**Funnelweb Bureau of Investigation**

Department of Justice

*Criminal Justice Special Cybersecurity Division*

THE ICARUS CASE - Formal Introduction

**Case File ID**: FWEB-2024-002  
**Classification**: Official - Sensitive  
**Date**: October 2, 2024  
**Author**: Sergeant M. Blackwidow  
**Status**: Open

**Introduction**

Congratulations. If you are reading this, you have been selected for the Icarus case.

On behalf of the Funnelweb County and the Department of Justice, we thank you for joining us in taking on this case. This case has plagued the division for several months, and so we have transferred this to our new *special* division, who will be led by [REDACTED]. If you are reading this document, you have been selected for this division as the cream of the crop in the cybersecurity division, and we entrust the results of this case with you. For further information on this, please email [REDACTED].

With the formalities out of the way, let me disclose the details of this case. We had been alerted earlier this year about the murders of 3 young adults, whose bodies were identified as listed below:

| **Name** | **Age/Gender** |
| --- | --- |
| Narlin Tanaka | 19M |
| Freiss Dembele | 20F |
| Molly Bastoni | 19F |

The families were informed as soon as they were identified, and understandably they are insistent on bringing the killer to justice. However, up until now, we’ve only run into dead ends. Thus, I urge you to progress through these cases and compile as much information as possible.

**Task**

Up until now, you have been trained in basic OSINT techniques, which is useful for identifying people in generic situations, finding data and information that is completely public and accessible to everyone. We are **certain** that your OSINT techniques will prove useful for these cases, however, you will be required to hone your skills even more. From here on out, you will be in unchartered territory recovering fragments of a URL that will point you straight to the evil lair of the killer; we are aware that the URL is formatted as such:

**p1nnoch1o-{secret hash}.onrender.com**

Fragments of this hash can be recovered from the endpoints of each of the cases you investigate above, and trust me;

You’ll know them when you see them.