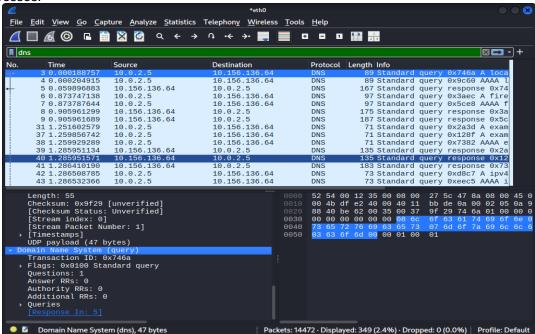
Wireshark Packet Capture Report

This report provides an analysis of network traffic captured using Wireshark. The capture session involved browsing websites and generating network activity. The data was filtered by different protocols including DNS, HTTP, and TCP to identify key traffic patterns.

1. DNS Protocol Analysis

The DNS (Domain Name System) protocol was captured showing domain resolution queries and responses. DNS packets are essential for translating human-readable domain names into IP addresses.



2. HTTP Protocol Analysis

HTTP traffic was captured, showing both GET and POST requests. One notable POST request included login form data being sent in plaintext, which indicates an insecure transmission.

```
<u>File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help</u>
• - 1 1 2 3
                                                                                                                                                                                                                                                                                                                                                  × - - +

        Time
        Source

        13739 168.874047790
        104.18.11.224

        13867 172.853744283
        10.0.2.5

        13819 173.155048030
        44.228.249.3

        13876 175.237845060
        10.0.2.5

                                                                                                                                                Destination
                                                                                                                                                                                                                                                           423 GET /static/app/partials/pop
533 HTTP/1.1 200 OK (text/html)
521 GET /twitter-bootstrap/2.3.1
412 GET /ajax/popular?offset=0 H
                                                                                                                                                  44.228.249.3
                                                                                                                                                                                                                        HTTP
                                                                                                                                                   104.18.10.207
          1387 175.20063435 10.0.2.5
13884 175.311962318 104.18.10.207
13886 175.443913982 10.0.2.5
13891 175.557547136 44.228.249.3
13898 175.765704945 44.228.249.3
        14072 194.526708997 10.0.2.5
14074 194.826946662 44.228.249.3
14085 196.627255899 10.0.2.5
14093 196.929959893 44.228.249.3
14166 294.796411812 10.0.2.5
14168 205.101367916 44.228.249.3
                                                                                                                                                                                                                                                       585 PUST / LOGIN HITP/1.1 (APPLI
562 HTTP/1.1 302 FOUND (text/ht
459 GET / HTTP/1.1
1429 HTTP/1.1 200 OK (text/html)
                                                                                                                                                  10.0.2.5
                                                                                                                                                  44.228.249.3
                                                                                                                                                                                                                                                           436 GET /ajax/popular?offset=0 H
217 HTTP/1.1 200 OK (text/html)
                                                                                                                                                  10.0.2.5
                                                                                                                                                                                                                        HTTP
    14168 205.101367916 44.228.249.3 10.0.2.5

......0.. = Reset: Not set
.....0 = Syn: Not set
.....0 = Fin: Not set
[TCP Flags: .....AP...]
Window: 65535
[Calculated window size: 65535]
[Window size scaling factor: -2 (no window scaling u Checksum: 0x341a [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
| [SEQ/ACK analysis]
| TCP payload (531 bytes)
| Hypertext Transfer Protocol
- POST /login HTTP/1.1\r\n
Request Method: POST
                                                                                                                                                                                                                                          34 1a 00 00 50 4f

48 54 54 50 2f 31

74 65 73 74 68 74

62 2e 63 6f 6d 0d

74 3a 20 4d 6f 7a

58 31 31 3b 20 4c

34 3b 20 72 76 3a

6b 6f 2f 32 30 31

66 6f 78 2f 31 32

74 3a 20 74 65 78

6c 69 63 61 74 69

6d 6c 2c 61 70 70

6d 6c 3b 71 3d 30

2e 38 0d 0a 41

61 67 65 3a 20 65

30 2e 35 0d 0a 41

64 66 68 27 2a 2a

60 40 41 50
                                                                                                                                                                                                                                                                                                            HTTP Request Method (http.request.method), 4 bytes
                                                                                                                                                                                       Packets: 14472 · Displayed: 154 (1.1%) · Dropped: 0 (0.0%) Profile: Default
```

3. Sensitive Data Exposure

The captured HTTP POST request to 'testhtml5.vulnweb.com/login' contained plaintext credentials: - Username: admin - Password: admin ka papa This highlights the risk of transmitting sensitive data without encryption.

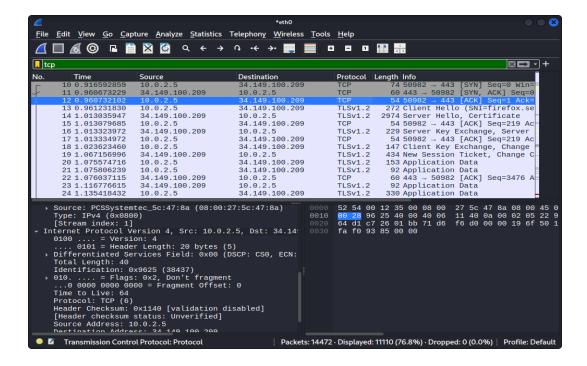
```
Wireshark · Packet 14072 · eth0
               Connection: keep-alive\r\n
Referer: http://testhtml5.vulnweb.com/\r\n
Upgrade-Insecure-Requests: 1\r\n
Priority: u=0, i\r\n
                                             <u>in frame: 14074]</u>
uest URI: http://testhtml5.vulnweb.com/login]
        HTML Form URL Encoded: application/x-www-form-urlencoded
> Form item: "username" = "admin"
> Form item: "password" = "admin ka papa"
                    4c 65 6e 67 74 68 3a 20
69 6e 3a 20 68 74 74 70
74 6d 6c 35 2e 76 75 6c
0d 0a 43 6f 6e 6e 65 63
65 70 2d 61 6c 69 76 65
72 3a 20 68 74 74 70 3a
6d 6c 35 2e 76 75 6c 6e
0d 0a 55 70 67 72 61 64
72 65 2d 52 65 71 75 65
50 72 69 6f 72 69 74 79
0d 0a 0d 0d 75 73 65 72
69 6e 26 70 61 73 73 77
                                                                                                    33 37 0d 0a 4f 72 69 67
3a 2f 2f 74 65 73 74 68
6e 77 65 62 2e 63 6f 6d
74 69 6f 6e 3a 20 6b 65
0d 0a 52 65 66 65 72 65
2f 2f 74 65 73 74 68 74
77 65 62 2e 63 6f 6d 2f
65 2d 49 6e 73 65 63 75
73 74 73 3a 20 31 0d 0a
3a 20 75 3d 30 2c 20 69
6e 61 6d 65 3d 61 64 6d
                                                                                                                                                                                         Length: 37..Orig
in: http://testh
tml5.vul nweb.com
..Connec tion: ke
                                                                                                                                                                                          ep-alive ··Refere
r: http://testht
ml5.vuln web.com/
                                                                                                                                                                                           ··Upgrad e-Insecu
re-Reque sts: 1··
                                                                                                                                                                                           Priority : u=0,
                      69 6e 26 70 61 73 73
6e 2b 6b 61 2b 70 61
                                                                                                                                                                                            n+ka+pap a
File Data (http.file_data), 37 bytes

√ Show packet bytes

                                                           Layout: Vertical (Stacked)
                                                                                                                                                                                                                                × Close
                                                                                                                                                                                                                                                                 🖸 Help
```

4. TCP Protocol Analysis

TCP packets show the handshake and data transfer process between the client and server. Several TLS-encrypted sessions were observed, indicating secure communication channels.



Summary of Findings

1. DNS queries reveal the domains being accessed. 2. HTTP traffic shows unencrypted credentials being transmitted. 3. TCP packets indicate both encrypted and unencrypted communication. 4. Sensitive information should always be transmitted over HTTPS to ensure security.