүдийг нээнэ, анализ хийнэ.
- Packet өгөгдлийн 16-тын тооллын системээр илэрхийлэгдсэн (hex) файлаас вайршарк (wireshark) програм руу импорт хийнэ. Packet өгөгдлийг ашиглаж буй протоколоор нь дэлгэрэнгүйгээр харуулна.
- Цуглуулж авсан пакет өгөгдлийг хадгална.
- Цуглуулсан пакет 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.

³ <https://www.academia.edu/41226241/Wireshark>

WIRESHARK АШИГЛАН СҮЛЖЭЭНИЙ УРСГАЛД АНАЛИЗ ХИЙХ НЬ

- Олон төрлийн шалгуур үзүүлэлт, параметр ашиглан пакет (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 дороос хийх боломжтой.



ЗУРАГ 1. WIRESHARK ПРОГРАМ СҮЛЖЭЭГЭЭР ДАМЖИГДАЖ БУЙ ПАКЕТ (ПАКЕТ) ӨГӨГДЛИЙГТ ДЭЛГЭЦЭНД ХАРУУЛЖ БУЙ БАЙДАЛ.

Вайршарк (wireshark) програм дараах зүйлсийг хийхгүй.⁴

- **Халдлага илрүүлэхгүй** – Сүлжээгээр сэжигтэй, эсвэл халдлагын мэдээлэл дамжиж байгааг вайршарк (wireshark) програм танихгүй.
- Мөн хэрэглэгчид ямар нэгэн **анхааруулга өгөхгүй**. Хэрэглэгч өөрөө л эдгээр сэжигтэй пакет (packet) өгөгдлүүдийг хянах, анализ хийх үйлдлээ гар аргаар хийнэ.
- Wireshark програм нь пакет **өгөгдөл үүсгэхгүй** мөн сүлжээгээр ямар нэгэн **өгөгдөл дамжуулдаггүй**.
- Сүлжээ рүү чиглэсэн ямар нэгэн **идэвхтэй үйлдлийг хийдэггүй**.

1.4. Wireshark програмыг суулгах заавар⁵

Wireshark програмыг хэрэглэхийн тулд wireshark програмаа өөрийн системд суулгасан байх шаардлагатай.

Windows болон Mac OS үйлдлийн системүүд дээр ажиллаж байгаа тохиолдолд <https://www.wireshark.org/download.html> вэб хуудаснаас өөрийн системд тохирох файлыг татан авч шууд суулгана.

Linux эсвэл FreeBSD гэх мэт үйлдлийн системүүд дээр wireshark програмыг суулгахдаа эх код source code-оос нь install хийж суулгах боломжтой. Ихэнх Linux тархац дээр wireshark програмын package суулгац байдаг боловч эдгээр хувилбар нь хуучин байх магадлал өндөр байдаг. Тиймээс Linux тархац болон FreeBSD гэх мэт үйлдлийн системүүд дээр 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.

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

⁴ <https://www.academia.edu/41226241/Wireshark>

⁵ <https://www.academia.edu/41226241/Wireshark>

Эх код (source) болон бинар тархцуудыг (binary distributions)-ыг татаж авах

Эх код (source) мөн бинар тархцуудыг (binary distributions) вайршарк (wireshark)-ын вэб хуудаснаас / <https://www.wireshark.org/> / татаж авах боломжтой. Татаж авах холбоосоор ороод өөрт хэрэгтэй бинари (binary) эсвэл (source package)-г сонгоно. Хэрэв 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. Өмнө нь вайршарк (wireshark) програмыг суулгаж байсан бол заавал ингэх шаардлагагүй байж болно.

Виндовс (Windows) орчинд Вайршарк (wireshark) суулгах

Вайршарк (Wireshark) програмын Виндовс (windows) орчинд суух Windows installer файл нь үйлдлийн системийн платформ болон хувилбарыг өөрийн нэрдээ агуулдаг.

Жишээлбэл: **Wireshark-win32-1.12.7.exe** гэх мэт. Вайршарк (Wireshark) програмын суулгац нь өөрийн багцдаа WinPcap програмыг 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> вэб хуудаснаас татаж аваад windows installer буюу .exe өргөтгөлтэй файлыг ажиллуулахад автоматаар 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.

1.5. Үндсэн цонхны тайлбар

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

Вайршарк (Wireshark) програмыг 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

WIRESHARK АШИГЛАН СҮЛЖЭЭНИЙ УРСГАЛД АНАЛИЗ ХИЙХ НЬ

	харуулах самбар (Packet details pane)-т үзүүлж буй мэдээллийн дараагийнх хэсэг рүү шилжих
Up	Өмнөх пакет (packet) руу эсвэл Пакетын мэдээллийг дэлгэрэнгүй харуулах самбар (Packet details pane)-т үзүүлж буй мэдээллийн өмнөх мэдээллийн хэсэг рүү шилжих
Ctrl+Down, F8	Пакетыг жагсаан харуулах самбар (Packet list pane) хэсэгт пакет идэвхжээгүй 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 идэвхжээгүй 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 холбогдож 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 рүү 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 идэвхэжсэн 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 рүү үсэрнэ.
Return, Enter	Пакетын мэдээллийг дэлгэрэнгүй харуулах самбар (Packet Details Pane) хэсгийн мод (tree) хэлбэрийн бүтцийг нээж, хаах үйлдлийг хийдэг.
Дэлгэцийн аль хэсэг идэвхэжсэнээс үл хамааран үндсэн цонхон дээр бичсэн тэмдэгтүүд шүүлтүүрийн (filter) хэсэгт бичигддэг.	

1.5.1.Цэс (Menu) Вайршарк (wireshark) програмын үндсэн цэс

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 идэвхжихгүй. Ямар үед идэвхгүй байх вэ гэвэл жишээлбэл та аль хэдийн хадгалчихсан файлаа ямар нэгэн өөрчлөлт оруулалгүйгээр хадгалах гэх мэт.



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ЗУРАГ 2. WIRESHARK ҮНДСЭН ЦЭС

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

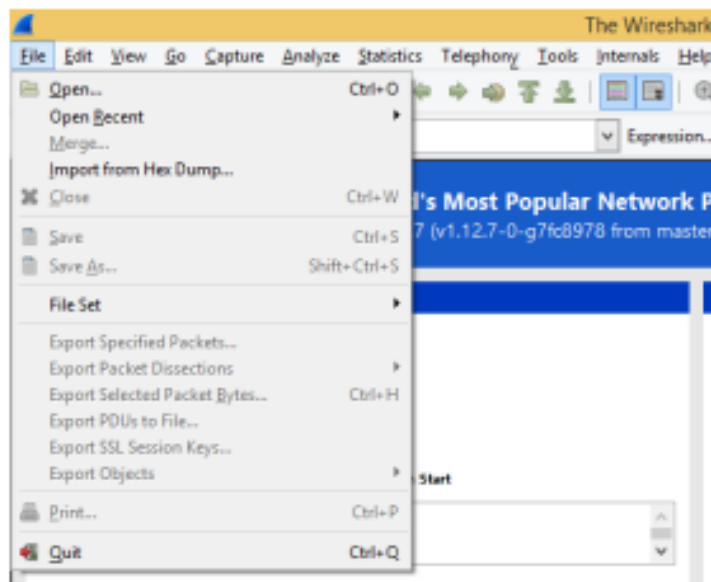
File	File цэс нь цуглуулсан файлуудыг нэгтгэх, нээх, хадгалах, хэвлэх, экспорт хийх эсвэл вайршарк (wireshark) програмаас гарах гэсэн үйлдлүүдийг хийдэг.
Edit	Edit цэсийг ашиглан пакет (packet) хайх, цагийн лавлагаа харах эсвэл пакетуудыг идэвхжүүлэх (mark), профайлын тохиргоо хийх, өөрийн тохиргоог хийх (preferences) зэрэг үйлдлүүдийг хийх боломжтой
View	Энэ цэсийг ашиглан цуглуулсан пакет (packet)-уудыг өнгөөр ялгах, дэлгэцийн үсгийн фонт өөрчлөх, пакет (packet)-ыг тусдаа шинэ цонхонд харуулах пакетын мэдээллийг дэлгэрэнгүй харах хэсгийн мод (tree) мэдээллийг задалж дэлгэх, хумих гэх мэт дэлгэцэд мэдээллийг ямар байдлаар харуулж болох бүхий л тохиргоог хийх боломжтой байдаг.
Capture	Энэ цэс нь сүлжээгээр дамжиж буй пакет (packet) өгөгдлийг чагнах, чагнах процессыг зогсоох, чагнах явцын шүүлтүүрийг засварлах боломж олгодог.
Analyze	Analyze цэс дэлгэцийн шүүлтүүрийг тохируулан идэвхжүүлэх, протоколын задлах хэсгүүдийг идэвхжүүлэх, болиулах, хэрэглэгчийн тодорхойлж өгсөн байдлаар сүлжээний пакет (packet) өгөгдлийг задлах мөн TCP урсгал

WIRESHARK АШИГЛАН СҮЛЖЭЭНИЙ УРСГАЛД АНАЛИЗ ХИЙХ НЬ

	(stream)-ыг дагах гэх мэт үйлдлүүдийг хийдэг.
Statistics	Энэ цэс нь нийт пакет (packet)-уудын хураангуйлсан статистик мэдээллийг харах мөн протоколын шаталсан хэлбэрийн статистикийг харах гэх мэт үйлдлийг хийх боломжийг хэрэглэгчид олгодог.
Telephony	Энэ цэс нь медиа анализ, урсгалын диаграмм, протоколын шаталсан статистик гэх мэт утсан холбоотой хамааралтай статистик мэдээллийг харах боломжоор хэрэглэгчийг хангадаг.
Tools	Tools цэс нь Firewall ACL Rules үүсгэх гэх мэт вайршарк (wireshark) програм дээр хэрэгжүүлэх боломжтой байдаг хэрэглүүрүүдийг (tools) ашиглах боломж олгодог. 3.13. “Tools цэс” 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.
Help	Энэ цэс нь хэрэглэгчид туслах зарим нэгэн энгийн туслах командууд, текст горимоос өгөх командуудын тайлбар мөн хэрэгцээтэй вэб хандалт ашиглан авах боломжтой заавар зэргийг үзэх боломжоор хэрэглэгчийг хангадаг.

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

1. File цэс



ЗУРАГ 3.FILE ЦЭС

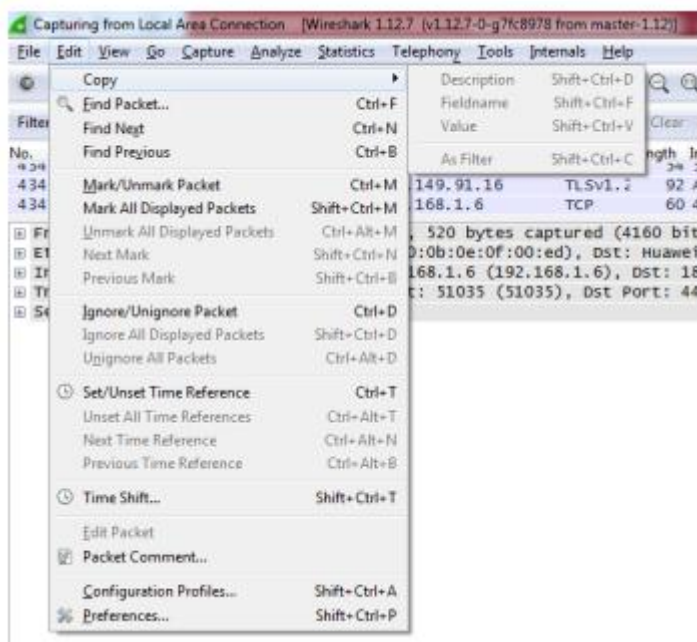
Цэс	Товчлу урын хослол	Тайлбар
Open...	Ctrl+O	Энэ цэс нь цуглуулсан сүлжээний өгөгдлийг вайршарк дээр нээх үйлдлийг хийхэд тань таныг хөтөлнө
Merge		Энэ цэс нь вайршарк дээр нээлттэй байгаа пакет (packet) файл дээр нэмж өөр пакет (packet)-ын файлыг нэгтгэдэг.
Open Recent		Энэ цэс нь сүүлд нээсэн файлуудыг файлуудыг танд дэд командын сонголт хэлбэрээр харуулдаг. Ингэснээр та эдгээр дэд сонголтоос сонгох замаар сүүлд нээж үзсэн файлуудыг шууд нээх боломжтой.
Import from Hex Dump...		Энэ цэс нь хекс (hex) утгыг нь агуулсан текст файлыг импорт хийх цонхыг нээж өгнө.
Close	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.
Save	Ctrl+S	Энэ цэс нь цуглуулсан файлыг хадгалдаг. Өгөгдөл байдлаар хадгалах файлын нэрийг тохируулж өгөөгүй бол тухайн файлыг хадгалах үйлдлийг хөтлөх цонх (Save Capture file as dialog box) гарч ирнэ.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
Save As...	Shift+Ctrl+S	Энэ цэс нь цуглуулсан байгаа пакет файлаа өөрийн хүссэнээр өөрчлөн хадгалах боломжийг хэрэглэгчид

		олгоно. Энэ үйлдлийг хийх үед Save Capture File As цонхыг ашиглан гэртээ харих боломжтой болно.
FileSet> List Files		Энэ цэс нь файлын багц (file set) дотор орших файлуудын жагсаалтыг үзүүлдэг. Энэ цэс нь Вайршаркын файлын багцын жагсаалт цонхыг нээх ба түүгээр дамжуулан дээр дурдсан үүргээ биелүүлдэг.
FileSet>Next File		Одоогоор ачаалагдсан байгаа файл нь файлын багц (file set) –ын нэг хэсэг байвал энэ команд нь файлын багц (file set)-ийн дараагийн файл руу шилжүүлнэ. Ачаалагдсан байгаа файл файлын багц (file set)-д хамаарахгүй эсвэл файлын багцын хамгийн сүүлийн файл байвал саарал өнгөтэй байх ба биелэх боломжгүй байна.
FileSet> Previous File		Одоогоор ачаалагдсан байгаа файл нь файлын багц (file set) –ын нэг хэсэг байвал энэ команд нь файлын багц (file set)-ийн өмнөх файл руу шилжүүлнэ. Ачаалагдсан байгаа файл файлын багц (file set)-д хамаарахгүй эсвэл файлын багцын хамгийн эхний файл байвал саарал өнгөтэй байх ба биелэх боломжгүй байна.
Export > File		Энэ цэс нь одоо дэлгэцэд харуулж буй чагнаж, цуглуулсан пакет (packet) өгөгдлийг бүгдийг нь (эсвэл хэсэгчилсэн байдлаар) файл болгон экспорт хийдэг. Ингэхдээ вайршарк экспорт хийх цонхыг ашигладаг.
Export > Selected Packet Bytes	Ctrl+N	Энэ цэс нь пакетын мэдээллийг байтаар харуулах самбарт (packet bytes pane) идэвхжүүлсэн байгаа байтуудыг бинар (binary) файл руу экспорт хийж гаргадаг. Энэ хэсэг нь мөн л вайршарк экспорт хийх цонхоор дамжин хийгдэнэ.
Export > Objects > HTTP		Энэ цэс нь чагнаж цуглуулсан HTTP объектуудыг бүгдийг нь (эсвэл хэсэгчлэн) локал файл руу экспорт

WIRESHARK АШИГЛАН СҮЛЖЭЭНИЙ УРСГАЛД АНАЛИЗ ХИЙХ НЬ

		хийнэ. Энэ цэс нь Вайршарк HTTP объектын жагсаалт (Wireshark HTTP object list)-ыг харуулдаг.
Export > Objects > DICOM		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.
Export > Objects > SMB		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.
Print	Ctrl+P	Цуглуулсан пакет (packet) файлуудыг бүгдийг нь (эсвэл хэсэгчлэн) хэвлэх үйлдэл хийнэ. Энэ цэс нь Вайршарк хэвлэх (wireshark print) цонхыг дэлгэцэд харуулдаг.
Quit	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.

1.5.2.Edit цэс



ЗУРАГ 4.EDIT ЦЭС

Edit цэсийг дараах хүснэгтээр дэлгэрэнгүй тайлбарлалаа.

Зураг 2. Edit цэсийн команд

Цэс	Гарын товчлуурын хослол	Тайлбар
Copy > Description	Shift+Ctrl+D	Энэ цэс нь дэлгэрэнгүй мэдээллийг нь харуулах самбар (detailed view)-д идэвхжүүлсэн байгаа өгөгдлийн тодорхойлолтыг санах ой руу (clipboard) хуулдаг.
Copy > Fieldname	Shift+Ctrl+F	Энэ цэс нь дэлгэрэнгүй мэдээллийг нь харуулах самбар (detailed view)-д идэвхжүүлсэн байгаа өгөгдлийн талбарын нэрийг (fieldname) санах ой руу (clipboard) хуулдаг
Copy > Value	Shift+Ctrl+V	Энэ цэс нь дэлгэрэнгүй мэдээллийг нь харуулах самбар (detailed view)-д идэвхжүүлсэн байгаа өгөгдлийн утгыг (value) санах ой руу (clipboard) хуулдаг

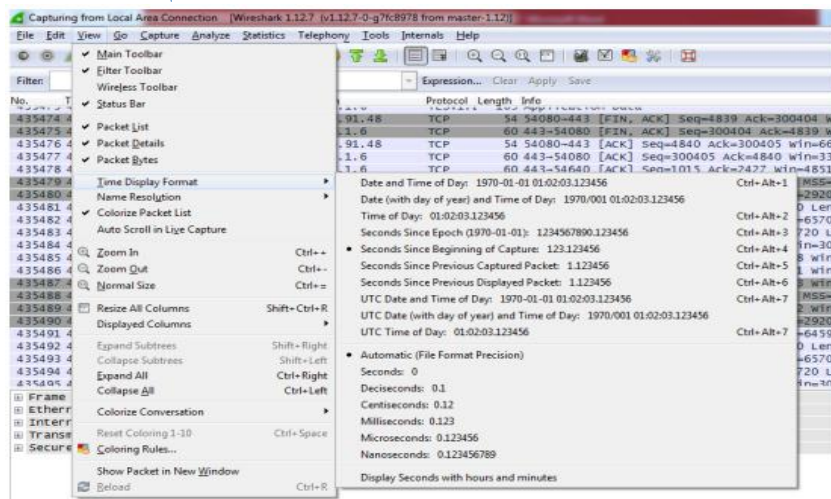
WIRESHARK АШИГЛАН СҮЛЖЭЭНИЙ УРСГАЛД АНАЛИЗ ХИЙХ НЬ

Copy > As Filter	Shift+Ctrl+C	Copy > As Filter Shift+Ctrl+C Энэ цэс нь дэлгэрэнгүй мэдээллийг нь харуулах самбар (detailed view)-д идэвхжүүлсэн байгаа өгөгдлийг дэлгэцийн пакетуудыг шүүх хэсэгт ашигладаг. Энэхүү дэлгэц
Find Packet	Ctrl+F	Энэ цэс нь төрөл бүрийн шалгуур ашиглан өөрт хэрэгтэй пакетаа хайж олох цонхыг танд харуулдаг.
Find Next	Ctrl+N	Таны хайж буй шалгуурт тохирсон дараагийн пакетыг танд олж өгнө
Find Previous	Ctrl+B	Таны хайж буй шалгуурт тохирсон өмнөх пакетыг танд олж өгнө.
Mark/Unmark Packet	Ctrl+M	Идэвхтэй байгаа пакет (packet)-ыг тэмдэглэнэ/тэмдэглэгээг арилгана (mark/unmark).
Toggle Marking Of All Displayed Packets	Shift+Ctrl+Alt+M	Дэлгэцэд байгаа бүх пакет (packet)-уудыг тэмдэглэх/тэмдэглэгээг байхгүй болгох (mark/unmark).
Mark All Displayed Packets	Shift+Ctrl+M	Дэлгэцэд байгаа бүх пакет (packet)-ыг тэмдэглэнэ (mark).. Find Previous Mark Shift+Ctrl+B Тэмдэглэгдсэн пакет (
Unmark All Displayed Packets	Ctrl+Alt+M	Дэлгэцэд байгаа бүх пакет (packet)-уудын тэмдэглэгээг байхгүй (unmark) болгох.
Find Next Mark	Shift+Ctrl+N	Тэмдэглэгдсэн пакет (marked packet)-уудаас дараагийн тэмдэглэгээтэй пакет (marked packet)-г олно
Ignore Packet (toggle)	Ctrl+D	Ignore Packet (toggle) Ctrl+D Идэвхтэй байгаа пакетад (packet) үл ойшоосон (ignore) тэмдэглэгээ тавина.
Ignore All Displayed Packets (toggle)	Shift+Ctrl+D	Дэлгэцэд байгаа бүх пакетуудыг үл ойшоосон/үл ойшоогоогүй (ignore/unignore) гэсэн тэмдэглэгээгээр тэмдэглэнэ.
UnIgnore All Packets	Ctrl+Alt+D	Бүх пакетуудыг (packet) үл ойшоогоогүй

WIRESHARK АШИГЛАН СҮЛЖЭЭНИЙ УРСГАЛД АНАЛИЗ ХИЙХ НЬ

		(UnIgnored) гэсэн тэмдэглэгээгээр тэмдэглэнэ
Set Time Reference (toggle)	Ctrl+T	Энэ цэс нь идэвхтэй 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.
Un-Time Reference All Packets	Ctrl+Alt+T	Пакет (Packet)-уудын дээрх цагийн лавлагаа (time reference) байхгүй болгоно
Find Next Time Reference	Ctrl+Alt+N	Энэ цэс нь цагийн лавлагаа (time reference) болон тохируулагдсан пакет (packet)-уудаас дараагийн цагийн лавлагаа (time reference) болж буй пакет (packet)-ыг хайж олно.
Find Previous Time Reference	Ctrl +Alt+B	Энэ цэс нь цагийн лавлагаа (time reference) болон тохируулагдсан пакет (packet)-уудаас өмнөх цагийн лавлагаа (time reference) болж буй пакет (packet)-ыг хайж олно.
Configuration Profiles	Shift+Ctrl+A	Энэ цэс нь профайл тохиргоо хийх цонх руу хөтөлдөг.
Preferences...	Shift+Ctrl+P	Энэ цэс нь вайршарк (wireshark) програмыг удирддаг параметруудийг тохируулах боломжийг олгодог. Энд тохируулсан тохиргоогоо хадгалах, дараа нь вайршарк (wireshark) програмыг эхлүүлэх үед өмнөх тохиргоотойгоор ажиллуулах гэх мэт зүйлсийг хийх боломжтой.

1.5.3.View цэс



ЗУРАГ 5.VIEW ЦЭС

View цэсийн 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)

Цэс	Гарын товчлуурын хослол	Тайлбар
Main Toolbar		Энэ цэс нь үндсэн товчлуурууд (main toolbar)-ын хэсгийг үндсэн цонхонд (main windows) харуулах, дэлгэцээс алга болгох үйлдлийг хийдэг.
Filter Toolbar		Энэ цэс нь шүүлтүүрийн товчлууруудыг (filter toolbar) үндсэн цонхонд харуулах эсвэл алга болгох үйлдлийг хийнэ.
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.
Packet List		Энэ цэс нь пакетыг жагсаалт хэлбэрээр харуулах самбарыг (packet list pane) үндсэн цонхонд харуулах эсвэл үндсэн цонхноос алга болгох үйлдэл хийнэ.

WIRESHARK АШИГЛАН СҮЛЖЭЭНИЙ УРСГАЛД АНАЛИЗ ХИЙХ НЬ

Packet Details		Энэ цэс нь пакетын мэдээллийг дэлгэрэнгүй харуулах самбарыг (packet details pane) үндсэн цонхонд харуулах эсвэл үндсэн цонхноос алга болгох үйлдэл хийнэ.
Packet Bytes		Энэ цэс нь пакетын мэдээллийг байтаар харуулах самбарыг (packet bytes pane) үндсэн цонхонд харуулах эсвэл үндсэн цонхноос алга болгох үйлдэл хийнэ.
Time Display Format > Date and Time of Day: 1970-01-01 01:02:03.1 23456		Энэ хэсгийг сонгосноор вайршарк (wireshark) програм сүлжээнээс барьж авсан пакет (packet)-уудын ирсэн цагийг мэдээллийг он, сар, өдөр, цаг гэсэн бүтэцтэйгээр харуулдаг. "Time of Day", "Date and Time of Day", "Seconds Since Beginning of Capture", "Seconds Since Previous Captured Packet", "Seconds Since Previous Displayed Packet" гэсэн сонголтууд нь нэгэн зэрэг сонгогдох боломжгүй бөгөөд нэг удаад зөвхөн аль нэгийг нь л сонгох боломжтой
Time Display Format > Time of Day: 01:02:03.1 23456		Энэ хэсгийг сонгосноор вайршарк (Wireshark) програм пакет (packet)-ын цагийн мэдээллийг тухайн өдрийн цагаар гаргана уу.
Time Display Format > Seconds Since Epoch (1970-01-01)		Энэ хэсэг нь пакет (packet)-ын цагийн мэдээллийг 1970-01-01 00:00:00 эхлэн тоолсон секундйн хэмжигдэхүүнээр харуулна.

WIRESHARK АШИГЛАН СҮЛЖЭЭНИЙ УРСГАЛД АНАЛИЗ ХИЙХ НЬ

Time Display Format > Seconds Since Beginning of Capture: 123.12345 6		Энэ хэсгийг сонгосноор вайршарк (wireshark) програм пакетын (packet)-ын цагийн мэдээллийг харуулахдаа пакет (packet) цуглуулж эхэлсэн хугацаанаас хойших секундээр хэмжин харуулдаг.
Time Display Format > Seconds Since Previous Captured Packet: 1.123456		Энэ сонголтыг идэвхжүүлснээр пакет (packet)-ын цагийн мэдээллийг өмнө нь хүлээн авсан пакет (packet)-аас хойш хэдэн секундийн дараа ирж байгаа байдлаар нь харуулна
Time Display Format > Seconds Since Previous Displayed Packet: 1.123456		Энэ сонголтыг идэвхжүүлснээр пакет (packet)-ын цагийн мэдээллийг өмнөх пакетыг дэлгэцэд харуулснаас хойш хэдэн секундийн дараа дэлгэцэд харуулж байгаа секундээр хэмждэг.
Time Display Format > Automatic (File Format		Энэ хэсгийг сонгосноор пакет (packet)-ын цагийн мэдээллийг цуглуулсан файлын форматад тодорхойлсон нарийвчлалаар харуулна.

WIRESHARK АШИГЛАН СҮЛЖЭЭНИЙ УРСГАЛД АНАЛИЗ ХИЙХ НЬ

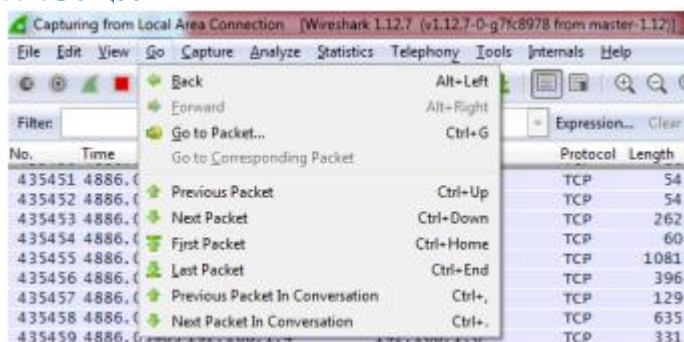
Precision)		
Time Display Format > Seconds: 0		Энэ сонголтыг сонгосноор вайршарк (wireshark) програм пакет (packet)-ын цагийн мэдээллийг секундйн нарийвчлалтайгаар харуулна.
Time Display Format > ...seconds: 0		Энэ хэсгийг сонгосноор вайршарк (wireshark) програм пакет (packet)-ын цагийн мэдээллийг секунд, 1/10 сек, 1/100 сек, 1/1000 сек гэх мэт нарийвчлалтай харуулдаг.
Time Display Format > Display Seconds with hours and minutes		Энэ хэсгийг сонгосноор вайршарк (wireshark) програм пакетын цагийн мэдээллийг цаг минутын хамтаар секундйн нарийвчлалтайгаар харуулдаг.
Name Resolution > Resolve Name		Энэ сонголт нь идэвхтэй байгаа пакет (packet)-ын нэрийн хөрвүүлэлтийг хийдэг.
Name Resolution > Enable for MAC Layer		Энэ сонголт нь вайршарк (wireshark) програм MAC хаягийг нэр лүү хөрвүүлэх эсэхийг удирддаг.
Name Resolution > Enable for Network Layer		Энэ хэсэг нь вайршарк (wireshark) програм сүлжээний хаягуудыг нэрийн хөрвүүлэлт рүү хөрвүүлэх эсэхийг удирддаг.

WIRESHARK АШИГЛАН СҮЛЖЭЭНИЙ УРСГАЛД АНАЛИЗ ХИЙХ НЬ

Name Resolution > Enable for Transport Layer		Энэ хэсэг нь вайршарк (wireshark) програм transport түвшний хаягийг нэрийн хөрвүүлэлт рүү хөрвүүлэх эсэхийг удирддаг.
Colorize Packet List		Энэ хэсэг нь пакетын жагсаалт (packet list)-ыг өнгөөр ялгах эсэхийг удирдана. Өнгөөр ялгах нь чагнах, цуглуулсан пакет (packet)-ыг дэлгэцэд хэвлэх үйлдлийг удаан болгодог.
Auto Scroll in Live Capture		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 дэлгэцэд харагдахгүйгээр доод талд нь нэмэгдэж явна
Zoom In Ctrl++		Үсгийн фонтыг томруулна.
Zoom Out Ctrl+-		Үсгийн фонтыг багасгана.
Normal Size Ctrl+=		Үсгийн фонтын хэмжээг хэвийн болгоно.
Resize All Columns Shift+Ctrl+R		Багана бүрийн өргөнийг өгөгдлийнх уртад тааруулан өөрчлөх. Их хэмжээний өгөгдөлтэй байгаа үед баганын хэмжээг тааруулах нь илүү их хугацаа зарцуулах магадлалтай
Displayed Columns		Энэ хэсэг нь дэлгэцэд харуулахаар тохируулсан багануудыг нэгтгэн удирдана. Эдгээр тохиргоогоор пакетын жагсаан харуулах самбар (packet list pane) харуулж байгаа багануудыг дэлгэцэд харуулах эсвэл дэлгэцэд харуулахгүй байх тохируулгыг хийнэ
Expand Subtrees		Энэ сонголт нь пакетын мэдээллийг дэлгэрэнгүй харуулах самбар (packet details pane)-т байрлах мод

Shift+Right		(tree) хэлбэрийн бүтцийн мэдээллийг задалж харуулна.
Collapse Subtrees Shift+Left		Энэ сонголт нь пакетын мэдээллийг дэлгэрэнгүй харуулах самбар (packet details pane)-т байрлах мод (tree) хэлбэрийн бүтцийн мэдээллийг хумьж хаана.
Expand All Ctrl+Right		Пакетын мэдээллийг дэлгэрэнгүй харуулах самбар (packet details pane) дахь мод (tree) хэлбэрийн бүтэцтэй мэдээллийг бүгдийг нь задална
Collapse All Ctrl+Left		Пакетын мэдээллийг дэлгэрэнгүй харуулах самбар (packet details pane) дахь мод (tree) хэлбэрийн бүтэцтэй мэдээллийг бүгдийг нь хумьж хаана
Coloring Rules		Энэ сонголт нь пакетыг жагсаан харах самбар (packet list pane)-т байгаа пакет (packet)-уудыг өөрийн сонгосон шүүлтүүрийг ашиглан өөр өнгөөр ялган харах тохиргоог хийх боломжийг олгодог
Show Packet in New		Энэ сонголт нь сонгож авсан пакет (packet)-ыг тусдаа цонхонд нээж Window харах боломжийг олгодог. Тусдаа нээгдсэн цонхонд зөвхөн мод (tree) хэлбэрийн бүтцээр мэдээллийг нь дэлгэрэнгүй харах мөн байтаар харах самбарын мэдээллүүд л агуулагддаг
Reload	Ctrl+R	Энэ сонголт нь одоогийн цуглуулсан байгаа пакет (packet) файлыг дахин ачаалалдаг.

1.5.4.Го цэс



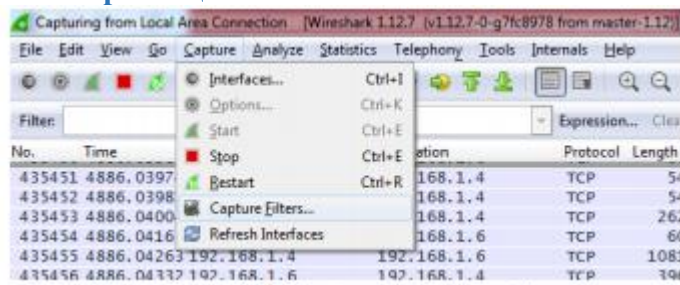
ЗУРАГ 6.Go цэс

Go цэсийн командуудын тайлбарын доор үзүүлсэн хүснэгтэд харууллаа.

Цэс	Гарын товчлуурын хослол	Тайлбар
Back Alt+Left		Пакетын түүх (Packet history) хэсэгт хадгалагдсан байгаа пакет (packet)-уудын дарааллын дагуу хамгийн сүүлд хандсан пакет (packet) руу очно.. Go to Corresponding Packet Протокол талбар дээр идэвхэжсэн 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.
Forward	Alt+Right	Пакетын түүх (Packet history) хэсэгт хадгалагдсан байгаа пакет (packet)-уудын дарааллын дагуу тухайн пакетын өмнө хандсан пакет (packet) руу очно. Back цэсийн эсрэг үйлдэл
Go to Packet	Ctrl+G	Пакет (Packet)-ын дугаарыг нь зааж өгснөөр тухайн (packet) руу очно.
Go to Corresponding Packet		Протокол талбар дээр идэвхэжсэн 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.
Previous Packet	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 идэвхжээгүй байсан ч гэсэн

		өмнөх пакет (packet) руу нь шилжүүлдэг.
Next Packet Ctrl+Down		Пакетыг жагсаан харуулах самбарт (Packet list pane) байгаа пакет (packet)-ын дараагийн пакет (packet) руу очно. Энэ команд нь пакетыг жагсаан харуулах самбар (packet list pane) хэсэгт компьютерийн гар идэвхжээгүй байсан ч гэсэн өмнөх пакет (packet) руу нь шилжүүлдэг.
First Packet Ctrl+Home		Пакет жагсаан харуулах самбар (Packet list pane) дахь хамгийн эхний пакет (packet) дээр очно
Last Packet Ctrl+End		Пакет жагсаан харуулах самбар (Packet list pane) дахь хамгийн сүүлийн пакет (packet) дээр очно
Previous Packet In Conversation	Ctrl+	Одоогийн пакетын (packet) харилцан мэдээлэл (conversation) дамжуулалтын өмнөх пакет руу аваачдаг.
Next Packet In Conversation	Ctrl+	Одоогийн пакетын (packet) харилцан мэдээлэл (conversation) дамжуулалтын дараагийн пакет руу аваачдаг.

1.5.5.Capture цэс



ЗУРАГ 7.CAPTURE ЦЭС

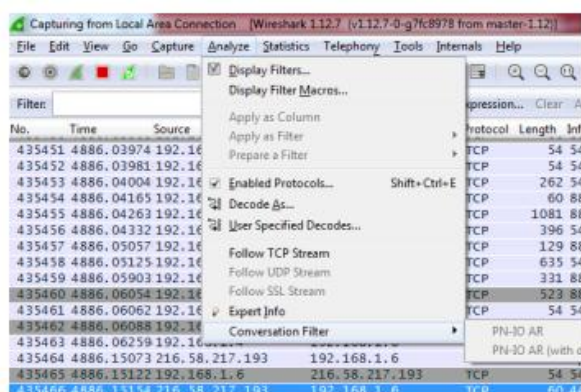
Capture цэсийн тайлбарыг доор хүснэгтэд тайлбарлан үзүүлээ.

Цэс	Гарын товчлуурын хослол	Тайлбар
Interfaces	Ctrl+I	Энэ сонголт нь сүлжээний интерфэйсүүд дээр ямар ачаалалтай мэдээлэл дамжигдаж буй мэдээллийг харуулдаг цонх руу хөтөлнө.
Options...	Ctrl+K	Энэ сонголт нь сүлжээг чагнахдаа ямар тохиргоотойгоор

WIRESHARK АШИГЛАН СҮЛЖЭЭНИЙ УРСГАЛД АНАЛИЗ ХИЙХ НЬ

		чагнах тохиргоог хийх цонх руу хөтөлдөг. Мөн эндээс чагнах үйлдлийг эхлүүлж болдог.
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 зогсооно.
Restart	Ctrl+R	Пакет чагнах үйлдлийг дахин эхлүүлдэг. Ингэхдээ өмнө нь хэрэглэж байсан тохиргоог ашигладаг.
Capture Filters		Энэ сонголт нь сүлжээний интерфейс дээгүүрх пакет өгөгдлийг чагнахдаа шүүлтүүр тохируулж чагнах боломж олгох мөн түүнчлэн шүүлтүүрийн тохиргоог шинээр үүсгэх түүндээ нэр өгч дараа нь ашиглахад бэлэн болгох боломжтой.

1.5.6. Analyze цэс



ЗУРАГ 8 ANALYZE ЦЭС

Analyze командын тайлбарыг хүснэгтэд үзүүлээ.

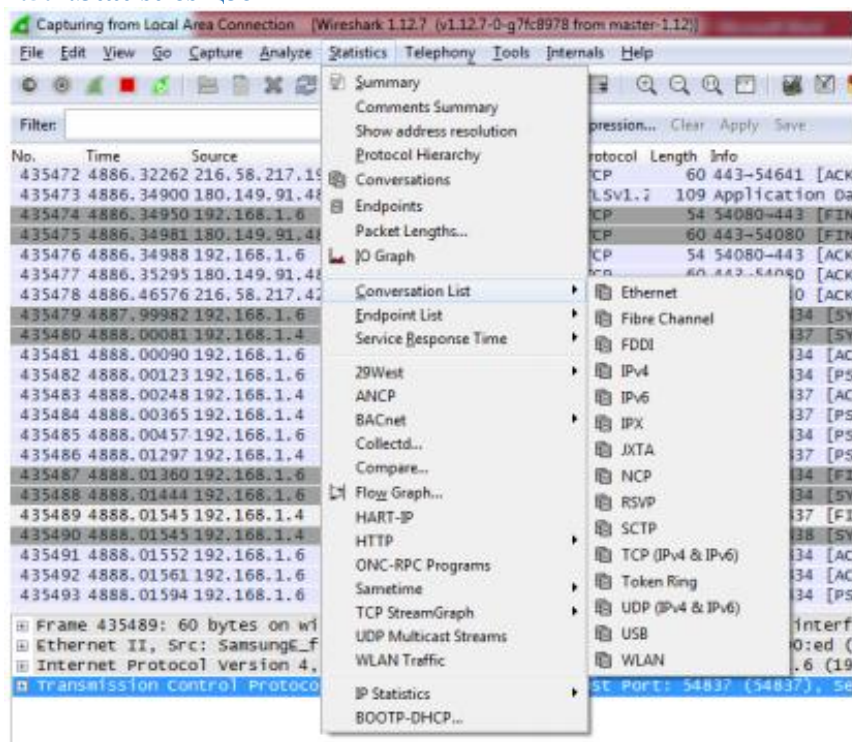
Цэс	Гарын товчлуурын хослол	Тайлбар
Display Filters		Энэ цэс нь дэлгэцэд харуулж байгаа (packet)-уудыг шүүлтүүрээр оруулах, шүүлтүүрийг шинээр үүсгэх, түүндээ нэр өгч хадгалах зэрэг үйлдлийг хийх цонх руу хэрэглэгчийг хөтөлнө.
Display Filter Macros		Энэ цэс нь дэлгэцийн шүүлтүүрийн макро үүсгэх цонх руу хөтөлнө. Энэ цонхыг ашиглан макро үүсгэх, үүсгэсэн макрог засварлах гэх мэт

WIRESHARK АШИГЛАН СҮЛЖЭЭНИЙ УРСГАЛД АНАЛИЗ ХИЙХ НЬ

		үйлдлүүдийг хийх цонхыг нээдэг. Эдгээр макродоо нэр өгөх хадгалах, дараа ашиглахаар тохируулж болно.
Apply as Column		Энэ цэс нь пакетын протоколын хэсэгт идэвхэжсэн 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 идэвхжүүлдэг. 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 холбооснуудаар холбогдоно) сонголтууд байдаг.
Prepare a Filter > ...		Эдгээр сонголтууд нь одоо идэвхтэй байгаа шүүлтүүрийг өөрчлөх хэдий ч тэдгээрийг одоо идэвхтэй байгаа дэлгэцийн шүүлтүүр болгон идэвхжүүлэхгүй. 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 холбооснуудаар холбогдоно) сонголтууд байдаг
Enabled Protocols...	Shift+Ctrl+E	Энэ команд нь протоколыг задлан харуулах хэсгийг (dissector) идэвхжүүлэх/идэвхгүй болгох үйлдлийг хийдэг
Decode As...		Энэ цэс нь тодорхой пакет (packet)-уудыг заагдсан (хэрэглэгч өөрөө тодорхойлж өгсөн протокол байж болно) протоколын дагуу

		задалдаг.
User Specified Decodes...		Энэ сонголт нь өөрийн зааж өгсөн протоколын дагуу пакет (packet)-уудыг задлан харуулдаг.
Follow TCP Stream		Энэ цэс нь сонгогдсон байгаа TCP пакет (packet)-тай ижилхэн холболт ашиглаж байгаа бүх TCP сегментүүдийг тусад нь дэлгэцэд харуулдаг.
Follow UDP Stream		Өмнөх командтай ижилхэн үйлдэл хийнэ гэхдээ UDP пакет (packet)-ын хувьд энэхүү үйлдлийг хийдэг
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 – шинэ хэсэг нэмэх, эндээс холболт үүсгэх (link from here)
Conversation Filter > ...		Энэ хэсэгт харилцан мэдээлэл солилцож буй холболтыг шүүж харах шүүлтүүр олно. (conversation filter) XXX – SSL түлхүүрүүдийг хэрхэн хангах вэ?
Expert Info		Энэ хэсэг нь цуглуулсан пакет (packet)-уудын талаар ахисан түвшинд хэрэглэгдэх мэдээллийг харуулна. Эдгээр мэдээллийн хэмжээ нь протоколуудаас хамаардаг бөгөөд түүнчлэн эдгээр мэдээллүүд нь маш дэлгэрэнгүй харуулдаг.

1.5.7. Statistics цэс



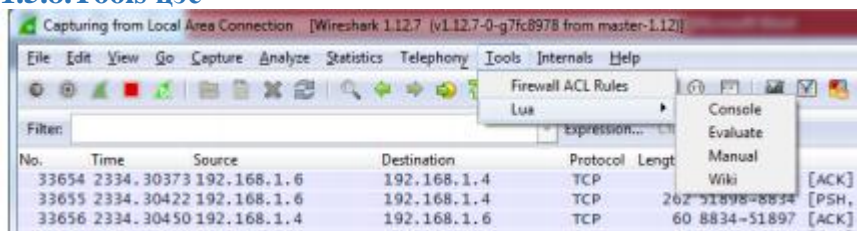
ЗУРАГ 9 STATISTICS

Statistics цэсийн дэлгэрэнгүй тайлбарыг доорх хүснэгтээр харууллаа.

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

Цэс	Гарын товчлуурын хослол	Тайлбар
Summary		Цуглуулж авсан өгөгдлийн талаарх мэдээллийг харуулна.
Protocol Hierarchy		Протоколын статистик мэдээллийн шаталсан бүтцийг мод (tree) хэлбэрээр харуулна.
Conversations		Харилцан мэдээлэл дамжуулсан 2 төгсгөлийн цэгүүдийн талаарх статистик мэдээллийг харуулна.
Endpoints		Өгөгдөл дамжуулж буй эсвэл хүлээн авч буй төгсгөлийн цэгүүдийг (хаягийг) харуулдаг.

1.5.8.Tools цэс

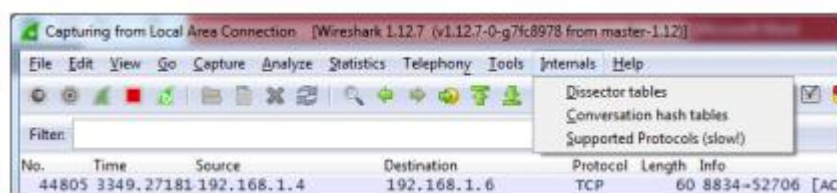


ЗУРАГ 10. TOOLS ЦЭС

Дараах хүснэгтэд tools цэсийн тайлбарыг үзүүлээ.

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.

1.5.9. Internals цэс



ЗУРАГ 11. INTERNALS ЦЭС

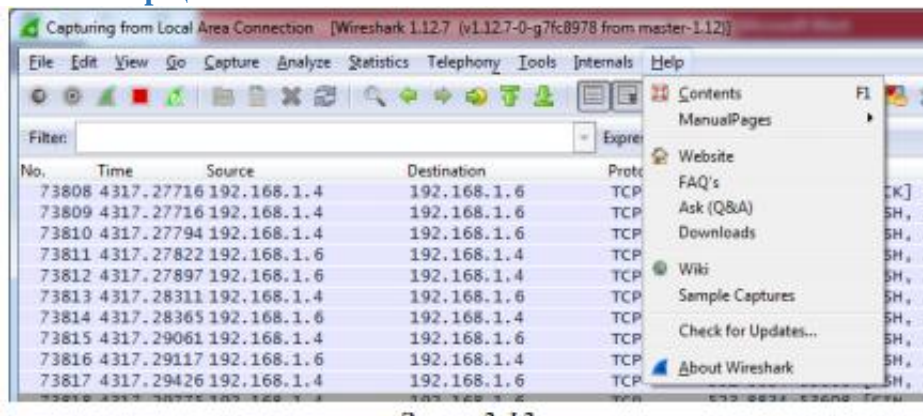
Дараах хүснэгтээр Internals цэсийг тайлбарлалаа.

Цэс	Гарын товчлуурын хослол	Тайлбар
Dissector tables		Энэ цэс нь дэд задаргааны хоорондын хамаарлыг

WIRESHARK АШИГЛАН СҮЛЖЭЭНИЙ УРСГАЛД АНАЛИЗ ХИЙХ НЬ

		агуулсан хүснэгтийг харуулдаг.
<i>Supported Protocols (slow!)</i>		<i>Энэ цэс нь вайршарк (wireshark) програмын дэмжиж буй протоколууд тэдгээрийн талбаруудын талаарх мэдээллийг харуулдаг.</i>

1.5.10. Help цэс



ЗУРАГ 12.HELP ЦЭС

Дараах хүснэгтэд Help цэсийн тайлбарлан үзүүлээ.

Цэс	Гарын товчлуурын хослол	Тайлбар
Contents F1		Энгийн хэрэглээний туламжийн мэдээллийг харуулна.
Manual Pages > ...		Энэ хэсэг нь хэрэглэх зааврыг вэб броузер ашиглан харуулна. (Локал дээр суусан байгаа хэрэглэх заавар (user guide)). Website Энэ цэс нь https://www.wireshark.org/ вэб хуудсыг нээнэ.
FAQ's		FAQ асуултуудыг вэб броузер дээр харуулна.
Sample Captures		Энэ хэсэг нь вэб хуудас нээх ба энэ хуудас дээр жишээ болгон хэрэглэж болох сүлжээний пакет(packet) өгөгдлүүд байна. Энэ цэс нь https://wiki.wireshark.org/ вэб хуудсыг нээнэ.
Downloads		Энэ цэс нь https://www.wireshark.org/ вэб хуудсыг нээнэ. Wiki Энэ цэс нь

		https://wiki.wireshark.org/ вэб хуудсыг нээнэ.
Wiki		Энэ хэсэг нь вэб хуудас нээх ба энэ хуудас дээр жишээ болгон хэрэглэж болох сүлжээний пакет(packet) өгөгдлүүд байна. Энэ цэс нь https://wiki.wireshark.org/ вэб хуудсыг нээнэ.
About wireshark		Энэ сонголт нь вайршарк (wireshark) програмын талаар мэдээллийг дэлгэрэнгүйгээр өгнө. Жишээлбэл: Вайршарк (wireshark)-г хэрхэн суулгасан (build), ямар ямар нэмэлт залгааснууд (plug-ins) ачаалагдсан байгаа гэх мэт ...

1.6.Үндсэн товчлуурууд (Main Toolbar)

Үндсэн товчлуурууд (Main toolbar) нь хэрэглэгчдийн байнга хэрэглэдэг функцүүдийг товчлуур болгон агуулсан байдаг ба эдгээр нь байнга хэрэглэдэг функцүүд, командуудаа хурдан сонгох боломжийг олгоно. Энэхүү товчлууруудыг (toolbar) хэрэглэгч өөрийн хүссэнээр өөрчлөх боломжгүй хэдий ч View цэсийн тохиргоог ашиглан дэлгэцэд харагдахгүй болгон тохируулж болно.











Цэсийн 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 хадгалах товчлуур саарал өнгөтэй байна.)













Товчлуур	Товчлуурын нэр	Харгалзах цэсийн сонголт	Тайлбар
	Interfaces...	Capture/Interfaces...	Энэ товчлуур нь Сүлжээний орчинд чагнах боломжтой байгаа интерфэйсүүдийг жагсаан харуулна.
	Options...	Capture/Options...	Энэ хэсэг нь сүлжээг чагнах сонголтуудыг харуулна. Энэ хэсгээс та пакет (packet) чагнах үйлдлийг

WIRESHARK АШИГЛАН СҮЛЖЭЭНИЙ УРСГАЛД АНАЛИЗ ХИЙХ НЬ

			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 зогсооно.
	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.
	Save As...	File/Save As...	Одоо ачаалагдсан байгаа пакет (packet) өгөгдлийг өөрийн хүссэн файлын өргөтгөлтэйгөөр хадгалах боломжийг олгоно. Энэ товчлуур нь Цуглуулсан Файлыг хадгалах цонхыг нээдэг.
	Close	File/Close	Нээлтэй байгаа цуглуулсан пакет (packet)- уудыг хаана. Хэрэв хадгалж амжаагүй бол хадгалах эсэхийг асуусан цонхыг харуулна.
	Reload	View/Reload	Дэлгэцэд харж буй ачаалагдсан пакет (packet) өгөгдлийг дахин ачаална.
	Find Packet...	Edit/Find Packet...	Пакет (packet) хайх цонхыг нээнэ.
	Go Back	Go/Go Back	Пакетын түүх хуудас (packet history)- д бичигдсэн байгаа өмнөх пакет (packet) дээр очно..
	Go Forward	Go/Go Forward	Пакетын түүх хуудас (packet history)- д бичигдсэн байгаа дараагийн пакет (packet) дээр очно.
	Go to Packet...	Go/Go to Packet...	Пакет (packet)-ын дугаараар тухайн

WIRESHARK АШИГЛАН СҮЛЖЭЭНИЙ УРСГАЛД АНАЛИЗ ХИЙХ НЬ

			пакет (packet) дээр очно
	Go To First Packet	Go/First Packet	Цуглуулсан пакет (packet)-уудын хамгийн эхний пакет (packet) дээр очно.
	Go To Last Packet	Go/Last Packet	Цуглуулсан пакет (packet)-уудын хамгийн сүүлийн пакет (packet) дээр очно.
	Colorize	View/Colorize	Пакет (packet)-уудыг өнгөөр ялгах/өнгөөр ялгахыг болиулах үйлдлийг хийнэ.
	Auto Scroll in Live Capture	View/Auto Scroll	Сүлжээг чагнаж байх үед пакетуудыг жагсаан харуулах самбар (packet list pane)-т байгаа пакетуудын хамгийн сүүлийн packet-ийг дэлгэцэд багтаан харуулах
	Zoom In	View/Zoom In	Үсгийн фонт томруулах
	Zoom Out	View/Zoom Out	Үсгийн фонт жижигрүүлэх
	Normal Size	View/Normal Size	Үсгийн фонт хэвийн хэмжээтэй болгох
	Resize Columns	View/Resize Columns	Багануудын хэмжээг дахин өөрчлөх, ингэснээр багануудын агуулга нь баганад яг таарна.
	Capture Filters...	Capture/Capture Filters	Сүлжээний интерфейсийг чагнах үед шүүлтүүр ажиллуулах цонхыг нээнэ. Эндээс та шинэ шүүлтүүрийн дүрэм үүсгэх, түүндээ нэр өгөх, хадгалах үйлдлүүдийг хийх боломжтой.
	Display Filters...	Analyze/Display Filters...	Товчлуур нь дэлгэцэд харуулах пакет (packet)-уудыг шүүлтүүрээр оруулах цонхыг харуулна. Мөн та шинэ шүүлтүүрийн дүрэм үүсгэх түүндээ нэр өгөн хадгалах

WIRESHARK АШИГЛАН СҮЛЖЭЭНИЙ УРСГАЛД АНАЛИЗ ХИЙХ НЬ

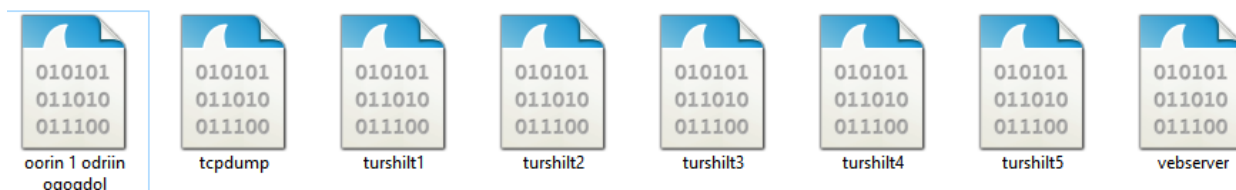
			боломжтой.
	Coloring Rules...	View/Coloring Rules...	Энэ товчлуур нь хэрэглэгчийн сонгосон шүүлтүүрийн дагуу пакет (packet)-уудыг өнгөөр ялгах үйлдлийг хийдэг. Эндээс та шинээр өнгөөр ялгах дүрэм бичих, хуучин дүрмийг өөрчлөх гэх мэт үйлдлүүдийг хийх боломжтой. Олон пакет (packet) өгөгдөл байгаа үед ингэж өнгөөр ялгаж харах нь ажлыг маш ихээр хөнгөвчилдөг.
	Preferences...	Edit/Preferences	Энэ товчлуур нь вайршарк (wireshark) програмыг удирдах параметруудийг тохируулах боломжийг олгоно. Өөрийн хүссэн тохиргоог хийх, түүнийгээ хадгалах гэх мэт үйлдлүүдийг хийх боломжтой.
	Help	Help/Contents Help	Help цэсэд байрлах хэрэглэгчид туслах зориулалттай вайршарк (wireshark)-ыг хэрхэн хэрэглэх талаарх мэдээллийг үзүүлнэ

БҮЛЭГ 2. ТҮРШИЛТ СУДАЛГААНЫ ХЭСЭГ

2.1 Судалгааны өгөгдөл цуглуулах

1. Wireshark программ ашиглан дараах өгөгдлүүдийг бичиж авсан.

- 12-503 Компьютерийн лабораторийн нэг компьютерийн 5 өдрийн өгөгдөл
- Өөрийн компьютерийн 1 өдрийн өгөгдөл



ЗУРАГ 1. СУДАЛГААНЫ ӨГӨГДӨЛ

Энэ хэсэгт Wireshark программ ашиглан сүлжээг хэрхэн чагнах, чагнасан өгөгдлөө хэрхэн хадгалах заавар боловсруулсан.

- Алхамчилсан текст заавар
- Дэлгэц бичсэн видео заавар

2.1.1. Wireshark програм ашиглан өгөгдөл чагнах алхамчилсан заавар

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

Чагнах функцийг эхлүүлэх

Дараах аргуудыг ашиглан вайршарк програмаар пакет чагнах үйлдлийг эхлүүлж болдог.

- Үндсэн цонх дээр харагдах интерфейс дээр хулганыг 2 удаа дарах
- Чагнах боломжтой интерфейсүүдийн талаарх мэдээллийг харах боломжтой. Ингэхдээ (Capture ▾ Options) –ийг ашиглана.
- Виндовс орчинд Интерфейс чагнах үйлдэл хэрхэн эхлүүлэхийг,

Эхлүүлэх (Start) товчлуурыг дарж чагнах процессыг эхлүүлж болно.

- Одоогоор идэвхтэй байгаа тохиргооны дагуу чагнах бол Capture ▾ Start эсвэл эхний товчлуур (first toolbar)-г дарж шууд чагнах процессыг эхлүүлж болно.
- Хэрэв чагнах интерфейснхээ нэрийг мэдэж байгаа бол командын горимоос дараах командыг ашиглан чагнах процессыг эхлүүлж болно.

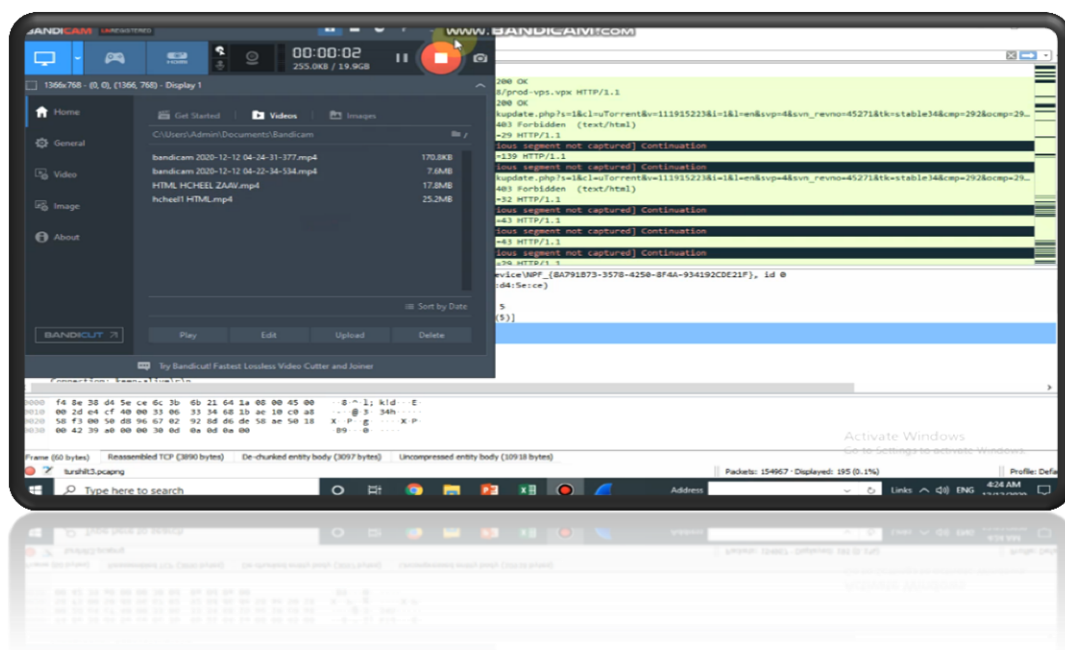
Чагнах фрэйм (Capture frame)

- Интерфейсийн 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) идэвхэжсэн эсвэл идэвхжээгүй талаарх мэдээлэл
- Пакет бүр дээр чагнагдах хамгийн их өгөгдлийн хэмжээ. Өгөгдөл 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 хирээст талбар (checkbox)-г хэрээсэлж тэмдэглэснээр тухайн интерфейсээс чагнахаар сонгож байна гэсэн үг. Интерфейс дээр хулганын товчийг 2 удаа дарснаар Интерфейсийн тохиргоог засварлах (Edit Interface Settings) –г гаргаж ирнэ.

2.1.2. Wireshark програм ашиглан өгөгдөл чагнах видео заавар

Өгөгдөл чагнах процессыг эхлүүлж буй болон дуусаад хадгалж буй процессыг дэлгэц бичих програм ашиглан бичсэн болно.



ЗУРАГ 2. WIRESHARK АЖИЛЛУУЛАХ ВИДЕО ЗААВАР

2.2. Чагнасан файльтай ажиллах

Энэ хэсэгт дараах үйлдлүүдийг хийв.

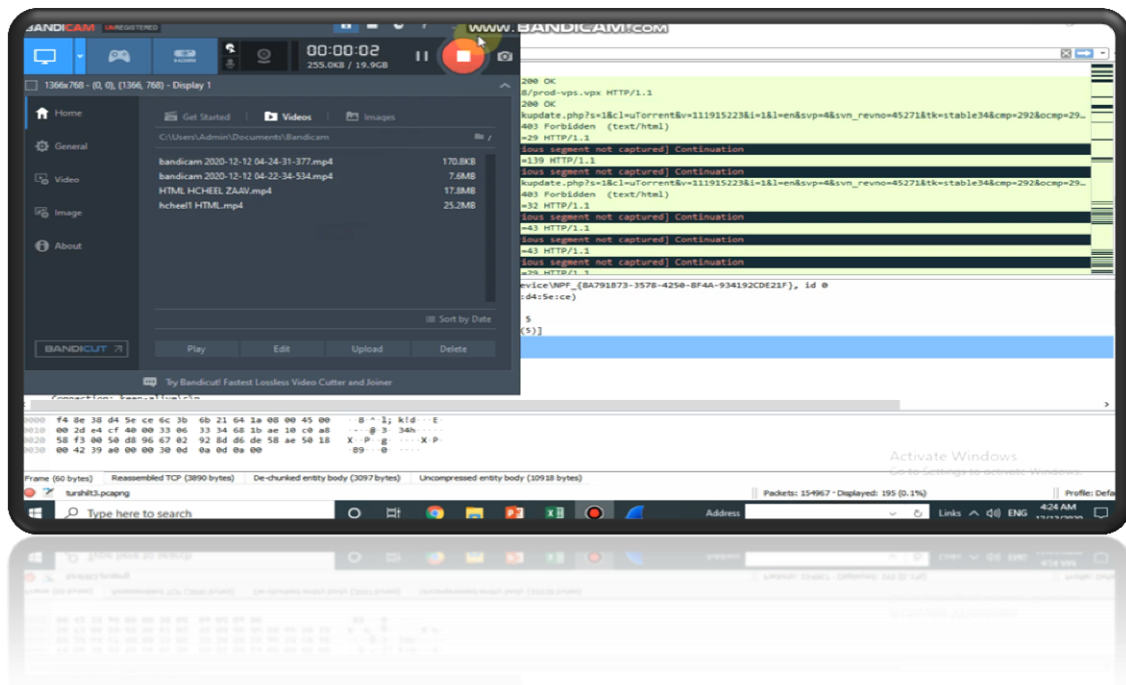
1. Лабораторийн нэг компьютерийн 5 өдрийн өгөгдлийг ашиглан оюутнууд ямар сайтыг түлхүү ашигладгийг илрүүлэх
2. Өөрийн компьютерийн нэг өдрийн өгөгдлийг ашиглан сүлжээгээр дамжсан зураг болон бусад файлыг задалж харах

2.2.1. HTTP протоколоор шүүлт хийх видео заавар

Мэдээлэл зүйн тэнхимийн 503 лабораторийн 25-р компьютер дээр хичээлийн 5 өдрийн турш програмыг ажиллуулан бичиж авсан өгөгдөлд wireshark ашиглан анализ хийсэн байгаа.

- Оюутнууд ямар сайт түлхүү ашиглаж байгааг илрүүлэхийн тулд чагнасан файлаасаа http протоколоор шүүлт хийж пакет тус бүрээс сайтын хаягуудыг гаргаж авсан болно.

Мөн хэрхэн протоколоор шүүлт хийх зааврыг видео хэлбэрээр болон алхамчлан боловсруулав.

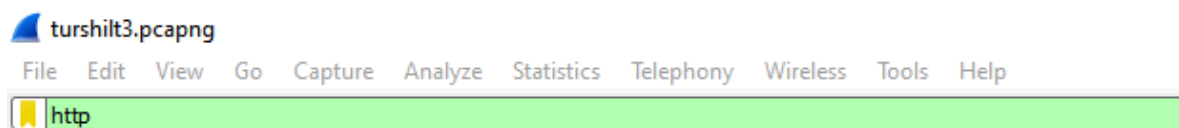


ЗУРАГ 3.ЛАБОРАТОРИЙН 5 ӨДРИЙН ӨГӨГДӨЛ

2.2.2. HTTP Протоколоор шүүлт хийх алхамчилсан заавар

Алхам 1. Wireshark-ыг цуглуулсан өгөгдлөө нээх

Алхам 2. HTTP протоколыг хайх



ЗУРАГ 4. HTTP ПРОТОКОЛЫГ ХАЙХ

Алхам 3.

Шүүсэн өгөгдлөө гаргаж ирэх

17.043451	5852	104.27.174.16	192.168.88.243	HTTP	60	HTTP/1.1 200 OK (text/html)
60.687288	12791	192.168.88.243	184.86.217.156	HTTP	275	GET /image/global.4872.acentoprodimg.1f77e721-e057
60.687289	12792	192.168.88.243	184.86.217.156	HTTP	276	GET /image/global.4872.acentoprodimg.1f77e721-e057
60.745578	12794	184.86.217.156	192.168.88.243	HTTP	1514	[TCP Previous segment not captured] Continuation
60.745841	12797	184.86.217.156	192.168.88.243	HTTP	1514	[TCP Previous segment not captured] Continuation
60.746237	12800	184.86.217.156	192.168.88.243	HTTP	1514	[TCP Previous segment not captured] Continuation
60.746766	12804	184.86.217.156	192.168.88.243	HTTP	1514	[TCP Previous segment not captured] Continuation
60.746766	12807	184.86.217.156	192.168.88.243	HTTP	1040	Continuation[Malformed Packet]
60.908974	12842	192.168.88.243	184.86.217.156	HTTP	479	GET /image/global.30004.acentoprodimg.b18e0377-812
60.968705	12851	184.86.217.156	192.168.88.243	HTTP	1514	[TCP Previous segment not captured] Continuation
60.968947	12855	184.86.217.156	192.168.88.243	HTTP	1514	[TCP Previous segment not captured] Continuation

ЗУРАГ 5. ШҮҮСЭН ӨГӨГДӨЛ

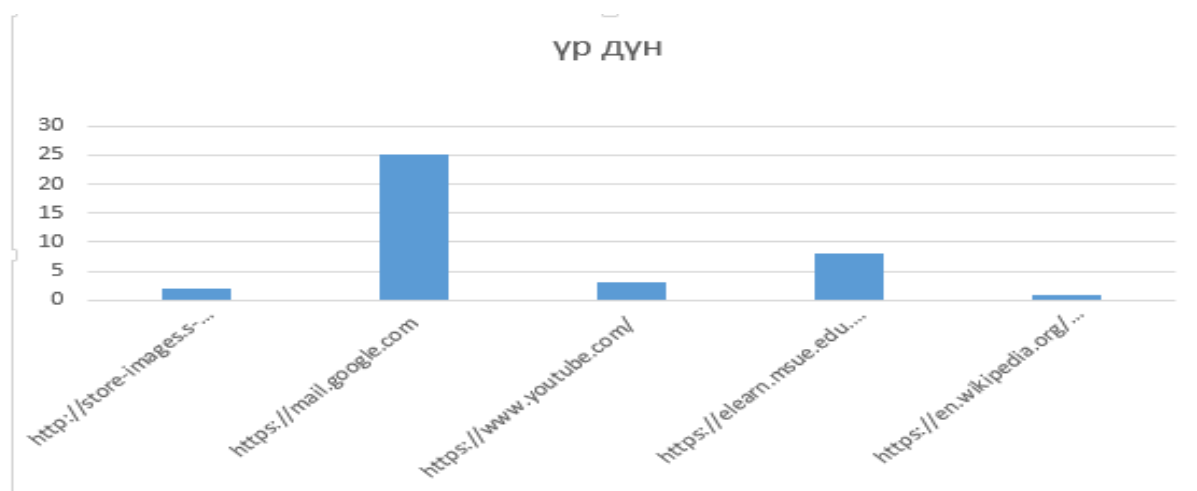
Лабораторийн 5 өдрийн урсгал шүүж байхад оюутнууд ямар сайтаар их ордгийг задлан шинжилж харуулсан.

-google

-facebook

-youtube

-elearn гэх мэт сайтуудаар илүү их орсон судалгааны үр дүнд гарч ирсэн.



ЗУРАГ 6. ШҮҮЖ АВСАН ӨГӨГДӨЛД ИЛЭРСЭН САЙТУУДЫН ДАВТАМЖ

2.2.3. Сүлжээгээр дамжсан зураг болон бусад файлыг задлаж харах

Өөрийн компьютерийн нэг өдрийн өгөгдлийг wireshark програм дээр нээж дараах үйлдлийг хийж гүйцэтгэв.

- Сүлжээгээр дамжиж буй файлуудыг замаас нь чагнаж харахын тулд File цэсний Export object-HTTP арга ашигласан.
- Гаргаж авсан файл, зургийн жишээ харуулбал

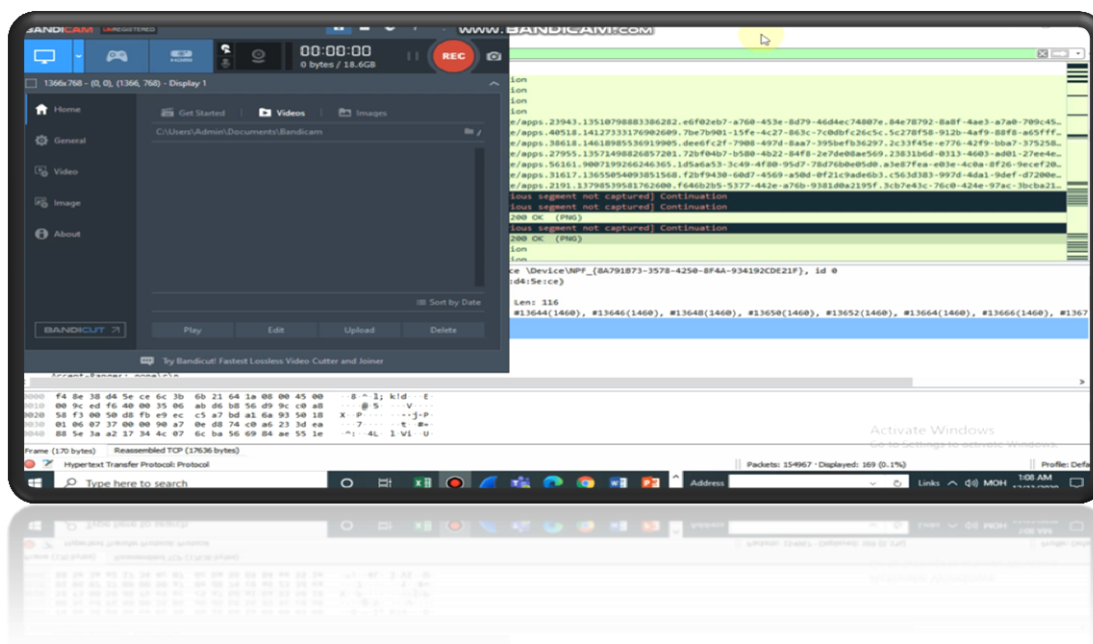
Name	Date modified	Type	Size
admin	12/4/2020 4:45 PM	File	1 KB
back.gif	12/4/2020 4:45 PM	GIF File	1 KB
blank.gif	12/4/2020 4:45 PM	GIF File	1 KB
ChFnb29nLXBoaXNoLXNoYXZhchAAGI33...	12/4/2020 4:45 PM	File	4 KB
ChFnb29nLXBoaXNoLXNoYXZhchAAGIH...	12/4/2020 4:45 PM	File	159 KB
ChFnb29nLXBoaXNoLXNoYXZhchAAGIH...	12/4/2020 4:45 PM	File	87 KB
ChFnb29nLXBoaXNoLXNoYXZhchAAGIH...	12/4/2020 4:45 PM	File	188 KB
ChFnb29nLXBoaXNoLXNoYXZhchAAGM...	12/4/2020 4:45 PM	File	54 KB
ChNnb29nLW1hbHdhcmUtc2hhdmFyEAE...	12/4/2020 4:45 PM	File	70 KB
ChNnb29nLW1hbHdhcmUtc2hhdmFyEAE...	12/4/2020 4:45 PM	File	127 KB
downloads%3fclient=navclient-auto-ffox...	12/4/2020 4:45 PM	2&WRKEY=AKEG...	5 KB
downloads%3fclient=navclient-auto-ffox...	12/4/2020 4:45 PM	2&WRKEY=AKEG...	1 KB
favicon(1).ico	12/4/2020 4:45 PM	Icon	1 KB
favicon.ico	12/4/2020 4:45 PM	Icon	1 KB
index.php%3f=PHPE9568F34-D428-11d2...	12/4/2020 4:45 PM	PHP%3F=PHPE956...	3 KB
index.php%3f=PHPE9568F35-D428-11d2...	12/4/2020 4:45 PM	PHP%3F=PHPE956...	3 KB
index.php%3f=SUHO8567F54-D428-14d...	12/4/2020 4:45 PM	PHP%3F=SUHO85...	3 KB
owned(1).png	12/4/2020 4:45 PM	PNG File	17 KB
owned.png	12/4/2020 4:45 PM	PNG File	17 KB
unknown.gif	12/4/2020 4:45 PM	GIF File	1 KB
update(1).php	12/4/2020 4:45 PM	PHP File	1 KB

ЗУРАГ 7. СҮЛЖЭЭГЭЭР ДАМЖСАН ФАЙЛУУД ГАРГАЖ АВСАН БАЙДАЛ



ЗУРАГ 8. СҮЛЖЭЭГЭЭР ДАМЖСАН ЗУРАГ

2.2.4. Чагнасан файлаас зураг ялгаж харах видео заавар



ДҮГНЭЛТ

Онолын судалгааны хэсэгт Wireshark програмтай холбоотой судалсан гол гол мэдээллээ оруулснаас гадна програмын цонх буюу интерфейс тус бүрийг дэлгэрэнгүй тайлбартайгаар орууллаа. Wireshark программыг өмнө огт судалж байгаагүй болохоор эхнээс нь эхлээд бүх зүйлсийг нь сурах шаардлагатай болсон судалгаагаа интернет сайт англи, монгол wireshark-ийн тухай гарын авлага, номуудаас эш татан бичсэн.

Туршилт судалгааны хувьд Wireshark программыг өөрийн компьютерт болон лабораторийн компьютерт суулгав. Ингэснээр дараах өгөгдлүүдийг бичиж авсан. Үүнд:

- 12-503 Компьютерийн лабораторийн нэг компьютерийн 5 өдрийн өгөгдөл,
- Өөрийн компьютерийн 1 өдрийн өгөгдөл

Ингээд гол өгөгдлөө цуглуулж авсны дараагаар тухайн өгөгдлийг wireshark програм ашиглан шинжлэх боломжтой болсон. Туршилтын хэсэгт лабораторийн өгөгдлүүдээс оюутнуудын ашигладаг сайтуудын мэдээллийг пакет шүүж, тэдгээрээ задлан харж цуглуулсан мөн өөрийн компьютерээс бичсэн өгөгдлөөс файлуудыг ялган задалж харууллаа.

Ингэхдээ түүнийг хийх алхам бүрийг тайлбарласнаас гадна wireshark дээр ажиллах үедээ дэлгэц бичиж видео заавар боловсруулсан болно.

Wireshark-ийг сүлжээний өгөгдөлд задлан шинжилгээ хийж, мэдээлэл гаргаж авахад ашиглаж болохоос гадна сүлжээгээр дамжиж буй өгөгдлийн бүтцийг тайлбарлахын тулд мэргэжлийн хичээл буюу компьютерийн сүлжээ, сүлжээний техник хангамж зэрэг хичээлүүдэд хавсаргаж орвол илүү тохиромжтой санагдлаа.

Мөн энэхүү судалгааны ажлыг хийснээр онолын мэдлэгээ бататгаж, илүү их мэдээллийг олж, туршилт хийж чадсанаараа үр дүнтэй болсноос гадна цаашид сүлжээгээр дамжиж буй өгөгдлүүдийг илүү сонирхон судлах хэрэгтэй гэдгийг ойлгосон юм.

АШИГЛАСАН МАТЕРИАЛЫН ЖАГСААЛТ

Chung, T. (2009). *How to capture packets*.

Evaluation of the Capabilities of WireShark as a tool for. (2007).

gang, b. (2015). *Wireshark програм хэрэглэгчдийн гарын авлага*. УБ.

Wireshark, I. t. (n.d.).

Базар. (2015). *Wireshark програм хэрэглэгчдийн гарын авлага*. Улаанбаатар .

Д.Бямбадорж, С. (2017). *Дотоод сүлжээгээр дамжиж буй өгөгдлөөс*. Улаанбаатар хот