**Biztonság és védelem az**

**informatikában**

**2. gyakorlati feladat**

Készítette: Baranyi Gábor  
CRC7FC

Felhasznált programok:

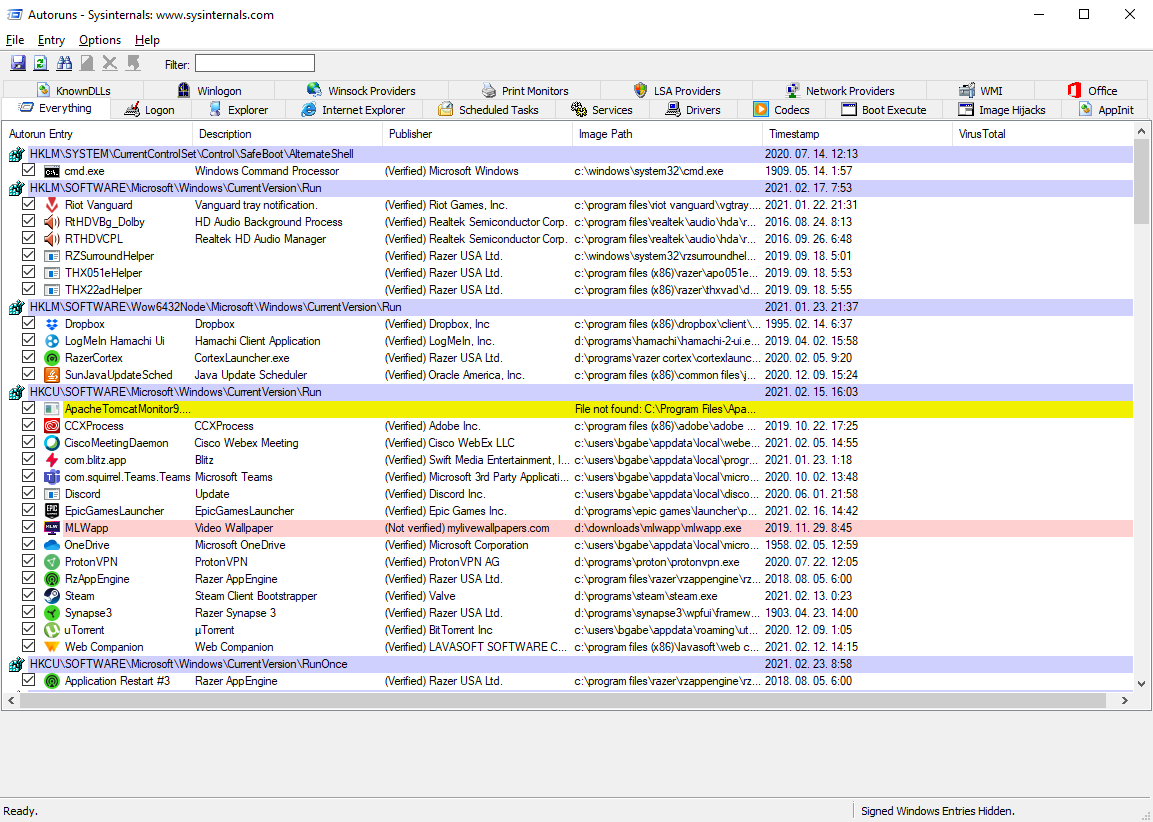
WindowsPortableApps, TcpView, ProcessExplorer, AutoRuns, WireShark

2021.02.18

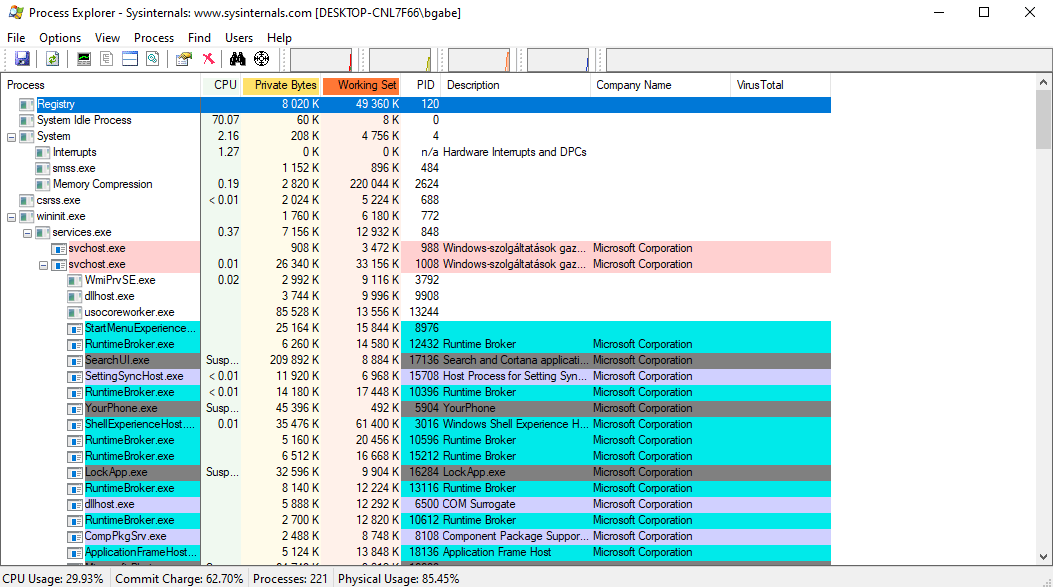
**Bot, Worm behatoló detektálása**

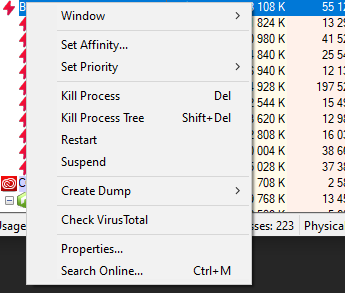
Miután a leírtak szerint letöltöttem a WindowsPortableApps, tcpView, ProcessExplorer és AutoRuns alkalmazásokat, és a licenseket is jóváhagytam az Autoruns programot indítottam el.

Ezen alkalmazás segítségével a jelenleg futó alkalmazásokat tudom megtekinteni:



A részletesebb vizsgálathoz ProcessExplorer-t használtam, melyet a feladat leírásban megjelölt linken töltöttem le.

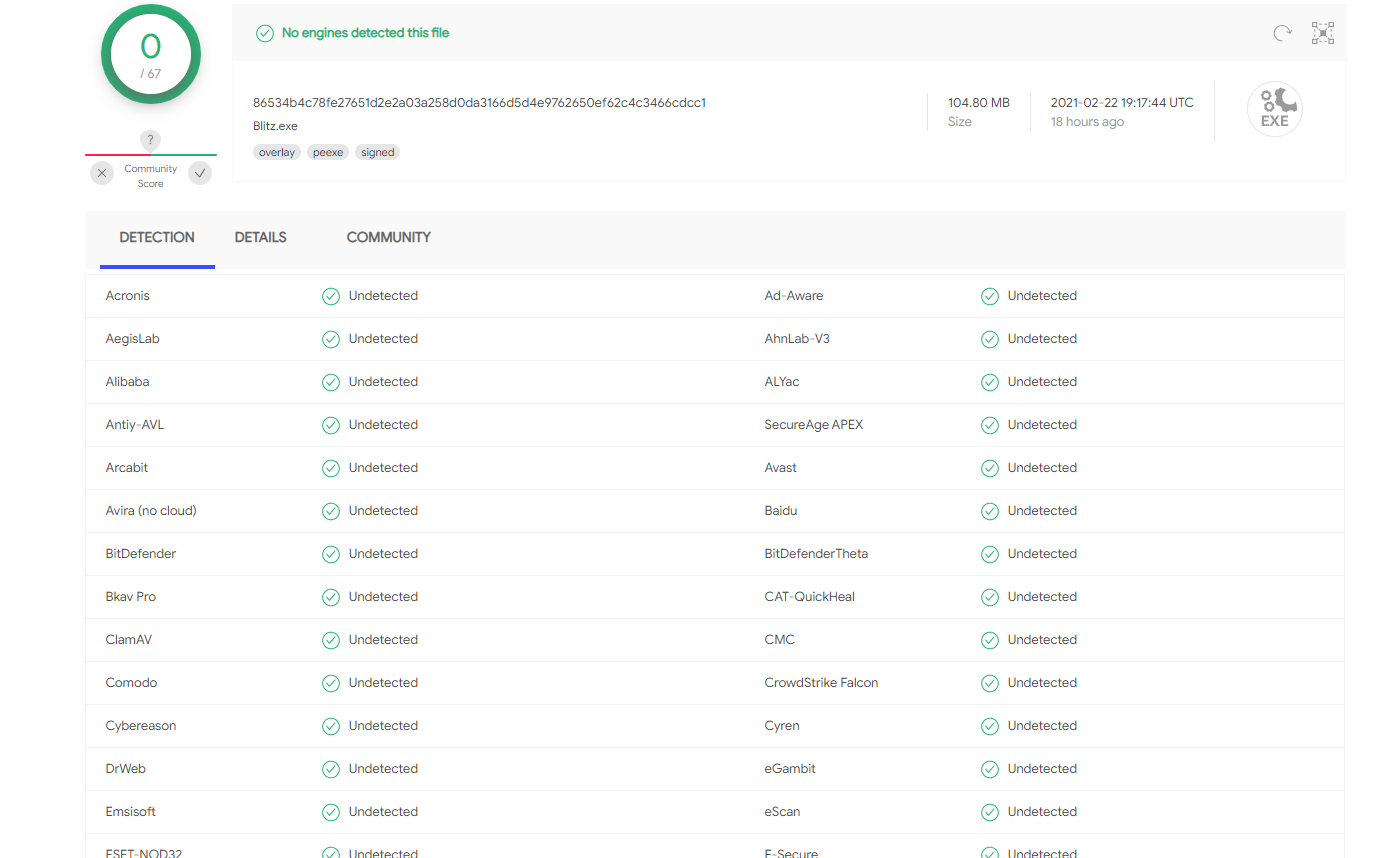


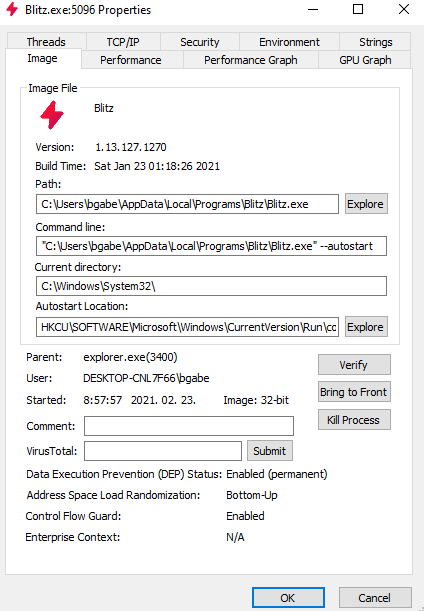


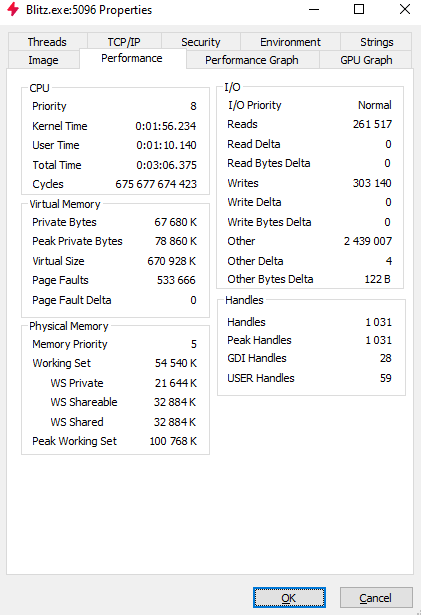
Lehetőségünk van leállítani újraindítani elindítani, illetve felfüggeszteni az alkalmazásokat.

Gyanús programok esetén még esélyünk van egy Check VirusTotal lehetőségre is mely során a programról készített egyedi hash-t vírus keresőket tartalmazó weblapra küldi el, majd megtekinthetjük az eredményeket a legutolsó sorban lévő ’0/75’- re kattintva.

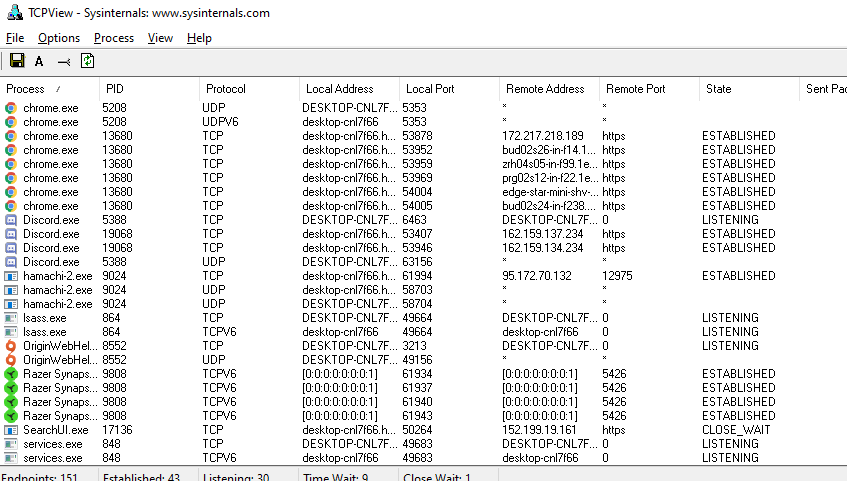


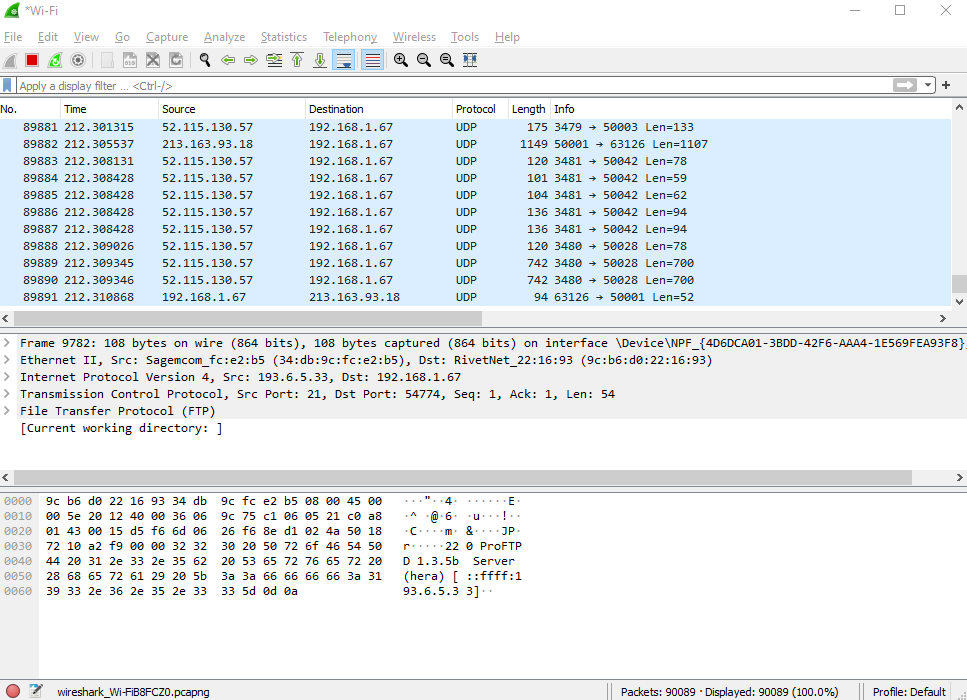


Egy futó alkalmazásra jobb gombbal kattintva majd a properties menüpontot kiválasztva Részletes információt kapunkhatunk róla. Ilyenek például: a verziószám, a program indulási helye, adott user azonosító, aki használja és a futtatás kezdetének időpontja.A Performance fülön keresztül pedig további információkhoz juthatunk a processzor, a virtuális, illetve fizikai memória adatairól, valamint a I/O műveletekről.

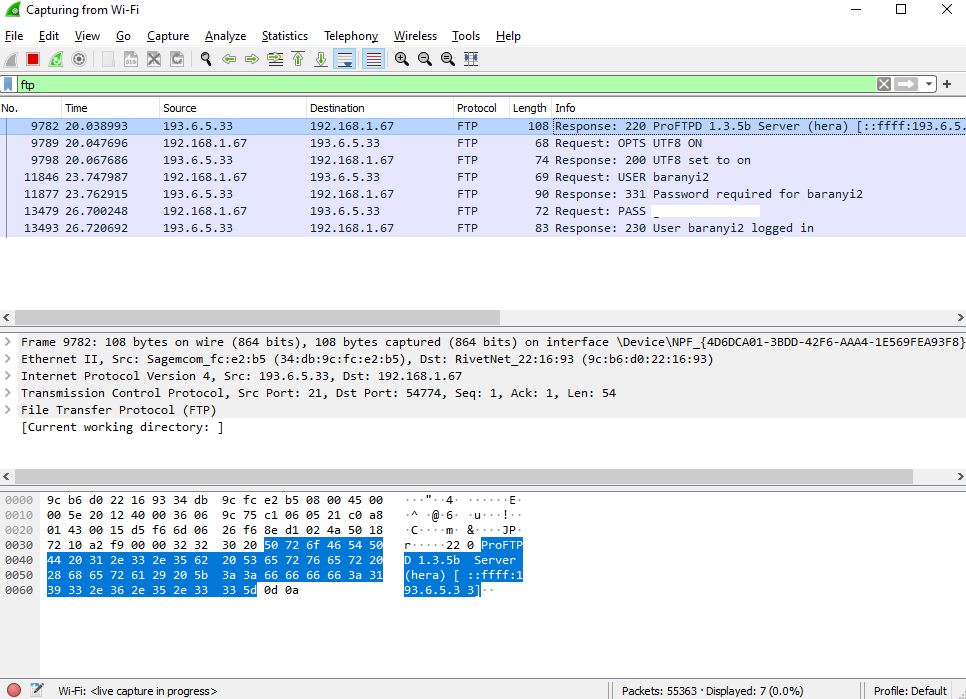


A harmadik TcpView melyel az éppen futó alkalmazások hálózati használati tulajdonságát tudom elemezni. A state oszlopban a státusz tulajdonság szerepel mely azt jelzi, hogy a program vár a kapcsolódásra ’Listening’ vagy pedig már kapcsolódott ’Established’.



Végül már csak a wireShark maradt kipróbálásra.

A leírtak szerint a Commanderrel bejelentkeztem a Miskolci egyetem ftp-szerverére és ki capture-öltem a bejelentkezési információkat.

****