Universidad Continental

FACULTAD DE INGENIERÍA

Escuela Académico Profesional de Ingeniería de Sistemas e Informática

Tesis

Security Evaluation of Open Access Wi-Fi Networks in a Public University in Junin, Peru

Brayan Marlon Aguilar Solis
Fabrizio Arnaldo Orcada Vega
Carlos Daniel Guevara Chamorro
Deyby Maycol Huamanchahua Canchanya
Héctor José Valcárcel Castillo

Para optar el Título Profesional de
Ingeniero de Sistemas e Informática

Huancayo, 2024

INFORME DE CONFORMIDAD DE ORIGINALIDAD DE TRABAJO DE INVESTIGACIÓN

A : Decano de la Facultad de Ingeniería
DE : Job Daniel Gamarra Moreno
Asesor de trabajo de investigación
ASUNTO : Remito resultado de evaluación de originalidad de trabajo de investigación
FECHA : 26 de Junio de 2024

Con sumo agrado me dirijo a vuestro despacho para informar que, en mi condición de asesor del trabajo de investigación:

Título:
"Security Evaluation of Open Access Wi-Fi Networks in a Public University in Junin, Peru "

URL / DOI:
10.1109/INTERCON59652.2023.10326029

Autores:
1. Brayan Marlon Aguilar Solis – EAP. Ingeniería de Sistemas e Informática
2. Fabrizio Arnaldo Orcada Vega – EAP. Ingeniería de Sistemas e Informática
3. Carlos Daniel Guevara Chamorro – EAP. Ingeniería Mecatrónica
4. Deyby Maycol Huamanchahua Canchanya – EAP. Ingeniería Mecatrónica
5. Héctor José Valcárcel Castillo – EAP. Ingeniería Mecatrónica

Se procedió con la carga del documento a la plataforma "Turnitin" y se realizó la verificación completa de las coincidencias resaltadas por el software dando por resultado 11 % de similitud sin encontrarse hallazgos relacionados a plagio. Se utilizaron los siguientes filtros:

• Filtro de exclusión de bibliografía	SI □	NO ☒
• Filtro de exclusión de grupos de palabras menores N° de palabras excluidas **(en caso de elegir "SI")**:	SI □	NO ☒
• Exclusión de fuente por trabajo anterior del mismo estudiante	SI ☒	NO □

En consecuencia, se determina que el trabajo de investigación constituye un documento original al presentar similitud de otros autores (citas) por debajo del porcentaje establecido por la Universidad Continental.

Recae toda responsabilidad del contenido del trabajo de investigación sobre el autor y asesor, en concordancia a los principios expresados en el Reglamento del Registro Nacional de Trabajos conducentes a Grados y Títulos – RENATI y en la normativa de la Universidad Continental.

Atentamente,

La firma del asesor obra en el archivo original
(No se muestra en este documento por estar expuesto a publicación)

Security Evaluation of Open Access Wi-Fi Networks in a Public University in Junin, Peru

Brayan Aguilar
Department of Systems and Computer Engineering
Universidad Continental
Huancayo, Perú
72773177@continental.edu.pe

Fabrizio Orcada
Department of Systems and Computer Engineering
Universidad Continental
Huancayo, Perú
73144681@continental.edu.pe

Carlos Chamorro
Department of Mechatronics Engineering
Universidad Continental
Huancayo, Perú
72123851@continental.edu.pe

Deyby Huamanchahua
Department of Electrical and Mechatronics Engineering
Universidad de Ingenieria y Tecnologia - UTEC
Lima, Perú
dhuamanchahua@utec.edu.pe

Hector Valcarcel-Castillo
Department of Mechatronics Engineering
Universidad Continental
Huancayo, Perú
hvalcarcel@continental.edu.pe

***Abstract*—This article develops a topic of interest for users who can access the Internet and do not know the dangers of connecting to a free access network where the administrator of this is unknown, so a connection to this network would not be recommended. The central theme of this research is to demonstrate the risks of connecting to unknown access networks. The methodology used was the evaluation of how many users were being connected to the network created to monitor. The data obtained from users already connected have also been evaluated. According to the days they were connected through the networks, there is a strong demand for connected users. The conclusions show that some users are unaware of the dangers of connecting to one of these networks mentioned above and the risk of the amount of information that a person connected to the same network can obtain with the help of programs already created for its correct use. This work is a product of evaluating the dangers of connecting to an unknown network in Huancayo, Peru.**

Keywords—Data, Network, Traffic, Security evaluation, Open access.

I. Introduction

In today's hyper-connected world, the internet has become an integral part of our daily lives, serving as a bridge that links us to a vast array of activities—from managing work emails and exchanging crucial documents to engaging in social media and seeking instant information. The ubiquity of this connectivity, however, raises important questions about the risks associated with accessing the internet from unreliable networks, as opposed to the perceived safety of trusted environments like our homes. This interconnectedness has transformed into a necessity, yet the security challenges faced, especially in public networks provided as supplementary services, are often overlooked [1][2][3].

This article delves into the comprehensive landscape of network security, highlighting the intricate protocols impacting various layers of networks worldwide [4][5]. Proposals such as Wireless Intrusion Detection Systems (WIDS) are explored as effective methods to mitigate risks associated with public internet networks, addressing vulnerabilities that could be exploited to compromise network availability [6][7].

The research presented here is distinct in its focus on Huancayo, providing new insights into security concerns in public Wi-Fi networks that may differ from studies conducted elsewhere [8]. The aim is to shed light on the data obtainable in freely accessible Wi-Fi networks, utilizing tools like Wireshark and delving into the layers of the OSI model to assess security levels and understand the protocols at play [9][10].

Through compelling visuals, we present a stark reality—numerous locations where individuals, particularly students relying on university-provided free Wi-Fi, are potentially exposed to security risks [11]. This exploration seeks to not only reveal the vulnerabilities but also prompt a critical examination of security practices in prominent institutions like universities and large public spaces [12].

As we navigate this exploration of internet security, it becomes evident that the landscape is constantly evolving, presenting both challenges and opportunities. With the growing dependence on digital connectivity, understanding the nuances of network security is paramount. This research not only aims to uncover potential threats in public Wi-Fi networks but also to contribute to the broader discourse on safeguarding our interconnected world. By delving into the specific context of Huancayo and employing tools that reveal the intricacies of network traffic, we strive to empower users, institutions, and policymakers with knowledge that can enhance the resilience of our digital infrastructure. Together, let's delve deeper into the layers of security, unveiling insights that can shape a more secure and interconnected future.

Join us on this journey as we unravel the intricate web of internet security, providing a fresh perspective on the challenges and solutions that impact us all.

II. Methodology

For the evaluation of the security in Wi-Fi networks [13] with free access, the following was taken into consideration:

978-8-3503-1557-8/23/$31.00 ©2023 IEEE

It can be seen how the users (victim) and users (intruder) can be simultaneously logged, one in the program where personal information can be observed and the other into a social media interface when entering the Log-in data of the victim user. Taking this into consideration, the intruding user can access the Log-in information of the victim user and can watch every personal data previously submitted into the victim user account, as shown explicitly in the following figure. (Refer to Figure 1); it is demonstrated how these processes work in a flow chart.

The flow chart, with its unique lines, figures, charts, and information, was made using a program named Microsoft Visio which is very known because of the reliable, famous, and stable diagramming tool [14] primarily to create flow charts and every kind of diagram as this one shown below.

There are several areas in the university where any student can access the Wi-Fi signal and be able to enter their personal information into a log-in interface. Intruders may give the data captured a lousy use. The process of reaching the information capture is easy to understand and complete. There are also some images below, which are related to the explanation given before.

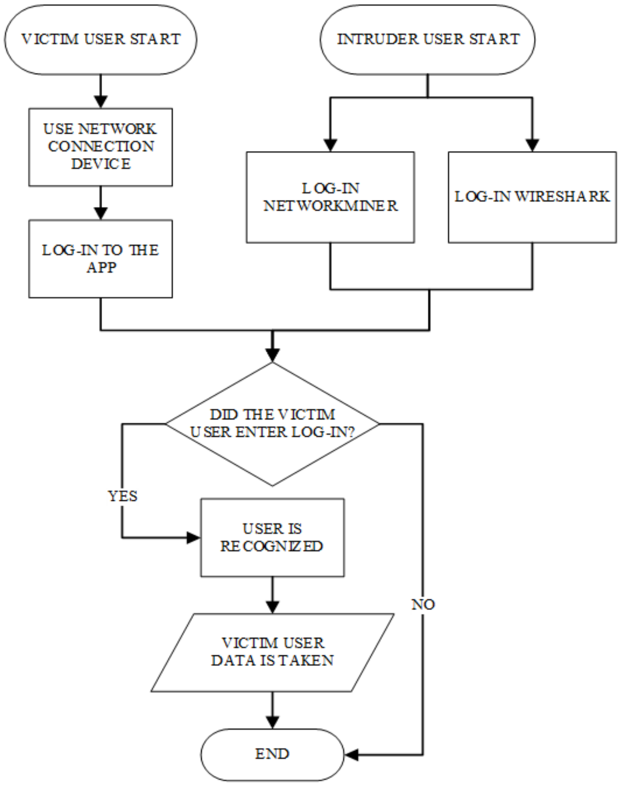


Fig. 1. Flow chart of the user data capture process

A. Participants

This snapshot of our investigation stems from the dynamic hub of connectivity provided by the Continental University's free Wi-Fi network in Huancayo [15]. Picture this: a bustling environment where students, the primary protagonists in our study, seamlessly interweave their academic pursuits with the convenience of free Wi-Fi. Take a glance at Figure 2—a beacon indicating the availability of this invaluable resource. Now, imagine stepping into the vibrant recreational space of Hall I (see Figure 3), where our initial samples were gathered—a melting pot of ideas, collaboration, and Wi-Fi connectivity. But that's not all—Figure 4 unveils another hotspot, Pavilion E's courtyard, a rendezvous point for more students tapping into the allure of free Wi-Fi. Join us as we journey through these visual narratives, capturing the essence of connectivity within the vibrant confines of Continental University.

Fig. 2. Referential image Wi-Fi zone indicator.

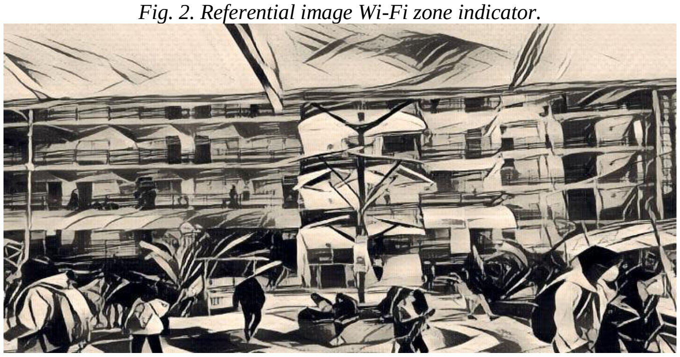


Fig. 3. Referential image place one for student recreation.

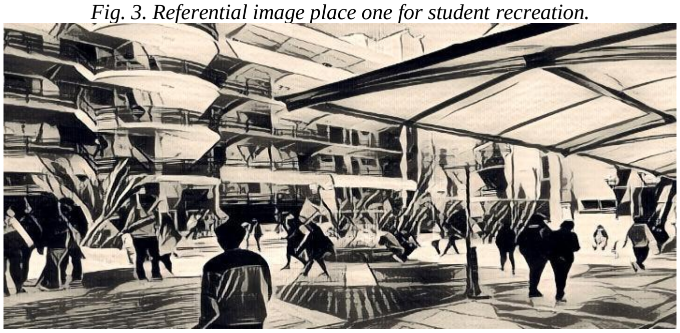


Fig. 4. Referential image place two for student recreation.

B. Design

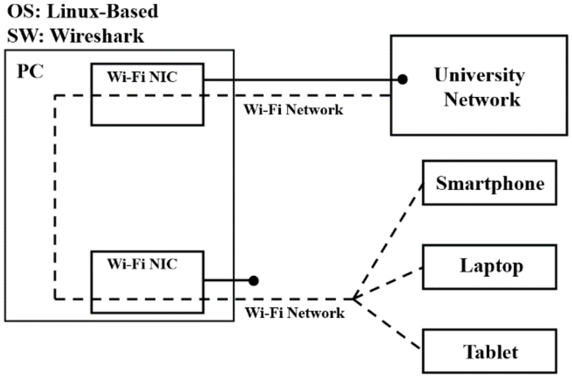
For the current research, we employed the Wireshark program on a Linux operating system to capture packets. Subsequently, we utilized a program on the Windows platform to visualize the previously captured data traffic. Wireshark [16, 17] stands out as software designed for analyzing communication network protocols, presenting data with its entire structure in an orderly and specific manner. The operation of the Wireshark software allows for the examination of the traffic that existed at the specific time of analysis. The chosen network served as the focal point for scrutinizing data and

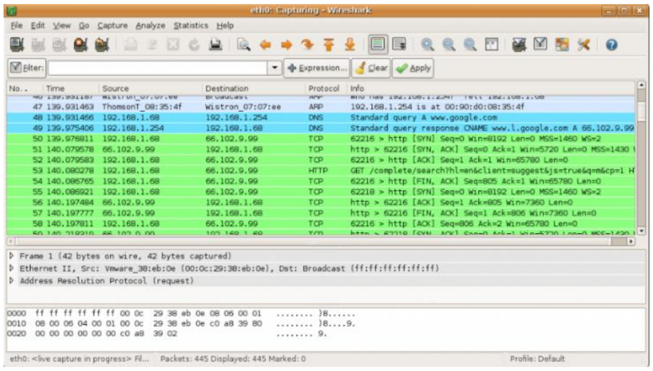
978-8-3503-1557-8/23/$31.00 ©2023 IEEE

discerning unique characteristics during instances when students were actively logged into their respective accounts. In Figure 5, witness the intricacies of connecting electronic devices via Wi-Fi [18], a process meticulously analyzed using the Wireshark software.

Fig. 5. Referential image of the use of the Wireshark program in Linux.

When utilizing Wireshark, the visualization of information in the capture console reveals distinct colors, each indicative of the type of packet or protocol in the collected data. Red packages signify errors, green packages represent TCP, yellow packages denote UDP, blue packages correspond to ICMP, and gray packages signify low-level protocol packets. A reference figure (refer to Figure 6) illustrates how data is collected and categorized based on these color-coded distinctions.



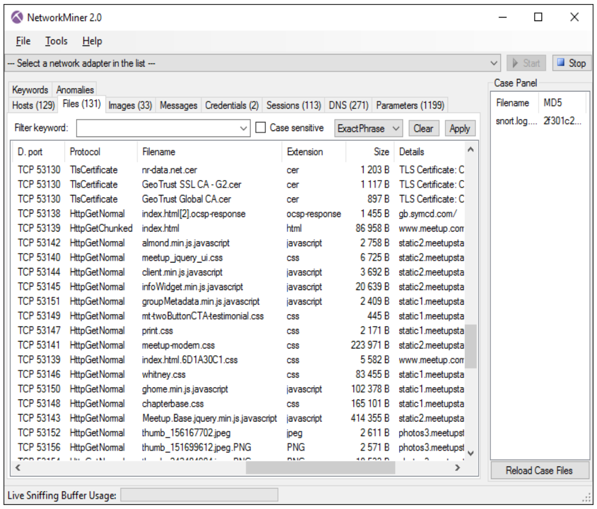

eth0: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply

```
No. .  Time        Source             Destination       Protocol  Info
 47 139.931463  ThomsonT_08:35:4f  Wistron_07:07:ee  ARP       192.168.1.254 is at 00:90:d0:08:35:4f
 48 139.931466  192.168.1.68       192.168.1.254     DNS       Standard query A www.google.com
 49 139.975406  192.168.1.254      192.168.1.68      DNS       Standard query response CNAME www.l.google.com A 66.102.9.99
 50 139.976811  192.168.1.68       66.102.9.99       TCP       62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
 51 140.079578  66.102.9.99        192.168.1.68      TCP       http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430
 52 140.079583  192.168.1.68       66.102.9.99       TCP       62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
 53 140.080278  192.168.1.68       66.102.9.99       HTTP      GET /complete/search?hl=en&client=suggest&js=true&q=m&cp=1 H
 54 140.086765  192.168.1.68       66.102.9.99       TCP       62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
 55 140.086921  192.168.1.68       66.102.9.99       TCP       62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
 56 140.197484  66.102.9.99        192.168.1.68      TCP       http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
 57 140.197777  66.102.9.99        192.168.1.68      TCP       http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
 58 140.197811  192.168.1.68       66.102.9.99       TCP       62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0

▷ Frame 1 (42 bytes on wire, 42 bytes captured)
▷ Ethernet II, Src: Vmware_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▷ Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 00 0c  29 38 eb 0e 08 06 00 01   ........ )8......
0010  08 00 06 04 00 01 00 0c  29 38 eb 0e c0 a8 39 80   ........ )8....9.
0020  00 00 00 00 00 00 c0 a8  39 02                     ........ 9.

eth0: <live capture in progress> Fil...   Packets: 445 Displayed: 445 Marked: 0        Profile: Default
```

Fig. 6. Referential image of the use of the Wireshark program in Linux.

C. Instruments

The capturing of network traffic was executed using the Wireshark program [19, 20]. To facilitate a more user-friendly examination of the traffic packets collected from the university's free Wi-Fi network, the NetworkMiner tool was deployed [21, 22, 23]. NetworkMiner, a specialized software, is employed to structure and organize the data gleaned from the Wireshark program, enhancing the overall clarity and tidiness of the information for subsequent analysis [24]. Following this, the compiled information from the connected network is presented within a specified time range, revealing the extension and type of [25] utilized in each transmitted packet (Refer to Figure 7).



D. port	Protocol	Filename	Extension	Size	Details
TCP 53130	TlsCertificate	nr-data.net.cer	cer	1 203 B	TLS Certificate: C
TCP 53130	TlsCertificate	GeoTrust SSL CA - G2.cer	cer	1 117 B	TLS Certificate: C
TCP 53130	TlsCertificate	GeoTrust Global CA.cer	cer	897 B	TLS Certificate: C
TCP 53138	HttpGetNormal	index.html[2].ocsp-response	ocsp-response	1 455 B	gb.symcd.com/
TCP 53139	HttpGetChunked	index.html	html	86 958 B	www.meetup.com
TCP 53142	HttpGetNormal	almond.min.js.javascript	javascript	2 758 B	static2.meetupsta
TCP 53140	HttpGetNormal	meetup_jquery_ui.css	css	6 725 B	static2.meetupsta
TCP 53144	HttpGetNormal	client.min.js.javascript	javascript	3 692 B	static2.meetupsta
TCP 53145	HttpGetNormal	infoWidget.min.js.javascript	javascript	20 639 B	static2.meetupsta
TCP 53151	HttpGetNormal	groupMetadata.min.js.javascript	javascript	2 409 B	static1.meetupsta
TCP 53149	HttpGetNormal	mt-twoButtonCTA-testimonial.css	css	445 B	static1.meetupsta
TCP 53147	HttpGetNormal	print.css	css	2 171 B	static1.meetupsta
TCP 53141	HttpGetNormal	meetup-modern.css	css	223 971 B	static2.meetupsta
TCP 53139	HttpGetNormal	index.html.6D1A30C1.css	css	5 582 B	www.meetup.com
TCP 53146	HttpGetNormal	whitney.css	css	83 455 B	static1.meetupsta
TCP 53150	HttpGetNormal	ghome.min.js.javascript	javascript	102 378 B	static1.meetupsta
TCP 53148	HttpGetNormal	chapterbase.css	css	165 101 B	static1.meetupsta
TCP 53143	HttpGetNormal	Meetup.Base.jquery.min.js.javascript	javascript	414 355 B	static2.meetupsta
TCP 53152	HttpGetNormal	thumb_156167702.jpeg	jpeg	2 611 B	photos3.meetupst
TCP 53156	HttpGetNormal	thumb_151699612.jpeg.PNG	PNG	2 571 B	photos3.meetupst

Filename	MD5
snort.log....	2f301c2...

Fig.7. Referential image of the use of the NetworkMiner program.

D. Procedure

Upon initiating the program, the selection of the network card to be employed is a crucial step [26]. The subsequent observation involves tracking the pages visited by users connected to the network. Upon identifying a potential target, the program patiently awaits their access to social media platforms. Once the victim engages in social media activities, such as entering a username and password [27, 28], the program captures the necessary information during the log-in process, utilizing the HTTP web page access protocol. The comprehensive flowchart depicting the general process employed to extract data from an individual within the network, monitored by the Wireshark software, is illustrated below (Refer to Figure 8). This methodological approach emphasizes a careful and ethical process of data acquisition within the monitored network. It's important to underscore that these actions are conducted for research purposes, aiming to understand potential vulnerabilities rather than for any malicious intent. By visualizing the step-by-step flowchart, we gain insights into how data is collected during routine online activities. This process not only highlights the importance of safeguarding personal information online but also underscores the need for continuous vigilance against potential security threats. As we delve into the intricacies of network monitoring, it becomes evident that awareness, education, and proactive security measures are crucial in maintaining the integrity of digital interactions within connected environments.

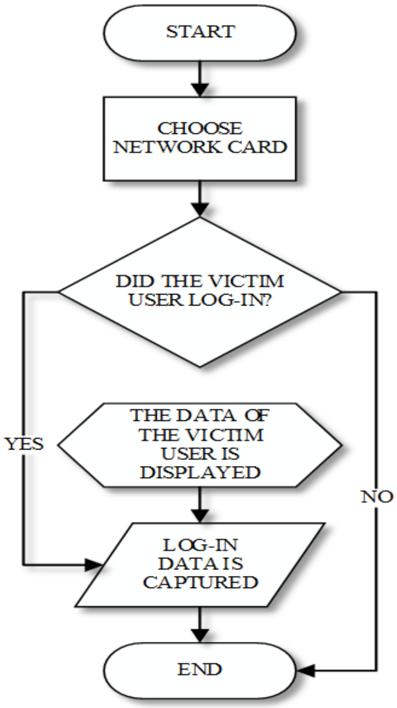

START
CHOOSE NETWORK CARD
DID THE VICTIM USER LOG-IN?
YES
NO
THE DATA OF THE VICTIM USER IS DISPLAYED
LOG-IN DATA IS CAPTURED
END

Fig. 8. Data capture Flow chart

III. Results

Thanks to the evaluation of the network, it was possible to show that people connected to this free Wi-Fi network are sure that they have entrusted their data to third parties [29] and, therefore, can be seen by strangers who may be spying on the web. Thus, the following results are shown in the subsections down here.

A. Obtaining access keys

The access email was obtained, the respective password to access through the victim user’s network to the different types of social media mentioned below, and the number of people who could be detected as connected. A bar chart shows the use of the best-known social media within a period where the number of people related to the mentioned services is observed (Refer to Figure 9).

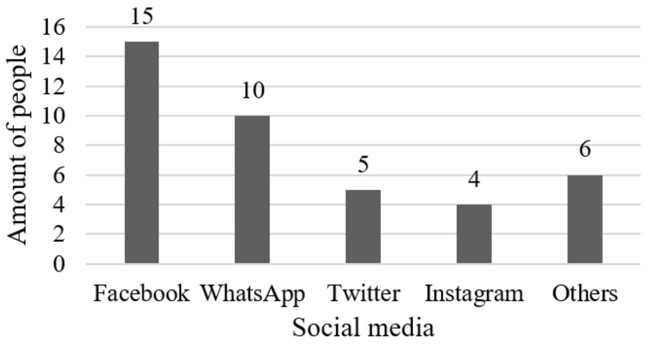


Fig. 9. Number of users connected to the different social media.

B. View images

Evidence was made in the number of images downloaded or viewed on a specific day of the week, taking Tuesday as a reference, measuring every two hours from 08:00 a.m. to 10:00 p.m. of the mentioned day. Then, the number of images viewed and downloaded during different periods obtained from the Wireshark program is shown (Refer to Figure 10).

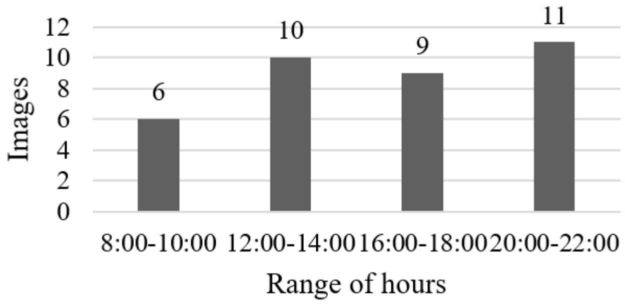
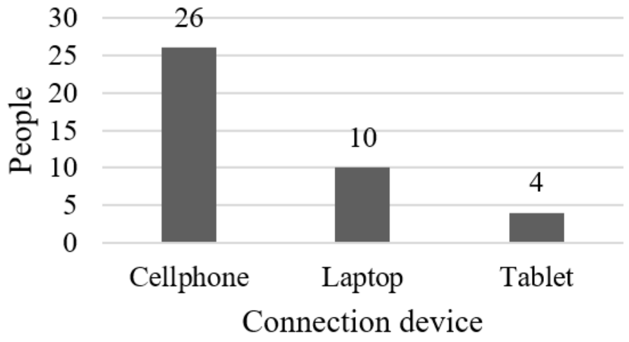


Fig.10. Number of images viewed or downloaded.

C. Confidential data

Employing these network traffic capture programs facilitates the extraction of packets traversing the HTTP protocol, a pivotal Internet communication protocol. This enables the retrieval of diverse data, encompassing activities on platforms such as WhatsApp, Facebook, Dropbox, and even detailed information about the connected device, including the cell phone model and associated user data [30, 31]. The adjacent table provides a comprehensive breakdown, detailing the devices linked to individuals who successfully connected during a specific timeframe stipulated for this investigative process (Refer to Figure 11 and Figure 12).

Additionally, it's crucial to emphasize the ethical considerations and lawful use of such tools. The utilization of these programs for research purposes underscores the importance of respecting privacy and adhering to ethical standards. By shedding light on the potential insights gleaned from network traffic, this research contributes to the ongoing discourse on digital security, encouraging a balance between technological exploration and ethical responsibility.



978-8-3503-1557-8/23/$31.00 ©2023 IEEE

Fig. 11. Number of people connected from different devices.

Fig. 12. Referential Image people using different kinds of devices.

D. General traffic on the Wi-Fi network

Thanks to the program, the visualization of network traffic across the entire evaluation period becomes possible. This provides valuable insights into the fluctuation of connected users during specific intervals. A notable observation is the recurrent pattern of users maintaining sessions initiated at specific times every two hours throughout the day. The subsequent presentation of two figures encapsulates a wealth of information collected at various times and days of the week. The first image depicts the number of individuals connected during a Tuesday, marking the initiation of the initial tests with the Wireshark software (Refer to Figure 13 and Figure 14). Additionally, the subsequent figure portrays users connected to the Continental University's Wi-Fi network throughout the entire week, covering the days from Monday to Sunday within the predefined time range for this investigation (Refer to Figure 15).

Furthermore, these visualizations serve not only to elucidate patterns in user connectivity but also to underscore the dynamic nature of network usage. Understanding these temporal variations is pivotal for enhancing network management and cybersecurity protocols in educational institutions and beyond.

As we delve into the intricacies revealed by the program's capability to visualize network traffic, a nuanced understanding emerges. The recurrent pattern of user sessions initiated at specific intervals every two hours highlights the rhythm of connectivity throughout the day. Figures 13 and 14 offer a detailed snapshot of user engagement on a Tuesday, showcasing the robust testing phase with the Wireshark software. Meanwhile, Figure 15 provides a comprehensive overview of user connections spanning the entire week, offering insights into usage trends from Monday to Sunday. These visualizations not only quantify user engagement but also present an opportunity to fine-tune network management strategies. It's crucial to recognize that such observations contribute not only to the refinement of cybersecurity protocols but also to the broader understanding of how users interact with and depend on network resources within educational institutions and similar settings.

Fig. 13. Referential Image users connected in a day of data capture.

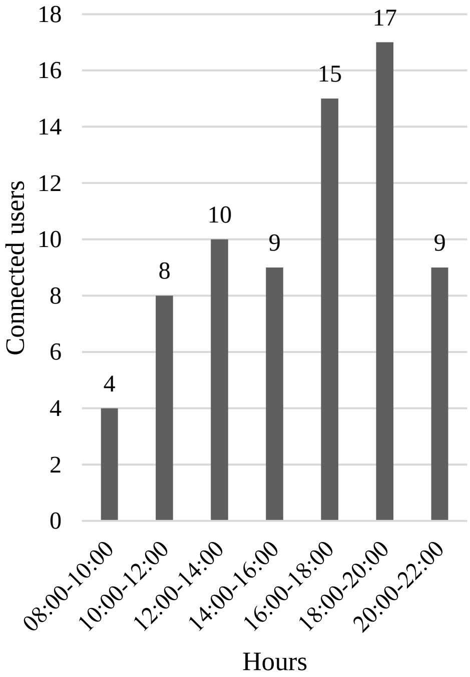


Fig. 14. Number of users connected in a day of data capture.

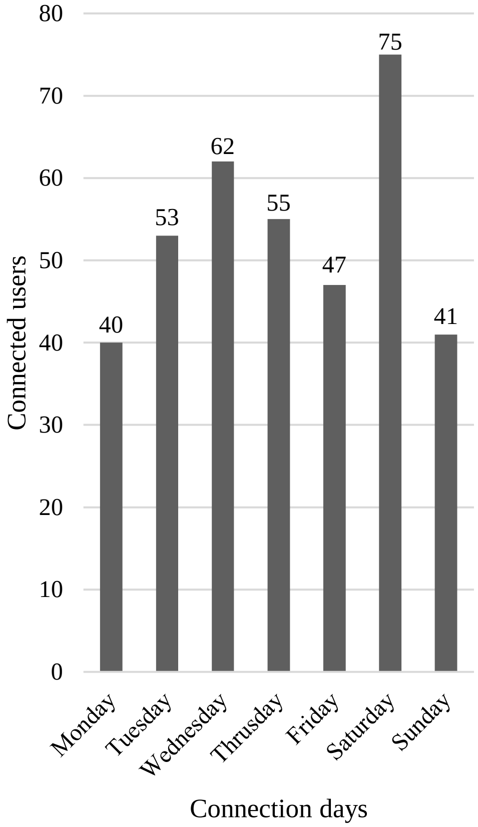


Fig. 15. *Number of users connected during the week of data capture.*

IV. Discussion of results

It was observed that some users seek to connect to access networks to access the Internet without caring about the risks that these may bring, which will repeatedly be mentioned below. Besides, it was possible to show how easy it is to deceive a user with the name of Free Wi-Fi to obtain their data, evidenced by the large number of users connected to our network.

As we can see in the table, it was possible to obtain browsing data from the users connected to the network; among these, we find the images that they were viewing at that time, it was also possible to observe the number of users who are accessing the different social networks, and it was also possible to access the confidential data of the connected devices. As part of the users' data, it is possible to know from what model of devices they are connected, their tastes, with whom they communicate frequently, or simply what they were looking forward to at that moment.

The most apparent limitation within the study occurs in the legal field [32], as it is known in the rules of hacking ethics. In the democratic state of Peru, using information by people who do not consent to use is prohibited. That is why the study could not become broader or show the actual use of the experiment for which everything shown in this work is carried out in a field controlled by the project's executors with the due consent of the people who were violated [33].

V. Conclusions

In conclusion, the information that can be obtained within software such as Wireshark is the total network traffic we carry out; once connected within a free network, anyone with network knowledge could see our activity on the mentioned one.

For people with high-security knowledge, it would not be a problem to obtain essential data such as passwords and others, even with the security offered by sites with HTTP security protocols; taking this as necessary, it is recommended not to use accessible networks if it is required to use or manage sensitive information.

The lines below are the most relevant findings that confirm the danger to personal data when connecting to a Wi-Fi network with unrestricted access, which are the following:

- Inexperienced users will not be uncertain about connecting to free Wi-Fi networks.
- Data packets traveling through the Internet can be captured with the help of programs used in network auditing.
- Users connected to the network can obtain access credentials, browsing data, and data from their connected device.

Now, some solutions will be shown lines below to avoid this kind of intruders when accessing to a public Wi-Fi Network where there are many users who can log in to certain social media and compromised accounts.

❖ Utilize a Virtual Private Network (VPN): Network can be encrypted before being transmitted over the internet. Consequently, even if someone intercepts the transmission, the will only encounter encrypted data, which is practically indecipherable without the appropriate key; then, it converts IP address because a VPN conceals your authentic IP address and substitutes it with that of the remote server, this leads that websites and services you engage with only perceive the IP address of the server and finally the secure tunnel that is the connection between your device and the remote server where you are, thwarting others on the same network (such as in a public Wi-Fi network) from observing your activities. The advantages of using this tool are Privacy and Anonymity because it safeguards your privacy by concealing your location and online activities, Security on Public Networks because it facilitates secure browsing specially on insecure public Wi-Fi networks and Access to Restricted Content by changing your virtual location to access geographically restricted content.

❖ Secure Browsing through HTTPS: This is a protocol that is always guaranteeing the transfer of information over the Internet using an SSL/TLS encryption layer. When accessing an HTTPS-enabled website, your browser and the server engage in encrypted communication, safeguarding any sent or received data from third-party interception. Secure websites are equipped with digital certificates authenticating the server's identity, assuring users that they are connecting to the correct site and not a malicious replica. This approach offers protection against data interception, as HTTPS prevents spying and manipulation by third parties. Users can easily verify a secure website by checking for the padlock icon and “https://” denomination in the browser address bar, instilling confidence in the site’s identity.

By implementing these solutions collective, alongside other security measures, a robust defense against vulnerabilities in public networks is established.

Then, we want to add that this work will be expanded shortly. It must be verified that if the information encrypted by HTTPS security protocols can be decrypted, the time it takes to do it must be seen. The data collected in this article may become more extensive and complex, so there will be more of this collection; in addition, more cases will be formulated to prove when and where users can compromise their data and lose their personal information.

Finally, for those who wish to continue this work, we will gladly provide them with all the information and tools to expand this topic further.

References

[1] W. Garcia, J. Herrera, M. Wellington, “5G y el internet de las cosas: Revisión Sistematica”, Revista Iberica de sistemas y tecnologias de información. Ecuador, July 2021.

[2] W. Martinez, D. Avila, “Ciberseguridad en las redes sociales”, Uniandes Episteme. Ecuador, vol. 8, pp. 211-234, June 2021.

[3] L. Bernardo, “State of the art: Smart home security challenges based on Iot.” July 2021.

[4] J. Salgado Silva, J. Villota Trejo, D. Ramirez Coral, V. Teran Ballesteros, “Sharenting: Adicción a Internet, autocontrol y fotografias online de menores, Revista cientifica de educomunicacion. Madrid, pp. 99, 2020

[5] C. Abril, A. Escobar, “Electronic civil surveillance: review oriented to communications for monitoring and a case,” Vision Electronica. Colombia, vol. 2, December 2019.

[6] R. Macias, M. Bone, F. Quiñonez, J. Mendoza, G. Estupíñan, “Casos frecuentes, penalización y prevención de los delitos informáticosenelEcuador: una breve revisión sistemática”, Sapienza: International Journal of Interdisciplinary Studies, vol. 3, April 2022.

[7] W. Giral, H. Celedon, E. Galvis, A. Zona, “Redes inteligentes en el sistema electrico colombiano”, Tecnura. Bogota, vol. 21, Sept. 2017.

[8] Carlos G. Romero, Luis A. Balseca, F. Saenz, J. Diaza, “The state of the art in intrusion detection in 802.11i networks”, Maskay vol.6, December 2016.

[9] D. Ñanga, J. Vizñay, “Access and security to the wifi network through CISCO identity services engine (ise) technology for users of the Indurama Company of Cuenca, Ecuador,” Polo del conocimineto, vol. 5, February 2020.

[10] V. P. Tintin, J. R. Caiza, F. S. Caicedo, “Arquitectura de redes de información. Principios y Conceptos”, Dominio de las ciencias, vol. 4, pp. 103-122, April 2018.

[11] C. Stiven Abril, A. Escobar Diaz, “Electronic civil surveillance: review oriented to communications for monitoring and a case,” vol. 2, June 2019.

[12] M. Paula Langer, C. Leones Bazzi, G. Lopez Sepulveda, “Estudio de tecnologias y protocolos de comunicación para redes de sensores inalambricos aplicados a la agricultura.”, pp. 368-381, October 2020.

[13] A. Arias, J. Ruiz, E. Espinoza, “Programming wireless sensor networks to apply in the Internet of Things (IoT): a systematic review,” Revista Computo Aplicado, vol. 2, Sept. 2018.

[14] Singh, K. (2023, April 26). GEEKFLARE. Retrieved from https://geekflare.com/microsoft-visio.

[15] J. Esteban de Leon, “Mejores practicas de seguridad en el teletrabajo: una revision.”, Institución universitaria tecnológico de Antioquia, December 2020.

[16] D. A. León, J. G. Martinez, I. A. Ardila, “Artificial intelligence for traffic control in data networks: A Review”, Entre ciencia e ingeniería, vol. 16, May 2022.

[17] P. Prasanya Devi, R. Kannan, M. Ravindran, M, “A Novel Analysis of Wireless Network Monitoring using Wireshark,” *Restaurant Business*, vo. 118, pp. 27-33, 2019.

[18] J. Mora, H. Parra, “Dynamic spectrum allocation in new generation wireless networks: an approach to state of the art,” Publicación e investigación. Bogota, December 2021.

[19] V. Ndatinya, Z. Xiao, “Network Forensic Analysis using Wireshark,” *International Journal of Sensor Networks*, vol. 10, 2015.

[20] A. Kumar, J. B. Yadav, “Comparison: Wireshark on different parameters,” *International Journal of Engineering and Computer Science*, vol.5, no. 3, 2017.

[21] R. Chowdhary, S. L. Tan, J. Zhang, S. Karnik, V. B. Bajic, J. S. Liu, “Context-specific protein network miner--an online system for exploring context-specific protein interaction networks from the literature,” *PLoS One*, vol. 7, no. 4, 2012. doi 10.1371/journal.pone.0034480. Epub 2012 Apr 6.

[22] L. F. Sikos, “Packet analysis for network forensics: A comprehensive survey,” *Forensic Science International: Digital Investigation*, vol. 32, 2020.

[23] G. Jain, Anubha, “Application of SNORT and Wireshark in Network Traffic Analysis,” *IOP Conf. Ser.: Mater. Sci. Eng*, 2021.

[24] S. Alvernia, D. Rico, “Análisis de una red en un entorno ipv6: una mirada desde las intrusiones de red y el modelo tcp/ip”, Rev. Colomb. Tecn. Avanz, May 2017.

[25] D. Quirumbay, C. Castillo, I. Coronel, “Una revisión del aprendizaje profundo aplicado a la ciberseguridad”, pp. 57-65, June 2022.

[26] M. Sastoque, G. Puerto, C. Suarez, “Opportunities to implement Software Defined Radio in network sensors,” Rev. Fac. Ing. Colombia, vol. 26, May 2017.

[27] C. Martinez, Y. Cruz, “Technological Trends and Challenges of Computer Security,” Pol. Con. Ecuador, vol. 3, April 2018.

[28] L. Machuca, R. Braul, “Metodologias mas usadas en la seguridad de base de datos”, pp. 121-130, June 2022.

[29] L. Salazar, “Literature review Software Defined Networking for VoIP, SDN - Revisión de literatura Redes Definidas por Software para manejo de VoIP”, February 2022.

[30] J. Aranda, E. Sacoto, D. Haro, F. Astudillo, “5G networks: A review from the perspectives of architecture, business models, cybersecurity, and research developments”, Novasinergia. Riobamba, vol. 4, June 2021.

[31] L. Romero, F. Artigas, C. Anias, “Redes de sensores inalambricos definidas por software”, RIELAC, vol. 41, pp. 39-50, May 2019.

[32] A. Oña, M. Morales, L. Toledo, “Revisión sistemática del estado del arte de las Tecnologías de Información y Comunicación (TICS) y Seguridad Alimentaria”, Altec. Medellin, vol. 3, December 2019.

[33] S. Sakshi, K. Suresh, “Capabilities of Wireshark as Intrusion Detection System,” *International Journal of Recent Technology and Engineering*, vol. 8, January 2020.

978-8-3503-1557-8/23/$31.00 ©2023 IEEE