CELLEBRITE ANNUAL

Industry Trend Survey

2019: Law Enforcement

Cellebrite

Digital intelligence
for a safer world

Table of Contents

Executive Summary

Cellebrite recently conducted an industry trends survey targetting Law Enforcement. The two main purposes of the survey were to ask Law Enforcement personnel:

1. What types of digital data being used in modern-day investigations are most important?
2. What role does technology play in resolving investigations?

The prominent role digital data plays in criminal cases has previously been acknowledged (85% of criminal investigations include some form of digital data), so establishing the relevancy of collecting digital data was not a focus of the survey. Instead, the survey focused on the impact of digital data in investigating and prosecuting criminal cases including:

- What types of digital sources are being used in investigations.
- Which digital sources and data are most frequently used and considered the most important.
- The challenges to accessing digital data.
- The impact to productivity and ability to resolve investigations.

Methodology

The survey was conducted online. Email communications were sent to known members of Law Enforcement requesting them to complete the survey. The invitation was sent to a global audience. The first question in the survey asked recipients to identify their roles within their organizations. The four roles they could choose from were:

- Investigator
- Examiner
- Agency Manager
- Prosecutor

Response

Over 2700 Law Enforcement personnel completed the survey with the majority of the respondents coming from investigators and examiners. The responses and the volunteered comments provided valuable insight into how Cellebrite should develop solutions going forward. Armed with the information gathered in the survey, Cellebrite can hopefully direct future innovation toward areas that will have the most impact to accelerate time to evidence and expedite the resolution of investigations.

Key Findings

Some of the more important points gathered from the survey included the following:

- Mobile phones remain the most frequently used and most important digital source for investigations.
- The variety of digital sources used in investigations is increasing. Sources, such as Wearables and Smart Home Technology, are being used with more frequency during investigations.
- The two most common challenges to extracting data from mobile phones are locked phones and encrypted data.
- Law Enforcement agencies are averaging 3-month backlogs on investigations.
- Despite the backlogs, variety of digital sources and the amount of digital data that typically needs to be reviewed in an investigation, the vast majority of Law Enforcement agencies are reviewing this information manually instead of using analytics solutions.

Investigator

Overview

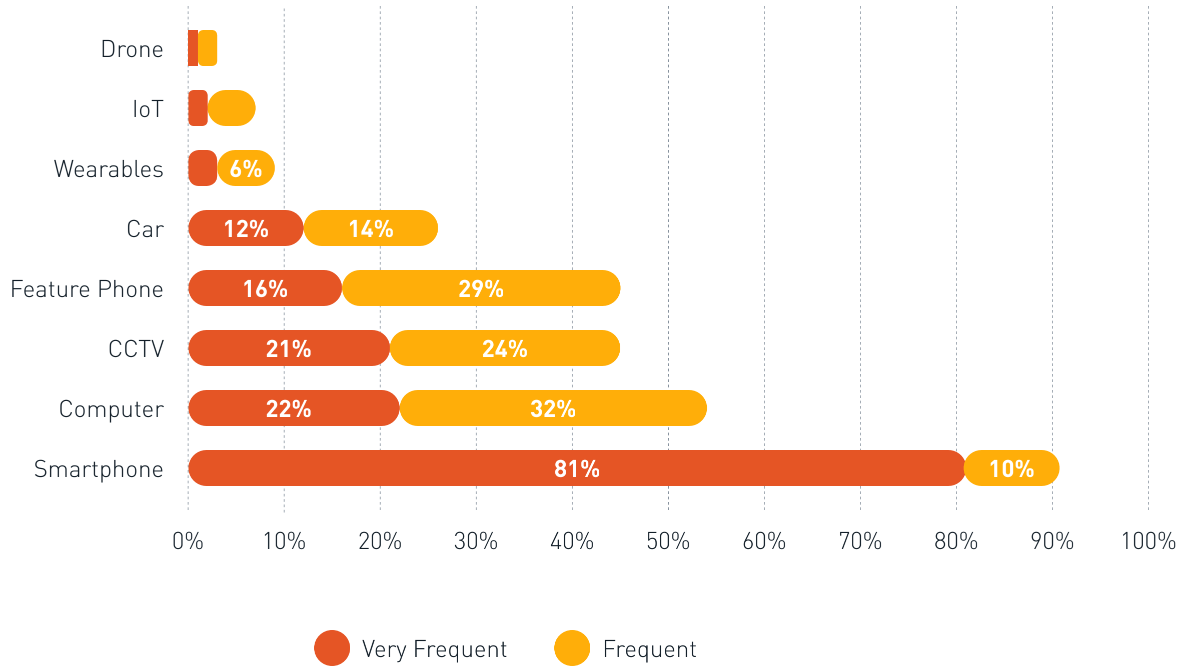
The questions in this section focused on which digital sources and types of digital data were most impactful to investigators and their cases. The data revealed that investigators worldwide face the same challenges when incorporating digital evidence into their investigations. Specifically, the amount of data typically involved and the growing number of digital sources that could be potentially used as sources of evidence were common challenges to investigators.

Wearables and IoT devices are seeing a significant increase as relevant data sources for evidence, during investigations, but other technology appeared with great frequency in the comments section. Gaming systems were the mostly commonly mentioned source with more than one respondent saying that these systems were being used to store child porn.

The majority of investigators are also using manual review methods for examining digital data, which is proving to be counterproductive to case closure and using digital evidence as a formative lead source.

DIGITAL DATA

In the past year, how frequent did the following evidence sources appear in your investigations?

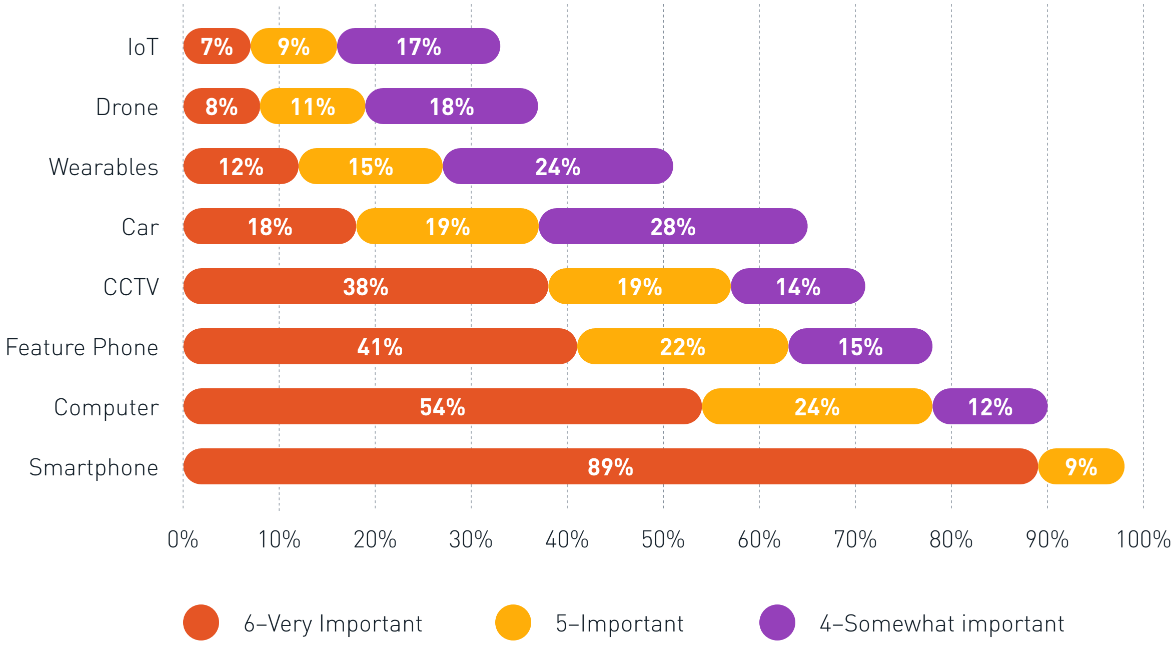


SUMMARY

Smartphones remain the primary source for digital evidence followed by computers and feature phones. (Feature phones are defined as "lacking the functionality of smart phones"). The findings validate previous suppositions that Law Enforcement is seeing a steady increase in the variety of digital sources with Cars, Wearables (Smartwatches, FitBit, etc.) and IoT devices becoming more prominent. CCTV is used more in EMEA than in other regions.

DIGITAL DATA

Please rate the importance of each to an investigation:

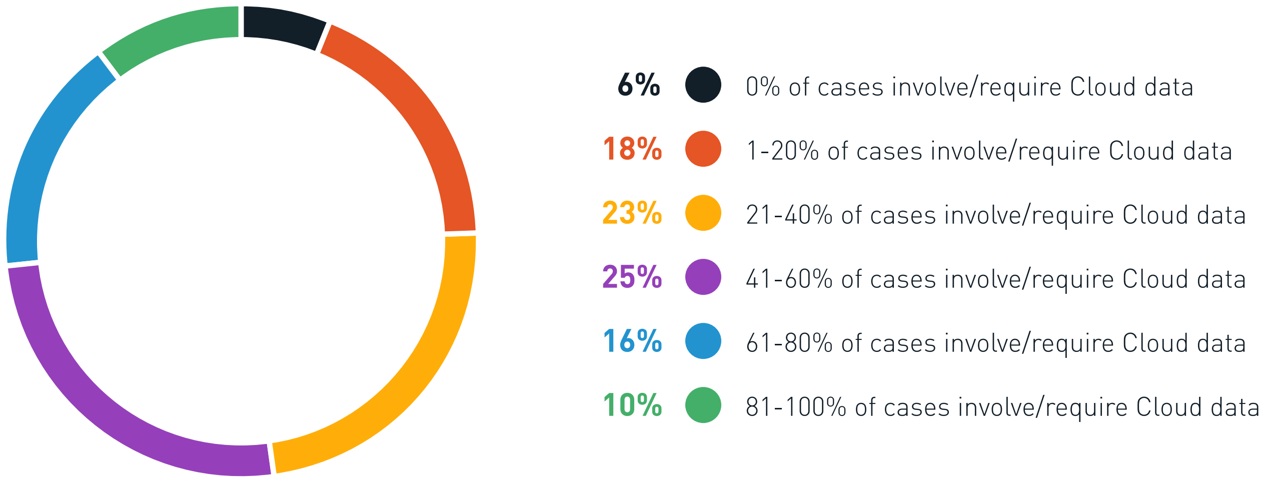


SUMMARY

In a follow-up to the previous question, the importance of each digital source matched their usage in investigations. Overall, the importance of digital sources to an investigation can be seen by the higher dominance of 6–Very Important and 5–Important Ratings on digital sources such as smartphones, computers and feature phones. CCTV did show a sharp increase in importance versus usage.

DIGITAL DATA

What percentage of your cases involve/require access to data stored on Cloud sources?

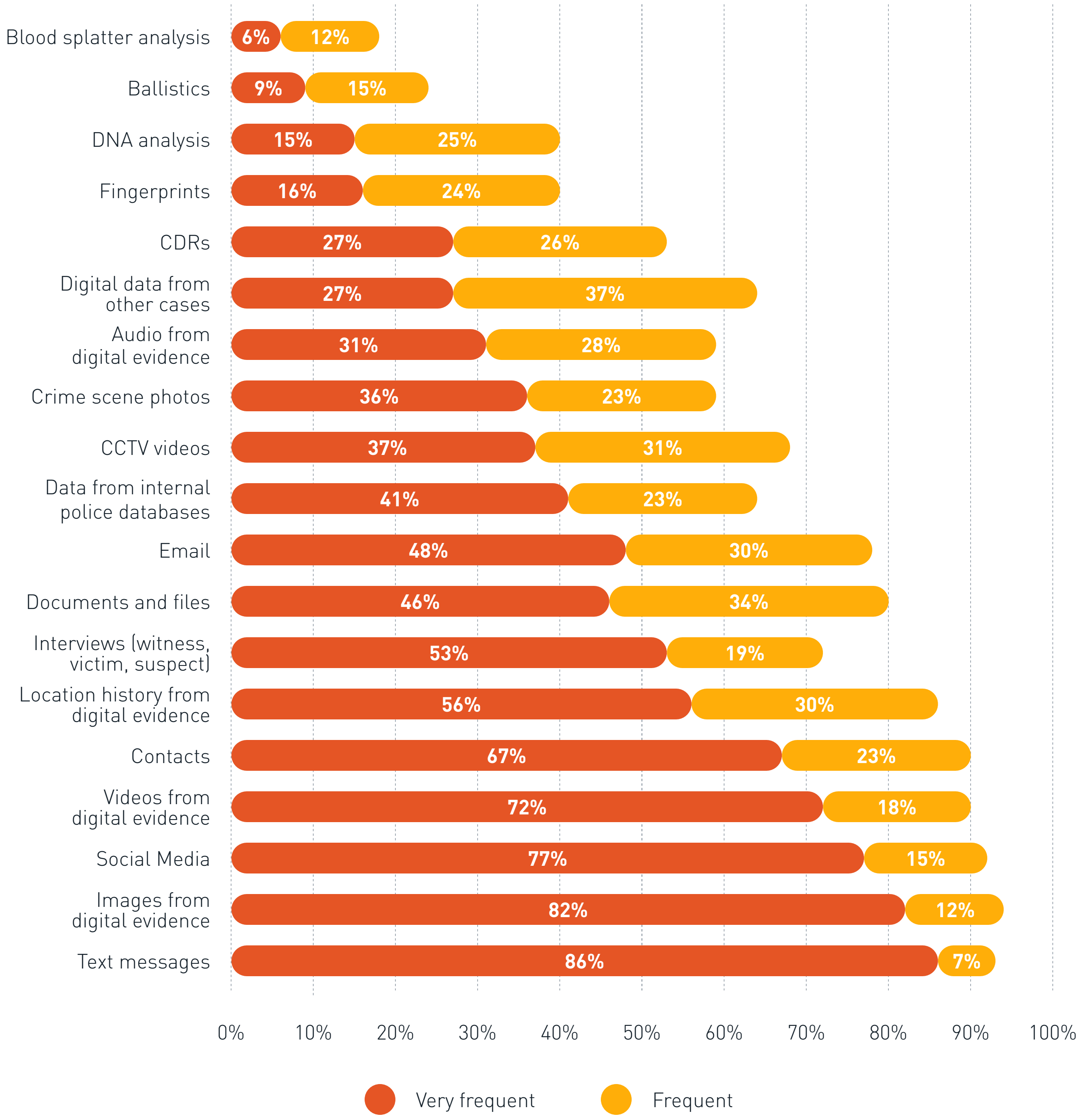


SUMMARY

There was a near equal distribution of Cloud Data used in investigations. The survey revealed a greater importance on physical devices than cloud data during the investigation process.

DIGITAL DATA

What data types do you most frequently review in a typical investigation?

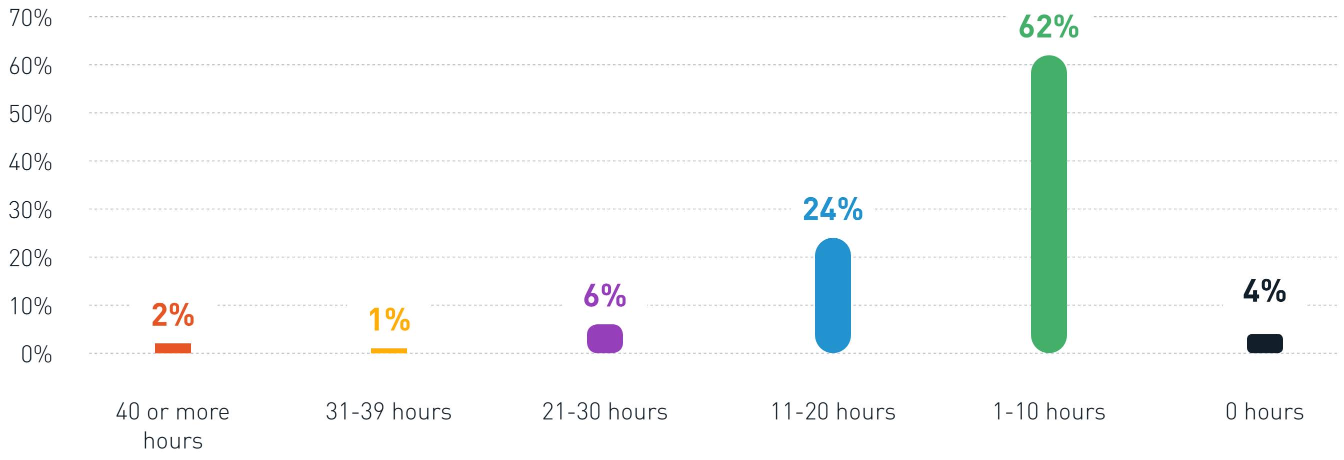


SUMMARY

The first question in this section compared digital sources used to gather potential evidence to physical sources. Communications, such as email, texts and social media, are importance sources of evidence, along with contacts and location history. Although digital evidence cannot take the place of physical evidence, the results show it is an equally important source of information in many investigations.

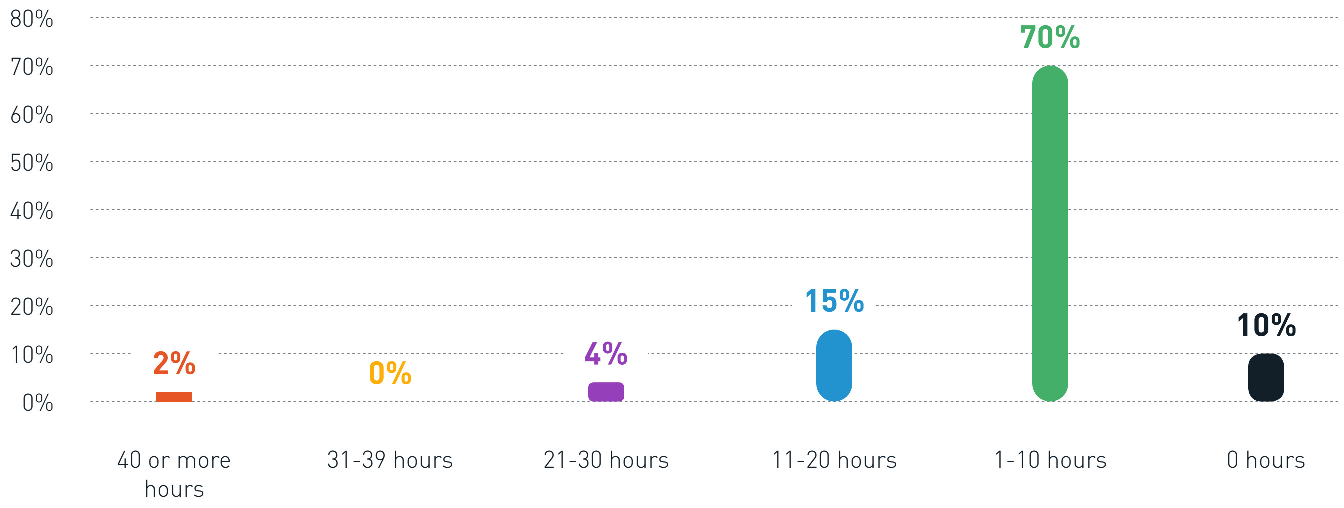
PRODUCTIVITY

In the past week, how much time did you spend reviewing digital photos?



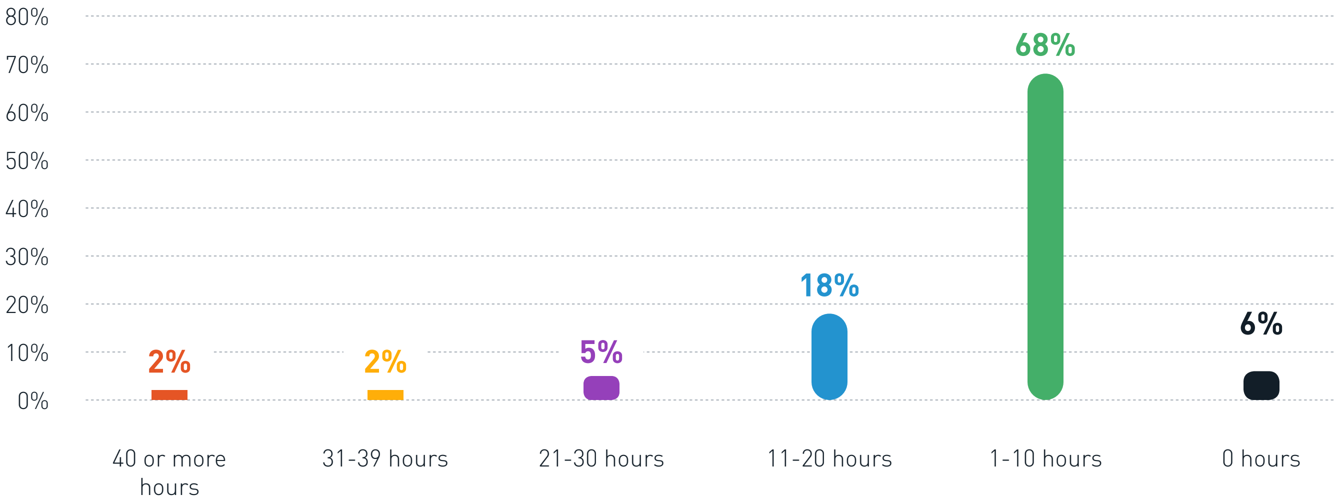
PRODUCTIVITY

In the past week, how much time did you spend reviewing recorded videos?



PRODUCTIVITY

In the past week, how much time did you spend reviewing text messages?

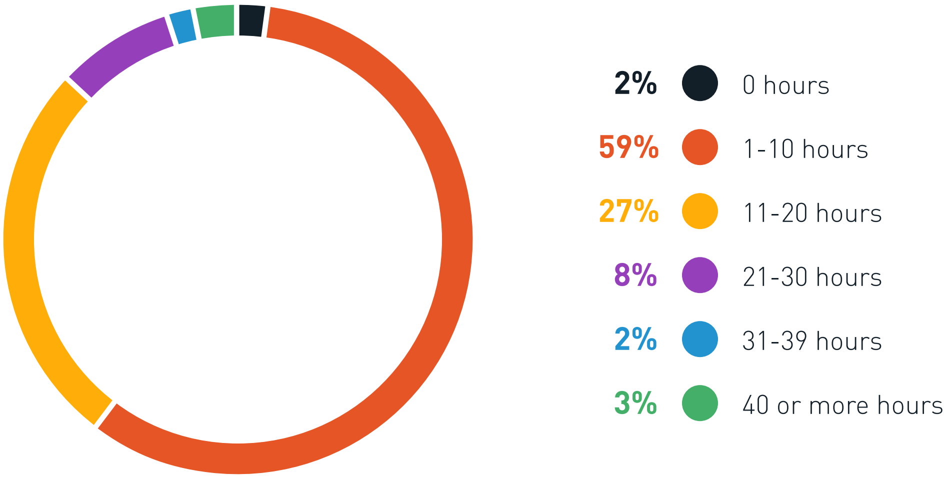


SUMMARY

As we looked at the most frequently used digital data sources, we also asked about the amount of time investigators spend reviewing these sources for potential digital evidence. The results showed that the review of just three data types could dominate the investigative process with the weighted average of 10, 7, and 9 hours respectively. The review of digital data in investigations is a time-consuming process that could easily delay the resolution of cases.

PRODUCTIVITY

In the past week, how much time did you spend on reporting?

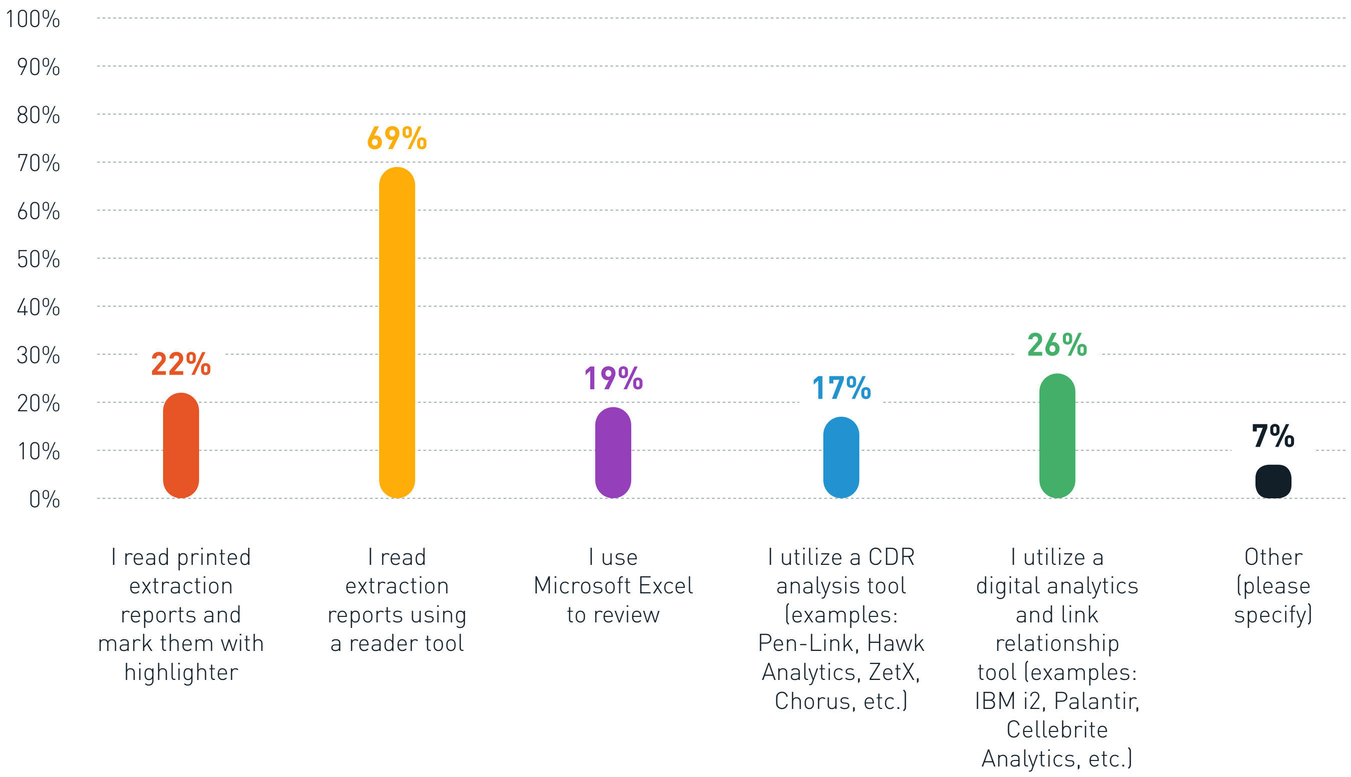


SUMMARY

Beyond the review of digital data is the reporting function that everyone in Law Enforcement must adhere to as part of the investigative process. Although the types of reports and reporting requirements may differ from region to region or even agency to agency, the majority of those surveyed spent a weighted average of 11 hours on reporting functions.

PRODUCTIVITY

How do you review the data from forensic extraction(s) for a case?

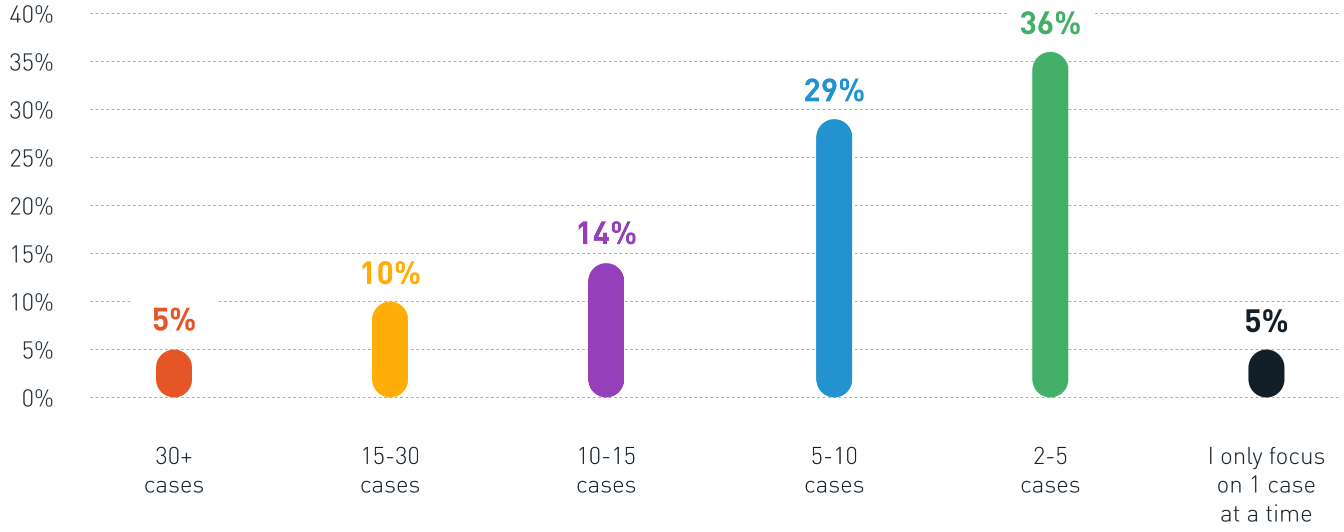


SUMMARY

Beyond extraction is the need to review large amounts of digital data that is typically related to an investigation. The vast majority of investigators employ a "Reader Tool" to review data extracted from digital devices and sources.

WORKLOAD

How many cases do you work on at any given time?

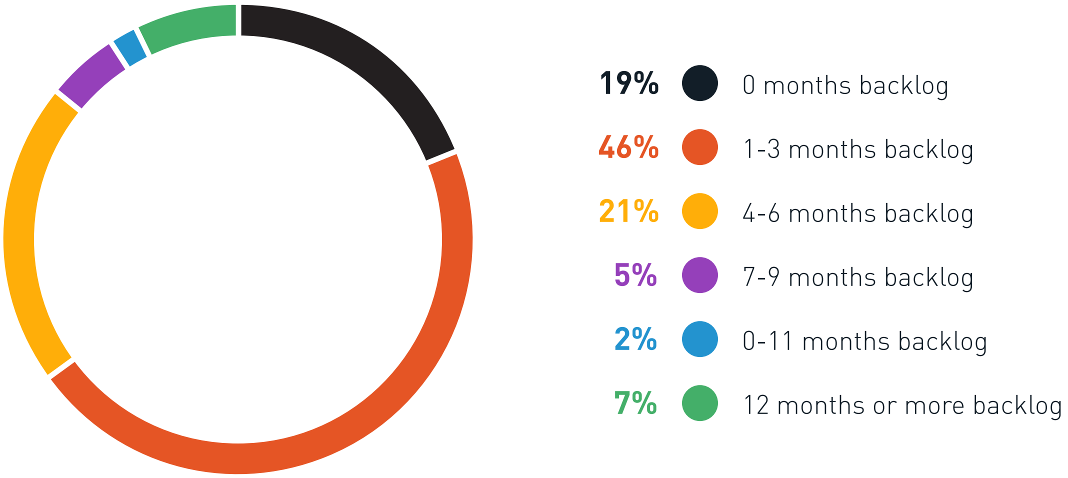


SUMMARY

Investigators typically work an average of 7-10 cases at any given time, with 33% managing anywhere from 5-15 cases at one time.

WORKLOAD

How backlogged are you in cases?

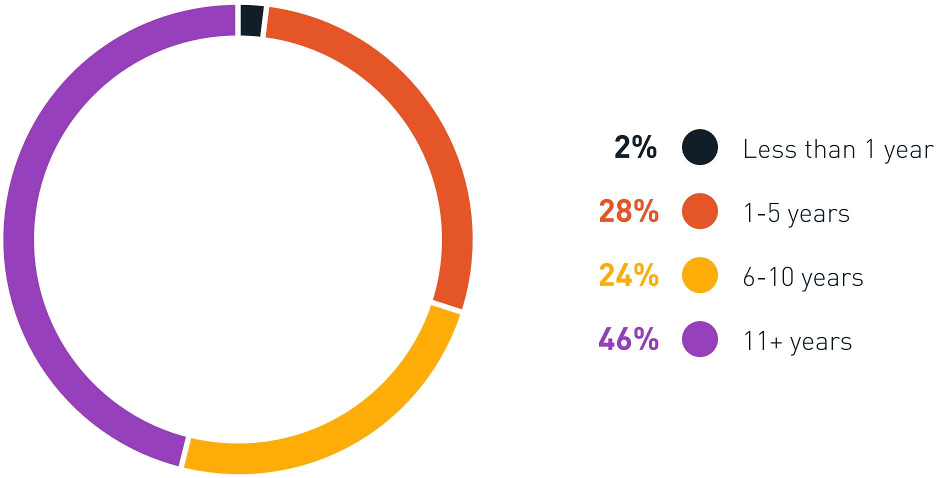


SUMMARY

The average backlog on cases is **3 months**.

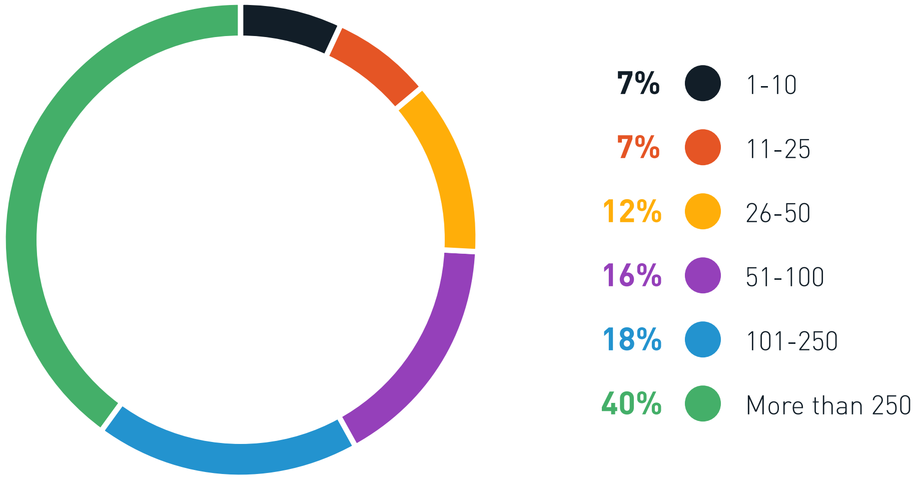
DEMOGRAPHICS

How long have you worked in this field?



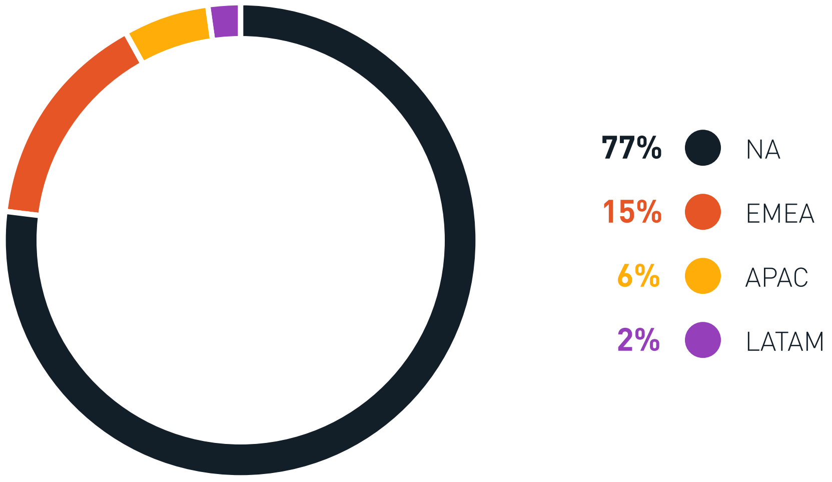
DEMOGRAPHICS

How many people are employed at your organization?



SURVEY SUMMARY

Regional Breakdown of Survey Results.



Examiner

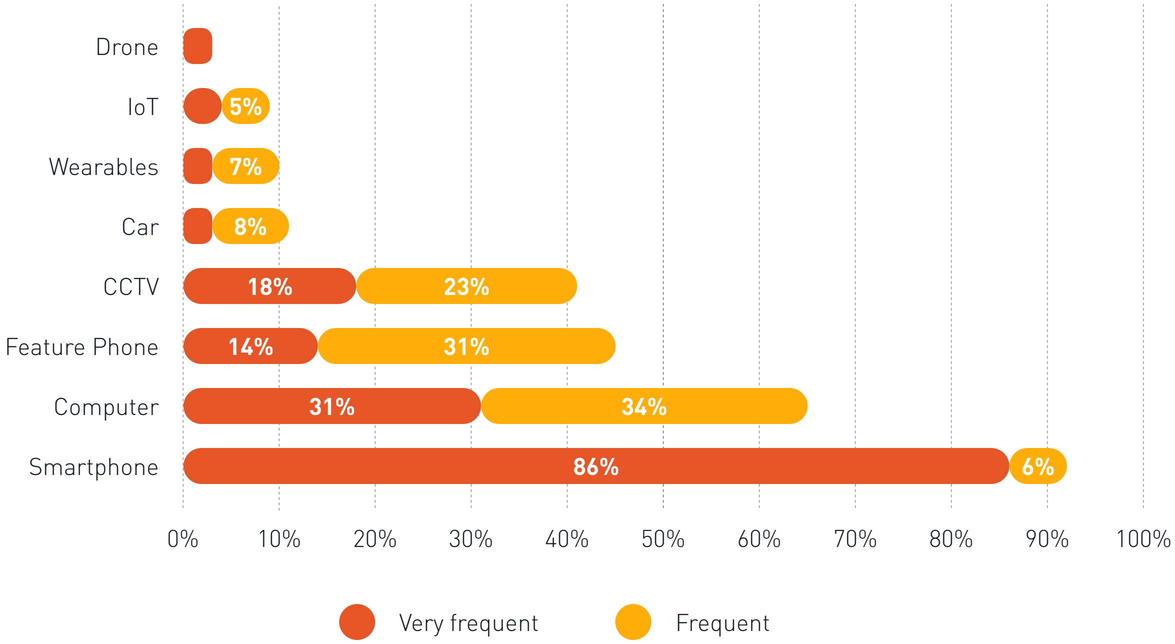
Overview

The questions in this section focused on the challenges most typically found when extracting data from digital sources. Mobile phones were the primary source for evidence. A key finding was that data from encrypted applications was the second most noted challenge behind locked phones. The data showed an exponential increase in the use of encrypted communication applications as well as some newer communication methods that have become preferred methods for the criminal element.

Productivity was the main challenge for examiners using advanced technology making it increasingly challenging to unlock and extract data from digital devices.

DIGITAL DATA

In the past year, how frequent did the following evidence sources appear in your investigations?

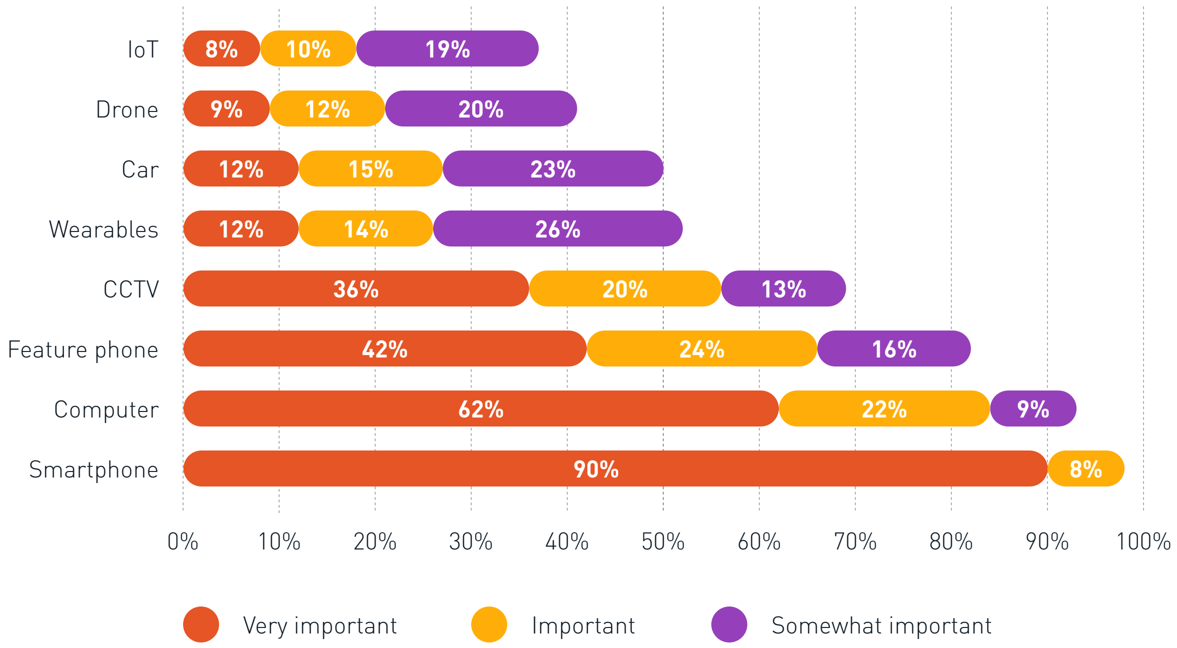


SUMMARY

Smartphones are the most frequently used data source for investigations, followed by computers and feature phones. CCTV was more frequently used in specific regions, such as EMEA, versus North America.

DIGITAL DATA

Please rate the importance of each to an investigation:

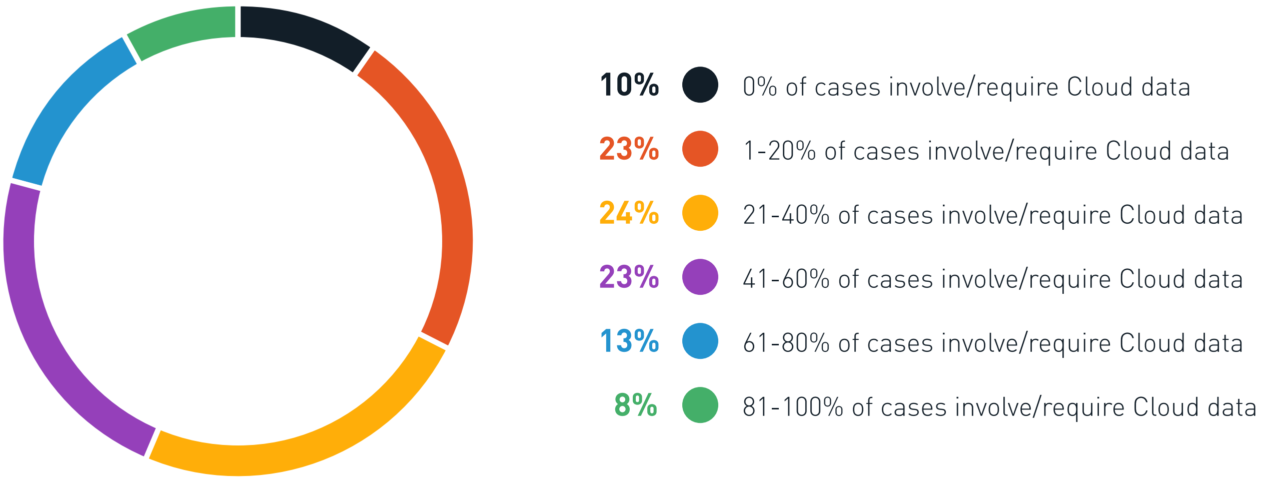


SUMMARY

This matches the frequency of sources in the previous question. One exception is that a higher value was placed on CCTV footage when available. Wearables were also valued highly especially when compared to their frequency of use.

DIGITAL DATA

What percentage of your cases involve/require access to data stored on Cloud sources?

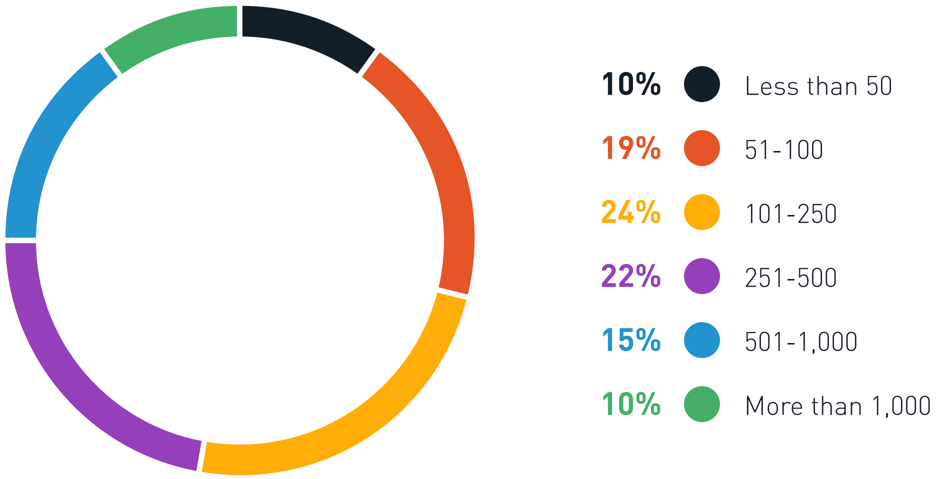


SUMMARY

Cloud data appears in approximately half of all investigations. Typically, this data involves social media or application data that does not reside on the physical device.

PRODUCTIVITY

How many mobile device examinations do you or your team conduct a year?

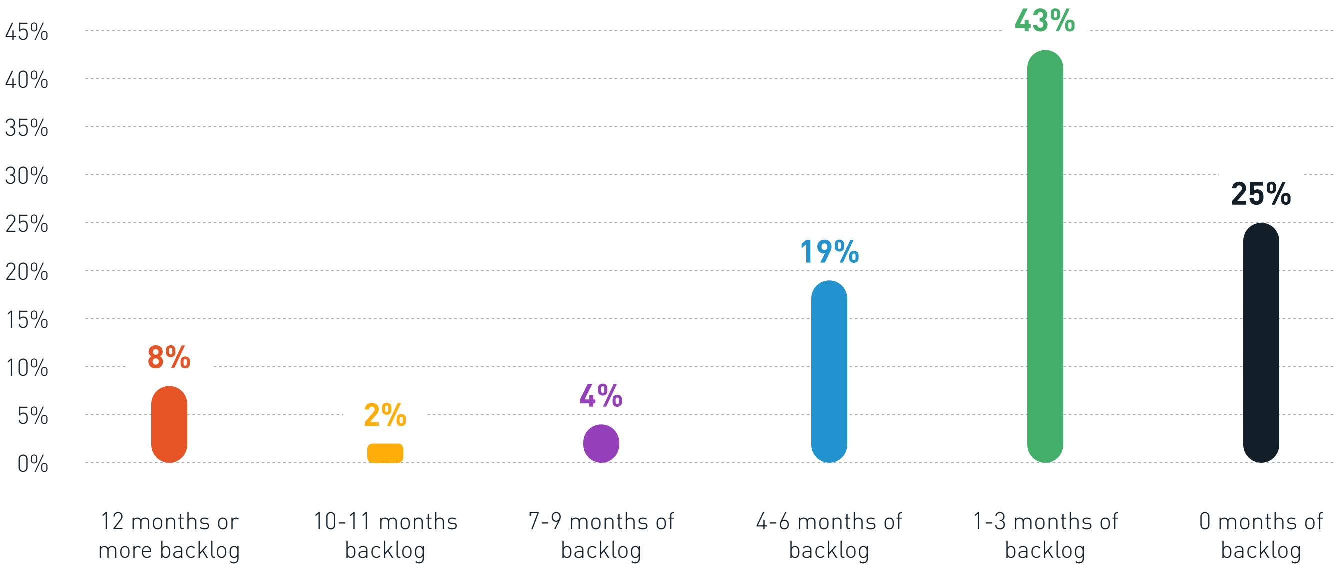


SUMMARY

With over 2/3 of the labs examining well over 100 mobile devices per year, it is evident they play an integral part in investigations.

PRODUCTIVITY

How backlogged are digital forensic examinations in your lab?

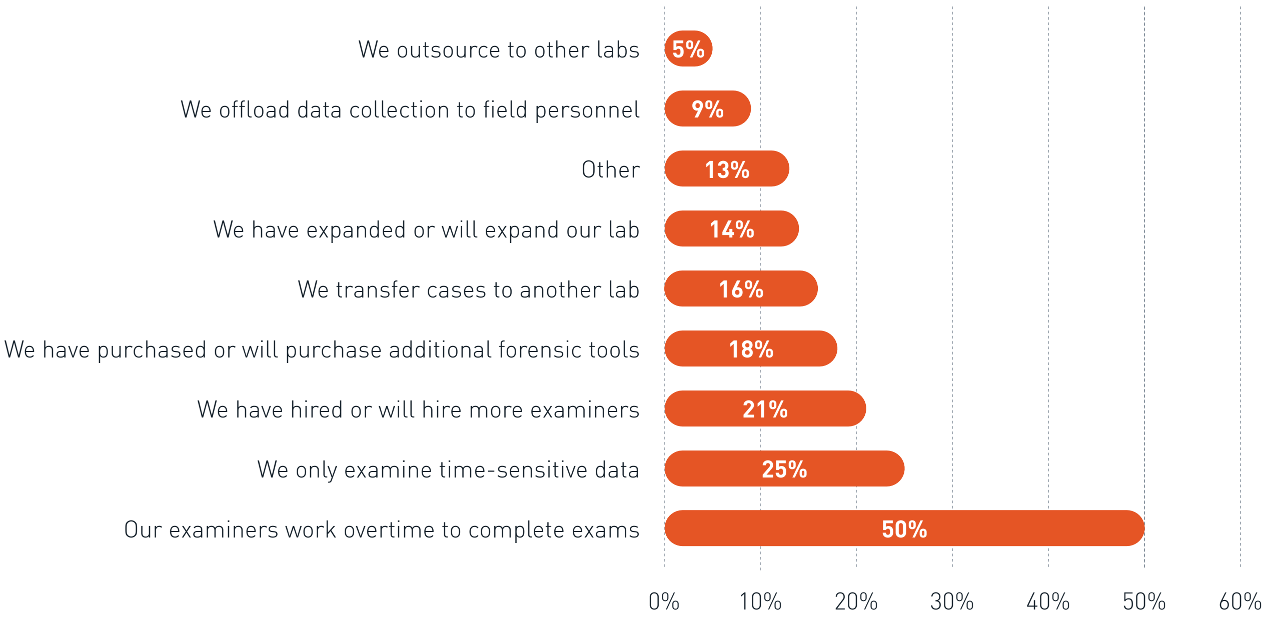


SUMMARY

The majority of examiners reported a backlog in extracting of data from mobile phones. The weighted average was a **backlog of 3 months**.

PRODUCTIVITY

How do you handle backlogs? (Please select any and all that apply)

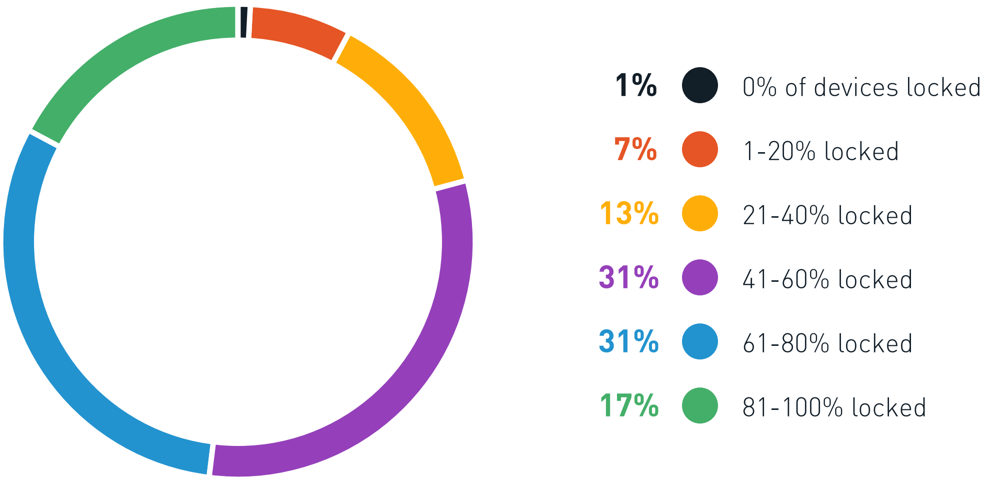


SUMMARY

Half of all labs require overtime to handle the backlog. The second option to use selective extraction of data could mean that valuable data is being “left behind” and is not available for review.

PRODUCTIVITY

What percentage of devices that reach your lab are locked?

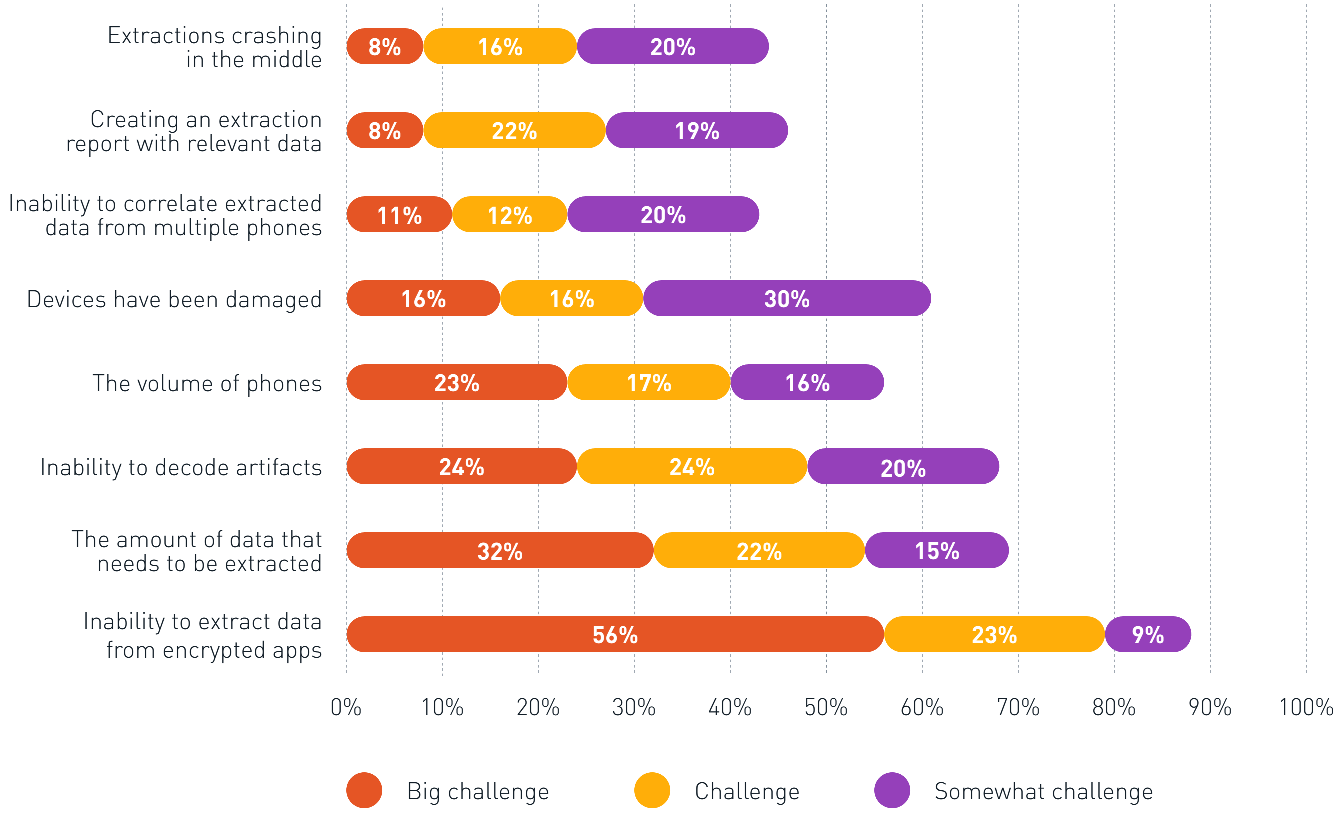


SUMMARY

The weighted average of all devices being locked is 59%. This could be one of the primary factors causing the average backlog of 3 months found in labs throughout the world.

PRODUCTIVITY

Aside from the mobile device being locked, what are the biggest challenges you face when performing digital extractions?

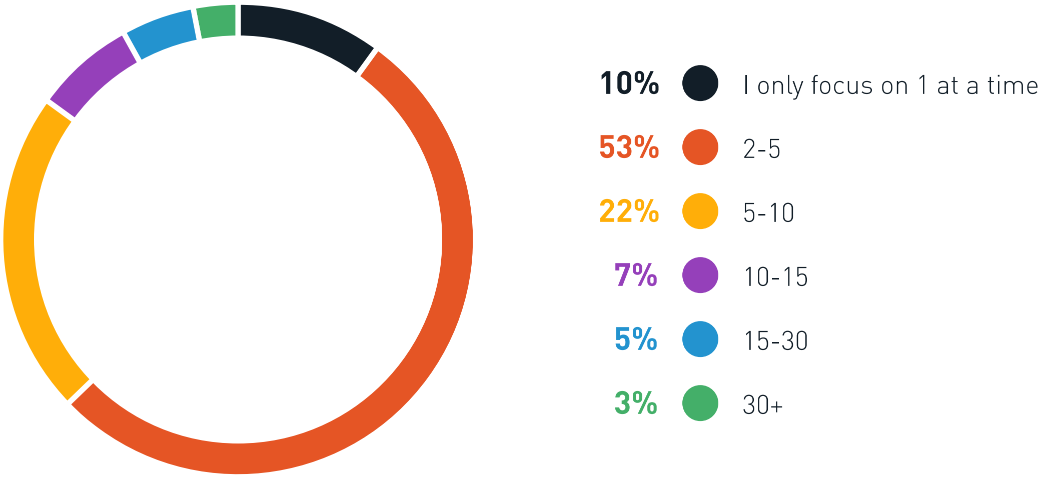


SUMMARY

Once mobile phones are successfully unlocked there are still other challenges that need to be resolved to successfully extract data. Encrypted applications, followed by the amount of data needing to be extracted, were the two most significant challenges examiners face after locked phones.

WORKLOAD

How many cases do you work on at any given time?

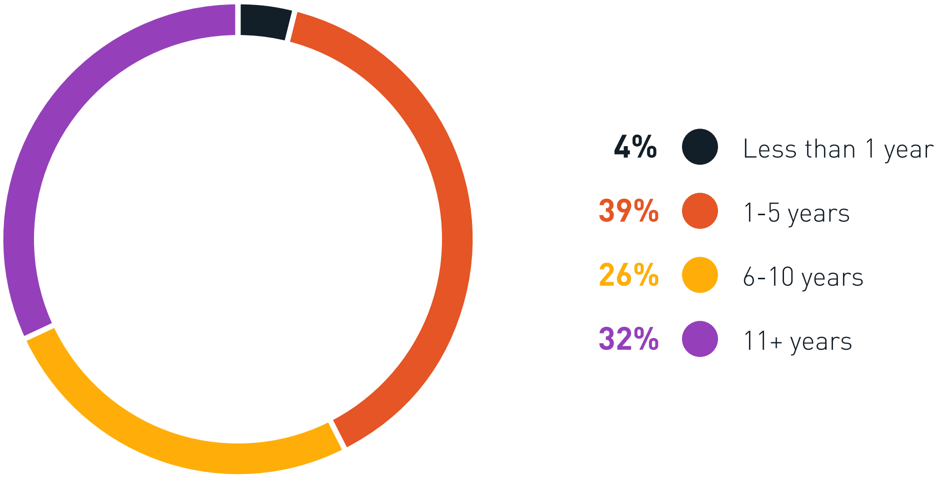


SUMMARY

The weighted average for the number of cases worked on simultaneously by examiners is **5-8**. A typical case could have multiple devices that require data extraction.

DEMOGRAPHICS

How long have you worked in this field?

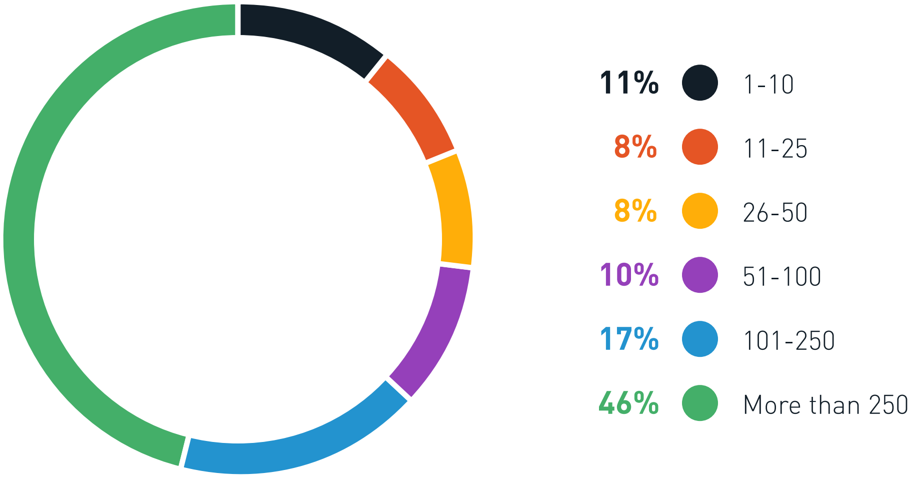


SUMMARY

The findings show that examiners have worked fewer years in their field, when compared to investigators.

DEMOGRAPHICS

How many people are employed at your organization?

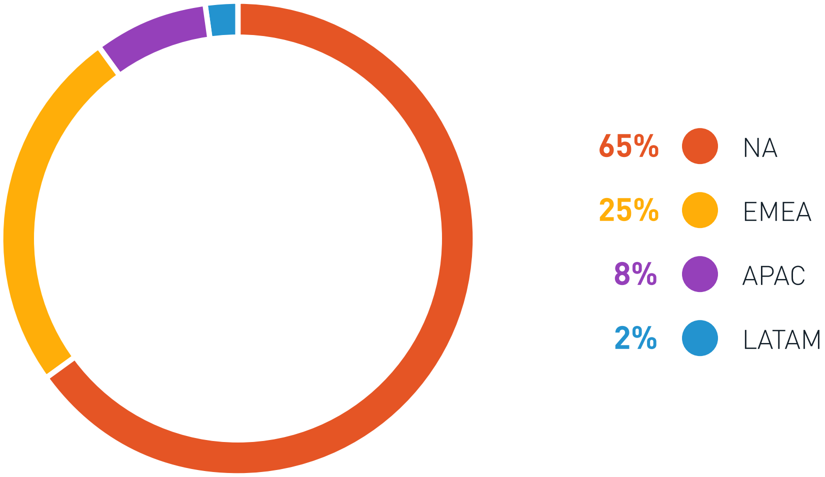


SUMMARY

Many of our respondents from larger organizations since few stand-alone agencies can afford the cost of maintaining their own lab. Many agencies outsource their data extraction needs or use regional labs.

SURVEY SUMMARY

Regional breakdown of survey results



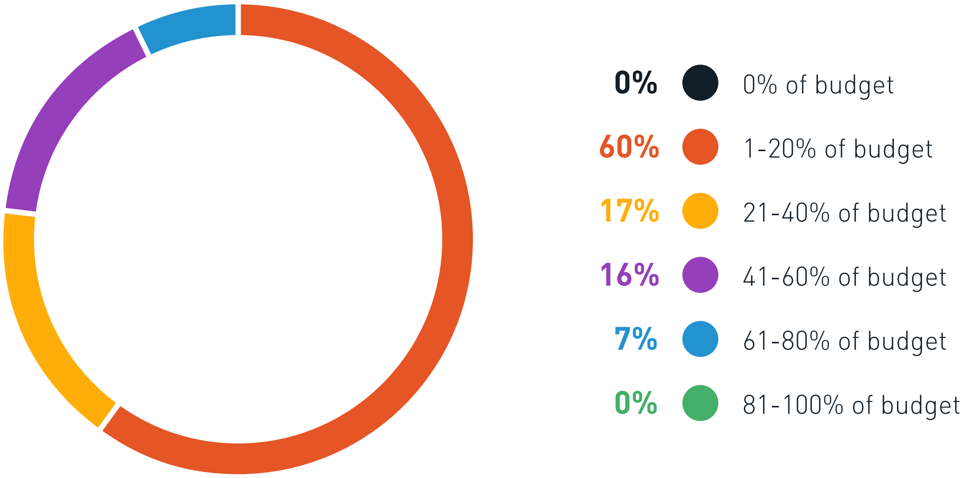
Agency Management

Overview

The questions in this section focused on the decisions that agency managers must make involving budget, personnel and priorities. The survey revealed that agency management will once again invest a significant portion of their budget in digital forensics technology and training. The survey results also showed that the evolution in investigations continues with an increased focus on technology and digital data.

BUDGET

What percent of your total budget do you allocate toward software for improving investigations?

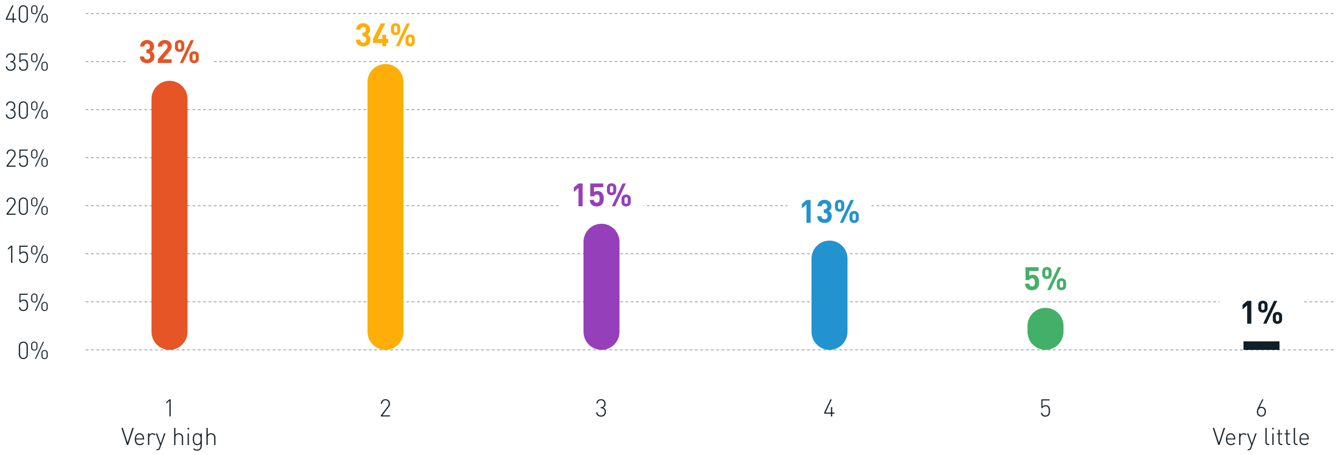


SUMMARY

The global weighted average of budgets being allocated to software and technology upgrades was 26%.

BUDGET

How much of a role does price play in your decision making?

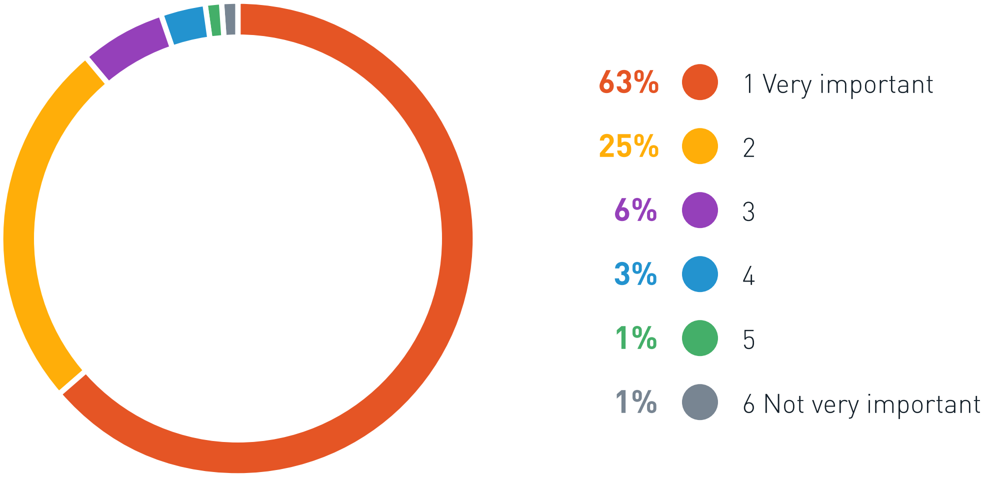


SUMMARY

Price continues to play an important role in decision making as budgets and spending are scrutinized carefully.

DIGITAL DATA

How important to you is governance and management of data?

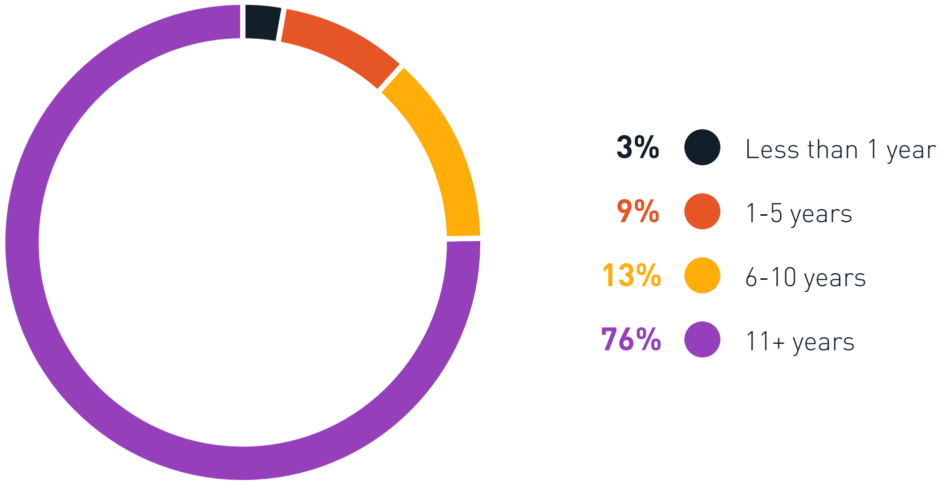


SUMMARY

For agency management, secure collaboration is an important part of their data management.

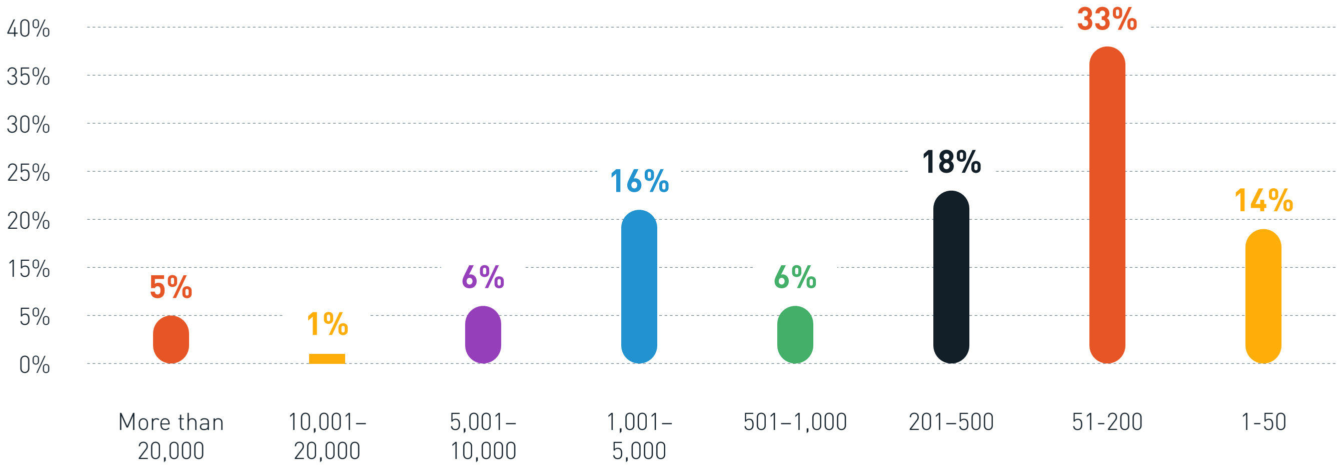
DEMOGRAPHICS

How long have you worked in this field?



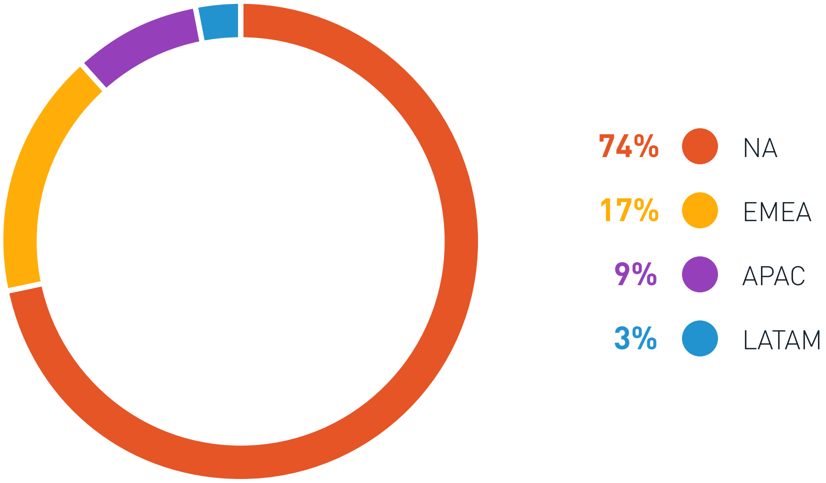
DEMOGRAPHICS

How many people are employed at your organization?



SURVEY SUMMARY

Regional breakdown of survey results


74% ● NA
17% ● EMEA
9% ● APAC
3% ● LATAM