

Son Tung Thuong

10-03-2005 | Anaheim, California | sontung346@gmail.com | +1714-705-5346 | My Linkedin | My Portfolio

About me

I am a second-year Information Security student from Vietnam, passionate about uncovering cyber threats through **Threat Intelligence, Digital Forensics, Incident Response, and Malware Analysis**. I actively compete in CTFs and explore real-world attack simulations to build practical skills.

I aim to join a **professional SOC or DFIR, CTI, Malware Analysis team** as an intern, where I can both learn and contribute—whether it's analyzing incidents, responding to threats, or hunting adversary behaviors in complex environments.

Certifications

- **Ethical Hacker** – click to view more
- **Google Cybersecurity Certificate** – click to view more

Education

Posts and Telecommunications Institute of Technology, Ho Chi Minh City Aug 2023 – May 2025

- **Cumulative GPA: 3.04/4.0** (Engineering degree of Information Security)
- **Class Monitor** – Led academic coordination and student activities for a class of 60 students.
- **3rd Prize – PTITHCM CTF 2024** which held by PTITHCM
- Engaged in cybersecurity communities, workshops, and hands-on labs in malware analysis and digital forensics.

Technical Skills

- **Threat Detection & Incident Response:** Cross-platform forensics (Windows/Linux/macOS/Android/iOS), memory/disk/log analysis (Volatility, FTK, Autopsy, Sysmon), threat intel with OSINT tools (Shodan, Sherlock, holehe).
- **Malware Analysis:** Knowledge of techniques (DLL Injection, Registry Tampering). Static (IDA Pro, Ghidra, dnSpy) & Dynamic (strace, Wireshark, Any.run) analysis on PE/ELF in C/C++, .NET, ASM, Python.
- **Adversary Tradecraft:** Persistence (Registry, Cron, LD_PRELOAD), MITRE ATT&CK mapping, Cyber Kill Chain implementation.
- **Tools & Techniques:** Sysinternals, Splunk, Wazuh, Wireshark. Integrated RE for IOC extraction.
- **AD Forensics:** Detect Golden Ticket, DCSshadow; track lateral movement (PSEXEC, WMI), parsing Active Directory snapshot using AD Explorer.
- **Capture The Flag (CTF):**
 - Team leader of **f4n_n3r0**, currently ranked 3rd in Vietnam and 42nd in the world on CTFtime.org
 - Actively competes in CTFs with a focus on Forensics, Web Security, Steganography, and OSINT challenges.
 - **Top 1** – CyberMaterial HackHavoc CTF (Hosted by CyberMaterial)
 - **Top 1** – Cygenix CTF (Hosted by Cybergenix Security)
 - **Top 23** – Black Hat USA CTF (Hosted by Bugcrowd)
 - **Top 9** - VishwaCTF 2025 (Hosted by CyberCell VIIT)
 - **Top 6** - ApoorvCTF 2025 (Hosted by Cybersecurity Club, IIIT Kottayam)
 - **Top 7 - Merit Prize** – Hacktheon Sejong 2025 Finals (Hosted by Sejong City)
- **Programming:**
 - Proficient in C/C++, Python and Powershell for automating forensic workflows, parsing logs and PCAPs, and decoding/decrypting data during incident investigations.
 - Basic DSA / Encryption Techniques: Sort/Search, AES, RC4.

Soft Skills

- **Technical Communication:**

- Explained complex DFIR and Threat Hunting concepts to non-technical teammates through clear, concise writeups and debriefs.
- Documented key forensic findings and investigation steps in case reports, including screenshots, tool outputs, and timeline analysis.

- **Collaboration & Leadership:**

- Led a 4-member CTF team to top 10 finish by coordinating roles (RE, crypto, forensics, pwn, web, OSINT)
- Resolved conflicts during group projects by aligning technical approaches with shared goals

- **Problem-Solving Mindset:**

- Investigated security incidents by performing forensic triage, timeline reconstruction, and disk/memory artifact extraction.
- Analyzed unusual file/system behaviors (e.g., tampered logs, modified headers) to trace attacker footprints and persistence techniques.