Task: Bootleg Iodine
Operation: N.E.T.
Team: adrianb

By inspecting the .pcap network capture using Wireshark we can notice that the file transfer uses a weird protocol. Seems to be some sort of ftp. After taking a look at a implementation of the transfer protocol [1], we can notice that the file is sent in chunks. It appears that each chunk of data from the file is followed by ".<filename>". Also, it seems that the data is encoded in what appears to be base32, so we have only printable ASCII characters as data. This should be easy to parse using a simple regex like ''([A-Z0-9=]+)\.myfile' in order to extract the data. The next script outputs the base32 encoding that was transmitted using pyftpd.

```
#!/usr/bin/env python2
import dpkt
import re

reader =
dpkt.pcap.Reader(open('bootleg_iodine_b462e0e66e87e07b9fe15ec03b51dd321547e386.pcap'))

res = ''
for ts, data in reader:
    r = re.search('([A-Z0-9=]+)\\.myfile', data)
    if r:
        res += r.groups()[0]
        print(r.groups()[0])

print(res)
```

By decoding the output of the script we get the sent .pdf file, which contains the flag.

Flag: csc2016{rGMlTotCX6W2I5lxQHoV4zgHebc24RPf}

[1] http://pyftpd.sourcearchive.com/documentation/0.8.4.5/pyftpd_8py-source.html