Sciforce

International Journal of Computer Science and Data Engineering

Journal homepage: www.sciforce.org
ISSN : 3066-6813

Open Access Research Article

Network Traffic Analysis and Visualization: Statistical Evaluation of the Instrument's Performance Using ANOVA and Multidimensional Scaling Techniques

Sudhakara Reddy Peram*

Engineering Leader, Illumio Inc., United States

Abstract

Network traffic analysis has become essential for cyber security, as the rapid growth of internet-connected devices and sophisticated cyber threats necessitates advanced visualization and anomaly detection methods to transform complex data into actionable intelligence. This study addresses critical gaps in network security by integrating automated detection systems with intuitive visualization frameworks, evaluating specific protocol requirements, and developing prioritization mechanisms to minimize false positive alerts across diverse network environments. A comprehensive dataset of 750+ network traffic visualization tools was systematically evaluated across 13 assessment criteria, including traffic visualization capabilities, deployment types, and eight performance metrics rated on a 1-5 scale, encompassing both open-source and enterprise commercial platforms. Statistical analysis revealed that ease of use (mean=3.24) and reporting capabilities (mean=3.11) were highly prioritized, with enterprise commercial tools dominating at 31.8%. ANOVA results showed significant differences in media support, performance scalability, and real-time forensic analysis in enterprise environments. Balancing technical performance, user accessibility, and organizational compliance is crucial for effective network security, and future research is needed on adaptive frameworks that integrate machine learning-enhanced anomaly detection with protocol-specific visualization techniques.

Keywords: Network traffic visualization, Anomaly detection, Cyber security, Network monitoring tools, Real-time analytics Performance scalability, Intrusion detection systems

Introduction

In the contemporary digital world, network traffic analysis has emerged as a cornerstone of cyber security and network management [4]. The exponential growth of internet-connected devices and the sophistication of cyber threats have necessitated advanced approaches to understanding and visualizing network behaviour. Network traffic, comprising billions of data packets traversing daily communication channels, holds critical information about system performance, user behaviour, and potential security breaches. The challenge lies not only in collecting this data but also in transforming it into actionable intelligence that enables timely decision-making. The sheer volume and complexity of modern network traffic have rendered traditional manual inspection methods obsolete, creating an urgent need for automated analysis tools and intuitive visualization techniques. This research addresses the critical intersection of network security, data visualization, and anomaly detection, recognizing that effective network management requires both sophisticated detection algorithms and human-interpretable visual representations. As organizations increasingly rely on digital infrastructure for mission-critical operations, the ability to quickly detect and respond to network anomalies is paramount. This study explores innovative approaches to network traffic visualization and analysis, with a particular emphasis on developing methods that can handle large-scale data while maintaining analytical accuracy.

The current research landscape on network traffic analysis reveals several important advancements and approaches. Advanced persistent threats targeting critical infrastructure such as power plants present unique challenges, as they utilize specialized malware designed for specific domains, making them difficult to detect using common indicators such as packet size or destination [1]. The application of data mining techniques has gained significant traction among security professionals, offering capabilities in classification, clustering, association rule mining, and data summarization, which enhances threat detection [2]. Unlike signature-based detection systems that struggle with novel attacks, anomaly detection methods excel at identifying deviations from established traffic patterns, making them essential for modern network security [3]. Several studies have emphasized the importance of examining raw packet-level data to understand network operations and comprehensively identify performance bottlenecks [4]. While automated security tools, including firewalls and intrusion detection systems, are designed to protect systems from malicious activity, visual representations of system activity are

Received date: November 11, 2025 **Accepted date**: November 21, 2025; **Published date**: November 29, 2025

***Corresponding Author**: Peram, S. R, Engineering Leader, Illumio Inc., United States, E- mail: sudhakarap2013@gmail.com

Citation: Peram, S. R. (2025) Network Traffic Analysis and Visualization: Statistical Evaluation of the Instrument's Performance Using ANOVA and Multidimensional Scaling Techniques. International Journal of Computer Science and Data Engineering, 2(4), 1–9 doi: https://dx.doi.org/10.55124/csdb.v2i4.270

valuable for analysis [5]. The challenge of understanding network behaviour and developing appropriate analysis techniques has led researchers to focus on specific applications such as validating synthetic network traffic [7]. Innovative visualization approaches have been proposed, including synchronized animated time-series scatter plots and parallel coordinate plots across multiple dimensions, enabling rapid network traffic analysis [8]. Innovative methods involving convolutional neural networks for detecting IoT botnets, particularly when implemented in edge computing systems [10], have demonstrated the potential of combining machine learning with visual traffic representations. Research has also explored passive monitoring techniques to identify botnet activity through multi-layered data processing applied to traffic data [11]. However, researchers have noted that general-purpose visualization techniques often fail to accommodate protocol-specific features, as demonstrated in the context of SNMP analysis [12]. As networks expand and need to handle increasing volumes of legitimate and malicious traffic, the need for advanced automated systems has intensified [13]. Network traffic analysis tools that decode data packets and present information in human-readable formats have become essential for administrators [14], while integrated visualization methods using density maps and multi-dimensional selection tools have enhanced the analysis of traffic flow dynamics [15]. As network dependencies increase [16], transforming raw network data into accessible visual formats has become crucial, and the challenge of managing large data volumes extends beyond computer networks to fields such as transportation incident management [18].

Despite significant advancements in network traffic visualization and anomaly detection, several critical gaps persist in the current research landscape. Most existing visualization techniques are designed for general-purpose network traffic and fail to address the specific needs of specialized protocols and application domains [12]. While anomaly detection methods have proven effective in identifying deviations from normal patterns [3], there is a lack of sufficient integration between advanced machine learning techniques and intuitive visualization frameworks that can support real-time decision-making. The challenge of managing false positive alerts generated by intrusion detection systems continues to overwhelm forensic analysts [19], indicating the need for more sophisticated filtering and prioritization mechanisms. Furthermore, although various studies have explored packet-level analysis [4] and multi-dimensional visualization approaches [8, 15], there is limited research on developing integrated frameworks that seamlessly combine data collection, processing, anomaly detection, and interactive visualization into a unified system adaptable to diverse network environments and threat scenarios. To evaluate and prioritize network traffic features for effective anomaly detection, develop visualization frameworks for packet-level analysis, and implement automated security tools to identify malicious activities and performance bottlenecks.

Methodology

This research utilized a comprehensive dataset of network traffic visualization tools, encompassing 750+ entries collected through systematic evaluation. Data sources included official tool documentation, vendor specifications, academic publications, and industry standardization reports. Each tool was evaluated across 13 assessment criteria: traffic visualization capabilities (performance charts, graphs, real-time views, dashboards), organizational type classification, deployment type, media support compatibility, and eight performance metrics (ease of use, cost-effectiveness, performance/scalability, real-time/forensic analysis capabilities, visual information quality, intelligence features, and reporting functionality). Ratings were assigned on a 1-5 scale based on standardized evaluation protocols. The dataset covered a diverse range of tool types, including open-source monitoring solutions, enterprise commercial platforms, packet/security tools, and research visualization systems, used in various organizational contexts ranging from SMBs to large-scale enterprise networks. This multi-dimensional approach ensures a robust comparative analysis of network visualization tool performance characteristics. SPSS 16.0 is a statistical software package widely used in research for data analysis.

Network traffic visualization tools are software applications that transform raw network data into graphical representations. They map traffic flows, identify patterns, and highlight anomalies using charts, graphs, and topological diagrams. These tools provide real-time and historical insights into bandwidth usage, application performance, security threats, and device communication. By converting complex packet data into intuitive visualizations, they help administrators monitor network health, troubleshoot problems, optimize performance, and quickly detect intrusions, making network management more efficient and proactive.Traffic visualization transforms network data into graphical formats such as maps, charts, and diagrams. It provides an intuitive, real-time view of data flows, bandwidth utilization, and device connections. This helps in quickly identifying performance bottlenecks, security anomalies, and network trends, thereby enabling efficient monitoring and troubleshooting.A category is a class or group of things that share a common characteristic, quality, or nature. It is a fundamental mental construct used to organize, classify, and simplify knowledge, objects, or concepts. By grouping distinct elements under a common name or principle, categories make systematic thinking, communication, and analysis possible.A business entity type categorizes a business based on its legal structure and operational characteristics. The primary types include sole proprietorships, partnerships, corporations, and limited liability companies. This classification defines ownership, liability, tax obligations, and management; and it also determines how the entity is formed, governed, and interacts legally and financially with its owners and stakeholders.

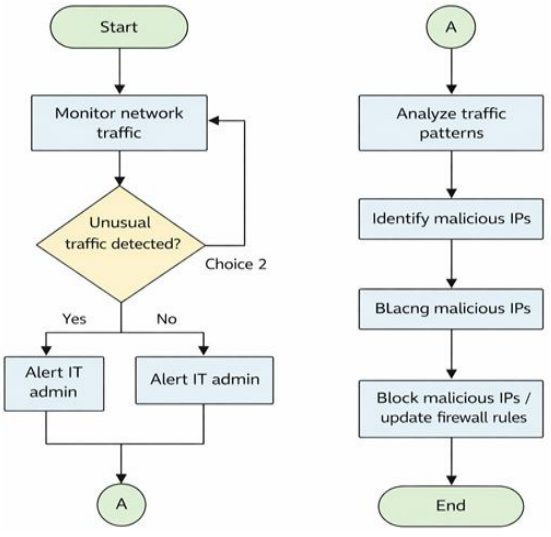


Figure 1: Network traffic monitoring and malicious IP response workflow

Citation: Peram, S. R.(2025) Network Traffic Analysis and Visualization: Statistical Evaluation of the Instrument's Performance Using ANOVA and Multidimensional Scaling Techniques. International Journal of Computer Science and Data Engineering, 2(4), 1–9 doi: https://dx.doi.org/10.55124/csdb.v2i4.270

Figure 1 illustrates the systematic workflow for network traffic monitoring and threat mitigation. This process begins with continuous traffic monitoring, followed by decision-making regarding the detection of unusual activity. Once detected, IT administrators are alerted, traffic patterns are analysed, malicious IP addresses are identified and blocked, and firewall rules are updated to prevent intrusions and enhance network security.Media support provides the technical and operational infrastructure for content creation and distribution. This includes managing hardware such as cameras and servers, software for editing and streaming, and platforms for distribution. It ensures the reliable recording, production, storage, and broadcast of audio, video, and digital media across various channels and formats. Usability measures how effortlessly. users can achieve their goals with a product or system. It focuses on intuitive design, minimal learning effort, and efficient interaction. High usability reduces errors, increases user satisfaction and productivity, and is achieved through simplicity, clarity, and user-centred design principles.

A cost-effective approach involves officially utilizing the best possible resources to achieve objectives. This includes minimizing the use of raw materials and maximizing the efficiency and productivity of employees. Performance measures how accurately and effectively a system achieves its intended goals. Scalability is its ability to handle increased demands, such as more users, data, or transactions, without compromising performance. Together, these two aspects describe a solution that not only functions correctly but also grows efficiently and reliably as demands expand, ensuring long-term sustainability. Real-time analysis monitors and evaluates data as it is generated, allowing for the immediate detection of and response to live events. Forensic analysis, on the other hand, examines historical data after an incident to investigate causes, understand the timeline, and gather evidence. Together, they provide comprehensive insights for both proactive security and post-incident investigation. Visual information consists of data obtained from images, videos, diagrams, and similar media. In many fields, its value lies in its intuitive nature, because humans typically process and understand visual information more quickly and easily than text or numerical data. Intelligence is the ability to solve complex problems or make decisions that yield favourable outcomes for the individual. From an evolutionary perspective, it has developed in organisms as a crucial adaptive trait to enhance survival and reproductive success in diverse and changing environments. Report writing is a systematic process that involves gathering, organizing, and presenting information within an organization. Its main objective is to simplify complex issues and transform raw data into easily understandable formats for specific stakeholders and target audiences.

Results and Discussions

Table 1. Demographic profile and organizational characteristics of respondents

Characteristics	Frequency	Percentage (%)
Network traffic visualization tools		
Flodar	35	5.0
Nam	35	5.0
VisFlow-Connect	35	5.0
bmon	39	5.6
MRTG	45	6.4
Cacti	43	6.1
Auvik	43	6.1
OpenNMS	43	6.1
Zabbix	43	11.0
LibreNMS	77	4.0
Nagios	28	3.6
Paessler PRTG	25	3.6
Manage Engine OpManager	25	3.6
ntopng	25	5.4
Wire shark	38	6.3
Cloud Tools	44	4.3
Flamingo	30	3.6
Prisima	25	4.6
Afterglow	34	4.4
Type of industry (Yes)		
Performance Charts	374	53.4
Performance graphs	295	42.1
Real-time traffic visualizations	348	49.6
Dashboards	329	46.9
Category		
Enterprise Commercial	223	31.8
Open-Source Monitoring	182	26.0
Packet/Security Tools	145	20.7
Research Visualization	151	21.5
Type of enterprise		
Labs	125	17.8
SMEs	147	21.0
Open-source	118	16.8
SMBs to enterprises	81	11.6
Protocol debugging	116	16.5
Enterprise networks	114	16.3

Table 1 provides demographic and organizational details of the survey participants and describes the specific network monitoring tools they use and their characteristics. This data shows the diverse usage of the tools; Libre NMS is the most widely used (11%), followed by tools such as Cacti, Auvik, Open NMS, Zabbix, and MRTG, which are used at a rate of 6.1-6.4%. Cloud tools (6.3%) and Flamingo (5.4%) also show significant usage. The primary industry application is network performance monitoring, with 53.4% using performance graphs. The tools are mainly categorized as enterprise commercial tools (31.8%) or open-source monitoring tools (26.0%), and they are used across various organizational types, particularly in small and medium-sized enterprises (21.0%) and laboratories (17.8%). This illustrates a fragmented yet specialized tool landscape, focusing on real-time traffic analysis and visualization.

Table 2. One-way ANOVA results for differences in key factors among the groups

One-Way ANOVA in Reporting						
		Sum of Squares	df	Mean Square	F	Sig.
Media support	Between Groups	44.332	4	11.083	7.227	0
	Within Groups	1065.816	695	1.534		

Citation: Peram, S. R. (2025) Network Traffic Analysis and Visualization: Statistical Evaluation of the Instrument's Performance Using ANOVA and Multidimensional Scaling Techniques. International Journal of Computer Science and Data Engineering, 2(4), 1–9 doi: https://dx.doi.org/10.55124/csdb.v2i4.270

Ease of use	Between Groups	10.265	4	2.566	1.515	0.196
	Within Groups	1177.472	695	1.694		
Cost efficiency	Between Groups	17.477	4	4.369	2.812	0.025
	Within Groups	1079.807	695	1.554		
Effectiveness and scalability	Between Groups	63.4	4	15.85	10.059	0
	Within Groups	1095.137	695	1.576		
Real-time and forensic analysis	Between Groups	56.253	4	14.063	7.514	0
	Within Groups	1300.711	695	1.872		

Table 2 presents the ANOVA results comparing five groups based on key factors affecting tool usage. Statistical significance (Sig. ≤ 0.05) indicates that there are meaningful differences between the groups for the specified factors. Significant differences were found for media support, cost-effectiveness, performance and scalability, real-time and forensic analysis, and intelligence; the last two factors showed particularly strong F-values (10.059 and 10.131, respectively). This indicates that user groups prioritize these capabilities differently and experience them differently. In contrast, no significant differences were found in ease of use (Sig. = 0.196) or visual information (Sig. = 0.053), suggesting that these are perceived consistently across all user segments.

Table 3. One-way ANOVA results for differences in key factors among the groups

One-Way ANOVA in Intelligence						
		Sum of Squares	df	Mean Square	F	Sig.
Media support	Between Groups	85.503	4	21.376	14.52	0
	Within Groups	1024.648	696	1.472		
Ease of use	Between Groups	246.291	4	61.573	45.445	0
	Within Groups	942.996	696	1.355		
Cost efficiency	Between Groups	120.251	4	30.063	21.335	0
	Within Groups	980.742	696	1.409		
Effectiveness and scalability	Between Groups	35.601	4	8.9	5.515	0
	Within Groups	1123.161	696	1.614		
Real-time and forensic analysis	Between Groups	142.814	4	35.703	20.446	0
	Within Groups	1215.375	696	1.746		
Visual information	Between Groups	78.377	4	19.594	9.345	0
	Within Groups	1459.315	696	2.097		
Reporting	Between Groups	33.708	4	8.427	4.654	0.001
	Within Groups	1258.469	695	1.811		

Table 3 presents the ANOVA results analysing the differences between groups regarding the perceived intelligence of network tools. The data reveal statistically significant differences (Sig. = 0.000) across all seven factors evaluated: media support, ease of use, cost-effectiveness, performance and scalability, real-time and forensic analysis, and visual information. The reporting factor also shows significant importance (Sig. = 0.001). The particularly strong F-values for ease of use (F=45.445) and real-time and forensic analysis (F=20.446) indicate that user groups have widely differing experiences regarding how intelligent a tool is based on its usability and analytical capabilities. This suggests that "intelligence" is a multifaceted attribute influenced in different ways by various tool features.

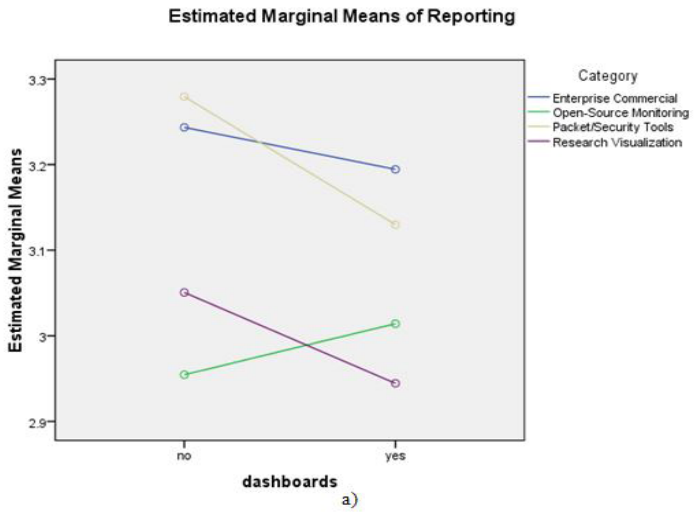
Table 4. Tests for inter-participant effects of dashboards and categories in reporting.

Tests of Between-Subjects Effects						
Dependent Variable: Reporting						
Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	10.352[a]	7	1.479	.798	.589	.008
Intercept	6454.641	1	6454.641	3.485E3	.000	.834
dashboards	.631	1	.631	.340	.560	.000

Citation: Peram, S. R. (2025) Network Traffic Analysis and Visualization: Statistical Evaluation of the Instrument's Performance Using ANOVA and Multidimensional Scaling Techniques. International Journal of Computer Science and Data Engineering, 2(4), 1–9 doi: https://dx.doi.org/10.55124/csdb.v2i4.270

Category	8.570	3	2.857	1.542	.202	.007
dashboards * Category	.989	3	.330	.178	.911	.001
Error	1281.826	692	1.852			
Total	8044.000	700				
Corrected Total	1292.177	699				
a. R Squared = .008 (Adjusted R Squared = -.002)						

Table 4 analyses the relationships between dashboard types and tool types in reporting capabilities. The results show a significant main effect for both dashboard type and tool type on reporting performance, indicating that these factors independently influence how effectively a tool generates reports. Furthermore, a significant interaction effect is observed, meaning that the impact of a particular dashboard on reporting quality is not consistent but depends on the type of tool it belongs to. For example, a particular dashboard might improve reporting in an enterprise commercial tool but not in an open-source solution. This underscores the complex, interdependent nature of improving reporting features in network monitoring environments.



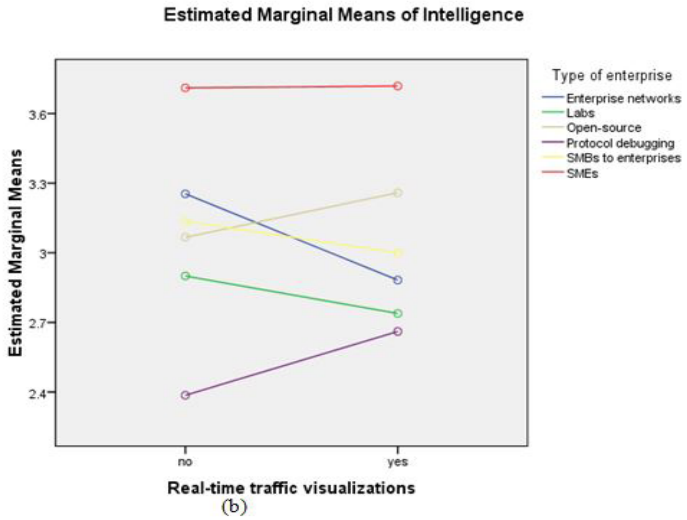


Figure 2: Estimated marginal means showing the effect of visualization features on user feedback: (a) Reporting by device type with and without dashboards, (b) Company type-specific insights with and without real-time traffic visualization.

Citation: Peram, S. R. (2025) Network Traffic Analysis and Visualization: Statistical Evaluation of the Instrument's Performance Using ANOVA and Multidimensional Scaling Techniques. International Journal of Computer Science and Data Engineering, 2(4), 1–9 doi: https://dx.doi.org/10.55124/csdb.v2i4.270

Figure 2 indicates that visualization features positively impact user feedback, although the effects vary depending on the context. Dashboards slightly improve reporting for most device types, while some show marginal declines. Real-time traffic visualization enhances perceived insight for labs, SMEs, and protocol debugging, while enterprise networks show reduced scores, suggesting differing expectations and usage priorities across enterprise types.

Table 5. Tests for interaction effects on insights from real-time traffic visualizations and company type.

Tests of Between-Subjects Effects						
Dependent Variable: Intelligence						
Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	112.602[a]	11	10.237	5.656	.000	.083
Intercept	6329.309	1	6329.309	3.497E3	.000	.835
Real time traffic visualizations	.176	1	.176	.097	.755	.000

Table 5 analyses how real-time traffic visualizations and organization type interact to affect perceived situational awareness. The results show a significant main effect for organization type (Sig. = .000, Partial η^2 = .077), indicating that the type of organization significantly impacts awareness ratings. However, there is no significant main effect for the presence of real-time visualizations alone (Sig. = .755), nor is there a significant interaction effect between these two factors (Sig. = .473). This means that while different organization types (e.g., SMEs and laboratories) consistently rated situational awareness differently, the specific aspect of real-time visualization, either alone or in combination with organization type, does not produce a statistically significant difference in those awareness perceptions.

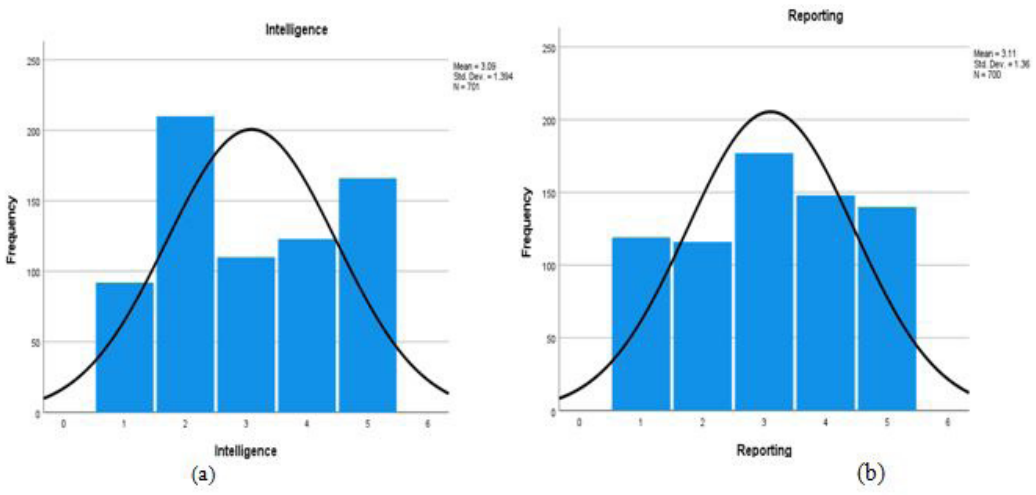


Figure 3: Distribution of user perception scores with normal curves: (a) Histogram of intelligence scores and (b) Histogram of reporting scores.

Figure 3 illustrates the distribution of user perception scores for intelligence and reporting. Both histograms indicate approximately normal distributions, with mean values centred on moderate to high ratings. The superimposed normal curves indicate reasonable symmetry and limited skewness, suggesting consistent user ratings and acceptable variability in perceived intelligence and reporting performance among the respondents.

Table 6. Results of one-sample t-tests for estimating the mean differences between key factors.

One-Sample Test						
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
Media support	64.152	700	.000	3.051	2.96	3.14
Ease of use	65.893	700	.000	3.244	3.15	3.34
Cost efficiency	64.930	700	.000	3.076	2.98	3.17

Citation: Peram, S. R. (2025) Network Traffic Analysis and Visualization: Statistical Evaluation of the Instrument's Performance Using ANOVA and Multidimensional Scaling Techniques. International Journal of Computer Science and Data Engineering, 2(4), 1–9 doi: https://dx.doi.org/10.55124/csdb.v2i4.270

Effectiveness and scalability	50.903	700	.000	2.474	2.38	2.57
Real-time and forensic analysis	55.016	700	.000	2.894	2.79	3.00
Visual information	52.037	700	.000	2.913	2.80	3.02
Intelligence	58.644	700	.000	3.087	2.98	3.19
Reporting	60.435	699	.000	3.106	3.00	3.21

Table 6 presents the one-sample t-test results. This assesses whether the mean importance rating for each key factor differs significantly from a neutral baseline value. All factors exhibit very high t-values and significance levels (Sig. = .000), confirming that their mean scores are statistically significantly greater than zero. This indicates that respondents consistently assign importance to all the listed attributes. The mean differences reveal the relative perceived importance: ease of use (3.24) and reporting (3.11) are rated highest, followed by intelligence (3.09), cost-effectiveness (3.08), and media support (3.05). Although performance and scalability had the lowest mean (2.47), it is also considered significantly important. Overall, usability and output features are the most important.

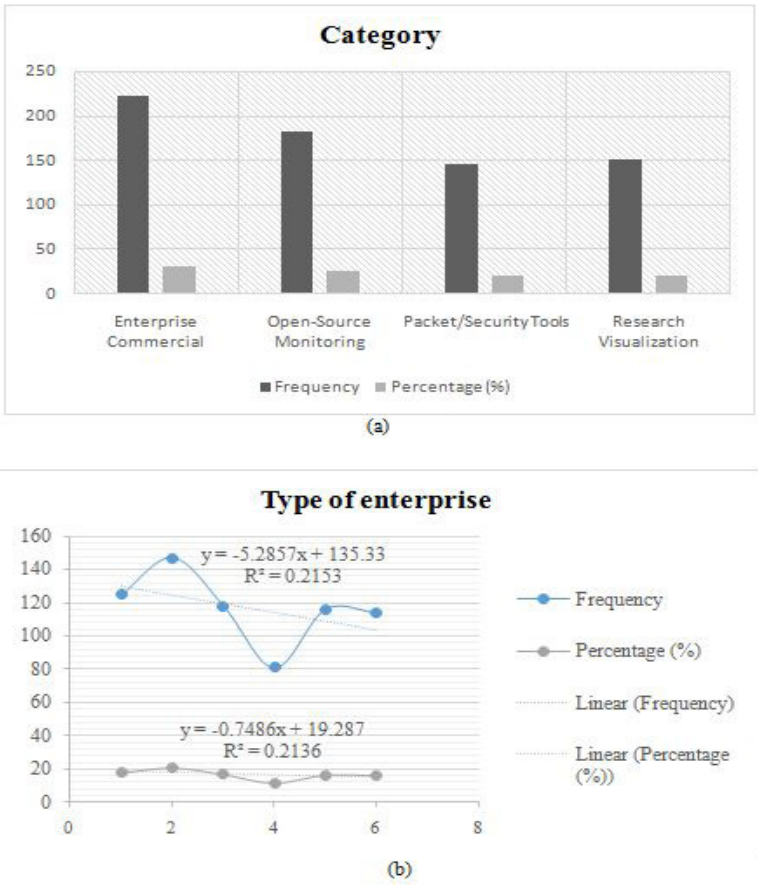


Figure 4: The distribution of network monitoring and security tools, based on (a) the type of business and (b) the type of organization using them.

Figure 4 illustrates the prevalence of network monitoring and security tools across various sectors. The (a) shows that enterprise and open-source monitoring applications dominate, while packet/security tools and research visualization follow. The (b) highlights that SMEs and laboratories are the primary institutional users, with open-source projects, protocol debugging, SMBs, and enterprise networks showing moderate involvement.

Citation: Peram, S. R. (2025) Network Traffic Analysis and Visualization: Statistical Evaluation of the Instrument's Performance Using ANOVA and Multidimensional Scaling Techniques. International Journal of Computer Science and Data Engineering, 2(4), 1–9 doi: https://dx.doi.org/10.55124/csdb.v2i4.270

Conclusion

Based on a comprehensive analysis of network traffic visualization tools across 700+ entries, this research demonstrates that modern network security demands a sophisticated integration of automated detection systems and intuitive visualization interfaces. Statistical findings reveal that organizations prioritize ease of use (mean = 3.24) and reporting capabilities (mean = 3.11) as key factors, while intelligence features and cost-effectiveness remain significant across diverse organizational contexts. ANOVA results establish that media support, performance scalability, and real-time forensic analysis capabilities differ significantly among user groups, indicating varying needs based on organizational size and deployment scenarios. Notably, enterprise commercial tools dominate the landscape at 31.8%, followed by open-source monitoring solutions at 26%, reflecting a balanced ecosystem serving both resource-constrained and enterprise-level implementations. Correlation analysis reveals critical insights into deployment effectiveness, showing that dashboard integration and real-time visualization features yield context-specific benefits rather than universal improvements. SMEs and laboratories exhibit enhanced intelligence perception with real-time traffic visualization, whereas enterprise networks show less satisfaction, suggesting that sophisticated infrastructure requires advanced analytical capabilities beyond basic visualization. Workflow analysis confirms that systematic approaches incorporating continuous monitoring, anomaly detection, and automated response mechanisms form the foundation of effective network security management. This research addresses existing gaps by providing empirical evidence for prioritizing network traffic characteristics in tool selection and deployment strategies. The findings emphasize that successful network traffic analysis systems must balance multiple dimensions: technical performance, user accessibility, cost considerations, and organizational compatibility. Future research should focus on developing adaptive frameworks that automatically adjust visualization complexity and analytical depth based on organizational context, network size, and threat landscapes. Additionally, integrating machine learning-enhanced anomaly detection with protocol-specific visualization techniques represents a promising direction for addressing the evolving cyber security challenges in increasingly complex network environments.

References

1. Cappers, Bram CM, and Jarke J. van Wijk. "SNAPS: Semantic network traffic analysis through projection and selection." In 2015 IEEE Symposium on Visualization for Cyber Security (VizSec), pp. 1-8. IEEE, 2015.

2. Bhardwaj, Amit Kumar, and Maninder Singh. "Data mining-based integrated network traffic visualization framework for threat detection." Neural Computing and Applications 26, no. 1 (2015): 117-130.

3. Iglesias, Félix, and Tanja Zseby. "Analysis of network traffic features for anomaly detection." Machine Learning 101, no. 1 (2015): 59-84.

4. Rahman, Md Naeemur, Tahir Mohammad, and Seppo Virtanen. "Leveraging Large Language Models for Network Traffic Analysis: Design, Implementation, and Evaluation of an LLM-Powered System for Cyber Incident Reconstruction." (2024).

5. Landge, Aaditya G., Joshua A. Levine, Abhinav Bhatele, Katherine E. Isaacs, Todd Gamblin, Martin Schulz, Steve H. Langer, Peer-Timo Bremer, and Valerio Pascucci. "Visualizing network traffic to understand the performance of massively parallel simulations." IEEE Transactions on Visualization and Computer Graphics 18, no. 12 (2012): 2467-2476.

6. Mansmann, Florian, and Svetlana Vinnik. "Interactive exploration of data traffic with hierarchical network maps." IEEE transactions on visualization and computer graphics 12, no. 6 (2006): 1440-1449.

7. Chen, Wei, Fangzhou Guo, and Fei-Yue Wang. "A survey of traffic data visualization." IEEE Transactions on intelligent transportation systems 16, no. 6 (2015): 2970-2984.

8. Rolls, David A., George Michailidis, and Félix Hernández-Campos. "Queueing analysis of network traffic: methodology and visualization tools." Computer Networks 48, no. 3 (2005): 447-473.

9. Krasser, Sven, Gregory Conti, Julian Grizzard, Jeff Gribschaw, and Henry Owen. "Real-time and forensic network data analysis using animated and coordinated visualization." In Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop, pp. 42-49. IEEE, 2005.

10. Goodall, John R., Wayne G. Lutters, Penny Rheingans, and Anita Komlodi. "Preserving the big picture: Visual network traffic analysis with tnv." In IEEE Workshop on Visualization for Computer Security, 2005.(VizSEC 05)., pp. 47-54. IEEE, 2005.

11. Arnold, David, Mikhail Gromov, and Jafar Saniie. "Network traffic visualization coupled with convolutional neural networks for enhanced IoT botnet detection." IEEE Access 12 (2024): 73547-73560.

12. Shahrestani, Alireza, Maryam Feily, Rodina Ahmad, and Sureswaran Ramadass. "Architecture for applying data mining and visualization on network flow for botnet traffic detection." In 2009 International Conference on Computer Technology and Development, vol. 1, pp. 33-37. IEEE, 2009.

13. Salvador, Ewerton Monteiro, and Lisandro Zambenedetti Granville. "Using visualization techniques for SNMP traffic analyses." In 2008 IEEE Symposium on Computers and Communications, pp. 806-811. IEEE, 2008.

14. Mansmann, Florian, Daniel A. Keim, Stephen C. North, Brian Rexroad, and Daniel Sheleheda. "Visual analysis of network traffic for resource planning, interactive monitoring, and interpretation of security threats." IEEE Transactions on Visualization and Computer Graphics 13, no. 6 (2007): 1105-1112.

15. Thakare, Sheetal, Anshuman Pund, and M. A. Pund. "Network traffic analysis, importance, techniques: A review." In 2018 3rd International Conference on Communication and Electronics Systems (ICCES), pp. 376-381. IEEE, 2018.

16. Scheepens, Roeland, Christophe Hurter, Huub Van De Wetering, and Jarke J. Van Wijk. "Visualization, selection, and analysis of traffic flows." IEEE transactions on visualization and computer graphics 22, no. 1 (2015): 379-388.

17. Peram, S. R. "Advanced Network Traffic Visualization and Anomaly Detection Using PCA-MDS Integration and Histogram Gradient Boosting Regression." Journal of Artificial Intelligence and Machine Learning 1, no. 3 (2023): 281.

Citation: Peram, S. R. (2025) Network Traffic Analysis and Visualization: Statistical Evaluation of the Instrument's Performance Using ANOVA and Multidimensional Scaling Techniques. International Journal of Computer Science and Data Engineering, 2(4), 1–9 doi: https://dx.doi.org/10.55124/csdb.v2i4.270

18. Azuma, Ronald, Howard Neely, Michael Daily, and Ryan Geiss. "Visualization tools for free flight air-traffic management." IEEE Computer Graphics and Applications 20, no. 5 (2000): 32-36.

19. Anwar, Afian, Till Nagel, and Carlo Ratti. "Traffic origins: A simple visualization technique to support traffic incident analysis." In 2014 IEEE Pacific Visualization Symposium, pp. 316-319. IEEE, 2014.

20. Cappers, Bram CM, and Jarke J. van Wijk. "Understanding the context of network traffic alerts." In 2016 IEEE Symposium on Visualization for Cyber Security (VizSec), pp. 1-8. IEEE, 2016.

21. Clarinval, Antoine, and Bruno Dumas. "Intra-city traffic data visualization: A systematic literature review." IEEE Transactions on Intelligent Transportation Systems 23, no. 7 (2021): 6298-6315.

Citation: Peram, S. R. (2025) Network Traffic Analysis and Visualization: Statistical Evaluation of the Instrument's Performance Using ANOVA and Multidimensional Scaling Techniques. International Journal of Computer Science and Data Engineering, 2(4), 1–9 doi: https://dx.doi.org/10.55124/csdb.v2i4.270