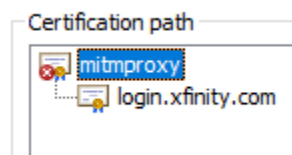
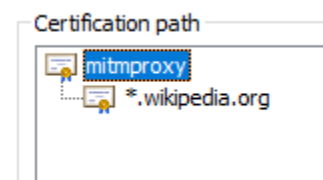


```
student@kali: ~ 01:40
File Actions Edit View Help
Flows
>> GET http://x1.c.lencr.org/
    ← 304 application/pkix-crl [no content] 63ms
GET http://burlingtoncityarts.org/
    ← 301 [no content] 28ms
GET http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/auth...
    ← 200 application/vnd.ms-cab-compressed 59.97k 108ms
GET https://www.burlingtoncityarts.org/ HTTP/2.0
    ← 200 text/html; charset=UTF-8 10.81k 118ms
GET https://www.burlingtoncityarts.org/sites/default/files/css/css_sBC-merr0GYa... HTTP/2.0
    ← 200 text/css 7.57k 130ms
GET https://www.burlingtoncityarts.org/sites/default/files/css/css_1G1WwdMdOt2S... HTTP/2.0
    ← 200 text/css 11.71k 145ms
GET https://www.burlingtoncityarts.org/sites/default/files/css/css_AbpHGcgLb-kR... HTTP/2.0
    ← 200 text/css 21b 159ms
GET https://www.burlingtoncityarts.org/themes/bca/logo.png HTTP/2.0
    ← 200 image/png 16.52k 164ms
GET https://www.burlingtoncityarts.org/sites/default/files/styles/full_width_sl... HTTP/2.0
    ← 200 image/jpeg 114.26k 429ms
GET https://www.burlingtoncityarts.org/sites/default/files/styles/full_w
    [1/27] [*:8080]
```

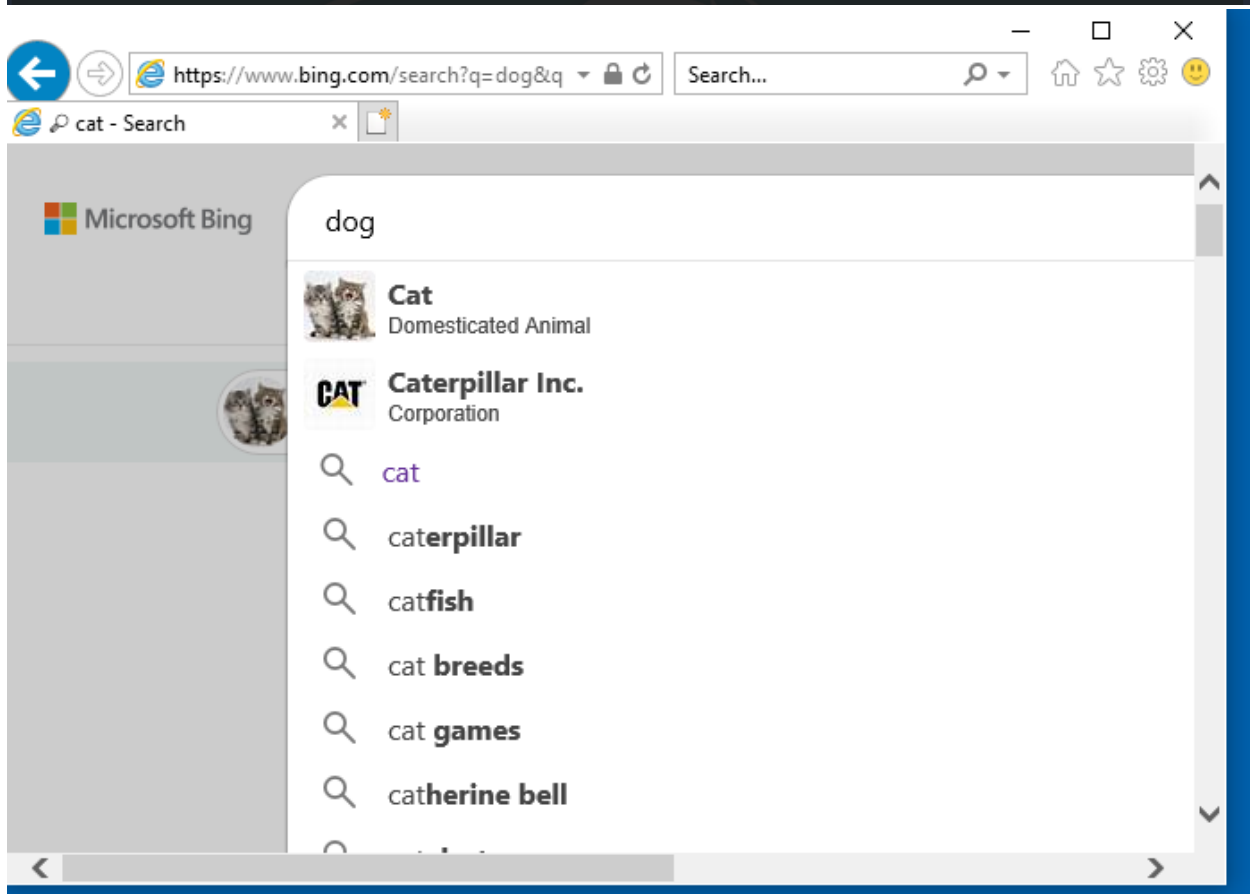
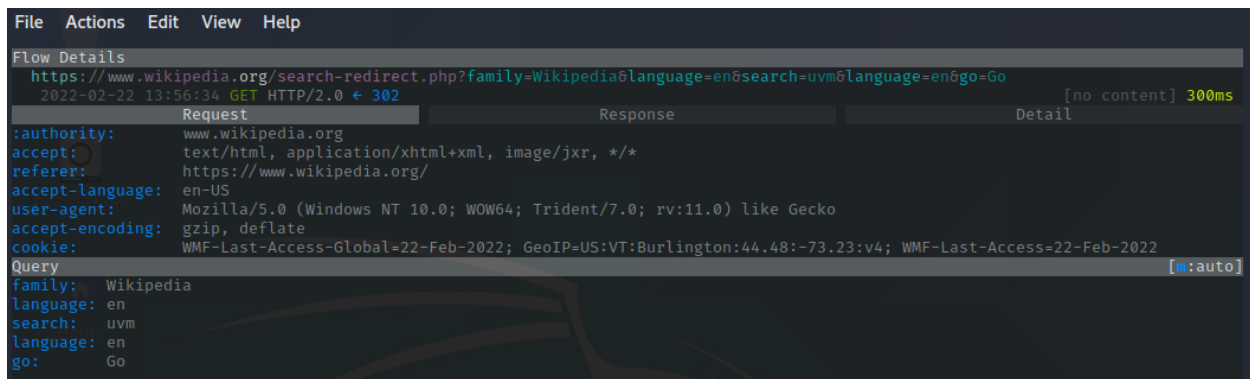


The Cert Error is due to the proxy creating an untrusted CA Cert. There is also only one certificate after that and there is no other form of verification that they are legit. \



It was able to run because the Cert we had just downloaded was placed in the Trusted Root Certification Authorities folder and is believed to be a trusted proxy.

```
Query
search: champlain college
go:      Go
ns0:     1
```



```
mitmproxy --replace :~q:dog:cat
```

A malicious attacker could use the MITMPROXY Replace in order to take control of the device. This could be a website or URL replacement to a custom webpage.