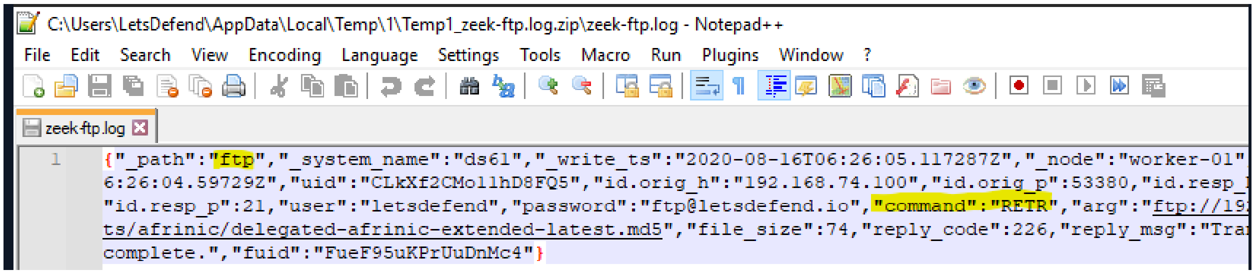
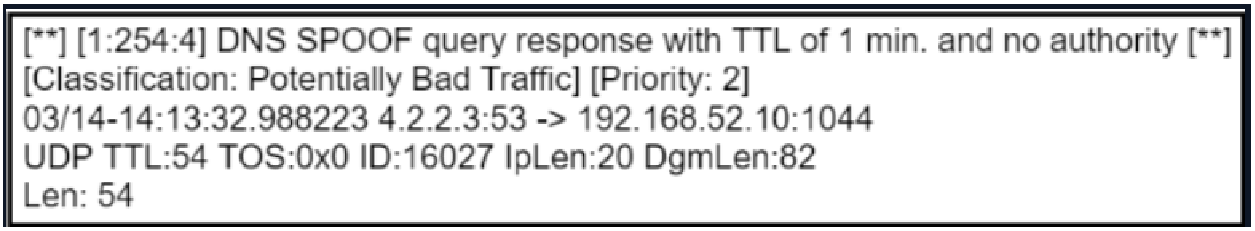

C:\Users\LetsDefend\AppData\Local\Temp\1\Temp1_zeek-ftp.log.zip\zeek-ftp.log - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
zeek-ftp.log

```
{"_path":"ftp","_system_name":"ds61","_write_ts":"2020-08-16T06:26:05.117287Z","_node":"worker-01"
6:26:04.597292","uid":"CLkXf2CMo1lhD8FQ5","id.orig_h":"192.168.74.100","id.orig_p":53380,"id.resp_
"id.resp_p":21,"user":"letsdefend","password":"ftp@letsdefend.io","command":"RETR","arg":"ftp://19
ts/afrinic/delegated-afrinic-extended-latest.md5","file_size":74,"reply_code":226,"reply_msg":"Tra
complete.","fuid":"FueF95uKPrUuDnMc4"}
```

Question: What is the FTP command used for file transfer according to the given Zeek IDS FTP log? **“Command”: “RETR”**



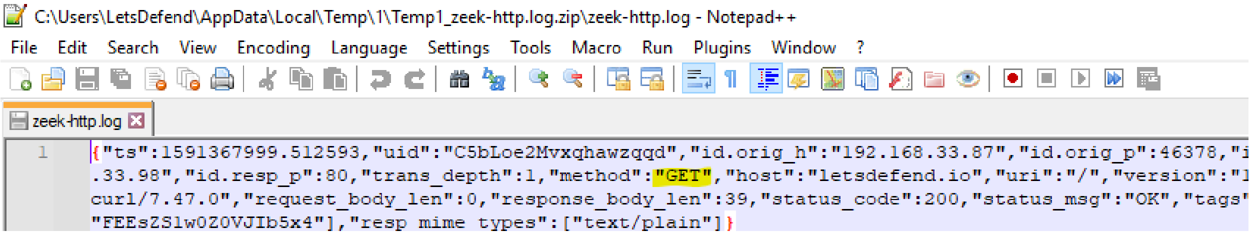
```
[**] [1:254:4] DNS SPOOF query response with TTL of 1 min. and no authority [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
03/14-14:13:32.988223 4.2.2.3:53 -> 192.168.52.10:1044
UDP TTL:54 TOS:0x0 ID:16027 IpLen:20 DgmLen:82
Len: 54
```

Check the Snort IDS log, according to the OSI model, which layer 7 network protocol does it belong to? **DNS**

Question: According to the Snort IDS log, what is the IP address from which the response came? **4.2.2.3**

How many of the following are tools in the IDS type?

1. Snort
2. Volatility
3. OllyDbg
4. Suricata
5. Zeek/Bro
6. REMnux


C:\Users\LetsDefend\AppData\Local\Temp\1\Temp1_zeek-http.log.zip\zeek-http.log - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
zeek-http.log

```
{"ts":1591367999.512593,"uid":"C5bLoe2Mvxqhawzqqd","id.orig_h":"192.168.33.87","id.orig_p":46378,"i
.33.98","id.resp_p":80,"trans_depth":1,"method":"GET","host":"letsdefend.io","uri":"/","version":"1
curl/7.47.0","request_body_len":0,"response_body_len":39,"status_code":200,"status_msg":"OK","tags"
"FEEsZS1w0Z0VJIb5x4"],"resp mime types":["text/plain"]}
```

Question: What is the HTTP request method according to the given Zeek IDS HTTP log?
“GET”