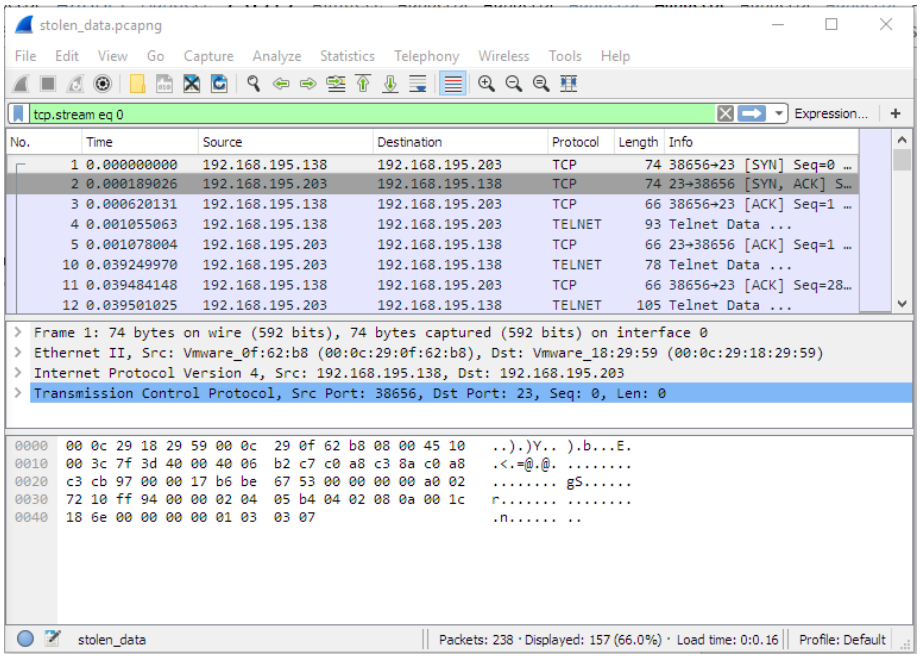
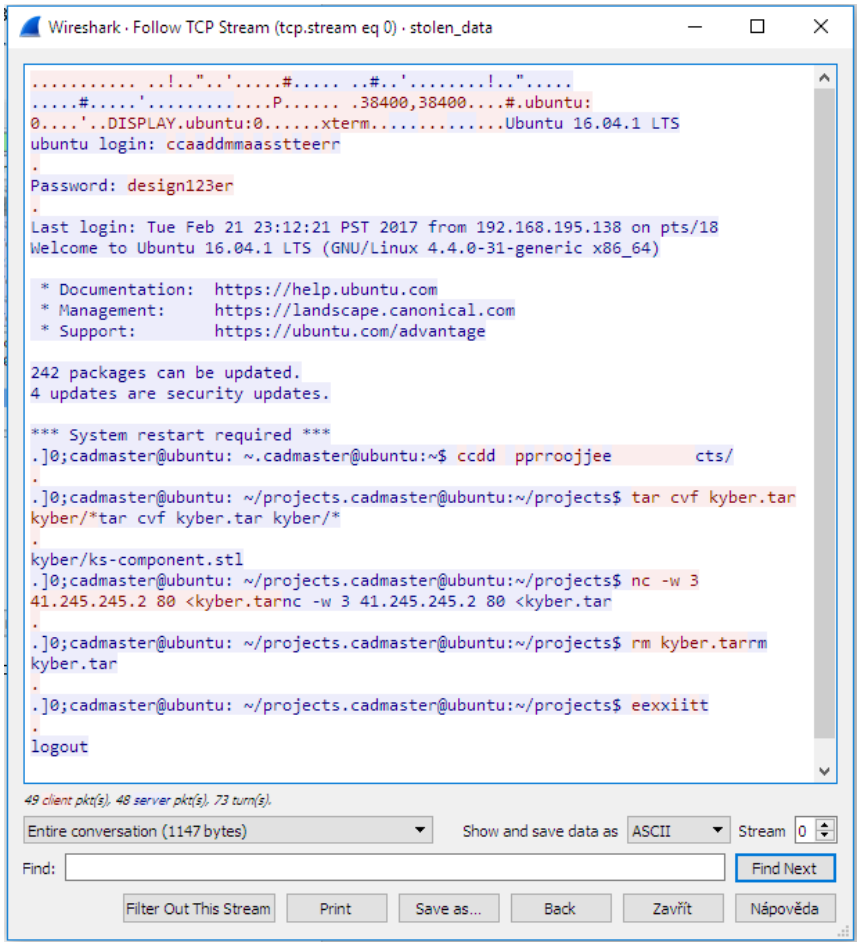
Řešení:

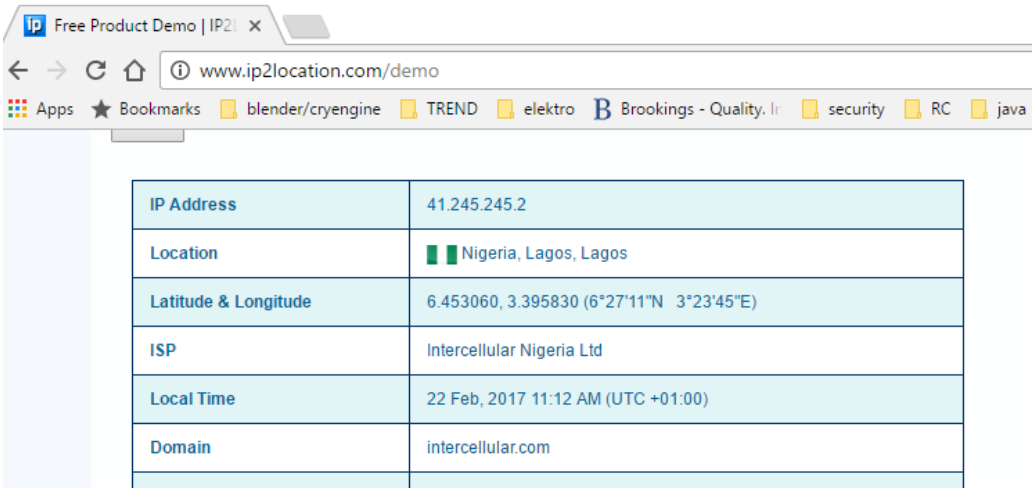
1. Dodaný soubor pcap otevřeme v programu wireshark
2. Najdeme komunikaci mezi stanicí `192.168.195.138` a serverem `192.168.195.203`



3. Je patrné, že se jedná o telnet spojení, obsah komunikace zobrazíme pomocí funkce Follow TCP stream.

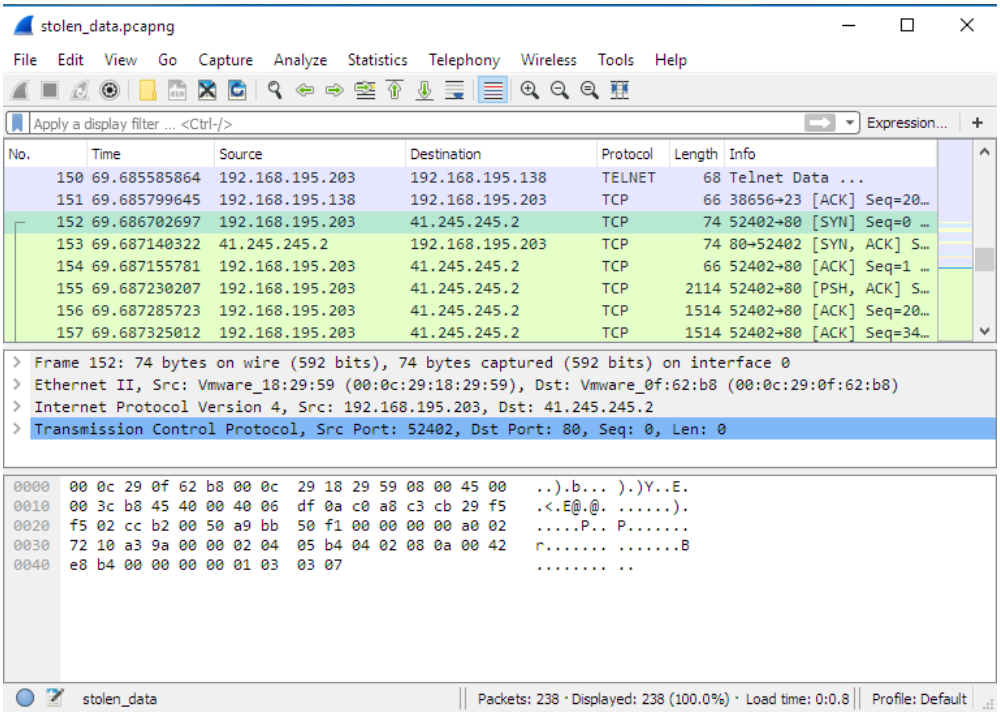


4. Ze zjištěných údajů je možné odpovědět na doplňující otázku – útočník se přihlásil jako `cadmaster` s heslem `design123er`. Dále je možno zjistit, že útočník zaarchivoval složku `projects/kyber/` do souboru `kyber.tar`. Tento soubor následně odeslal na adresu `41.245.245.2`.
   Z výše uvedeného plyne odpověď na druhou doplňující otázku – Afrika. *Rozsah 41.0.0.0 spravuje AFRINIC a tuto konkrétní adresu lokační služby řadí většinou do Nigérie (některé ale i do JAR nebo Kamerunu proto je vhodnější odpověď na úrovni kontinentu)*

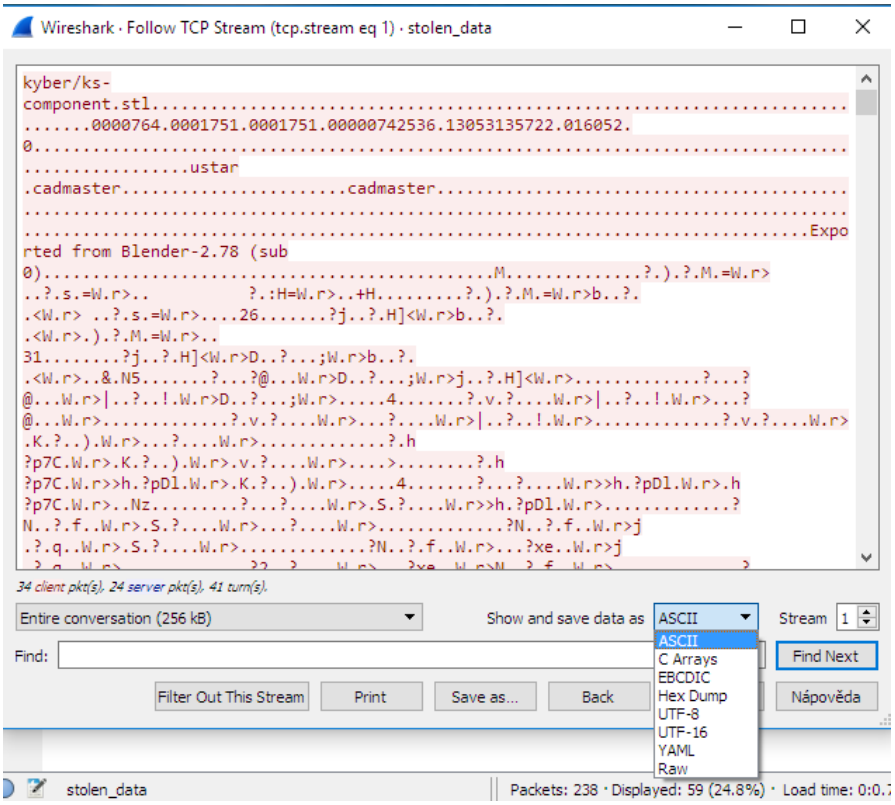


IP Address	41.245.245.2
Location	Nigeria, Lagos, Lagos
Latitude & Longitude	6.453060, 3.395830 (6°27'11"N 3°23'45"E)
ISP	Intercellular Nigeria Ltd
Local Time	22 Feb, 2017 11:12 AM (UTC +01:00)
Domain	intercellular.com

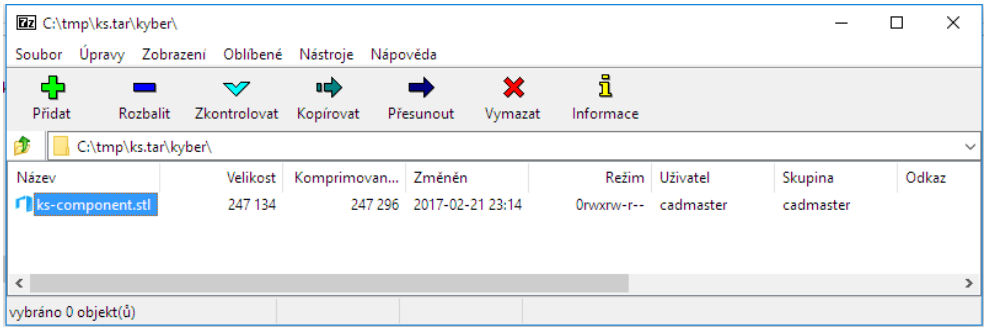
5. Na základě poznatků z předchozího bodu vyhledáme komunikaci mezi `192.168.195.203` a `41.245.245.2`, která obsahuje soubor odeslaný příkazem `nc`.



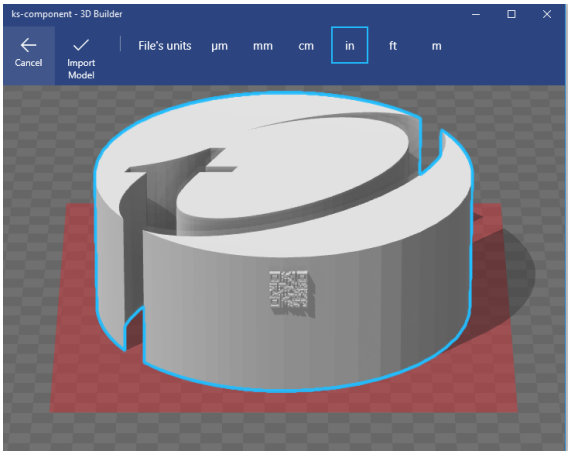
6. Funkcí Follow TCP stream zobrazíme obsah komunikace, která obsahuje přenesený soubor a následně ji uložíme do souboru např. opět `kyber.tar` pomocí funkce „Save as“. Je důležité uložit data jako RAW (viz volba „show and save data as“).



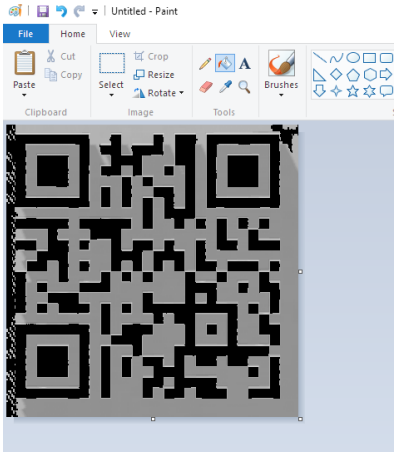
7. Výsledný soubor je archivem .tar, který obsahuje hledaný soubor:



8. Samotný soubor je 3d model .stl, který obsahuje QR kód:



9. Přímo z modelu kód pravděpodobně nepůjde naskenovat – je možné udělat screenshot a následně upravit např. v paintu



10. Dále naskenovat mobilem nebo některou z online aplikací: Správné řešení je TM-TP-2017