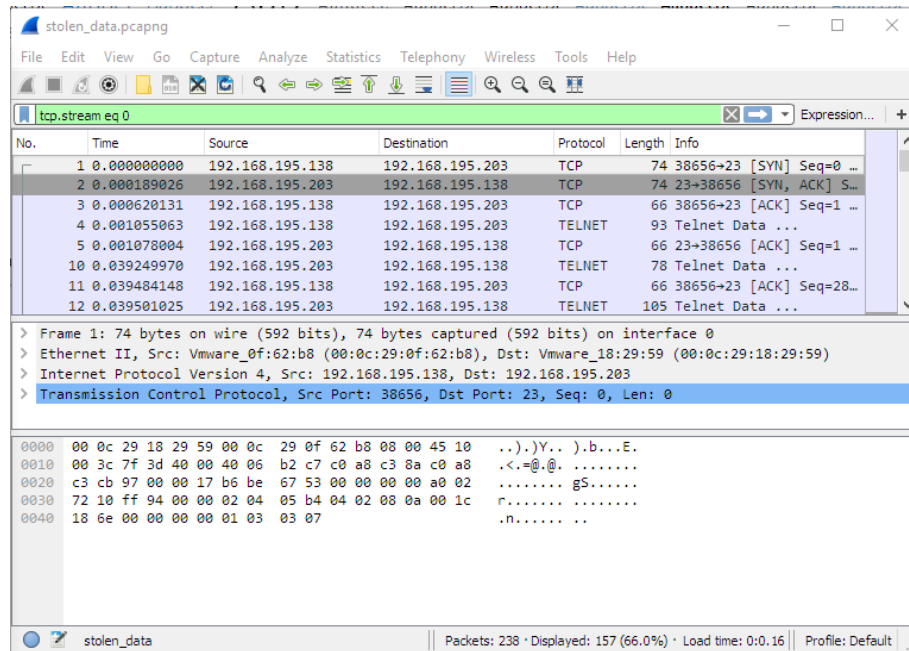
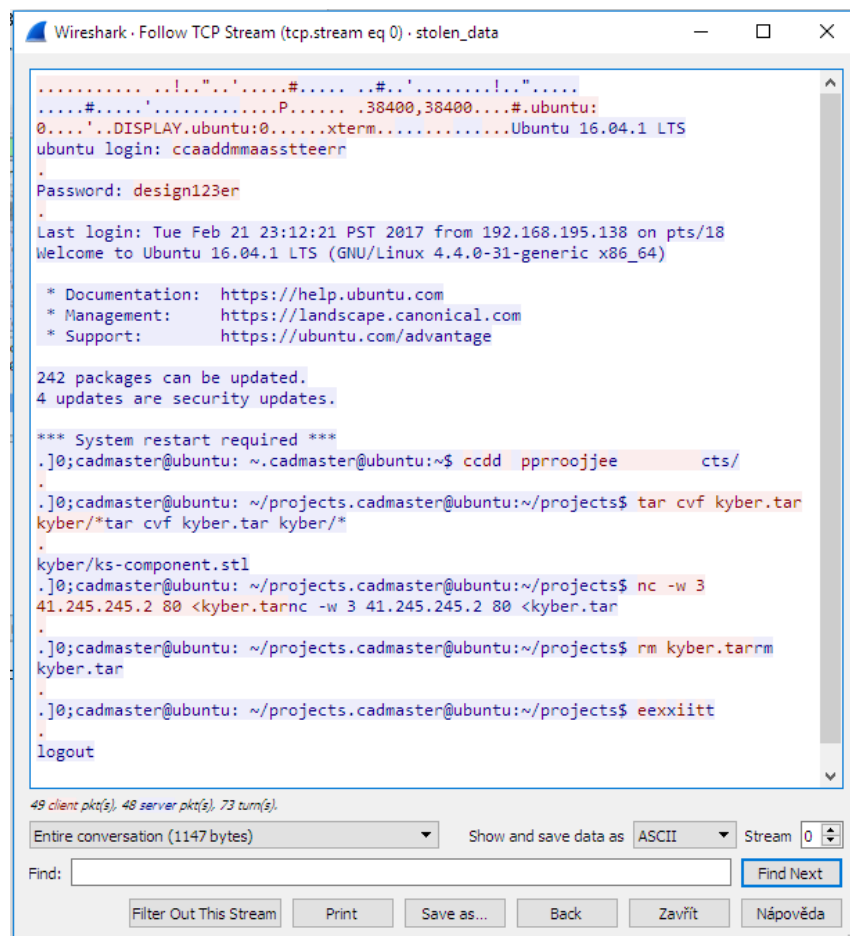


## Řešení:

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`.

stolen\_data.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
150	69.685585864	192.168.195.203	192.168.195.138	TELNET	68	Telnet Data ...
151	69.685799645	192.168.195.138	192.168.195.203	TCP	66	38656+23 [ACK] Seq=20...
152	69.686702697	192.168.195.203	41.245.245.2	TCP	74	52402+80 [SYN] Seq=0 ...
153	69.687140322	41.245.245.2	192.168.195.203	TCP	74	80+52402 [SYN, ACK] S...
154	69.687155781	192.168.195.203	41.245.245.2	TCP	66	52402+80 [ACK] Seq=1 ...
155	69.687230207	192.168.195.203	41.245.245.2	TCP	2114	52402+80 [PSH, ACK] S...
156	69.687285723	192.168.195.203	41.245.245.2	TCP	1514	52402+80 [ACK] Seq=20...
157	69.687325012	192.168.195.203	41.245.245.2	TCP	1514	52402+80 [ACK] Seq=34...

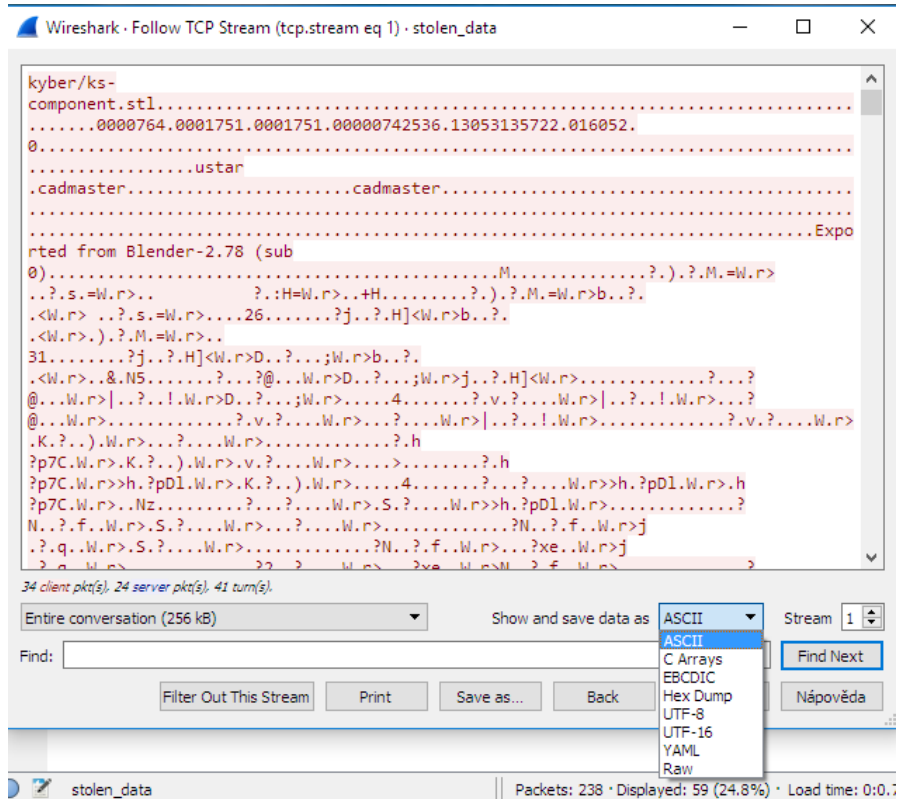
> Frame 152: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0  
 > Ethernet II, Src: Vmware\_18:29:59 (00:0c:29:18:29:59), Dst: Vmware\_0f:62:b8 (00:0c:29:0f:62:b8)  
 > Internet Protocol Version 4, Src: 192.168.195.203, Dst: 41.245.245.2  
 > Transmission Control Protocol, Src Port: 52402, Dst Port: 80, Seq: 0, Len: 0

```

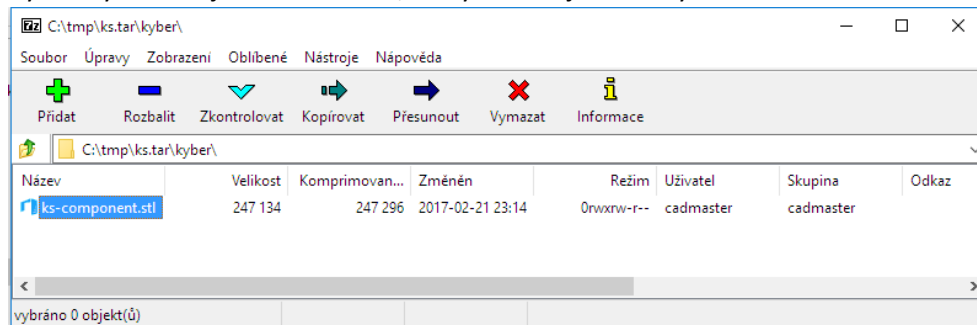
0000  00 0c 29 0f 62 b8 00 0c 29 18 29 59 08 00 45 00  ..).b...).)Y..E.
0010  00 3c b8 45 40 00 40 06 df 0a c0 a8 c3 cb 29 f5  .<.E@.@. ....).
0020  f5 02 cc b2 00 50 a9 bb 50 f1 00 00 00 00 a0 02  ....P..P.....
0030  72 10 a3 9a 00 00 02 04 05 b4 04 02 08 0a 00 42  r.....B
0040  e8 b4 00 00 00 00 01 03 03 07  .....
```

stolen\_data | Packets: 238 · Displayed: 238 (100.0%) · Load time: 0:0.8 | Profile: Default

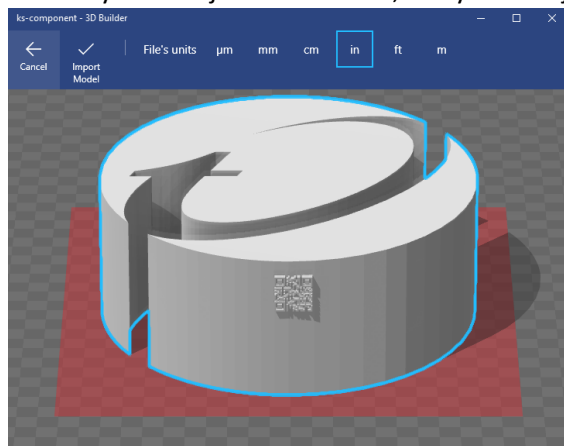
- Funkcí Follow TCP stream zobrazíme obsah komunikace, která obsahuje přenesený soubor a následně ji uložíme do souboru např. opět `kyber.tar` pomocí funkce „Save as“. Je důležité uložit data jako RAW (viz volba „show and save data as“).



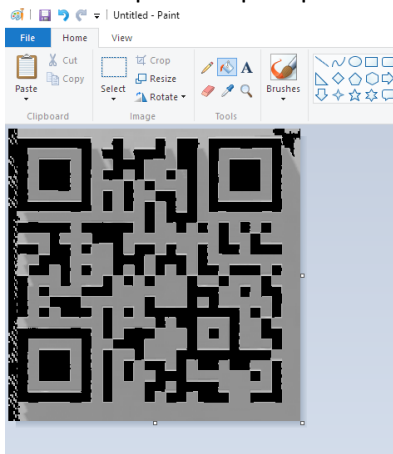
- Výsledný soubor je archivem `.tar`, který obsahuje hledaný soubor:



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



9. Přímou 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**

