Telegram in 2026:

The Definitive OSINT & Investigations Handbook

CONTENTS

Written by: Ari Ben-Am
Senior Analyst at Falkor & Founder of Telemetry

FALKOR
All your intelligence

Executive Summary

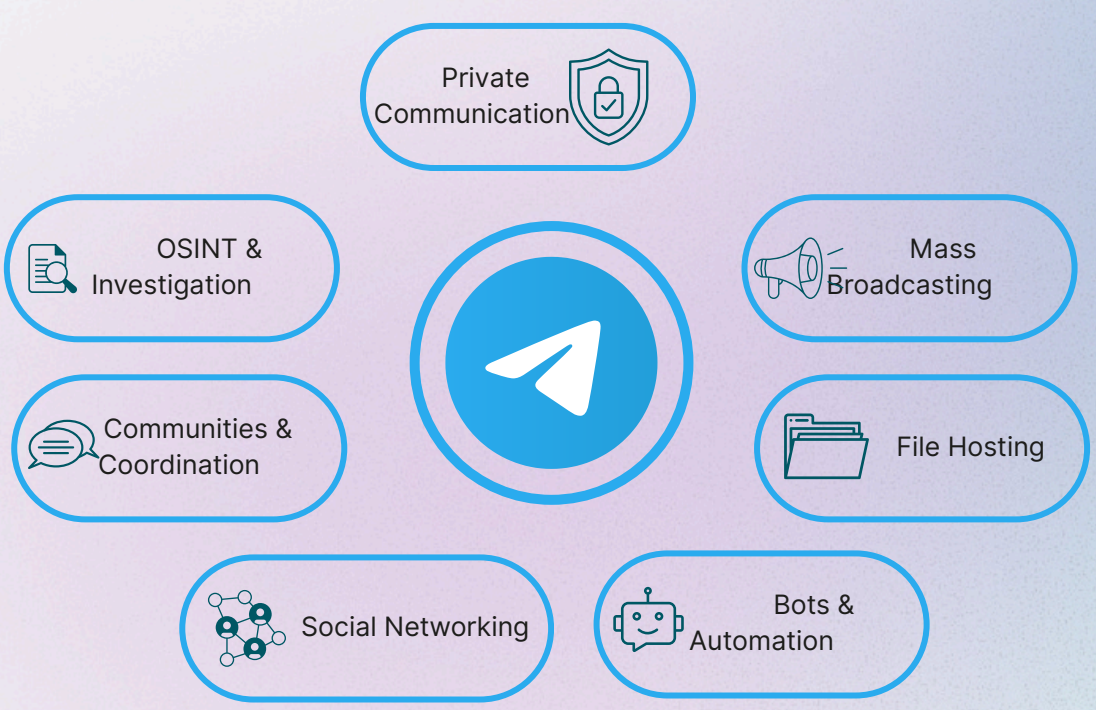
Telegram appears constantly in the news. Be it for its use in Russian and Iranian virtual espionage and recruitment, its role as a hub of cybercrime, its centrality in news coverage and beyond, Telegram is the new frontier of the internet, for both good and bad.

Many are still wrapping their heads around this new reality. Telegram is one of the world's most widely used communications platforms, but describing it simply as a "messaging app" significantly understates what it has become. Over the past decade, Telegram has evolved into a hybrid ecosystem that combines private communication, mass broadcasting, file hosting, automation infrastructure, and social networking into a single platform.

For ordinary users, Telegram offers speed, convenience, synchronization across devices, and access to enormous online communities. For journalists, activists, political movements, cryptocurrency communities, and researchers, it offers resilience, scalability, and comparatively permissive moderation. For investigators and OSINT practitioners, Telegram has become one of the most important — and challenging — sources of open digital intelligence available today.

Telegram: More Than a Messaging App

A hybrid ecosystem for communication, broadcasting, automation, and OSINT



Telegram differs from traditional social networks because its ecosystem is fragmented across channels, groups, private communities, bots, invite links, and external indexing systems. Communities frequently migrate, rename themselves, rotate invite links, or fragment under pressure. Media spreads rapidly across interconnected ecosystems, often crossing language barriers and platform boundaries within minutes.

At the same time, Telegram's architecture creates unique investigative opportunities. Persistent message histories, massive multimedia archives, large-scale public broadcasting, automated collection, and cross-platform linking all make Telegram unusually rich as an investigative environment.

Telegram is also important to understand not simply as an application, but as an ecosystem. Operationally, Telegram functions simultaneously as:

- A messaging platform
- A broadcasting system
- A media archive
- A cloud file-hosting service
- A social network
- An automation platform
- A livestreaming environment
- A coordination space
- A distribution layer for narratives and media

This convergence is one of the reasons Telegram has become so central to modern online movements and investigations. Political campaigns, activist groups, extremist organizations, cryptocurrency communities, scam networks, journalists, and researchers all use the same underlying infrastructure in radically different ways.

For investigators, understanding Telegram therefore requires understanding not only individual chats or channels, but the broader ecosystems, workflows, and migration patterns that emerge around them. This guide provides a practical overview of Telegram as an operational environment: how it works, how communities organize themselves, how identities function, how information spreads, how investigators can protect themselves operationally, and how Telegram investigations can be conducted effectively at scale.

Understanding Telegram's Architecture

Telegram is primarily cloud-based. Most communications are stored on Telegram infrastructure and synchronized automatically across devices. This cloud-oriented design differentiates Telegram from many other communication platforms.

Feature	What it means	Why it matters
Cloud-based storage	Most Telegram communications are stored on Telegram infrastructure rather than only on local devices.	Enables persistent histories, searchable conversations, and large-scale media storage.
Cross-device synchronization	Users can move between mobile, desktop, and web clients without local backups or QR-code pairing.	Supports seamless access, faster content distribution, and continuity across devices.
MTProto protocol	Telegram uses its own protocol, designed for speed and reliability under poor network conditions.	Helps explain Telegram's popularity in regions with unstable infrastructure, censorship, or bandwidth limits.
Investigative implications	Telegram is not end-to-end encrypted by default; channels, groups, supergroups, and media archives are generally cloud-based spaces.	These public and semi-public environments create valuable visibility for investigators.

Cloud-based by design. Searchable at scale. Operationally significant for investigators.

Cloud Chats vs. Secret Chats

One of the most persistent misconceptions about Telegram is the belief that all communications are end-to-end encrypted. In practice, Telegram separates communications into Cloud Chats and Secret Chats.

Cloud Chats

Cloud Chats represent the overwhelming majority of Telegram activity. They include standard one-to-one conversations, groups, supergroups, and channels. These communications are encrypted in transit but stored on Telegram's cloud infrastructure so that they can be searched, synchronized, and accessed across devices. This design is useful for usability and scale, but it means these communications are not end-to-end encrypted in the same way as Signal or WhatsApp messages.

Secret Chats

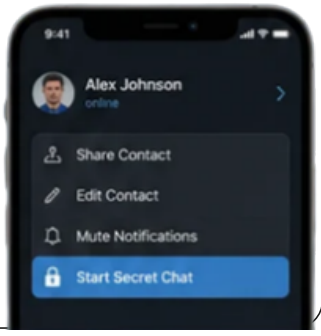
Secret Chats are Telegram's optional end-to-end encrypted mode. They exist only between two users, are device-specific, do not synchronize to the cloud, and support self-destruct timers. Secret Chats cannot be used for groups or channels, which means that most public Telegram activity happens outside Telegram's strongest encryption model.

Key differences

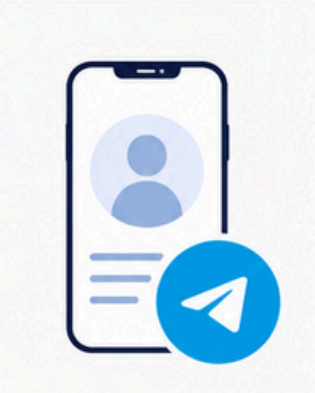
Cloud Chats	Secret Chats
Default mode	Optional mode
Store in Telegram's cloud	End-to-end encrypted
Searchable and synchronized across devices	Device-specific
Used for groups, channels, and most activity	Not synchronized to the cloud
	Available only between two users

To start a Secret Chat on mobiile

1. Open a user profile
2. Tap the profile options menu
3. Select "Start Secret Chat"



Telegram Identities and User Structure



Telegram identities are layered and flexible. Unlike social platforms that emphasize persistent public identities, Telegram allows users to operate with varying degrees of visibility and pseudonymity.

A Telegram identity may include a user ID, username, display name, phone number, profile photo, biography, linked channels, and behavioral patterns. These elements do not carry equal investigative weight. Some are persistent, while others can change quickly.

User IDs

- Every Telegram account has a unique numerical identifier known as a User ID. This identifier is globally unique, internally persistent, and widely used by Telegram APIs and automation tools.
- User IDs are often more reliable than usernames because usernames can change repeatedly. When possible, investigators should preserve user IDs, group IDs, and channel IDs rather than relying only on visible names.
- User IDs are not normally visible in Telegram's standard interface, but they can often be extracted through Telegram APIs, exported metadata, OSINT tooling, or helper bots such as @userinfobot.

➡ Investigative value: More stable and reliable than visible profile names.

User IDs

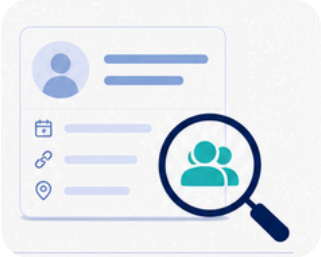
- Telegram usernames begin with @, are globally unique, and are optional. A username allows a user, channel, group, or bot to be publicly discoverable through Telegram search and direct links such as t.me/username.
- Users can configure usernames under:

  Settings → Username

- From an investigative perspective, usernames are useful but fragile. They may change at any time, abandoned usernames may later be reused, and high-value usernames may transfer ownership through Telegram's blockchain-linked identity ecosystem.
- When documenting usernames, investigators should preserve screenshots, numeric IDs, message links, invite links, and timestamps whenever possible.

➡ Investigative value: Useful for discovery, but weak if documented without supporting identifiers.

Profile Signals and Phone Numbers



In Telegram, visible profile elements may appear weak on their own, but together they can provide valuable attribution and correlation signals.

Display Names and Profile Metadata

Telegram users can freely choose display names, including emoji-heavy names and Unicode-heavy identities. These names are not unique and may change frequently.

Although display names are weak identifiers, they can still provide useful contextual information including language, cultural references, ideology, behavioral patterns, and attempts at obfuscation.

Telegram profiles may also expose:

Profile Photos	Biographies	Lenguage indicators	Linked channels	Geographic references

These details are often valuable during attribution analysis, persona tracking, and cross-platform correlation. Reverse-image searching profile photos alone can occasionally produce substantial investigative leads.

Investigative value: Weak as identifiers, but highly useful as contextual signals.

Phone Numbers

Telegram registration fundamentally depends on phone numbers, but users may hide their phone numbers from others. Visibility can be restricted to contacts, nobody, or selected users.
Users can configure usernames under:
Phone-number visibility settings are located under:

Settings → Privacy and Security → Phone Number

Operationally, phone numbers function as Telegram's hidden root identity layer rather than a consistently visible public identifier. Disposable numbers, virtual SIM providers, and anonymous Telegram-compatible numbers further complicate attribution.

Investigative value: Foundational for registration, but not always visible and often operationally obscured.

What investigators should remember:

Display names can change.
Usernames can change. Phone numbers may be hidden. The strongest approach is to combine stable identifiers with contextual profile signals.

TON, Fragment, and Blockchain Identity Infrastructure

Telegram's ecosystem increasingly overlaps with blockchain-based infrastructure through TON, also known as The Open Network.
TON supports wallet integration, cryptocurrency transfers, username ownership, digital asset marketplaces, and Telegram-linked identity assets.
In some regions, Telegram Wallet functionality may appear under:

Settings → Wallet

Or through official wallet bots and integrations.

Fragment

Fragment is Telegram's marketplace for usernames, anonymous numbers, and related digital identity assets. It is accessible through fragment.com.

Fragment allows users to purchase premium usernames, trade short usernames, and acquire anonymous Telegram-compatible numbers. Ownership is tied to TON blockchain assets.

Telegram usernames can now function as transferable digital assets. This is especially important for investigations involving high-profile channels, cryptocurrency ecosystems, scam operations, or influence campaigns.

Investigators should avoid assuming that continuity of username equals continuity of operator. Historical ownership may differ from current ownership.

Fragment also allows acquisition of anonymous numbers usable for Telegram registration. These numbers avoid traditional telecom registration systems and increase pseudonymity, making telecom-based attribution more difficult.

Key Takeaway

TON and Fragment introduce blockchain-native identity infrastructure into Telegram. This creates new opportunities for users—but also new challenges for investigators.
Understanding how usernames, wallets, and anonymous numbers are created, owned, and transferred on TON is now essential for effective OSINT operations.

Telegram Communities: Channels, Groups, and Supergroups

Telegram's ecosystem revolves around several communication structures, each designed for different forms of interaction and dissemination. Understanding these structures is essential for ecosystem mapping and investigative analysis.

Channels

Channels are one-way broadcast systems where administrators publish content to subscribers. Channels may be public or private. Public channels are searchable, possess usernames, and may accumulate millions of subscribers.
Caja pequeña / callout:

To create a channel

1. Tap the compose/new message icon
2. Select New Channel
3. Choose public or private visibility
4. Configure username and permissions

Groups and Supergroups

Basic groups are smaller collaborative chat environments designed for ordinary communication. As communities grow, they often migrate into supergroups. Supergroups are Telegram's large-scale community infrastructure. They support large memberships, persistent histories, granular moderation, anti-spam controls, topic segmentation, and anonymous administrator posting.

Administrative controls

- Group Info → Administrators
- Permissions
- Manage Group

Investigative value

Why Supergroups Matter to Investigators

Unlike channels, supergroups often expose interaction patterns among members, making them valuable for identifying social structures, moderators, recurring participants, escalation patterns, and migration behavior.

Public and Private Communities

Public communities

- Searchable
- Public usernames
- Often indexed externally

VS

Private communities

- Require invite links
- Not broadly indexed
- Common in criminal ecosystems, vetting operations, restricted ideological networks, and operational coordination environments

Their existence may still become visible through leaked invite links, screenshots, forwarded posts, or references in public channels.

Invite links and community migration

Invite links are central to how Telegram ecosystems grow, migrate, and survive moderation pressure. They also help investigators map relationships, fragmentation, and operational behavior across communities.

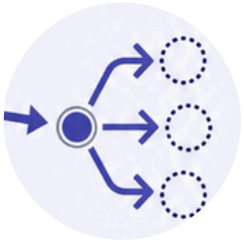
Invite Links

Common formats include t.me/groupname and t.me/+abcdef123456.
Administrators manage them through Group/Channel Info → Invite Links. Telegram supports multiple active links, expiring links, limited-use links, and approval-based joins.

Investigative value: Invite links can expose backup communities, organizational relationships, ecosystem fragmentation, and migration behavior.

Community Migration

Communities under pressure often maintain mirror channels, backup groups, redundant invite infrastructures, and emergency migration instructions. Tracking invite-link propagation can reveal broader operational networks.



Investigative value: Migration patterns help reveal resilience, moderation evasion, and network continuity.

Bots, Automation, and BotFather

Telegram's automation ecosystem supports moderation, content dissemination, monitoring, scraping, archiving, and workflow orchestration. Investigators often use bots for keyword alerts, RSS ingestion, channel monitoring, IOC collection, translation, notifications, and archival workflows. Telegram's official bot-management system is @BotFather.

To create a bot

1. Open @BotFather
2. Run /newbot
3. Choose a bot name
4. Choose a unique username ending in bot
5. Receive the API token

Investigatively, bot infrastructure can reveal operational sophistication, naming conventions, shared infrastructure, automation pipelines, and administrative relationships. Leaked bot tokens can provide substantial operational access to associated systems.

Mini Apps and Telegram APIs

Telegram increasingly supports embedded web applications, often referred to as Mini Apps or Telegram Web Apps. These applications operate inside Telegram chats, bots, or channels and provide interactive services without requiring users to leave the Telegram ecosystem.

Mini Apps and embedded web applications

Mini Apps are especially common in cryptocurrency ecosystems, TON infrastructure, marketplaces, scam environments, gaming communities, payment systems, and subscription services. Operationally, they blur the line between messaging platform and browser environment. A Telegram bot may launch embedded websites, wallet interfaces, login systems, payment portals, interactive dashboards, trading platforms, or browser-based services directly inside Telegram.

Why Mini Apps matter

- Domains
- APIs
- Wallet systems
- Authentication flows
- External hosting providers

Malicious ecosystems frequently use embedded web applications for credential theft, phishing, wallet compromise, malware delivery, and fake verification systems. Investigators should treat Telegram Mini Apps with the same caution applied to unknown external websites or browser-based infrastructure.

Telegram APIs and OSINT collection

Telegram exposes several APIs that dramatically expand its usefulness for both developers and investigators. The Bot API is HTTP-based and designed for automation. It is documented at core.telegram.org/bots/api. Telegram also exposes full client APIs based on MTProto. Developers can create API credentials through my.telegram.org.

Popular libraries

- Telethon
- Pyrogram
- GramJS
- MadelineProto

These frameworks are widely used for scraping, monitoring, archival systems, threat intelligence, media archiving, and narrative tracking. Telegram's openness to automation is one reason it has become such a central platform for large-scale monitoring and analysis.

What investigators should remember

Mini Apps extend Telegram into browser-like environments, while APIs extend it into large-scale automation and collection. Together, they make Telegram unusually rich — and unusually risky — as an investigative environment.

Native Search and Discovery

Telegram includes several built-in discovery systems, but each comes with important limitations. Global search is accessible through the main search bar at the top of the application. It can surface public channels, public groups, usernames, and bots. However, indexing is incomplete, discovery algorithms are opaque, and historical visibility is limited. Public channels and groups may exist for years without appearing reliably in Telegram search results.

In-Chat Search

In-chat search is often more valuable for investigations. Within a specific group or channel:

1. Open the community
2. Tap the group or channel name
3. Select the search icon

> This allows keyword search inside that specific history, which can be especially powerful in long-running communities.

Investigative value: In-chat search provides direct access to specific conversations and historical content that may not be discoverable through global search.

Media, Link, and File Filtering

Telegram's filtering systems are among its most useful investigative features. They transform many channels into searchable repositories rather than simple chat environments.

To access filters:

1. Open a channel or group
2. Tap the header
3. Review sections such as:
   - Media
   - Files
   - Links
   - Music
   - Voice

Media filtering

Media filtering allows investigators to quickly isolate photos, videos, documents, audio, voice notes, and GIFs. This is useful for identifying propaganda videos, leaked documents, malware samples, maps, screenshots, and other intelligence artifacts.

Investigative value: Media filters accelerate review and help surface visual and multimedia evidence quickly.

Link filtering

Link filtering is especially valuable for mapping external shared links, investigating identity websites, cryptocurrency services, donation portals, backup communities, cloud repositories, and cross-platform ecosystems.

Investigative value: Link analysis helps reveal how Telegram communities connect to external services and broader operational networks.

Document filtering

Document filtering can surface PDFs, ZIP archives, APKs, Office documents, datasets, and research collections. Original filenames often remain intact, which can assist provenance analysis, malware tracking, and cross-platform correlation.

Investigative value: File metadata and original filenames can provide important clues about origin, distribution, and operational behavior.

Key Takeaway

Telegram's native search and filtering tools are imperfect, but they are highly valuable for investigators. While global search has clear limitations, in-chat search and media, link, and file filters can significantly improve discovery, historical review, and infrastructure mapping.

File Storage, Caching, and Persistence

Telegram functions not only as a messaging platform, but also as a large-scale cloud file-hosting system. Most media shared in standard chats, groups, supergroups, and channels is stored within Telegram's cloud infrastructure and synchronized across devices. This allows users to re-download files without the sender being online, access media across devices, maintain persistent media histories, and operate channels as long-term repositories.

Local caching and storage behavior

At the same time, Telegram clients also cache large amounts of content locally on devices. Depending on settings, Telegram may automatically download and locally store images, videos, documents, voice messages, and channel media. This cached data may persist even after content is deleted remotely.

Auto-download may store

- Images
- Videos
- Documents
- Voice messages
- Channel media

Settings locations

Automatic media download: Settings → Data and Storage → Automatic Media Download

Storage usage and cache controls: Settings → Data and Storage → Storage Usage

Investigators should strongly consider disabling automatic downloads, using isolated research devices or virtual machines, periodically clearing Telegram caches, and separating investigative and personal environments.

Upload method matters

Telegram distinguishes between media uploaded normally and files uploaded "as documents." Standard uploads may be compressed or transcoded, while files uploaded as documents are more likely to preserve original filenames, metadata, and binary integrity.

File hashes and media fingerprinting

Telegram's media ecosystem creates opportunities for tracking information operations and coordinated campaigns. Recent investigations, including CheckFirst's Operation Overload research, have highlighted how Telegram media artifacts can serve as correlation points across campaigns and dissemination networks.

Common forensic uses

- Duplicate detection
- Malware correlation
- Archive deduplication
- Cross-platform matching

Common hash types

- MD5
- SHA1
- SHA256

Investigators frequently compute MD5, SHA1, and SHA256 hashes against Telegram-exported media. However, Telegram may alter media depending on upload method. As a result, hash mismatches do not always mean different source material, and perceptual hashing may sometimes be more useful than cryptographic hashing alone.

Telegram Clients: Mobile, Desktop, Web, and Translation Workflows

Telegram behaves differently across clients. Each environment offers distinct operational advantages and limitations that directly impact evidence collection, monitoring, and analysis. Investigators should understand how each client works in practice and choose the right tool for the task.

1. Telegram Desktop

For most investigative work, Desktop is generally the preferred client. It is more practical for large-scale review, media triage, exporting data, archival collection, analysis, long-term monitoring, large supergroups, years of message history, comparing media, and preserving evidence.

Export Path: Settings → Advanced → Export Telegram Data

Exports can include chats, media, files, JSON metadata, and HTML archives.

2. Mobile Clients

Mobile clients are useful for real-time monitoring, push notifications, rapid triage, voice communication, and field investigations.
However, investigators must be aware of OPSEC concerns, automatic media caching, device-level metadata exposure, and accidental interaction risks.
Dedicated research devices are strongly recommended.

Review carefully

- Auto-download settings
- Call settings
- Peer-to-peer options
- Location permissions
- Notification previews

3. Telegram Web

Telegram Web is useful for lightweight access, temporary sessions, and compartmentalized investigations.

Browser benefits include session isolation, containerization, disposable workflows, and multi-account management.

Web clients are generally less capable for archival workflows, exports, media management, and long-term investigative review.

Feature parity across Web, Desktop, Android, and iOS is inconsistent. Investigators should not rely exclusively on a single client.

4. In-App Translation

Telegram's native translation functionality is increasingly important for multilingual investigations.

Enable via Settings → Language → Show Translate Button

Translate within Telegram :

- Individual messages
- Entire channels
- Group discussions

Review carefully

- Foreign-language extremist ecosystems
- International influence operations
- Regional conflict reporting
- Cross-border scam networks
- Multilingual propaganda campaigns

Caution: Machine translation may lose nuance, slang, ideological terminology, coded language, sarcasm, or hidden references. Translation is an investigative aid — not a substitute for linguistic expertise.

Organizing Investigations with Chat Folders and Topics

As investigations scale, Telegram can quickly become operationally difficult to manage. Investigators may simultaneously monitor hundreds of channels, multiple language ecosystems, breaking events, extremist communities, scam networks, research groups, collection bots, and alerting channels.
Telegram's folder and topic systems are therefore operationally important, not merely organizational conveniences.

1. Telegram Desktop

Telegram supports custom chat folders that allow investigators to separate communities into structured investigative environments.

Folders can be configured under:

Settings → Chat Folders

Operationally, folders become especially important during large investigations because they reduce noise and allow investigators to move quickly between ecosystems without relying on global search.

Investigators commonly create folders for:

- Active investigations
- Regional monitoring
- Language-specific ecosystems
- Extremist networks
- Cryptocurrency communities
- Collection bots
- Media review
- Archived channels
- High-priority alerts

2. Topics and Sub-Communities Inside Groups

Telegram supergroups may also enable Topics, sometimes referred to as threaded discussions or internal sub-channels.

When enabled, a supergroup becomes divided into separate discussion spaces focused on different subjects. These function similarly to lightweight forum categories or Discord channels inside a single Telegram group.

A single supergroup may therefore contain separate topics for announcements, technical support, regional discussions, media sharing, off-topic chat, or operational coordination.

Why topics matter to investigators

For investigators, topics are important because they segment conversations, reduce noise, reveal internal organization, expose specialized subgroups, and separate operational discussion from social interaction.

In some investigations, the most operationally significant conversations may occur within a small topic inside a much larger community rather than in the primary group feed itself.

Key Takeaway

As Telegram ecosystems grow, organizational features become investigative tools. Chat folders help analysts manage external complexity, while topics help reveal internal structure and the most meaningful conversations inside large communities.

Using Telemetry and Falkor in Telegram investigations

As investigations scale, Telegram can quickly become operationally difficult to manage. Investigators may simultaneously monitor hundreds of channels, multiple language ecosystems, breaking events, extremist communities, scam networks, research groups, collection bots, and alerting channels. Telegram's folder and topic systems help reduce noise and create structure — but investigators also need tools that help them search, monitor, connect, and act on what they find.

Telemetry

Search, monitor, and surface signals

Telemetry supports Telegram investigations with advanced search, discovery, insights, and analytics. It is useful for identifying relevant channels, groups, conversations, and patterns across the wider Telegram ecosystem.

- Broad Telegram search and discovery
- Monitoring across channels and groups
- Insights that help surface relevant signals

FALKOR

Connect findings and move to action

Falkor helps investigators turn collected Telegram signals into structured investigations. It supports linking findings, organizing context, and building clearer investigative workflows across people, entities, and cases.

- Organize findings into investigations
- Connect entities, context, and activity
- Move from signals to actionable insight

How they work together

1. Monitor Telegram ecosystems
2. Search channels, groups, and messages with Telemetry
3. Organize communities with folders and topics
4. Connect findings and investigate further with Falkor

Why folders and topics still matter

Telegram chat folders help investigators separate active investigations, regional monitoring, language-specific ecosystems, archived networks, cryptocurrency communities, collection bots, media review, extremist channels, and high-priority alerts.

Topics inside subgroups reduce noise, reveal internal organization, and help analysts focus on the most operationally significant discussions.

Key takeaway

Chat folders and topics create structure inside Telegram. Telemetry helps investigators find and monitor what matters, while Falkor helps them connect findings and turn those signals into action. Together, they support a more organized and scalable investigative workflow.

Investigation tips and practical workflows

ATelegram investigations are most effective when approached as iterative workflows rather than isolated searches. Investigators should combine platform-native features with cross-platform checks to move from discovery to attribution more efficiently.

1. Reuse handles across platforms

Telegram usernames are frequently reused across platforms. Searching the same handle across social media, forums, GitHub, and crypto services can quickly generate attribution leads.

2. Use filters to reduce noise

Telegram's media, file, and link filters allow investigators to isolate documents, videos, malware samples, external infrastructure, and backup channels without manually reviewing entire histories.

3. Search locally, not only globally

Telegram's local search is often more effective than global search for investigations. Searching within channels and groups for usernames, domains, wallet addresses, invite links, or file types can uncover historical references and operational details quickly.

4. Work as a workflow

A practical workflow often starts with discovery, moves into targeted in-channel search, then isolates media, links, and files for review, and finally pivots into cross-platform attribution and documentation.

Key takeaway

The strongest Telegram investigations are structured and repeatable. Start broad, narrow with local search and filters, and then expand outward through cross-platform analysis to surface stronger investigative leads.

Investigator OPSEC on Telegram

Investigators should treat Telegram as an active environment, not a passive archive.

1. Privacy and Visibility

Telegram supports custom chat folders that allow investigators to separate communities into structured investigative environments.

Under: Settings → Privacy and Security
Investigators should carefully review:

- Phone number visibility
- Profile photo visibility
- Forwarded-message attribution
- Calls
- Group permissions
- Last-seen status

In most investigative contexts, investigators should hide phone numbers, restrict who can add them to groups, limit profile visibility, and use dedicated research accounts.

2. Passkeys, Two-Step Verification, and Account Protection

Investigators should strongly secure Telegram accounts against takeover, phishing, and SIM-swap attacks. Telegram supports both traditional two-step verification passwords and passkey-based authentication.

Two-step verification settings available under:

Settings → Privacy and Security → Two-Step Verification

Passkeys available under:

Settings → Privacy and Security → Passkeys

Telegram passkeys allow authentication using Face ID, fingerprint authentication, device PINs, and platform credential managers.

For investigative accounts, investigators should strongly consider:

- Enabling two-step verification
- Enabling passkeys
- Using unique passwords
- Separating investigative and personal recovery emails
- Monitoring active sessions regularly

Active sessions can be reviewed under:
→Settings → Devices
Investigators should periodically terminate unknown or stale sessions.

3. Automatic Media Downloads

Telegram may automatically download images, videos, documents, or voice messages depending on settings.

Review:
→Settings → Data and Storage → Automatic Media Download

Investigators should strongly consider disabling automatic downloads to reduce exposure to malware, disturbing media, large forensic footprints, and unwanted local storage.

4. Calls, Peer-to-Peer Connections, and IP Exposure

Telegram voice calls can establish peer-to-peer connections between users in some circumstances. When enabled, this may allow the other party to infer network information, including IP addresses.

To reduce this risk:

- Open Settings → Privacy and Security → Calls
- Locate Peer-to-Peer
- Set it to:
  - Nobody
  - Or My Contacts

Investigators should avoid accepting unsolicited Telegram calls from unknown users or targets.

Where operational sensitivity is high, investigators should additionally consider:

- VPNs
- Isolated research devices
- Separate research accounts
- Distinct network environments

Data Export and Evidence Preservation

Telegram Desktop includes native export functionality.

To export data:

1. Open Telegram Desktop
2. Go to Settings
3. Select Advanced
4. Choose Export Telegram Data

Users can export:

- Chats
- Media
- Files
- JSON metadata
- HTML archives

This is operationally significant because entire communities can be archived locally, deleted content may persist in prior exports, and large-scale evidence preservation becomes feasible.

When preserving material, investigators should retain:

- Message links
- Timestamps
- Filenames
- Media files
- Screenshots
- Exported metadata

Stories, Voice Chats, and Ephemeral Content

Telegram increasingly supports ephemeral and real-time communication formats beyond ordinary text messaging.

Stories appear at the top of the interface similarly to other social platforms and may contain images, videos, text, links, and short-lived updates. Although less central investigatively than channels and groups, Stories may expose behavioral patterns, real-time activity, travel indicators, personal associations, or operational timing.

Telegram communities also increasingly rely on voice chats and livestream functionality for real-time communication, coordination, and broadcasting.

Voice chats are especially common in:

- Political movements
- Activist communities
- Extremist ecosystems
- Cryptocurrency projects
- Breaking-news environments

Operationally, voice environments are important because they often contain more candid or immediate communication than text channels. Participants may reveal accents, native languages, geographic cues, behavioral patterns, internal hierarchies, or real-time reactions.

Unlike text content, however, voice chats are often less persistently archived and may disappear unless actively preserved.

Investigators monitoring voice ecosystems should therefore consider:

- Timestamping events
- Recording where legally appropriate
- Preserving participant lists
- Capturing linked chats and surrounding context
- Tracking future scheduled sessions

Administrative Structures and Anonymous Posting

Telegram communities frequently have sophisticated moderation hierarchies.

Administrators may:

- Ban users
- Delete messages
- Restrict posting
- Approve memberships
- Manage invite links
- Post anonymously

Administrative permissions are managed through:

Group Info → Administrators

Anonymous administrator mode significantly complicates attribution because messages appear as originating from the group itself rather than identifiable individuals.

Message Forwarding and Attribution

Forwarding is one of Telegram's core dissemination mechanisms. Messages, media, files, and posts can rapidly propagate across interconnected channels, groups, and private chats through Telegram's native forwarding functionality.

Operationally, forwarding behavior is often central to narrative amplification, propaganda spread, ecosystem mapping, influence tracking, and cross-community coordination.

Forwarded messages may preserve partial provenance metadata including:

- Original channels
- Sender references
- Timestamps
- Source attribution

However, attribution may also be intentionally restricted. Some users and communities disable forwarding attribution entirely, while some channels prohibit forwarding altogether.

Forwarding, Saved Messages, and Personal Archiving

Telegram also includes a feature called Saved Messages, which functions as a private cloud-based personal archive.

Accessible directly from the main chat list, Saved Messages allows users to:

- Store forwarded posts
- Save files and media
- Archive links
- Preserve notes
- Organize investigative material

For investigators, Saved Messages often becomes an operational workspace for temporary evidence collection, media triage, link preservation, cross-device synchronization, and investigative bookmarking.

Because Saved Messages syncs across devices and supports search functionality, many investigators use it as an internal staging environment before exporting or formally archiving material.

Operational Security Culture

Many Telegram communities possess mature operational security practices.

Common behaviors include:

- Rotating invite links
- Backup channels
- Disposable accounts
- Anonymous administrators
- Anti-scraping warnings
- Migration instructions
- Message deletion policies

Sophisticated communities frequently assume persistent monitoring and adapt accordingly.

Investigative Challenges

Despite Telegram's value as an intelligence source, the platform presents substantial investigative difficulties. Many of these challenges stem not from encryption itself, but from the structure and scale of Telegram's ecosystem.

1. Discoverability Limitations

Telegram's native search functionality is incomplete, inconsistent, and often opaque. Public channels and groups may exist for years without appearing reliably in global search results. Communities frequently:

- Rename themselves
- Rotate usernames
- Fragment into backup channels
- Migrate entirely under pressure

As a result, investigators rarely discover ecosystems through Telegram search alone. Discovery often depends on:

- Invite links
- Forwarded posts
- External indexing services
- Cross-platform references
- Third-party tooling
- Human collection

2. Language and Translation Barriers

Telegram ecosystems are highly international, and narratives frequently spread across multiple languages simultaneously. Machine translation helps but is imperfect. Slang, irony, coded language, ideological terminology, memes, and insider references often translate poorly.

Communities may also intentionally manipulate:

- Spelling
- Transliteration
- Unicode characters

...to evade moderation and discovery.

3. Scale and Volume

Large Telegram ecosystems may contain:

- Millions of messages
- Thousands of interconnected channels
- Vast media repositories
- Constant reposting behavior
- Rapid narrative amplification

Without structured tooling and collection workflows, investigators can quickly become overwhelmed by volume alone.

4. Attribution Difficulties

Telegram allows:

- Disposable accounts
- Hidden phone numbers
- Anonymous administrators
- Multiple usernames
- Anonymous member lists
- Rapid migration between identities

Communities may disappear suddenly, reappear elsewhere, or split into multiple successor ecosystems.

5. Operational Security Culture

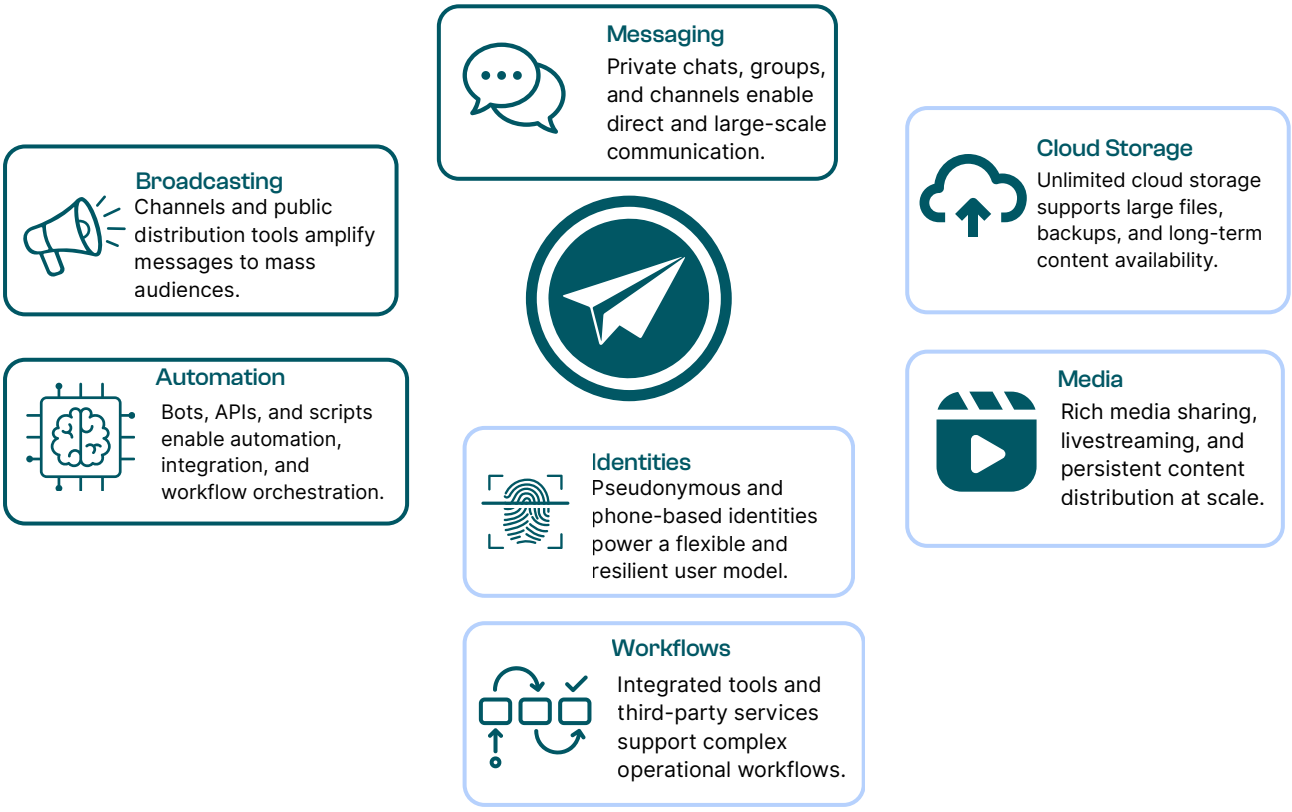
Many communities assume they are being monitored and adopt mature operational security practices, including:

- Rotating invite links
- Vetting new members
- Using backup channels
- Posting anti-scraping warnings
- Limiting forwards
- Deleting messages
- Migrating during enforcement events

These behaviors significantly complicate discovery, tracking, and long-term collection.

Conclusion

Telegram's design, capabilities, and ecosystem dynamics make it one of the most influential platforms of the modern digital era. Understanding how its components interconnect is essential for accurate discovery, contextual analysis, and effective intelligence operations.



Telegram is not merely a messaging platform. It is a hybrid ecosystem combining messaging, broadcasting, cloud storage, automation infrastructure, file distribution, social networking, livestreaming, and blockchain-linked identity systems.

Its scalability, permissive moderation posture, automation capabilities, and media infrastructure have made it central to modern information operations, political mobilization, criminal ecosystems, activist coordination, and online communities worldwide.

For investigators and OSINT practitioners, Telegram offers extraordinary intelligence opportunities — but only when approached with a clear understanding of its architecture, identities, discovery systems, operational behaviors, media ecosystems, and limitations.

Effective Telegram investigations increasingly depend not only on understanding Telegram itself, but also on leveraging external tooling, large-scale analysis systems, and cross-platform investigative workflows capable of operating at ecosystem scale.