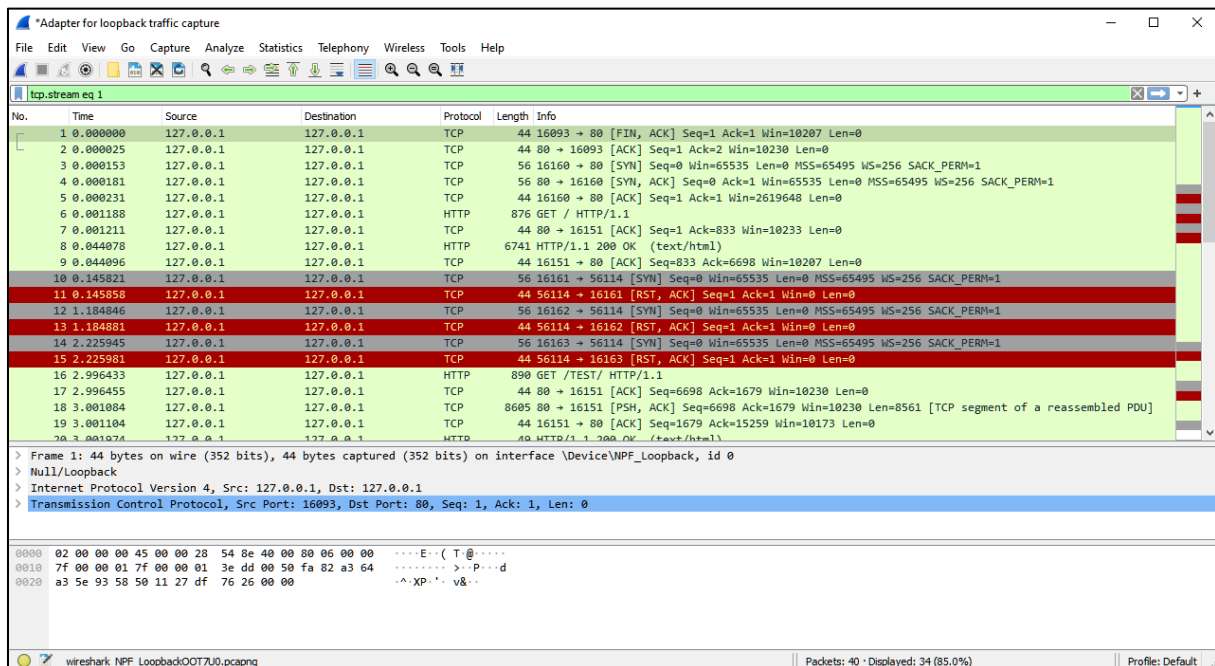


Protokol

Denial of Service (DoS)

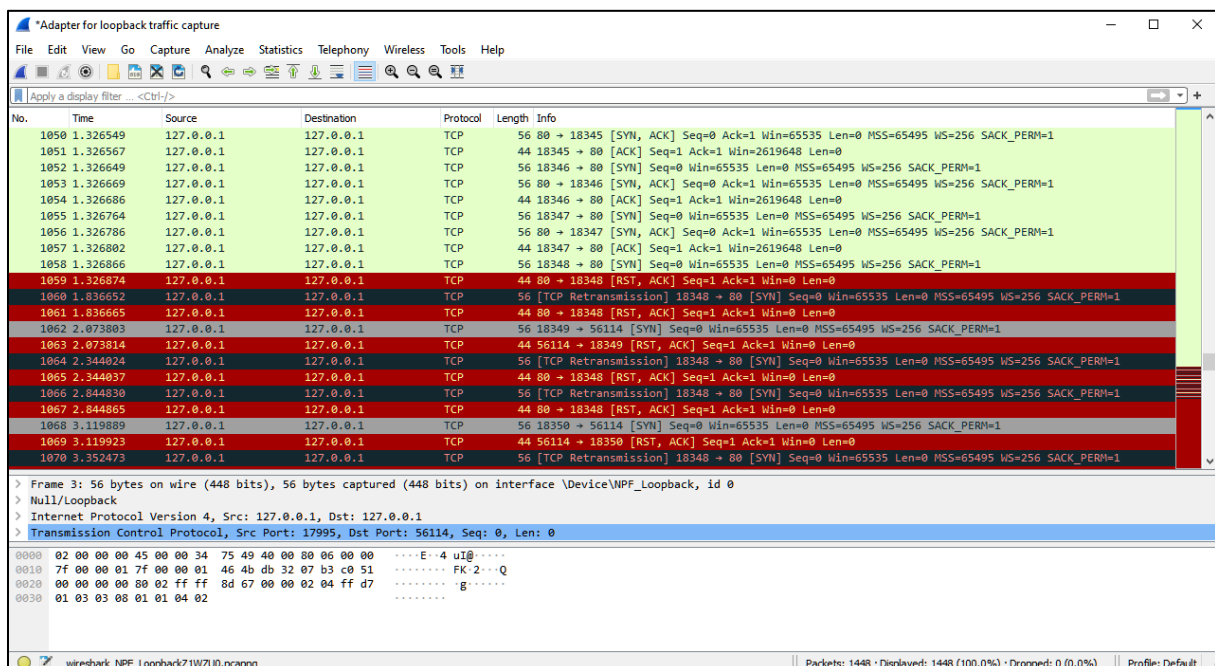
Běžný provoz webové aplikace



Obrázek 1 - Výpis komunikace s webovou aplikací pomocí Wireshark

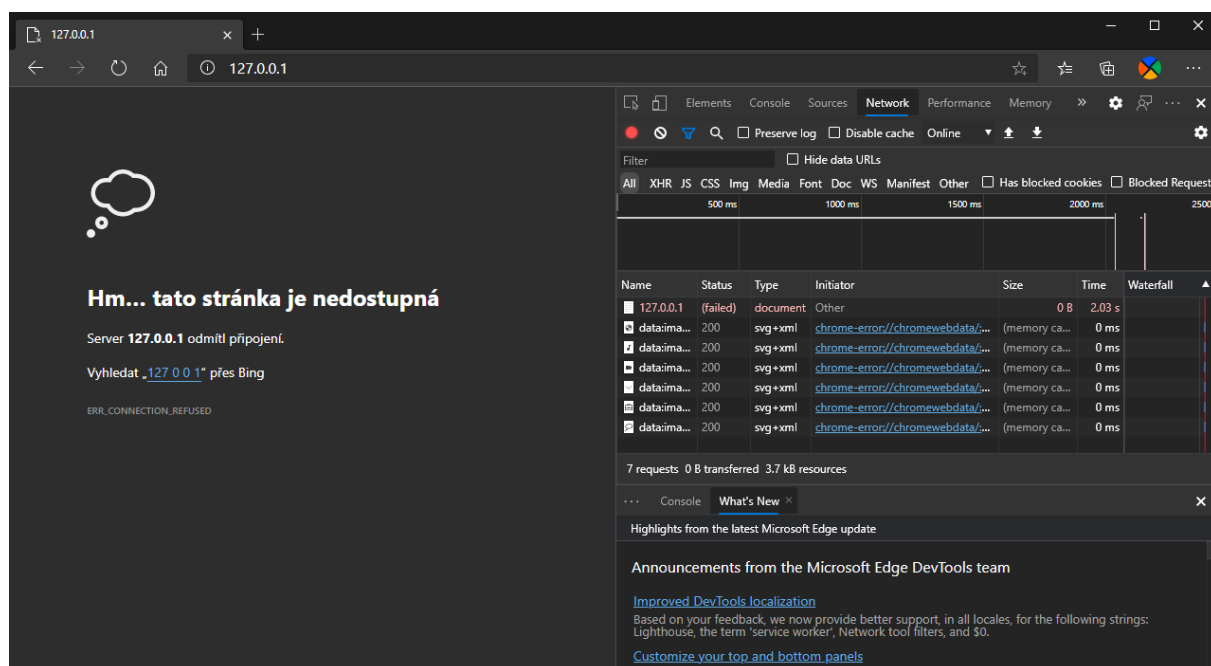
Webová aplikace funguje na portu 80 a vrací HTTP odezvu, díky které je možné webovou aplikaci zobrazit v prohlížeči. Webová stránka momentálně není přetížená a je plně funkční.

Provoz webové aplikace během DoS útoku



Obrázek 2 - Výpis komunikace s webovou aplikací během DoS útoku pomocí Wireshark

Webová aplikace je zahlcena požadavky o TCP spojení a není schopna přijímat další požadavky. Na web se tedy není možné připojit a prohlížeč zobrazuje chybovou hlášku ERR_CONNECTION_REFUSED.



Obrázek 3 - Webová aplikace během DoS útoku v Microsoft Edge 87

Popis útoku (HTTP Flood attack)

Každý server má určitý omezený počet prostředků, které může využít pro komunikaci s uživatelem. Tento útok spočívá v tom, že útočník odesílá velké množství HTTP požadavků na cílový server, čímž jej kompletně zahlťe. Server poté nemá žádné volné prostředky pro další komunikaci s běžnými uživateli a stává se nedostupným.

Útok je zákeřný především tím, že jeho požadavky není možné jednoduše odlišit od požadavků běžných uživatelů, tedy např. vyšší, než obvyklý počet návštěvníků může server zahltit úplně stejným způsobem.