TCP/IP repetition

Formål

Formålet med denne øvelse er at få et praktisk kendskab til programmet *Wireshark* og opfriske viden om Internet Protokollen. Programmet Wireshark anvendes til netværks analyse og protokol analyse. Programmet er opdelt i en monitor del og en capture del. Monitor delen bruges til at overvåge nettet og få statistiske oplysninger om nettet. Capture delen bruges til at opsamle data pakker (fx Ethernet) fra nettet og analysere protokollerne der er i pakkerne. Som måleobjekt bruger vi pc'erne og kommandoen PING. Bagerst i øvelse er der en hjælpeside som forklarer capture skærmens opbygning.

Opgaver

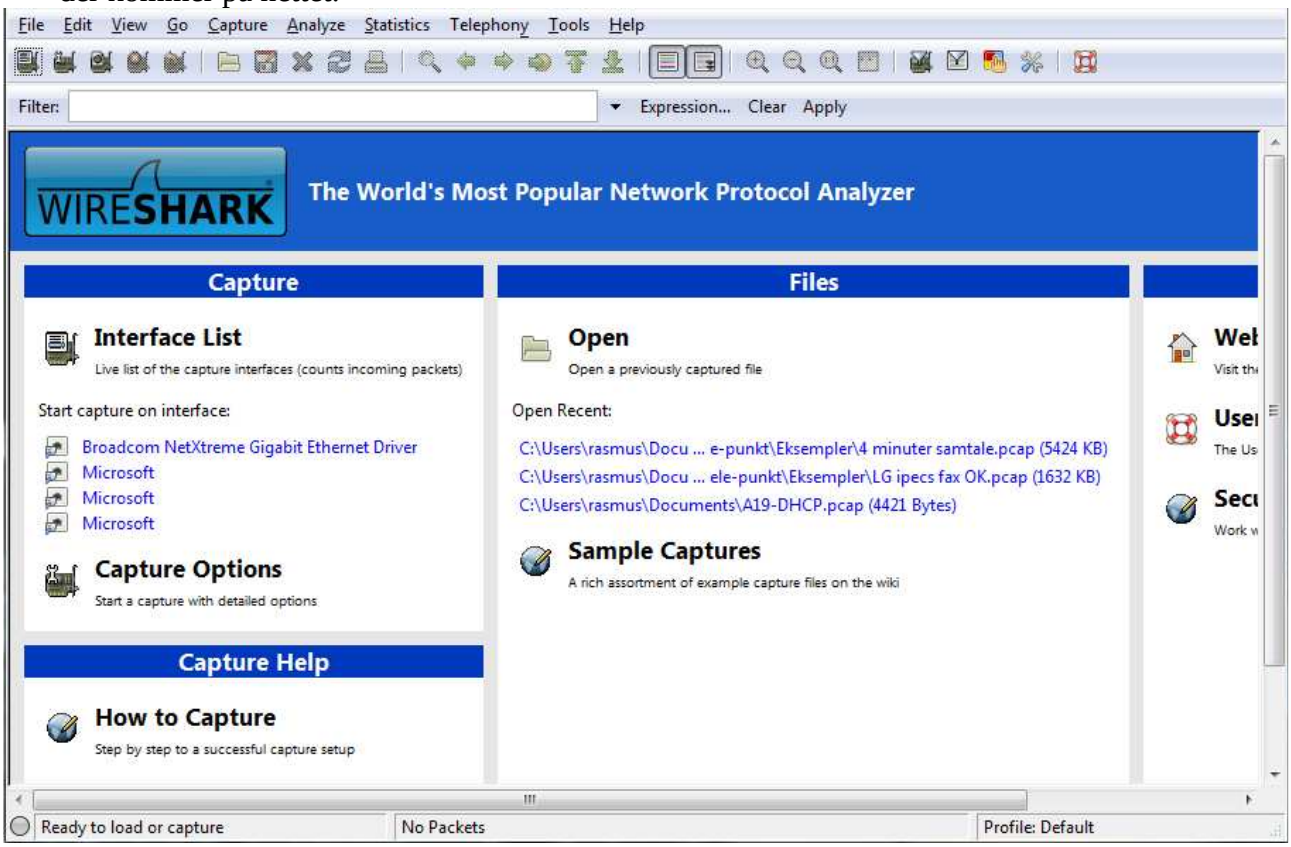
1. I skal først undersøge hvilken IP adresse jeres computer har. Fra kommando prompten (vælg **Start | Kommandoprompt**) startes programmet **IPCONFIG**

   Noter hvilken IP adresse maskinen har nu: _____

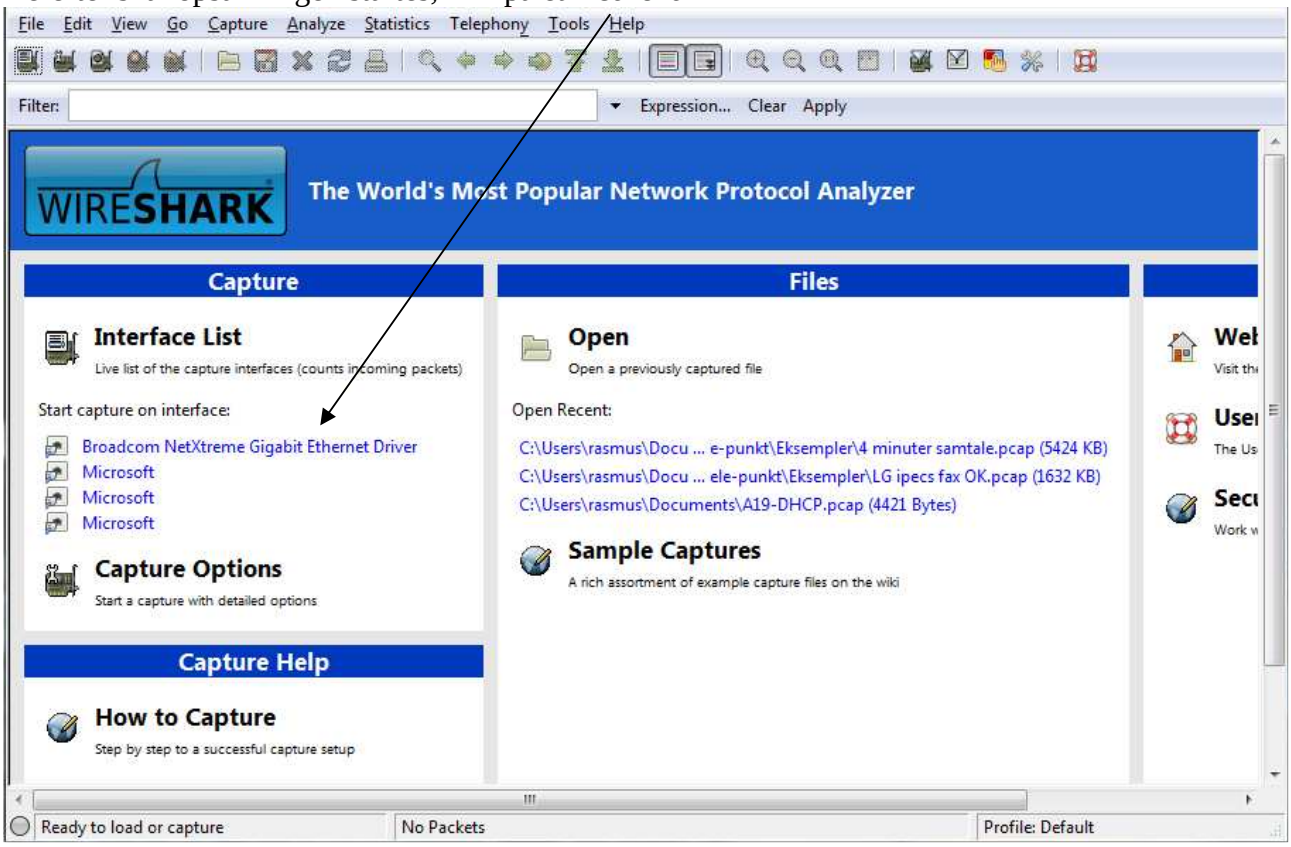
2. Start programmet Wireshark på computeren, vælg følgende:

   Start | Alle Programmer | Wireshark

   Programmet skal bruge mindst et netkort til dataopsamling, vælg et kort fra interface listen**.** Wireshark sætter netkortet i promiscuous mode, hvilket betyder at netkortet opsamlet alt hvad der kommer på nettet.



Herefter skal opsamlingen startes, klik på et **Netkort**



Prøv nu at sende en PING til computer ved siden af din. Start fra kommando prompten og indtast følgende: **PING IP adresse** på nabo maskinen.

Når PING kommandoen er færdig klikkes på **Stop Capture.**

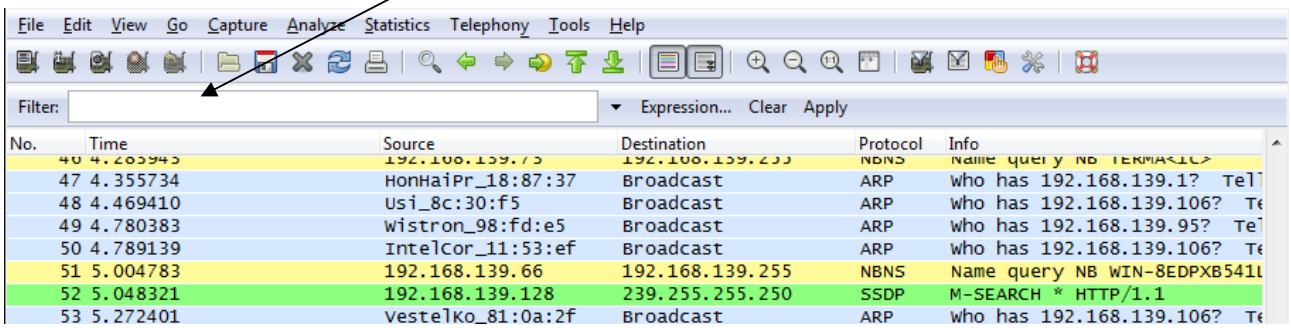
Noter TTL (Time To Live) værdien for en af de pakker som du sender, altså PING Req: _____

Noter TTL værdien for en af de pakker som du modtager, altså PING Reply: _____

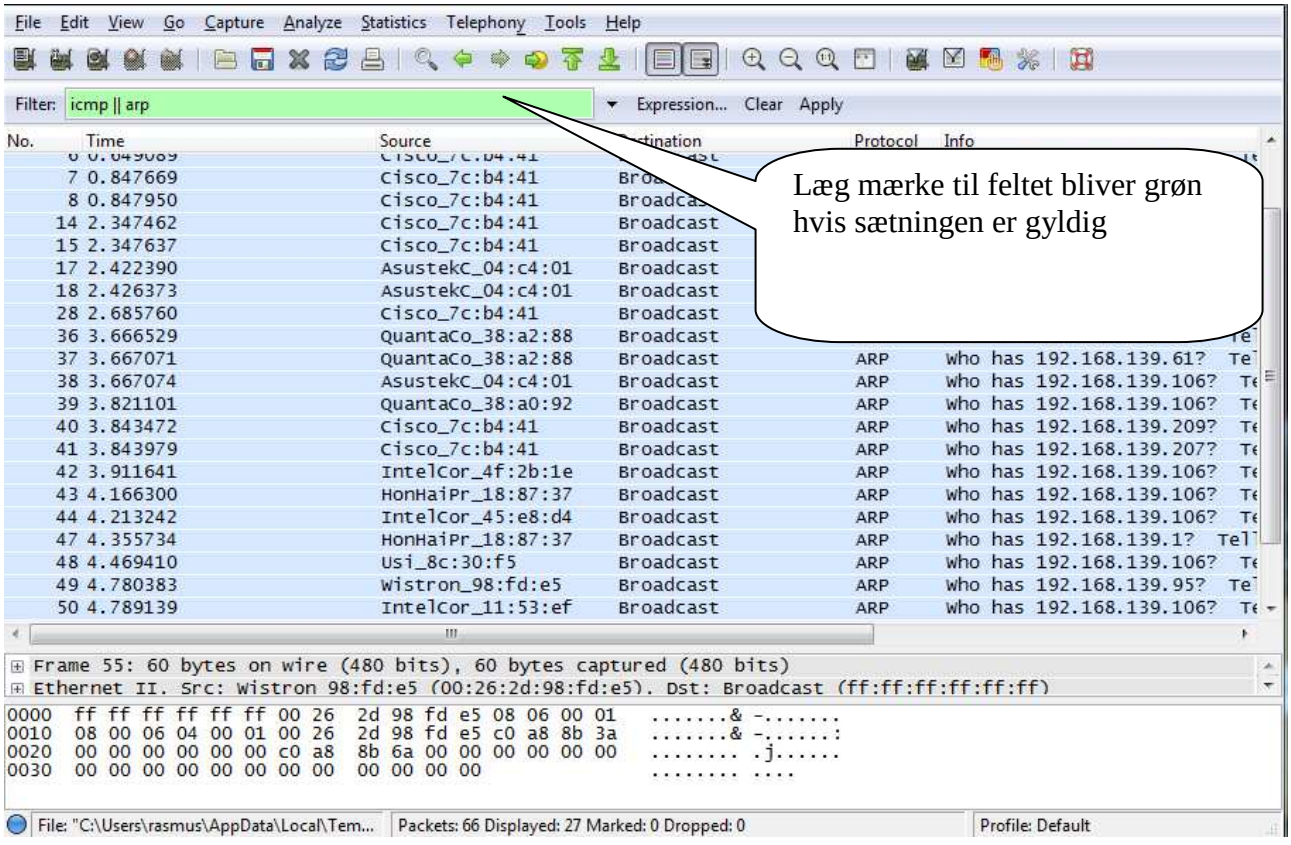
Display filter

Som du kan se i den foregående opsamling er der datapakker fra mange af de andre computere. For at fjerne dem skal der opsættes et filter, der filtrere alle pakker væk som ikke er til din computers fysiske adresse (MAC adresse). Alle pakker opsamles stadig, men kun de pakker du ønsker at se vises på skærmen.

Overst i Wireshark vinduet befinder **Display Filter** indstillingerne sig. Skriv et nyt filter og klik på Apply knappen.



Hvis man fx kun vil se ping og den forudgående arp kan man skriv "icmp || arp". "||" betyder eller når man programmere. Og vil her vise både ping(ICMP) og arp pakker.



Opsamling af netværkstrafik med filter

Du skal nu prøve at opsamle en PING kommando igen, men denne gang med filteret aktiveret. For at få det hele med skal du slette ARP cachen, som er computerens dynamiske tabel til oversættelse af IP adresser til MAC adresser.

For at slette ARP cachen på computeren indtastes fra kommando prompten: **ARP -d**

Start opsamlingen igen og prøv at sende en PING til computer ved siden af din. Når PING kommandoen er færdig stoppes capture.

For at se indholdet af ARP cachen indtastes følgende fra kommando prompten: **ARP -a**

Noter indholdet af ARP cachen: _____

Noter rækkefølgen af de opsamlede pakker (skriv en forkortet tekst fra kolonnen **Summary**):

Pakke 1: (F.eks. 'ARP Request') _____

Pakke 2: _____

Pakke 3: _____

Pakke 4: _____

Pakke 5: _____

Pakke 6: _____

Pakke 7: _____

Pakke 8: _____

Pakke 9: _____

Pakke 10: _____

Undersøg hvilke protokoller en PING-anmodning (Echo Request) indeholder:

_____

_____

_____

3. Du skal nu prøve at opsamle en TRACERT kommando. Lav en opsamling hvor du foretager en TRACERT til **www.iana.org** uden filter:

   Hvor mange gange pinges den første IP-adresse? _____

   _____

   Hvad er værdien af TTL i det første ping ? _____

   _____

   Hvilken information hentes i det første DNS-opslag ? _____

   _____

   Hvilken information hentes i de efterfølgende DNS-opslag ? _____

   _____