**Network Traffic Capture Report**

**Name:** Divyanshu Singh  
**Tool Used:** Wireshark  
**File Name:** capture file.pcap

**Capture .pcap file link:-** http://go.microsoft.com/fwlink/p/?LinkId=255141

**1. Capture Summary**

* **Total Packets Captured:** 6,380
* **Duration:** Approximately 1 minute
* **Interface:** eth0 (Virtualized Environment - VMware)

**2. Protocols Identified**

✅ **DNS (Domain Name System)**

* Resolving domain names to IP addresses
* Example Query to resolve domain name
* Traffic between 192.168.138.136 and DNS servers

✅ **TCP (Transmission Control Protocol)**

* Connection establishment and data transfer
* Includes SYN, ACK, 3-way handshake, and application data
* Communication with servers such as 34.36.137.203

✅ **HTTP (Hypertext Transfer Protocol)**

* Web browsing activity captured
* Requests for .jpg, .gif, .css, .ico, .jsp files
* Example:
* GET /images/home1.jpg HTTP/1.1

✅ **TLSv1.3 (Transport Layer Security)**

* Secure encrypted communication
* Seen during HTTPS connections (port 443)
* Handshake and cipher exchange details captured

**3. Notable Packet Examples**

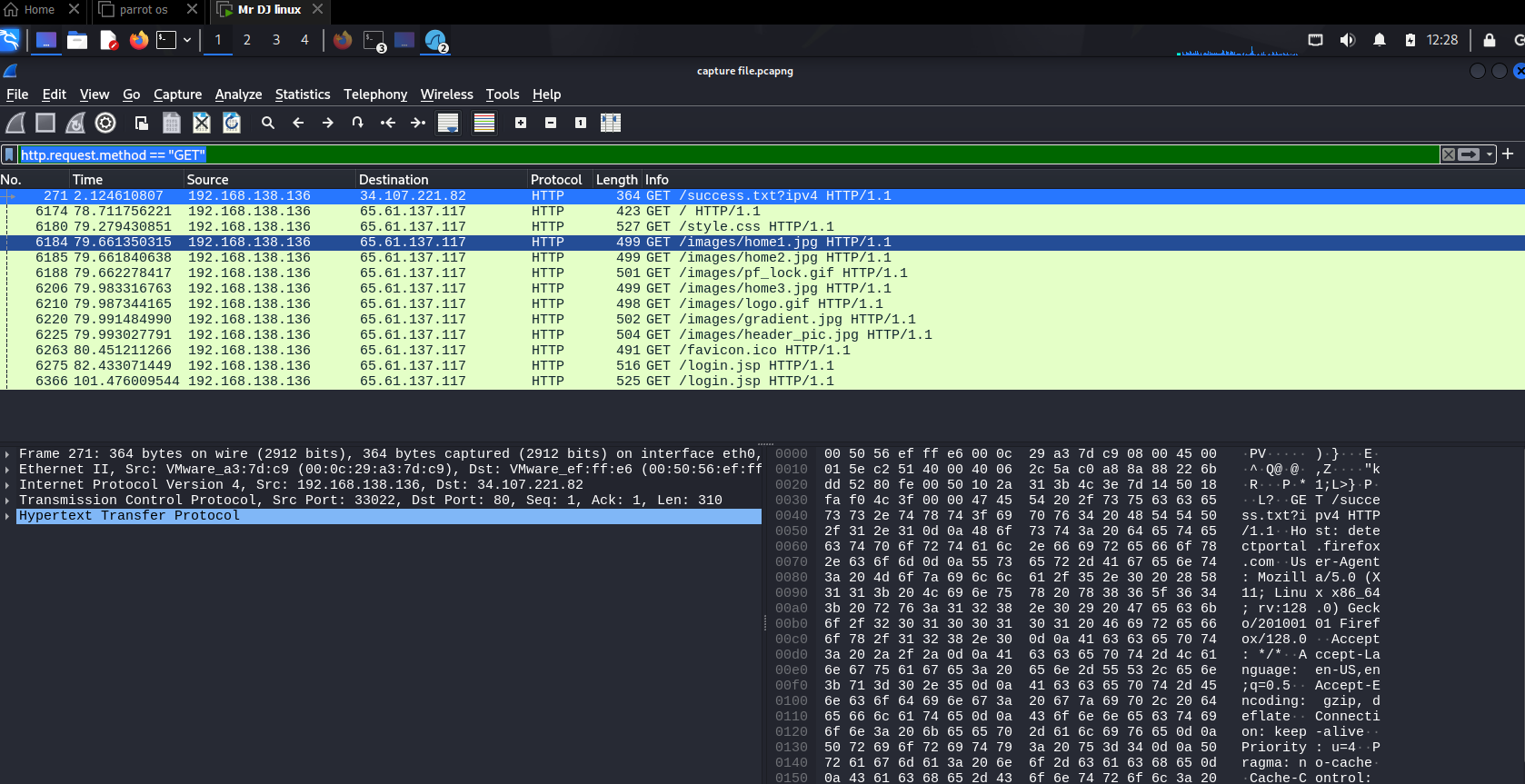
| **No.** | **Protocol** | **Source IP** | **Destination IP** | **Info** |
| --- | --- | --- | --- | --- |
| 1 | DNS | 192.168.138.136 | 192.168.138.2 | Standard query - domain resolution |
| 4 | TCP | 192.168.138.136 | 34.36.137.203 | SYN packet initiating connection |
| 6 | TCP | 34.36.137.203 | 192.168.138.136 | SYN-ACK response from remote server |
| 8 | TLSv1.3 | 192.168.138.136 | 34.36.137.203 | Client Hello initiating TLS handshake |
| 271 | HTTP | 192.168.138.136 | 34.107.221.82 | GET /success.txt?ipv4 HTTP/1.1 |
| 6184 | HTTP | 192.168.138.136 | 65.61.137.117 | GET /images/home1.jpg HTTP/1.1 |

**4. Observations**

✔ DNS queries were performed successfully to resolve domains.  
✔ TCP 3-way handshakes and encrypted TLS sessions indicate secure communication establishment.  
✔ Multiple HTTP GET requests suggest website browsing, requesting image assets, CSS files, and login pages.  
✔ The environment appears to be a virtual machine (VMware) based on captured MAC addresses.

**5. Conclusion**

The packet capture shows standard web browsing behavior in a controlled network. Multiple protocols interact as expected, including DNS for name resolution, TCP for reliable connections, HTTP for web resource retrieval, and TLS for encryption. No anomalies detected in the visible traffic.

[](capture%20file.pcapng)