

Cutting Us Some Slack

Joseph Pochron whos us how to use Onna to acquire data from Cloud Collaboration tools like Jira, Confluence, and Slack.

Are you ready for it? The Slack revolution is upon us. In 2015, an article was posted on Time.com titled “How E-Mail Killer Slack Will Change the Future of Work.” The good news is, Slack has yet to replace email; the bad news is if you haven’t heard of or dealt with Slack, you need to read this article and get up to speed because it’s going to show its face in your investigations or legal discovery. For context, Slack’s usage by a global workforce is staggering the interoffice chat app boasts 8 million users, and is valued at \$7 billion. On February 4, 2019, Slack confidentially filed for IPO, with the hope of reaching a \$10 billion valuation.

Slack, at its core is a highly organized instant messaging platform that allows users to create channels or message other users. Channels can be public, private, and can be named to the user’s liking. Similarly, users can send private messages to a single or group of Slack users. Additionally, a user has the option to add file attachments to channels or messages, introducing another item of evidentiary value. There’s also a historical component to Slack; many instant messaging platforms are ephemeral by design. Slack channels retain their posts and any user that can access the channel can read historical posts. As I mentioned prior, Slack’s popularity has dubbed it the “email killer” and a driver of changing how we communicate in the workplace, but the data retention component also makes it attractive to replacing certain elements of file/network shares.

Who Needs to be Concerned About Slack?

eDiscovery refers to the discovery process of electronic data as it relates to litigation or government investigations. It’s estimated that the global eDiscovery market will jump from a \$.924 billion industry to \$18.9 billion by the year 2020. What some readers may not know, is that the first step in eDiscovery is the need for a proper and legally sound collection of data. For this reason, digital forensic professionals are often used to ensure data integrity and minimize arguments of metadata or data spoliation. Digital forensic professionals working in eDiscovery have been faced with a significant challenge over the last few years collecting data from cloud-based platforms.

These platforms, commonly referred to as “P.a.a.S. (aka Platform as a Service) or “S.a.a.S (aka Software as a Service)”, have grown increasingly popular in businesses due to their ability to connect a global workforce. In fact, cloud adoption continues to grow worldwide on average organizations have 730 cloud apps, with 25% utilizing over 1000 cloud apps. Additionally, these applications can be run from a web browser, computer, or a mobile device, elevating the Examiner’s need to be knowledgeable on where data collection can and should take place. ▷

Slack’s popularity has dubbed it the “email killer” and a driver of changing how we communicate in the workplace.



Review is Important

It's important to remember, for eDiscovery matters, the format of legal review is just as important as the ability to acquire this data. Know your 3rd party tool and how it can transfer data to review platforms like Relativity. It's important to identify that Slack's corporate export is not provided in a "review-friendly" format and additional conversion is needed to allow for legal review.

The implementation of these applications in the business world have changed how teams communicate and interact, but present real challenges in the world of digital forensics and eDiscovery. Although there's a litany of these application currently in the marketplace, I'm going to focus on Slack due to the immense popularity and the volume of users. It's also worth noting the need for a digital forensic examiner to acquire and analyse data from Slack, or similar applications for corporate investigations is not only needed but will be vital in coming years. Digital Forensic professionals dealing with corporate investigations or eDiscovery will need to understand the best practices, and limitations on acquiring Slack for forensic analysis.

From an eDiscovery and digital forensic perspective, it's important to understand a vital characteristic of the "cloud-based" era that impacts our ability to acquire data. Even if it hasn't been explicitly stated, it's clear that, philosophically, most companies are not in the market of building eDiscovery products, or mechanisms that export data to the same standard that industry professional have grown accustomed to obtaining and reviewing. Aside from Microsoft's Security and Compliance or Google's Vault for GSuite products, the ability to acquire, search, refine, and isolate data will vary greatly per platform.

So how does the forensic examiner obtain Slack data? The answer really depends on the organization, their retention plan, and current plan in place. Let's look at a few options.

Export Directly From Slack

Also referred to as Slack's "corporate export" this allows a Workspace Owner or Slack Admin to export messages and files from public channels. Although this is a great feature made freely available by Slack, its immediate usability for discovery or analysis are a bit challenging. Messages from public channels will be exported in a JSON format, a format not very user-friendly for large-scale legal review or manual forensic analysis. Additionally, the export will contain a JSON file for each day the channel was in use, potentially resulting in hundreds of files per channel. If the organization is a heavy Slack user, the volume of data can quickly mount at this stage in the process.

It's important to note that the type of Slack plan in place affects the data you can immediately access. Public channel data is readily available to a Workspace owner or Slack

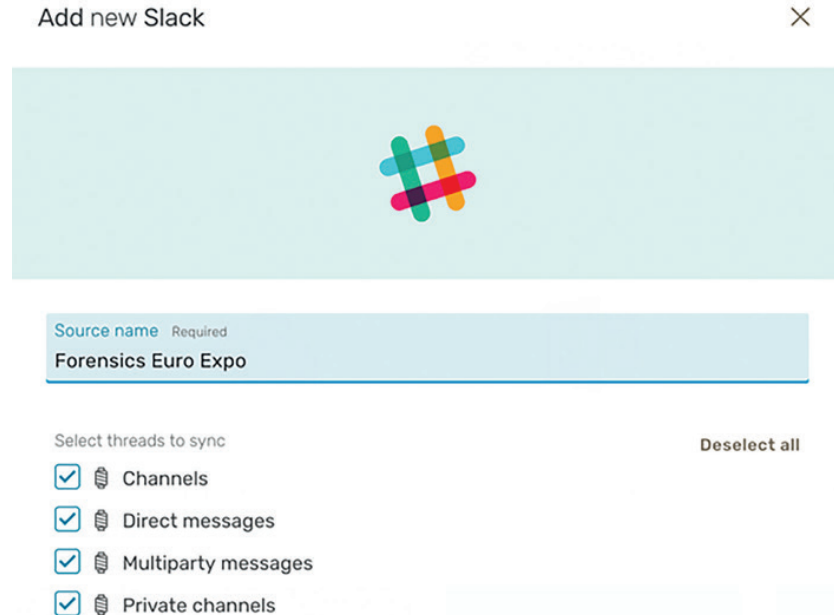


Figure 1. Onna Discovery API

admin on the Basic and Plus plans. As of May 25th, 2018, Slack did away with the Compliance Export, replacing it with "Corporate Export." The Corporate Export is available for Plus plans and no additional charges are required to implement this tool. However, in what appears to be a move to ensure EU GDPR and general legal privacy compliance, Slack requires workspace owners and admins to apply to Slack to gain access to their workspace private channel and private message data. Slack requires the submission of either legal process, employee consent, or a requirement under applicable law. Slack requires this sent with the application, otherwise the application will most likely be rejected.

Presuming that the application is accepted, and all public and private Slack data is obtained, it's important to note that for Basic and Plus plan users, file attachments will be provided via links within the JSON file. If an examiner needs to collect or analyse those files, a separate task to download those items will be required. Collecting from user's on Slack enterprise plan will be a different experience; although the message data is still provided as JSON files, private message and channel data is produced without the need of going through the application process because that is baked into the upgrade process.

3rd Party Archive

A relatively new feature for Slack eDiscovery is the collection of Slack data from third-party archive systems. These types of platforms, such as Smarsh or Global Relay, for example,

Know your Client's Retention Policy

4 options exist:

- Keep everything
- Keep all messages, but don't track revisions
- Delete messages and their revisions after
- Let workspace members override these settings

Information governance

Talk to your client's about information governance

- Put a litigation readiness plan in place
- Develop a game plan for Slack archiving
- Utilize an archive that can export this data for legal review
- Know your internal costs to export data from your archiving solution
- Choose an archive or tool with legal hold options for Slack data.

```
Today, 10:01 AM [AUDIT][UPLOADED and synced into App][CFPD1E25P20190126](Channel #forensicseuroexpo jpochron - 2019-01-26 (UTC))
Today, 10:01 AM [AUDIT][UPLOADED and synced into App][CFR36QC3H20190126](Channel #forensicresearch jpochron - 2019-01-26 (UTC))
Today, 10:01 AM [AUDIT][UPLOADED and synced into App][CFPD1JZ0R20190126](Channel #digitalforensicsmag jpochron - 2019-01-26 (UTC))
```

Figure 2. Onna Audit Logging of Data

```
Today, 10:01 AM Channel #forensicseuroexpo jpochron - 2019-01-26 (UTC) metadata_extraction Done.
Today, 10:01 AM Channel #forensicseuroexpo jpochron - 2019-01-26 (UTC) metadata_extraction Done.
Today, 10:01 AM Channel #forensicseuroexpo jpochron - 2019-01-26 (UTC) metadata_extraction [x] Now processing...
Today, 10:01 AM Channel #forensicseuroexpo jpochron - 2019-01-26 (UTC) metadata_extraction [x] Now processing...
Today, 10:01 AM Channel #forensicresearch jpochron - 2019-01-26 (UTC) metadata_extraction Done.
Today, 10:01 AM Channel #forensicresearch jpochron - 2019-01-26 (UTC) metadata_extraction Done.
```

Figure 3. Onna Processing Audit Logs

A relatively new feature for Slack eDiscovery is the collection of Slack data from third-party archive systems.

have been great systems for retrieval of more traditional data types such as email, and clearly recognized the importance of adding Slack as a possible archiving source. From the author's perspective these work well for information governance and retention scenarios. If your corporate client already has these systems in place, the ability to obtain Slack data will be efficient; if your client doesn't have this in place you'll need to look towards a "one-off" solution.

Discovery API

Luckily for forensic and eDiscovery professionals, Slack provides a stronger, alternative option for data acquisition. Through Slack's Discovery API, calls can be made to collect all available Slack data. Attachments, provided as links in the corporate export, are available for collection through the Discovery API, a significant reduction of time and providing a more comprehensive data collection. There are a few tools that connect to Slack via their Discovery API. I've found Onna to be the most useful and efficient for leveraging the Discovery API, which I'll highlight below, but no matter what tool used, archiving or real-time collection, the benefits of utilizing Slack's Discovery API should be the key takeaway.

Connectivity

Onna provides an easy interface for connecting to a Slack account via the Discovery API. The Discovery API will allow the examiner to collect all public channels, private channels, multiparty

and private messages. Additionally, if only the collection of one type of data, private messages for example, this level of granularity is possible.

An important feature of the Discovery API for the forensic examiner is the ability to acquire edited or deleted messages. This feature is impacted by retention settings in Slack Enterprise, but retention is set to "keep everything" by default, so unless the admin has altered that setting, deleted messages will be intact and available through the Discovery API. This is a crucial feature for forensic examiners to understand if Slack communication is important to their forensic analysis, obtaining Slack data through the Discovery API rather than Slack's corporate export or through data recovered from Slack databases on a physical device should yield a broader set of evidence. Granted, the need to authenticate to the Slack environment is needed to obtain user data through the Discovery API, which may not always be possible in the investigation, but if it is, it's important to understand that the recovery of deleted data is available.

Logging

Any tool a forensic examiner is using should have the ability to verify the data or evidence collected. One important feature of Onna's interface, is the audit logging of data collected through Slack's Discovery API. This allows examiners, in real-time to confirm data that's been collected, but also review any errors that may have occurred. >

EXPERT TIP

To avoid a high level of duplication when exporting data through the Discovery API, it's recommended to collect all public and private channel data through an admin account. Even if the admin is not active in each and every channel, the privileges of the admin account can export all channel data.

WARNING

Readers should be aware that Slack's Free Plan will only retain 10,000 messages per workspace. This is important to keep in mind when developing a strategy and workflow!

Rather than dealing with JSON files, Onna will render Slack message data to HTML and file attachments will be preserved in their native form. For this reason, the examiner is also presented with processing audit logs, while data is being prepped for export or immediate searching.

Real-Time Searching

The real strength of Onna for the forensic examiner is the search capabilities that it has to offer. Additionally, as data is acquired and processed, the ability to start searching and analysing data in real-time is doable, providing a bonus triage component. Once the connection between Onna and Slack completes, data will start to sync and populate the dedicated workspace for that matter. Since a full sync of data can take a several hours to complete, having immediate access to partially collected information helps to expedite analysis in a triage-style approach.

From the author's perspective, a lot of buzz has been created about "how" to collect Slack data, especially due to the popularity and spike in the sheer volume that requires collection and analysis. Tools like Onna that can import this data, but also provide the granularity post-processing to run complex searches and find the responsive document or relevant evidence, is huge. It seems to be a forgone conclusion that Slack will continue to gain in popularity which means more Slack data showing up in litigation or investigations. Sifting through that data will continue to be a complex task; having a game plan ahead of time will be paramount. As it relates to searching, there's a few crucial points to keep in mind.

Archiving

An organization can choose to archive channels; they are "deleted" from the organization's Slack workspace, but they are no longer in rotation for communication purposes. The following screenshots show a search of "CPSO" and "Calypso" across a Slack workspace by a Slack admin.

As you can see in Figures 4 and 5, neither term returned any positive hits. We then collected the same Slack workspace through Onna and ran the same search criteria.

As you can see in Figures 6 and 7, we now return positive hits on our

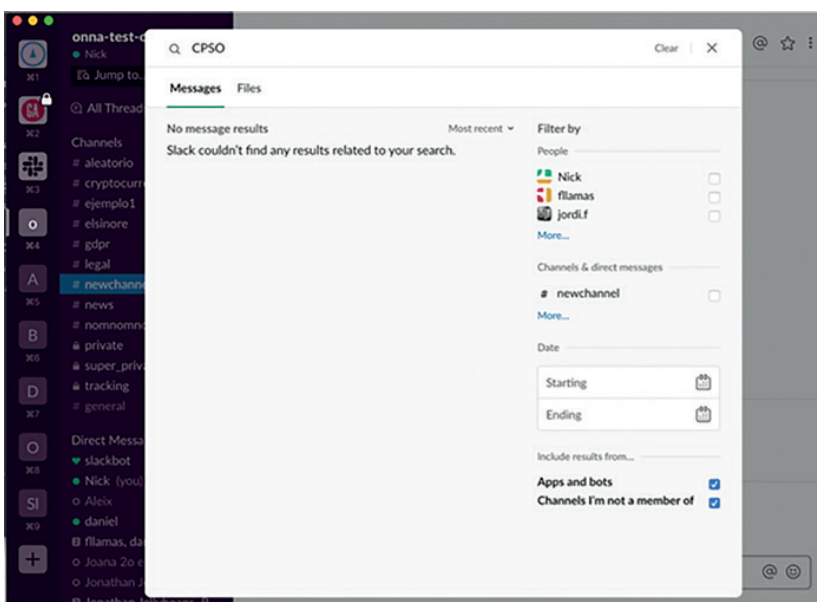


Figure 4. CPSO Search

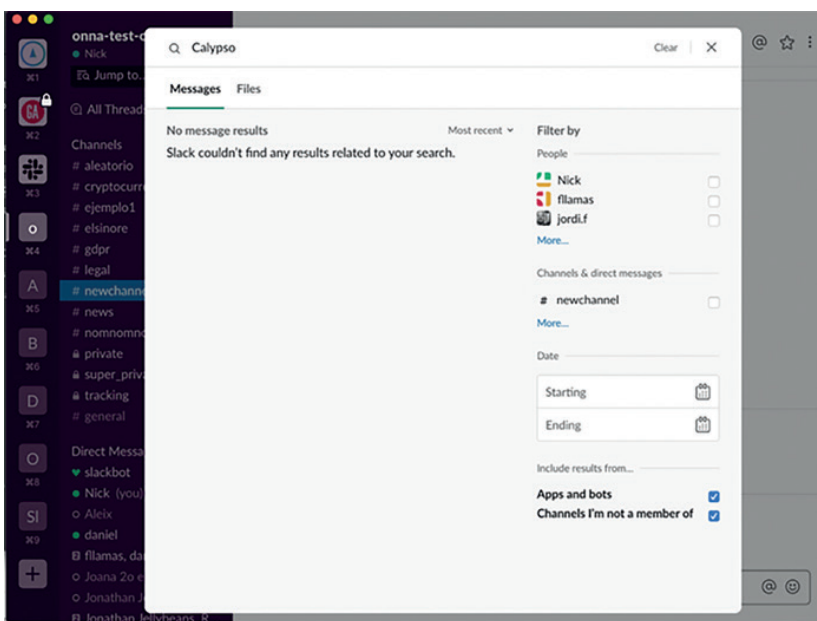


Figure 5. Calypso Search

search criteria. Why the difference?

This highlights an important nuance to how examiners acquire data from cloud-based platforms. The hits did not return any results within the platform, even with admin-level credentials because the channel was archived and, therefore not searchable. Through Slack's Discovery API, we're able to acquire archived channels, have that data processed to make it searchable, and we now receive positive results from the archived channel.

Deleted or Edited Messages

It's also worth noting the presence of deleted or edited messages in the screenshots. Most forensic professional will want to obtain deleted messages as part of their investigation. It's important to understand that deleted or edited messages are not provided in the corporate export, even if you have a client that successfully exports data through Slack's native corporate export, you won't obtain this information and will need to utilize the Discovery API to acquire this data.

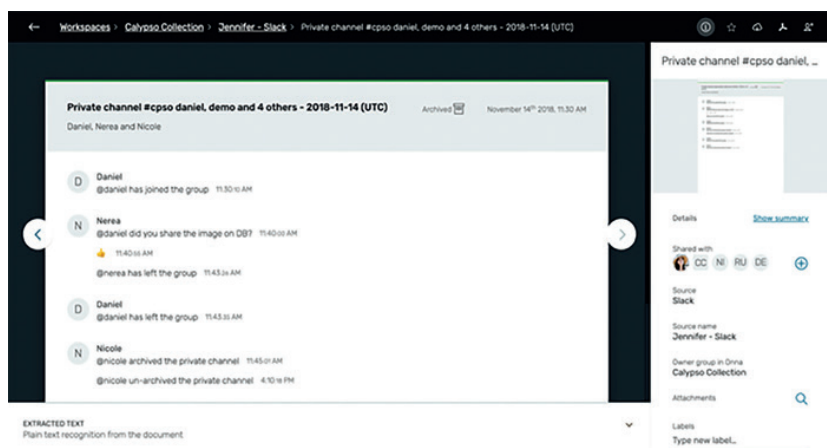


Figure 6. CPSO Search Using Onna

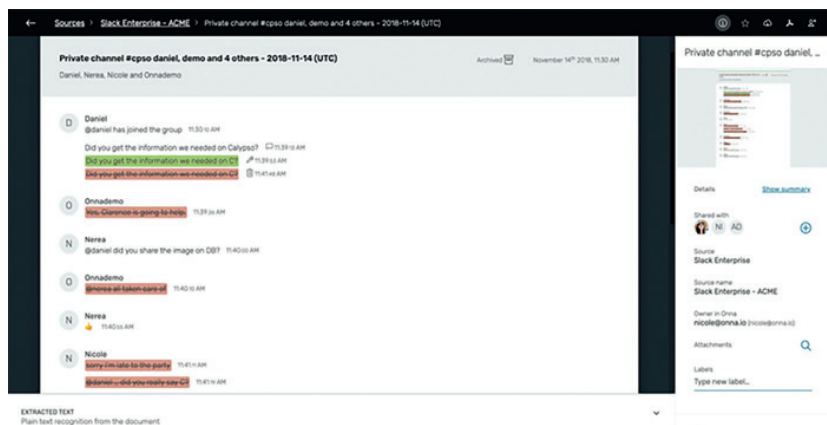


Figure 7. Search Using Onna

It's important to understand that deleted or edited messages are not provided in the corporate export, even if you have a client that successfully exports data through Slack's native corporate export, you won't obtain this information.

Conclusion

The popularity of Slack simply enhances a trend in digital forensics acquisition of data from the endpoint, especially for business, forward platforms like Slack will not be sufficient for forensic analysis. Examiners will also need to research and comprehend the strengths and limitations of data acquisition through the various options available to them. Understandably, this approach to data acquisition of cloud-based solutions is not a "one-size-fits-all"

for forensic examiners. Public sector forensic examiners primarily working on "street" crimes instead of "suite" crimes will probably not see much value in this approach. But for the rest of the digital forensics' community, working on corporate investigations, or being utilized in an eDiscovery capacity, these practices will be important to implement as Slack continues grow. Who knows, maybe we'll need to write a follow-up article in two years when Slack has replaced email. •

FURTHER READING

<https://abrignoni.blogspot.com/2018/10/finding-slack-app-messages-in-ios.html>
Great blog post by Alexis Brignoni on Slack forensic artefacts within iOS. Extremely useful for those examiners that can't use the tips from this article and are left with just the mobile device.

<https://abrignoni.blogspot.com/2018/09/finding-slack-messages-in-android-and.html>
Another great blog post from Alexis Brignoni on Slack forensic artifacts on Android. Follow his research either at his blog "Initialization Vectors" or follow him at his twitter handle @AlexisBrignoni!

REFERENCES

1. <http://time.com/4092354/how-e-mail-killer-slack-will-change-the-future-of-work/>
2. <https://www.forbes.com/sites/curtissilver/2019/02/04/slack-confidentially-files-for-ipo-because-its-a-tech-company/#438eaf987f85>
3. <https://www.oxfordjournal.com/state-of-e-discovery-2018/>
4. <https://www.oxfordjournal.com/state-of-e-discovery-2018/>
5. <https://www.netskope.com/wp-content/uploads/2015/04/NS-Cloud-Report-WW-Apr15-RS-00.pdf>
6. <https://get.slack.help/hc/en-us/articles/201658943-Export-your-workspace-data#apply-to-download-all-data>



Joseph Pochron is the President of TransPerfect's Forensic Technology and Consulting division. He provides advisory services for clients around the world, developing strategy and executing projects related to digital forensics. Based in San Francisco, he helped expand TransPerfect's legal services into the San Francisco, Los Angeles, and Chicago markets. He leads a global network of forensic labs and technical specialists in the U.S., Europe, and Asia.