

# CIH OSINT 26.03.2022 - Writeup

Hello ! Ceci est la solution du challenge proposé durant la conférence.

Évidemment, **contient du spoil**.

## Liste des informations

On recense les informations qu'on a dans l'énoncé :

- La photo a été prise hier.
- L'avion qu'on recherche est celui qui a décollé juste avant l'avion Eurowings

De plus, sur la photo, on a :

- Deux immatriculations d'avion, **OE-LBC** et **D-ABGJ**, avec leurs compagnies, respectivement Austrian et Eurowings
- Trois hôtels en arrière plan : Ibis, Novotel, et Hilton.

## Exploitation

On va commencer à rechercher l'historique du vol Eurowings sur FlightRadar24.

Sur la journée du 25, l'avion a effectué les trajets suivants :

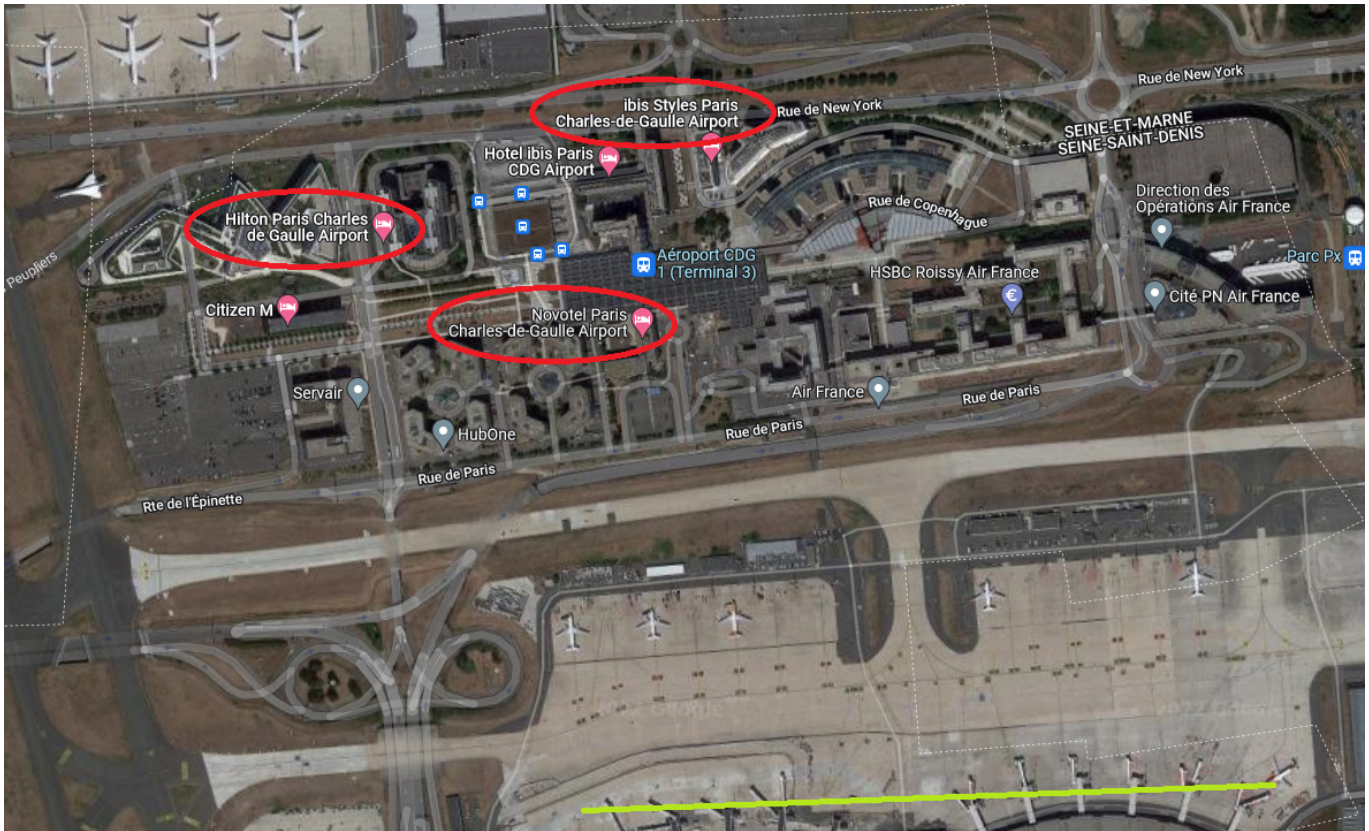
25 Mar 2022	Paris (CDG)	Hamburg (HAM)	EW7407	1:16	19:50	20:09	21:25	Landed 21:25	 KML	 CSV	 Play
25 Mar 2022	Hamburg (HAM)	Paris (CDG)	EW7406	1:12	17:30	17:41	19:10	Landed 18:53	 KML	 CSV	 Play
25 Mar 2022	Palma de Mallorca (PMI)	Hamburg (HAM)	EW7581	2:23	13:45	14:03	16:40	Landed 16:26	 KML	 CSV	 Play
25 Mar 2022	Hamburg (HAM)	Palma de Mallorca (PMI)	EW7580	2:22	10:20	10:39	13:00	Landed 13:01	 KML	 CSV	 Play
25 Mar 2022	Cologne (CGN)	Hamburg (HAM)	EW7039	0:47	08:40	08:43	09:45	Landed 09:30	 KML	 CSV	 Play
25 Mar 2022	Hamburg (HAM)	Cologne (CGN)	EW7038	0:42	07:00	07:06	08:05	Landed 07:49	 KML	 CSV	 Play

Croisons cela avec les trajets du Austrian :

25 Mar 2022	Paris (CDG)	Vienna (VIE)	OS418	1:33	20:10	20:35	22:05	Landed 22:08	<a href="#">KML</a>	<a href="#">CSV</a>	<a href="#">Play</a>
25 Mar 2022	Vienna (VIE)	Paris (CDG)	OS417	1:35	17:20	17:39	19:25	Landed 19:14	<a href="#">KML</a>	<a href="#">CSV</a>	<a href="#">Play</a>
25 Mar 2022	Oslo (OSL)	Vienna (VIE)	OS336	1:54	13:40	13:54	16:00	Landed 15:48	<a href="#">KML</a>	<a href="#">CSV</a>	<a href="#">Play</a>
25 Mar 2022	Vienna (VIE)	Oslo (OSL)	OS335	2:03	10:20	10:27	12:40	Landed 12:30	<a href="#">KML</a>	<a href="#">CSV</a>	<a href="#">Play</a>
25 Mar 2022	Vienna (VIE)	Oslo (OSL)	OS335	—	10:17	—	—	Unknown	<a href="#">KML</a>	<a href="#">CSV</a>	<a href="#">Play</a>
25 Mar 2022	Athens (ATH)	Vienna (VIE)	OS804	1:57	06:00	06:13	07:15	Landed 07:09	<a href="#">KML</a>	<a href="#">CSV</a>	<a href="#">Play</a>

On voit que les deux étaient à Paris (CDG) à la même heure le 25.

En vérifiant, il y a en effet les bons hôtels proche de l'aéroport :



La photo a donc été prise depuis un emplacement situé sur la ligne verte.

Le vol qui nous intéresse est donc celui qui a décollé de Paris (CDG) juste avant l'Eurowings, prévu à 19h50 le 25/03.

En cherchant l'historique des décollages de CDG, on trouve ceci :

19:45	OU978	Dzaoudzi (DZA)	Air Austral	788	Canceled
19:50	AF1246	Warsaw (WAW)	Air France	A320 (F-GKXZ)	Departed 20:04
19:50	EW7407	Hamburg (HAM)	Eurowings	A319 (D-ABGJ)	Departed 20:09
19:55	LH2235	Munich (MUC)	Air Dolomiti	E195 (I-ADJX)	Departed 20:19
20:00	BJ543	Monastir (MIR)	Nouvelair	A320 (TS-IND)	Departed 20:55
20:00	FX9147	Memphis (MEM)	FedEx	B77L (N883FD)	Departed 20:14
20:05	5F902	Chisinau (KIV)	Fly One	320	Canceled
20:10	LX645	Zurich (ZRH)	Swiss	BCS3 (HB-JCC)	Departed 20:50
20:10	OS418	Vienna (VIE)	Austrian Airlines	A321 (OE-LBC)	Departed 20:35
20:20	AF1630	Milan (MXP)	Air France	E190 (F-HBLP)	Departed 20:39
20:25	AF1246	Paris (CDG)	Air France	E190	Departed 19:50

On voit que l'identifiant de l'avion (F-GKXZ) colle plutôt bien avec ce que l'on voit sur la photo.

Pour finir, on va donc chercher l'heure d'arrivée du vol F-GKXZ :

25 Mar 2022	Paris (CDG)	Warsaw (WAW)	AF1246	1:56	19:50	20:04	22:10	Landed 22:00
-------------	-------------	--------------	--------	------	-------	-------	-------	--------------

Notre **criminel** a donc pris le vol AF1246, immatriculé F-GKXZ, à destination de Warsaw, qui est arrivé à 22:00.