Forgalmi mérések a gyakorlatban

Mérési feladatok

1. A Wireshark alapvető funkcióinak használata

1.1 Nyissa meg a Wireshark alkalmazást és indítsa el a csomagrögzítést. Van-e bármilyen csomagforgalom? Ha igen, mi ennek a magyarázata?

1.2 Indítson böngészőt, és nyisson meg egy tetszőleges oldalt. Szűrje ki csak azokat a csomagokat, melyek a honlap letöltéséhez kapcsolódtak. Milyen szűrőt használt?

1.3 Zárjon be minden alkalmazást, ami jelentős forgalmat bonyolít a 443-as TCP porton. Indítsa el a Google Chrome böngészőt és nyisson meg egy megfelelően nagy méretű HTTPS oldalt. Szűrje ki Wiresharkban az oldal letöltéséhez kapcsolódó forgalmat. Állítsa be a Wiresharkot, hogy dekódolja a titkosított forgalmat (lásd. Tudnivalók). Milyen nehézséget okozhat forgalmi elemzés szempontjából a HTTPS?

2. Youtube adatforgalom szűrése és elemzése

2.1 Nyissa meg böngésző segítségével a Youtube oldalát és keressen egy megfelelően hosszú videót, majd indítsa el. Szűrje ki a videó letöltéséhez kapcsolódó csomagokat, ezeket mentse csv fájlba. Számolja ki a csomaghossz várható értékét és relatív szórását. Vizsgálja meg a csomagok hosszának eloszlását hisztogram segítségével. Értelmezze az eredményt.

2.2 Vizsgálja meg a csomagok érkezési időit és időközeit. Készítsen az időközökről statisztikát (várható érték, relatív szórás) és értékelje ezt. Ezután vizsgálja meg az érkezési időközök tapasztalati eloszlásfüggvényét például hisztogram segítségével. Mit tapasztal?

3. VoIP forgalom szűrése és elemzése – opcionális feladat

3.1 Indítson el egy tetszőleges VoIP alkalmazást, indítson rajta hívást és vizsgálja meg a hozzá tartozó forgalmat. (Érkezési időközök, csomaghossz statisztikák.) Milyen különbségeket tapasztal a korábbi forgalmi mintákhoz képest?

3.2 Indítson hívást a Discord nevű böngészőből használható VoIP alkalmazás segítségével és vizsgálja meg a hozzá tartozó forgalmat. Hasonlítsa ezt össze a korábbi eredményekkel.

4. Passzív forgalmi mérés

4.1 Töltse le a mérésvezető által megadott capture fájlt és elemezze azt. Nyerje ki az alábbi információkat (részletek a Tudnivalók című dokumentumban):
- A teljes forgalom sebessége 1 másodperces lépésközzel
- A csomaghosszak eloszlása
- A forgalom protokollok szerinti megoszlása
- A legnépszerűbb portok statisztikái

4.2 (Opcionális feladat) Nyerje ki az alábbi hoszt és flow alapú statisztikákat:
- A forgalom megosztása hosztok szerint. A forgalom mekkora részéért felelősek a népszerű hosztok?
- A forgalom flow-k szerinti statisztikái. Milyen a flow-k hosszának eloszlása? És a flow-k méretének eloszlása?