Cvičenie Wireshark

Na firemnú sieť zaútočili hackeri a šéf Vás požiadal o pomoc pri analyzovaní sieťovej premávky počas útoku. Pomôžte mu vyriešiť nasledujúce úlohy v čo najkratšom možnom čase.

1.) V sieti prebehol útok aj na DNS server. Vyfiltrujte všetky záznamy, ktoré spĺňajú nasledujúce podmienky:

1. protokol DNS
2. IP adresa 10.20.30.2
3. dĺžka rámca 130B alebo 80B

2.) Útočník sa skúsil prihlásiť na url adresu obsahujúcu "secret.php" útokom hrubou silou. Vyfiltrujte všetky záznamy, ktoré spĺňajú nasledujúce podmienky:

1) protokol http (0.5 boda)
2) cieľová adresa 10.10.5.17 (0.5 boda)
3) url adresa obsahuje reťazec "secret.php" (1 bod)

Bonus:

1) Zistite IP adresu útočníka. (0.5 boda)
2) Nájdite aspoň 1 meno a heslo. (0.5 boda)

PCAP súbor na analýzu: https://stubask-my.sharepoint.com/:u:/g/personal/ivan_kotuliak_stuba_sk/ESCeQqxv_mpJmgCUsBzY14wB27ZYiwMLrgpNRlLd13YCHw

Používateľská príručka: https://www.wireshark.org/docs/wsug_html_chunked/