With the rapid evolution of cyber-enabled crimes, it has been observed that offenders are increasingly moving away from conventional operating systems such as Windows and macOS (Macintosh Operating System), and are instead adopting privacy-focused and non-standard operating systems specifically designed to evade surveillance, attribution, and forensic analysis.

Cybercriminals and organized threat actors are known to use operating systems such as Tails (The Amnesic Incognito Live System), Kali Linux, Ubuntu, and other Linux-based or live-boot environments to conduct activities including encrypted communication, anonymous browsing, cyber intrusions, financial fraud, and coordination of criminal operations. These operating systems often offer features such as memory-only execution, built-in anonymization, encryption by default, and minimal artifact retention, posing significant challenges to law-enforcement investigations.

At present, there is a lack of consolidated understanding regarding:

1. The range of operating systems commonly used by cybercriminals for conducting cyber threats and organized criminal activities.

2. The freely available open-source or public tools that are most frequently downloaded and misused from the internet for activities such as anonymization, intrusion, communication, and data exfiltration.

3. The forensic feasibility and limitations of examining non-standard or privacy-oriented operating systems, particularly live or amnesic systems such as Tails.

4. The availability and effectiveness of forensic tools and methodologies capable of acquiring, preserving, and analysing digital artefacts from such operating systems without compromising evidentiary value.

Objective of the Exercise

The objective of this problem is to:

- Identify and categorize operating systems commonly exploited by cybercriminals.

- Map commonly misused freely available tools associated with these operating systems.

- Examine forensic challenges and investigative blind spots posed by amnesic and non-persistent systems.
- Propose forensic tools, techniques, and workflows that can be used to analyse devices running Tails OS and other similar non-standard operating systems in a legally sound and technically reliable manner.

Expected Outcome

The problem-solving team is expected to:

- Provide a comparative assessment of criminal usage patterns across different operating systems.
- Identify high-risk tools and utilities that require focused monitoring.
- Recommend forensic acquisition and analysis strategies suitable for live, volatile, or encrypted operating environments.
- Highlight gaps in current forensic capabilities and suggest potential solutions or research directions