Engineering and Technology Journal e-ISSN: 2456-3358

Volume 11 Issue 06 June-2026, Page No.- 10658- 10665

DOI: 10.47191/etj/v11i06.42, I.F. – 8.595

Metadata-Based Characterization of Day–Night Internet Traffic Using Wireshark Capture and Python/Jupyter Analysis

Marwa K. Hasan

Technical Engineering College - Kirkuk, Northern Technical University, Kirkuk, 36001, Iraq

ABSTRACT: This study presents a packet level analysis of daytime and nighttime Internet traffic using Wireshark and processing in Python using Anaconda/Jupyter Notebook based on metadata. Three representative Internet scenarios were studied: a university website, a scientific website, and an educational YouTube video-streaming scenario. In each scenario, packet traffic was captured twice – on the same day, once during the day and once during the night. The acquired records were exported from Wireshark in CSV format and analyzed by means of several traffic indicators, e.g., total packet number, traffic volume, mean packet length, packet-size distribution, cumulative packet behavior, protocol composition and correlation patterns of packet rate and traffic volume. The results showed that the day-night traffic variation was highly dependent on the type of accessed service. For the University website packet count fell from 21760 during the day to 17250 at night, traffic volume fell from 17.99 MB to 10.78 MB. Scientific website also showed a reduction from 13887 to 10218 packets and 9.15 MB to 6.07 MB respectively. But YouTube traffic was increased at night with packet count increased from 25112 to 26875 and traffic volume increased from 21.46 MB to 24.84 MB. Protocol analysis showed that TCP and TLSv1.3 were dominant in University and Scientific traffic, whereas YouTube traffic showed a higher proportion of UDP and QUIC, especially in nighttime capture. Correlation analysis further confirmed that each website category produced a distinct temporal traffic signature. Overall, the proposed framework provides a reproducible and privacy-preserving approach for analyzing day–night Internet traffic behavior using Wireshark-captured metadata and Python-based visualization.

KEYWORDS: Wireshark; Network traffic analysis; Metadata-based traffic analysis; Packet-level analysis; Day–night traffic comparison; Python-based visualization; QUIC protocol.

I. INTRODUCTION

The rapid growth of Internet-based services has made network traffic analysis an essential task for understanding communication behavior, evaluating network performance, and identifying service-dependent traffic patterns. Modern users access different types of online services, including institutional websites, scientific platforms, cloud-based applications, and video-streaming services. Each service generates different packet-level characteristics in terms of packet count, packet length, protocol composition, traffic volume, and temporal activity. Therefore, packet-level traffic analysis provides useful insight into how different Internet services behave under real operating conditions.

Network performance can be affected by several factors, including excessive bandwidth consumption, traffic bursts, packet loss, retransmissions, latency, and throughput degradation. Ashaari et al. [1] analyzed the performance of a small office/home office network under multiple-device connections and showed that Wireshark-based traffic capture can be used to evaluate quality-of-service indicators such as packet transfer, round-trip time, latency, and throughput. Similarly, Tuli [2] used Wireshark to analyze network performance parameters in a home-based network environment and demonstrated the usefulness of Wireshark statistical tools for studying packet-level behavior and network integrity.

Wireshark is widely adopted as a packet-capture and traffic-analysis tool because it enables the collection of live network packets and provides detailed information such as packet time, source and destination addresses, protocol type, packet length, and packet information [3]. In addition to direct packet inspection, Wireshark allows captured records to be saved and exported into structured formats, making it suitable for further offline analysis. This capability is especially important when the goal is not only to look at the packets, but to set up a reproducible statistical workflow to compare the traffic behavior under different conditions.

In this context, Wireshark provides the packet acquisition layer and Python-based analysis in Anaconda/Jupyter Notebook provides the computational layer for preprocessing, feature extraction, statistical comparison and visualization. Anaconda Navigator provides a graphical user interface for managing Python environments and packages, and Jupyter Notebook supports interactive computational documents containing code, text, equations, and visualizations [4], [5]. The integration means that reproducible Python workflows can be applied to packet-level metadata exported from Wireshark, facilitating more systematic analysis than using just Wireshark interface statistics.

Due to the wide use of encryption, the direct inspection of payload is becoming more and more limited in modern Internet environments. Consequently, traffic analysis has shifted to metadata-based features such as packet timing, packet size, protocol type, packet rate, and traffic volume. Papadogiannaki and Ioannidis [6] reviewed encrypted network traffic analysis and emphasized the significance of traffic-analysis techniques following the widespread adoption of encrypted communication channels. TLS-encrypted traffic is a challenge for traditional inspection methods, especially in terms of security monitoring and traffic classification, as pointed out by Oh et al. [7]. Therefore, the analysis based on the metadata still has its value as it can expose the traffic behavior without reconstructing or looking into the private payload content. Modern transport protocols, especially in video-streaming

services, increase the importance of metadata-based traffic analysis. QUIC is a multiplexed and secure transport protocol built on UDP that provides structured communication, low latency connection establishment, network path migration, and built-in security mechanisms [8]. HTTP/3 encodes HTTP semantics over QUIC, and employs QUIC to provide confidentiality, integrity protection, peer authentication, and reliable delivery per stream [9]. Hence, the packet level behavior of multimedia services such as YouTube could be very different from normal browsing websites especially in terms of packet rate, packet length, traffic volume and protocol composition.

Packet-level analysis of network traffic is a vital method for understanding network behavior, debugging performance issues, and identifying unusual communication patterns. Sikos [10] gave a comprehensive survey on packet analysis for network forensics, and pointed out that the packet-level data can help network monitoring, intrusion detection, traffic reconstruction and pattern identification. This confirms the validity of packet-based analysis as a reliable method for studying communication behavior at different network layers.

Recent studies have also shown the practical value of Wireshark as a packet-capture and traffic-analysis tool. Mabsali et al. [11] investigated the effectiveness of Wireshark in detection of attacks and vulnerabilities in network traffic. It was shown that captured packets can be used to provide useful information for network monitoring and security assessment. Although their research mainly focused on detecting attacks, they argue for a wider use of Wireshark as a useful tool for extracting packet-level indicators, such as protocols, packet lengths and communication patterns.

Packet level analysis has also been used for modern Internet applications, especially applications generating dynamic and bursty traffic. Karamollahi et al. [12] used packet level traces from Wireshark to study Zoom traffic performance anomalies in a campus network environment. Their work demonstrated that packet-level traces are more easily understood in terms of traffic bursts, packet timing and variation in network load when looking at application behavior. This is relevant to the present study as institutional, scientific, and educational video streaming may have different temporal traffic signatures.

Also, previous work in network traffic logging and application-level measurements showed that traffic behavior is highly dependent on the type of online service being accessed. Web browsing, video conferencing and video streaming differ in data transfer mechanisms, session duration, protocol usage and user interaction and hence do not have the same packet patterns. Thus, it is important to compare different website categories to understand how the type of service influences the number of packets, traffic volume and distribution of packet sizes.

Video-streaming traffic is one of the most important categories of modern Internet traffic since it generally produces a higher traffic volume and more continuous data transfer than ordinary web browsing. Loh et al. [13] presented a YouTube dataset for modeling mobile streaming traffic and for streaming analysis. Their dataset included YouTube streaming measurements and highlighted the importance of studying video traffic using network-level and application-level information. This supports the inclusion of YouTube as a separate scenario in the present study because educational video streaming is expected to produce packet behavior that differs from university and scientific web browsing.

The transport protocol used for video delivery also affects streaming behavior. Chellappa and Bartos [14] compared DASH video streaming over HTTP/3/QUIC and HTTP/2/TCP. Their results showed that HTTP/3 over QUIC can improve some quality-of-experience indicators under certain network conditions, especially for low-latency streaming algorithms. This is important because the present results also showed a strong contribution of UDP/QUIC-related traffic in the YouTube scenario, especially during nighttime capture.

More recent research by Sidhu and Bentaleb [15] further examined video streaming over QUIC and showed that QUIC implementation, congestion control, and adaptive bitrate behavior can significantly influence video-streaming performance. These findings confirm that video-streaming traffic should not be analyzed in the same way as ordinary browsing traffic, because its packet-level behavior is affected by streaming logic, buffering, transport protocol selection, and network conditions.

Although previous studies have investigated Wireshark-based traffic analysis, packet-level monitoring, encrypted traffic, and video-streaming behavior, most of them focused on general network performance, security monitoring, application-specific traffic, or protocol-level evaluation. Limited attention has been given to comparing packet-level behavior across different website categories under two-time conditions within the same network environment. In particular, the difference between daytime and nighttime traffic behavior for institutional browsing, scientific browsing, and educational video-streaming traffic remains insufficiently investigated.

Therefore, this study investigates day–night variations in packet-level Internet traffic using Wireshark and Python-based analysis. Three representative Internet scenarios were selected: a university website, a scientific website, and an educational YouTube video-streaming scenario. For each scenario, packet traffic was captured twice on the same day: once during the daytime and once during the nighttime. The captured records were exported from Wireshark in CSV format and analyzed using Anaconda/Jupyter Notebook. The analysis focused on total packet count, total traffic volume, mean packet length, packet-length distribution, cumulative packet behavior, protocol composition, and correlation patterns of packet rate and traffic volume among website categories.

The main contribution of this study is the development of a simple, reproducible, and metadata-based framework for comparing daytime and nighttime Internet traffic behavior across different website categories. Unlike works relying primarily on Wireshark interface statistics, this work combines Wireshark packet acquisition with Python-based statistical visualization to provide a clearer comparative interpretation of temporal packet behavior, service-dependent traffic structure and protocol-level differences.

II. METHODOLOGY

A. Design of experiments and packet acquisition

This paper proposes an experimental framework, based on metadata, to compare the behavior of the Internet traffic in the day and at night, under controlled access conditions. We collected packet-level data using Wireshark and processed it in Python in the Anaconda/Jupyter notebook environment. Three typical Internet access scenarios were studied: a university website, a scientific website and an educational YouTube video streaming scenario. These scenarios were selected to represent different traffic patterns such as institutional browsing, scientific-content browsing, and educational multimedia streaming.

The packet traffic for each website category was captured twice on the same day, once during daytime and once during nighttime. This design was chosen to compare packet-level

network behaviour under two temporal conditions, while keeping the website category and the general network environment as consistent as possible. For each experiment, the selected website category was opened for approximately five to six minutes, while Wireshark was used to capture the packets transmitted through the selected network interface.

For consistency of experiments, the same computer, network connection, browser environment and capture procedure were used for all daytime and nighttime experiments. Packet capture was performed with background applications minimized to decrease non-relevant network activity.

The captured records consisted of the following standard packet-level metadata: packet number, timestamp, source address, destination address, protocol type, packet length, and packet information. The packet records were exported out of Wireshark at the end of each capture session in comma-separated values files. The analysis was limited to packet-level information based on the metadata (time, protocol, source, destination, and packet length). The privacy-oriented nature of the study was preserved, and no private payload content was reconstructed or inspected.

B. Experimental matrix and dataset structure

The final dataset includes six CSV files corresponding to three selected website categories under two temporal conditions. The first group was day time captures and the second group was night time captures collected the same day. Each CSV file had the following fields: number of packets, time, source address, destination address, protocol, packet length and packet information. These fields enabled the extraction of packet-count, traffic-volume, protocol-distribution and time-dependent traffic features.

C. Data preprocessing and feature extraction

The exported CSV files were imported to the Jupyter Notebook, a Python data-analysis environment. Preprocessing stage was designed to normalize the datasets before feature extraction. First of all CSV files were read in and checked for consistent column names. Then, each dataset was assigned with two categorical labels, i.e. the website category and the capture condition. The website categories were ordered as University, Scientific, and YouTube. The capture conditions were ordered as Day and Night.

The time column was used as the reference variable for temporal analysis. Traffic-volume indicators were derived by converting packet lengths to numerical values. Packet timestamps were aggregated into one-second bins for time-series analysis. This enabled us to compute the number of packets per second and the traffic volume per second for each website category and capture condition.

To describe the network behavior, several quantitative features were extracted from each packet-capture file. These were the total number of packets, total amount of traffic, average packet size, packet rate and traffic rate. These features were used to compare traffic intensity and packet-size behavior between daytime and nighttime capture conditions.

The main equations used in the analysis were:

$$T = t_{max} - t_{min} \quad (1)$$

$$B = \sum_{i=1}^{N} L_i \quad (2)$$

$$V_{MB} = B / 1024^2 \quad (3)$$

$$\bar{L} = B / N \quad (4)$$

$$R_p = N / T \quad (5)$$

$$R_b = 8B / (T \times 10^6) \quad (6)$$

where T is the capture duration in seconds; t_{max} and t_{min} are the maximum and minimum packet timestamps; N is the total number of packets; L_i is the length of packet i; B is the total traffic volume in bytes; V_{MB} is the total traffic volume in megabytes (MB); $\bar{L}$ is the mean packet length; R_p is the packet rate in packets per second; and R_b is the traffic rate in Mbps.

D. Protocol, time-series, and cumulative traffic analysis

Protocol-level behavior was examined by counting the occurrence of each protocol in every dataset. We identified the dominant protocols separately for each website category and capture condition. This analysis was important as different website categories generate different protocol signatures. For example, browsing-based traffic was mainly characterized by the presence of TCP and TLS-based packets, while YouTube traffic showed a more prominent presence of UDP and QUIC packets, reflecting the nature of the multimedia streaming and the modern encrypted transport mechanisms.

To study the temporal traffic behavior, packets were aggregated into one second bins. Then two time-dependent indicators were calculated: packets per second and traffic volume per second. The daytime and nighttime capture conditions were used as indicators to characterize the traffic intensity over time for each website category.

We also plotted cumulative packet curves to get an idea of the overall packet accumulation trend over the capture period. The steeper the cumulative curve, the higher the packet arrival rate. Flat parts indicate lower activity or temporary traffic pauses. This representation is useful to find differences on traffic stability and burst behavior between day and night network conditions.

E. Statistical reproducibility and visualization

The processed data were visualized in publication quality plots generated in Python. The graphical analysis consisted of grouped bar diagrams for total traffic volume and average packet length, superimposed histograms for packet-size comparison, time-series graphs for packets per second, cumulative packet-count graphs, protocol-distribution diagrams, and correlation heatmaps.

Correlation heatmaps were computed from per second packet-rate and traffic-volume series. The heatmaps were used to assess the similarity of the temporal traffic patterns of the three categories of websites in the daytime and night-time capture scenarios. The degree of similarity between traffic profiles was quantified by the Pearson correlation coefficient.

All the analysis steps were done in Jupyter Notebook to ensure reproducibility. The same code structure was applied to all datasets including file loading, preprocessing, feature extraction, statistical summarization and figure generation. Figures were prepared in Times New Roman font and exported at high resolution for journal submission. Final plots were saved as high-quality images, PNG and TIFF (600 dpi) with PDF versions retained when vector output was required.

F. Methodological limitations

While the capture sessions were designed to provide a consistent basis for comparison between daytime and nighttime traffic, the analysis remains limited to the specific network environment, browser activity, selected website categories, and capture durations used in this study.

TABLE I. SUMMARY OF THE COLLECTED WIRESHARK DATASETS

Condition	Website type	Duration (s)	Total packets	Total traffic (MB)	Mean packet length (bytes)	Packet rate (packets/s)	Traffic rate (Mbps)
Day	University	322.42	21,760	17.99	866.72	67.49	0.468
Night	University	334.90	17,250	10.78	655.58	51.51	0.270
Day	Scientific	329.67	13,887	9.15	691.08	42.12	0.233
Night	Scientific	306.15	10,218	6.07	622.45	33.38	0.166
Day	YouTube	358.50	25,112	21.46	895.92	70.05	0.502
Night	YouTube	367.27	26,875	24.84	969.16	73.18	0.567

The network traffic can be affected by background system activity, server-side behavior, cache status, local bandwidth fluctuation and user interaction with the website. Thus, the results should be interpreted as a controlled case study of packet behavior, not as a universal representation of all Internet traffic. In future work we may extend this analysis by increasing the number of websites, repeating captures over multiple days, controlling background traffic more strictly, and including additional statistical or machine-learning-based classification methods.

III. RESULTS AND DISCUSSION

This section presents a comparison of the captured network traffic at packet level during the day and night. The results are discussed in terms of temporal packet-rate behavior, traffic volume, packet-size distribution, cumulative packet behavior, protocol composition, and correlation patterns for the three selected Internet scenarios: University, Scientific, and YouTube.

A. Temporal packet-rate behavior

Figure 1 presents the temporal variation of packet rate for the University, Scientific, and YouTube traffic under daytime and nighttime conditions. The results show that packet activity was highly dynamic during the capture period and varied according to both the website category and the time of data collection.

For the University website, the daytime traffic showed stronger packet-rate bursts, particularly between approximately 3 and 4.5 min, indicating higher packet-generation activity during the daytime capture. In contrast, the nighttime University traffic exhibited lower overall activity, with intermittent bursts distributed over the capture period. This agrees with the total packet-count results, where the University traffic decreased from 21,760 packets during the day to 17,250 packets at night.

For the Scientific website, both daytime and nighttime captures showed burst-like behavior, especially at the beginning of the capture period. However, the daytime traffic maintained additional packet-rate bursts toward the later part of the experiment, while the nighttime traffic remained relatively lower after the initial activity. This confirms that the Scientific website generated higher packet activity during the daytime condition.

The YouTube traffic showed a different pattern from the University and Scientific websites. High packet-rate bursts appeared mainly at the early stage of the capture, which can be attributed to video loading and buffering behavior. The nighttime YouTube traffic also showed strong packet activity and more sustained fluctuations compared with the browsing-based websites. This behavior is consistent with the higher nighttime traffic volume observed for YouTube, where the total traffic increased from 21.46 MB during the day to 24.84 MB at night.

Overall, the time-series results indicate that ordinary browsing traffic produced intermittent packet-rate bursts, whereas YouTube video traffic exhibited more intensive and streaming-related packet activity. Therefore, the temporal packet behavior was strongly influenced by the type of Internet service as well as the day–night capture condition.

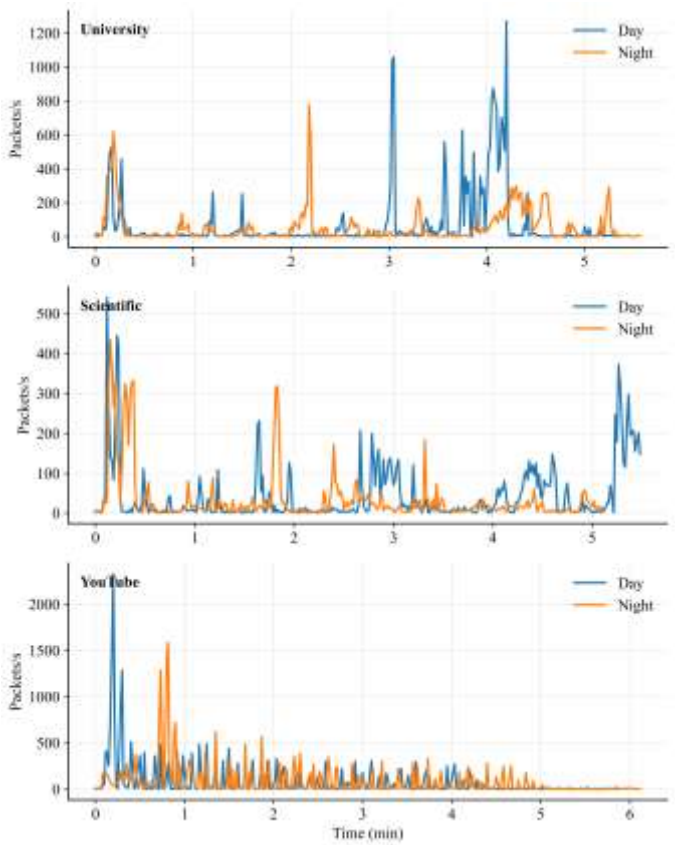


Figure 1. Temporal packet-rate profiles under day and night conditions

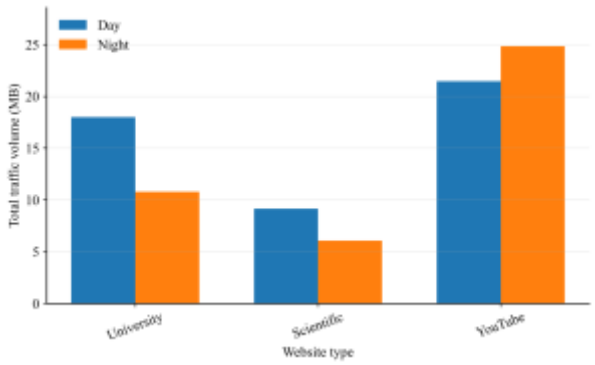
B. Traffic-volume and packet-size behavior

Figure 2 compares the total traffic volume and mean packet length for the University, Scientific, and YouTube scenarios under daytime and nighttime conditions. As shown in figure 2(a), the University and Scientific websites generated lower traffic volume at night compared with the daytime captures. For the University website, the total traffic volume decreased from 17.99 MB during the day to 10.78 MB at night, representing a reduction of approximately 40.1%. Similarly, the Scientific website decreased from 9.15 MB to 6.07 MB, corresponding to a reduction of about 33.7%.

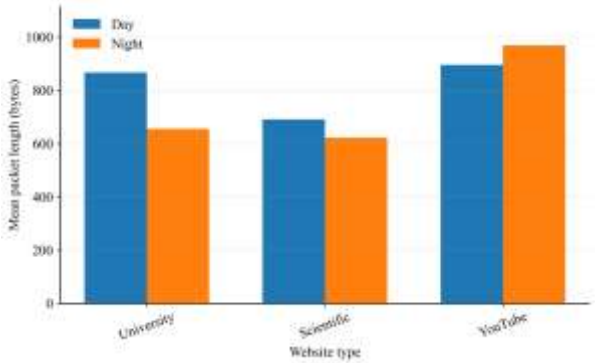
In contrast, YouTube showed an opposite trend, where the total traffic volume increased from 21.46 MB during the day to 24.84 MB at night. This indicates that the educational video-streaming

scenario produced stronger nighttime traffic intensity than the browsing-based websites.

Figure 2(b) shows that the mean packet length followed a similar service-dependent pattern. The University website reduced from 866.72 bytes during the day to 655.58 bytes at night while the Scientific website reduced from 691.08 bytes to 622.45 bytes. These reductions suggest that the packets in the night-time browsing traffic were relatively smaller, or that there were fewer large packets carrying data. Conversely, the average packet length of YouTube increased from 895.92 bytes in daytime to 969.16 bytes in nighttime, which is consistent with the higher traffic volume in nighttime as shown in figure 2(a). In summary, the results presented in figure 2 show a strong dependence of the day–night traffic variation on the Internet service type, with browsing-based traffic decreasing at night and video-streaming traffic increasing.



(a) total traffic volume



(b) mean packet length

Figure 2. Comparison of traffic volume and mean packet length between day and night: (a) total traffic volume, (b) mean packet length

C. Cumulative packet behavior

Figure 3 illustrates the cumulative packet-count profiles of University, Scientific and YouTube traffic during daytime and nighttime conditions. The cumulative plots provide a good representation of the accumulation of packet arrivals over the time of the capture for each website category. In general, steeper slope means higher packet arrival rate and flatter region means lower traffic activity.

The night-time curve of the University website showed more packet accumulation at the beginning and middle of the capture. However, the daytime curve increased sharply in the later stage, especially after about 240 s, and finally reached a higher final packet count than the nighttime curve. This confirms that the University scenario generated a larger total number of packets during the daytime capture despite the temporary nighttime increase at earlier periods.

Progressive packet accumulation was observed for day and night conditions for the Scientific website. The nighttime curve was higher for much of the capture period indicating a stronger early accumulation. However, the daytime curve increased more steeply towards the final stage and finished with a significantly higher total packet count. This behavior is consistent with the previous time-series results indicating more powerful late-stage packet bursts during the daytime capture.

The YouTube traffic showed a different cumulative pattern than the browsing-based websites. The curves for both day and night increased rapidly, reflecting the high packet activity of video-streaming traffic. The daytime curve had rapid early accumulation and the nighttime curve continued to accumulate steadily and eventually outperformed the daytime curve. This results in a slightly higher aggregate number of packets at night, which is in line with the earlier observed increase in nighttime traffic volume for YouTube.

In general, Figure 3 shows that the cumulative packet behavior varies with the website category and the time of capture. The University and Scientific websites had higher final cumulative packet counts during the daytime condition, while YouTube had slightly stronger cumulative packet activity at night, consistent with its video-streaming behavior.

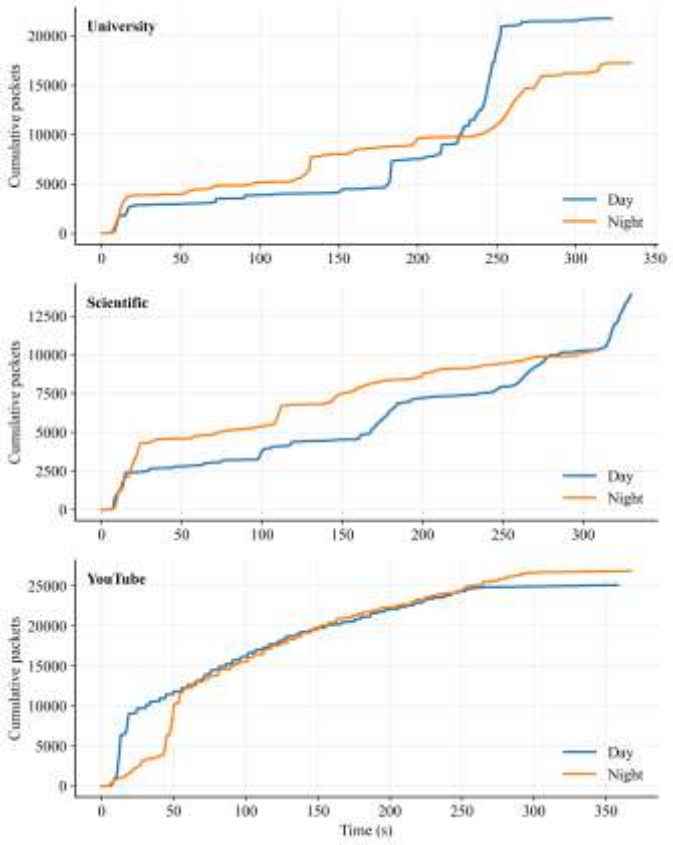


Figure 3. Day–night cumulative packet-count profiles.

D. Packet length frequency distribution

Figure 4 shows the packet length frequency distribution for the University, Scientific and YouTube traffic during day and night conditions. The histogram results show that the packet lengths were not evenly distributed but the traffic was mainly concentrated in two regions: small packets and large packets. Small packets are usually associated with control, acknowledgement, DNS, TLS handshaking, and connection-management traffic, while large packets are usually associated with traffic that carries data.

Both the university and scientific websites exhibited a high frequency of small packets in the daytime and nighttime captures, with large packets close to the maximum packet length

also playing a significant role. However, the distributions during the day were generally more prominent than the during the night, in particular for the large-packet region. This is consistent with the higher daytime traffic volume and packet activity reported earlier for these two browsing-based websites. Distribution was clearly different for the browsing-based sites, as opposed to YouTube. The histogram reveals a high concentration of large packets, particularly at the upper end of the packet-length range. This is due to the streaming nature of YouTube traffic where the delivery of video generates a large number of data carrying packets. The nighttime YouTube traffic showed the strongest large-packet concentration, confirming the earlier observation that YouTube generated high traffic volume at night.

Figure 4 shows the packet size distribution, which gives more information besides the total packet count. The University and Scientific websites presented mixed small and large browsing-related packets, while YouTube presented a stronger large-packet pattern associated with video-streaming traffic.

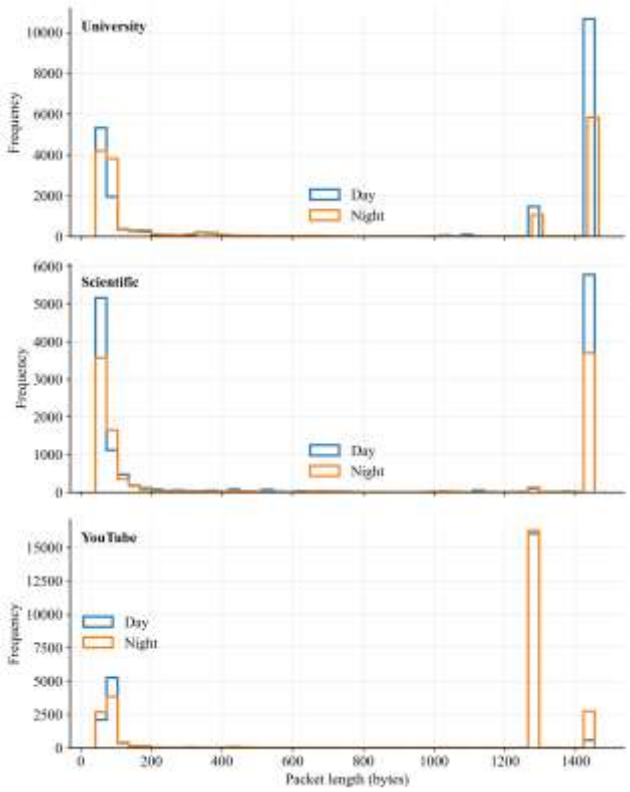


Figure 4. Day–night packet-length frequency distribution.

E. Protocol-composition analysis

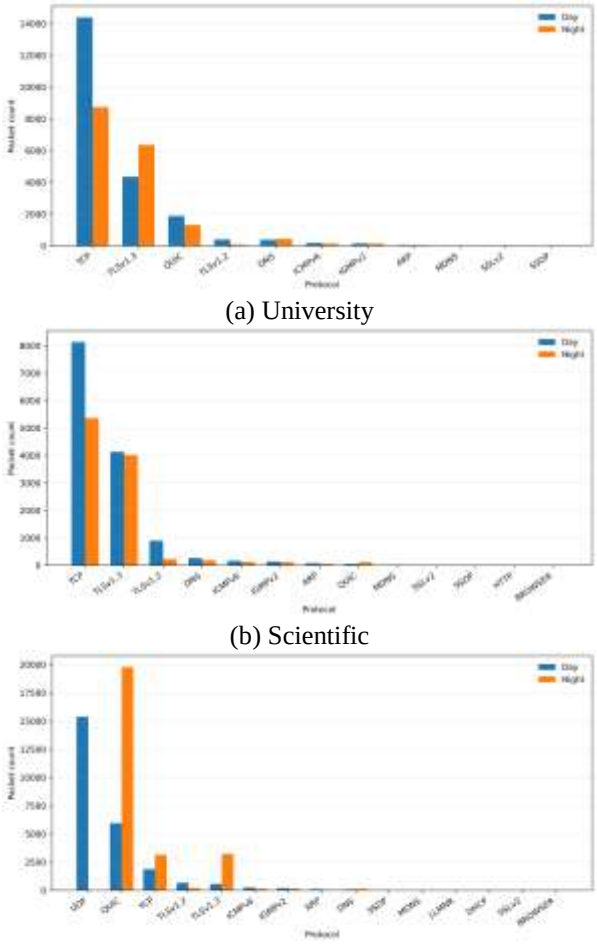
Figure 5 compares the protocol level packet-count of the three selected Internet scenarios under daytime and nighttime conditions. The results show that the dominant protocols were clearly different according to the category of the Web site and the time of capture.

On the University website, TCP was the dominant protocol in both daytime and nighttime captures, indicating that the traffic was mostly related to traditional connection-oriented web communication. However, the count of TCP packets dropped was high during the night while TLSv1.3 became more visible. Lower overall traffic volume suggests that encrypted web communication was still in progress at the time of the nighttime capture.

For the Scientific website, the dominant protocols were TCP and TLSv1.3. The daytime capture had more TCP packets than the nighttime capture, which is consistent with the previous results showing higher daytime packet activity and traffic volume. The presence of TLSv1.3 in both cases indicates that the Scientific website traffic was primarily encrypted browser-based communication.

The distribution of the YouTube protocol was significantly different than the University and Scientific websites. For the daytime capture, UDP and QUIC were the most common protocols, with UDP being the largest contributor. By contrast, in the nighttime capture, QUIC was the overwhelmingly dominant protocol. This behavior is typical for video-streaming traffic, where QUIC over UDP is frequently used for fast, encrypted multimedia delivery. The strong contribution of nighttime QUIC is consistent with the larger nighttime traffic volume and mean packet length observed previously.

In general, figure 5 shows that the protocol composition is strongly dependent on the Internet service type. University and Scientific traffic was largely TCP/TLS while YouTube traffic was dominated by UDP/QUIC related behavior particularly during nighttime video streaming.



(a) University

(b) Scientific

(c) YouTube

Figure 5. Day–night protocol packet-count comparison: (a) University, (b) Scientific, and (c) YouTube.

F. Packet Rate and Traffic Volume Correlation Analysis

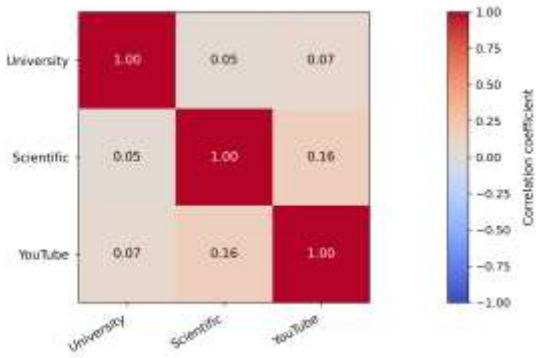
Figure 6 shows the correlation heatmaps for evaluating the similarity of temporal traffic behavior among the University, Scientific and YouTube scenarios. Each traffic pattern is perfectly correlated with itself, hence the diagonal entries are 1.00. The off-diagonal entries describe the similarity among different categories of websites. As shown in figure 6(a), the daytime packet-rate correlations were weak among the three websites. The highest correlation was observed between the Scientific and YouTube traffic, with a value of 0.16, while the University–Scientific and University–YouTube correlations

were only 0.05 and 0.07, respectively. This indicates that the three websites had largely independent packet-rate patterns during the daytime capture.

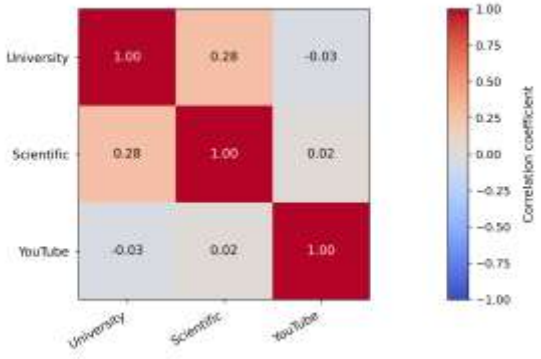
For the nighttime packet rate, figure 6(b) shows a slightly higher correlation between the University and Scientific websites, with a value of 0.28. This suggests that the two browsing-based websites shared more similar nighttime packet-rate behavior than YouTube. In contrast, YouTube remained weakly correlated with the other two websites, confirming its different streaming-related traffic pattern.

Figures 6(c) and 6(d) show the correlation heatmaps of traffic volume. During the day, the traffic-volume correlations were almost negligible, ranging from −0.01 to 0.02. At night, the University–Scientific correlation increased to 0.22, while the correlations involving YouTube remained close to zero. On the other hand, this confirms that YouTube traffic has a different pattern in the temporal volume than browsing based websites.

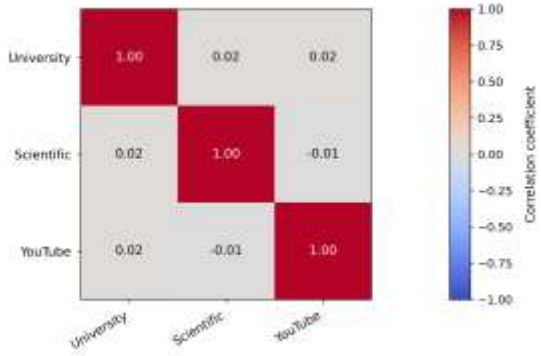
Figure 6 shows that overall, the temporal traffic signature of each website category was different. Low correlation values indicate that the behavior of the traffic was more strongly correlated with the type of internet service than with the capture time alone. The University and Scientific websites exhibited similar behavior throughout the night, while YouTube was the most distinguishable due to its video streaming nature.



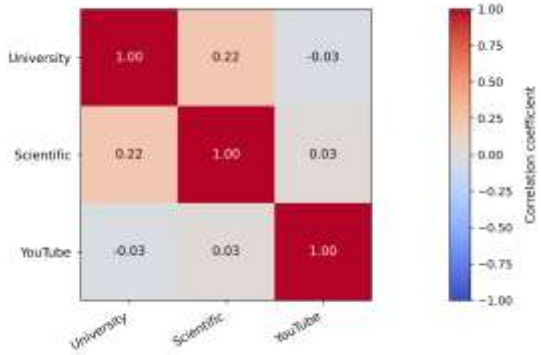
(a)



(b)



(c)



(d)

Figure 6. Correlation heatmaps of packet rate and traffic volume under day and night conditions: (a) packet rate during daytime, (b) packet rate during nighttime, (c) traffic volume during daytime, and (d) traffic volume during nighttime.

G. General discussion of the results

The combined results showed that the traffic behavior in the daytime and the nighttime were significantly different depending on the category of the website and the nature of the accessed Internet service. University and Scientific browsing traffic generally showed higher daytime activity in the number of packets, traffic volume and mean packet length. On the contrary, YouTube traffic showed a more pronounced nighttime behavior. This can be attributed to its video streaming nature and the dominant role of QUIC/UDP based communication. We found that each website category generates a unique temporal traffic signature in all the experiments we conducted, including packet-length distribution, cumulative packet profiles, protocol-composition results, and correlation analysis. This means that the time of capture plays a role not only on the behavior at packet level but also on the service type, communication protocol and traffic generation mechanism.

IV. CONCLUSION

This paper provides a comparative analysis of daytime and nighttime Internet traffic at the packet level using Wireshark and processing through Python in Anaconda/Jupyter Notebook. Different representative scenarios on the Internet were studied: a university website, a scientific website, and an educational video on YouTube. In all cases, packets were recorded twice on the same day, in the daytime and nighttime, and analyzed with several traffic indicators, such as packet count, traffic volume,

mean packet length, packet-size distribution, cumulative behavior, protocol composition, and correlation patterns.

The results showed that the variation of the day and night traffic was strongly dependent on the type of the accessed Internet services. Night-time activity was less than daytime captures for the University and Scientific websites. On the University website, the total packet count dropped from 21,760 packets to 17,250 packets, which is a decrease of about 20.7%. The traffic volume also dropped from 17.99 MB to 10.78 MB, which is a decrease of about 40.1%. Likewise, the Scientific website dropped from 13,887 to 10,218 packets and from 9.15 MB to 6.07 MB, which are decreases of 26.4% and 33.7%, respectively. On the other hand, there has been more activity on YouTube during night. The number of packets increased from 25112 to 26875 packets and the traffic volume increased from 21.46MB to 24.84MB. This was an increase of almost 7.0% and 15.8%.

The packet-size distribution, cumulative packet profiles and protocol-composition analysis confirmed that the differences observed were not a simple matter of traffic volume. In the University and Scientific traffic, TCP and TLSv1.3 were the dominant protocols, while in the YouTube traffic, UDP and QUIC had a higher contribution, especially at the nighttime capture. The correlation heatmaps also showed a weak similarity among the three website categories, indicating that each service generated a unique temporal traffic signature.

The results confirm that the time of capture and the type of accessed service influence the behavior of Internet traffic at the packet level. The proposed framework offers a simple, reproducible and privacy preserving approach for the analysis of Wireshark captured metadata using Python based visualization. Future work could extend this analysis to more websites, repeat captures over multiple days, test different network environments, and make use of machine-learning methods for automatic traffic classification and day–night pattern recognition.

REFERENCES

1. M. N. Ashaari, M. Kassim, R. Ab. Rahman, and A. R. Mahmud, "Performance Analysis on Multiple Device Connections of Small Office Home Office Network," Baghdad Science Journal, vol. 18, no. 4(Suppl.), pp. 1457–1464, 2021, doi: 10.21123/bsj.2021.18.4(Suppl.).1457.
2. R. Tuli, "Analyzing Network Performance Parameters Using Wireshark," International Journal of Network Security & Its Applications, vol. 15, no. 1, pp. 1–13, 2023, doi: 10.5121/ijnsa.2023.15101.
3. Wireshark Foundation, "Wireshark User's Guide," official documentation, accessed May 2026.
4. Anaconda, Inc., "Anaconda Navigator Documentation," official documentation, accessed May 2026.
5. Project Jupyter, "Jupyter Notebook Documentation," official documentation, accessed May 2026.
6. E. Papadogiannaki and S. Ioannidis, "A Survey on Encrypted Network Traffic Analysis: Applications, Techniques, and Countermeasures," ACM Computing Surveys, vol. 54, no. 6, Article 123, pp. 1–35, 2021, doi: 10.1145/3457904.
7. C. Oh, J. Ha, and H. Roh, "A Survey on TLS-Encrypted Malware Network Traffic Analysis Applicable to Security Operations Centers," Applied Sciences, vol. 12, no. 1, Article 155, 2022, doi: 10.3390/app12010155.
8. J. Iyengar and M. Thomson, "QUIC: A UDP-Based Multiplexed and Secure Transport," RFC 9000, Internet Engineering Task Force, 2021, doi: 10.17487/RFC9000.
9. M. Bishop, "HTTP/3," RFC 9114, Internet Engineering Task Force, 2022, doi: 10.17487/RFC9114.
10. L. F. Sikos, "Packet analysis for network forensics: A comprehensive survey," Forensic Science International: Digital Investigation, vol. 32, Article 200892, 2020, doi: 10.1016/j.fsidi.2019.200892.
11. N. A. L. Mabsali, H. Jassim, and J. Mani, "Effectiveness of Wireshark Tool for Detecting Attacks and Vulnerabilities in Network Traffic," in Proceedings of the 1st International Conference on Innovation in Information Technology and Business (ICIITB 2022), Advances in Computer Science Research, vol. 104, pp. 114–135, 2023, doi: 10.2991/978-94-6463-110-4_10.
12. M. Karamollahi, C. Williamson, and M. Arlitt, "Packet-Level Analysis of Zoom Performance Anomalies," in Proceedings of the 2023 ACM/SPEC International Conference on Performance Engineering, pp. 221–232, 2023, doi: 10.1145/3578244.3583725.
13. F. Loh, F. Wamser, F. Poignée, S. Geißler, and T. Hoßfeld, "YouTube Dataset on Mobile Streaming for Internet Traffic Modeling and Streaming Analysis," Scientific Data, vol. 9, Article 293, 2022, doi: 10.1038/s41597-022-01418-y.
14. S. Chellappa and R. Bartos, "Is QUIC Quicker with HTTP/3? An Empirical Analysis of Quality of Experience with DASH Video Streaming," in 2022 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 2022, doi: 10.1109/ANTS56424.2022.10227765.
15. J. S. Sidhu and A. Bentaleb, "Video Streaming Over QUIC: A Comprehensive Study," ACM Transactions on Multimedia Computing, Communications, and Applications, 2026, doi: 10.1145/3793674.