

Lab Objective This document provides a comprehensive, beginner-friendly analysis of real network traffic using Wireshark, with a focus on identifying potential cybersecurity threats. Each protocol-level observation is interpreted and explained in a manner suitable for students with limited background in cybersecurity.

In your case these will be different but similar analysis

Figure 1: tcp_analysis_retransmission

Page	Line	Doc	Doc Date	Phone	Length	Doc	Destination unreachable	Communication administratively filtered
	187	3.12787263	77.235.47.38		102.168.64.2	120P		
	188	3.12777348	77.235.47.38		102.168.64.2	120P	Destination unreachable	Communication administratively filtered
	434	3.12788478	102.168.64.2		172.64.166.152	120P	Destination unreachable	Port unreachable
	435	3.12788428	102.168.64.2		172.64.166.152	120P	Destination unreachable	Port unreachable
	444	3.12788453	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	451	3.17831574	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	452	3.14488819	102.168.64.2		172.64.166.152	120P	Destination unreachable	Port unreachable
	453	3.14487874	102.168.64.2		172.64.166.152	120P	Destination unreachable	Port unreachable
	454	3.14488819	77.235.47.38		102.168.64.2	120P	Destination unreachable	Communication administratively filtered
	499	3.17111311	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	588	3.16612138	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	593	3.16616112	102.168.64.2		172.64.166.152	120P	Destination unreachable	Port unreachable
	593	3.16611112	102.168.64.2		172.64.166.152	120P	Destination unreachable	Port unreachable
	594	3.16688493	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	1624	3.14488819	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	1286	4.88641246	77.235.47.38		102.168.64.2	120P	Destination unreachable	Communication administratively filtered
	1287	3.17991111	102.168.64.2		166.22.1.97	120P	Destination unreachable	Port unreachable
	1360	4.88641274	102.168.64.2		166.22.1.97	120P	Destination unreachable	Port unreachable
	1361	3.17991111	102.168.64.2		166.22.1.97	120P	Destination unreachable	Port unreachable
	1368	4.88631424	102.168.64.2		166.22.1.97	120P	Destination unreachable	Port unreachable
	1369	3.17991111	102.168.64.2		166.22.1.97	120P	Destination unreachable	Port unreachable
	1822	5.89138862	102.168.64.2		172.64.166.152	120P	Destination unreachable	Port unreachable
	1823	3.17991111	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	1832	3.124242613	102.168.64.2		166.22.1.97	120P	Destination unreachable	Port unreachable
	1833	3.124242613	77.235.47.38		102.168.64.2	120P	Destination unreachable	Communication administratively filtered
	1834	4.88641872	77.235.47.38		102.168.64.2	120P	Destination unreachable	Communication administratively filtered
	2125	3.17991111	102.168.64.2		166.22.1.97	120P	Destination unreachable	Port unreachable
	2428	5.97138819	102.168.64.2		172.64.166.152	120P	Destination unreachable	Port unreachable
	2515	3.17991111	102.168.64.2		172.64.166.152	120P	Destination unreachable	Port unreachable
	2712	7.28035815	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	4558	5.83137721	35.214.126.108		102.168.64.2	78	Destination unreachable	Port unreachable
	4558	5.83137721	78.214.126.108		102.168.64.2	78	Destination unreachable	Port unreachable
	4932	8.88428762	102.168.64.2		166.22.1.97	120P	Destination unreachable	Port unreachable
	4933	3.17991111	102.168.64.2		166.22.1.97	120P	Destination unreachable	Port unreachable
	5878	8.88627888	77.235.47.38		102.168.64.2	120P	Destination unreachable	Communication administratively filtered
	5879	3.17991111	77.235.47.38		102.168.64.2	120P	Destination unreachable	Communication administratively filtered
	5155	8.90488735	35.214.126.108		102.168.64.2	78	Destination unreachable	Port unreachable
	5155	8.90488735	78.214.126.108		102.168.64.2	78	Destination unreachable	Port unreachable
	5478	5.26453194	35.214.126.108		102.168.64.2	78	Destination unreachable	Port unreachable
	5488	5.26525262	35.214.126.108		102.168.64.2	78	Destination unreachable	Port unreachable
	5489	5.26525266	35.214.126.108		102.168.64.2	78	Destination unreachable	Port unreachable
	6128	8.90488735	35.214.126.108		102.168.64.2	78	Destination unreachable	Port unreachable
	6129	8.90488735	78.214.126.108		102.168.64.2	78	Destination unreachable	Port unreachable
	6238	18.51139419	35.214.126.108		102.168.64.2	78	Destination unreachable	Port unreachable
	6238	18.51139419	78.214.126.108		102.168.64.2	78	Destination unreachable	Port unreachable
	6248	18.51139242	35.214.126.108		102.168.64.2	78	Destination unreachable	Port unreachable
	6248	18.51139242	78.214.126.108		102.168.64.2	78	Destination unreachable	Port unreachable
	6249	18.72999112	102.168.64.2		172.64.166.152	120P	Destination unreachable	Port unreachable
	6249	18.72999112	102.168.64.2		172.64.166.152	120P	Destination unreachable	Port unreachable
	7403	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.16.41.184	120P	Destination unreachable	Port unreachable
	7406	11.14444414	102.168.64.2		166.1			

1. Understanding the Context: Why Analyze Network Traffic?

This lab specifically examines:

2. DNS Traffic Analysis (Application Layer - OSI Layer 7)

DNS translates human-readable domain names (like `www.google.com`) into IP addresses that machines use to communicate. It is a foundational protocol that operates at Layer 7.

Observed Behavior:

- A series of DNS queries from 192.168.64.2 to 192.168.64.1.
- Many queries target legitimate services like Google Fonts, analytics services, and CDNs.
- Queries include additional OPT fields (EDNS0 extensions) and CNAME chains.

What is a CNAME?

CNAME stands for Canonical Name. It is a type of DNS record that maps one domain name (an alias) to another domain name (the canonical or "true" name). For example, a DNS request to `track.example.com` might return a CNAME record pointing to `analytics.service.com`, which is the actual server handling the request.

This redirection capability can be abused by third-party trackers. Instead of directly including third-party analytics scripts, a website owner might set up a subdomain that uses a CNAME to point to an external tracking domain. To a user or a casual inspection tool, all requests appear to go to the site's own domain (e.g., `track.mysite.com`), effectively hiding the presence of third-party trackers.

Potential Security Issues:

1. **Tracking and Profiling:**
 - Domains like `google-analytics.com`, `vidoomy.com`, and `inmobi.com` are commonly used for user tracking.
 - CNAME records that chain through multiple domains may mask third-party trackers by making them appear as first-party requests.
2. **DNS Tunneling (Hypothetical):** DNS tunneling is a method where an attacker encodes data from a compromised system into DNS queries. These queries are then sent to an attacker's controlled DNS server, which decodes the information. This technique bypasses most traditional network defenses because DNS is generally trusted and rarely blocked by firewalls.

For example, an infected computer might convert sensitive data into a long string and send a query like `abcd1234.compromised-data.evil.com`. The domain `evil.com` is owned by the attacker, who can log the full query and decode the data. This allows covert communication and data exfiltration even from restricted networks.

A second method involves encoding command-and-control messages into the DNS response itself. The malware sends a lookup request, and the attacker's server responds with encoded instructions. This lets the attacker control the compromised system using only DNS traffic, which is usually unmonitored.

Why It Matters:

Malicious actors may hide data transfers or command-and-control messages in DNS traffic. Even benign services may reduce privacy by sharing data with multiple trackers.

3. TCP/TLS Traffic Analysis (Transport & Session Layers - OSI Layers 4 & 5)

What is TCP?

TCP ensures reliable data delivery between systems by managing how data is broken into packets, transmitted, and reassembled. TLS (often used with HTTPS) encrypts this data to provide confidentiality and integrity.

Observed Behavior:

- Numerous retransmissions (standard, fast, and spurious) between internal host and multiple external IPs.
- Packet loss inferred from TCP PDU reassembly messages.

Potential Security Issues:

1. **Denial of Service (DoS) Symptoms:** DoS attacks are designed to exhaust system resources, making a device or service unavailable to legitimate users. In the observed case, persistent retransmissions and TCP packet reassemblies could mean the host is overwhelmed by malformed or excessive traffic. An attacker might simulate connection attempts that are intentionally incomplete or delayed to keep sessions open, thereby overloading the system's memory or processing power. Such TCP-level flooding is a hallmark of volumetric or protocol DoS attacks and can be particularly damaging when not rate-limited.
2. **Man-in-the-Middle (MITM) Suspicions:** MITM attacks occur when an adversary secretly intercepts and potentially alters communications between two parties. One method to implement this involves delaying or modifying TCP packets. For example, a rogue router or compromised access point might intercept packets, inject its own sequence numbers, or strip authentication headers. The result: increased retransmissions and confusing behavior visible in packet captures. These symptoms may be the only visible clues that someone is sitting between the client and the server, inspecting or tampering with encrypted sessions before relaying them.
3. **Poor Network Hygiene:** Not every retransmission is malicious. However, frequent and unexplained retransmissions can reveal poor configurations such as overloaded routers, misconfigured TCP window sizes, or even faulty network cables. From a cybersecurity standpoint, unreliable infrastructure is dangerous: it increases the likelihood that attacks will go unnoticed or misattributed. Moreover, attackers can exploit this instability, for instance, by launching attacks when they know legitimate monitoring tools are struggling to maintain reliable packet visibility.

Why It Matters:

Reliable transmission and proper session management are crucial for secure communications. Anomalies at these layers may expose vulnerabilities or point to underlying attack attempts.

4. ICMP Traffic Analysis (Network Layer – OSI Layer 3)

What is ICMP?

ICMP (Internet Control Message Protocol) is a support protocol used by network devices to send diagnostic or control messages. It does not carry application data but reports conditions such as unreachable hosts or network errors. Common tools like ping and traceroute use ICMP to check connectivity or path information.

Observed Behavior

- A significant number of Destination Unreachable ICMP messages were recorded.
- These messages fell into two categories:
 - **Port unreachable** – indicating that a host was reachable, but the specific port had no application listening.
 - **Communication administratively filtered** – showing that a firewall or policy explicitly blocked communication attempts.

Potential Security Issues

1. Reconnaissance and Port Scanning

Attackers often begin their campaigns with a technique called *network reconnaissance*. One approach is to send traffic to many ports and record the ICMP responses. If a port is closed, the attacker might receive a Port unreachable message. If a firewall is present, it may return a Filtered message or nothing at all.

For example, a scanner might probe 192.168.64.2 on ports 21, 22, 80, 443, etc., and based on the ICMP replies, determine:

- Which ports are active,
- Which services are exposed, and
- What kind of firewall rules are in place.

This helps the attacker construct a map of the network and identify targets for exploitation.

2. Firewall Activity Insight

Seeing ICMP messages like “administratively filtered” confirms that firewalls or security appliances are actively controlling traffic. This is generally good. However, the *presence and behavior* of those filters can still inform attackers. If a firewall responds consistently to certain types of traffic, it may leak information about its ruleset, version, or vendor.

For defenders, these ICMP logs are valuable—they confirm that security policies are being enforced. But from an adversary’s view, this feedback loop can be reverse-engineered to bypass filters.

3. Evasion and Probing Attempts

A large volume of ICMP traffic may indicate stealthy probing. Advanced attackers use automated tools to send probes slowly and spread out across time to avoid triggering alerts. Others might disguise their scans as legitimate network testing tools. In this way, ICMP becomes a double-edged sword: helpful for administrators, but also useful for attackers trying to fly under the radar.

Why It Matters

Even though ICMP is a simple protocol, it can become a powerful reconnaissance tool in the wrong hands. Unmanaged ICMP behavior may unintentionally leak details about your network structure, firewall logic, and exposed services. Learning how to interpret ICMP messages helps cybersecurity professionals spot early signs of scanning, misconfiguration, or intentional evasion.

Wireshark Observation Table: Suspicious Behaviors & Display Filters

Observation / Potential Threat	Wireshark Display Filter
TCP retransmissions (DoS, congestion, MITM)	tcp.analysis.retransmission
Fast retransmissions (network instability)	tcp.analysis.fast_retransmission
Spurious retransmissions (timing or duplication issue)	tcp.analysis.spurious_retransmission
TCP zero window (DoS / slow client response)	tcp.analysis.zero_window
TCP resets (abrupt termination, possible scan evasion)	tcp.flags.reset == 1
Unusual TCP port usage (scan/recon attempts)	tcp.port == 0 or check uncommon ports like tcp.port == 6667
Cleartext HTTP (data leakage risk)	http

Observation / Potential Threat	Wireshark Display Filter
Suspicious User-Agent in HTTP header (malware/beacons)	http.user_agent contains "curl" or "bot"
Repeated DNS queries (tunneling or tracking)	dns and sort by dns.qry.name
Long DNS names or uncommon subdomains (exfiltration via tunneling)	dns.qry.name contains "-" or dns.qry.name matches ".{50,}"
CNAME chains (potential tracker masking)	dns and inspect dns.cname fields
TXT records in DNS (may carry embedded data)	dns.qry.type == 16
AAAA (IPv6) queries (rarely used, used in evasion sometimes)	dns.qry.type == 28
ICMP unreachable messages (port scanning or misconfigurations)	icmp.type == 3
ICMP Echo requests (pings, possibly scanning)	icmp.type == 8
ICMP Flood (DoS/scan evasion)	icmp and high frequency or same source
TLS handshake failures (MITM, expired certs)	tls.alert_message_level == 2
TLS without SNI (Server Name Indication)	tls.handshake.extensions_server_name == ""
Multiple SSL sessions without proper close (possible C2 channel)	ssl.record.version and lack of ssl.alert_message
DHCP activity from unauthorized clients	bootp
ARP spoofing or poisoning attempts	arp.duplicate-address-frame or arp with multiple MACs for 1 IP
Malformed packets (potential exploit attempts)	malformed
SMB traffic (lateral movement, ransomware)	smb or smb2
Unusual SMB shares being accessed	smb.file contains "admin" or "C\$"
NBNS (NetBIOS) name queries (older recon technique)	nbns
Unencrypted credentials (e.g., FTP, Telnet)	ftp.request.command == "PASS" or telnet
Traffic to known blacklisted IPs	Use a custom IP list or filter like ip.addr == 1.2.3.4

OSSEC-WUI Limitations and CLI Use with Wazuh-Control

The OSSEC Web User Interface (WUI) is no longer reliably operational due to the outdated nature of its PHP codebase. In particular, modern PHP interpreters generate compatibility issues with syntax involving `{}` and `[]`, leading to rendering failures or broken functionality.

As a result, we manage OSSEC/Wazuh entirely via the command line using the wazuh-control interface, which is robust, scriptable, and compatible with modern deployments.

Clean Reinstallation of OSSEC/Wazuh Manager (CLI-Based)

Step 1: Remove Previous Installation

```
sudo systemctl stop wazuh-manager  
sudo apt-get remove --purge wazuh-manager  
sudo rm -rf /var/ossec /etc/ossec-init.conf /var/log/ossec.log
```

Step 2: Install Wazuh Manager


```
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | sudo apt-key add  
-  
echo "deb https://packages.wazuh.com/4.x/apt/ stable main" | sudo tee  
    /etc/apt/sources.list.d/wazuh.list  
sudo apt-get update  
sudo apt-get install wazuh-manager  
sudo systemctl enable --now wazuh-manager
```

Step 3: Verify Manager CLI Access


```
/var/ossec/bin/wazuh-control status  
/var/ossec/bin/wazuh-control restart
```

Triggered Alerts from System Commands

These alerts are automatically triggered by OSSEC/Wazuh when executing system-level commands.

 Triggering Command: `sudo useradd testuser`

```
** Alert 1747208424.8449: - syslog,adduser,...
2025 May 14 10:40:24 slavdas-QEMU-Virtual-Machine->journald
Rule: 5902 (level 8) -> 'New user added to the system.'
User: testuser
May 14 07:40:23 ... useradd[103632]: new user: name=testuser; UID=1001,
...
uid: 1001
gid: 1001
home: /home/testuser
shell: /bin/sh
```

 Triggering Command: `sudo touch /etc/passwd`

```
** Alert 1747208424.9080: - pam,syslog,...
2025 May 14 10:40:24 slavdas-QEMU-Virtual-Machine->journald
Rule: 5502 (level 3) -> 'PAM: Login session closed.'
User: root
May 14 07:40:23 ... sudo[103630]: pam_unix(sudo:session): session closed
for user root
```

Understanding the Alert: Line-by-Line Breakdown

**** Alert 1747208424.8449: - syslog,adduser,...**

- Unique alert ID based on epoch timestamp.

- **Tags indicate source (`syslog`), action (`adduser`), and compliance references.**

For example:

- PCI-DSS 10.2.7 → Detect user creation
 - GDPR IV.35.7.d → Record of security events
 - HIPAA 164.312 → Access control events
- This mapping is **automatic** and helps in compliance audits.

2025 May 14 10:40:24 slavdas-QEMU-Virtual-Machine->journald

- Timestamp and host that generated the log.
- The log source (`journald`) is the systemd journal.

Rule: 5902 (level 8) -> 'New user added to the system.'

- Internal OSSEC rule ID and its severity level.
- Severity 8 is medium-high and reflects potential risk. (Severity level (1–15 scale).)

User: testuser

- Shows the user that was added. Extracted by Wazuh.

May 14 07:40:23 ... useradd[103632]: new user: ...

- Raw log showing command, user info, UID, GID, shell, and session source.

Parsed Fields (uid, gid, home, shell)

- Wazuh extracts these for visualization and filtering.