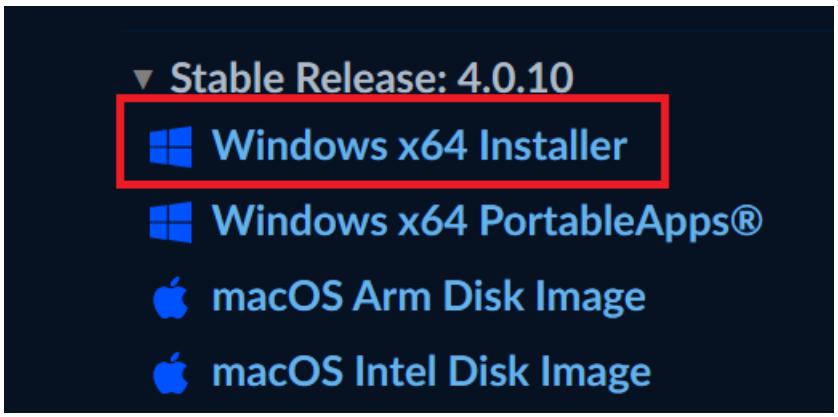
Installera Wireshark

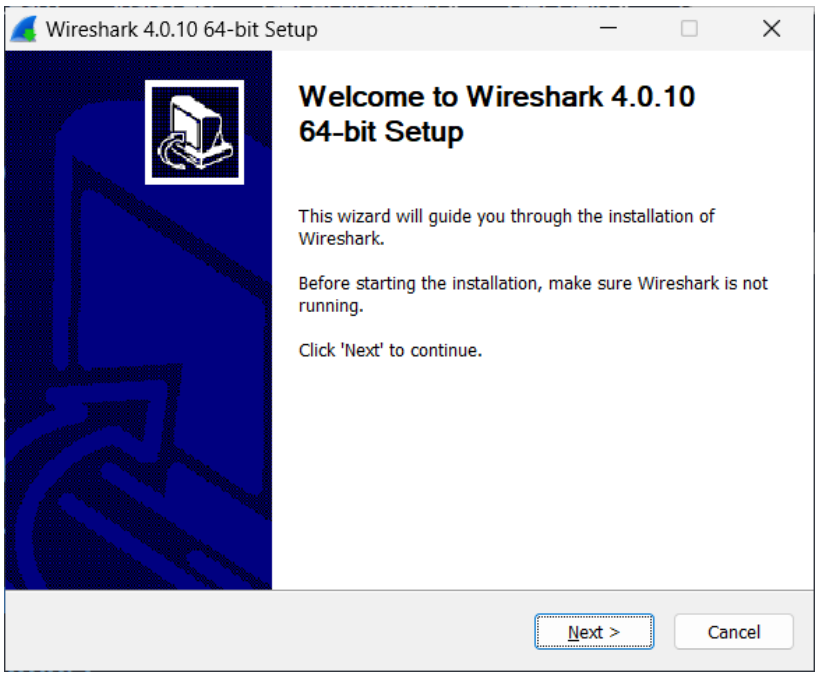
2023-11-01

1. Gå till https://wireshark.org
2. Välj **Download Wireshark Now** eller **Get Acquainted – Download**

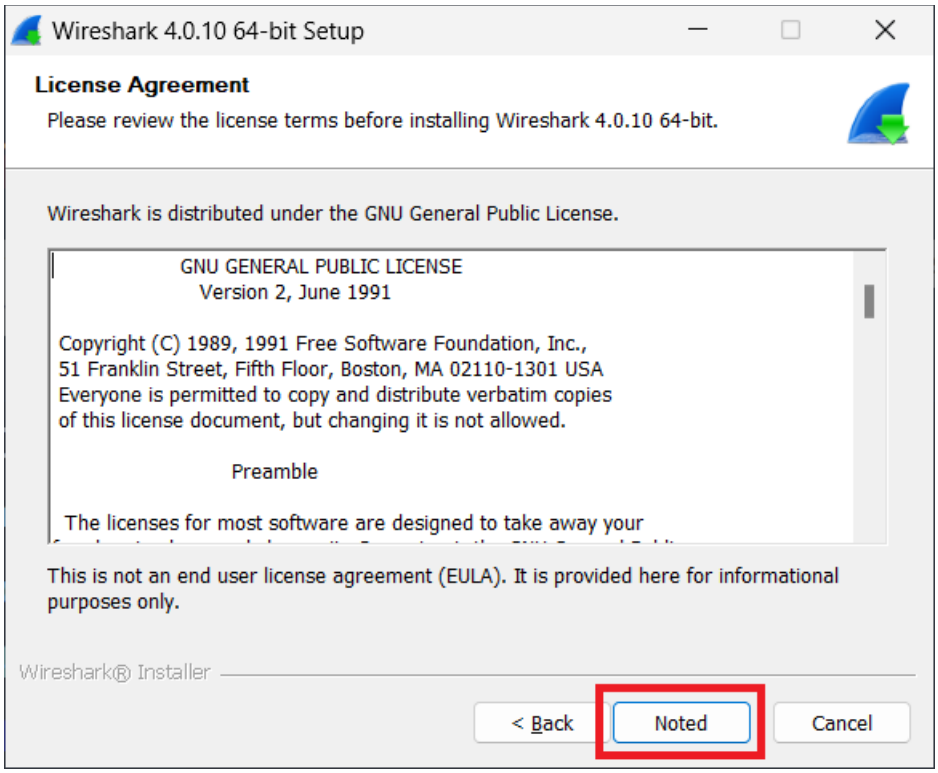
3. Välj **Windows x64 Installer**



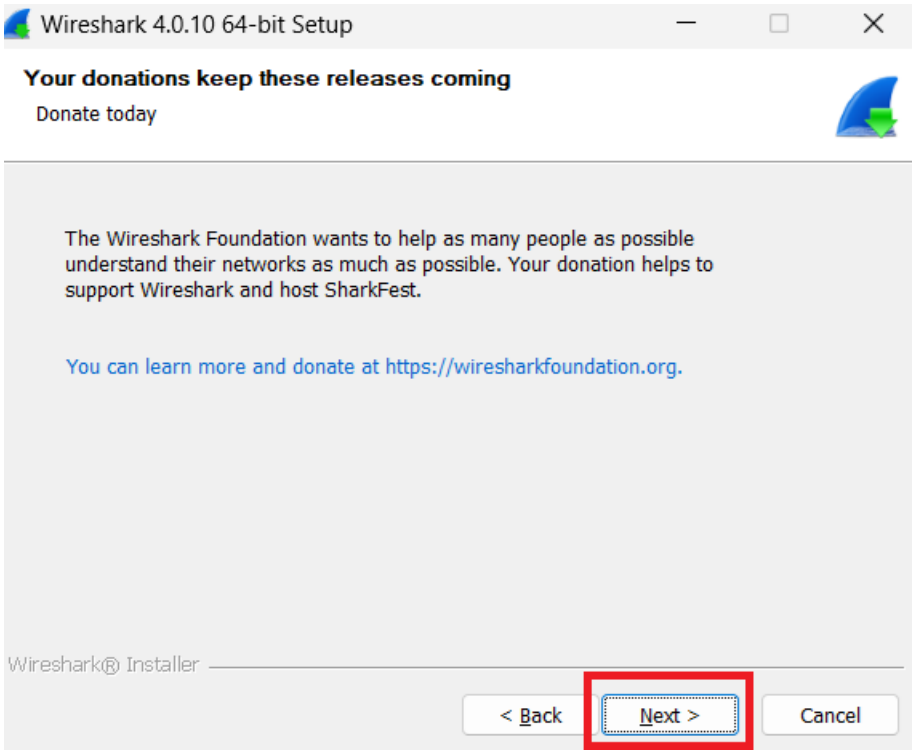
4. Starta installationen och klicka på **Next**



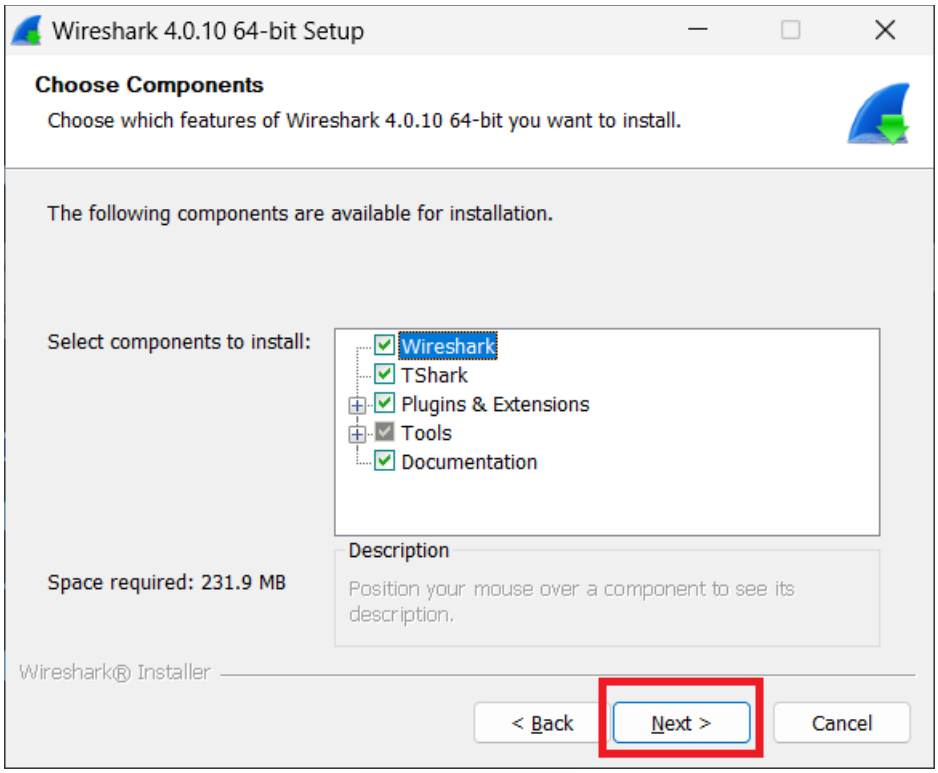
5. Klicka på **Noted**



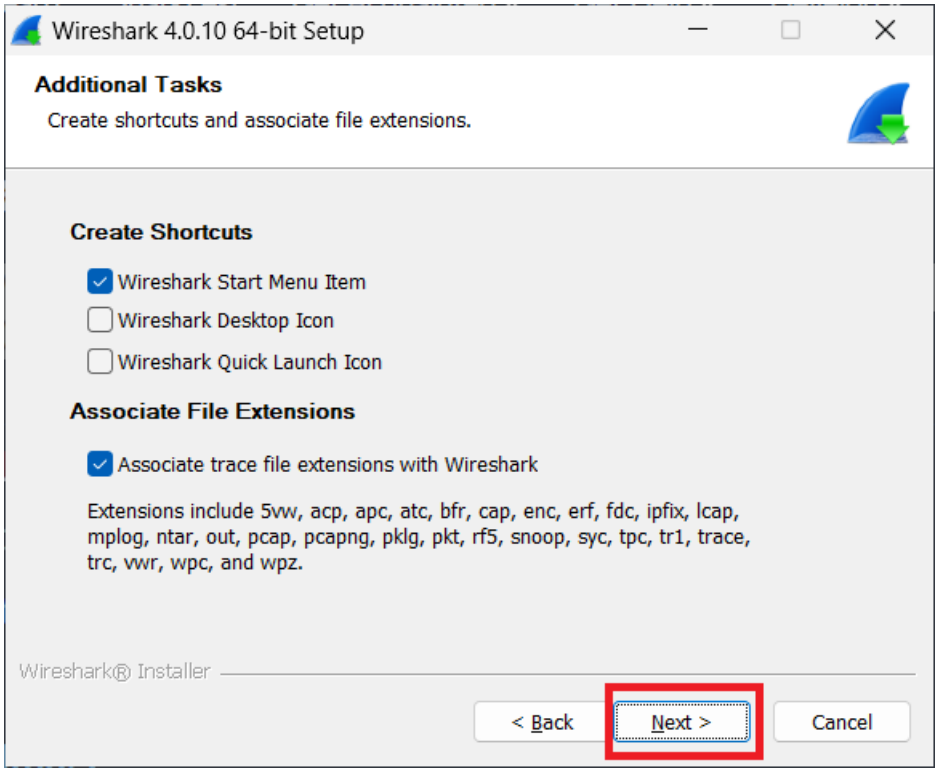
6. Klicka på **Next**



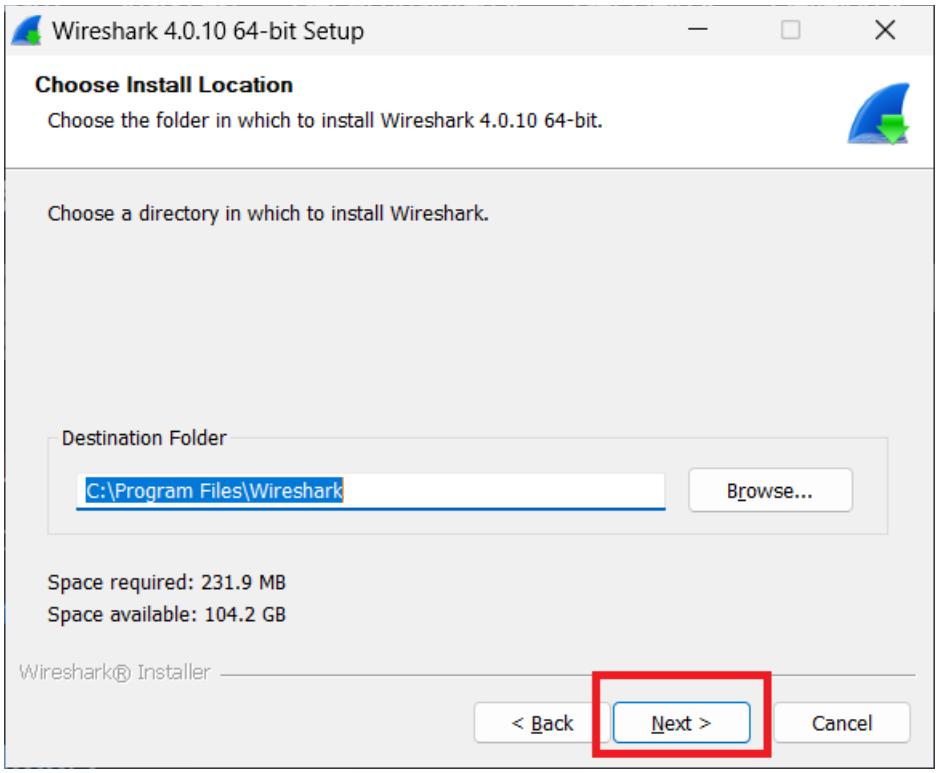
7. Klicka på **Next**



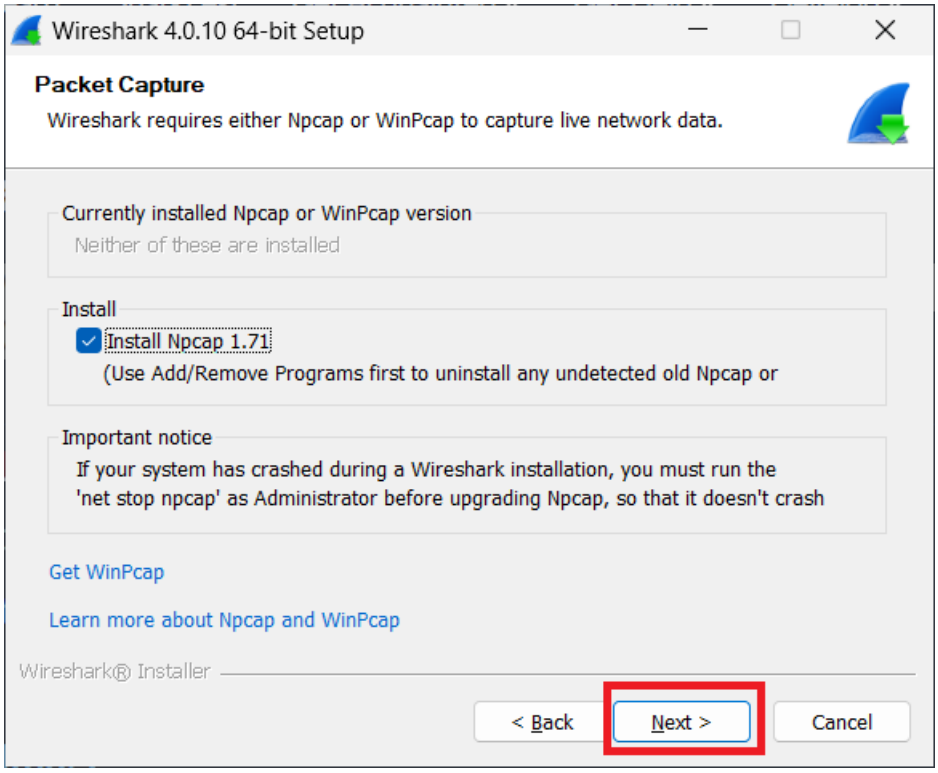
8. Klicka på **Next**



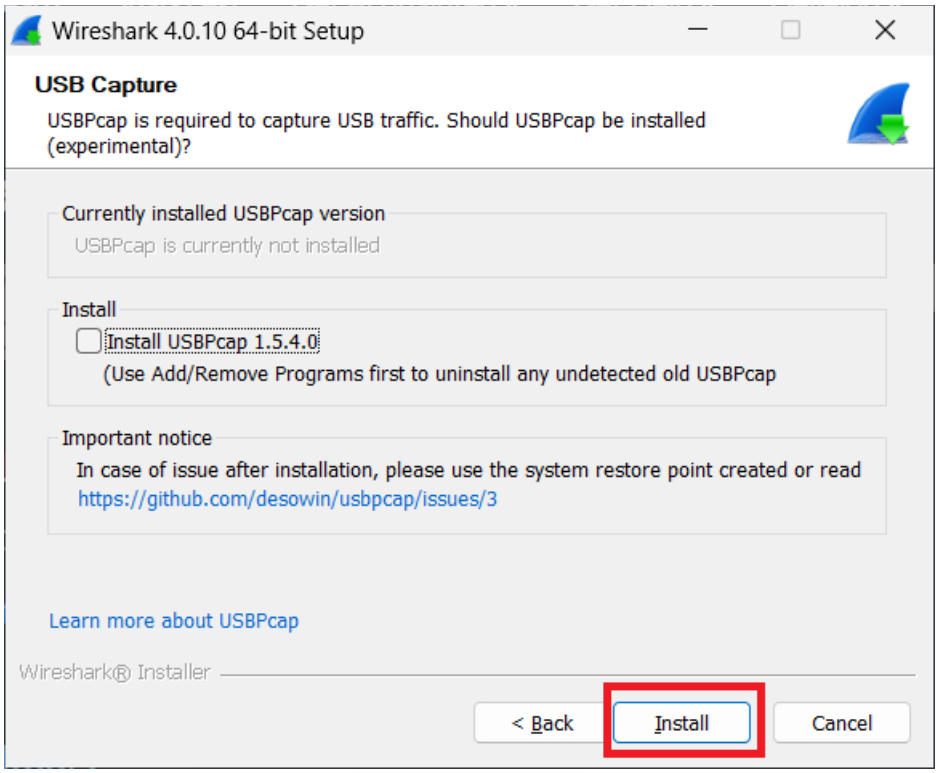
9. Klicka på **Next**

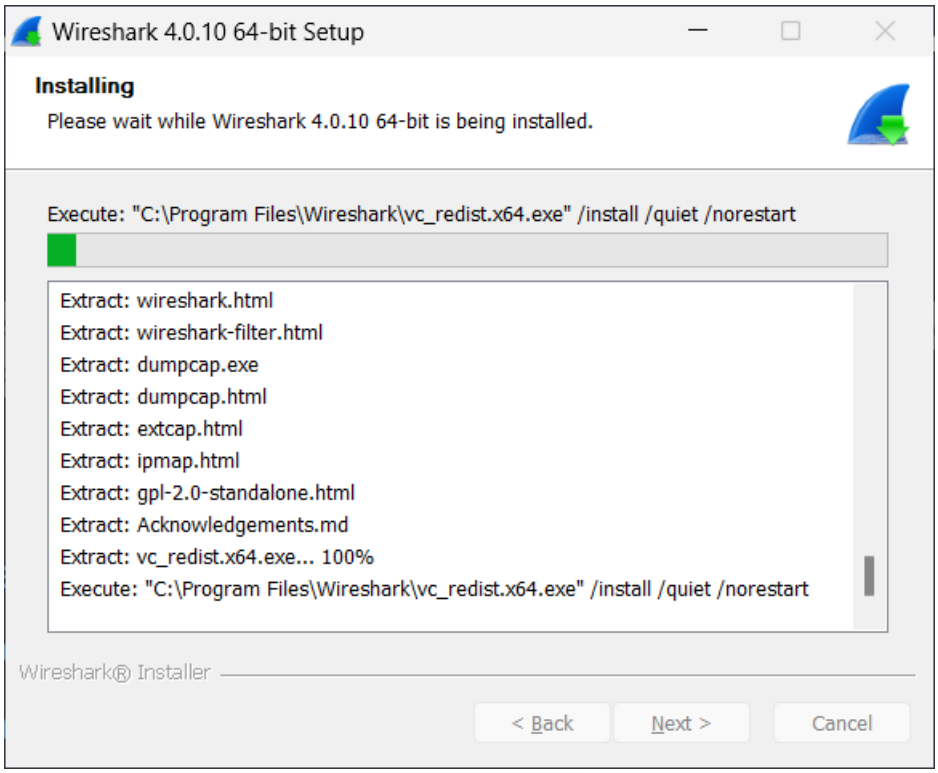


10. Klicka på **Next**



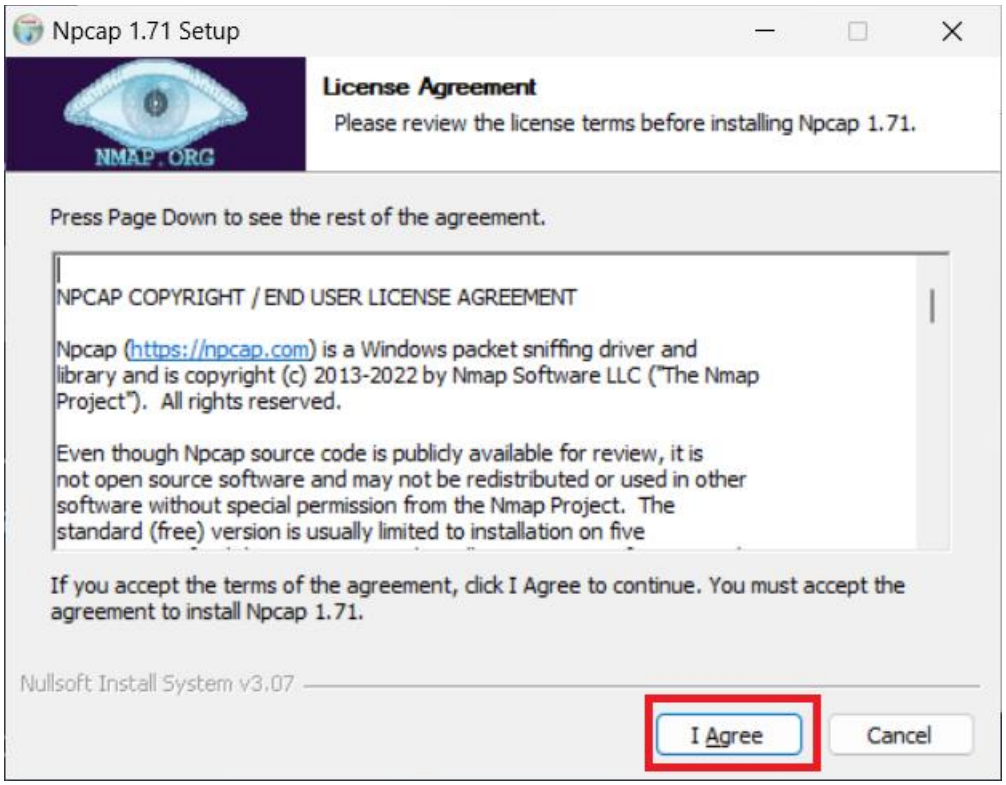
11. Klicka på **Install**



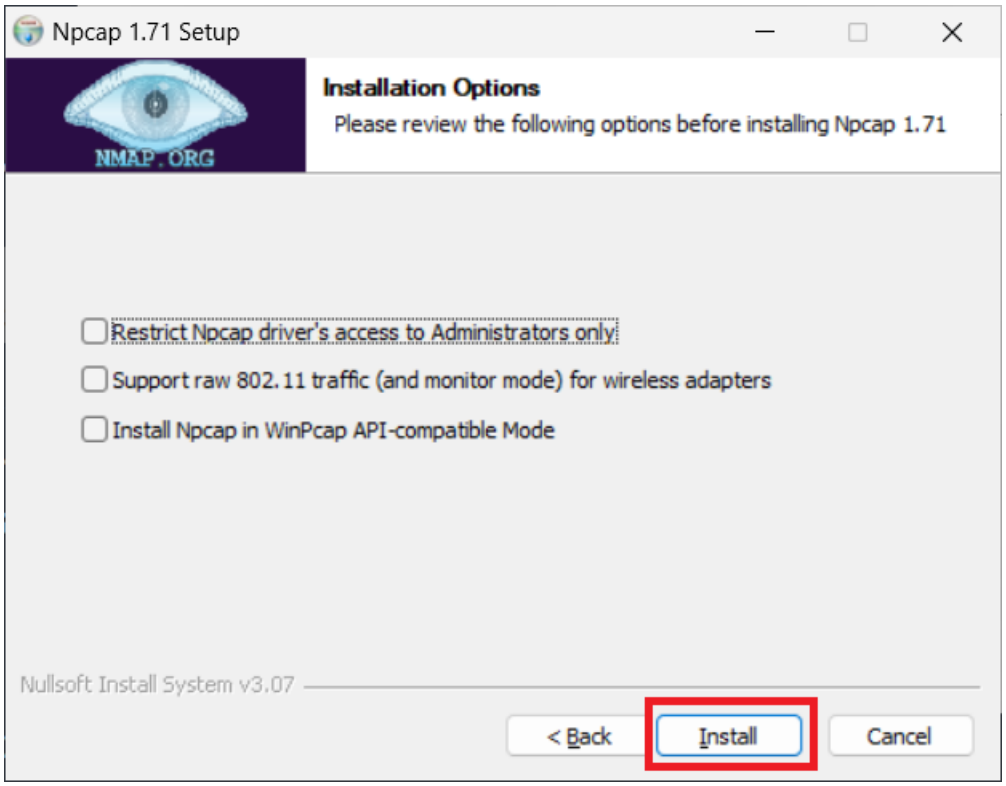


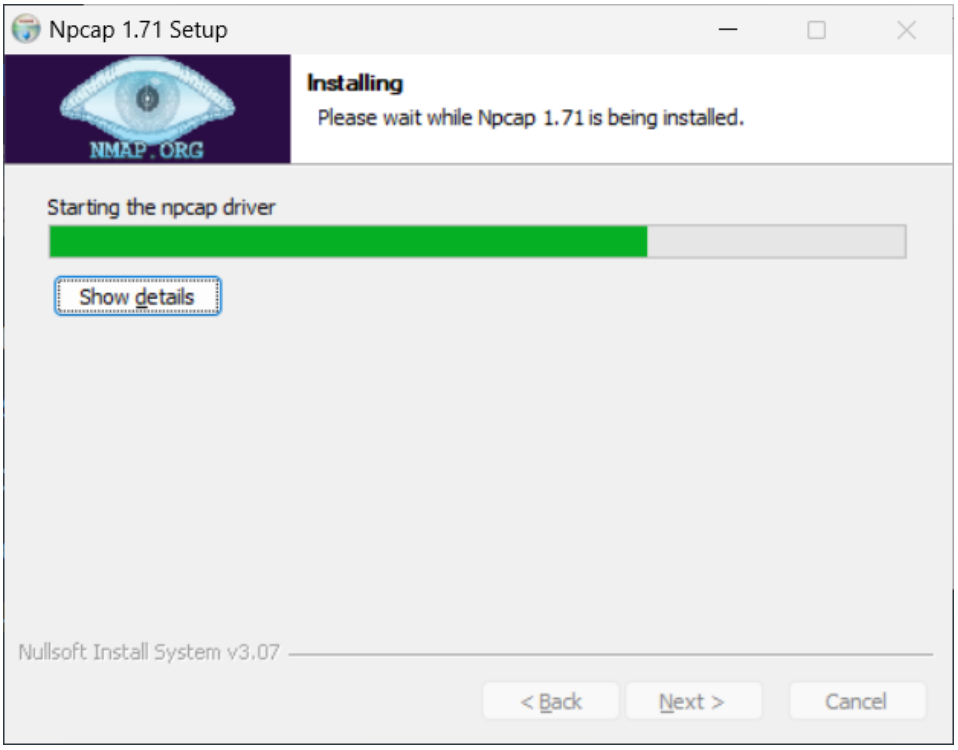
OBS under installationens gång så startar en separat installation av Npcap (se nästa bild)

12. Klicka på **I Agree**

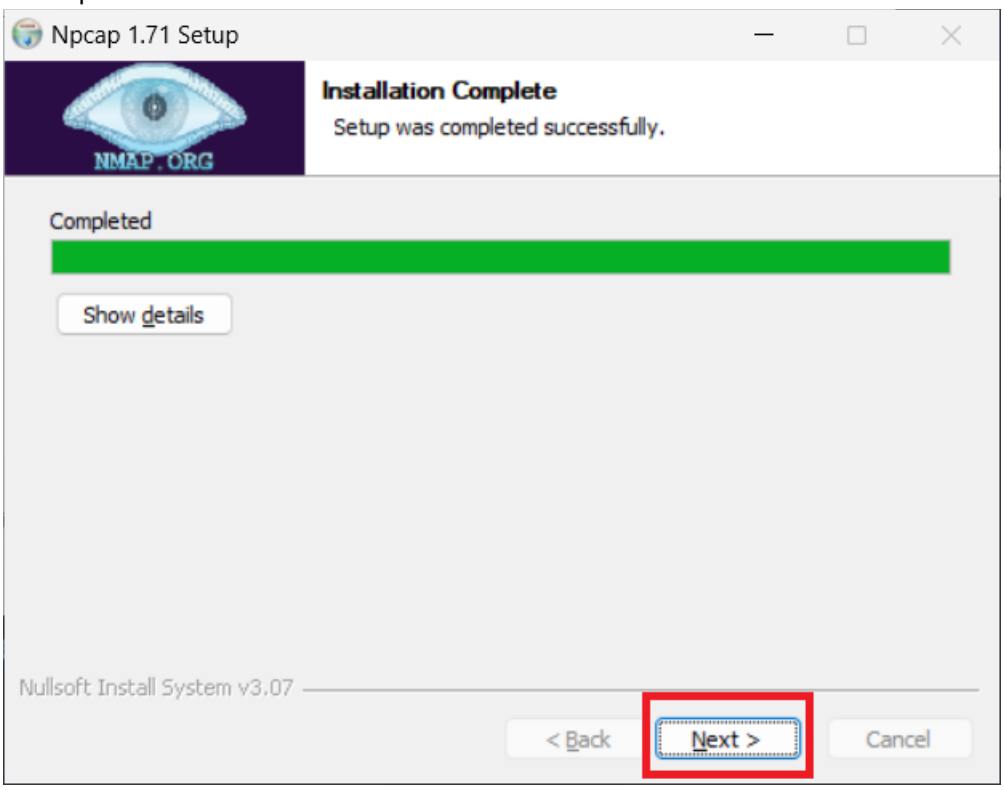


13. Klicka på **Install**

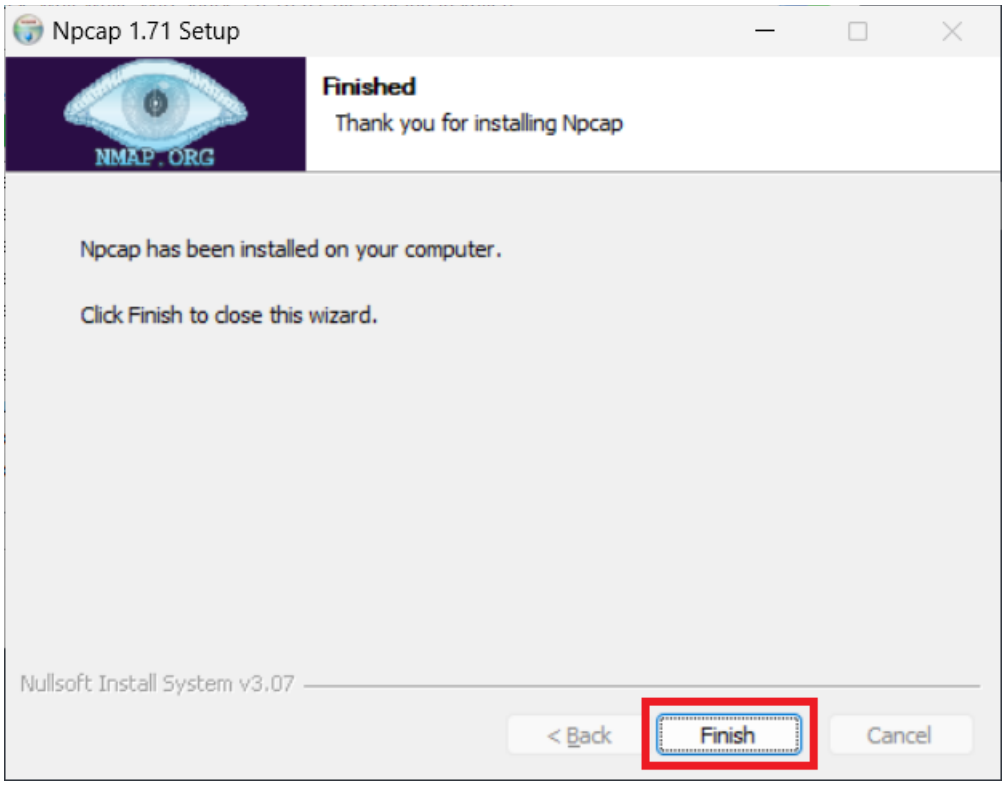




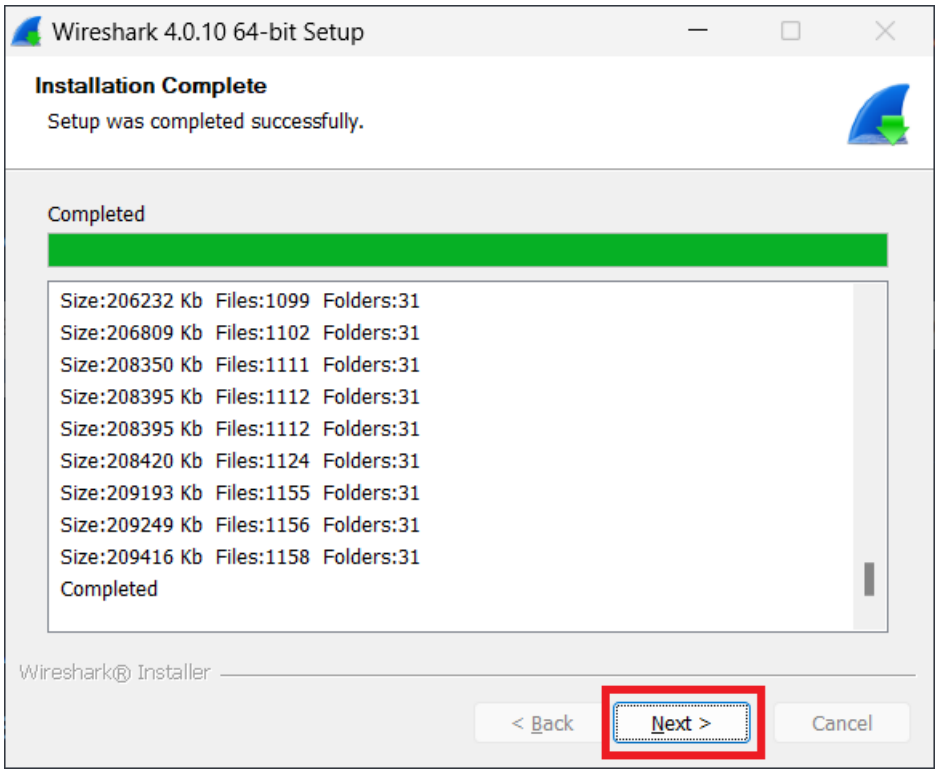
14. Klicka på **Next**



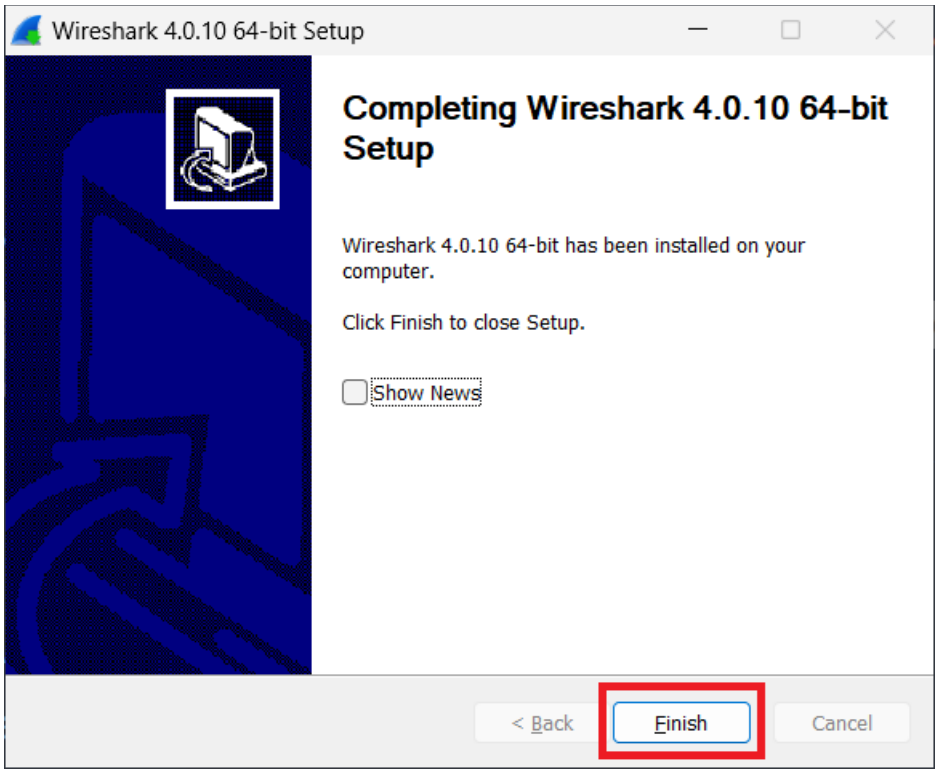
15. Klicka på **Finish**



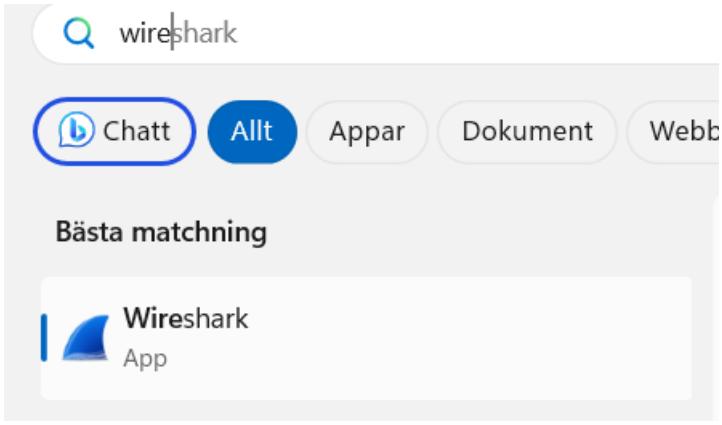
16. Klicka på **Next**



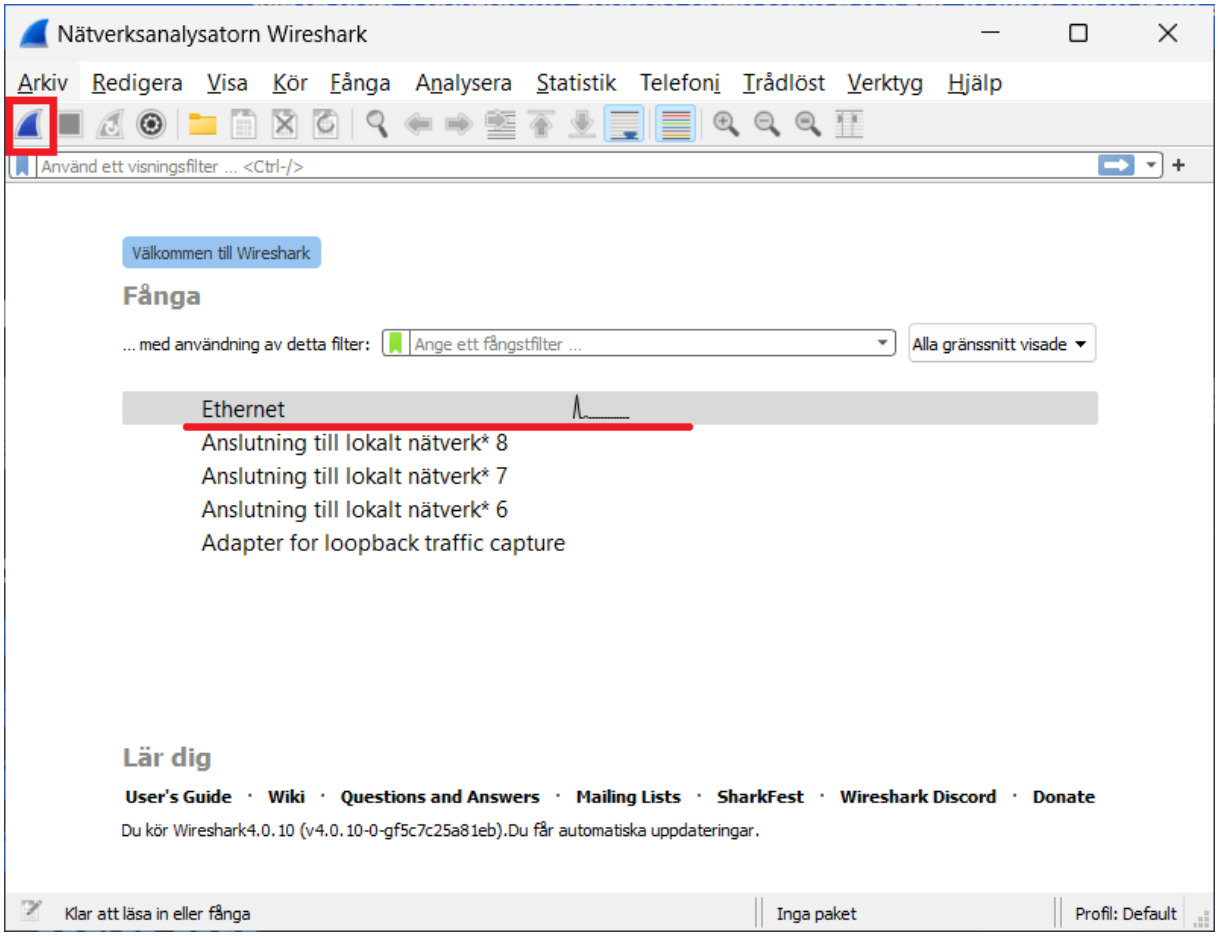
17. Klicka på **Finish**



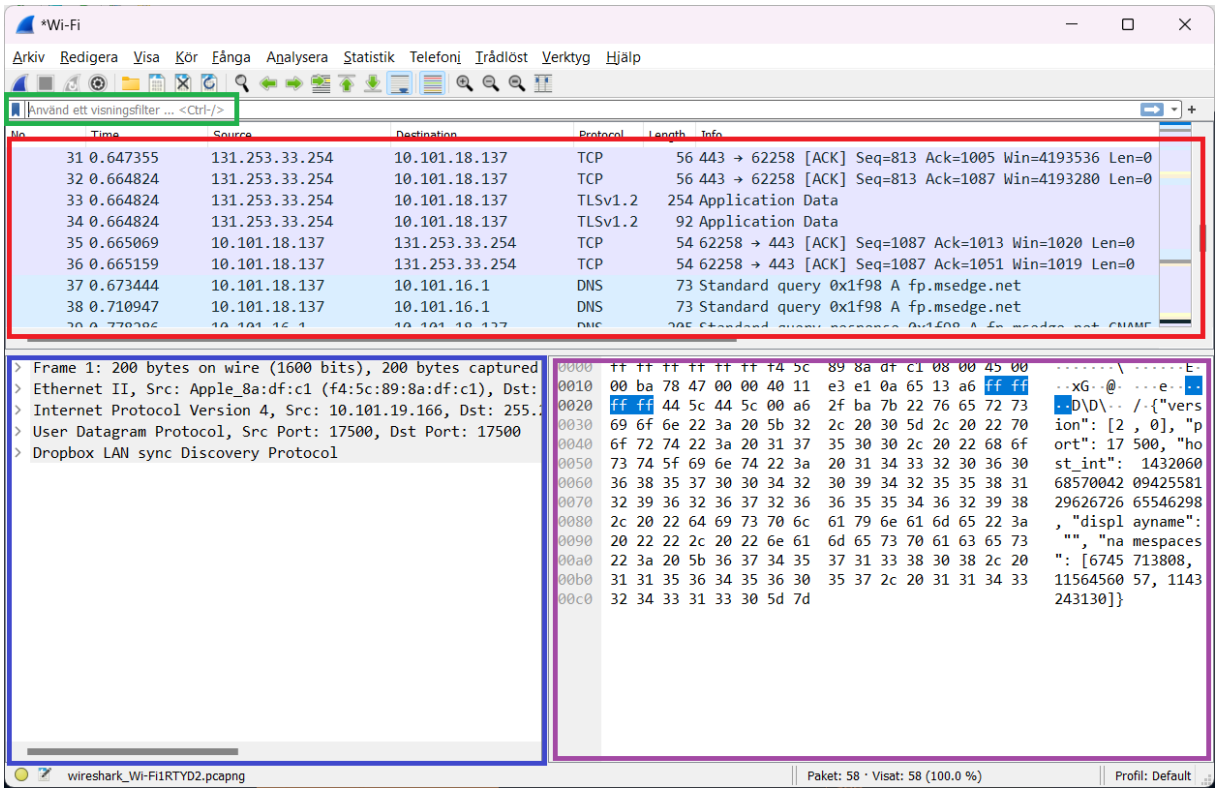
18. Starta **Wireshark**



19. Välj det nätverkskort som används i listan och klicka på **Börja fånga paket** (blå hajfenan). OBS namnet på aktuellt nätverkskort varierar från dator till dator, men vi kan se nätverksaktivitet i listan.



20. Klicka på stopp för att stoppa inspelningen/fångsten av paket.



I Wireshark så ser vi nu olika fönster.

I det **röda** fönstret ser vi alla paket (frames) som skickas till och från vårt nätverkskort i kronologisk ordning. Wireshark ger oss en kort sammanfattning av dessa och försöker identifiera vad som är vad. Inbyggt i Wireshark finns färdiga regler som färgar viss trafik i olika färger. Ju viktigare/intressantare trafik är, desto grällare färger oftast.

Markerar vi ett paket/frame så ser vi i det **blå** fönstret en översikt på innehållet i vårt paket/frame, lager för lager och vi kan undersöka header-informationen och innehållet.

I det **lila** fönstret ser vi motsvarande binära data representerat i hexadecimal form. Längst till höger ser vi samma data tolkat som tecken (teckenkodad data, ASCII/UTF-8).

Oftast vill vi filtrera ut viss trafik (paket) från alla paket som vi fångat. Detta gör vi i det **gröna** fältet. Att skriva ett korrekt filter kräver att vi skriver rätt syntax. Är allt ok så färgas fältet grönt. Är något fel så färgas fältet rött. **OBS** filtret kan ”hänga” sig och man kan då behöva trycka Enter i fältet igen för att uppdatera filtret.