

Wrap\_socket metodu, *do\_handshake\_on\_connect=False* parametresi belirtilmediği sürece handshake işlemini otomatik olarak başlatmaktadır. Bu nedenle kod içerisinde handshake'e özel herhangi bir kod gözükmemektedir. <sup>1</sup>

Kullanılan sertifikalar ve key'ler şu şekilde oluşturulmuştur <sup>2</sup>:

```
$openssl genrsa -aes256 -out ca.key 4096  
$ openssl req -new -x509 -nodes -key ca.key -out ca.pem -days 1000
```

Create a key and a certificate signing request (CSR) on a machine:

```
$ openssl genrsa -out server.key 4096  
$ openssl genrsa -out client.key 4096  
$ openssl req -new -key server.key -out server.csr  
$ openssl req -new -key client.key -out client.csr
```

Now you can sign the device key with your CA cert:

```
$ openssl x509 -CA ca.pem -CAkey ca.key -CAcreateserial -req -in server.csr -out  
server.pem -days 365  
$ openssl x509 -CA ca.pem -CAkey ca.key -CAcreateserial -req -in client.csr -out  
client.pem -days 365
```

---

### ***Kodun Çalıştırılması***

Kullanılan SSL kütüphanesinin Windows'ta kurulum zorluğu nedeniyle projeye Linux'da devam ettik. Buna rağmen yeni kurulan bir Ubuntu sistemde kodun sorunsuz çalışması için şu paketlerin kurulumuna ihtiyaç vardı:

```
sudo apt-get install openssl  
sudo apt-get install libssl-dev  
sudo apt-get install libffi-dev  
sudo apt-get install python3-openssl  
sudo apt-get install python3-pip  
sudo pip3 install pycrypto
```

Bu nedenle sizin de kodu kolaylıkla test edebilmeniz amacıyla 2 farklı sunucu açtık ve gerekli kurulumları yaparak projedeki tüm dosyaları yükledik. Uygun görürseniz test işlemini bu sunucular üzerinden yapabilirsiniz. (sunucu saatinin birkaç saat geri olmasından dolayı 'son değiştirme zamanı' şüphe uyandırabilir. Bu nedenle size

yolladığımız dosyaları sftp:// üzerinden bağlanıp tekrar yükleyebilirsiniz. Mevcut dosyalar root dizini altındadır.)

Sunucu IP'leri:  
46.101.202.226  
46.101.222.96

Kullanıcı: root  
Şifre: 8Bq1610T

Koddaki bazı sabitler `__init__` fonksiyonunda girilmiştir. Bu fonksiyonun içerisinde ilgili değerleri değiştirebilirsiniz. Örneğin gönderici de  
`self.filePath = "`  
`self.fileName = 'Data_Algorithms.pdf'`

Kısımları değiştirilmelidir. Eğer gönderilecek dosya, kodun çalıştığı dizinde `filePath` boş olmalıdır. `fileName` ise gönderilmek istenen dosya adı ile değiştirilmelidir.

Alıcı tarafında ise:

`self.loc = "`

Kısmı değiştirilebilir. Bu değişken, alınan dosyanın hangi dizine (location) kaydedileceğini belirtmektedir.

Hem gönderici hem de alıcıda ortak olan sertifika ve key parametreleri şu kısımdan değiştirilmelidir:

`self.context.load_cert_chain(certfile='server.pem', keyfile='server.key')`  
`self.context.load_verify_locations(cafile='ca.pem')`

`Ca.pem`, her iki taraf için de aynıdır. Aşağıda belirtileceği üzere root `ca`'yı ifade etmektedir.

Açmış olduğumuz sunucularda test işlemi ayrı olarak `bob.key`, `bob.pem` ve `bobca.pem` dosyaları bulunmaktadır. Hangi durumlarda hata durumlarının ortaya çıkacağını görmek amacıyla bunlar kullanılabilir.

Kod test edilirken önce gönderici taraf çalıştırılmaz. Ardından alıcı taraf çalıştırılıp ip bilgisi girilerek test edilebilir.

---

Dosyanın okunan son parçası gönderildikten sonra, (veri okunamadığından dolayı) en son karşı tarafa boş bir veri gönderiliyor. Bu durum alıcı için sorun olmuyor çünkü gelen veri boş olmadığı sürece dosyaya yazılıyor. Ancak ssl kütüphanesindeki implementasyon nedeniyle karşı tarafa boş bir veri (" ") gönderilemiyor.

Böyle bir durumla karşılaşıldığında EOF exception veriliyor (ssl.SSLEOFError: EOF occurred in violation of protocol). Bu durumun önüne geçmek amacıyla ikinci projede, aktarımın tamamlandığında kullandığımız gibi, gönderilecek veriyi " " olarak değil de "Done" olarak gönderdik. Böylece bu hatanın önüne geçilmiş olduk.

---

İlgili resimler aşağıdadır..

Resim-1: Başarılı bir dosya transferi örneği

```
root@ubuntu-512mb-fra1-01: ~
root@ubuntu-512mb-fra1-01:~# python3 gonderici_TCP.py
fra1-01 IP: 46.101.202.226
fra1-02 IP: 46.101.222.96
Public-Key: (4096 bit)
Modulus:
 00:bc:a2:c0:f1:54:61:b4:c3:c0:45:d0:c5:60:77:
 8c:19:95:02:90:d5:e4:6d:97:4e:10:c9:4d:5c:b1:
 ae:5b:8d:c3:4c:c1:7f:45:9b:fc:0f:d7:30:26:6e:
 12:0b:93:fa:de:d5:7b:33:fe:75:ec:f7:17:3f:64:
 6f:bd:1b:88:ae:1b:61:36:42:7c:ae:39:9d:2f:45:
 88:98:4b:6d:24:e1:03:cb:eb:2b:be:f4:1d:c3:d8:
 b5:e7:7b:38:ec:74:3b:4c:64:16:12:56:b5:73:b9:
 bc:0c:f6:d0:73:ff:b9:25:1d:73:e5:f4:db:23:47:
 fb:37:e6:78:8c:52:36:64:93:65:48:d9:11:b4:a3:
 fd:82:ce:ef:e0:3f:e0:bb:68:4d:3b:33:a9:83:11:
 31:9a:2c:6d:84:a7:ad:18:0b:58:08:c4:28:0b:54:
 50:49:cb:23:4f:c9:64:aa:42:16:cf:ba:29:9e:be:
 b7:db:67:90:d5:bc:89:93:f1:92:b6:36:df:12:cd:
 b2:ba:e5:c9:8c:10:77:15:34:c3:4b:b6:c6:c4:79:
 4c:17:3e:55:90:63:94:00:e1:f7:28:5c:c8:f1:cf:
 af:d0:4b:c8:92:8b:46:a9:ad:cb:1d:2c:6d:d1:18:
 b8:53:ca:4f:34:2f:cc:c9:e1:c9:9a:8f:c0:5e:56:
 17:db:bf:f6:a7:c1:c7:53:33:e4:61:1d:35:2b:7d:
 f1:4e:af:5e:4c:a0:90:81:a5:36:68:ce:f8:0c:74:
 1f:5a:55:60:78:18:45:1b:f0:bf:2a:98:d3:35:2a:
 65:7c:bd:e5:de:d3:b3:b4:47:d9:09:c5:73:c8:48:
 b4:7d:40:1f:06:b5:27:8f:27:df:4f:8d:9e:ed:34:
 be:16:1e:6b:ca:fd:6e:35:cb:84:7e:27:0c:ec:73:
 cc:80:b0:b5:10:90:6d:85:b0:68:5c:c7:81:ac:f9:
 4e:02:f9:0d:41:d9:8d:de:ac:b6:6a:e0:cd:bd:b7:
 c7:ef:ed:53:af:a7:8a:13:ac:a3:ab:4e:6b:26:67:
 56:c3:f7:cc:2f:91:d3:c7:d3:be:f5:bb:33:b9:90:
 90:19:e3:6d:c9:99:47:30:7b:85:13:0a:25:f8:22:
 38:76:d8:ae:91:7f:da:61:95:36:38:39:10:a0:97:
 42:b6:b4:76:a9:e7:00:be:59:91:2f:1f:08:8f:b5:
 67:4a:0d:fc:17:04:58:57:95:e8:f5:cb:d4:23:5b:
 56:d7:fa:29:53:7f:f5:bb:25:f9:41:9d:ad:3e:d9:
 e1:a6:61:ef:4e:19:0e:5d:79:b6:1b:91:2a:08:56:
 ad:77:92:38:30:13:84:85:7d:9e:3b:f7:cc:72:d1:
 1b:b5:5d
Exponent: 65537 (0x10001)
- Certificate Type -
X.509

***** GONDERME ISLEMI TAMAMLANDI *****

root@ubuntu-512mb-fra1-02: ~
root@ubuntu-512mb-fra1-02:~# python3 alici_TCP.py
fra1-01 IP: 46.101.202.226
fra1-02 IP: 46.101.222.96
Gonderici sunucunun IP'sini giriniz: 46.101.202.226
Public-Key: (4096 bit)
Modulus:
 00:f0:a4:07:a5:cd:e5:ef:3d:12:d5:46:62:ba:8b:
 93:a6:92:6f:c6:15:01:36:29:17:8e:8b:9a:aa:52:
 f6:df:1a:43:27:d0:b9:dc:e4:70:2b:cc:09:0e:c6:
 87:f3:58:85:73:9c:cd:72:30:dc:eb:99:a2:b1:62:
 de:f0:e1:3d:2c:ca:b7:6c:51:8e:56:61:ef:80:a0:
 20:1e:e4:2c:6c:57:d0:e7:b6:49:85:8e:1a:21:f2:
 19:73:82:7f:20:71:5d:89:b4:1a:0e:44:cd:97:99:
 91:fa:55:b9:77:9e:1f:58:00:dc:c6:d6:ee:44:53:
 3f:2a:52:5f:7e:f7:9b:f9:eb:82:d0:0b:57:66:3a:
 36:9c:4c:81:2d:38:25:2a:86:f6:84:b0:f7:7f:0e:
 af:84:21:86:81:4b:75:23:07:83:84:b5:48:26:cc:
 bc:ba:ce:cc:67:7c:9b:32:6c:9f:b4:8a:81:71:57:
 42:7d:e3:1e:f9:68:c4:19:c4:98:99:49:cd:ea:26:
 c2:41:6b:55:34:af:2d:61:0f:fd:6a:8d:59:32:3b:
 1f:28:0d:a5:c9:e0:af:d9:b7:f2:cc:71:ae:65:72:
 ec:59:48:c7:00:aa:f8:b8:0b:ba:64:c7:f6:40:c0:
 9e:22:49:1d:51:00:e2:17:e5:e7:24:f5:e2:44:56:
 db:07:38:7f:29:7a:53:61:ce:90:b8:bf:77:0f:1c:
 73:11:34:e3:72:3f:81:22:82:5a:14:6c:49:c8:e6:
 9c:d0:c5:ca:9f:10:7d:55:e3:d7:71:b8:59:2a:d7:
 6e:44:a8:60:71:73:a3:0b:bc:02:8c:90:19:4c:f4:
 bc:0f:ff:56:70:f6:37:dc:b6:d4:bd:25:15:78:90:
 9b:3c:8e:c7:e4:6b:df:33:2f:dc:4a:2d:1a:f5:ba:
 bc:22:5a:c0:18:c5:38:4d:6a:d4:1e:8f:2b:c2:94:
 20:13:b0:5d:64:8a:5a:58:04:f4:97:ce:82:c7:5a:
 1e:0d:1b:5c:fd:c4:ba:a0:77:cc:1a:34:9e:96:30:
 ea:07:6d:69:ea:ea:2c:b4:0a:4f:5e:74:d5:13:01:
 8c:1b:c8:93:14:38:fb:15:96:9f:aa:85:c6:e8:8e:
 7e:22:34:99:42:6d:3e:1d:38:d9:93:3f:bb:6c:8a:
 e6:3c:f9:24:68:2a:2f:11:f5:53:2a:4f:a2:51:da:
 50:55:bd:24:85:a4:7c:5f:4c:53:f3:f5:69:24:07:
 56:2c:e5:ce:b6:1e:03:1d:28:06:9d:46:02:26:34:
 ad:17:67:80:de:c1:76:83:38:86:0b:9f:c4:e6:3f:
 02:fa:3f:3e:01:b3:92:ec:31:12:f8:8b:89:e2:e1:
 41:ae:3b
Exponent: 65537 (0x10001)
- Certificate Type -
X.509

***** ALMA ISLEMI TAMAMLANDI *****
root@ubuntu-512mb-fra1-02:~# md5sum Data_Algorithms.pdf
0e0ef8efbf129c2a01554b2d044ac5aa Data_Algorithms.pdf
root@ubuntu-512mb-fra1-02:~# md5sum Data_Algorithms_alindi.pdf
0e0ef8efbf129c2a01554b2d044ac5aa Data_Algorithms_alindi.pdf
root@ubuntu-512mb-fra1-02:~#
```



Resim-2: Alicidaki keyfile, bob.key ile değiştirilmiştir.

[X509: KEY\_VALUES\_MISMATCH] key values mismatch

Değiştirilen key, sertifika ile uyuşmadığının bu istisna meydana gelmiştir.

```
root@ubuntu-512mb-fra1-01: ~  
root@ubuntu-512mb-fra1-01:~# python3 gonderici_TCP.py  
fra1-01 IP: 46.101.202.226  
fra1-02 IP: 46.101.222.96  
Public-Key: (4096 bit)  
Modulus:  
00:bc:a2:c0:f1:54:61:b4:c3:c0:45:d0:c5:60:77:  
8c:19:95:02:90:d5:e4:6d:97:4e:10:c9:4d:5c:b1:  
ae:5b:8d:c3:4c:c1:7f:45:9b:fc:0f:d7:30:26:6e:  
12:0b:93:fa:de:d5:7b:33:fe:75:ec:f7:17:3f:64:  
6f:bd:1b:88:ae:1b:61:36:42:7c:ae:39:9d:2f:45:  
88:98:4b:6d:24:e1:03:cb:eb:2b:be:f4:1d:c3:d8:  
b5:e7:7b:38:ec:74:3b:4c:64:16:12:56:b5:73:b9:  
bc:0c:f6:d0:73:ff:b9:25:1d:73:e5:f4:db:23:47:  
fb:37:e6:78:8c:52:36:64:93:65:48:d9:11:b4:a3:  
fd:82:ce:ef:e0:3f:e0:bb:68:4d:3b:33:a9:83:11:  
31:9a:2c:6d:84:a7:ad:18:0b:58:08:c4:28:0b:54:  
50:49:cb:23:4f:c9:64:aa:42:16:cf:ba:29:9e:be:  
b7:db:67:90:d5:bc:89:93:f1:92:b6:36:df:12:cd:  
b2:ba:e5:c9:8c:10:77:15:34:c3:4b:b6:c6:c4:79:  
4c:17:3e:55:90:63:94:00:e1:f7:28:5c:c8:f1:cf:  
af:d0:4b:c8:92:8b:46:a9:ad:cb:1d:2c:6d:d1:18:  
b8:53:ca:4f:34:2f:cc:c9:e1:c9:9a:8f:c0:5e:56:  
17:db:bf:f6:a7:c1:c7:53:33:e4:61:1d:35:2b:7d:  
f1:4e:af:5e:4c:a0:90:81:a5:36:68:ce:f8:0c:74:  
1f:5a:55:60:78:18:45:1b:f0:bf:2a:98:d3:35:2a:  
65:7c:bd:e5:de:d3:b3:b4:47:d9:09:c5:73:c8:48:  
b4:7d:40:1f:06:b5:27:8f:27:df:4f:8d:9e:ed:34:  
be:16:1e:6b:ca:fd:6e:35:cb:84:7e:27:0c:ec:73:  
cc:80:b0:b5:10:90:6d:85:b0:68:5c:c7:81:ac:f9:  
4e:02:f9:0d:41:d9:8d:de:ac:b6:6a:e0:cd:bd:b7:  
c7:ef:ed:53:af:a7:8a:13:ac:a3:ab:4e:6b:26:67:  
56:c3:f7:cc:2f:91:d3:c7:d3:be:f5:bb:33:b9:90:  
90:19:e3:6d:c9:99:47:30:7b:85:13:0a:25:f8:22:  
38:76:d8:ae:91:7f:da:61:95:36:38:39:10:a0:97:  
42:b6:b4:76:a9:e7:00:be:59:91:2f:1f:08:8f:b5:  
67:4a:0d:fc:17:04:58:57:95:e8:f5:cb:d4:23:5b:  
56:d7:fa:29:53:7f:f5:bb:25:f9:41:9d:ad:3e:d9:  
e1:a6:61:ef:4e:19:0e:5d:79:b6:1b:91:2a:08:56:  
ad:77:92:38:30:13:84:85:7d:9e:3b:f7:cc:72:d1:  
1b:b5:5d  
Exponent: 65537 (0x10001)  
- Certificate Type -  
X.509  
***** GONDERME ISLEMI TAMAMLANDI *****  
[ ]
```

```
root@ubuntu-512mb-fra1-02: ~  
root@ubuntu-512mb-fra1-02:~# python3 alici_TCP.py  
fra1-01 IP: 46.101.202.226  
fra1-02 IP: 46.101.222.96  
Gonderici sunucunun IP'sini giriniz: 46.101.202.226  
[X509: KEY_VALUES_MISMATCH] key values mismatch (_ssl.c:2536)  
Traceback (most recent call last):  
  File "alici_TCP.py", line 93, in <module>  
    alici.run()  
  File "alici_TCP.py", line 60, in run  
    cert = self.ssl_socket.getpeercert(binary_form=True)  
AttributeError: 'NoneType' object has no attribute 'getpeercert'  
root@ubuntu-512mb-fra1-02:~# [ ]
```

Resim-3: Alicida hem keyfile bob.key ile, certfile da bob.pem ile değiştirilmiştir.

[SSL: TLSV1\_ALERT\_UNKNOWN\_CA] tlsv1 alert unknown ca (\_ssl.c:600)

Artık key ve sertifika uyumludur ancak durum ca file ile çelişmektedir. Bu nedenle bu istisna meydana gelmiştir.

```
root@ubuntu-512mb-fra1-01: ~
root@ubuntu-512mb-fra1-01:~# python3 gonderici_TCP.py
fra1-01 IP: 46.101.202.226
fra1-02 IP: 46.101.222.96
Public-Key: (4096 bit)
Modulus:
  00:bc:a2:c0:f1:54:61:b4:c3:c0:45:d0:c5:60:77:
  8c:19:95:02:90:d5:e4:6d:97:4e:10:c9:4d:5c:b1:
  ae:5b:8d:c3:4c:c1:7f:45:9b:fc:0f:d7:30:26:6e:
  12:0b:93:fa:de:d5:7b:33:fe:75:ec:f7:17:3f:64:
  6f:bd:1b:88:ae:1b:61:36:42:7c:ae:39:9d:2f:45:
  88:98:4b:6d:24:e1:03:cb:eb:2b:be:f4:1d:c3:d8:
  b5:e7:7b:38:ec:74:3b:4c:64:16:12:56:b5:73:b9:
  bc:0c:f6:d0:73:ff:b9:25:1d:73:e5:f4:db:23:47:
  fb:37:e6:78:8c:52:36:64:93:65:48:d9:11:b4:a3:
  fd:82:ce:ef:e0:3f:e0:bb:68:4d:3b:33:a9:83:11:
  31:9a:2c:6d:84:a7:ad:18:0b:58:08:c4:28:0b:54:
  50:49:cb:23:4f:c9:64:aa:42:16:cf:ba:29:9e:be:
  b7:db:67:90:d5:bc:89:93:f1:92:b6:36:df:12:cd:
  b2:ba:e5:c9:8c:10:77:15:34:c3:4b:b6:c6:c4:79:
  4c:17:3e:55:90:63:94:00:e1:f7:28:5c:c8:f1:cf:
  af:d0:4b:c8:92:8b:46:a9:ad:cb:1d:2c:6d:d1:18:
  b8:53:ca:4f:34:2f:cc:c9:e1:c9:9a:8f:c0:5e:56:
  17:db:bf:f6:a7:c1:c7:53:33:e4:61:1d:35:2b:7d:
  f1:4e:af:5e:4c:a0:90:81:a5:36:68:ce:f8:0c:74:
  1f:5a:55:60:78:18:45:1b:f0:bf:2a:98:d3:35:2a:
  65:7c:bd:e5:de:d3:b3:b4:47:d9:09:c5:73:c8:48:
  b4:7d:40:1f:06:b5:27:8f:27:df:4f:8d:9e:ed:34:
  be:16:1e:6b:ca:fd:6e:35:cb:84:7e:27:0c:ec:73:
  cc:80:b0:b5:10:90:6d:85:b0:68:5c:c7:81:ac:f9:
  4e:02:f9:0d:41:d9:8d:de:ac:b6:6a:e0:cd:bd:b7:
  c7:ef:ed:53:af:a7:8a:13:ac:a3:ab:4e:6b:26:67:
  56:c3:f7:cc:2f:91:d3:c7:d3:be:f5:bb:33:b9:90:
  90:19:e3:6d:c9:99:47:30:7b:85:13:0a:25:f8:22:
  38:76:d8:ae:91:7f:da:61:95:36:38:39:10:a0:97:
  42:b6:b4:76:a9:e7:00:be:59:91:2f:1f:08:8f:b5:
  67:4a:0d:fc:17:04:58:57:95:e8:f5:cb:d4:23:5b:
  56:d7:fa:29:53:7f:f5:bb:25:f9:41:9d:ad:3e:d9:
  e1:a6:61:ef:4e:19:0e:5d:79:b6:1b:91:2a:08:56:
  ad:77:92:38:30:13:84:85:7d:9e:3b:f7:cc:72:d1:
  1b:b5:5d
Exponent: 65537 (0x10001)
- Certificate Type -
X.509

*****      GONDERME      ISLEMI      TAMAMLANDI      *****

[SSL: NO_CERTIFICATE_RETURNED] no certificate returned
(_ssl.c:600)
```

```
root@ubuntu-512mb-fra1-02: ~
root@ubuntu-512mb-fra1-02:~# python3 alici_TCP.py
fra1-01 IP: 46.101.202.226
fra1-02 IP: 46.101.222.96
Gonderici sunucunun IP'sini giriniz: 46.101.202.226
[SSL: TLSV1_ALERT_UNKNOWN_CA] tlsv1 alert unknown ca (_ssl.c:600)
Traceback (most recent call last):
  File "alici_TCP.py", line 93, in <module>
    alici.run()
  File "alici_TCP.py", line 60, in run
    cert = self.ssl_socket.getpeercert(binary_form=True)
  File "/usr/lib/python3.4/ssl.py", line 671, in getpeercert
    return self._sslobj.peer_certificate(binary_form)
AttributeError: 'NoneType' object has no attribute 'peer_certificate'
root@ubuntu-512mb-fra1-02:~#
```



Resim-4: Alicida hem keyfile bob.key ile, certfile bob.pem ve cafile da bobca.pem ile değiştirilmiştir.

[SSL: CERTIFICATE\_VERIFY\_FAILED] certificate verify failed (\_ssl.c:600)

Gönderici de 'tlsv1 alert unknown ca' exception'ı gözükmüştür.

Artık alici tarafındaki her şey birbiriyle uyumludur ancak gönderici tarafında tanınmadığı için bu istisna meydana gelmiştir.

```
root@ubuntu-512mb-fra1-01: ~
root@ubuntu-512mb-fra1-01:~# python3 gonderici_TCP.py
fra1-01 IP: 46.101.202.226
fra1-02 IP: 46.101.222.96
Public-Key: (4096 bit)
Modulus:
 00:bc:a2:c0:f1:54:61:b4:c3:c0:45:d0:c5:60:77:
 8c:19:95:02:90:d5:e4:6d:97:4e:10:c9:4d:5c:b1:
 ae:5b:8d:c3:4c:c1:7f:45:9b:fc:0f:d7:30:26:6e:
 12:0b:93:fa:de:d5:7b:33:fe:75:ec:f7:17:3f:64:
 6f:bd:1b:88:ae:1b:61:36:42:7c:ae:39:9d:2f:45:
 88:98:4b:6d:24:e1:03:cb:eb:2b:be:f4:1d:c3:d8:
 b5:e7:7b:38:ec:74:3b:4c:64:16:12:56:b5:73:b9:
 bc:0c:f6:d0:73:ff:b9:25:1d:73:e5:f4:db:23:47:
 fb:37:e6:78:8c:52:36:64:93:65:48:d9:11:b4:a3:
 fd:82:ce:ef:e0:3f:e0:bb:68:4d:3b:33:a9:83:11:
 31:9a:2c:6d:84:a7:ad:18:0b:58:08:c4:28:0b:54:
 50:49:cb:23:4f:c9:64:aa:42:16:cf:ba:29:9e:be:
 b7:db:67:90:d5:bc:89:93:f1:92:b6:36:df:12:cd:
 b2:ba:e5:c9:8c:10:77:15:34:c3:4b:b6:c6:c4:79:
 4c:17:3e:55:90:63:94:00:e1:f7:28:5c:c8:f1:cf:
 af:d0:4b:c8:92:8b:46:a9:ad:cb:1d:2c:6d:d1:18:
 b8:53:ca:4f:34:2f:cc:c9:e1:c9:9a:8f:c0:5e:56:
 17:db:bf:f6:a7:c1:c7:53:33:e4:61:1d:35:2b:7d:
 f1:4e:af:5e:4c:a0:90:81:a5:36:68:ce:f8:0c:74:
 1f:5a:55:60:78:18:45:1b:f0:bf:2a:98:d3:35:2a:
 65:7c:bd:e5:de:d3:b3:b4:47:d9:09:c5:73:c8:48:
 b4:7d:40:1f:06:b5:27:8f:27:df:4f:8d:9e:ed:34:
 be:16:1e:6b:ca:fd:6e:35:cb:84:7e:27:0c:ec:73:
 cc:80:b0:b5:10:90:6d:85:b0:68:5c:c7:81:ac:f9:
 4e:02:f9:0d:41:d9:8d:de:ac:b6:6a:e0:cd:bd:b7:
 c7:ef:ed:53:af:a7:8a:13:ac:a3:ab:4e:6b:26:67:
 56:c3:f7:cc:2f:91:d3:c7:d3:be:f5:bb:33:b9:90:
 90:19:e3:6d:c9:99:47:30:7b:85:13:0a:25:f8:22:
 38:76:d8:ae:91:7f:da:61:95:36:38:39:10:a0:97:
 42:b6:b4:76:a9:e7:00:be:59:91:2f:1f:08:8f:b5:
 67:4a:0d:fc:17:04:58:57:95:e8:f5:cb:d4:23:5b:
 56:d7:fa:29:53:7f:f5:bb:25:f9:41:9d:ad:3e:d9:
 e1:a6:61:ef:4e:19:0e:5d:79:b6:1b:91:2a:08:56:
 ad:77:92:38:30:13:84:85:7d:9e:3b:f7:cc:72:d1:
 1b:b5:5d
Exponent: 65537 (0x10001)
- Certificate Type -
X.509

*****      GONDERME      ISLEMI      TAMAMLANDI      *****

[SSL: NO_CERTIFICATE_RETURNED] no certificate returned
(_ssl.c:600)
[SSL: TLSV1_ALERT_UNKNOWN_CA] tlsv1 alert unknown ca (
_ssl.c:600)

root@ubuntu-512mb-fra1-02: ~
root@ubuntu-512mb-fra1-02:~# python3 alici_TCP.py
fra1-01 IP: 46.101.202.226
fra1-02 IP: 46.101.222.96
Gonderici sunucunun IP'sini giriniz: 46.101.202.226
[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed (_ss
l.c:600)
Traceback (most recent call last):
  File "alici_TCP.py", line 93, in <module>
    alici.run()
  File "alici_TCP.py", line 60, in run
    cert = self.ssl_socket.getpeercert(binary_form=True)
  File "/usr/lib/python3.4/ssl.py", line 671, in getpeercert
    return self._sslobj.peer_certificate(binary_form)
AttributeError: 'NoneType' object has no attribute 'peer_certif
icate'
root@ubuntu-512mb-fra1-02:~#
```

Resim-5: Alicidaki keyfile, mevcut olmayan bir dosya olarak verilmiştir  
[certfile/certfile/cafile parametrelerinden birisi verilen dosya konumunda bulunamadi]

```
root@ubuntu-512mb-fra1-01: ~  
root@ubuntu-512mb-fra1-01:~# python3 gonderici_TCP.py  
fra1-01 IP: 46.101.202.226  
fra1-02 IP: 46.101.222.96  
[  
  
root@ubuntu-512mb-fra1-02: ~  
root@ubuntu-512mb-fra1-02:~# python3 alici_TCP.py  
fra1-01 IP: 46.101.202.226  
fra1-02 IP: 46.101.222.96  
Gonderici sunucunun IP'sini giriniz: 46.101.202.226  
certfile/certfile/cafile parametrelerinden birisi verilen dosya  
konumunda bulunamadi  
Traceback (most recent call last):  
  File "alici_TCP.py", line 93, in <module>  
    alici.run()  
  File "alici_TCP.py", line 60, in run  
    cert = self.ssl_socket.getpeercert(binary_form=True)  
AttributeError: 'NoneType' object has no attribute 'getpeercert'  
root@ubuntu-512mb-fra1-02:~#
```

- 1)[https://docs.python.org/3/library/ssl.html#ssl.SSLContext.wrap\\_socket](https://docs.python.org/3/library/ssl.html#ssl.SSLContext.wrap_socket)
- 2)<http://crypto.stackexchange.com/questions/26591/tls-encryption-with-a-self-signed-pki-and-python-s-asyncio-module>