# REPORT
# OSINT Email Enumeration & Validation

*v1.0.1*

Author:

**Eldon Gabriel**

March 31, 2025

# Table of Contents

**Disclaimer:** This report documents the authors' personal work in completing laboratory exercises. This reflects the authors' independent understanding and application of publicly available tools and techniques. No MCSI proprietary instructional videos, lab guides, or specific content from the original exercise were posted, shared, or distributed, ensuring full compliance with academic and professional policies.

## Revision History

| Version | Date | Author | Description of Changes |
|---|---|---|---|
| 1.0.0 | 10/17/2025 | Eldon G. | Initial draft. |
| 1.0.0 | 03/31/2026 | Eldon G. | Updated formatting & added figures 1-3 screenshots |

# 1.0 Email Reconnaissance and Validation

## 1.1 Project Description

An **Open-Source Intelligence (OSINT**) exercise was performed to find and check potential email addresses linked to a target domain and person using public data sources.

## 1.2 Scope

The work focused on:

1. Locating email addresses within publicly accessible **PDF files** using targeted search queries.
2. Generate educated email guesses based on the identified **naming conventions**.
3. Testing mailbox validity using online email **verification tools**.

## 1.3 Tools and Environment

- **Kali Linux** virtual machine, running within a **Virtual Private Network** (**VPN**)
- `Google Search` (using advanced operators/dorks)
- Email verification tools: **Hunter.io**, **CentralOps.net**
- Local text editor for documentation

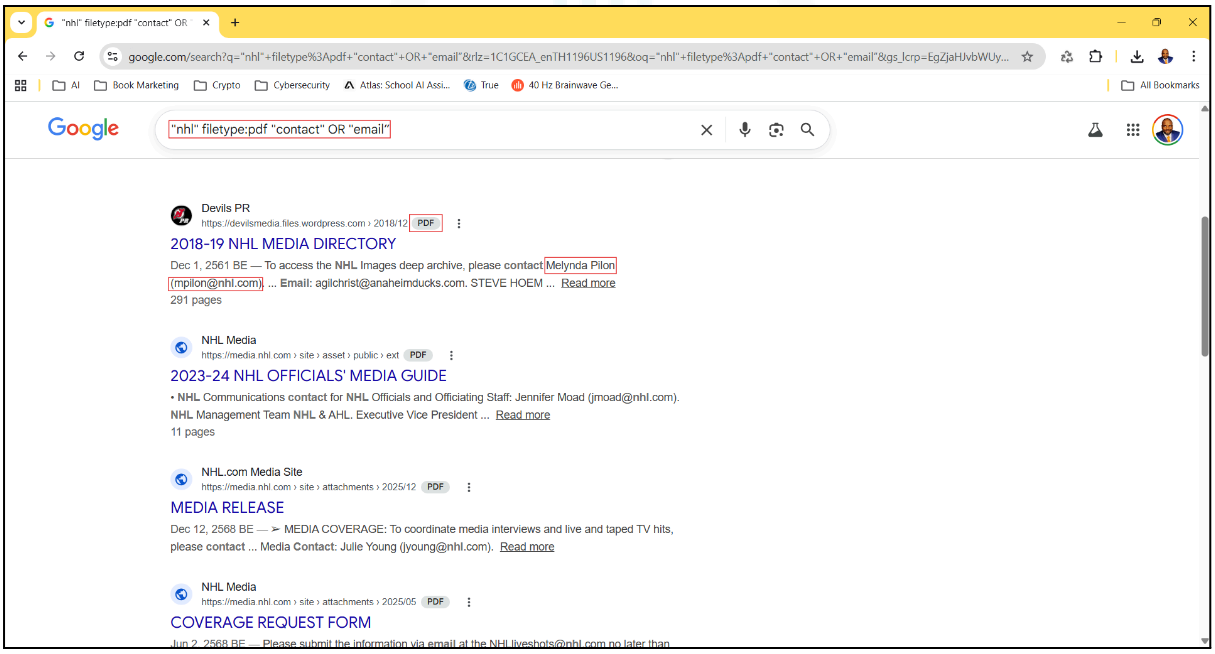
# 2.0 Execution

## 2.1 Reconnaissance

Google dorks were used to locate exposed PDF documents containing contact information. This involved leveraging the `filetype:pdf` operator in conjunction with organization-specific keywords. An example of a successful query pattern is as follows:

```
"example company name" filetype:pdf "contact" OR "email”
```

The PDFs provided both a reference **organization email** and a **personal email** that served as baselines for the pattern analysis.


"nhl" filetype:pdf "contact" OR
google.com/search?q="nhl"+filetype%3Apdf+"contact"+OR+"email"&rlz=1C1GCEA_enTH1196US1196&oq="nhl"+filetype%3Apdf+"contact"+OR+"email"&gs_lcrp=EgZjaHJvbWUy...
AI
Book Marketing
Crypto
Cybersecurity
Atlas: School AI Assi...
True
40 Hz Brainwave Ge...
All Bookmarks
Google

"nhl" filetype:pdf "contact" OR "email”

Devils PR
https://devilsmedia.files.wordpress.com › 2018/12 PDF
2018-19 NHL MEDIA DIRECTORY
Dec 1, 2561 BE — To access the **NHL** Images deep archive, please **contact** Melynda Pilon (mpilon@nhl.com). ... **Email**: agilchrist@anaheimducks.com. STEVE HOEM ... Read more
291 pages

NHL Media
https://media.nhl.com › site › asset › public › ext PDF
2023-24 NHL OFFICIALS' MEDIA GUIDE
• **NHL** Communications **contact** for **NHL** Officials and Officiating Staff: Jennifer Moad (jmoad@nhl.com). **NHL** Management Team **NHL** & AHL. Executive Vice President ... Read more
11 pages

NHL.com Media Site
https://media.nhl.com › site › attachments › 2025/12 PDF
MEDIA RELEASE
Dec 12, 2568 BE — ➢ MEDIA COVERAGE: To coordinate media interviews and live and taped TV hits, please **contact** ... Media **Contact**: Julie Young (jyoung@nhl.com). Read more

NHL Media
https://media.nhl.com › site › attachments › 2025/05 PDF
COVERAGE REQUEST FORM
Jun 2, 2568 BE — Please submit the information via **email** at the NHL liveshots@nhl.com no later than

**Figure 1:** Screenshot of a Google “dork” search. March 31, 2026. Eldon G.

## 2.2 Pattern Analysis

From the organization’s email (e.g., *mpilon@nhl.com*), I identified the corporate **naming convention**: `[first initial][last name]`. This format was verified against other staff members within the same document to ensure its accuracy.

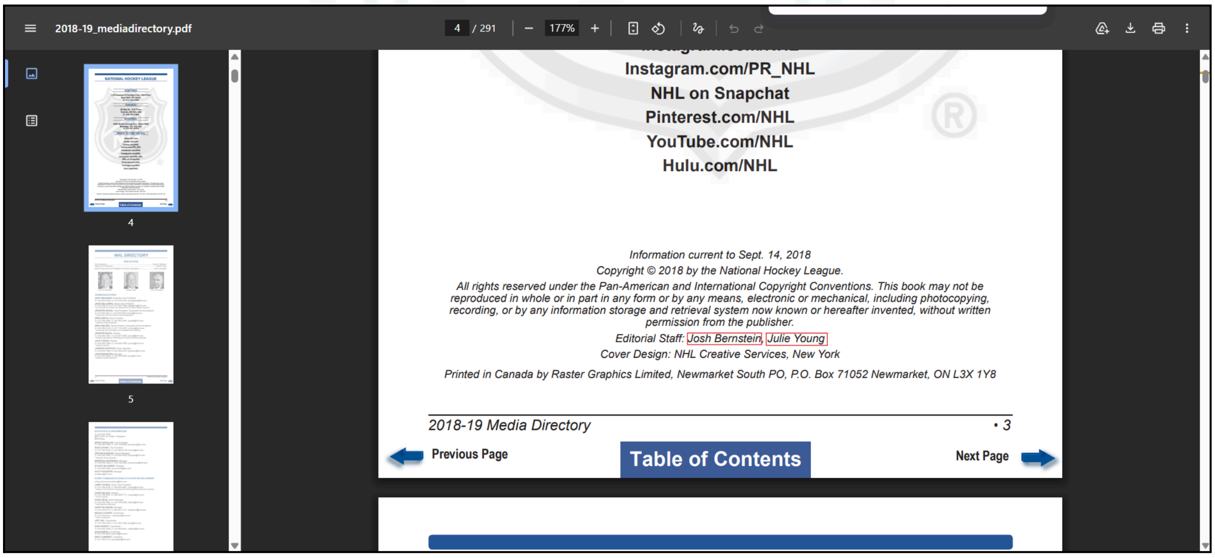
## 2.3 Email Guess Generation

**Organization Guesses:** Using the established `[first initial][last name]` pattern, I generated organizational email guesses for two other employees mentioned in the file:

- *Jbernstein@nhl.com*
- *jyoung@nhl.com*

**Personal Guesses:** For email *jbernstein@nhl.com*, I created expanded guesses across three other providers. I maintained the username *josh.bernstein1*.

- *josh.bernstein1@yahoo.com*
- *josh.bernstein1@gmail.com*
- *josh.bernstein1@cloud.com*



Instagram.com/PR_NHL
NHL on Snapchat
Pinterest.com/NHL
YouTube.com/NHL
Hulu.com/NHL

*Information current to Sept. 14, 2018*
*Copyright © 2018 by the National Hockey League.*
*All rights reserved under the Pan-American and International Copyright Conventions. This book may not be reproduced in whole or in part in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system now known or hereafter invented, without written permission from the publisher.*
*Editorial Staff: Josh Bernstein, Julie Young*
*Cover Design: NHL Creative Services, New York*
*Printed in Canada by Raster Graphics Limited, Newmarket South PO, P.O. Box 71052 Newmarket, ON L3X 1Y8*

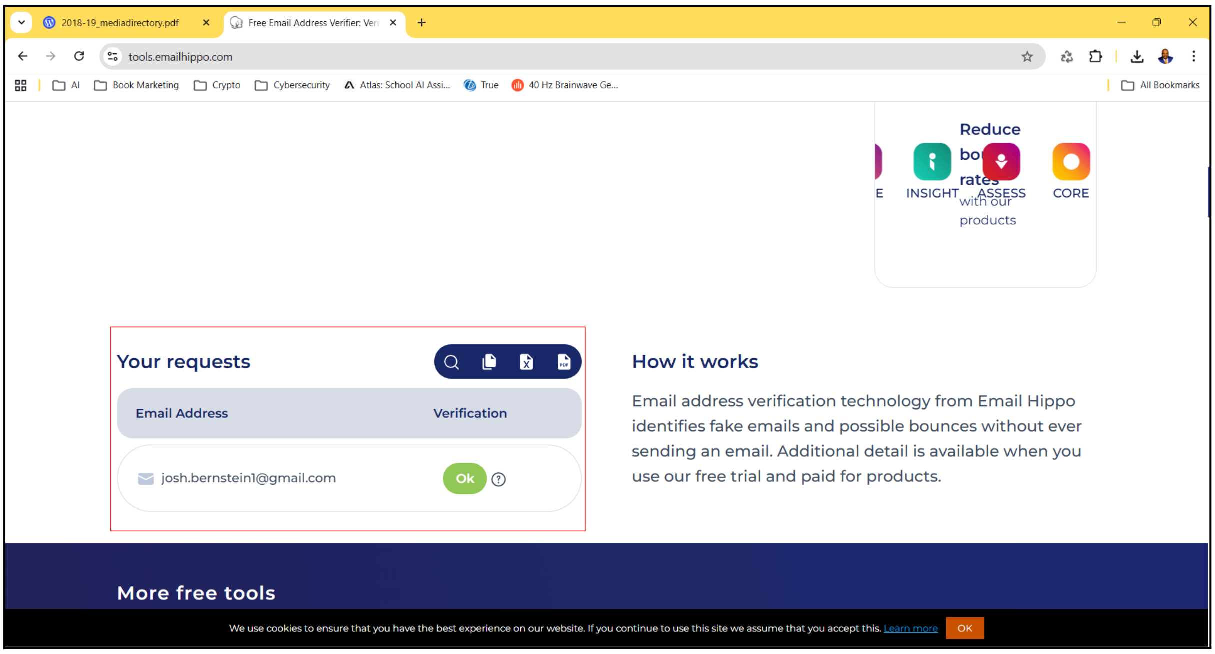
*2018-19 Media Directory* • 3

**Figure 2:** Screenshot of Editorial Staff without contact information. March 31, 2026. Eldon G.

## 2.4 Verification

Each guessed address was tested using an online verification tool. This process checks for the existence of the mailbox by querying the MX records of the domain and/or attempting an **SMTP connection** (depending on the tool).

**Key Observation:** Results varied from a definitive **“valid”** to **“unknown”** or **“risky,”** highlighting the importance of using multiple tools and acknowledging the limitations of free-tier services. At least one of the guessed email addresses returned a definitive 'valid' response, which was cross-validated by one of the verification tools.



Your requests

| Email Address | Verification |
|---|---|
| josh.bernstein1@gmail.com | Ok |

How it works

Email address verification technology from Email Hippo identifies fake emails and possible bounces without ever sending an email. Additional detail is available when you use our free trial and paid for products.

We use cookies to ensure that you have the best experience on our website. If you continue to use this site we assume that you accept this. Learn more

**Figure 3:** Screenshot of verified email address. March 31, 2026. Eldon G.

# 3.0 Findings

## 3.1 Summary Findings

- The naming convention of the target organization was confirmed to be **predictable and uniform**, which allowed for successful enumeration.
- At least one of the guessed email addresses returned a definitive **“valid”** response for all verification tools.
- Verification tools exhibit varying levels of accuracy and are subject to rate limitations under their free-service tiers, which can impact the reliability of the final results.

# 4.0 Conclusion

## 4.1 Key Takeaways

- **Publicly exposed PDFs** and other documents are primary sources for quickly identifying internal organizational naming conventions.
- Email enumeration remains a **practical and low-cost** initial step in OSINT investigations.
- Verification accuracy depends heavily on the **tool's methodology** (e.g., simple MX check vs. full SMTP validation).

## 4.2 Security Implications & Recommendations

**Audit and Redaction:** Organizations should implement strict policies to audit and redact sensitive employee contact information from all publicly accessible documents, including PDFs files.

**Use Aliases:** Replace direct staff emails with **generic contact aliases** (e.g., *info@, support@*) in public materials to prevent automated data harvesting from these sources.

**Ethical Boundary:** Investigators must strictly adhere to the legal and moral limits of OSINT; verified addresses must **never** be used for contact, intrusion, or social engineering attempts.