lineal

lineal.com

Learn more about better
eDiscovery tech and services.

LINEAL FORENSICS

Forensic Collections Guide 2026

LEARN MORE

Visit us at
lineal.com or email
info@lineal.com.

DATA-FOCUSED LEGAL

Reviewed and refreshed by Lineal's Forensic Collection experts for 2026 to include new and emerging data sources, this guide includes key collection updates for many of the sources.

Introduction

This data collection guide is designed to give readers the building blocks and recommendations for collecting modern data sources. It includes workflows, best practices, and recommendations for data collection and preservation. The collection recommendations in this guide are based on standard eDiscovery and investigation principles. For clients of Lineal, the recommendations set out in this guide help support and enhance data processing and review workflows using Lineal Cloud & the Amplify^{TM} suite.

	Cellebrite	Oxygen	Purview	Google Vault	Native Export	API Extraction
Google Workspace	✓	✓	●	✓	✓	✓
Slack Collections	●	●	●	●	✓	✓
X (Twitter)	✓	✓	●	●	✓	✓
Instagram	●	●	●	●	✓	✓
Meta (Facebook)	✓	✓	●	●	✓	✓
Messenger (Meta / Facebook)	✓	✓	●	●	✓	✓
WhatsApp Messenger	✓	✓	●	●	✓	●
Signal	✓	✓	●	●	●	●
SMS/MMS	✓	✓	●	●	●	●
Telegram Messenger	✓	✓	●	●	✓	●
Microsoft 365	●	●	✓	●	✓	✓
Microsoft Teams	●	●	✓	●	●	✓

Forensic Collections

Generative AI Platforms

The adoption of generative AI platforms such as Microsoft Copilot, Google Gemini, and OpenAI ChatGPT has grown rapidly in business environments. These tools are increasingly integrated into daily workflows, supporting productivity, research, and decision-making.

Interactions with AI platforms can contain business-critical information, including user prompts, uploaded documents, AI-generated content, summaries, and metadata. Collecting data from AI platforms requires a tailored, platform-specific approach due to differences in architecture, retention, and access controls.

Lineal's Capabilities for Capturing Generative AI Data

Lineal provides comprehensive capabilities to identify, preserve, and collect data from generative AI platforms while maintaining forensic defensibility and alignment with enterprise ecosystems such as Microsoft 365 and Google Workspace.

Key capabilities include:

- **Platform-Specific Data Acquisition**
  Capture AI interactions and prompts, uploaded documents, and associated metadata from platforms such as Microsoft Copilot and Google Gemini.
- **Preservation and Defensibility**
  All data is collected in a forensically sound manner, suitable for regulatory, litigation, or internal investigations.
- **Tailored Collection Approach**
  Lineal evaluates platform-specific retention policies, access rights, and organizational configurations to determine the most appropriate collection method—whether full export or selective capture.

Handling Generative AI Data with Forensic Integrity

Lineal applies rigorous forensic standards when collecting and analyzing data from generative AI platforms to ensure accuracy, reliability, and defensibility. AI-generated content can sometimes include hallucinated metadata—artificial or inconsistent timestamps, author fields, or contextual references—that do not reflect actual system events.

Our approach includes:

- **Verification of Metadata**
  Cross-referencing AI-generated metadata against enterprise systems (e.g., Microsoft 365, Google Workspace) to validate authenticity.
- **Documentation & Transparency**
  Clear reporting of any anomalies, including hallucinated metadata, to ensure reviewers and legal teams understand the limitations and context of the data.

This methodology ensures that generative AI–sourced evidence is presented accurately, with a defensible explanation of any inconsistencies, reducing risk in legal or regulatory matters.

Forensic Collections

Enterprise Cloud Systems

Google Workspace

Google Workspace, formerly known as G-Suite, is a subscription-based cloud productivity platform that provides organisations with a suite of collaboration and communication tools, including Gmail, Google Drive, Google Chat, Google Meet, Google Calendar, and other Workspace services. These applications support modern, flexible working practices and enable effective collaboration across distributed teams.

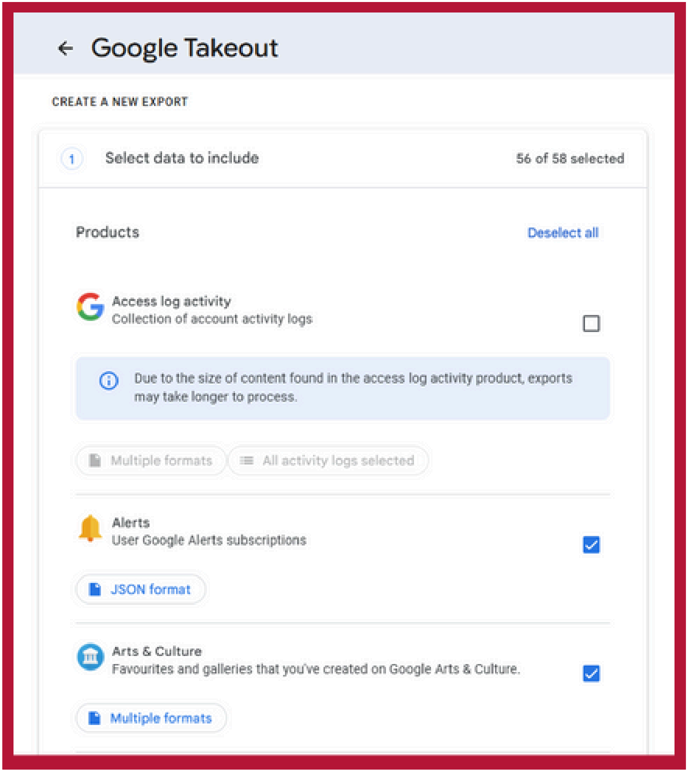
In situations involving legal proceedings, regulatory compliance, or internal investigations, organisations may be required to preserve, search, and collect user data in a defensible manner. Google Workspace includes built-in security, compliance, and eDiscovery capabilities that support repeatable and auditable data collection across multiple data sources.

The most common and recommended methods for collecting data from Google Workspace are Google Takeout and Google Vault. Google Takeout allows for the export of data associated with individual user accounts, whilst Google Vault is designed for organisations that require data retention, legal hold, search, and export capabilities across larger user populations. Additionally, Google provides an admin-level Workspace Data Export tool, which offers more granular control over exported data and may be used in specific collection scenarios.

Google Takeout

Performing a Google Takeout export is a straightforward process that can be carried out by individual users in a few steps.
A Google Takeout export is initiated by navigating to takeout.google.com and authenticating with the relevant Google user account, subject to organisational policies or administrative restrictions.

Once authenticated, the user can select from 58 Google services, including Gmail, Google Drive, Google Calendar, Contacts, Google Chat, Google Meet, Google Docs, and other Google Workspace and account-related services. The number of available services may change over time as Google adds, retires, or restructures products.



← Google Takeout

CREATE A NEW EXPORT

1 Select data to include — 56 of 58 selected

Products — Deselect all

Access log activity
Collection of account activity logs ☐

Due to the size of content found in the access log activity product, exports may take longer to process.

Multiple formats | All activity logs selected

Alerts
User Google Alerts subscriptions ☑

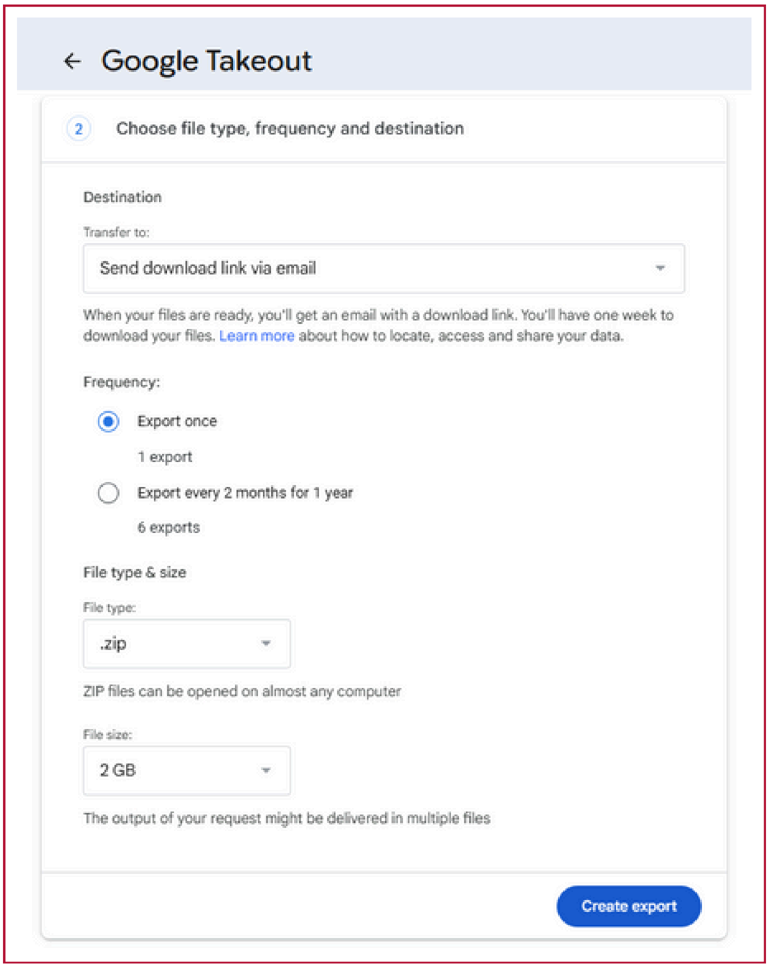
JSON format

Arts & Culture
Favourites and galleries that you've created on Google Arts & Culture. ☑

Multiple formats

If the scope of data required is unknown, it is recommended to select all available services and perform data culling during post-collection processing. Alternatively, a more targeted export can be performed by selecting only the specific services relevant to the matter.

After selecting the desired services, the user can specify the export settings, including the file format (we recommend .zip) and the maximum file size, which can be set to 1 GB, 2 GB, or 4 GB. If the export exceeds the selected size, Google Takeout will split the data into multiple archive files. Once the export is ready, the user receives an email notification with a time-limited download link for each archive file.



2 Choose file type, frequency and destination

Destination

Transfer to: Send download link via email

When your files are ready, you'll get an email with a download link. You'll have one week to download your files. Learn more about how to locate, access and share your data.

Frequency:

● Export once
1 export

○ Export every 2 months for 1 year
6 exports

File type & size

File type: .zip

ZIP files can be opened on almost any computer

File size: 2 GB

The output of your request might be delivered in multiple files

Considerations and Limitations

Google Takeout is a user-initiated collection method and provides limited administrative oversight. Legal holds cannot be applied, and audit logging and chain-of-custody controls are limited when compared to Google Vault. As such, Google Takeout is best suited for self-collection, small-scale matters, or scenarios where Google Vault licensing is not available.

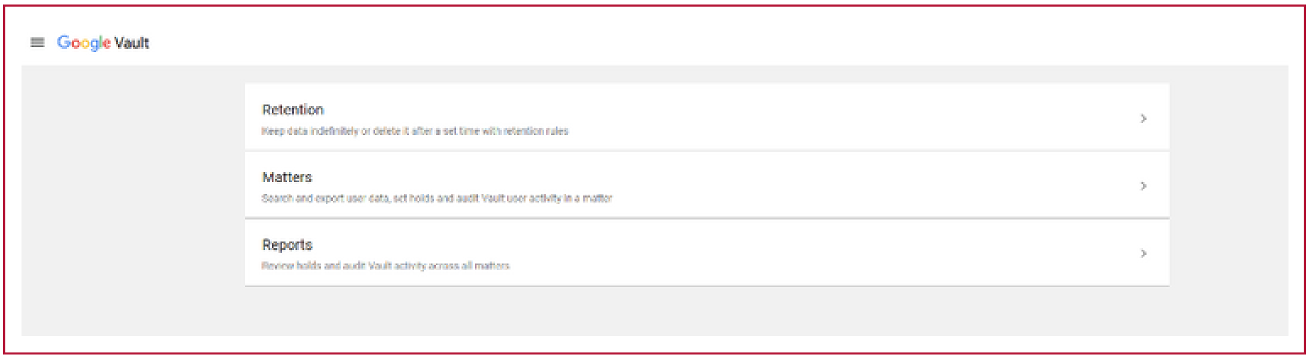
Google Vault

Google Vault is a licensed data preservation and eDiscovery service offered by Google to help organisations protect, retain, search, and export data in compliance with legal, regulatory, and internal investigation requirements. Vault provides an effective method to comply with legal obligations, such as applying legal holds on custodians and targeting or collecting user data while maintaining robust audit logging.

Google Workspace Business Plus, Enterprise, and Education editions include Vault by default. For other Workspace plans, Vault can be purchased as an add-on license, allowing organisations to enable administrative-level retention and eDiscovery capabilities without upgrading the entire plan.

Vault operates at an administrative level, unlike Google Takeout, which is user-level. It supports multi-user searching, retention policies, and exports, making it the recommended solution for scenarios involving large numbers of custodians or enterprise-scale investigations.

Access to Vault is obtained by navigating to vault.google.com and authenticating with an account that has the appropriate Vault privileges. It is recommended to create a Matter for each legal case or investigation, which acts as a repository for all searches, holds, and exports related to that matter, providing a clear audit trail of all actions.



Retention
Keep data indefinitely or delete it after a set time with retention rules

Matters
Search and export user data, set holds and audit Vault user activity in a matter

Reports
Review holds and audit Vault activity across all matters

Once a Matter is created, searches can be conducted across supported data sources, including Gmail, Google Drive (My Drive and Shared Drives), Google Chat, Google Groups, Google Voice, and Google Calendar. Vault also supports the inclusion of Gemini app conversations, enabling admins to search prompts and responses and include them in exports.

For best practices, it is recommended to:

- **Search and export each data source separately.**
- **Perform exports per custodian per data source** to facilitate downstream processing and review.
- When searching Google Drive, **limit exports to files owned by the custodian** to avoid unnecessarily large datasets.
- Use **document IDs or URLs** for targeted collection of known items.
- Include **supplemental files provided by Google**, which contain critical metadata such as timestamps, ownership, and access information.
- Include **Drive-linked attachments referenced in Gmail messages** without requiring a full Drive collection.

Exports from Vault are **time-limited** and remain available for a defined period, so it is important to plan and retrieve data promptly. Vault is **not a backup solution**; its primary role is to support retention and eDiscovery, not operational restores.

Forensic Collections

Microsoft 365

With 354 million people using Microsoft 365 (M365) worldwide, Microsoft's Software as a Service (SaaS) offering has the potential to be a large source of data on any discovery matter. M365 offers a large variety of applications for communication (email and instant messaging), file storage and collaboration. Here, we cover the three most popular products: Exchange Online, SharePoint Online and Microsoft Teams. When it comes to preserving and collecting data from M365 sources, their data governance and compliance tool, Microsoft Purview, is something we recommend using. Its functions include applying legal hold, searching, and exporting data, amongst other things. Many features of Purview are accessible to users who have E3 or E5 licensing. However, data can be exported with the majority of Microsoft's M365 licensing models. It's robust enough and has plenty of documented workflow that it can be used by trained examiners, IT professionals or Legal teams. Below is our recommended purview approach for Email, OneDrive, and Teams chat.

Exchange Online (email)

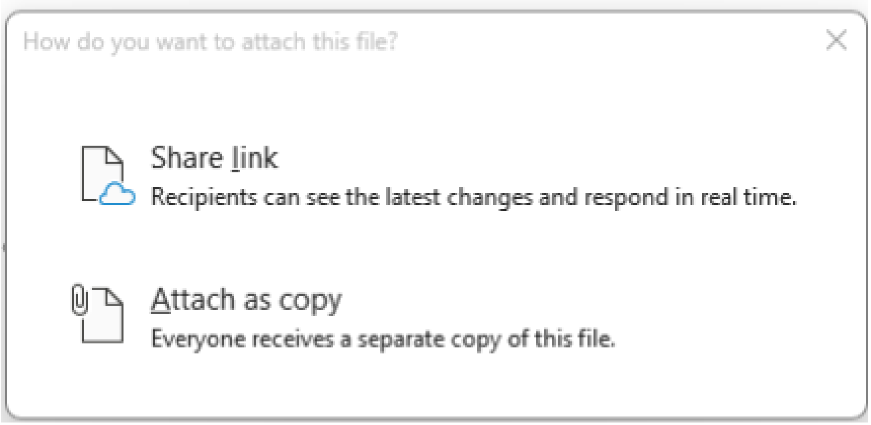
To export mailboxes from M365, Lineal advises that each custodian mailbox be exported in full, by the custodian, in PST format and not de-duplicated. Exports should be run per custodian or in batches to reduce the risk of export errors.

For each mailbox search and export set, the user can produce a set of reports that details what the exports include; errors and settings applied at export. These give great insight and should be exported as part of the process. Lineal has processes in place that review these logs for exceptions and errors, providing assistance if clients decide to perform self-collections.

Within the mailbox export, teams' chat data will also be included. Lineal recommends an exclusion filter is applied to excluded teams chat from the export. Then, run a separate search to only export the team's chat in a separate export set.

This has both source management and tracking benefits, along with better downstream processing and review workflows. Within a mailbox search, Microsoft Purview offers the functionality to apply date range parameters to your search - which filters out any hits of email data that does not fall within the date range parameter applied – reducing the time required to review additional data. Another important consideration to think about when formulating a preservation and collection strategy is the handling of modern attachments.

Modern attachments are where a user attaches a document to an email that is stored in their SharePoint/OneDrive and selects to share a link to the document rather than attach it as a copy.

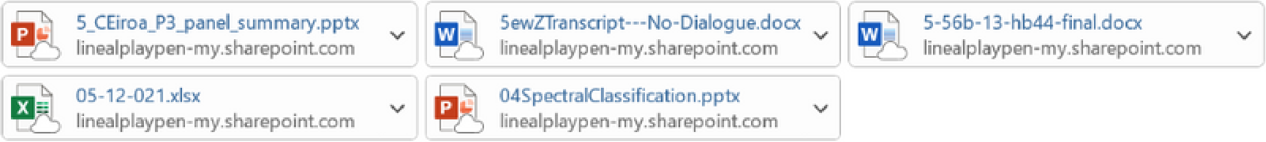


How do you want to attach this file?

Share link
Recipients can see the latest changes and respond in real time.

Attach as copy
Everyone receives a separate copy of this file.

An example of modern attachments is shown below.



5_CEiroa_P3_panel_summary.pptx
linealplaypen-my.sharepoint.com

5ewZTranscript---No-Dialogue.docx
linealplaypen-my.sharepoint.com

5-56b-13-hb44-final.docx
linealplaypen-my.sharepoint.com

05-12-021.xlsx
linealplaypen-my.sharepoint.com

04SpectralClassification.pptx
linealplaypen-my.sharepoint.com

The challenge with modern attachments is that they are stored in SharePoint or OneDrive rather than being embedded directly within the email message. When data is collected using Microsoft Purview, the email itself may be exported, but the underlying document referenced by the link is not included by default. As a result, the associated SharePoint site or OneDrive account where the document is stored must also be collected to ensure the full content is captured.

Lineal recommends that, when dealing with modern attachments, searches and exports are performed using Premium eDiscovery and Investigations within Purview, where licensing permits. This offering provides enhanced support for modern workloads, including Teams chat data, and more robust handling of cloud-based content.

It is also recommended that exports are configured differently from standard collections. Rather than exporting data in a traditional .PST format, the modern attachment workflow favors exporting emails as individual .MSG files and disabling the "friendly name" option. This approach helps preserve attachment references and metadata, supporting more accurate processing and review.

Secondly, using M365 API, known as Graph, to keep modern attachments with the parent email. If considering either of these options, it's recommended to speak to a Lineal consultant to discuss the requirements.

OneDrive & SharePoint

Lineal recommends Purview exports of both OneDrive and SharePoint Data sources. When exporting OneDrive or SharePoint, Lineal recommends full exports or targeted by date range. Exports should be one export per OneDrive or SharePoint site for effective custodian and source tracking. Results should not be de-duplicated, and the export format should be zip file format. Export reports should be generated and included as part of the export set so they can be reviewed prior to data processing. However, it's important to highlight that many corporations set users with 1TB space for OneDrive and way beyond this for SharePoint. Exporting large amounts of data from Purview can be very time-consuming and not without errors. It is recommended that data size reports be generated over SharePoint site and OneDrive accounts so there is a clear picture of how much data will potentially be exported when targeting entire sites or OneDrive accounts. For datasets larger than 500GB, exports should be split, or a targeted collection approach should be considered.

Microsoft Teams

When collecting Microsoft Teams chat data, it is important to ensure that all relevant data locations are included within the scope of the collection. This includes

- User mailboxes, which store messages from one-to-one and one-to-many chats
- Channel mailboxes, which store messages from Teams channels that the user is a member of
- User OneDrive accounts, which store documents shared in one-to-one and one-to-many chats
- Other chat participants' OneDrive accounts, which store documents received during one-to-one and one-to-many chats
- Channel SharePoint sites, which store documents shared within Teams channels.

For the most comprehensive and defensible collection, it is recommended that all of the above locations are collected.

When exporting data using this approach, user and channel mailboxes should be exported in full by custodian, in PST format, and without de-duplication. Similarly, OneDrive accounts and SharePoint sites should be exported in full by account or site, in ZIP file format and without de-duplication.

It should be noted, however, that this approach does not preserve the contextual relationship between chats, channels, and their associated attachments. If maintaining this context is a requirement, alternative collection methods - such as the Microsoft Graph API or Microsoft Purview eDiscovery (Premium) should be considered as part of the collection strategy.

Forensic Collections

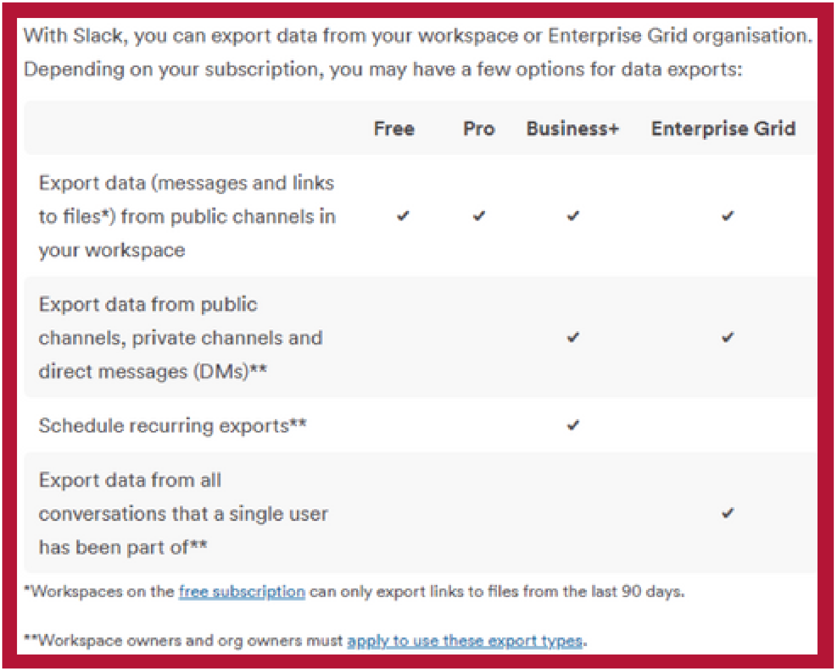
Chat Data Sources

Slack Collections

Instant messaging is often a faster and more utilized method of internal communication within organizations, and with over 40 million daily active users, Slack is one of the world's premiere instant messaging platforms. Slack has functionality for users to communicate via public channels, private channels, and direct messages, along with the ability to share files. This functionality is available to users regardless of the Slack subscription level in place. The subscription level only comes into consideration during any export or collection exercise. There are two main approaches we recommend for collecting Slack data: exporting from within Slack's Compliance center and utilizing Slack's Discovery API. The most notable difference is around the collection of attachment files: with a Slack Compliance export, collection sets will only contain a link to attachments (no actual attachment files will be collected), but by utilizing the Slack Discovery API collection method, the full file can be collected.

Compliance Export

Firstly, it is important to note that the subscription level will affect both the user experience and what is maintained by the system. For example, on a free plan, message history and files are only maintained for the last 90 days. Likewise, business customers can work in Slack channels with people outside their company. Therefore, it's important to highlight that the different levels of subscription and functionality will affect what data is included in a Slack compliance export. All subscription levels can export data from public channels, but only those on higher subscription levels (Business+ and Enterprise Grid) are able to export from private channels, and direct messages (DMs) as well.



With Slack, you can export data from your workspace or Enterprise Grid organisation. Depending on your subscription, you may have a few options for data exports:

	Free	Pro	Business+	Enterprise Grid
Export data (messages and links to files*) from public channels in your workspace	✓	✓	✓	✓
Export data from public channels, private channels and direct messages (DMs)**			✓	✓
Schedule recurring exports**			✓	
Export data from all conversations that a single user has been part of**				✓

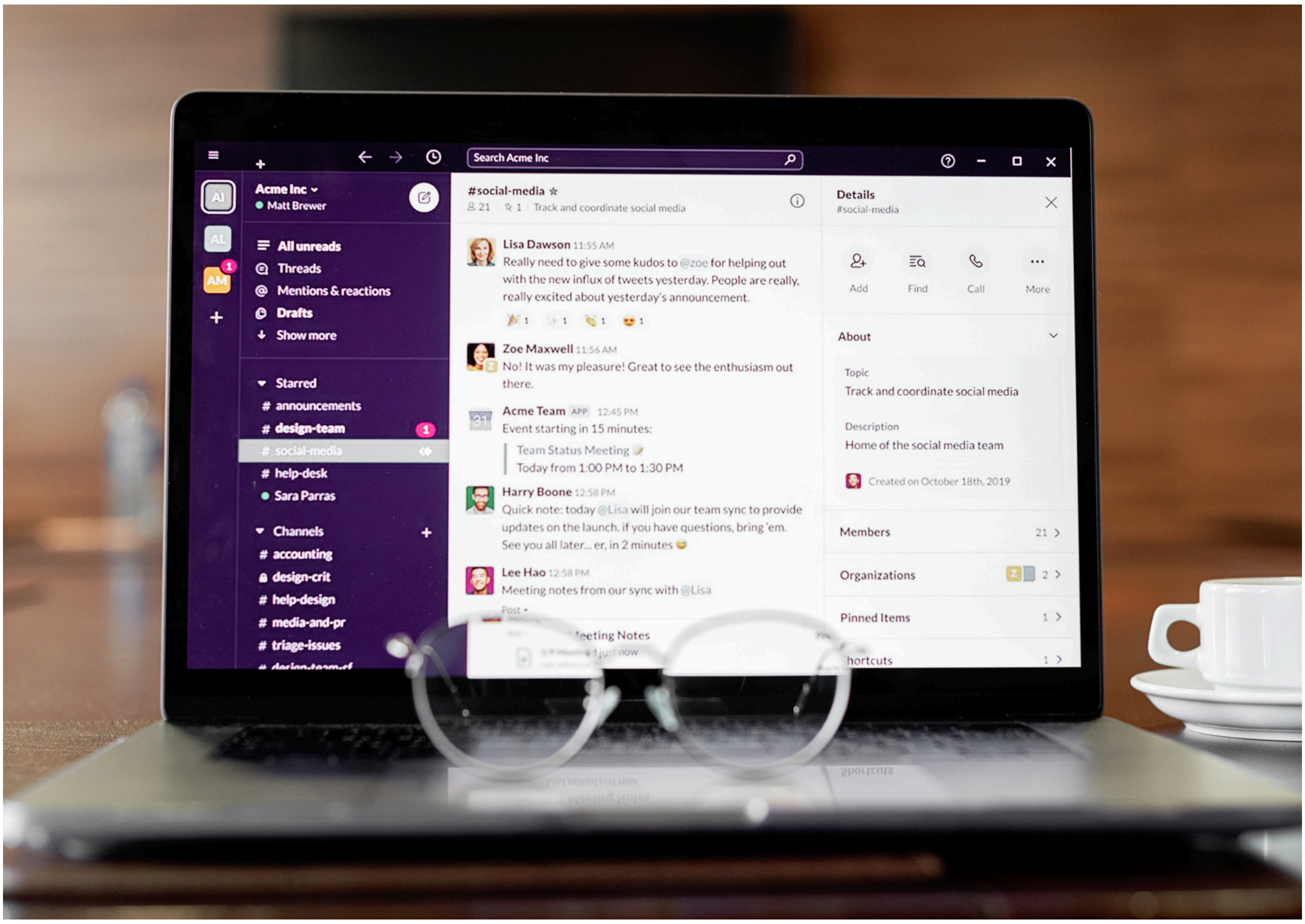
*Workspaces on the free subscription can only export links to files from the last 90 days.

**Workspace owners and org owners must apply to use these export types.

The compliance export method is one of the most common formats accepted when handling Slack data. Lineal has built workflows and applications to streamline the processing and review of Slack data in this format. However, it's important to note that the compliance export only contains chat messages and links to attachments. The actual files sent in a chat channel or private chat are not included. If chat attachments are required, then Lineal recommends an API collection, as discussed below.

Slack Discovery API Collection

Where it is necessary to collect the Slack messages and message attachments, we recommend using the Slack Discovery API. The discovery API provides read-only access to the Slack environment that allows for the collection of all chats as well as any chat attachments. Using the API involves certain requirements, such as the highest Slack license level (Enterprise Grid) and a specialized third-party toolset, and it's advised to speak to a Lineal consultant before using this method.



Lisa Dawson 11:55 AM
Really need to give some kudos to @zoe for helping out with the new influx of tweets yesterday. People are really, really excited about yesterday's announcement.

Zoe Maxwell 11:56 AM
No! It was my pleasure! Great to see the enthusiasm out there.

Acme Team APP 12:45 PM
Event starting in 15 minutes:
Team Status Meeting
Today from 1:00 PM to 1:30 PM

Harry Boone 12:58 PM
Quick note: today @Lisa will join our team sync to provide updates on the launch. if you have questions, bring 'em. See you all later... er, in 2 minutes

Lee Hao 12:58 PM
Meeting notes from our sync with @Lisa
Post
eeting Notes
just now

Forensic Collections

Web Based Data Sources

Social Media

Social media has become more prevalent in legal proceedings and internal investigations over the last decade. The approach to preservation and collection has improved over time; the first rule is always to act swiftly.

Data can be easily deleted, making it extremely difficult to recover. We recommend two collection approaches for the common platforms listed below: native data exports on an account level or utilizing Application Programming Interface (API) access that provides more collection controls.

The most notable difference is who can perform the collection. Social media platforms have made it very easy for authenticated users to export their own data with a few button clicks. Whereas API-based collection requires specialist tools such as Axiom Cyber, which requires trained users to operate.

If a user decides to export their data themselves in a self-collection approach, then the zip containers that contain the exported data should be left in a compressed state and transferred to the legal services provider in the same format. Furthermore, it's recommended that where possible a forensic examiner work with the end user to export and download the data as a further defensibility process.

Along with the two recommended collections types for social media account mentioned above, we also have capabilities to collect public facing accounts/posts if they are of interest. We can utilize tools like WebPreserver or GoFullPage to provide screenshots (In formats such as JPG, MHTML, PDF, etc.) of public facing posts or accounts if they are of interest to the client. With these methods it would require the client to provide any social media accounts or posts that they are interested in collecting and using the tools mentioned above to leverage the collections.

X (Twitter)

The Native Export feature in X allows a logged-in User to download the data X stores on them in either HTML or JSON format. Depending on the amount of data, this can take several days to prepare the data download.

Using the 'download my data' method is very simple. The user needs to log in to X, go to account settings and select 'your account.' Click 'Download an archive of your data', Enter the account password and select confirm. A confirmation code will be sent to the registered email address and/or phone number. Enter this code in the confirmation box, then click on 'request data.' When the download is ready, the user will receive a notification by email or push notification from the app. They can then download the data in .zip format, which can be sent to other applications for processing.

Downloadable data includes:

- Tweets
- Retweets
- Profile information
- Direct messages
- Moments
- Media files
- Address book
- Lists
- Interests and demographic information

Using the 'download my data' method is very simple.

- The user needs to log in to X, go to account settings and select 'your account.'
- Click 'Download an archive of your data',
- Enter the account password and select confirm.
- A confirmation code will be sent to the registered email address and/or phone number. Enter this code in the confirmation box, then click on 'request data.'

When the download is ready, the user will receive a notification by email or push notification from the app. They can then download the data in .zip format, which can be sent to other applications for processing.

API Collection

The X API allows for data capture, similar to the 'download my data' method. However, using the API allows for targeted collections. AN API collection is typically performed with forensic toolsets, such as Axiom Cyber. This approach allows for better post-collection analysis and searching of the data is more efficient than the 'download my data' option. If you are considering the use of API to perform an X data collection, it is advised to speak to a Lineal Consultant.

Instagram

The Native export feature in Instagram is very similar to X and allows logged-in User to download their data in HTML or JSON format.

The export contains the following:

- All archived videos, pictures, and stories
- End-to-end messages
- Profile information
- Comments
- Devices
- Connections, likes, searches, settings, shopping, contacts
- Threads data

To perform this export, the user must follow these steps:

1. Click More in the bottom left, then click Settings.
2. Click Accounts Center, then click Your Information and Permissions.
3. Click Download your Information, then click Request a download.
4. Select the profiles that you'd like to download information from. (Note: you can select a Facebook profile here too, but Lineal recommends keeping these separate and using the Facebook steps listed below.)
5. Click Next.
6. Select the information that you want to download. (Complete copy)
7. Choose the following file options:
    a. The date range (All time)
    b. The notification email – must be an email address associated with the account.
    c. The format of your download request. (HTML)
    d. The quality of photos, videos, and other media. (High)
8. Click Submit request.

Once Instagram has created the data archive, the user will be alerted that it is ready for download. The resulting zip can then be passed on for processing and review.

API

Instagram API allows for data capture, similar to the 'download my data' method. However, using the API allows for targeted collections. The API collection is typically performed with forensic toolsets, which means post-collection, analysis and searching of the data is more efficient than the 'download my data' option. If you are considering the use of API to perform an X data collection, it is advised to speak to a Lineal Consultant.

Facebook

The Native Export feature in Facebook allows a logged-in User to download their data in HTML or JSON format. However, unlike other platforms, Facebook allows users to selectively choose what data they want to include in the export, the media quality and the date range. Lineal recommends preserving all available data and then culling post-collection.

If all data is exported, then the following data is preserved:

- Profile Information
- Contact info
- Activity: posts, likes, tagged photos, comments, groups, Marketplace
- Photos
- Videos
- Friends
- Pokes
- Messages, Inbox
- Events
- Security details, Location History

To export the data from Facebook, a logged-in user should follow these steps:

1. Click on your profile picture in the top right, then click Settings & privacy.
2. Click Settings.
3. Click Accounts Center, then click Your Information and Permissions.
4. Click Download Your Information.
5. Click Request a Download.
6. Select the profiles that you'd like to download information from. (Note: you can select an Instagram profile here too, but Lineal recommends keeping these separate and using the Instagram steps listed above.)
7. Click Next.
8. Select the information that you want to download. (Complete copy)
9. Choose the following file options:
   a. The date range (All time)
   b. The notification email – must be an email address associated with the account.
   c. The format of your download request. (HTML)
   d. The quality of photos, videos and other media. (High)
10. Click Submit request.

Legal Process

Provided that legal authority is given (usually a court order), many social media sites have a process in place to provide the information that it stores on its users. Published guidelines from the most popular platforms can be found here.

https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support

https://www.facebook.com/help/instagram/494561080557017

https://www.facebook.com/help/494561080557017/

Forensic Collections

Mobile Devices & Chat

Mobile devices are among the most complex and volatile sources of electronically stored information (ESI). Advances in encryption, operating system security, application design, and cloud synchronization—combined with the widespread use of ephemeral messaging—continue to complicate defensible collection methods.

The method, timing, and scope of a mobile device collection directly determine the data that can be preserved and analyzed. As such, selecting the appropriate acquisition method at the outset is critical to avoiding data loss, re-collection, or evidentiary challenges.

Pre-Collection Assessment:

Prior to performing any mobile data collection, Lineal conducts a pre-collection assessment to determine the most appropriate acquisition methodology and to set clear expectations regarding the data that can be captured. The outcomes of this assessment directly influence both the scope and technical feasibility of the collection.

Key considerations include:

What are the collection requirements?

- What data is required from the mobile device (e.g., chat data, email, browsing history, documents, media)?
- Clearly defining the data requirements is critical, as it may dictate the available collection methods and level of access required.

What is the device make, model, and operating system version?

- The device type and OS version directly impact whether certain applications can be accessed, and which collection methods or formats are supported.

Are there Mobile Device Management (MDM) policies in place?

- MDM solutions may restrict or disrupt mobile data collections through enforced security controls.
- Where MDM is present, consultation with relevant IT personnel is recommended to understand policy limitations and to assess whether alternative collection approaches are feasible.

What is the device state and access level at the time of collection?

- Factors such as passcode availability, biometric access, encryption status, device condition, and network connectivity can affect collection feasibility and method selection.
- Understanding the device state in advance helps reduce delays, minimize handling risks, and ensure the most comprehensive and defensible collection possible.

Mobile Device Collection Formats

The selection of a mobile device collection format directly impacts the scope, completeness, and forensic value of the data acquired. Each collection method offers differing levels of access based on device type, operating system, security controls, and collection objectives. Where possible, the most comprehensive method should be selected to maximize data preservation and defensibility.

Physical Extraction

Most Comprehensive Collection Method

A physical extraction provides the deepest level of access to a mobile device and is considered the most comprehensive collection method available. This approach may capture:

- Operating system and system-level files
- Application and user data
- Deleted data and, in some cases, unallocated space

Physical extractions are recommended when:

- Deleted or hidden data recovery is required
- Devices require in-depth examination of forensic artefacts
- System-level artifacts are critical to the investigation

Due to evolving hardware security and operating system protections, physical extractions may not be feasible for all devices or OS versions. When achievable, however, this method offers the highest forensic value and long-term defensibility.

Full File System Extraction

Comprehensive Alternative

A full file system extraction captures the accessible file system of a mobile device, including:

- Files and directories
- Application data (including some secure apps) and databases
- System and configuration files
- Limited deleted artifacts

While this method does not provide access to all storage areas and is therefore less comprehensive than a physical extraction, it represents the next best available option and is supported across most modern iOS and Android devices.

Full file system collections provide an increased opportunity to identify forensic artifacts associated with ephemeral or disappearing messages from applications such as Signal and Telegram. Recovery of such data remains dependent on factors including device usage patterns, storage behavior, encryption, and the time elapsed since deletion.

Advanced Logical Extraction

Targeted, User-Level Collection

An advanced logical extraction focuses on capturing primarily user-generated data, such as:

- SMS and MMS messages
- Contacts and call logs
- Documents and media files
- Supported application-level data

This method does not provide access to the full file system and therefore offers limited visibility into deleted data or system artifacts. Advanced logical collections are best suited for matters where:

- The scope is narrowly defined
- Time or cost constraints exist
- Only specific data types are required

Application coverage varies by device and operating system. For example, on Android devices, certain third-party chat applications (e.g., WhatsApp) may require elevated collection methods to be fully captured.

Remote Mobile Device Collections

Lineal offers secure remote mobile device collection capabilities designed to rapidly and efficiently acquire mobile data without the need for physical device access. Leveraging advanced technology, remote collections can often be completed within hours, minimizing disruption to custodians while maintaining data integrity and security.

Remote collection capabilities support both iOS and Android devices and are particularly well-suited for geographically dispersed custodians or time-sensitive matters.`

Key Capabilities

Rapid Data Acquisition

- Perform collections quickly, often within hours, reducing delays associated with device shipping or in-person collection.

Secure Data Transfer

- Collected data is encrypted and transferred directly to Lineal's secure servers for immediate processing and analysis.

Configurable Collection Parameters

- Tailor collection scope to align with matter-specific requirements, including data types, and application focus.

Minimal End-User Involvement

- Designed to reduce custodian effort and business disruption while maintaining collection defensibility.

User-Friendly Experience

- Intuitive workflows enable efficient collections with clear guidance for end users, reducing error and support overhead.

Selective Mobile Collections (iOS & Android)

Lineal's remote collection process also supports selective mobile data acquisition, allowing targeted collections that focus on relevant information while minimizing exposure to personal data.

Selective Collection Benefits

Targeted Data Types

Collect specific categories of data such as:

- Chat and messaging data
- Media (photos, videos, audio)
- Calander entries
- Call logs and contacts

Reduced Data Volume

- Limiting collection scope helps reduce data bloat and expedites downstream processing and review.

Privacy-Conscious Approach

- Less intrusive to personal data, making selective collections well-suited for BYOD environments and privacy-sensitive matters.

Important Considerations

Due to operating system security controls and application-level encryption, certain chat or messaging applications may not be available for collection through remote or selective acquisition methods. Remote mobile collections leverage an advanced logical approach, which may limit access to specific third-party applications or deleted content.

Where critical data types are identified as being in scope, further discussion with a Lineal forensic consultant is recommended to assess feasibility and determine whether an alternative collection method—such as a full file system or physical extraction—is required.

Onsite Mobile Device Collection Capabilities

Lineal provides onsite mobile device collection services for matters requiring direct device access, advanced extraction methods, or enhanced forensic oversight. Onsite collections are particularly suited for complex devices, secured applications, and scenarios where remote collection is not feasible or appropriate.

Key Capabilities

Rapid Onsite Deployment

- Forensic consultants can be deployed onsite within 24–48 hours, enabling timely response for urgent or high-priority matters.

Global Coverage

- On-site mobile collections are supported worldwide, allowing Lineal to service custodians across multiple jurisdictions while maintaining consistent standards and defensibility.

Specialized Forensic Hardware & Expertise

- On-site collections are performed using specialized forensic hardware and industry-leading tools operated by experienced forensic consultants, enabling full file system extractions from modern mobile devices where technically feasible.

Access to Secured and Complex Data Types

- Direct device access allows for the collection of secured chat applications and other complex or restricted data types that may not be accessible through remote or logical collection methods.

Better eDiscovery
and Investigations

Forensic Collections Guide 2026

LEARN MORE

Visit us at
lineal.com or email
info@lineal.com.

DATA-FOCUSED LEGAL

Reviewed and refreshed by Lineal's Forensic Collection experts for 2026 to include new and emerging data sources, this guide includes key collection updates for many of the sources.