

Exercise 1

1. About 100

2.

They appear to be 14 characters long. Other than that, I can't see any pattern.
They appear to be random

3. It generates new domains each time.

Exercise 2 Part 1

1. About 70.

2.

According to whatismyipaddress.com, they are all corporate addresses. Some of them for microsoft updates. They likely belong to hosting companies.

3. It performs GET and POST requests.

```
12 Reassembled TCP Segments (51
Hypertext Transfer Protocol
  POST /home/ HTTP/1.1\r\n
    Cache-Control: no-cache\r\n
    Connection: Close\r\n
    Pragma: no-cache\r\n
    Accept: */*\r\n
    User-Agent: Mozilla/4.0 (comp
  Content-Length: 192\r\n
    Host: oavpyybehjtn.biz\r\n
    \r\n
```

4. The sample was able to connect.

```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    Server: nginx/1.4.4\r\n
    Date: Tue, 04 Feb 2014 07:48:58 GMT\r\n
    Content-Type: application/octet-stream\r\n
    Transfer-Encoding: chunked\r\n
    Connection: close\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 2.554347000 seconds]
    [Request in frame: 813]
    [Request URI: http://oavpyybehjtn.biz/home/
    HTTP chunked response
```

Exercise 2 Part 2

1.

It is connecting to microsoft services as well as a few suspicious sites such as bigdiscountsonline.info and endlessdeals.info.

2. It tries to request a text file.

```
Transmission Control Protocol, Src Port: 49168, Dst Port: 80, Seq: 1, Ack: 1
Hypertext Transfer Protocol
  GET /css/ notes/8179826378126.txt HTTP/1.1\r\n
  Connection: Keep-Alive\r\n
  Accept: */*\r\n
  Accept-Language: en-us\r\n
  User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)\r\n
  Host: endlessdeals.info\r\n
  \r\n
  [Full request URI: http://endlessdeals.info/css/ notes/8179826378126.txt]
  [HTTP request 1/2]
```

3. It is not successful.

```
Hypertext Transfer Protocol
  GET /css/ notes/8179826378126.txt HTTP/1.1\r\n
  Connection: Keep-Alive\r\n
  Accept: */*\r\n
  Accept-Language: en-us\r\n
  User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)\r\n
  Host: endlessdeals.info\r\n
  \r\n
  [Full request URI: http://endlessdeals.info/css/ notes/8179826378126.txt]
  [HTTP request 1/2]
```

