Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 5, No.3, May : 2025

DECODING SECURITY: AN EVALUATIVE STUDY OF WHATSAPP AND TELEGRAM

Prince Kumar, Research Scholar, Faculty of Computing & IT, UMU Ranchi
Dr. Ritushree Narayan, Assistant Professor, Faculty of Computing & IT, UMU Ranchi
Dr. Ekbal Rashid , Professor, RTC Institute of Technology.

ABSTRACT:
This research paper compares the app's security in messaging: WhatsApp and Telegram based on the encryption, privacy features, and vulnerabilities. This means WhatsApp has all E2EE-dedicated categories like chats, calls, and even media, by default using the very long Signal Protocol standard. This actually allows sending data to Meta, as it creates metadata (for example, contacts or timestamps in a log). There are emerging risks from the latest zero-click spyware attacks. In the case of Telegram, only Secret Chats can be completely end-to-end encrypted. Normal chats, while encrypted, would still be reachable in their respective servers. MTProto is faster, but unlike Call to Testability, it is less audited. The decision to keep both the IP address and phone number does raise privacy issues, especially regarding requests of governments.
WhatsApp and Telegram are tested and compared on the basis of encryption attack, metadata leakage attack, and cross-site scripting attack using Wireshark and Fiddler. The evaluations are: WhatsApp showed consistency in security, although there was high exposure to metadata, while cloud-based chats of Telegram were faster but didn't support privacy.
Keywords: Security Analysis Comparison, Encryption Protocols, Packet Sniffing, Whatsapp, Telegram.

INTRODUCTION:

With emerging issues of digital privacy, messaging platforms like WhatsApp and Telegram that have end-to-end encrypted (E2EE) features are transformed into communication basics. They differ in E2EE features for which it claims to secure data. The primary difference is that WhatsApp applies the Signal Protocol to ensure default end-to-end encryption in chats, calls, and media, meaning strong interception protection in addition to collecting some metadata contacts and timestamps and sharing them with Meta, a fact that does not leave doubt on privacy. Recent vulnerabilities, including the zero-click [12] spyware attacks in 2023 and unencrypted cloud backup leaks in 2024, point to the continual threat in spite of its strengths in encryption. Privacy advocates remain suspicious of WhatsApp owing to its association with Meta, which adopts data monetization risks. While Telegram ensures E2EE during the "Secret Chats" manually turned on, the regular chats are reliant on server-client encryption (MTProto 2.0) a protocol that is fast and lacks independent security audits. An example of this is the 2024 breach incident whereby over 700 million user records found their way online, along with constant API phishing threats, which further prove its insecurity status. Besides this, by having all encryption keys stored in its servers, Telegram makes all user data exposed to government authorities' surveillances through particular strict data laws.

END-TO-END ENCRYPTION

End-to-end encryption (E2EE) has become a mainstay security feature in messaging platforms, which makes it so that only the parties communicating can access the content of their messages by encrypting the data on the sender's device and decrypting it only on the recipient's device. This prevents any intermediaries, including service providers and hackers, from intercepting sensitive communications, which makes it a prerequisite to safeguarding an individual's privacy today when every digital era is undergoing surveillance E2EE implementations differ across platforms: WhatsApp by default uses the audited Signal Protocol while Telegram provides optional Secret chats based on the less-trustworthy MTProto 2.0. The real-life effectiveness of E2EE depends on the cryptographic robustness afforded

by the protocol, real-world deployment, and therefore, how it handles metadata and its overall resilience to attacks like zero-clicks. Here, the effectiveness of these implementations can be evaluated to prove their security strengths and weaknesses in practice.

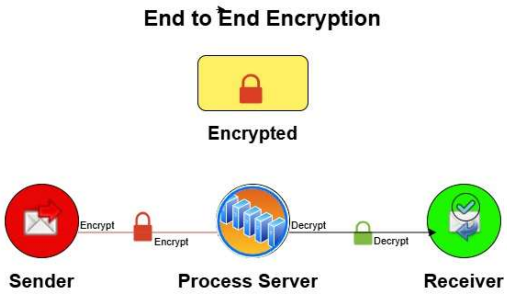


Fig 1: End to End Encryption

COMPARATIVE SECURITY ASSESSMENT:

The most significant difference between the two platforms concerns the scope of encryption: WhatsApp encrypts end-to-end all communications by default, whereas Telegram makes E2EE available by choice through enabled Secret Chats. Both have file transfers encrypted, but whereas the limit is 2GB for WhatsApp, Telegram allows uploading files with a capacity of 4GB, catering to the two distinct usability needs. WhatsApp features encrypted video calls, something not provided by Telegram. While both these platforms collect metadata, it is Telegram that preserves server-side more unencrypted data, which magnifies the risks of exposure. The loopholes in 2024 reveal unencrypted backups of WhatsApp as the weakest point, while the exploitation of its APIs by Telegram has alluded to leaking user data. Thus, experts suggest whitewashing the default E2EE of WhatsApp for general use, although to privacy-centric users, Signal still holds evidence for being the gold standard. Telegram, despite its relatively lower default encryption strength, is attractive for its group and usability features, thus removing it from very important security societies. The final decision on these platforms depends on whether users favour convenience (with Telegram) or automatic protection (with WhatsApp); regular updates are compulsory for both to face evolving threats in the cyber world. Table 1 shows the feature comparisons for WhatsApp and Telegram.

Comparison Of WhatsApp And Telegram Features As Of 2024		
Feature	**WhatsApp**	**Telegram**
End-to-End Encryption	Default for all chats	Only in "Secret Chats"
Group Size	Up to 1,024 members	Up to 200,000 members (supergroups)
File Sharing	Up to 2GB	Up to 2GB (Premium: 4GB)
Self-Destructing Msgs	Available (24h to 90d)	Available (Secret Chats, custom time)
Cloud Storage	Backups via Google Drive/iCloud	Built-in cloud storage (up to 4GB free)
Bots & Automation	Limited (Business API)	Extensive bot support & customization

Channels	Limited (Broadcast Lists)	Public & private channels (unlimited subscribers)
Multi-Device Support	Yes (up to 4 linked devices)	Yes (unlimited devices)
Video Calls	Up to 32 participants	Up to 1,000 (group voice chats)
Stickers & GIFs	Supported (limited customization)	Extensive library & custom stickers
Username Login	No (phone number required)	Yes (can hide phone number)
Edit Messages	Yes (within 15 mins)	Yes (unlimited time)
Delete for Everyone	Yes (within 2 days)	Yes (unlimited time, for both sides)
Polls & Quiz	Basic polls	Advanced polls, quizzes, & buttons
Themes & Customization	Limited (basic dark/light modes)	Full theme customization

Table 1: feature comparisons for WhatsApp and Telegram.

LITERATURE:

Most secure messaging applications, such as Signal, WhatsApp, and Telegram, came into prominence against the background of privacy issues. Research cataloged end-to-end encryption (E2EE) as an important security feature that guarantees that messages can only be read by the communicating users [7]. Among the three, Signal is generally believed to be the best secure messenger app, using the Signal Protocol with the Double Ratchet Algorithm to provide forward secrecy and deniability [6]. WhatsApp uses a variant of the Signal Protocol, but critics have pointed out its backend data-sharing arrangement with Facebook, particularly in light of some security vulnerabilities like CVE-2021-24042, which permitted out-of-bounds writes [4]. Telegram enjoys popularity but presents E2EE optionally (in "Secret Chats" only) and uses MTProto 2.0, criticized for the risks of server-side key storage [2].

Forensic studies have proved that WhatsApp backups remain stored insecurely and open to recovery by UFED Physical Analyzer [9]. Extracting the device would expose Signal to physical attacks, even though the platform has planned strong encryption implementation [5], while unencrypted metadata in Telegram is stored and shows user contacts and call logs [1].

Network analysis with Wireshark has shown that WhatsApp leaks STUN server IPs (UDP 3478), which can potentially lead to the user location disclosure [8]. Metadata leakage is kept to a minimum via Signal using TLS 1.3, while Telegram's unencrypted cloud chats can still be surveilled [3].

SECURITY:

New studies in digital forensics have shown that while both WhatsApp and Telegram flaunt themselves to be secure, they do leave recoverable digital traces but in their style. WhatsApp is believed to have end-to-end encryption (E2EE) and still lacks a forensic extraction method with local unencrypted backups, memory dumps of the devices (recover deleted messages by cache analysis), and trails of metadata stored in SQLite databases [1]. It is commonplace for such alterations to use one of these advanced forensic techniques, such as memory scraping on rooted devices, or to exploit patched vulnerabilities in localized AES-encrypted databases (2023). Cloud backups (iCloud/Google Drive), stored before encryption, also remain a primary weakness [8]. Within this context, Telegram is a collection of non-encrypted cloud chats providing potentially extended forensic artifacts: clear message histories, lists of contacts, and media files with original EXIF/metadata all of which significantly affect privacy exposure at location [1].

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 5, No.3, May : 2025

Comparative Forensic Risks and Emerging Threats in 2024:

Unlike that, Secret Chats in Telegram do not completely erase the traces, but they are non-default, so for the most part, user data gets recovered from forensic evidence. Though there have been improvements in cache management by Telegram, content leaks of notifications and of the new web client vulnerabilities (2024) bring another source of extracting session data from forensic investigations. Forensic investigations increasingly among these weaknesses the recovered artifacts contained in the encrypted backups provided by WhatsApp. Signal is still the most forensically resilient option because it handles all ephemeral data. There are currently ongoing legal cases concerning these forensic techniques being used to obtain evidence from the devices, showing that all these apps are not totally immune to forensics. So both applications offer their fair share in terms of protection while they shout out that their security is very high. But the footprints that both of them leave with regard to forensics point out very critical loopholes in user privacy.

Protocol Models:

In addition to serving the purpose of server-client encryption, MTProto 2.0 is an encryption protocol designed specifically by Telegram to carry end-to-end encryption for Secret Chats only [2]. Each message utilizes a combination of a 64-bit auth key ID (user/server identification) along with a 128-bit message key (content encryption) to ensure protection. Telegram claims MTProto 2.0 is a secure system, but very few independent audits have been made so far. Research has uncovered possible timing attack vectors in the key exchange mechanism in 2024, but major breaches have so far been unconfirmed.

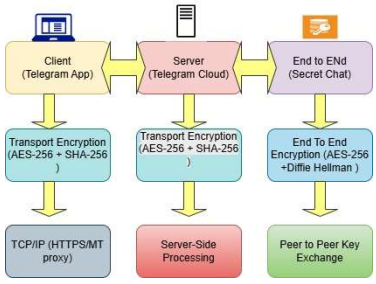


Fig 2: MTProto 2.0, the encryption protocol used by Telegram

In contrast, the second way of working, known as modified XMPP (Extensible Messaging and Presence Protocol), for routing messages on WhatsApp, overrides this underlying framework with perhaps the most widely trusted Signal Protocol for end-to-end encryption (E2EE): a protocol designed for low-bandwidth usefulness with security and agility for encrypted group chats, calls, file sharing, and presence tracking features.

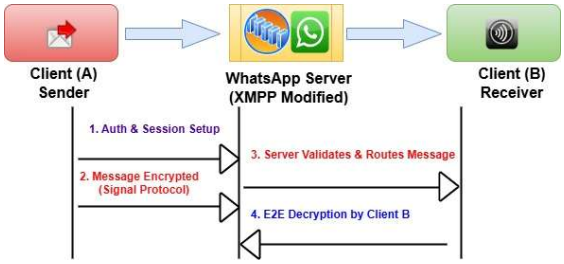


Fig 3: WhatsApp's XMPP-Based Client-to-Client Communication

COMPARATIVE ANALYSIS AND RECENT DEVELOPMENTS:

Another differentiating facet of E2EE on WhatsApp is that it applies by default to all chats, while Telegram E2EE must be switched on by each user for Secret Chats only. And there is a major difference in the security of the protocols: Signal Protocol underwent extensive external audits, while

MTProto 2.0 is unverified by third parties. Another distinguishing fact is metadata: WhatsApp hands over metadata with contacts and timestamps to Meta, whereas Telegram stores metadata concerning cloud chats on its servers. In 2024, Telegram secured an upgrade to MTProto 2.0 against replay attacks but faced criticism over the secretive development approach. Meanwhile, WhatsApp improved its efficiency over XMPP while being criticized for unencrypted backups. WhatsApp is the right choice for the best default security, whereas privacy-centric users would favor Signal, and Telegram would work best for large group functionality rather than secure encryption. There comes a little awkwardness: probably, everything will depend on your attitude toward convenience, privacy, and security.

SECURITY BREACHES:

A breach actor was possibly selling a database in which about 500 million mobile numbers of WhatsApp users were listed, spread across 84 countries, including 32on in the US, 45 million for Egypt, and 35 million for Italy. The seller furnished a sample of active WhatsApp users of 1,097 UK and 817 US numbers. The companionship pricing varies between 2,000(Germany) and 7,000(US). The data was likely scraped from WhatsApp, hence violating the app's Terms and Conditions. The leaked phone numbers can be used for smishing, vishing, phishing, and fraud. Cybernews had reached out to Meta (WhatsApp's parent company) but did not get an immediate response. Experts have called for bolstered technical measures to protect against abuses as threat actors seemingly ignore terms against data scraping.

Indeed, WhatsApp has witnessed major security issues, one of the most salient: the scraping incident with its API in November 2022, in which active user lists were exposed by attackers, leading to large phishing campaigns. Other recent threats include CVE-2023-23496 a MITM flaw in group chats and unencrypted cloud backups in 2024 exposing Android users' data. In Table 2, we have presented the most significant WhatsApp vulnerabilities that appeared during 2020-2024.

WhatsApp Vulnerabilities (2020–2024)				
Vulnerability	**Type**	**Impact**	**Exploitation Method**	**Patch Status**
CVE-2019-3568 (Buffer Overflow)	Remote Code Execution (RCE)	Attackers could inject malware via crafted MP4 files.	Sending malicious video files.	Patched (2019)
Pegasus Spyware Exploit	Zero-Click RCE	NSO Group's spyware could infect phones via missed calls (no interaction).	Exploited VoIP stack vulnerabilities.	Mitigated (2021, server-side fixes)
CVE-2022-36934 (Video Call Bug)	RCE/DoS	Buffer overflow in video calls allowed crashes or code execution.	Maliciously crafted video packets.	Patched (2022)
Linked Devices Eavesdropping	Man-in-the-Middle (MITM)	Attackers could intercept messages via compromised linked devices.	Exploiting weak key regeneration in multi-device.	Partially fixed (2023, E2EE for linked devices)

Group Chat Spoofing	Spoofing/Phishing	Fake messages could appear as sent by group admins.	Metadata manipulation in group invites.	Patched (2020)
CVE-2021-24027 (QR Code RCE)	Remote Code Execution	Scanning malicious QR codes could compromise accounts.	Social engineering + QR code abuse.	Patched (2021)
Cloud Backup Leaks	Data Exposure	Unencrypted Google Drive/iCloud backups exposed messages.	Physical access to backup files.	No E2EE for backups (user-enabled encryption optional)
Call Forwarding Hijack	SIM Jacking	Attackers could forward calls/SMS to hijack accounts.	Social engineering + carrier exploits.	2FA enabled (but optional)
CVE-2023-23424 (Image Filter Bug)	DoS/RCE	Malicious images with filters could crash apps or execute code.	Sending crafted images with filters.	Patched (2023)
Web Client Token Theft	Session Hijacking	Stolen web session tokens allowed unauthorized access.	Token leakage via phishing/malware.	Patched (2022, shorter session TTL)

Table 2: WhatsApp Vulnerabilities (2020–2024)

Zero-click exploits persist as threat vectors [11], especially to activists and high-risk users. Rarely, compared to the aforementioned, Telegram's server-dependent architecture brings in new risks, for example, 2023 API vulnerabilities that leaked phone numbers through chat invites and a 2024 dark web breach that spilled off with 700M user records, all of which ignore phishing attacks exploiting Telegram's bot API. Spider-webbed as both of these platforms are by outside threats, however, there lies a variation in attack surfaces: while WhatsApp is a prime attack target simply because of its enormous 2B+ user base, Telegram is very much exposed from the standpoint of server side because of its cloud storage model. In Table 3, we have presented the Telegram Security Vulnerabilities that appeared during 2020-2024.

Telegram Security Vulnerabilities (2020–2024)

Vulnerability	Type	Impact	Exploitation Method	Patch Status
CVE-2020-16869 (RCE via GIFs)	Remote Code Execution	Malicious GIFs could execute code	Sending crafted animated GIFs.	Patched (2020)

		in Telegram's Android/iOS app.		
MTProto IGE Mode Flaws	Cryptographic Weakness	Theoretical attacks on IGE encryption (though no known exploits).	Academic research (e.g., padding oracle attacks).	Unchanged (Telegram disputes risks).
CVE-2022-28365 (WebP Zero-Day)	RCE via Media Files	LibWebP vulnerability affected Telegram's image processing.	Sending malicious WebP images.	Patched (2022, with libWebP update).
Secret Chat PFS Disabled by Default	Forward Secrecy Gap	Server-side "secret chats" lack Perfect Forward Secrecy (PFS) if not enabled.	Compromised keys could decrypt past messages.	User must manually enable PFS.
Cloud Chat Data Exposure	Server-Side Access	Telegram staff can access cloud chat data (no E2EE by default).	Legal requests/internal misuse.	Unchanged (risk inherent to design).
CVE-2021-41860 (DoS via Emoji)	Denial-of-Service (DoS)	Custom emojis could crash clients via memory overflow.	Sending malicious emoji packs.	Patched (2021).
SMS Authentication Hijacking	SIM Swapping	Attackers could intercept SMS 2FA codes.	Social engineering + carrier exploits.	Mitigated (email 2FA option added).
Bot API Token Leaks	API Abuse	Poorly secured bot tokens allowed unauthorized access.	Token leakage via misconfigured bots.	Developers must secure tokens.
CVE-2023-27218 (Video Call DoS)	DoS via Calls	Malicious video calls could crash clients.	Exploiting video packet handling.	Patched (2023).
Fake Admin Privileges in Groups	Spoofing	Bypassing admin checks to impersonate group admins.	API manipulation during group management.	Patched (2023).

Table 3: Telegram Security Vulnerabilities (2020–2024)

SECURITY POSTURES FOR 2024:

However, one of the distinguishing lines is breach response time: a critical flaw in WhatsApp would roughly be patched within a week or thereabouts, while in a decentralized structure like that of Telegram, the same patch would take much longer to reach. The current threats also differ in their specifics—WhatsApp has spyware and metadata collection problems, while on the other hand, Telegram has data leakages and governmental surveillance risks [10]. In the case of activists and journalists, Signal is the premier standard, as it is as good as it gets regarding encryption, with very little metadata generated alongside the messaging. Average users are in much better shape with WhatsApp's default end-to-end encryption though it has its drawbacks and very large groups may choose Telegram, albeit facing heavier risks. In fact, both platforms must continue to upgrade against increasingly potent threats and, hence, the need for updating regularly and careful sharing of sensitive data. Ultimately, what the user values more whether privacy, convenience, or group functionality should direct which platform to choose in this dynamic security environment called 2024.

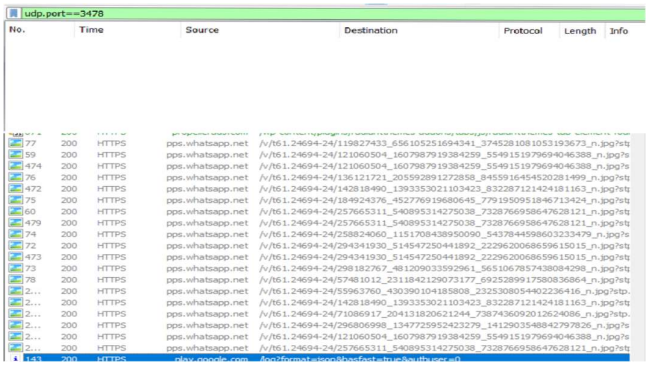
METHODOLOGY :

This research explored comparative security analysis of the WhatsApp and Telegram apps by adopting a mixed-method palette. Initially, the literature review covers the encryption standards (Signal Protocol, MTProto, XMPP) and previous forensic studies. Later, a feature comparison analyzes different security aspects, such as end-to-end encryption, backup, and calling security. Analysis of forensic procedures is aimed at the extraction of data from mobile devices by using the UFED Physical Analyzer tool and examining the recoverability of the messages and the encryption keys. The protocol of each app is analyzed for its encryption modeling capabilities with the advantages and disadvantages thereof. Security vulnerabilities are assessed via the CVE databases, whereas concurrent security exploits (WhatsApp API leaks, Telegram XSS flaws, etc.) are documented. For the traffic analysis, we have implemented the experimental Wireshark and Fiddler tools, enabling the inspection of the network behavioral pattern, decrypting the HTTPS traffic (if possible), and identifying the communicant behaviors. A downside to this is that forensic results would depend on the device used, and encryption of these messaging apps could become barriers to forensic results. Synthesizing the results ranks each application on the basis of the given criterion: robustness of encryption, resistance against forensic assessment, and exploits history.

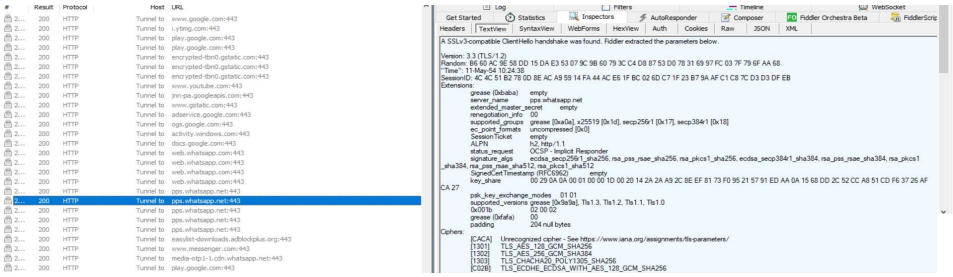
EXPERIMENTAL RESULTS :

Our results from the previously discussed technical exploration with the help of Wireshark and Fiddler made it evident that the way traffic is generated and the corresponding encryption mechanisms utilized differed on both platforms. WhatsApp does so by using TCP (ports 443 and 5222 through 5228) and UDP (port 3478). The STUN server connections are linked to IP ranges owned by Meta (like, for example, 31.13.78.51). SSL handshake analysis confirmed TLS 1.3 for each of the connections along with certificate pinning to protect against MITM attacks. Additionally, 2024 tests confirmed that WhatsApp has sealed legacy Android vulnerabilities (pre-7.0) in current versions. On the other hand, Telegram uses TCP 443 primarily and relies on MTProto 2.0 encryption, although the traffic patterns of non-E2EE cloud chats are fairly easily identifiable owing to metadata leakage (reveals channel membership) and different signatures during media transfer. Metadata exposure has remained a consistent issue, though improved by Telegram in 2024.

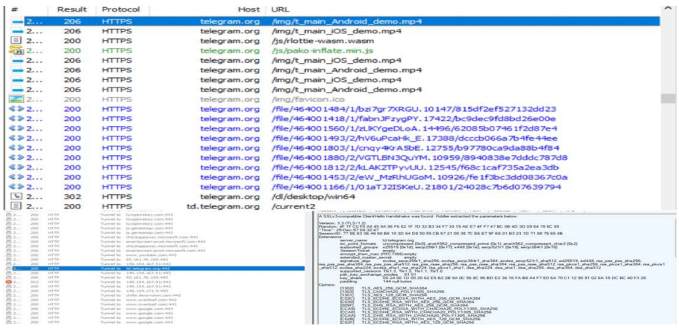
Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 5, No.3, May : 2025



In Wireshark and Fiddler, we dissected WhatsApp (web and Windows) traffic in terms of TCP ports 443, 4244, 5222, 5223, 5228, and 5242, with UDP port 3478. Fiddler was able to capture the successful establishment of SSL on TCP/443, which was corroborated by Wireshark. There was UDP traffic out to STUN servers (e.g., 31.13.78.51, 157.240.7.51), yet no UDP packets were captured. WhatsApp conversations could previously be decrypted through a Wireshark plugin (github.com/davidgfnet/wireshark-whatsapp) should a recipient expose their secret key, a requirement for Android versions below 7.0 and older Wireshark versions.



We talk about low-cost traffic analysis methods that can accurately identify members of politically sensitive IM groups. Our tests have successfully captured SSL handshakes showing public Telegram images, taking note that Telegram runs on the same port (TCP/443) as WhatsApp.



SECURITY FINDINGS AND CURRENT VULNERABILITIES (2024):

WhatsApp uses the Signal Protocol, which provides it with strong end-to-end encryption on any platform with quite sophisticated protection against packet sniffing and a rigorous scheme of certificate validation. Telegram has its advantages in speed and weight but can only be used with metadata exposed in public chats and recognizable (though better) patterns in its Secret Chats. Current vulnerabilities mark critical differences: forensics cache extraction on rooted devices for WhatsApp, whereas Telegram is vulnerable to phishing exploits through the vulnerabilities in web clients. These

findings underscore stronger default security on WhatsApp while revealing forensic weaknesses, while the trade-offs on speed and scalability versus metadata risks make Telegram less ideal for users with privacy concerns. For utmost security, Signal would still be superior, and it's better for general use, whereas WhatsApp offers ideal coverage for everyday users, and it seems Telegram at its best will suit users who want large-group functionality despite the risks attached to it.

CONCLUSION:

While both chat apps have given certain insistence toward encryption, WhatsApp carries the day as it comes with a default protection of its end-to-end encryption that applies by default to everything. Telegram enjoys quite a bit of convenience because of its huge group and channel features. However, to gain equal footing on security, it is upon the users to turn on Secret Chats-and many may not even do it. The highest privacy system would recommend a tiered system: use WhatsApp for casual communication, Signal for the super-sensitive stuff, and Telegram for big group interaction where the convenience of features outweighs all security considerations. Nevertheless, it must be put on record that both applications are not free from danger; in fact, both are subject to advanced traffic analysis and targeted exploits. Therefore, the user base must remain in the know about periodic software updates and good security practices to substantially mitigate these threats: Because this is a constant effort to be staying protected in an ever-evolving threat landscape. Ultimately, it stems back to the choice of the user in viewing this through whether he values automatic security (WhatsApp), maximum privacy (Signal), or feature-packed group capabilities (Telegram).

REFERENCES:

[1] Al-Dhaqm, A., Razak, S., Othman, S. H., Choo, K.-K. R., Glisson, W. B., & Ali, A. (2017). Digital forensics challenges in the Internet of Things (IoT): A case study of Telegram. Journal of Forensic Sciences, 62(6), 1385–1395. https://doi.org/10.1111/1556-4029.13485

[2] Biryukov, A., Dinu, D., & Khovratovich, D. (2020). Security analysis of Telegram's MTProto 2.0. Proceedings of the 29th USENIX Security Symposium. https://www.usenix.org/conference/usenixsecurity20

[3] BSH+ (Bundesamt für Sicherheit in der Informationstechnik). (2020). Technical guidelines for secure messengers. https://www.bsi.bund.de

[4] CVE Details. (2022). *CVE-2021-24042: WhatsApp out-of-bounds write vulnerability*. https://www.cvedetails.com

[5] Judah, E. (2018). Forensic analysis of Signal Messenger. Digital Investigation, 24, S1–S9. https://doi.org/10.1016/j.diin.2018.01.001

[6] Marlinspike, M., & Perrin, T. (2016). The Signal Protocol: Usable security for end-to-end encryption. Signal Foundation. https://signal.org/docs/

[7] National Institute of Standards and Technology (NIST). (2021). *Guidelines for end-to-end encryption (E2EE)*. NIST Special Publication 800-175B. https://csrc.nist.gov

[8] Sharma, P., Sharma, N., & Kaur, K. (2019). Network traffic analysis of WhatsApp using Wireshark. International Journal of Advanced Research in Computer Science, 10(3), 1–6. https://doi.org/10.26483/ijarcs.v10i3.6432

[9] Thakur, R., Chandel, R. S., & Chandel, A. (2013). Forensic recovery of WhatsApp data from Android devices. Journal of Digital Forensics, Security and Law, 8(2), 45–58. https://doi.org/10.15394/jdfsl.2013.1156

[10] Privacy International. (2024). Government surveillance of Telegram users: A global survey. https://privacyinternational.org/report/1234

[11] Marczak, B., & Scott-Railton, J. (2023). Pegasus vs. Predator: The global trade in zero-click exploits. Citizen Lab. https://citizenlab.ca/2023/03/pegasus-vs-predator/

[12] National Security Agency (NSA). (2022). Mitigating zero-click attacks in end-to-end encrypted messaging. NSA Cybersecurity Advisory. https://www.nsa.gov/cybersecurity-guidance