Fellowship Event Report: APRICOT 2025

Name: Tshering Dorji
Organization:Bhutan Computer Incident Response Team(BtCIRT), GovTech Agency
Event Attended: APRICOT 2025 MasterClass (KINDNS: DNS & DNSSEC operational best practices to improve the DNS Ecosystem)
Dates: February 20–23, 2025
Location:M World Hotel (https://www.mworldhotel.com.my/), Petaling Jaya, Malaysia

---

1. Introduction

As a cybersecurity professional from Bhutan, I was privileged to receive a fellowship to attend the **Asia Pacific Regional Internet Conference on Operational Technologies (APRICOT) 2025** Masterclass workshop on **KINDNS: DNS & DNSSEC operational best practices to improve the DNS Ecosystem.** This three-day workshop focused on improving the DNS ecosystem through best practices.

APRICOT 2025 was not just about technical knowledge; it also emphasized the importance of human networking, soft skills development, and building confidence. It provided an opportunity to learn from technical and business experts about the latest emerging technologies.

For me, APRICOT 2025 was an eye-opener. I was fortunate to connect with experts, expand my professional network, and deepen my understanding of the **Domain Name System (DNS)**.

---

2. Technical and soft skill workshops

2 (a). MasterClass workshop : KINDNS: DNS & DNSSEC operational best practices to improve the DNS Ecosystem:

I attended the **MasterClass on KINDNS: DNS & DNSSEC Operational Best Practices to Improve the DNS Ecosystem**, a technical workshop that deepened my understanding of **Domain Name System (DNS)**.

Fellowship Event Report: APRICOT 2025

The workshop was led by three experts in the DNS field: **Mr. Philip Paeps** from the **Network Startup Resource Center (NSRC)**, **Mr. Champika Wijayatunga** from the **Internet Corporation for Assigned Names and Numbers (ICANN)**, and **Ms. Nyamkhand Buluukhuu** from **Mobicom Group of Mongolia**. These resource persons possess extensive knowledge and expertise in DNS.

As a cybersecurity professional, I have not worked full-time in DNS systems, apart from configuring authoritative servers a few times in my career. However, attending this workshop and learning from these experts significantly enhanced my knowledge of DNS. Additionally, interacting with fellow participants from different countries, each with varying levels of expertise, allowed me to gain insights into their roles and responsibilities.

Before attending the workshop, I knew that DNS resolves hostnames to IP addresses but lacked an in-depth understanding of its working mechanism. Through this workshop, I learned how a DNS query is initiated from a client computer and how it fetches the requested data from the authoritative server. The query undergoes multiple layers of processing. If the requested website's IP is not found in the cache, the **recursive server** sends the request to the **root server**. The root server then checks the **gTLD (generic Top-Level Domain)** and responds to the recursive server, instructing it to contact the appropriate gTLD server. The gTLD server, in turn, knows the domain extension (e.g., .com, .org) but does not store the IP address. It then directs the recursive server to contact the specific **authoritative server**. Finally, the recursive server retrieves the correct IP from the authoritative server, and the requested website is displayed on the client's screen.

DNS is an old protocol, developed in **1984**, during a time when security was not a major concern, as there were fewer technologies and websites. However, with the expansion of the internet and the exponential growth of websites as a key marketing tool, **DNS has become a prime target for malicious attackers**. Threat actors exploit DNS vulnerabilities to **disrupt services, damage organizational reputations, and gain financial benefits**. Since traditional DNS does not use encryption, any data sent in plain text can be easily intercepted by attackers.

To address these security concerns, **Domain Name System Security Extensions (DNSSEC)** was introduced to protect critical information. During the workshop, we performed **hands-on lab exercises**, configuring DNSSEC and understanding its implementation.

The lab used **BIND9**, an open-source, full-featured, and widely deployed DNS software. We learned how to **generate DNSSEC keys** and register or upload them to a **customized registry** within the lab environment. **DNSSEC generates two types of keys:**

- **Zone Signing Key (ZSK):** Signs all the data in the zone files.

- **Key Signing Key (KSK):** Signs the ZSK file.

If the key generation is successful, we obtain four keys consisting of **private and public key pairs**.

Finally, we learned how to validate our **DNSSEC registration** with the parent registry using the command:

```
# dig +dnssec zone soa
```

Overall, this workshop was an **eye-opening experience**, equipping me with both **theoretical and practical knowledge** on **DNSSEC implementation** to enhance the security of DNS infrastructure.

2 (b). Skill workshops:

After the three-day technical workshop, the APRICOT fellows were given the privilege to attend a **skill development workshop**, which I found to be highly productive. In today's **VUCA (Volatile, Uncertain, Complex, and Ambiguous) world,** while strong technical skills are essential, it is **soft skills** that ultimately elevate individuals to leadership positions.

In this workshop, **Mr. Williams** through an online delivered a lecture on building confidence and essential skills for effective public speaking, followed by **Terry's** session on leadership development. He guided us through different leadership styles and introduced us to IKIGAI, a concept that helps lead a successful and fulfilling life in both professional and personal spheres.

Between different segments of the program, we engaged in **group exercises** based on the topics we had learned. At the end of the workshop, we were introduced to internet policy, a session led by **Mr. Robbie** from the Internet Society. We gained insights into how policies are adopted, and as part of the session, we worked in groups to defend a proposed policy, justify its importance, and gather support to secure votes for its approval.

---

3. Key Takeaways from the workshop

- Learned about DNS hierarchy and DNSSEC.

Fellowship Event Report: APRICOT 2025

- Gained hands-on experience in generating DNSSEC keys and communicating with the registry (parent domain). In my case, I would need to request Bhutan Telecom to update my DS set key in their zone file.
- Understood DNS attacks, such as DNS spoofing, and how to protect against them using DNSSEC.
- Learned about different leadership styles, their applications, and how to deliver an effective presentation by using body language and eye contact.

---

4. Application of Learnings from workshop

I plan to:

- Conduct a short class with my division colleagues to share my knowledge on DNS and DNSSEC
- Will propose to assist the cloud division to configure the DNSSEC in their authoritative DNS server

---

5. Networking and Collaboration

The **APRICOT 2025** workshop gave me the opportunity to reconnect with old friends whom I had not met for a long time and renew our friendships. It also provided me with a platform to build new connections with experts and fellow participants.

One of the major highlights of this workshop was the opportunity to finally meet in person someone like Mr.John and Mr.Terry I had been communicating with for a long time. Meeting them face-to-face was truly a joyful and fulfilling experience.

---

7. Conclusion

The APRICOT 2025 fellowship was an invaluable opportunity. I am immensely grateful to everyone involved in organizing this mega event and look forward to applying what I have learned to contribute to a more secure and connected Asia-Pacific region, while also giving back to the community.

Submitted by Tshering Dorji, Fellowship Candidate, (APRICOT 2025)

Fellowship Event Report: APRICOT 2025

Attachments

1. Photos from the conference.

 Participants with certificates	 Fellows closing dinner

---

Submitted by Tshering Dorji, Fellowship Candidate, (APRICOT 2025)