MIS 535 NETWORK AND SECURITY MANAGEMENT

PROJECT REPORT

Topic: Create a detailed "how-to" guide for using a network analysis tool like Wireshark or Security Onion to investigate and solve problems like rogue users/applications on a LAN or identify an illicit cryptocoin miner app running on computers on a network. Create an accompanying 10-15 minute video demo illustrating the steps from your how-to guide

BY

TEAM-4

Suvarna Donthamsetty

Sudha Rani Seeli

Manisha Vajhala

Archana Kanuri

INDEX

Objective

To investigate and solve network issues, including identifying rogue users/applications on a LAN and detecting illicit crypto mining activities using Wireshark.

Introduction to Wireshark

Wireshark is a powerful, open-source network protocol analyzer widely used for network troubleshooting, analysis, and security investigations. It captures and examines packets traversing a network in real time, providing granular visibility into network behavior. With its user-friendly interface and robust filtering options, Wireshark enables IT professionals, security analysts, and network engineers to dissect data for diagnosing issues or detecting anomalies.

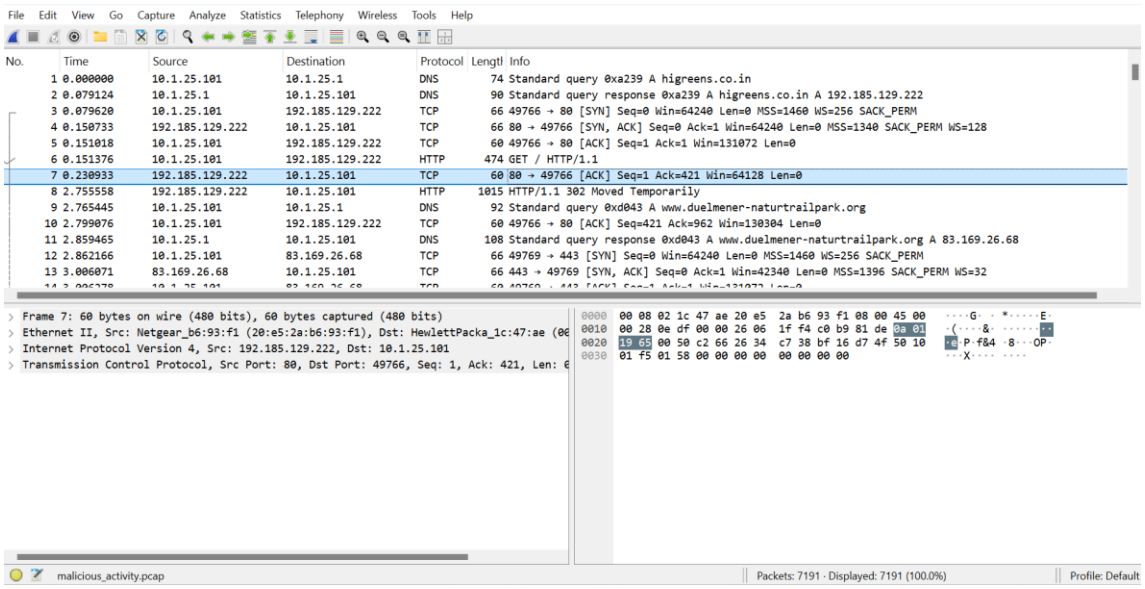
Why Choose Wireshark for This Project?

For this project, Wireshark was selected due to its unparalleled capabilities in network analysis and troubleshooting. Here's why it stands out:

1. **Comprehensive Protocol Support**: Wireshark supports thousands of network protocols, enabling thorough analysis of traffic across various layers.
2. **Real-Time Packet Capture**: The ability to capture packets in real time allows for immediate investigation of rogue users, unauthorized applications, or malicious activity.
3. **Advanced Filtering Options**: Wireshark's robust filtering syntax helps isolate suspicious traffic, such as illicit crypto mining or unauthorized DNS queries, making it ideal for targeted investigations.
4. **Visualization Tools**: Features like packet flow graphs and expert information summaries provide a clear representation of network traffic and potential issues.
5. **Free and Open Source**: Wireshark is accessible without licensing costs, making it a cost-effective tool for educational and professional purposes.
6. **Trusted by Professionals**: It's a widely trusted tool in the cybersecurity and networking domains, ensuring reliability for critical investigations.

Downloading the Sample Capture File

- **Source**: The sample capture file was obtained from Wireshark Sample Captures. This repository provides a variety of pre-captured network traffic files, ideal for testing and analysis.
- **Reason**: Using a sample capture file ensures access to diverse traffic scenarios, including DNS queries, TCP connections, and potential malicious activities, which simulate real-world conditions for this project.



The above pictures shows the data after loading it into the WireShark.

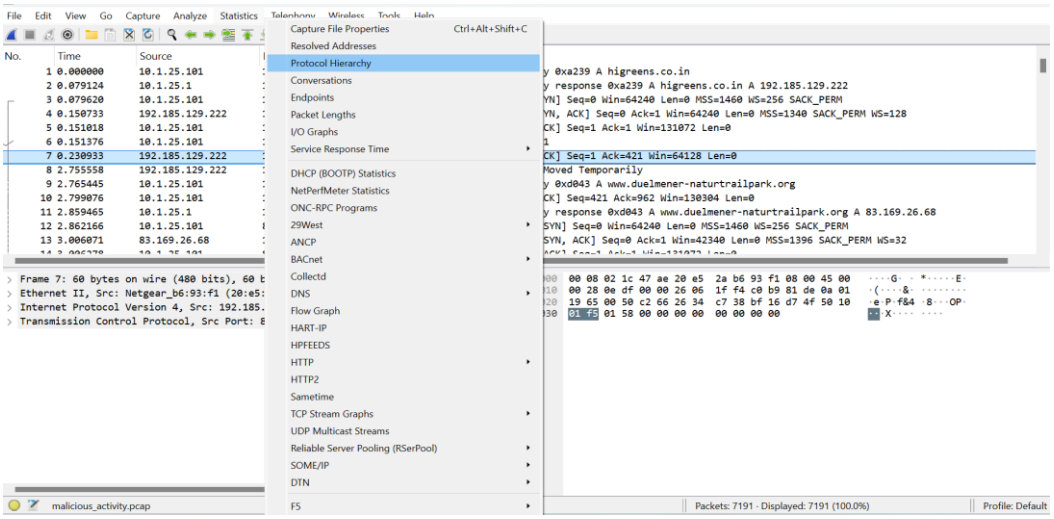
HTTP Analysis

The Hypertext Transfer Protocol (HTTP) is one of the most widely used protocols on the internet, facilitating communication between clients (e.g., web browsers) and servers. While it plays a vital role in legitimate web traffic, HTTP can also be exploited for malicious purposes, such as delivering malware, unauthorized file downloads, or exfiltrating sensitive data.

Analyzing HTTP traffic is critical for identifying threats like suspicious file transfers, unauthorized communications, and attempts to connect to malicious domains. By examining HTTP headers, methods (e.g., GET, POST), and content, investigators can uncover rogue activities and understand the nature of traffic within a network. This analysis provides insights into the behavior of both users and potential attackers, making it an essential component of network security monitoring.

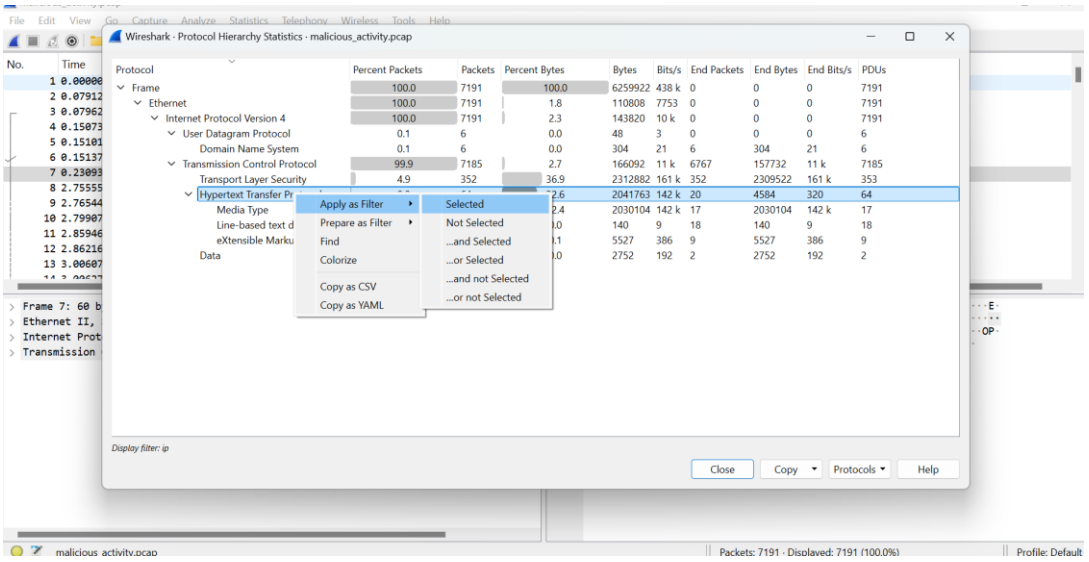
After opening the .pcap file in Wireshark, navigate to Statistics > Protocol Hierarchy.

Purpose: This step breaks down the captured packets by protocol, displaying the distribution of packets for protocols like Ethernet, TCP, UDP, HTTP, etc.



In the Protocol Hierarchy window, select the HTTP protocol and right-click to choose Apply as Filter > Selected.

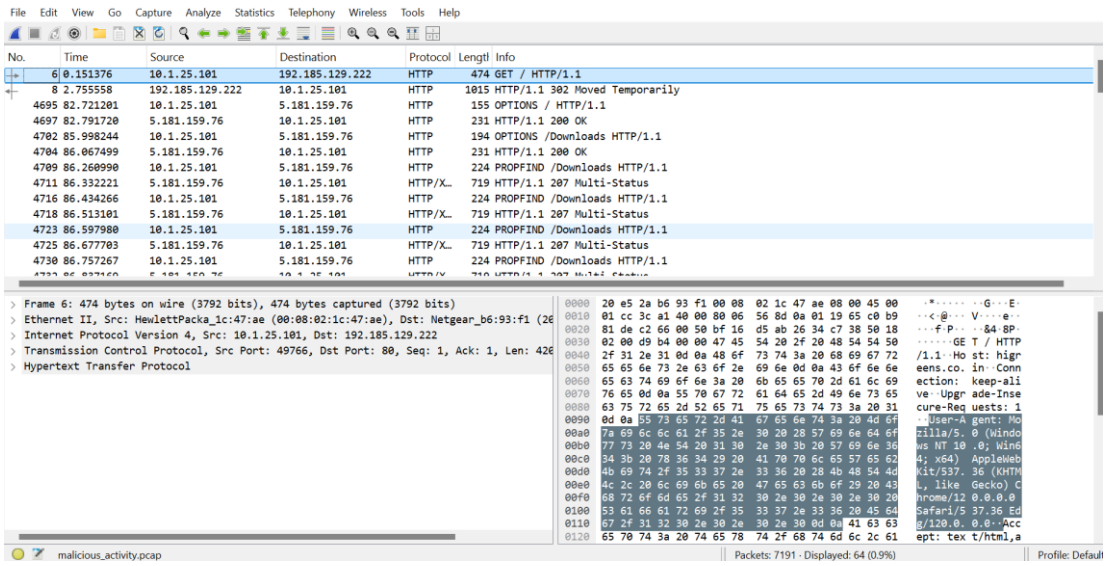
Purpose: This filter isolates HTTP traffic from the entire capture, allowing a detailed examination of web requests and responses.



Protocol Hierarchy Statics

View the filtered HTTP packets in the main interface. Key fields, such as Source, Destination, Protocol, and Info, are used to identify potential anomalies in HTTP requests.

Observation: Packets displayed include common HTTP methods like GET, POST, OPTIONS, or specific URLs that might indicate malicious downloads or communications.



After Selecting HTTP Filter

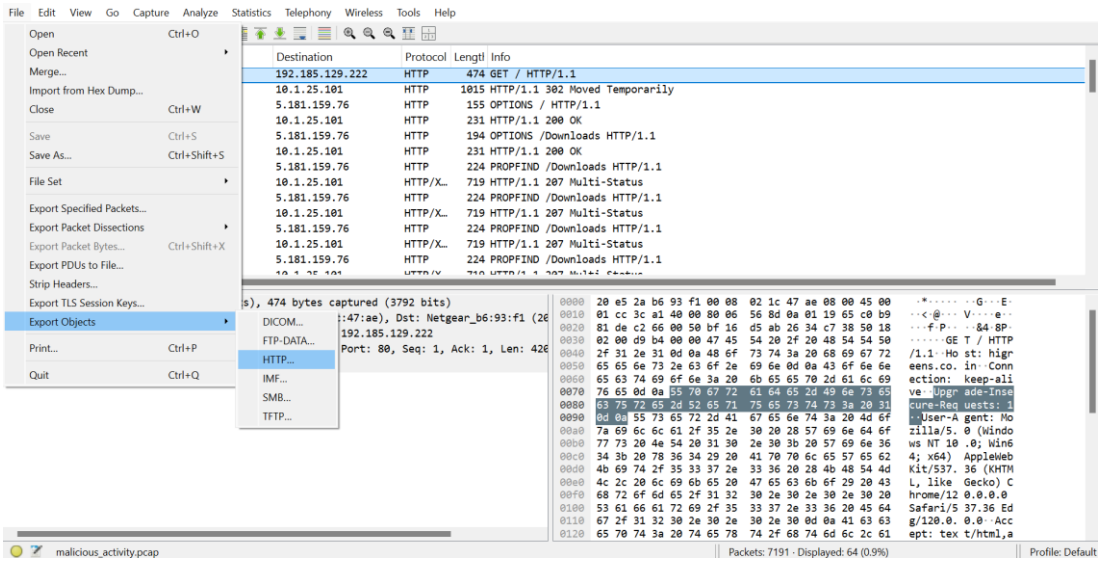
Navigate to File > Export Objects > HTTP to open the HTTP object list.

This list displays details like:

- **Hostname**: The server hosting the requested resource.

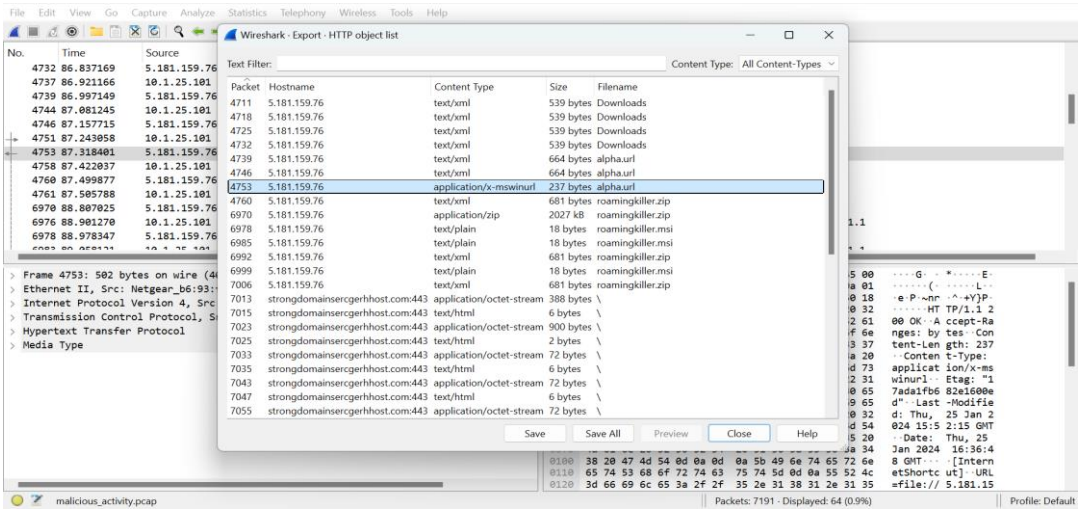
- **Content Type**: The MIME type of the response, e.g., text/html, application/octet-stream.
- **Size**: The size of the HTTP response.
- **Filename**: Names of the objects retrieved via HTTP.

Select potentially malicious objects (e.g., unusual .exe, .zip, .msi files) and save them for further analysis.



Exporting HTTP Objects

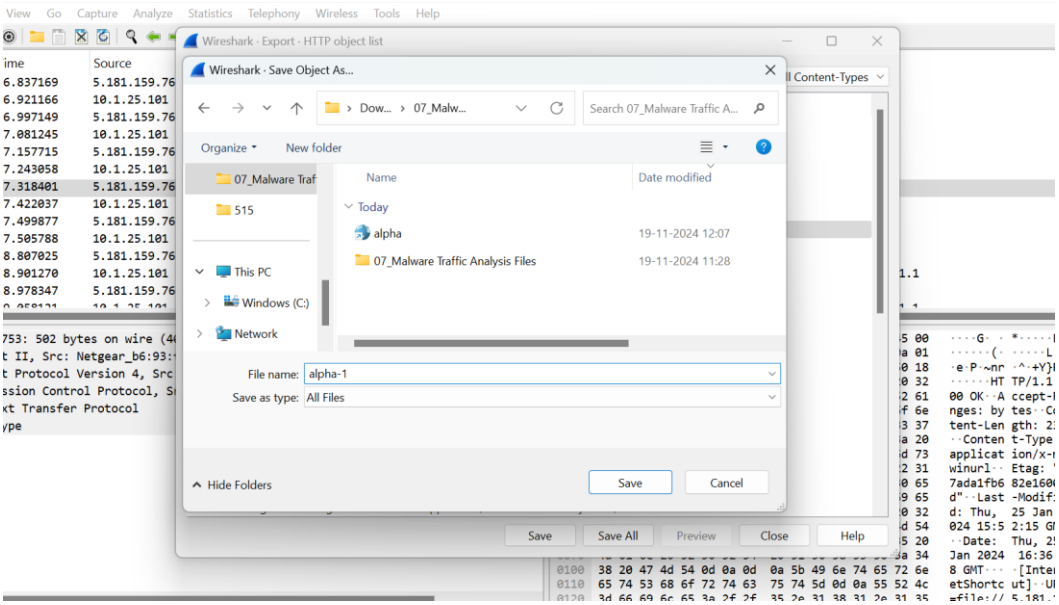
During the HTTP analysis in Wireshark, specific files, such as roamingkiller.zip and alpha-url, stood out due to their suspicious characteristics, including unusual file names, MIME types like application/x-mswinurl, and origin from untrusted domains such as strongdomainsercerghost.com. These indicators suggested potential rogue applications or malware on the network. To confirm their nature, these files were downloaded and analyzed further. The goal was to validate whether they posed a security threat, such as being part of a malicious payload or unauthorized software. By exporting these files from Wireshark and submitting them to VirusTotal, a comprehensive threat analysis was performed, providing insights into the files' risks and guiding appropriate mitigation steps.



Objects in HTTP

The saved file is uploaded to an online malware scanning platform, such as VirusTotal.

Purpose: To verify whether the downloaded files contain malicious content by cross-referencing them with threat databases.



Downloading Files

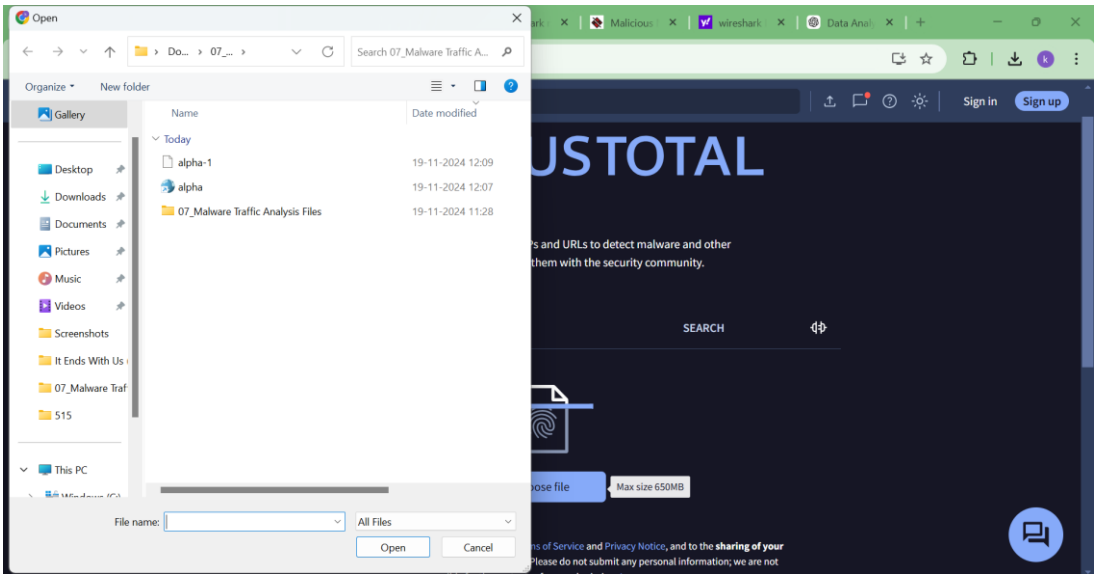
To confirm the suspicion of malicious intent and verify the safety of these files, We uploaded them to VirusTotal, an online malware scanning platform. VirusTotal aggregates results from multiple antivirus engines, offering a comprehensive threat analysis.

Screenshot of VirusTotal Home Page

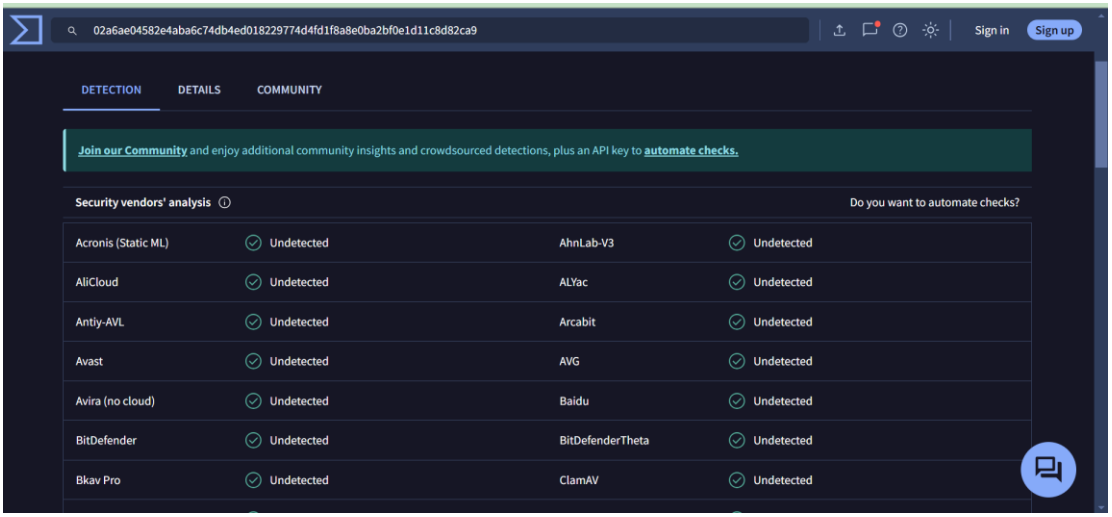
Steps Taken in VirusTotal Analysis

1. **File Upload**:
    - The files roamingkiller.zip and alpha-url were exported from Wireshark using the Export Objects > HTTP feature.
    - These files were saved locally and uploaded to VirusTotal for analysis.

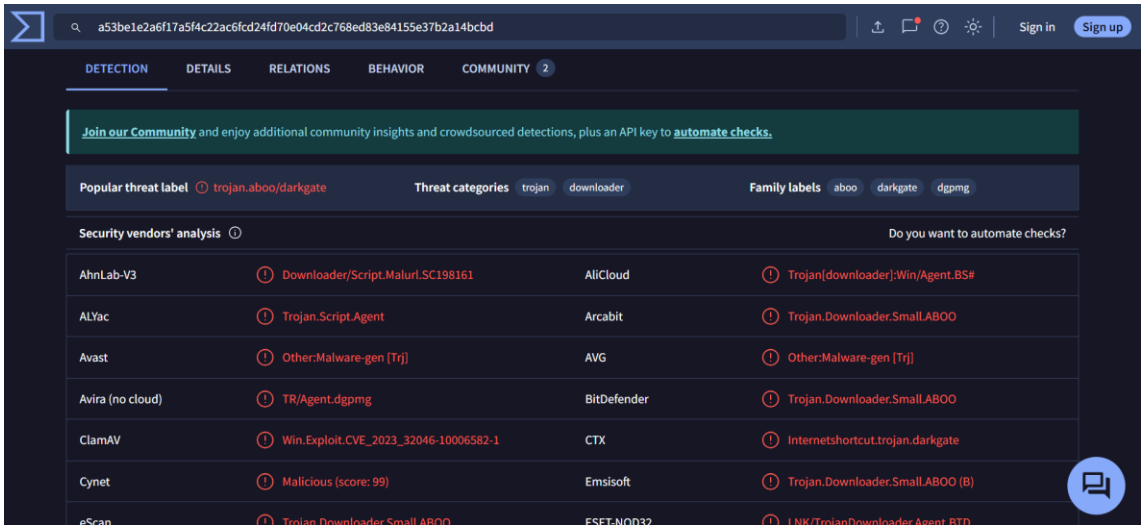
2. **Threat Analysis**:
    - VirusTotal scanned the files against multiple antivirus databases to identify:
        - Known malware.
        - Suspicious behaviors, such as data exfiltration or unauthorized execution.
    - It flagged several files with high-risk labels such as Trojan.Downloader, confirming the files' malicious nature.
3. **Results Obtained**:
    - The files were identified as harmful, containing trojans or other malware designed for unauthorized activities like downloading further payloads or compromising network systems.



Uploading File to VirusTotal



Result of Uploaded Files



Result of File Containing Rouge Applicants

Purpose of This Investigation

The decision to download and analyze these files aimed to:

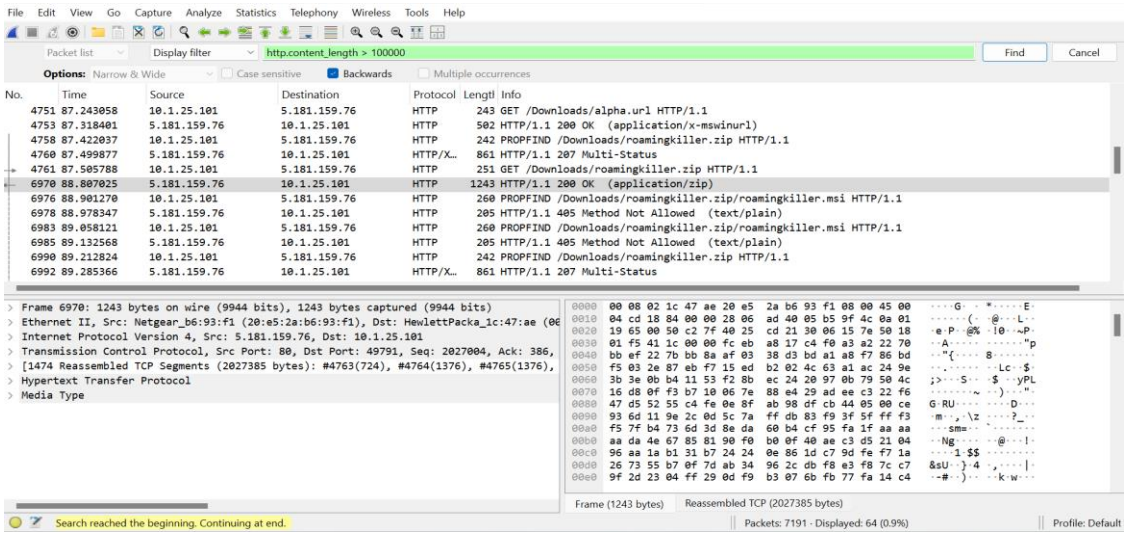
- Validate the presence of rogue applications on the network.
- Confirm their malicious nature using VirusTotal to justify further actions like blocking the source domains or removing the files from infected systems.

Analysing HTTP file with Filter:

Filter Used: http.content_length > 100000

Purpose: This filter isolates HTTP responses with content lengths greater than 100,000 bytes, focusing on large files such as executables or compressed archives that may indicate rogue software or malicious downloads.

Observation: Files like roamingkiller.zip were identified with a content length exceeding the threshold, aligning with the criteria for further scrutiny.



Applying Filter to HTTP File

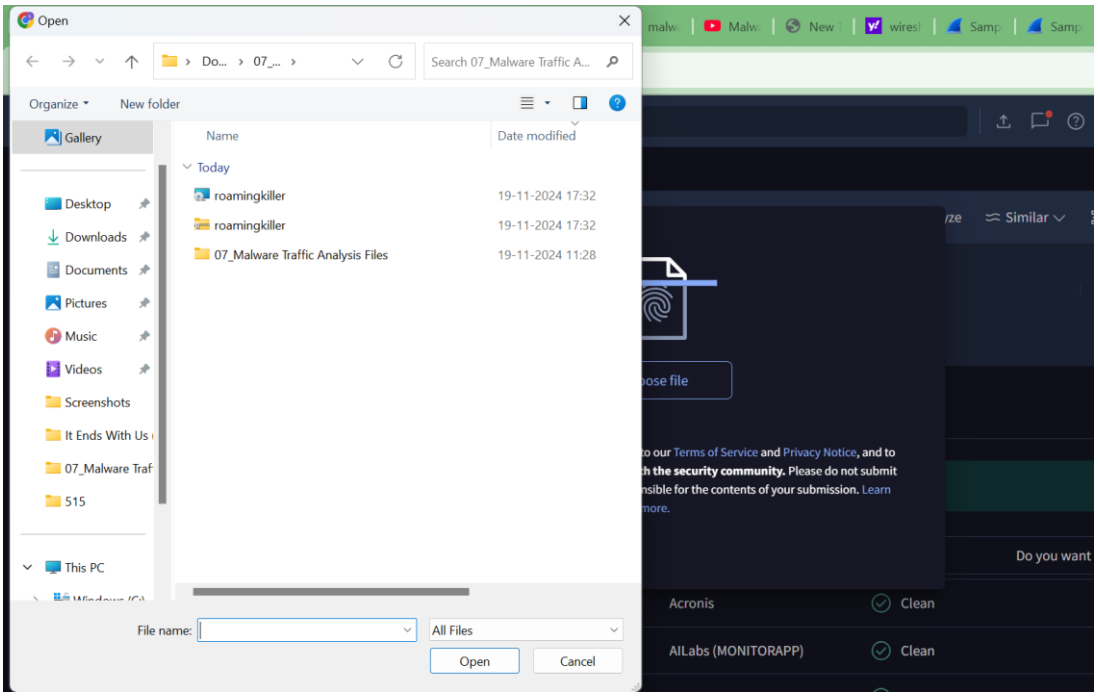
Files identified through the content-length filter were cross-referenced in the HTTP Object List for additional details, including:

- **Source Hostname**: Highlighting domains serving large suspicious files.
- **Content Type**: Revealing file formats like application/zip or application/octet-stream that could signify malicious content.

Files like roamingkiller.zip were flagged and exported for analysis.

In the Next Step The files extracted using the HTTP filter were uploaded to VirusTotal for verification:

- **File 1**: roamingkiller.zip
    - Flagged as malicious by 39/64 antivirus engines.
    - Classified as a Trojan downloader, posing a significant security risk.
- **File 2**: Chrome cache entry (text file).
    - No threats detected, confirming its benign nature.



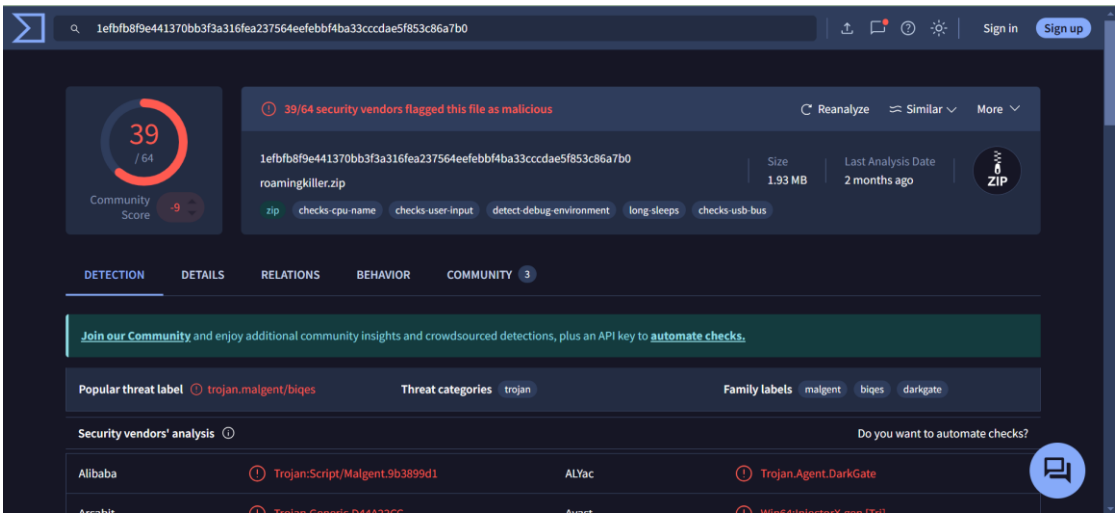
Uploading Files to VirusTotal

Threat Assessment:

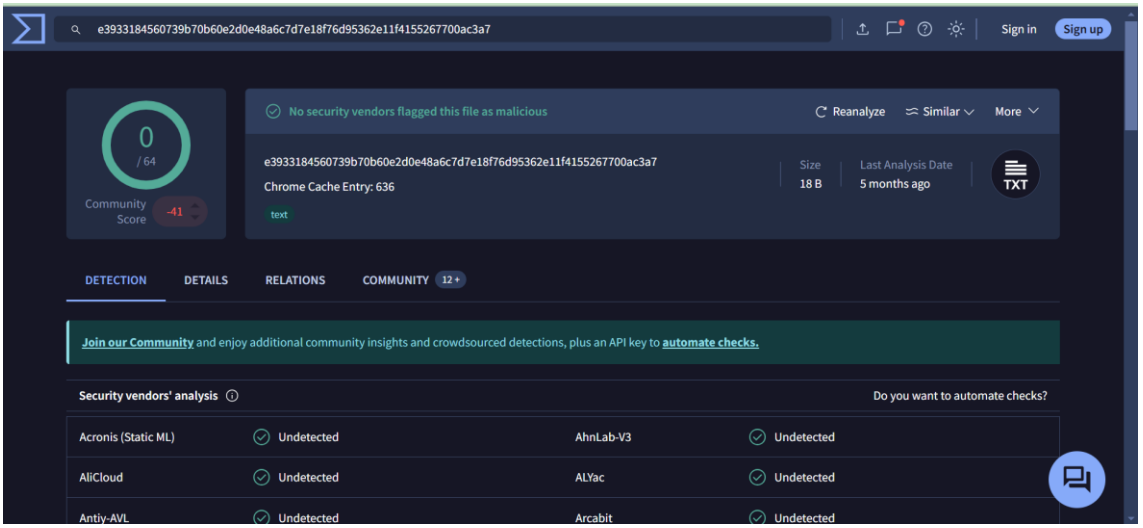
- Files flagged by VirusTotal, such as roamingkiller.zip, provided clear evidence of malicious activity on the network.
- The benign status of smaller files (e.g., cache entries) validated the efficiency of the filtering process.

Host Relevance:

- Domains hosting flagged files were noted for potential blocking or inclusion in network monitoring policies.



Result of Rouge Applicant File in VirusTotal



Result of File with no rouge applicants

Analysis of TCP

Transmission Control Protocol (TCP) is one of the core protocols of the internet, ensuring reliable communication between devices by establishing a connection, verifying data delivery, and managing retransmissions in case of packet loss. Analysing TCP traffic is critical for identifying unusual behaviour, such as unauthorized access, rogue applications, or malicious activities, as it often serves as the foundation for many application-layer protocols (e.g., HTTP, FTP).

In this project, TCP analysis focused on inspecting connection patterns, identifying suspicious ports, and analysing TCP flags to detect anomalies that could indicate potential security threats, such as unauthorized services or data exfiltration. By leveraging Wireshark's robust

filtering capabilities, we were able to narrow down specific TCP traffic for detailed examination and threat detection.

1) Filter by port to identify suspicious services:
Filtering by Specific Ports

- **Filter Used**: tcp.port == 4444
- **Purpose**: Port 4444 is commonly associated with mining tools like NiceHash and other malicious activities. Applying this filter helped isolate traffic potentially linked to rogue or unauthorized applications.
- **Observation**: No traffic matched the filter criteria for port 4444 in this case. This indicated no active communication or services running on this port.

Source and Destination Inspection

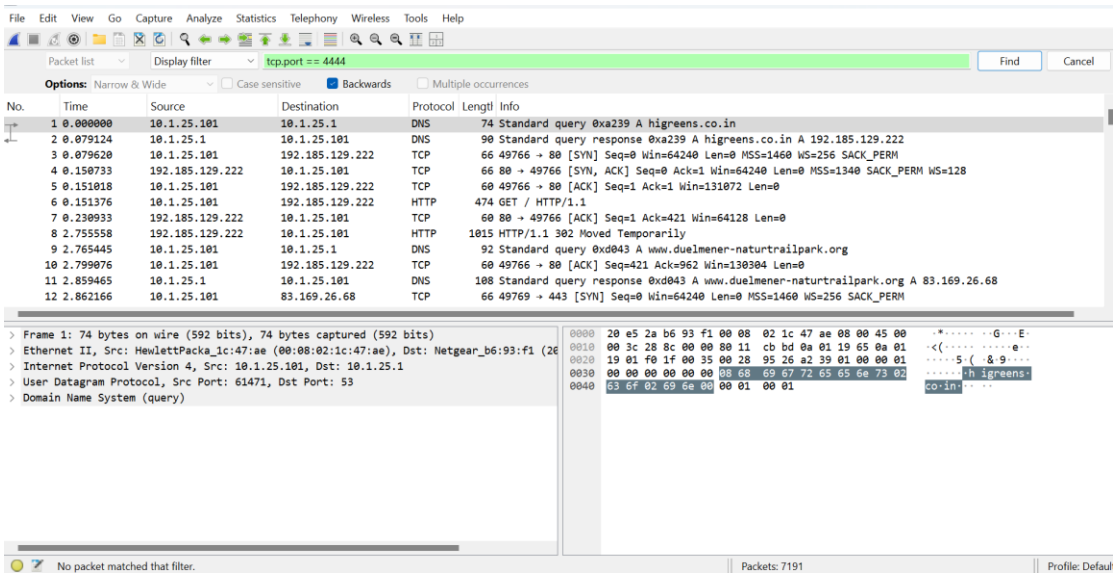
- **Focus**: Examined the source (10.1.25.101) and destination IPs in the packet list.
- **Verification**: The source IP (10.1.25.101) was cross-checked in VirusTotal to determine its reputation. The analysis revealed the IP address to be clean and private, with no malicious activity flagged.

TCP Flags Analysis

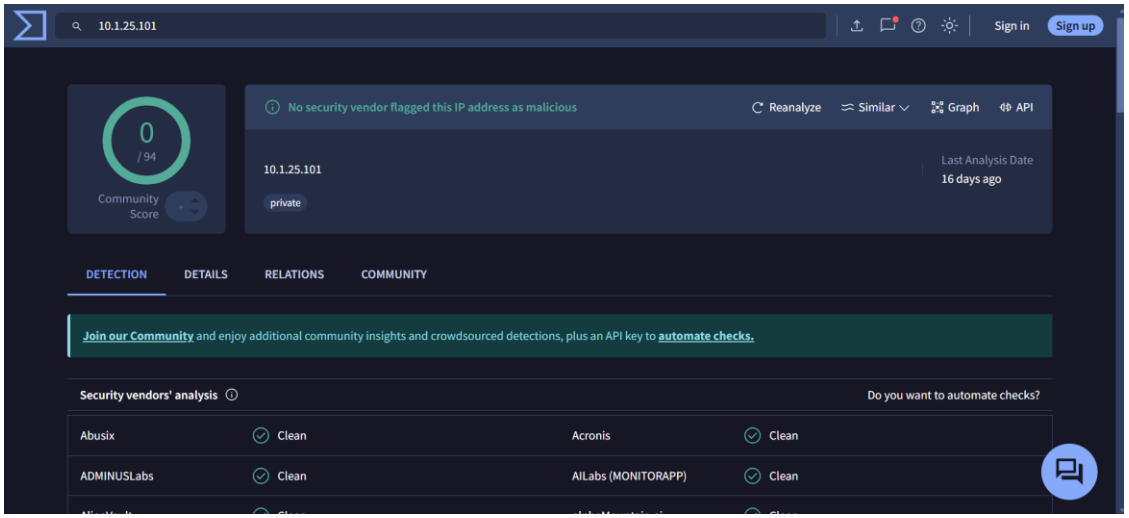
- **Purpose**: To check connection states and session initiation. SYN, ACK, and other TCP flag combinations were reviewed to detect anomalous or persistent connections that might indicate unauthorized access.

Result

- The absence of traffic on port 4444 suggested no mining or rogue activity tied to this specific port.
- Validation of the source IP (10.1.25.101) confirmed it as benign, reducing suspicion of its involvement in malicious activities.



Applying TCP Filers



Result of IP Address with no rouge applicants

Filtering Specific Ports

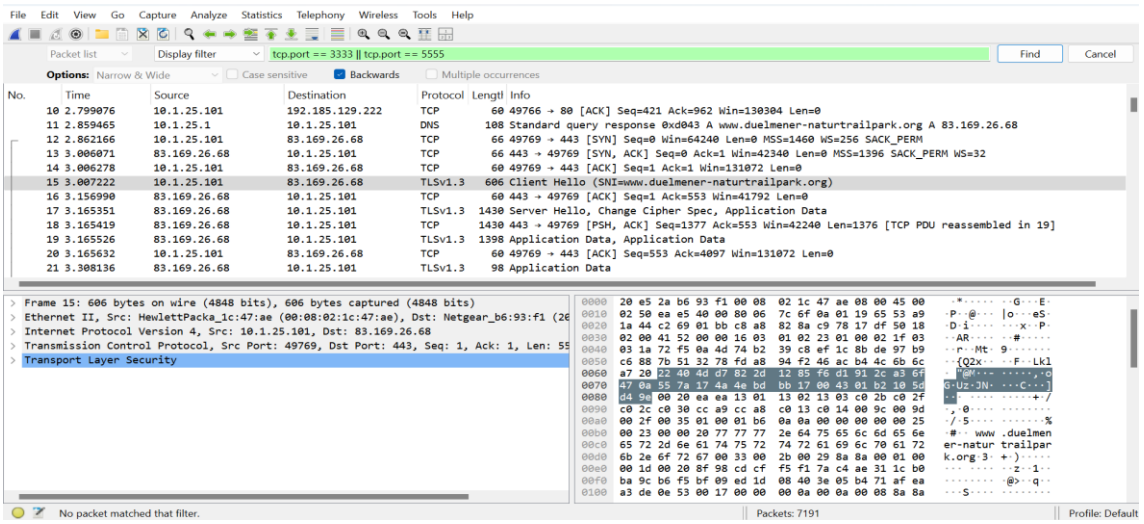
- **Filter Used**: tcp.port == 3333 || tcp.port == 5555
- **Purpose**: To identify traffic on ports often utilized by mining software or other malicious services.
- **Observation**: No packets matched this filter in the capture, indicating no active communications on these ports during the analyzed timeframe.

Cross-Referencing IP Addresses

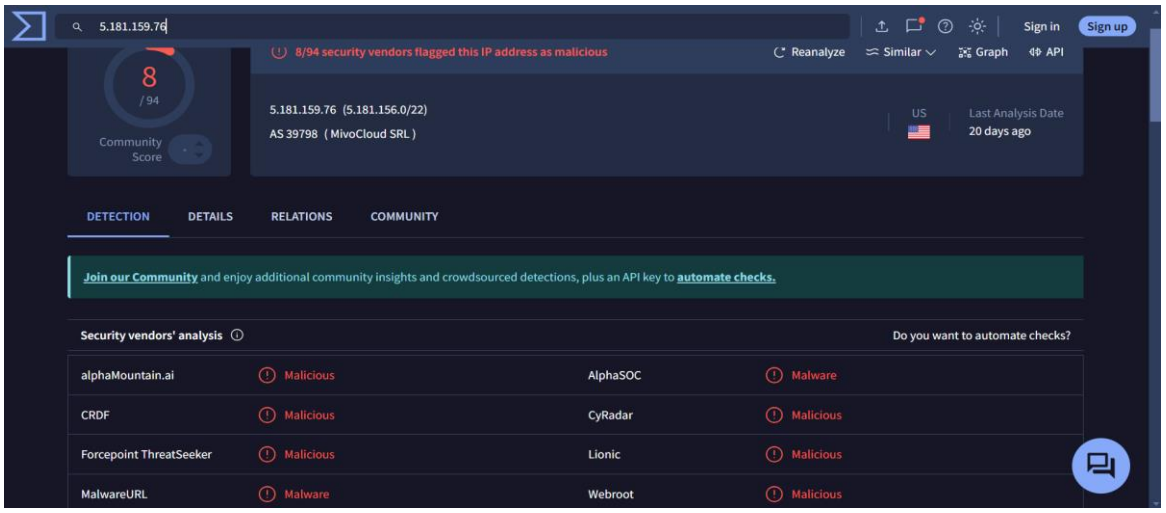
- **IP of Interest**: 5.181.159.76
    - This IP appeared frequently in TCP communications.
- **Validation with VirusTotal**:
    - **Result**: Flagged as malicious by 8/94 security vendors.
    - **Threat Details**: Associated with malware and suspicious activity, reinforcing the likelihood of unauthorized behavior originating from or involving this IP.

Conversation Analysis

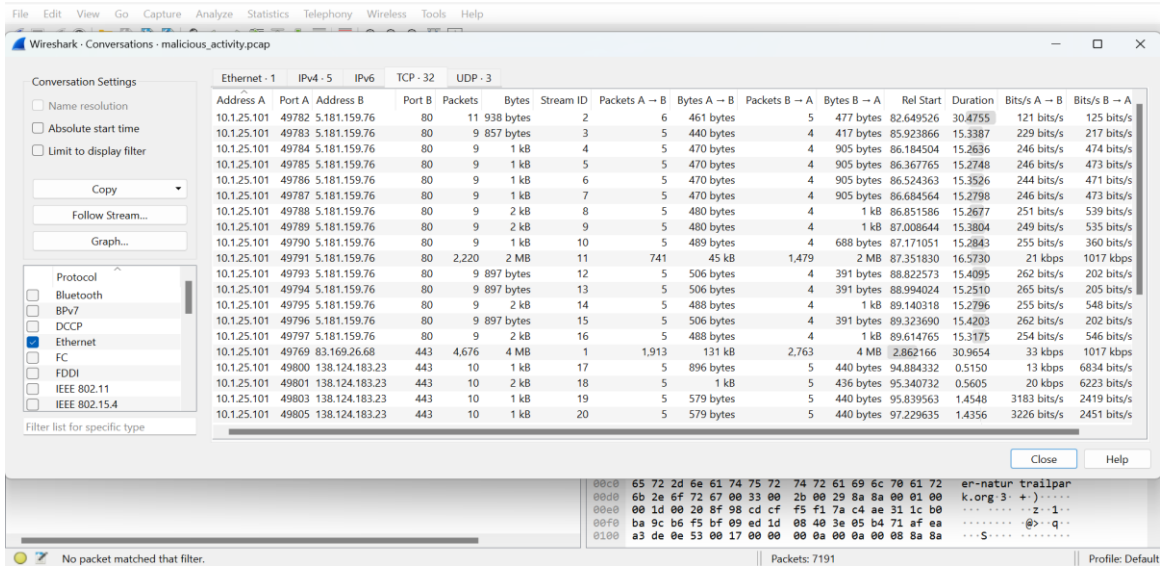
- **Wireshark Tool**: Statistics > Conversations
- **Purpose**: To get an overview of all TCP connections and assess the volume of data exchanged between IP addresses.
- **Key Findings**:
    - The connection between 10.1.25.101 and 5.181.159.76 was among the most active, with significant data transfer (over 2,220 packets and 1.4 MB).
    - These metrics suggest a potential unauthorized data exchange or malicious payload delivery.



Applying TCP Filter



Result of IP Address with rouge applicants



Conversations of detected File

2) Applying TCP Flags Filter

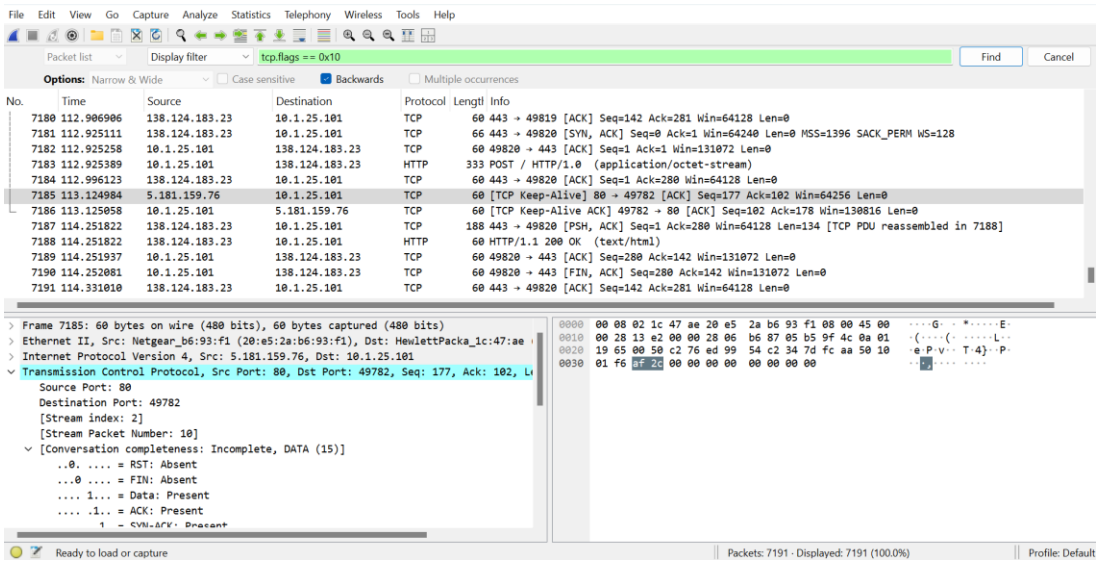
- **Filter Used**: **tcp.flags == 0x10**
- **Purpose**: This filter isolates packets with the ACK (Acknowledgment) flag, which is set after establishing a successful connection. Monitoring ACK packets can help detect active sessions or unusual persistent connections.
- **Observation**:
    - Connections to suspicious IPs, such as 5.181.159.76, were highlighted, revealing regular data exchanges.

Reviewing Conversations

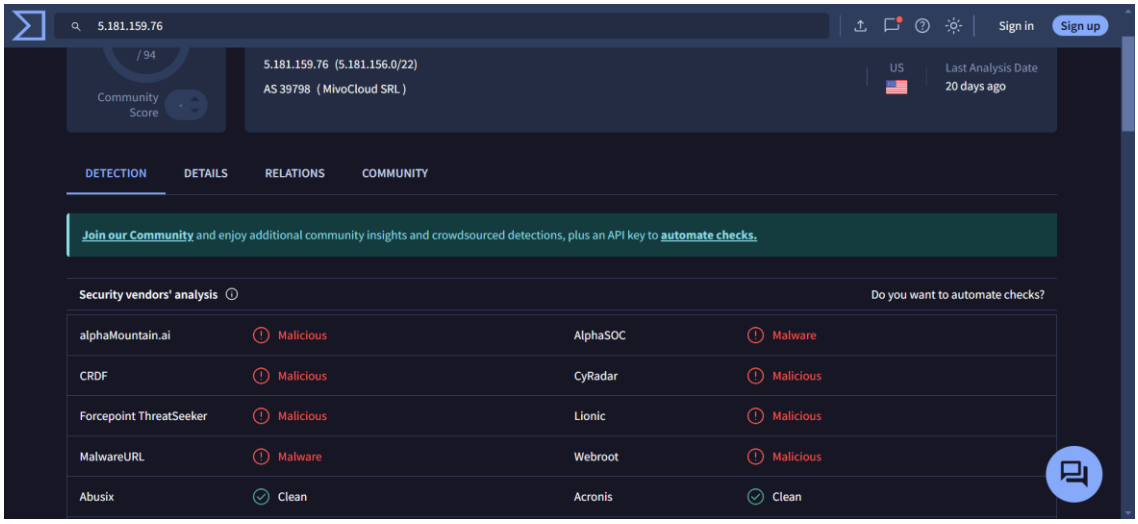
- Used Statistics > Conversations to analyze the total packets, bytes exchanged, and session duration.
- **Key Findings**:
    - A high-volume data exchange was observed between 10.1.25.101 and 5.181.159.76 over an extended duration.
    - The connection involved a substantial number of ACK packets, indicating continuous data acknowledgment and suggesting potential unauthorized data transfer.

IP Reputation Check

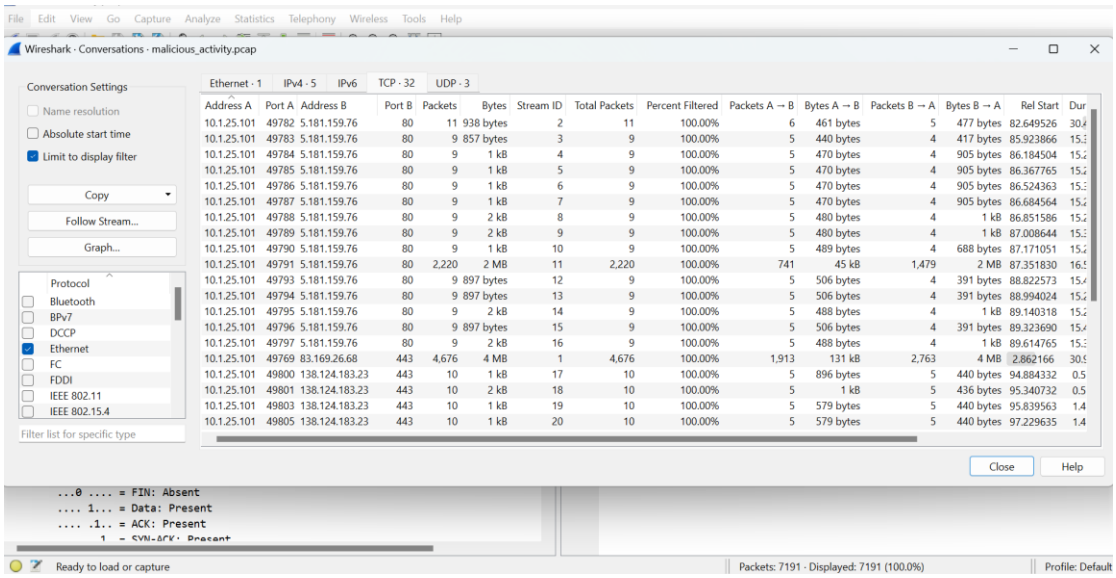
- The IP 5.181.159.76 was cross-referenced in VirusTotal.
- **Result**:
    - Flagged as malicious by multiple antivirus engines.
    - Associated with malware and suspicious activities, confirming the need for further investigation.



Applying Filter



Result of IP address



Conversation of detected File

3) Applying Stratum Filter

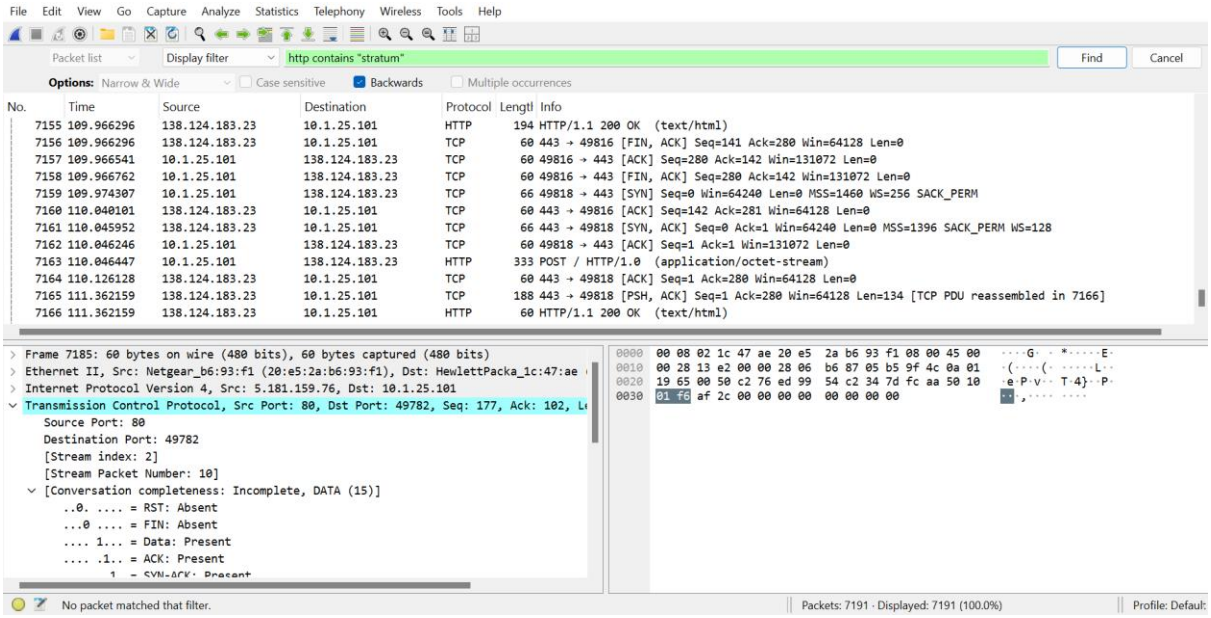
- **Filter Used**: http contains "stratum"
- **Purpose**: To filter HTTP traffic containing the keyword "stratum," which is often used in mining-related communications.
- **Observation**:
    - No packets matched the filter in this capture file. This indicates no direct evidence of mining activity using the Stratum protocol over HTTP.

Examining Related Connections

- Despite no hits on "stratum," related HTTP traffic, such as files or endpoints that could indirectly suggest mining activity, were analyzed for patterns. Other suspicious IP addresses, such as 5.181.159.76, were further investigated due to their malicious reputation.

Cross-Checking Mining Indicators

- Connections to mining pools often display characteristics such as:
    - Persistent and repetitive data packets.
    - Regular ACK and PSH-ACK flag combinations to maintain a continuous session.
- No such consistent mining patterns were observed in this case.



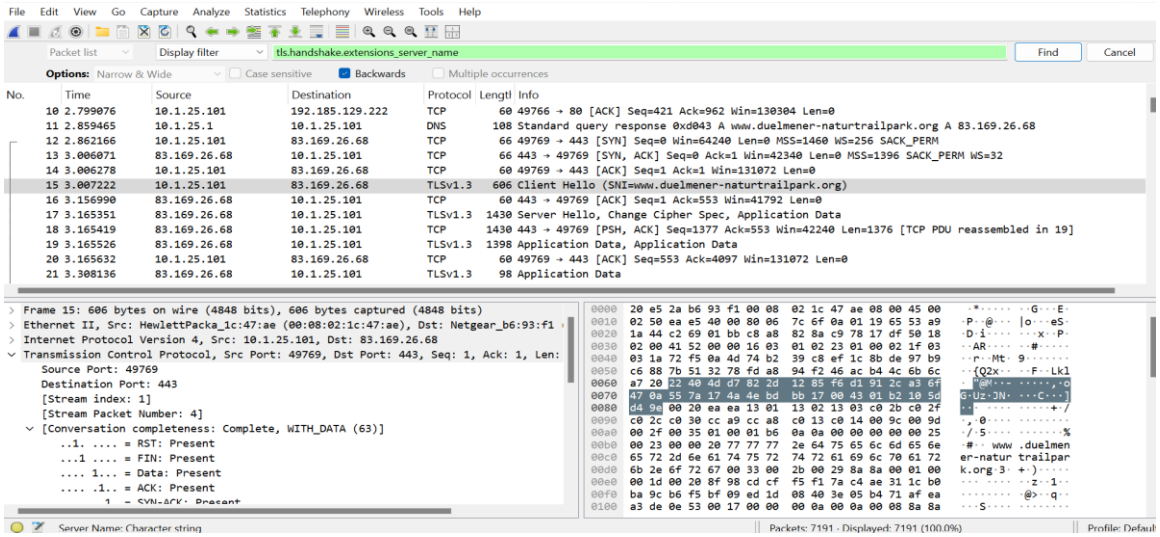
Applying Filter

Steps and Observations

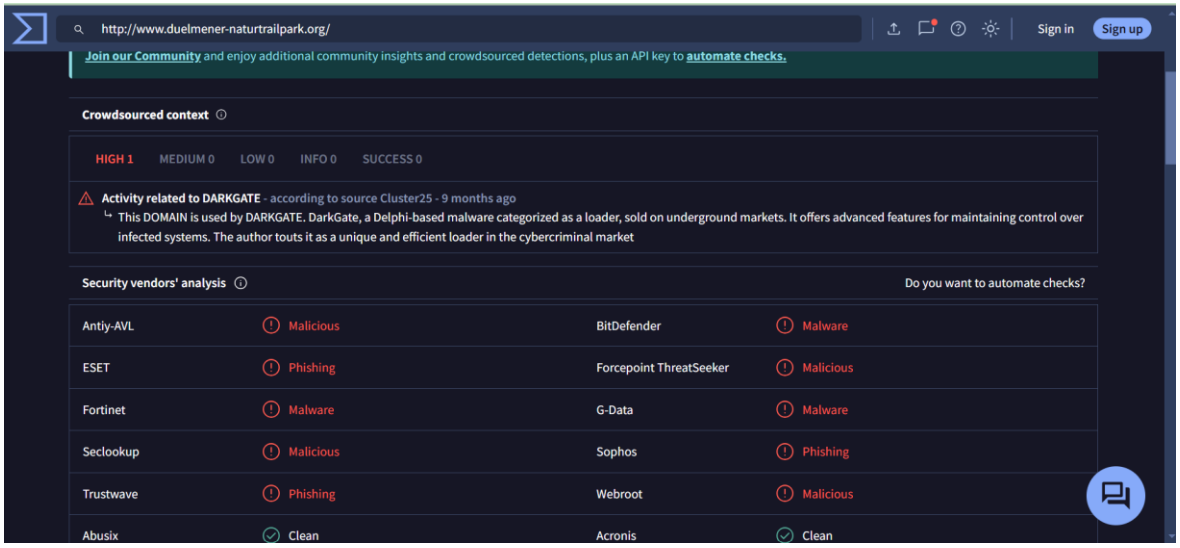
1. **TLS Handshake Analysis**
    - **Filter Applied**: tls.handshake.extensions_server_name
    - **Purpose**: To identify the hostname (SNI) during TLS handshake for domain tracking.
    - **Observation**:
        - The server name www.duelmen-naturtrailpark.org was extracted during the handshake.
        - This domain appeared in multiple packets, showing active encrypted communication.
2. **Domain Reputation Check**
    - **Validation with VirusTotal**:
        - **Result**: Flagged as high-risk due to association with DARKGATE, a malware loader.
        - **Threat Indicators**:
            - Malicious activity including phishing and malware distribution.

- Advanced control mechanisms for attackers.

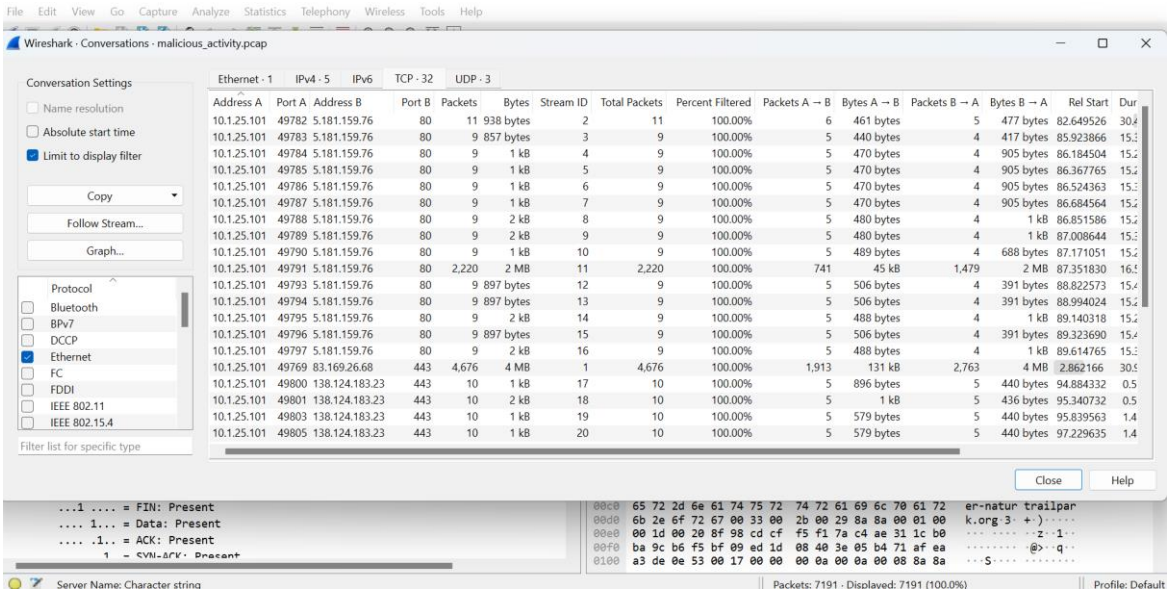
3. **Conversation Analysis**
    - **Tool Used**: Statistics > Conversations
    - **Findings**:
        - Persistent communication was observed between 10.1.25.101 (local IP) and IPs linked to the flagged domain.
        - Significant data transfer and continuous sessions indicate possible data exfiltration or control channel activity.
4. **Risk Assessment**
    - Encrypted traffic associated with this domain poses a high security risk, as encryption can be exploited to bypass traditional detection mechanisms.



Applying Filter



Result of uploaded link



Conversation of detected file

Analysing DNS

The Domain Name System (DNS) is a fundamental component of the internet, translating human-readable domain names into IP addresses required for communication. While critical for legitimate web activity, DNS can also be exploited for malicious purposes, such as data exfiltration, command-and-control (C2) communication, or redirecting users to phishing or malicious sites.

Analyzing DNS traffic is a vital step in network forensics, as it helps identify suspicious domain queries, unusual patterns, or unauthorized activity that may indicate security threats. By examining DNS queries, response times, and the nature of resolved domains, one can detect potential rogue users or malicious applications operating within the network. This analysis is especially effective in identifying early stages of attacks, such as malware communicating with its C2 server.

1) Filter Applied

- **Filter Used: dns.qry.name**
- **Purpose:** To isolate DNS query traffic, which reveals the domain names resolved by devices on the network.

Observation

- **Highlighted Query:**
    - The query strongdomainsercerghost.com was captured.
    - The domain resolved to the IP address 138.124.183.23, indicating an active DNS resolution.

Suspicion Indicators

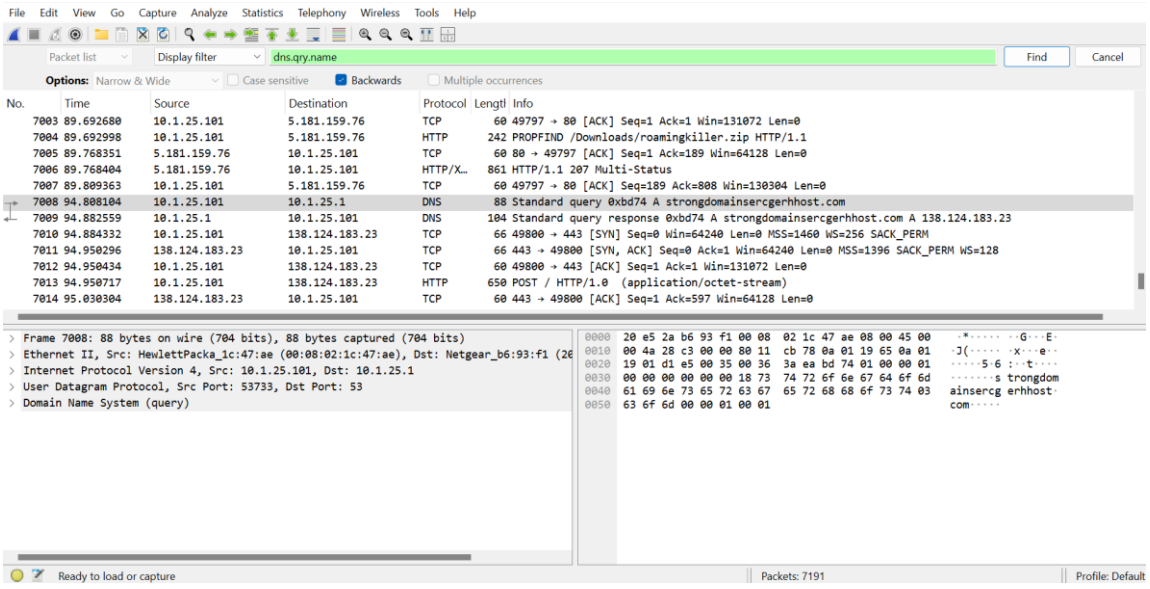
- **Domain Name:** The domain strongdomainsercerghost.com appears unusual and unrelated to typical business or user activities.
- **Potential Threat:** The naming pattern and lack of recognition in public databases suggest possible involvement in phishing, malware distribution, or C2 activities.

Cross-Referencing the Domain

- The domain was flagged for further validation using reputation tools like VirusTotal.
- Domains with ambiguous names often signify involvement in malicious campaigns.

Correlations in Traffic

- Examined subsequent traffic associated with the resolved IP address to identify patterns indicative of malicious activity.



Applying Filter

2) Filter Applied

- **Filter Used**: udp contains "fragmented"
- **Purpose**: To identify UDP packets containing the term "fragmented," which can signify attempts to bypass detection mechanisms or abuse protocols.

Observation

- No packets matched the applied filter, indicating no explicit signs of fragmented UDP traffic in this capture. However, other patterns of concern were identified in DNS traffic.

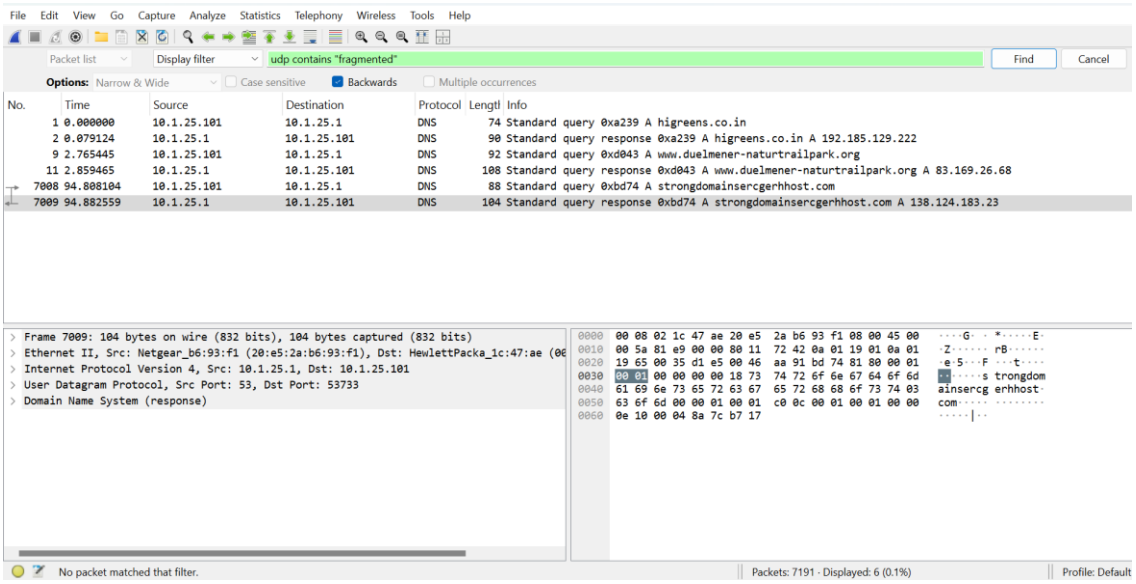
Correlations with DNS Queries

- DNS responses in the capture include domains such as:
    - strongdomainsercerghost.com resolving to IP 138.124.183.23.

- Such domains, combined with UDP activity, warrant further inspection for potential malicious behavior.

Potential Indicators

- While no fragmented packets were found, the presence of suspicious DNS responses suggests the need for additional checks, such as monitoring traffic volume and frequency to the resolved IP.



Applying Filter

3) Filter Applied

- **Filter Used**: dns.qry.name contains "malware" || dns.qry.name contains "mining"
- **Purpose**: To narrow down DNS traffic to domain queries containing the keywords "malware" or "mining," which are often associated with malicious activities or crypto mining operations.

Observation

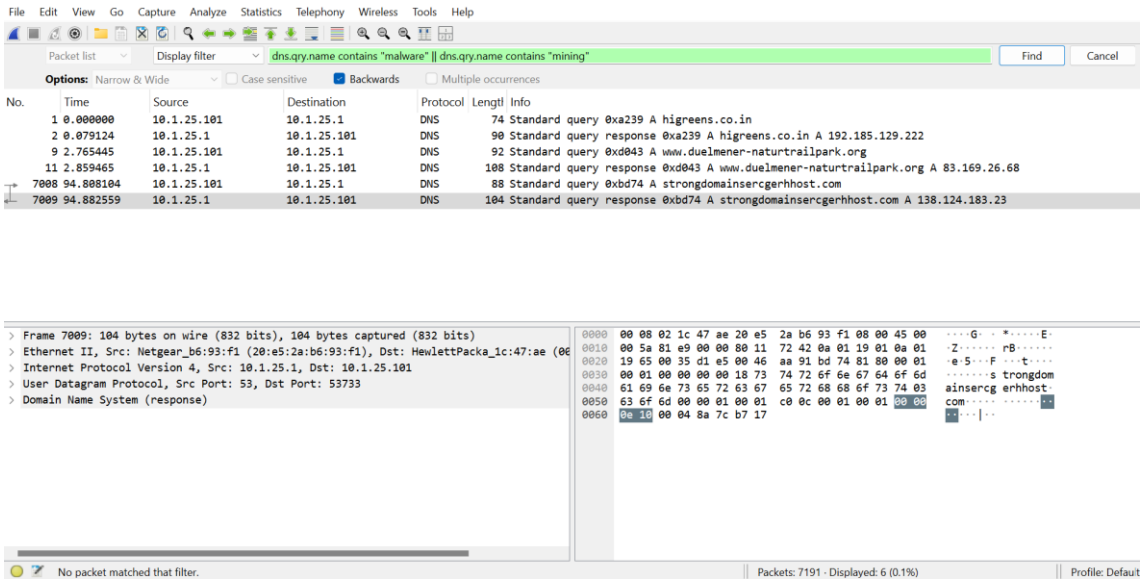
- **Result**: No packets matched the filter criteria in this capture, suggesting no direct evidence of queries to domains explicitly containing "malware" or "mining."

Contextual Findings

- While the applied filter did not yield results, other suspicious domains, such as strongdomainsercerghost.com, were observed in DNS traffic. Such domains, though not containing the keywords, may still pose a threat and warrant further analysis.

Additional Checks

- Cross-referenced domains like strongdomainsercerghost.com against reputation databases to assess potential malicious intent.
- Inspected related DNS responses and subsequent communication patterns for signs of unauthorized activity.



Applying Filter

4) Filter Applied

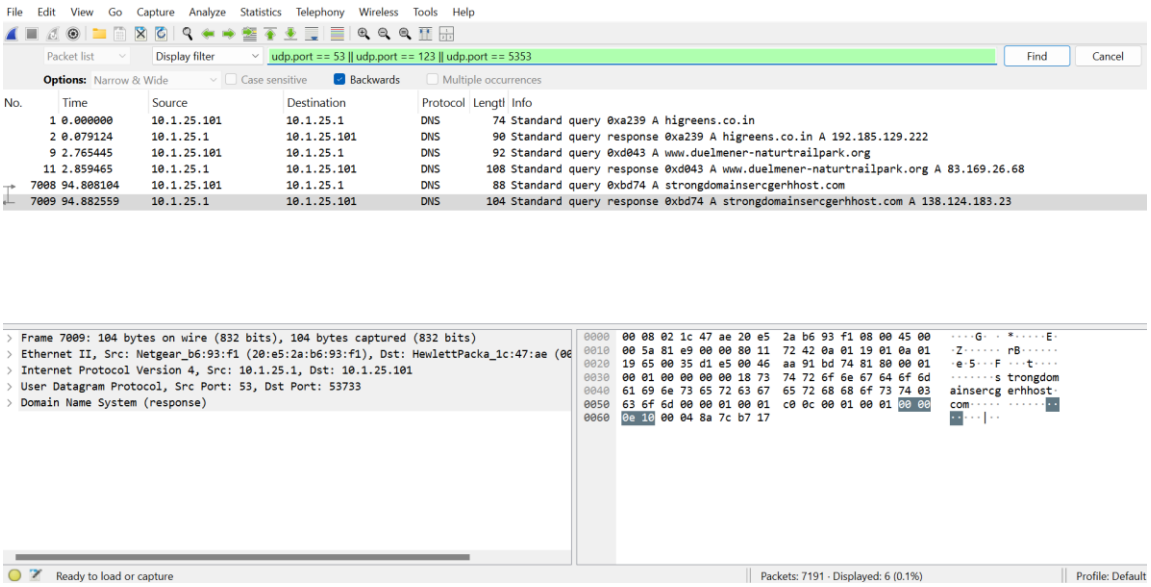
- **Filter Used**: udp.port == 53 || udp.port == 123 || udp.port == 5353
- **Purpose**: Focused on UDP traffic for:
    - **Port 53**: Associated with DNS tunneling for data exfiltration.
    - **Port 123**: Often abused in NTP amplification attacks.
    - **Port 5353**: Commonly used by mDNS, which can be exploited for lateral movement.

Observation

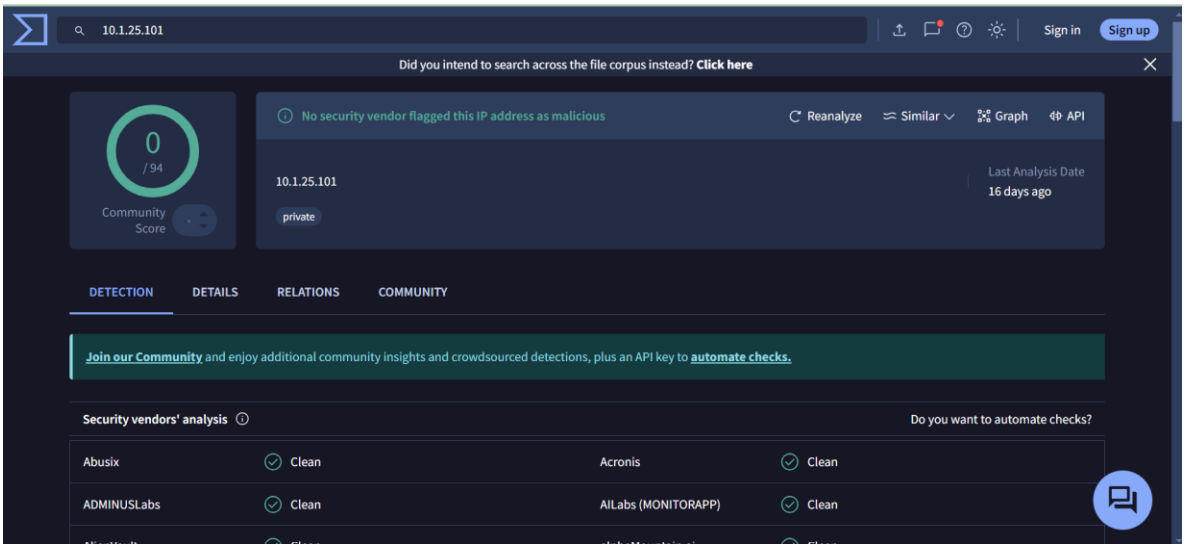
- Traffic on **Port 53**:
    - Standard DNS queries were observed, including strongdomainsercerghost.com resolving to IP 138.124.183.23.
    - While DNS queries were expected, the presence of suspicious domains raises concerns.
- No traffic on **Port 123** or **Port 5353**:
    - These results indicate no direct abuse of NTP or mDNS protocols in the capture.

Reputation Check

- The source IP 10.1.25.101 was validated using VirusTotal:
    - **Result**: No malicious activity flagged for this IP. It is a private IP, reducing immediate concerns.
- The resolved IP 138.124.183.23 (associated with strongdomainsercerghost.com) was flagged as potentially malicious during earlier checks.



Applying Filter



Result of Detected IP Address

Solutions for Resolving Rogue Application Issues

1. Strengthen Network Monitoring

- **Implement Advanced Filtering**:
    - Use filters to isolate suspicious traffic patterns, such as high-content-length HTTP packets, frequent DNS queries, or connections to suspicious ports.
- **Log and Alert Suspicious Activity**:
    - Configure intrusion detection systems (IDS) to flag anomalous traffic, such as communication with flagged domains (strongdomainsercerghost.com).

2. Domain Reputation Checks

- **Automate Domain Validation**:
    - Integrate reputation databases (e.g., VirusTotal) into your network monitoring tools to automatically flag malicious domains or IPs.
- **Block Suspicious Domains**:
    - Add domains like www.duelmen-naturtrailpark.org to a blacklist at the firewall level to prevent communication with malicious infrastructure.

3. Implement Application Whitelisting

- Restrict network communication to known, legitimate applications.
- Block unauthorized executables or archives, such as roamingkiller.zip, from being downloaded or executed.

4. Use Encrypted Traffic Analysis

- **Inspect TLS Handshake Data**:
    - Monitor server names (SNI fields) in encrypted traffic to detect connections to flagged domains.
- **Deploy TLS Interception**:
    - Use tools that decrypt and analyze encrypted traffic to identify malicious payloads or unauthorized communication.

5. Strengthen DNS Security

- **Enable DNS Filtering**:
    - Deploy secure DNS services (e.g., Cisco Umbrella) to block access to known malicious domains.
- **Monitor for DNS Tunneling**:
    - Use advanced DNS analysis tools to detect excessive queries or unusual query-response patterns.

6. Port-Level Access Controls

- **Block Unused Ports**:
    - Restrict traffic on unused or high-risk ports (e.g., 4444, 3333, 5555).
- **Monitor Active Ports**:
    - Continuously monitor ports like 53 (DNS), 123 (NTP), and 5353 (mDNS) for abnormal activity.

7. Enhance Endpoint Protection

- **Deploy Antivirus Solutions**:
    - Ensure all endpoints are equipped with updated antivirus software to detect and block malicious files like roamingkiller.zip.
- **Implement Endpoint Detection and Response (EDR)**:
    - Use EDR tools to monitor, detect, and mitigate rogue applications at the device level.

8. Conduct Regular Security Audits

- Perform periodic packet captures and network traffic analysis to identify anomalies.
- Use Wireshark or similar tools to audit traffic patterns and ensure compliance with network policies.

9. Educate Users

- Train users to avoid downloading files or visiting suspicious websites.
- Raise awareness about phishing attacks and unauthorized software installation.

10. Incident Response Plan

- Establish a robust incident response process to handle rogue applications.
- Ensure quick isolation of infected systems and removal of malicious applications.

Conclusion

This report demonstrates the effective use of Wireshark for detecting and analyzing rogue applications on a network. Through a detailed examination of HTTP, DNS, TCP, and UDP traffic, potential threats such as unauthorized file downloads, suspicious DNS queries, and malicious connections to flagged domains were identified. Key findings included high-risk domains like strongdomainsercerghost.com and www.duelmen-naturtrailpark.org, as well as the detection of suspicious activities linked to encrypted communication.

The analysis highlights the importance of targeted filtering, domain reputation checks, and protocol-specific investigations in identifying rogue applications. While no evidence of active mining operations or fragmented UDP traffic was found, suspicious connections and DNS queries raise concerns about potential command-and-control activities or data exfiltration.

To mitigate these risks, solutions such as domain blocking, application whitelisting, endpoint protection, and continuous network monitoring were recommended. By implementing these measures, organizations can proactively detect and prevent rogue applications from compromising network security. This report underscores the critical role of tools like Wireshark in enhancing visibility and safeguarding against evolving cyber threats.