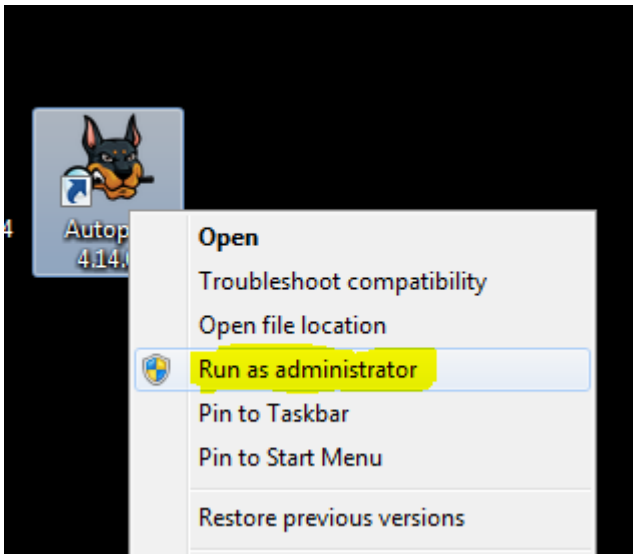
Taitaja2021 -kyberturvaohjelmistojen käyttöohjeet

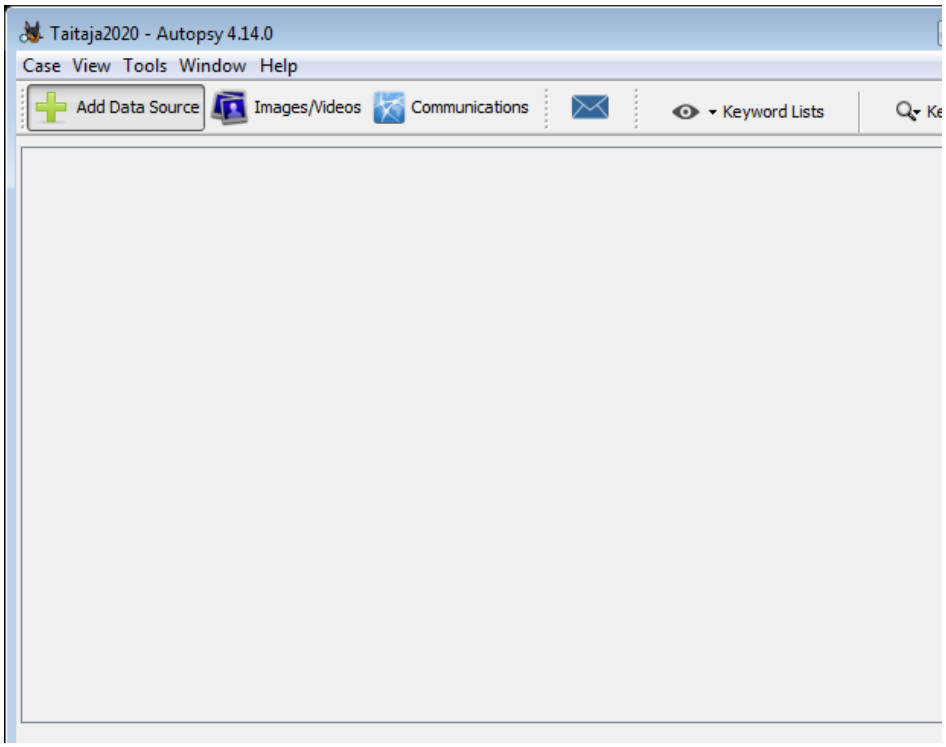
Autopsy

1. Käynnistä autopsy pääkäyttäjänä.

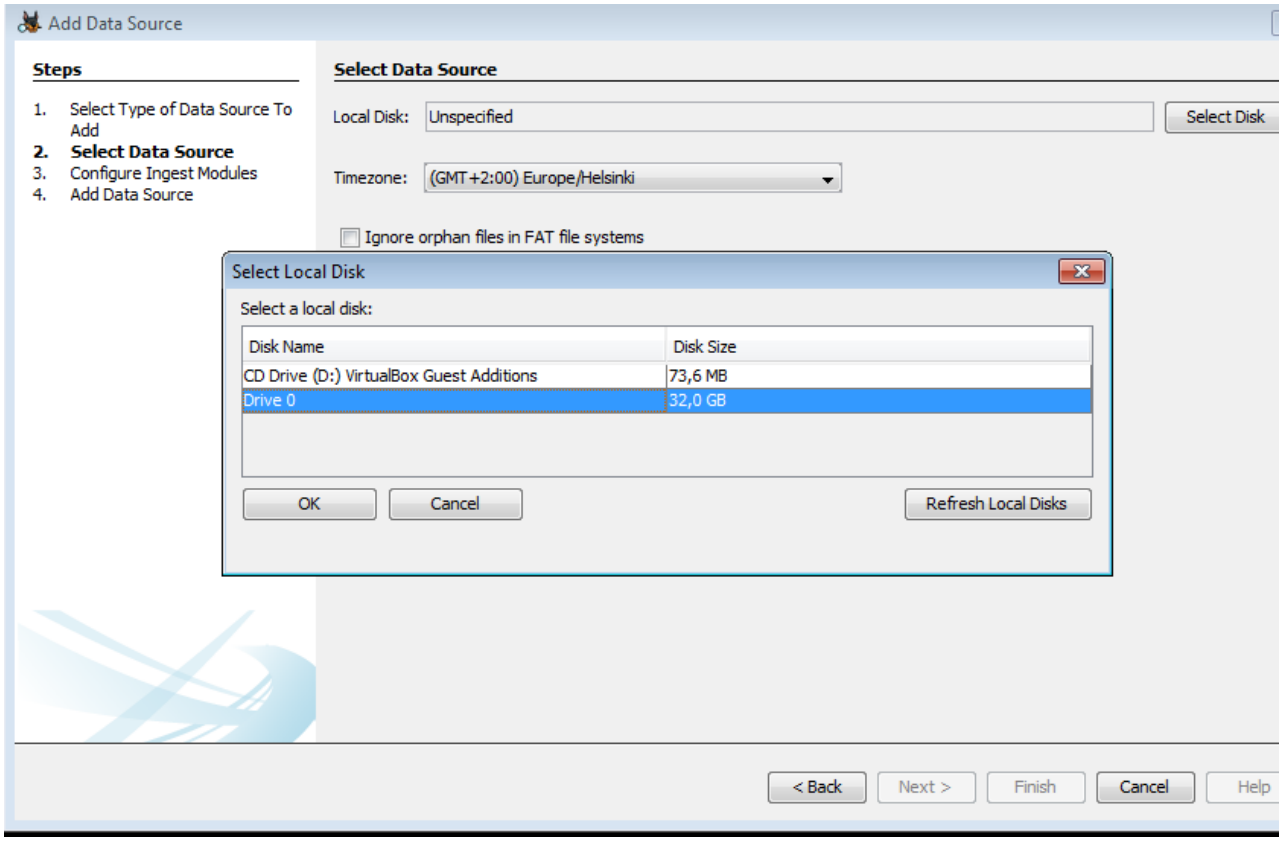


2. Avaa joko uusi tapaus tai avaa viimeisin.

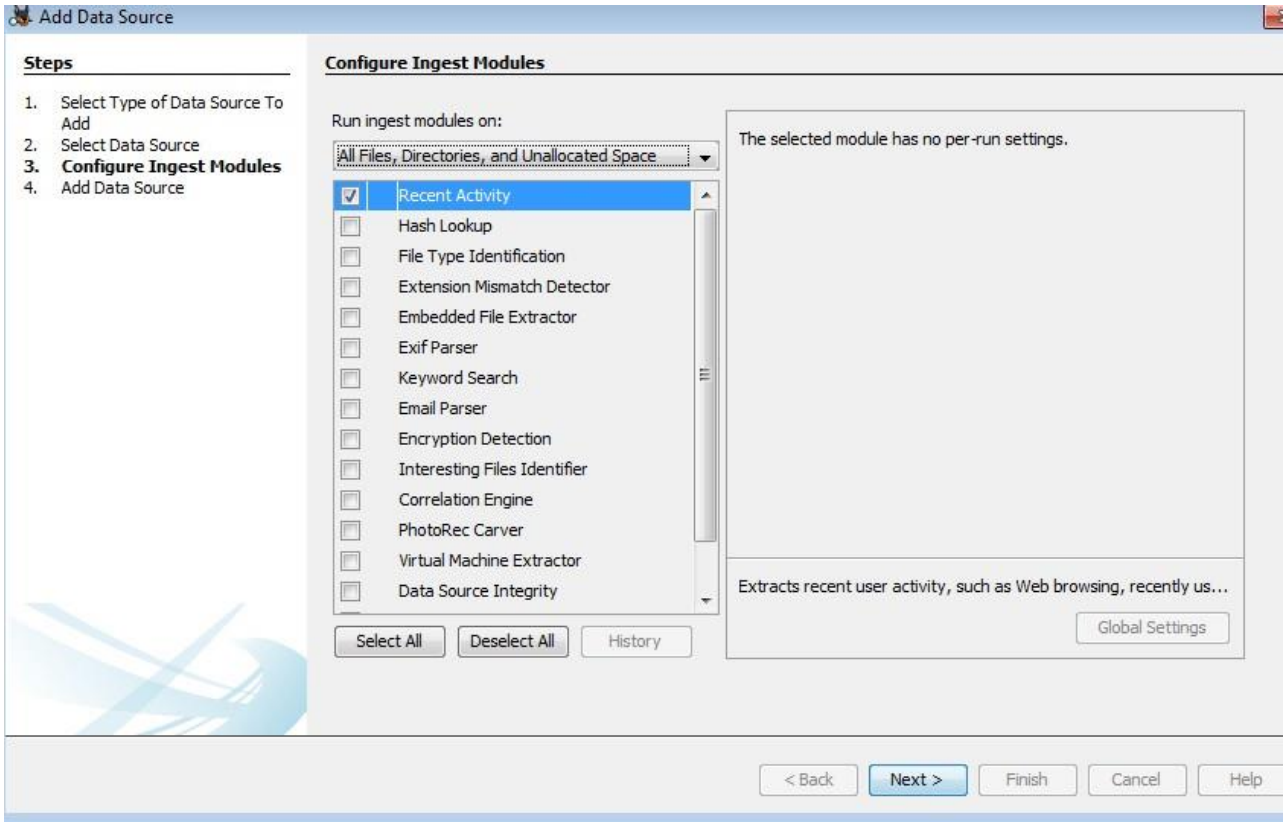
3. Lisää Datasource eli tietolähde, jota tutkitaan



4. Valitse Drive 0

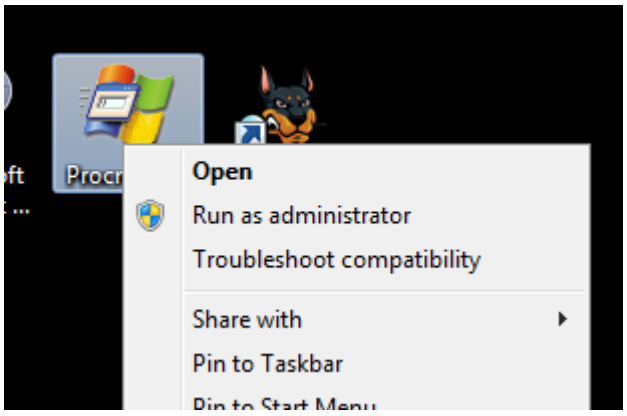


5. Suorita vain Recent Activity, se riittää tähän harjoitukseen.

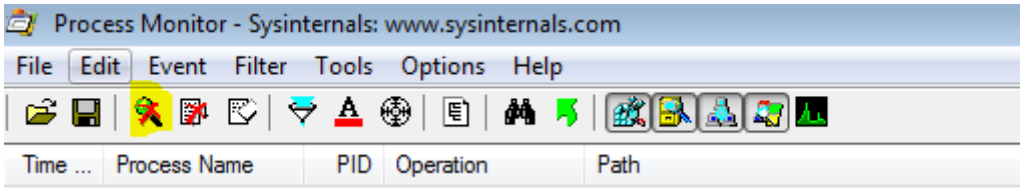


Procmon eli prosessimonitori

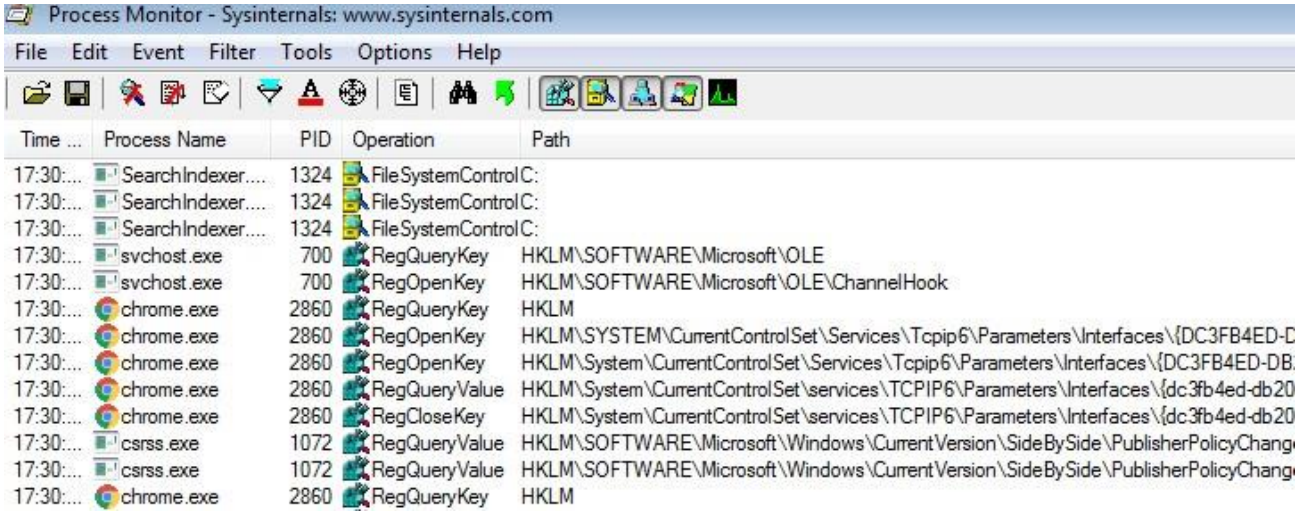
1. Aja pääkäyttäjänä



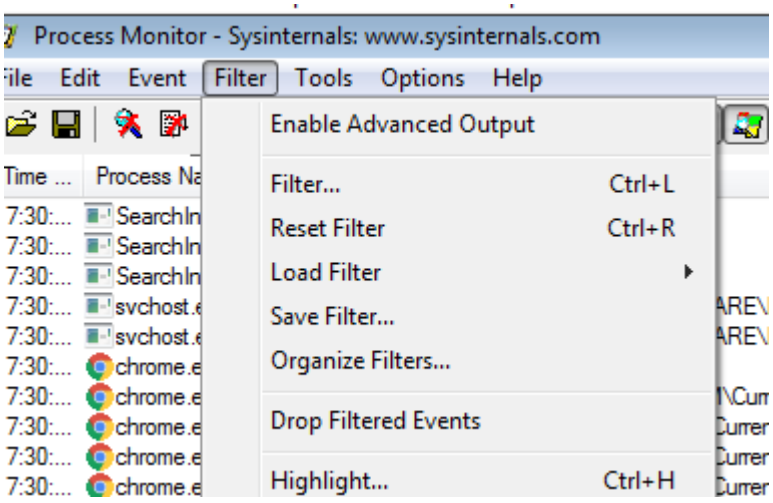
2. Ctrl + E tai kuvassa korostettu aloittaa capturen



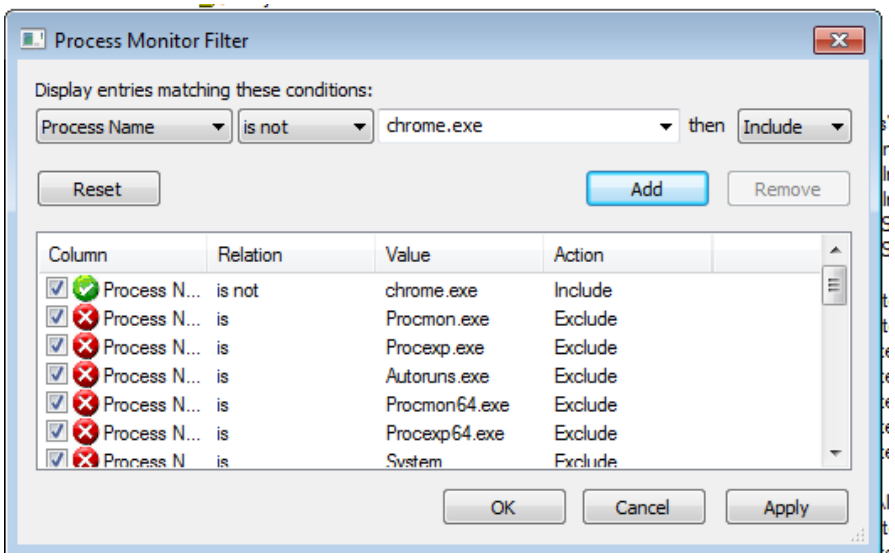
3. Process monitor listaa kaikkien prosessien toiminnot, Harjoituksessa riittää noin 5 minuutin tallennus, jonka jälkeen sen voi lopettaa ja alkaa tutkimaan prosesseja.



4. Prosesseja on paljon, joten kannattaa filteröidä varmat pois.

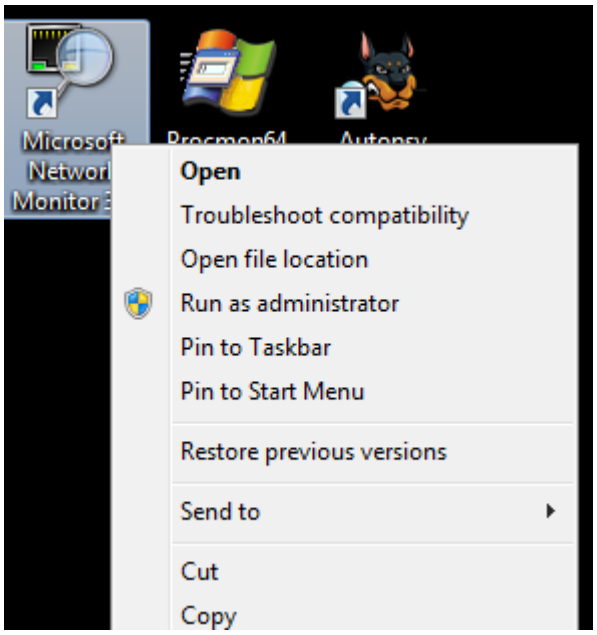


5. Filtereitä saa lisättyä painamalla add nappia,jonka jälkeen apply

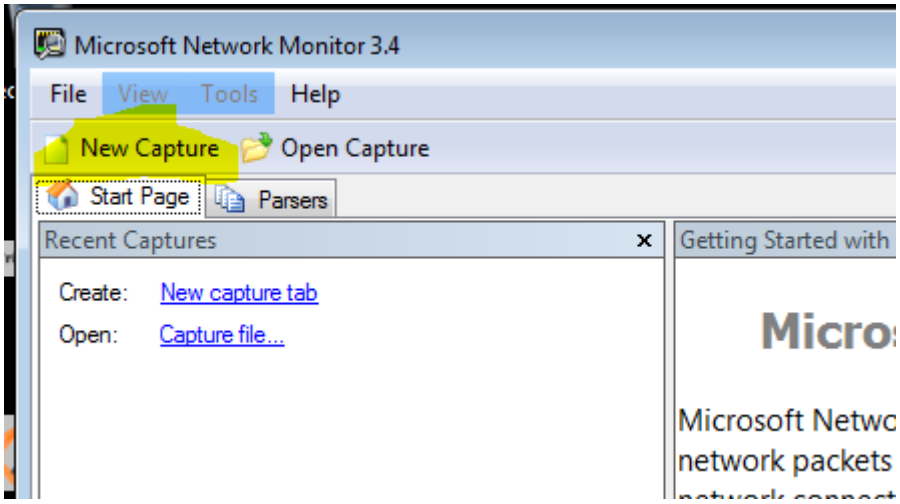


Netmon eli Network monitor

1. Suorita pääkäyttäjänä



2. Luo uusi tallennustieodsto eli capture



3. Aloita verkkoliikenteen tallennus, noin 5-10 minuuttia on riittävä tallennus pituus.