1. What is the operating system of the host from which the network traffic was captured? (Look at Capture File Properties, copy the details exactly)

**32-bit Windows 7 Service Pack 1, build 7601**

2. What is the full URL from which the ransomware executable was downloaded?

**http://10.0.2.15:8000/safecrypt.exe**

3. Name the ransomware executable file?

**safecrypt.exe**

4. What is the MD5 hash of the ransomware?

**4a1d88603b1007825a9c6b36d1e5de44**

5. What is the name of the ransomware?

**Teslacrypt**

6. What is the encryption algorithm used by the ransomware, according to the ransom note?

**RSA-4096**

7. What is the domain beginning with ‘d’ that is related to ransomware traffic?

**dunyamuzelerimuzesi.com**

8. Decrypt the Tender document and submit the flag

**BTLO-T3nd3r-Fl@g**