Cellebrite Digital intelligence for a safer world

CASE STUDY

Digital Evidence Confirms Players in Major Bitcoin Heist — and Leads to Their Convictions

Traditional policework helped track down the thieves targeting cryptocurrency data centers in Iceland, but digital intelligence from one suspect's mobile devices provided the proof of their involvement.

The Case

Iceland, with its low crime rate, cheap warehouse space, polar climate, and abundance of inexpensive geothermal energy, has become the world's leader in digital currency mining over the past several years. Sindri Thor Stefansson, an Icelandic man with a history of criminal activity and prison time, saw an opportunity to start his own Bitcoin mining operation — by stealing computers from cryptocurrency data centers located in the southwest region of Iceland.

Stefansson enlisted help from four other associates to execute his plan. Over a two-month period in 2018, the team broke into several cryptocurrency data centers, stealing more than $2 million worth of technology equipment — from motherboards to power accessories. For their very last hit, the thieves were even helped by a security guard. This brief but highly productive crime wave was reported to be the biggest burglary in the history of Iceland.

The Challenges

The owners of the cryptocurrency data centers weren't keen to advertise the break-ins, as they didn't want to upset their foreign investors. But one owner, whose data center in the town of Borgarnes was cleaned out by the thieves, did report the crime to the Icelandic Police — the Lögreglan. That decision set in motion an investigation that would eventually lead to the prosecution of Stefansson and his cohorts.

Date

2018

Challenge

To connect six suspects to the theft of more than $2M in tech equipment for mining Bitcoins from several cryptocurrency data centers in Iceland

Tools

- UFED Touch2
- Cellebrite Physical Analyzer
- Cellebrite Advanced Services

Result

Data from the main suspect's mobile devices, extracted and analyzed using Cellebrite's digital intelligence tools and services, proved the involvement of six suspects in the Bitcoin heist — and led to their convictions.

Traditional investigation tactics by the Lögreglan were highly effective in tracking down the suspects. Investigators reviewed footage from surveillance cameras and identified rental cars used in the crimes. They then identified the individuals who rented the cars, and started their surveillance of those individuals, using trackers, wiretaps, and other tools. Within about a week of setting up surveillance, they had rounded up several suspects, including Stefansson. But then, the investigators hit a wall.

Their key challenges were:

- Lack of cooperation by all the suspects, who would not admit to the crimes.
- The inability to gather digital evidence because the suspects would not grant investigators access to their mobile devices or provide them with their PINs.
- The sheer complexity of the investigation: The suspects had used many phones and phone numbers throughout their operation. Also, they had relied on online messaging apps like Telegram to create almost secure lines of communication.

The Solution

The investigators were eager to gather any digital intelligence from the suspects' devices that would clearly connect the thieves to the crimes and help lead to their convictions. After obtaining a court order to examine the devices, the investigators used Cellebrite's UFED Touch2 to access data from the phones of Stefansson's associates. They then applied the Cellebrite Physical Analyzer to examine the digital evidence. However, because the thieves had gone to such lengths to conceal their digital activity, the examination did not yield enough evidence to guarantee a conviction.

Sindri and two of his friends posted on social media after they met in Amsterdam after he escaped (all got sentences in the case).

"Cellebrite's Advanced Services team was able to extract every type of digital evidence imaginable from the suspect's iPhones — locations, images, Telegram messages — basically, everything we needed to prove the case and secure the convictions."

Detective Inspector Eiríkur Guðni Ásgeirsson, Serious Crimes Unit, Suðurnes Police.

"Without the evidence from those devices, I'm not sure we would've gotten the convictions. And I know we only managed to get a conviction of the suspect we located in Spain because of the Telegram messages on Stefansson's phones."

Detective Inspector Eiríkur Guðni Ásgeirsson, Serious Crimes Unit, Suðurnes Police.

The investigators remained hopeful that the data on Stefansson's two Apple iPhones would not only prove that he was the one who had planned the operation, but also provide evidence of the other suspects' involvement in helping him to steal equipment from the data centers. So, as a next step, the investigators sent Stefansson's phones to Cellebrite's Advanced Services team in Munich, Germany, for advanced device unlocking and data extraction.

How Digital Intelligence Helped Crack the Case

- The CAS team uncovered a trove of data from Stefansson's iPhones that was relevant to the Bitcoin heist — everything from geolocation information to images to Telegram messages.
- The Telegram messages that Stefansson had saved on his mobile devices helped lead investigators to another suspect in Spain.
- The digital intelligence that the CAS team helped to uncover from Stefansson's iPhones was exactly what investigators needed to prove their case and secure the thieves' convictions.

Sindri Þór Stefánsson is seen here in the middle of the picture on his way to Reykjavík District Court.

The Results

- Stefansson was sentenced to 4.5 years in prison for his role in the Bitcoin heist.
- Five other individuals were prosecuted, including the data center security guard. They received sentences ranging from six months to 4.5 years.
- Investigators in Iceland express confidence that they would not have been able to secure these convictions without the digital evidence that the CAS team extracted from Stefansson's iPhones.

"Every case has some type of digital evidence, and the sooner we get our hands on that evidence, the better. Only a few years ago, no one thought about using mobile phones or data from phone companies when working on a case. Today, it's standard procedure."

Detective Inspector Eiríkur Guðni Ásgeirsson, Serious Crimes Unit, Suðurnes Police.

To learn more about Cellebrite visit: Cellebrite.com

Sources

"The Big Bitcoin Heist," by Mark Seal, Vanity Fair, December 2019: https://www.vanityfair.com/news/2019/11/the-big-bitcoin-heist

About Cellebrite

For more than 20 years, Cellebrite has been the global leader and premiere provider of integrated digital intelligence solutions to law enforcement, military, government, and private enterprises worldwide. We help resolve investigations faster by addressing the growing challenges of an expanding digital world.

Developed in close partnership with our customers, our integrated suite of digital intelligence software, solutions, and training include: access to all devices, digital platforms and applications when and where teams need it; management and control of all relevant data in a secure and collaborative system; and powerful leverage to quickly reveal critical insights.

Our solutions seamlessly integrate with existing infrastructures that allow organizations to make command decisions more efficiently to better protect their communities.

- Learn more about Cellebrite Digital Intelligence Solutions at: www.cellebrite.com
- Contact Cellebrite globally at: www.cellebrite.com/contact

Cellebrite