WIRESHARK NETWORK TRAFFIC ANALYSIS REPORT

WIRESHARK NETWORK TRAFFIC ANALYSIS REPORT
Monitoring and Identifying Suspicious Network Activity

Conducted by:
Abosede Ogunlade
Cybersecurity Enthusiast & Analyst

Date: July 21, 2025

TABLE OF CONTENTS

INTRODUCTION

This network traffic analysis was performed to monitor live network activity, identify normal traffic patterns, and detect any unusual or potentially suspicious packets. The analysis was carried out using **Wireshark**, a network protocol analyzer commonly used by cybersecurity professionals.

OBJECTIVE

- Capture live network traffic on a home Wi-Fi network
- Identify normal vs. suspicious activity
- Provide recommendations for improving network security

TOOLS & METHODOLOGY

Tools Used

- **Wireshark** (latest version)

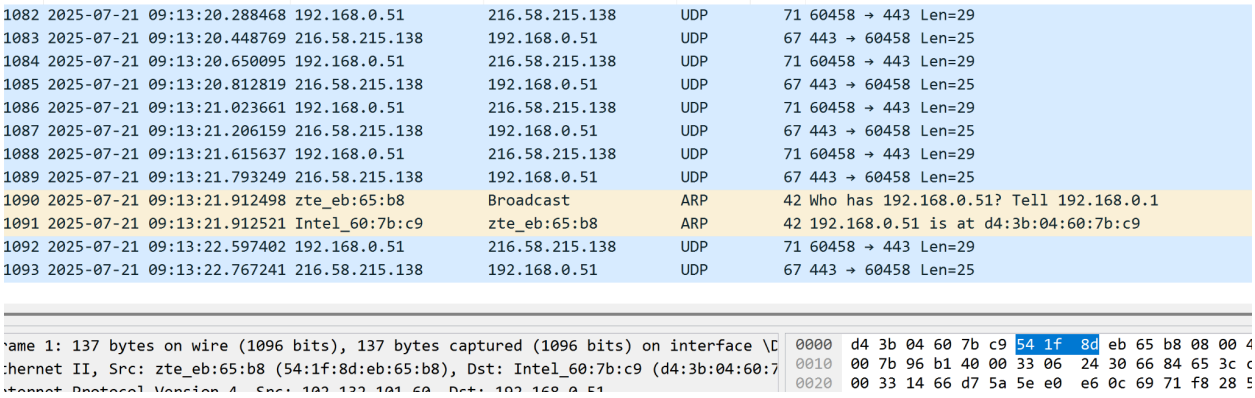
Process

1. Captured 5 minutes of live traffic over a Wi-Fi network.
2. Applied filters:
    - http → Analyze web traffic
    - dns → Check domain queries
    - tcp.port==445 → Check for SMB file-sharing traffic
3. Examined packet details for unusual IP addresses or protocols.

FINDINGS

4.1 Normal Traffic

- **TCP Port 80 (HTTP)**
    - **Status:** Normal web browsing activity
    - **Details:** Standard PSH, ACK flags with regular data flow.



```
1082 2025-07-21 09:13:20.288468 192.168.0.51     216.58.215.138   UDP   71 60458 → 443 Len=29
1083 2025-07-21 09:13:20.448769 216.58.215.138   192.168.0.51     UDP   67 443 → 60458 Len=25
1084 2025-07-21 09:13:20.650095 192.168.0.51     216.58.215.138   UDP   71 60458 → 443 Len=29
1085 2025-07-21 09:13:20.812819 216.58.215.138   192.168.0.51     UDP   67 443 → 60458 Len=25
1086 2025-07-21 09:13:21.023661 192.168.0.51     216.58.215.138   UDP   71 60458 → 443 Len=29
1087 2025-07-21 09:13:21.206159 216.58.215.138   192.168.0.51     UDP   67 443 → 60458 Len=25
1088 2025-07-21 09:13:21.615637 192.168.0.51     216.58.215.138   UDP   71 60458 → 443 Len=29
1089 2025-07-21 09:13:21.793249 216.58.215.138   192.168.0.51     UDP   67 443 → 60458 Len=25
1090 2025-07-21 09:13:21.912498 zte_eb:65:b8      Broadcast        ARP   42 Who has 192.168.0.51? Tell 192.168.0.1
1091 2025-07-21 09:13:21.912521 Intel_60:7b:c9    zte_eb:65:b8     ARP   42 192.168.0.51 is at d4:3b:04:60:7b:c9
1092 2025-07-21 09:13:22.597402 192.168.0.51     216.58.215.138   UDP   71 60458 → 443 Len=29
1093 2025-07-21 09:13:22.767241 216.58.215.138   192.168.0.51     UDP   67 443 → 60458 Len=25
```

```
ame 1: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits) on interface \D
thernet II, Src: zte_eb:65:b8 (54:1f:8d:eb:65:b8), Dst: Intel_60:7b:c9 (d4:3b:04:60:7
ternet Protocol Version 4, Src: 102.132.101.60, Dst: 192.168.0.51
```

```
0000  d4 3b 04 60 7b c9 54 1f  8d eb 65 b8 08 00 4
0010  00 7b 96 b1 40 00 33 06  24 30 66 84 65 3c c
0020  00 33 14 66 d7 5a 5e e0  e6 0c 69 71 f8 28 5
```

4.2 Suspicious Traffic

```
Internet Protocol Version 4, Src: 192.168.0.51, Dst: 2.23.210.7
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 52
   Identification: 0x9968 (39272)
 > 010. .... = Flags: 0x2, Don't fragment
   ...0 0000 0000 0000 = Fragment Offset: 0
   Time to Live: 128
   Protocol: TCP (6)
   Header Checksum: 0xcc61 [validation disabled]
   [Header checksum status: Unverified]
   Source Address: 192.168.0.51
   Destination Address: 2.23.210.7
```

```
 Transmission Control Protocol, Src Port: 80, Dst Port: 57779, Seq: 1, Ack: 125, Len
    Source Port: 80
    Destination Port: 57779
    [Stream index: 152]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 179]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 788830948
    [Next Sequence Number: 180    (relative sequence number)]
    Acknowledgment Number: 125    (relative ack number)
    Acknowledgment number (raw): 397729141
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 501
```

-
    - **Status:** Potentially unnecessary traffic
    - **Risk:** Could expose the system to external scanning or exploitation if left unchecked.

RECOMMENDATIONS

✔ Monitor network traffic regularly for unusual ports or DNS queries.
✔ Disable unnecessary services (e.g., SMB on port 445) if not required.
✔ Keep devices updated with the latest security patches.
✔ Consider using a firewall or Intrusion Detection System (IDS) for continuous monitoring.

CONCLUSION

The network appeared mostly normal, with typical web browsing and DNS traffic. However, some unnecessary or unusual packets were detected, which could potentially be exploited if not properly secured. Regular monitoring and basic hardening practices are recommended.