Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Proactive Cyber Threat Detection with Real-Time Network Traffic Analysis and Threat Intelligence Integration

D.Vedasamhitha[1], Prof. Dr. Suchita Rawat
Department of Forensic Science, Garden City Uiversity[1]

Abstract - This study proposes a proactive method for cyber threat detection by integrating real-time network traffic analysis with threat intelligence. The goal is to identify and analyse malicious network activities before they compromise data or systems. Live network traffic is captured from malicious web sources within a secure, isolated environment using Wireshark to monitor packet-level behaviour and detect suspicious communication patterns.

Captured packets are examined for anomalies such as unusual IPs, abnormal port usage, frequent DNS requests, irregular data sizes, and encrypted traffic flows. These indicators help identify threats like phishing, malware downloads, and command-and-control activities. The analysed data is then correlated with threat intelligence to verify and classify the nature of threats, improving accuracy and reducing false positives.

By merging behavioural observation with intelligence validation, this research demonstrates the effectiveness of proactive, continuous monitoring over reactive approaches. It highlights how real-time analysis and adaptive intelligence can strengthen cybersecurity resilience and enable faster, informed responses to evolving cyber threats.

Keywords: Cyber threat detection, real-time Network traffic, packet analysis, Threat intelligence, Malicious URLs, Wireshark

INTRODUCTION

Due to the exponential development of information technologies and their widespread adoption in the contemporary world, cyber risks have not only become more complex but also occurred more often (Stallings & Brown, 2018). Companies from any industry depend on secure and reliable infrastructure of a network and become exposed to malicious activities that may result in significant harm and affect their operations (Cisco, 2023). As a response to this issue, proactive approaches to cybersecurity gain increasing relevance, focusing on detecting and preventing rather than responding to any attacks (NIST, 2018).

Traditional methods of protection, such as signature-based detection or incident investigations, do not provide enough information about new types of malicious activities and therefore fail to identify potential threats promptly (Sommer & Paxson, 2010). As a result, attackers use advanced dynamic tactics that evade static approaches and go unnoticed during the early stages of any cyber-attack. This is why there has been an evident need for continuous surveillance technologies that can recognize any anomalies and potentially dangerous behaviours as soon as possible (Sanders & Smith, 2014).

Network Traffic analysis refers to the thorough process of studying the behaviour of communication in a network through the analysis of packets. Behaviours like unusual flags in TCP communications, suspicious sessions terminations, strange DNS queries, inconsistent packet sizes, and use of uncommon protocols usually suggest something malicious (Bejtlich, 2013). Advanced software programs such as Wireshark offer features such as capturing, filtering, and analysis of network traffic that help in deep packet inspection of potential threats (Orebaugh et al., 2007). Properly structured filtering procedures assist analysts to focus on suspicious activities, thus helping in decision making.

One of the major problems with the current threat detection process is differentiating legitimate behaviour from a malicious one. This is because attackers can easily establish systems that act in almost similar ways to the legitimate network behaviours by implementing things like domain impersonation, encrypting data, using dynamic IP addresses, frequent change of domains, among others (Liao et al., 2016). Also, most attackers implement security features like TLS that make it impossible to analyse packets in the network (Husák et al., 2018).

Apart from traffic behaviour analysis, incorporation of threat intelligence in monitoring operations greatly enhances detection accuracy by matching network behaviour patterns against known IOCs (Tounsi & Rais, 2018). These approaches enhance proactive

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

cybersecurity strategies by shifting from reactive response to predictive threat analysis that helps differentiate between harmless anomalies and actual threats. It is expected that such an approach will help minimize false alarms and enhance efficiency.

This paper explores the application of threat detection techniques for proactive cybersecurity in analysing real-time traffic using Wireshark and incorporating threat intelligence principles. Analysis of suspicious and non-suspicious websites will be done in a sandboxed environment with an emphasis on analysing network packets based on different protocols like DNS analysis, TCP flag checks, and TLS handshakes.

The purpose of the study is to analyse real-time network traffic that originates from malicious and non-malicious URLs in a sandboxed environment with the use of Wireshark. Anomalies at protocol level, namely abnormal behaviour of DNS query, TCP flag, TLS handshake, and abnormal session termination are determined. The researcher makes a comparison between the characteristics of the network traffic that originates from different types of URLs to be able to differentiate abnormal traffic from normal. Specific filtering tools are used to detect retransmission, reset packet, and unusual DNS resolution behaviour. Finally, the concepts of threat intelligence will be applied in order to make sense of the observed network anomalies and to find out whether any indicators of compromise can be identified. Overall, the study will showcase how effective is the technique of real-time network traffic analysis for detecting cyber threats (Sanders & Smith, 2014; Tounsi & Rais, 2018).

METHODOLOGY

3.1 Research Design

The methodology utilized for this investigation is that of experimental research to study the nature of network traffic behaviour for suspicious URLs as well as the behaviour of benign URLs. The experiment seeks to uncover anomalous protocols in network traffic behaviour, which may be indicative of any malicious cyber attack (Sanders & Smith, 2014). A carefully managed testbed was created in order to conduct this investigation while being able to avoid doing any harm to the computer. Real-time analysis and monitoring of packets was conducted to determine differences between malicious traffic and normal traffic.

Instead of using signature-based tools for threat detection, behavioural analysis of network packets was conducted to detect any possible IOCs. Such communication characteristics as DNS queries, TCP flags, TLS handshakes, and HTTP request behaviour were evaluated.

3.2 Experimental Environment

All web addresses were visited from a sandboxed environment with the help of Sandboxie Plus; the software works by isolating all the activities from the browser and ensuring that any harmful code cannot impact the underlying OS (Sandboxie Plus, 2023). Wireshark, an open-source packet analyser software that analyses network packets in real time, was used to analyse the traffic generated on the Internet.

Wireshark was used to analyse the packets in real-time transmission between the client computer and remote servers. The experiment was performed in an internet-enabled environment for this purpose.

3.3 Data Collection.

Data for network traffic analysis involved accessing multiple URLs that were labelled as suspicious or benign. Data from the suspected URLs was obtained using URLs obtained from public phishing sites and accessed in the sandboxed environment, ensuring the safety of interactions with malicious sites (PhishTank, 2023). Benign websites such as Wikipedia and GitHub were also considered in order to create baseline communication patterns.

Before browsing a particular URL, packet captures would be done to obtain full communication patterns. Such data consisted of requests related to DNS resolution, establishment of TCP sessions, TLS handshakes, HTTP request patterns, and the behaviour of packet exchange between source and destination IP addresses. Packets captured were then analysed for patterns of deviant behavior**.**

3.4 Traffic Analysis Parameters

The analysis focused on identifying anomalies across the following key network communication parameters:

DNS Behaviour: DNS requests were monitored for any unusual patterns such as excessive DNS requests for the same domain, questionable domain names, or unusual mappings between domain names and IP addresses, which could suggest domain spoofing or fast fluxing attacks (Passerini et al., 2008).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

TCP Communication Behaviour: The TCP packets were studied by looking into retransmissions, duplicates, reset packets, abnormal connection terminations, and general connection stability because these parameters have been known to indicate network attacks (Bejtlich, 2013).

TLS Handshake Behaviour: Handshake messages were checked in order to ensure the secure establishment of the connection, check that SNI values were correct, and make sure there was encryption negotiation. Inconsistency in handshakes could indicate that there were self-signed certificates or encryption malpractice (Husák et al., 2018).

HTTP Communication Patterns: HTTP request types like GET and POST were evaluated to find abnormal request sequences, irregular data transfer patterns, or communication protocols that do not conform to regular web browsing patterns (Sanders & Smith, 2014).

Packet Flow Characteristics: Observations were made on source/destination IP addresses, port numbers, and differences in packet sizes to detect communication anomalies which could be indicative of anomalous or covert behaviour within the network (Orebaugh et al., 2007).

3.5 Filtering Techniques

Wireshark display filters were applied to isolate specific protocol behaviour and efficiently identify communication anomalies. Structured filtering techniques enabled focused examination of suspicious traffic segments while minimising interference from background network noise.

The following filters were applied during the analysis:

Filter	Purpose
dns	Identify DNS query patterns and domain resolution behaviour
tcp.analysis.flags	Detect TCP-level issues including retransmissions and duplicate ACKs
tcp.flags.reset == 1	Isolate TCP reset packets indicating abrupt session termination
tls.handshake	Examine TLS handshake initiation and completion
tls. handshake.extensions_server_name	Inspect SNI values for domain verification
http. request.method	Analyse HTTP GET and POST request patterns

These filters collectively enabled systematic identification of unusual DNS behaviour, TCP instability, reset activity, TLS communication characteristics, and HTTP request anomalies associated with potentially malicious traffic.

3.6 Analysis Procedure

URLs were examined one by one, starting off with the appropriate packet capturing process prior to the actual access to the web page so that the entire communication process could be captured accurately.

The traffic collected during packet capture was then screened using the methods explained in Section 4.5, and protocol-based anomalies were identified.

For each URL, observations were made and evaluated based on threat intelligence principles to establish whether the traffic had any malicious or non-malicious characteristics (Tounsi & Rais, 2018). The malicious URLs should reveal characteristics including odd domain name structure, odd DNS queries, retransmission, resets, and abnormal session characteristics. On the other hand, the benign URLs were supposed to show consistent TLS handshake, normal session traffic, and proper DNS resolution typical of legitimate web communication (Bejtlich, 2013).

Comparative analysis was then conducted based on behavioural characteristics in order to draw important conclusions as presented in the next section**.**

4. RESULTS AND ANALYSIS

4.1 Overview of Analysed URLs

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

In total, seventeen URLs were tested in this study, of which fifteen were found to be suspicious, whereas two URLs were considered benign. The suspicious URLs were taken from the publicly available Phish Tank website, where all phishing reports can be verified and stored for future use (Phish Tank, 2023). On the other hand, two benign URLs www.wikipedia.org and github.com were chosen on the grounds of legitimacy and popularity, representing a standard benchmarking case for network communications.

The URLs were tested in an isolated sandbox environment through Sandboxie Plus software. Network packet capturing was done by utilising Wireshark with structured display filters for each layer of communication protocol such as DNS, TCP, TLS, and HTTP (Orebaugh et al., 2007). Each URL was tested independently with a focus on the unusual characteristics of network communications at a packet level.

To support structured analysis and facilitate meaningful cross-URL comparison, the suspicious URLs were categorised according to their dominant anomaly type. These categories include HTTP-based credential exfiltration, DNS-level anomalies and domain impersonation, TCP behavioural irregularities, TLS misuse, and advanced evasion techniques. A consolidated overview of all analysed URLs, their respective anomaly classifications, and the Wireshark filters applied during analysis is presented in Table 1.

No	URL	Category	Primary Anomaly Identified	Wireshark Filter Applied
1	linkedin-0151735332.marssa.com.br	Malicious	Unencrypted credential exfiltration via HTTP POST	http
2	flipkart.big-billion-offer.com	Malicious	DNS anomaly and subdomain-based brand impersonation	dns
3	icici-bank-login.com	Malicious	Plaintext HTTP communication and suspicious file streaming	http
4	bankofamerica-alerts.t35.com	Malicious	Persistent TCP beaconing and background communication	tcp
5	alibaba-163products-gallery.onlinewebshop.net	Malicious	Large unencrypted HTTP packets indicating data exfiltration	frame.len > 800 && (http || tcp)
6	snapchat-konto.com	Malicious	Anomalous User-Agent string and domain spoofing over HTTP	http.user_agent
7	youtube-alsves8wel7.t35.com	Malicious	Frequent TCP resets and unstable session behaviour	tcp.flags.reset == 1
8	paypal.com.web-scr.us	Malicious	Excessive DNS queries, NXDOMAIN responses, and tracker domains	Dns
9	nykaa.xyz	Malicious	TCP instability, BT-DHT peer-to-peer	bt-dht, tls, quic

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

			traffic, and encrypted flows	
10	pinterest-login.com	Malicious	TCP Zero Window events and persistent keep-alive sessions	Tcp
11	sites.google.com/view/acessopjonline	Malicious	TCP instability despite valid TLS encryption	tcp. analysis.flags
12	google.com/amp → vvr-sign.biz	Malicious	AMP-based redirection to an unrelated external domain	http.response.code == 301 || 302
13	airbnb.pl-oferta53334-macbook-air-m2.shop	Malicious	Concealed BitTorrent P2P	bittorrent, udp
14	br-icloud.com.br	Malicious	Incomplete TLS handshakes and repeated DNS anomalies	tls.handshake, dns
15	facebook.unitedcolleges.net	Malicious	HTTP continuation packets and TCP retransmissions	http, tcp.analysis.retransmission
16	www.wikipedia.org	Benign	No anomalies detected — stable DNS, TLS, and TCP behaviour	dns, tls.handshake
17	github.com	Benign	No anomalies detected — normal DNS resolution and TCP patterns	dns, tcp.analysis.flags

Table 1: Summary of Analysed URLs, Anomaly Classifications, and Applied Wireshark Filters Summary of Analysed URLs, Anomaly Classifications, and Applied Wireshark Filters

4.2 Analysis of Malicious URLs

4.2.1 HTTP-Based Phishing and Credential Exfiltration

URLs linkedin-0151735332.marssa.com.br, icici-bank-login.com, and alibaba-163products-gallery.onlinewebshop.net revealed network-level indicators of HTTP credential harvesting and unauthorised data extraction. Network communication on all three websites was made entirely on port 80 over HTTP without any encryption at the transport layer. Multiple HTTP POST commands targeting remote malicious endpoints were logged, with server replies returning HTTP 200 OK to confirm receiving the sent information. Specifically, for the alibaba-163products-gallery.onlinewebshop.net URL, traffic packets of more than 1,000 bytes in size were noted past the initial loading of the webpage. This indicated automated continuous background transfers of encoded data after an initial web-page visit. Brand names LinkedIn, ICICI Bank, and Alibaba were noted in the content of each respective website, despite the hosting being completely unrelated. Brand impersonation is commonly employed by phishers to trick victims into entering their credentials onto fake login webpages (Liao et al., 2016; Oest et al., 2020). Failure to use transport-layer encryption when communicating between victims' browsers and remote endpoints clearly implies sending plain-text credentials, which is a high-risk threat vector typical for credential harvesters (Heartfield & Loukas, 2015).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

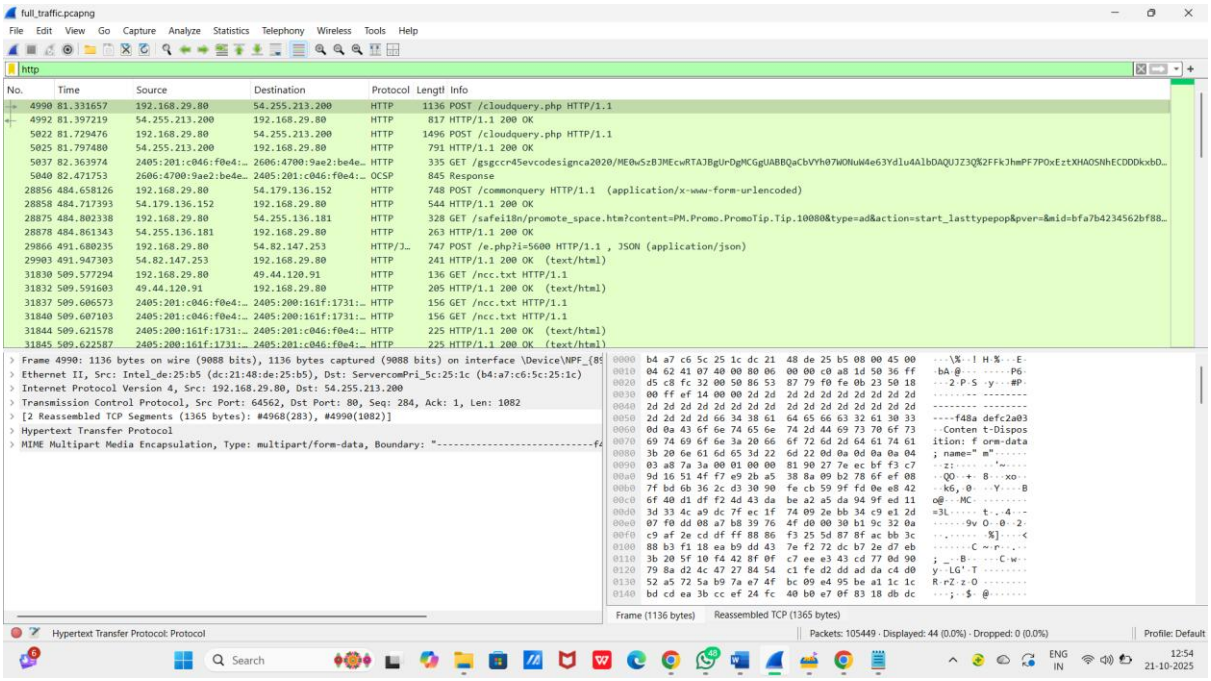

Figure 1 : Wireshark capture showing repeated HTTP POST requests to /Cloudeqry.php over port 80, indicating unencrypted credential exfiltration from linkedin-0151735332.marssa.com.br

4.2.2 DNS Anomalies and Domain Impersonation

The following two URLs, flipkart.big-billion-offer.com and paypal.com.web-scr.us, had distinctive signs of phishing infrastructure and automation at the DNS level. Regarding flipkart.big-billion-offer.com, there were numerous DNS lookups performed for both A and AAAA records in quick succession; the resolved IP addresses were not aligned with Flipkart's legitimate infrastructure. The domain structure included the trademarked brand name "Flipkart" as part of the domain sub name in conjunction with a completely unrelated TLD to imitate one of the organization's highly popular promotional campaigns and lure potential victims. Rapid IP resolution changes within short intervals may be indicative of fast-flux DNS hosting, a tactic used by malicious actors to avoid discovery and prevent dismantling of their infrastructure (Passerini et al., 2008). With regards to paypal.com.web-scr.us, there was another distinct pattern of anomaly involving several DNS queries performed within less than 0.1 seconds to indicate automated script activity rather than a user's normal browsing behaviour. Some DNS responses had the status code NXDOMAIN, which means that the query attempted to resolve a non-existent domain; this behaviour is characteristic of phishing kits, which attempt to dynamically load resources from various attacker-controlled servers (Antonakakis et al., 2011).

DNS queries were additionally directed toward tracker-related domains and resolved through third-party CDN infrastructure, indicating deliberate obfuscation of the true hosting location. Collectively, the observed DNS behaviour across both URLs reflects systematic efforts to impersonate legitimate services while concealing malicious infrastructure through evasive resolution techniques (Liao et al., 2016).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

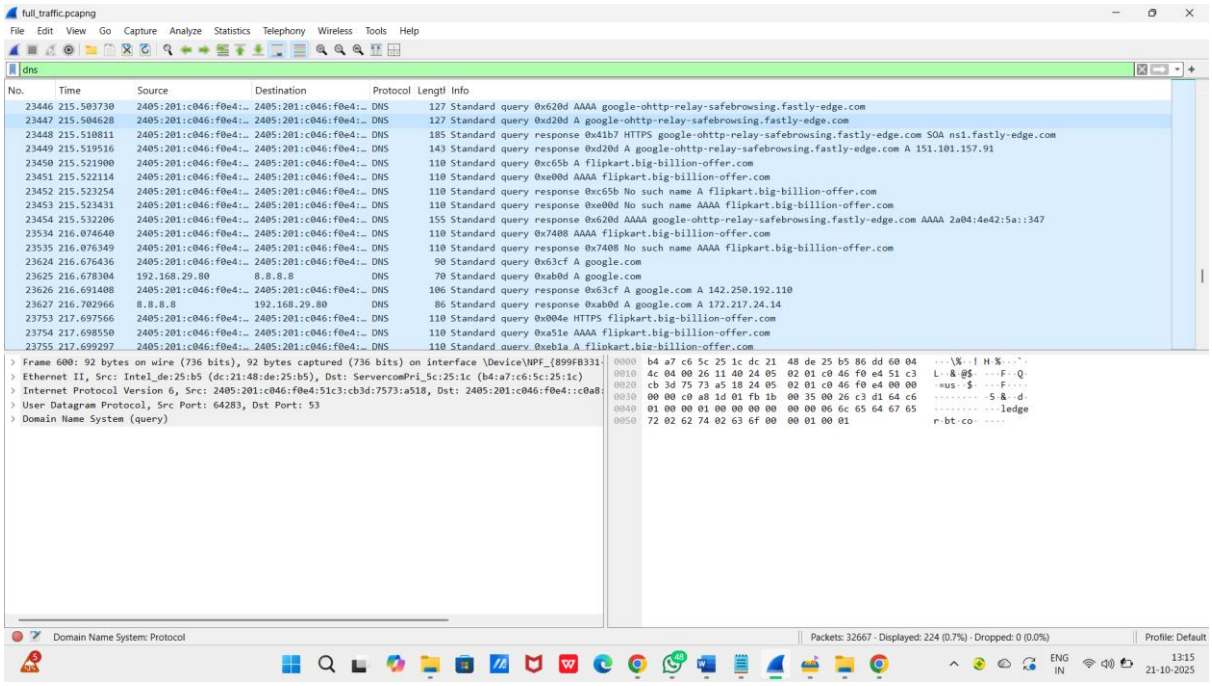

Figure 2: Wireshark packet capture displaying repeated DNS query responses for flipkart.big-billion-offer.com, including Standard query responses for A (IPv4) and AAAA (IPv6) records alongside multiple "No such name" (NXDOMAIN) responses, indicative of fast-flux DNS behaviour and domain impersonation activity

4.2.3 TCP Behavioural Anomalies and Session Instability

TCP level anomalies were detected from four websites; bankofamerica-alerts.t35.com, youtube-alsves8wel7.t35.com, nykaa.xyz and facebook.unitedcolleges.net. The anomalies were characterised by network session instability, frequent connection terminations, and regular background communication that could not be attributed to genuine browsing activities. Network activity from bankofamerica-alerts.t35.com showed persistent low volume TCP communication which entailed regular exchanges of ACK/PSH-ACK TCP segments sent from the same source IP to the same destination IP address in the absence of any activity initiated by users. Such unsolicited packet exchanges represent typical characteristics of a network beaconing process, a common form of C2 communication employed by attackers (Bayer et al., 2009). TCP Reset segments, retransmitted segments, and duplicate ACKS were observed during network sessions from youtube-alsves8wel7.t35.com, implying abnormal termination of such network sessions that were not consistent with long lived sessions employed by genuine video streaming networks. Similar network anomalies were observed for traffic from nykaa.xyz, where frequent TCP resets, TCP retransmissions, and bit torrent DHT communication protocol segments were detected. Network packets captured from facebook.unitedcolleges.net revealed HTTP continuation packets alongside out-of-order packet sequences, duplicate acknowledgments, and abrupt RST-initiated session terminations following data exchange behavioural indicators consistent with automated, scripted communication rather than normal user-driven browsing activity (Sanders & Smith, 2014). Across all four URLs, the observed TCP anomalies collectively reflect poorly configured or deliberately malicious backend infrastructure, wherein connection instability and abnormal termination patterns serve as reliable packet-level indicators of suspicious or compromised network communication.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

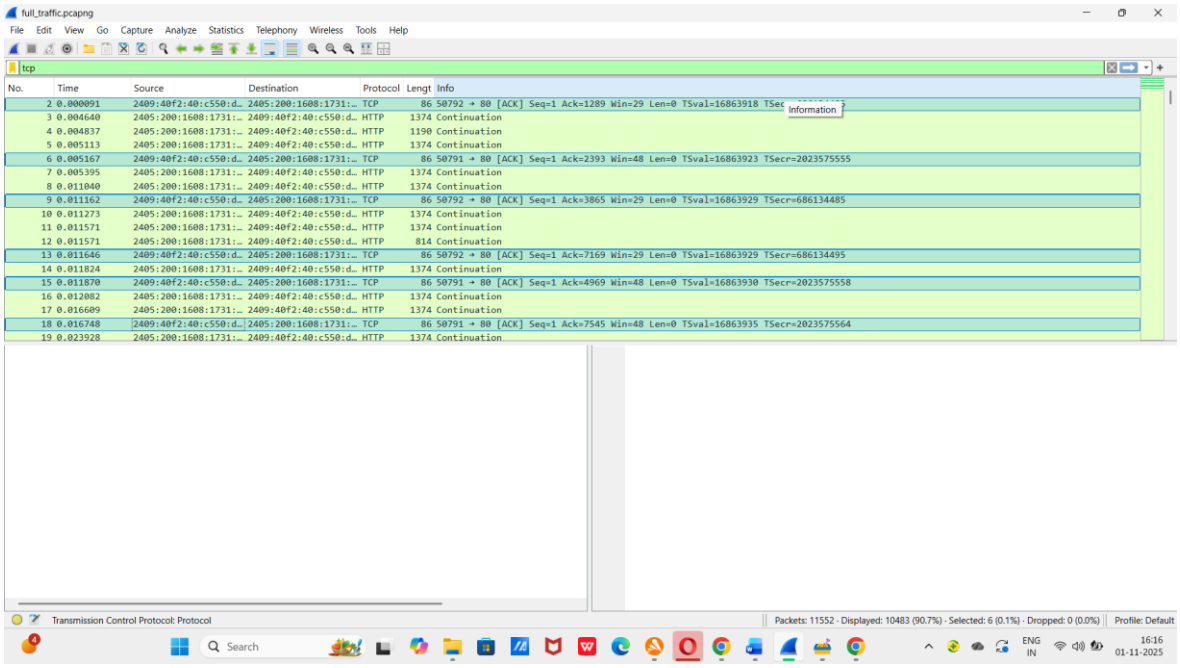

Figure 4: Wireshark packet capture displaying repeated HTTP Continuation packets of consistent length (1374 bytes) alternating with TCP ACK frames between identical source and destination addresses, observed during analysis of facebook.unitedcolleges.net, indicative of automated scripted communication inconsistent with normal user-driven browsing behaviour

4.2.4 TLS Misuse and Encryption Abuse

Three websites, pinterest-login.com, br-icloud.com.br, and sites.google.com/view/acessopjonline, showed signs of anomalies related to TLS encryption, including either partial TLS handshake, early session closure, or exploitation of genuine encryption technology to lend legitimacy to misleading information. Pinterest-login.com had TCP Zero Window events, as well as keep-alive packets, showing congestion on the server or communication between non-human entities. While TLS handshake was seen for the website, it had properties that did not match those of legitimate websites, showing that TLS was used to avoid detection and not secure data transmission between users (Husák et al., 2018). The network traffic of br-icloud.com.br involved partial TLS handshakes, where there were Client Hello and Server Hello messages before terminating the connection. Early closed TLS connections, such as those seen in the traffic, often occur in HTTPS phishing websites that attempt to appear legitimate by using encryption technology (Kotzias et al., 2018). The third URL, sites.google.com/view/acessopjonline, represented an interesting case whereby a successful TLSv1.2 and TLSv1.3 handshake was made using genuine Google certificates; however, at the same time, there was a high level of TCP retransmissions, duplicate ACKs, and connection resets in the traffic capture. The foregoing scenario shows that having a genuine TLS certificate does not necessarily mean that the traffic is benign in nature. In the same vein, a rising trend among cyber criminals is the exploitation of reputable web hosts to serve up misleading web pages with the advantages of using trusted security certificates (Oest et al., 2020).

4.2.5 Advanced Evasion Techniques

URLs such as google.com/amp/s/vvr-sign.biz/?cWNBq and airbnb.pl-oferta53334-macbook-air-m2. shop incorporated more advanced methods of evasion that transcended conventional phishing techniques and leveraged trusted infrastructure components along with hidden peer-to-peer communication. URL google.com/amp/s/vvr-sign.biz/?cWNBq made use of trusted AMP component in Google infrastructure to initiate traffic and send HTTP 301 and 302 redirect response headers to silently direct users from Google infrastructure to an external website vvr-sign.biz. DNS lookup resolved the URL to infrastructure belonging outside of Google after loading of AMP pages while query string parameters within URL suggested use of randomisation for session tracking and identification of victims within the attack (Oest et al., 2020). Moreover, TCP analysis indicated that there were retransmissions, duplicate acknowledgments, and quick FIN session terminations, which suggested that there was a shaky infrastructure on the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

backend, even though the entry looked to be legitimate. Malicious data was routed through Google AMP in order to avoid typical URL filters and exploit trust of users with regard to Google domain (Sabetta & Bezzi, 2019). As for the case of airbnb.pl-oferta53334-macbook-air-m2.shop, an entirely different evasion technique was discovered, which involved the extensive use of BitTorrent Distributed Hash Table protocol, characterized by repeated Get peers queries, Response Nodes messages, and peer searches using hash values, not only on port 6881 but also on port 37000. This sort of behaviour is highly inconsistent with e-commerce practices and implies that there was an underlying data transfer process taking place through torrents when the URL was loaded into the browser, which has often been observed to be used by crypto miners, advertisements, and other methods of delivering payloads (Kanich et al., 2008). Taken together, these examples indicate that modern-day phishing and malware have come to rely on exploiting platforms and using hidden network protocols to avoid detection, underscoring the need for behavioural packet analysis.

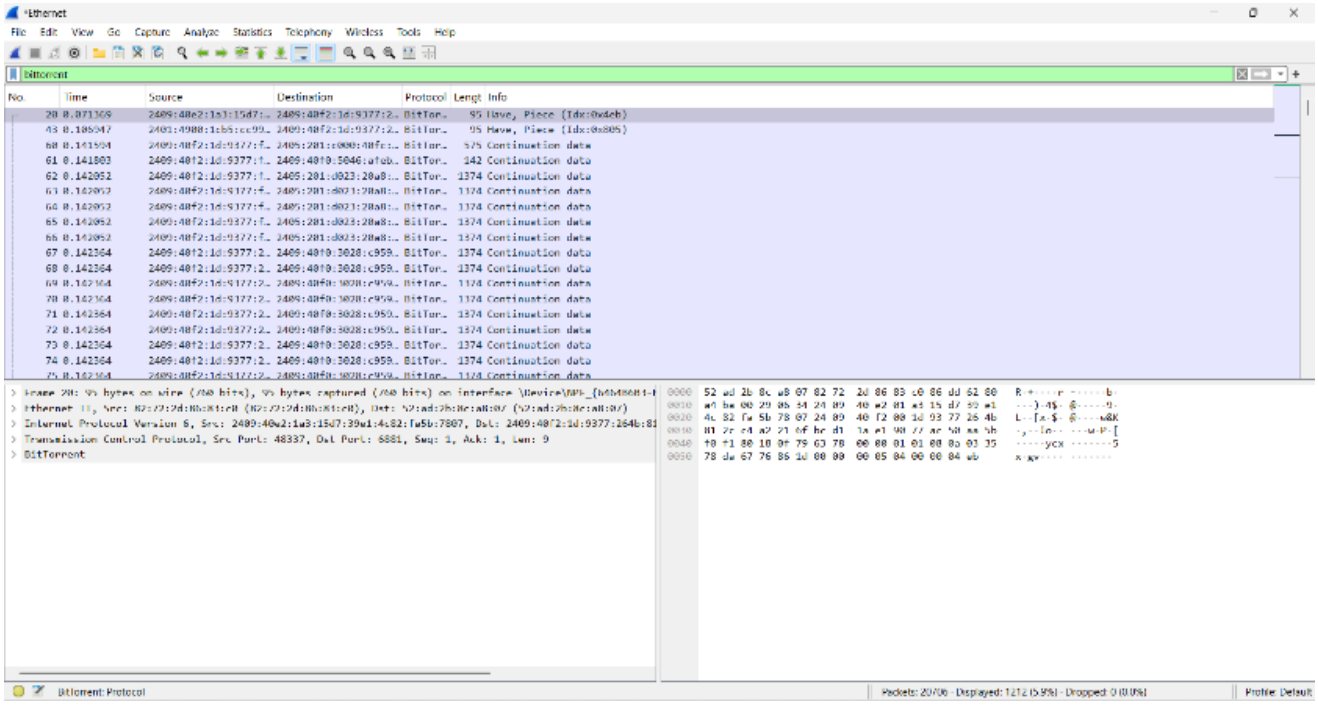

Figure 4: Wireshark packet capture displaying BitTorrent protocol traffic including repeated Continuation data packets observed during analysis of airbnb.pl-oferta53334-macbook-air-m2.shop, indicative of concealed peer-to-peer communication activity inconsistent with legitimate e-commerce web behaviour

4.3 Benign URL Analysis

The two benign URLs, www.wikipedia.org and github.com, were analysed to create an established benchmark of behaviour that can be used for comparison with abnormal behaviour seen in the malicious URLs. Analysis of traffic from www.wikipedia.org showed consistent DNS resolution with accurate A and AAAA records resolved using Wikimedia's Content Delivery Network (CDN) through a valid CNAME value (dyna.wikimedia.org). The traffic analysis shows completion of TLS handshake over port 443 using TLS 1.3. The SNI value was found to be accurate to the target site and without spoofing. There were traces of TCP retransmission and duplicates within the traffic capture but these were minimal and within acceptable range based on network latency without being deliberate or malicious (Bejtlich, 2013). Further analysis on github.com showed similar features in the form of proper DNS resolution without NXDOMAIN or any other suspicious domain name, ordinary TCP connections including keep alive and ZeroWindowProbe that were due to usual network congestion mitigation, and random distribution of RST packets to different external IP addresses rather than targeting just one IP address. Neither any regular beaconing activity, any irregular POST messages nor abnormal packet structures were found for any of the two URLs in question. It is evident that the characteristics of benign URLs are significantly different from the malicious URLs, especially in terms of unencrypted credential submission, fast-flux DNS resolution, TCP beaconing, incomplete TLS handshake, and covert P2P connection, which can be considered clear signs of malicious or phishing activity (Sanders & Smith, 2014; Husák et al., 2018).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

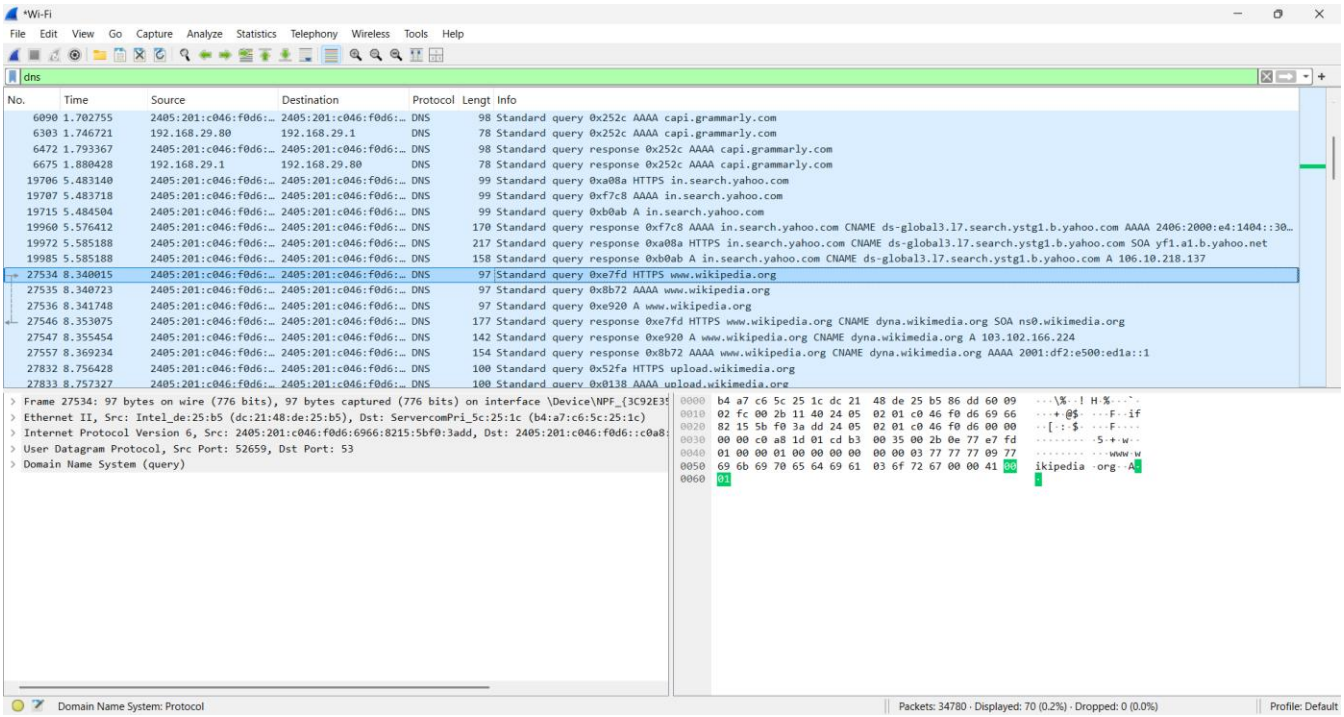

Figure 5: Wireshark packet capture displaying stable DNS resolution for www.wikipedia.org, showing valid CNAME mapping through Wikimedia CDN infrastructure (dyna.wikimedia.org) with consistent A and AAAA record responses and no anomalous query behaviour, representative of normal legitimate web communication

4.4 Comparative Summary

A thorough analysis of network traffic created by fifteen malicious and two benign URLs proved there is a noticeable difference between malicious and legitimate traffic patterns at the level of packets. Malicious traffic exhibited certain protocol-level anomalies such as an unencrypted submission of HTTP credentials, fast-flux DNS resolution, TCP beaconing, incomplete TLS handshakes and covert peer-to-peer communication. Each of these phenomena represents a unique yet interlinked mechanism employed by threat actors to conceal their activities in the process of carrying out their malicious intent. On the other hand, legitimate URLs featured consistent DNS resolution, full TLS handshake performed on port 443 and regular TCP communication with proper adjustment for network latency and congestion, as well as absence of any unusual packet patterns and behaviour at the protocol level. Importantly, sites.google.com/view/acessopjonline showed how legitimate TLS encryption and hosting does not imply benign traffic patterns, thus proving that evaluating certificates for cybersecurity purposes has some limitations (Oest et al., 2020). All of these results show how analysing packets proves valuable and necessary to proactively detect malicious activities that bypass signature-based security measures (Sanders & Smith, 2014; Bejtlich, 2013).

5. DISCUSSION

Based on the outcomes of this research, it can be concluded that the real-time analysis of traffic in a network through Wireshark software, supplemented with structured protocol-level filtering methods, offers a promising solution for the proactive identification of cyber threats within the confines of managed network environments. These behavioural anomalies, which have been observed during the course of this research through the fifteen malicious URLs ranging from HTTP-based credential theft to DNS spoofing, TCP errors, TLS attacks, and evasion tactics all validate that the behaviour of packets is indeed a reliable indicator of malice. One of the most important observations from this research is related to the variety of attack methods used by the investigated URLs. Instead of following a standard signature, the malicious web addresses adopted different and dynamic communication patterns specifically intended to bypass traditional defensive measures. The use of Google AMP technology in order to redirect victims to phishing sites and the employment of BitTorrent P2P protocols for the delivery of malware payloads through covert channels are examples of advanced evasion mechanisms that transcend the capacities of traditional intrusion detection systems (IDSs) based on signatures (Oest et al., 2020).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Analysis of TLS anomalies led to another important conclusion concerning the drawbacks of using encryption when evaluating trustworthiness. In particular, the example of sites.google.com/view/acessopjonline proved that properly encrypted and hosted web resources could be manipulated by adversaries in order to lend credence to fake information (Kotzias et al., 2018). This phenomenon coincides with a tendency reported in the literature according to which phishers make active use of trusted websites and encryption to mount their phishing attacks (Husák et al., 2018). Thus, the research findings imply that the TLS certificate should not be used as the sole criterion for assessing trustworthiness; instead, behavioural traffic analysis has to be conducted alongside other approaches.

The comparative analysis of malicious and benign URL traffic profiles further validated the analytical framework adopted in this study. Benign URLs consistently demonstrated stable DNS resolution, successful TLS handshake completion, and TCP communication patterns attributable to normal network latency, with no evidence of credential submission, beaconing behaviour, or covert protocol activity. The clear contrast between malicious and legitimate traffic characteristics confirms that structured packet-level behavioural indicators can be systematically applied to distinguish suspicious communication from normal browsing activity, supporting the feasibility of proactive threat detection through real-time network monitoring (Tounsi & Rais, 2018).

Inclusion of the threat intelligence concepts in the analytical process improved the interpretative quality of the results obtained. In particular, by placing the analysed network anomalies in the context of attacker TTPs, the researchers managed to go beyond mere descriptions of packets and to classify observed events based on their actual nature. The described methodology helped reduce potential interpretation errors arising from possible confusion between normal network dynamics and malicious communication attempts (Liao et al., 2016; Tounsi & Rais, 2018). Overall, the application of the selected approach is seen as improving cybersecurity strategies due to early detection of threats.

However, it should be noted that the employed methodology had its drawbacks. The study was performed in a sandboxed environment and relied on a limited number of URLs to analyse malicious activity.

Moreover, the dependence on manual packet-level analysis, even though it is quite successful in showing behavioural traits, may create scalability problems in networks with high amounts of traffic, in which automated pipeline processes would be necessary. Further research in this area may consider tackling such issues by applying the proposed analytical model to more extensive and heterogeneous URL data sets, incorporating machine-learning based anomaly detection algorithms alongside manual analysis, and testing the proposal under live corporate network settings (Sommer & Paxson, 2010).

6. CONCLUSION

The current study examines the use of real-time network traffic analysis as an early warning system for detecting cybersecurity threats, with Wireshark as the main tool used for capturing packets and analysing them in a controlled sandbox laboratory. By analysing the behaviour of network traffic produced by fifteen malware URLs and two control benign URLs, the paper shows that behavioural features at the protocol level such as unusual DNS behaviour, plain-text HTTP credential submission, TCP connection volatility, TLS connection irregularities, and hidden peer-to-peer communication can be used as trustworthy and practical criteria to differentiate malicious traffic from normal traffic.

Indeed, these results demonstrate that the presence of anomalies in terms of abnormal communication behaviour is consistently observed in case of phishing websites across several protocol layers; on the other hand, the communication carried out by normal websites is consistent and follows certain structures throughout the entire session. The range of attack methods detected, including such approaches as brand spoofing, fast-flux DNS hosting, AMP exploit, and hidden BitTorrent traffic, indicates the adaptiveness of today’s phishing attacks and the inability of simple signature-based solutions to detect them.

One of the major achievements of the research is its proof of the possibility of applying structured analysis on the packet level along with the ideas of threat intelligence and making the step from responding to incidents to proactively identifying threats. In addition, the combination of behavioural network analysis and contextual threat intelligence made it possible to understand the behaviour of attacks based on the knowledge of the tactics, techniques, and procedures used by attackers, increasing the accuracy of classification of discovered anomalies as threats. Moreover, the discovery of the possibility of misusing TLS encryption and legitimate hosting makes it clear why layered approaches should be applied for threat detection.

Indeed, the practicability of using Wireshark as a useful packet-level investigation tool within a well-controlled environment has been adequately proven by the results obtained in this research. The filtering methods used such as analysing the DNS queries, TCP flags, TLS handshakes, and HTTP requests have effectively helped to identify any behaviour that deviates from the norm, thus providing factual support for making decisions in detecting threats to security. Such conclusions add weight to the existing scientific

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

literature about the need to incorporate behaviour-based cybersecurity techniques to complement other traditional detection methods for better network security. Future studies should focus on expanding the scope of analysis undertaken in this research to incorporate automated anomaly detection models, and testing the viability of the proposed solution in real-life corporate networks.

REFERENCES

[1] Antonakakis, M., Perdisci, R., Lee, W., Vasiloglou, N., & Dagon, D. (2011). Detecting malware domains at the upper DNS hierarchy. *Proceedings of the 20th USENIX Security Symposium*, 1–16.

[2] Bejtlich, R. (2013). *The practice of network security monitoring: Understanding incident detection and response.* No Starch Press.

[3] Cisco. (2023). *Cisco annual internet report 2018–2023.* https://www.cisco.com/c/en/us/solutions/executive-perspectives/annual-internet-report/index.html

[4] Heartfield, R., & Loukas, G. (2015). A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. *ACM Computing Surveys*, *48*(3), 1–39. https://doi.org/10.1145/2835375

[5] Husák, M., Čermák, M., Jirsík, T., & Čeleda, P. (2018). HTTPS traffic analysis and client identification using passive SSL/TLS fingerprinting. *EURASIP Journal on Information Security*, *2018*(1), 1–14. https://doi.org/10.1186/s13635-018-0075-0

[6] Kanich, C., Kreibich, C., Levchenko, K., Enright, B., Voelker, G. M., Paxson, V., & Savage, S. (2008). Spamalytics: An empirical analysis of spam marketing conversion. *Proceedings of the 15th ACM Conference on Computer and Communications Security*, 3–14. https://doi.org/10.1145/1455770.1455774

[7] Kotzias, P., Razaghpanah, A., Amann, J., Paterson, K. G., Vallina-Rodriguez, N., & Caballero, J. (2018). Coming of age: A longitudinal study of TLS deployment. *Proceedings of the ACM Internet Measurement Conference*, 415–428. https://doi.org/10.1145/3278532.3278568

[8] Liao, X., Yuan, K., Wang, X., Li, Z., Xing, L., & Beyah, R. (2016). Acing the IOC game: Toward automatic discovery and analysis of open-source cyber threat intelligence. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 755–766. https://doi.org/10.1145/2976749.2978315

[9] NIST. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). National Institute of Standards and Technology. https://www.nist.gov/cyberframework

[10] Oest, A., Safaei, Y., Doupé, A., Ahn, G. J., Wardman, B., & Tyers, K. (2020). PhishTime: Continuous longitudinal measurement of the effectiveness of anti-phishing blacklists. *Proceedings of the 29th USENIX Security Symposium*, 379–396.

[11] Orebaugh, A., Ramirez, G., & Beale, J. (2007). *Wireshark & Ethereal network protocol analyser toolkit.* Syngress Publishing.

[12] Passerini, E., Paleari, R., Martignoni, L., & Bruschi, D. (2008). FluXOR: Detecting and monitoring fast-flux service networks. *Proceedings of the 5th International Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*, 186–206. https://doi.org/10.1007/978-3-540-70542-0_10

[13] PhishTank. (2023). *PhishTank — a free community site for anti-phishing.* OpenDNS. https://www.phishtank.com

[14] Sabetta, A., & Bezzi, M. (2019). A practical approach to the automatic classification of security-relevant commits. *Proceedings of the 2019 IEEE International Conference on Software Maintenance and Evolution (ICSME)*, 579–583. https://doi.org/10.1109/ICSME.2019.00088

[15] Sandboxie Plus. (2023). *Sandboxie Plus — open source sandboxing software.* https://sandboxie-plus.com

[16] Sanders, C., & Smith, J. (2014). *Applied network security monitoring: Collection, detection, and analysis.* Syngress Publishing.

[17] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. *Proceedings of the 2010 IEEE Symposium on Security and Privacy*, 305–316. https://doi.org/10.1109/SP.2010.25

[18] Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice* (4th ed.). Pearson Education.

[19] Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, *72*, 212–233. https://doi.org/10.1016/j.cose.2017.09.001

[20] Bayer, U., Comparetti, P. M., Hlauschek, C., Kruegel, C., & Kirda, E. (2009). Scalable, behavior-based malware clustering. *Proceedings of the 16th Annual Network and Distributed System Security Symposium (NDSS)*, 1–18.