# Procmon

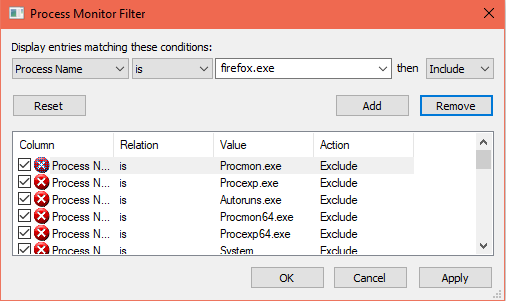
Procmon eli Process monitor on Sysinternals paketissa oleva ohjelmisto. Se on periaatteessa Task Manager steroideissa. Siitä löytyy paljon enemmän toimintoja ja syvällisempää tietoa.

Lataa ja asenna Procmon. <https://docs.microsoft.com/en-us/sysinternals/downloads/procmon>

Avaa Procmon järjestelmänvalvojan oikeuksin. Kun avaat sen se alkaa skannaaman konettasi ja etsii erilaiset prosessit. Kuvan timantista saat avattua suodattimen jonka avulla voit filteröidä mitä prosesseja seurataan.



Filteröinti ikkunasta voit muodostaa erilaisia filttereitä. Näin voisit mahdollisesti etsiä haittaohjelmia tietokoneelta.

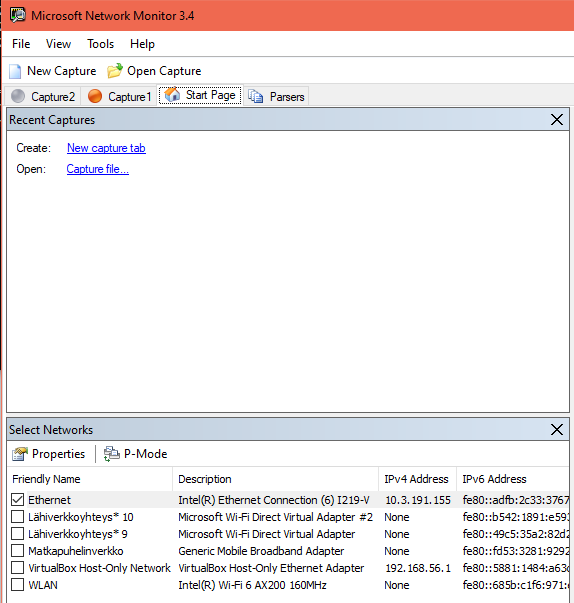


# Netmon

Netmon on Wiresharkin kaltainen ohjelmisto jolla pystyy monitoroimaan tietokoneen verkkoliikennettä.

Latausosoite: <https://www.microsoft.com/en-us/download/4865>

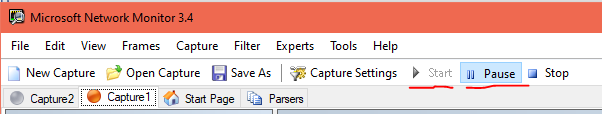
Aloitussivulta voit valita mitä verkkokorttia netmon kuuntelee kun se kaappaa liikennettä.



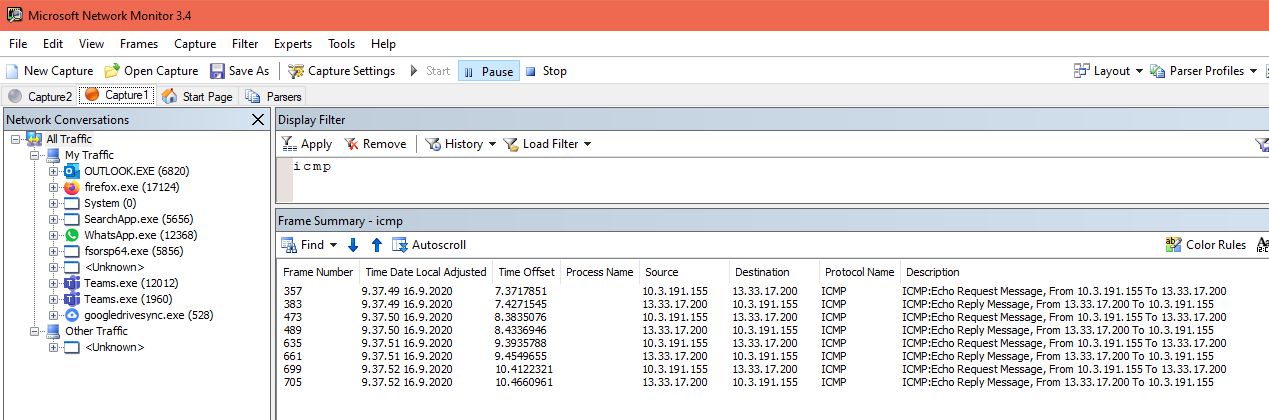
Jos netmon ei löydä mitään verkkokortteja seuraa tästä linkistä löytyviä ohjeita **kohdasta ”Findings and Solution (Part 1) – Missing Driver”**: <https://vbzine.wordpress.com/2011/05/21/resolve-why-no-network-adaptor-shows-up-in-microsoft-network-monitoring-tool-plus-bonus-issue/>

New capture kohdasta voit aloittaa uuden kaappauksen.

Start ja Pause näppäimillä voit aloittaa tai laittaa kaappauksen tauolle.



Kaappauksen jälkeen voit käyttää Display Filter kohtaa filtteröimään tuloksia. Tässä on etsitty kaikki ICMP liikenne. Tässä pingattiin osoitetta yle.fi.



Ohjelmaa voisi käyttää esimerkiksi kun yritetään jäljittää haittaohjelmaa joka kommunikoi hallintapalvelimen kanssa. Hallintapalvelimen voi lähettää zombille (jolla haittaohjelma sijaitsee) komentoja joita sen tulee tehdä ja ajoittaisia viestejä jotka kertovat että zombi on edelleen elossa.

Liikenteen seasta voi myös löytyä epäilyttävää liikennettä jonka voi havaita netmonilla.

# Autopsy

Autopsy on ohjelmisto joka kerää kaikenlaista tietoa tietokoneesta jota voidaan käyttää hyödyksi tietoturvassa. Se on erityisen kätevä kun pitää selvittää miten jokin asia tapahtui. Esimerkiksi miten jokin haittaohjelma tuli yrityksen laitteelle.

Latausosoite: <https://www.autopsy.com/download/>

Osoitteesta: <https://medium.com/@tusharcool118/autopsy-tutorial-for-digital-forensics-707ea5d5994d> löytyy hyvät ohjeet Autopsyn käyttöön.

**HUOM! Step 6 kohdassa valitse vain Recent History niin skannaus ei kestä niin kauan aikaa.**