**Funnelweb Bureau of Investigation**

Department of Justice

*Criminal Justice Special Cybersecurity Division*

THE ICARUS CASE - The Investigation of Freiss Dembele

**Case File ID**: FWEB-2024-004  
**Classification**: Official - Sensitive  
**Date**: October 2, 2024  
**Author**: Sergeant M. Blackwidow  
**Status**: Open

**Debrief**

|  |  |  |
| --- | --- | --- |
| **Name** | **Age/Gender** | **URL to append** |
| Freiss Dembele | 20F | /nomad.html |

Following the death of Narlin Tanaka, our investigators realised his secret account was following an account, which has now been identified to be the private account of another person of interest, Freiss Dembele, who was murdered around the time Narlin was. Our latest leads suggest that Freiss may have been targeted due to her tendency to log her ‘solo dates’ publicly, revealing a **lot** of information about her location.

While investigating Freiss’ activity, we've uncovered a pattern in her posts that might reveal how his personal information became vulnerable. Some handy GeoOSINT skills and social engineering could have allowed the attacker to piece together crucial data leading up to the attack.

Our forensic analysts have been focusing on a specific Instagram account linked to Freiss **@fr3iss** — her friends claimed they believe this account belonged to Freiss.

**Task**

From our intelligence, we know that the profile contains a crucial clue—her one and only story highlight. It looks like she logged her day out, but she also shared a script which may prove very valuable in leading us back to the killer.

Analysts believe that by decrypting the suspicious code, you may be able to produce a hash key.

Our detectives have tipped that the following resource might help:

* [Finding locations/landmarks from photos: a comprehensive tutorial in GeoOSINT](https://www.youtube.com/watch?v=ctJk3LhtHxc)

**Conclusion**

This case demonstrates the dangers of sharing real-time location data and coded information online without secure privacy settings. Investigators suspect that the attacker used this public information and the coded messages to track Freiss’s whereabouts before the attack.

**GOOD LUCK.**