Forensic Analysis of Container Snapshot Chains for Post-Event Reconstruction

Radostin Stoyanov - PhD Student, Scientific Computing Group
Collaboration with Lorena Goldoni, Adrian Reber, Christopher Hargreaves
Supervisors: Prof. Rodrigo Bruno, Prof. Wes Armour

Why Kubernetes forensics is hard?

How attackers stay stealthy in Kubernetes?

- Masquerade as legitimate workloads[1, 2]
- Leverage native tools & APIs (kubectl, bash, python)[1, 2]
- Maintain persistence (e.g., DaemonSets, CronJobs)[1, 2]
- Exploit unpatched APIs/runtimes without disruption[3, 4]
- Steal credentials silently[4]

[1] MITRE ATT&CK - Containers Matrix
[2] Microsoft's Threat Matrix for Kubernetes
[3] Kubernetes CVE Feed
[4] https://github.com/cdk-team/CDK

Why Kubernetes forensics is hard?

Cloud-Native, Runtime-Focused Threats[1,2]

- In-memory malware (no disk artifacts)
- Living-off-the-land binaries in containers (bash, wget, python)
- Exploiting container runtime & kernel interfaces
  - e.g., privilege escalation from Pod to node (CVE-2019-5736)

Kubernetes Attack Surface[3]

- API-based attacks: RBAC misconfigurations, token reuse, API scraping
- Lateral movement via compromised service accounts
- Sidecar injection and workload mutation at runtime

[1] Cloud Native Security Whitepaper
[2] Microsoft's Threat Matrix for Kubernetes
[3] Microsoft Threat Intelligence, *Understanding the Threat Landscape for Kubernetes and Containerized Assets*

Why traditional forensics fails in Kubernetes?

Challenges with Classic Forensic Assumptions

- Assume static hosts and persistent storage
- Require node-level access and workload disruption
- Focus on disk artefacts, missing memory and runtime state
- Fail with ephemeral containers and rescheduled Pods
- Weak evidence attribution and chain of custody in clusters

Schmid et al. *Limits to the Forensic Analysis of Container Applications in Cloud Environments*. (2025)
Gharaibeh et al. *Don't, Stop, Drop, Pause: Forensics of CONtainer CheckPOINTs (ConPoint)*. (2024)

Our contributions

- Forensic Snapshot Chains (FSC)
  - Uses successive checkpoints as a timeline to reconstruct events
  - Investigate in-memory and fileless attacks in ephemeral containers
- Incremental Snapshot Acquisition
  - Captures only the changes between snapshots
  - Reducing performance overhead and storage requirements
- Checkpoint Analysis
  - Interpret successive forensic artifacts from checkpoint images
  - Enable reconstruction of attack progression over time

What is a Forensic Container Snapshot?

From Alerts to Digital Evidence





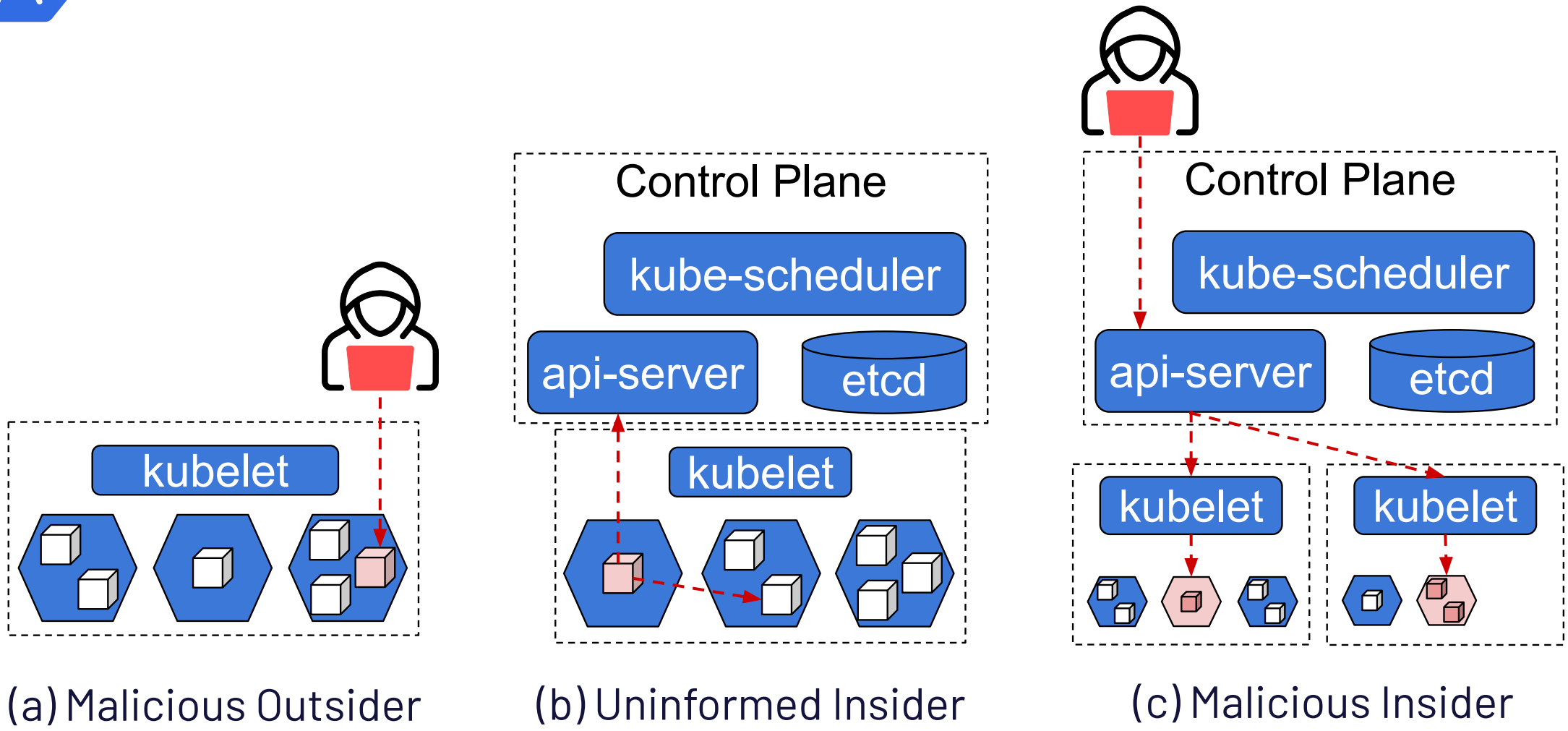
Forensic Readiness

A proactive approach ensuring systems and networks are prepared to efficiently collect, preserve, and analyze evidence when a security incident occurs[1]

Extended Audit Logging ✚ *Automated Checkpointing*

Jason Sachowski, *Implementing Digital Forensic Readiness: From Reactive to Proactive Process*. (2016)

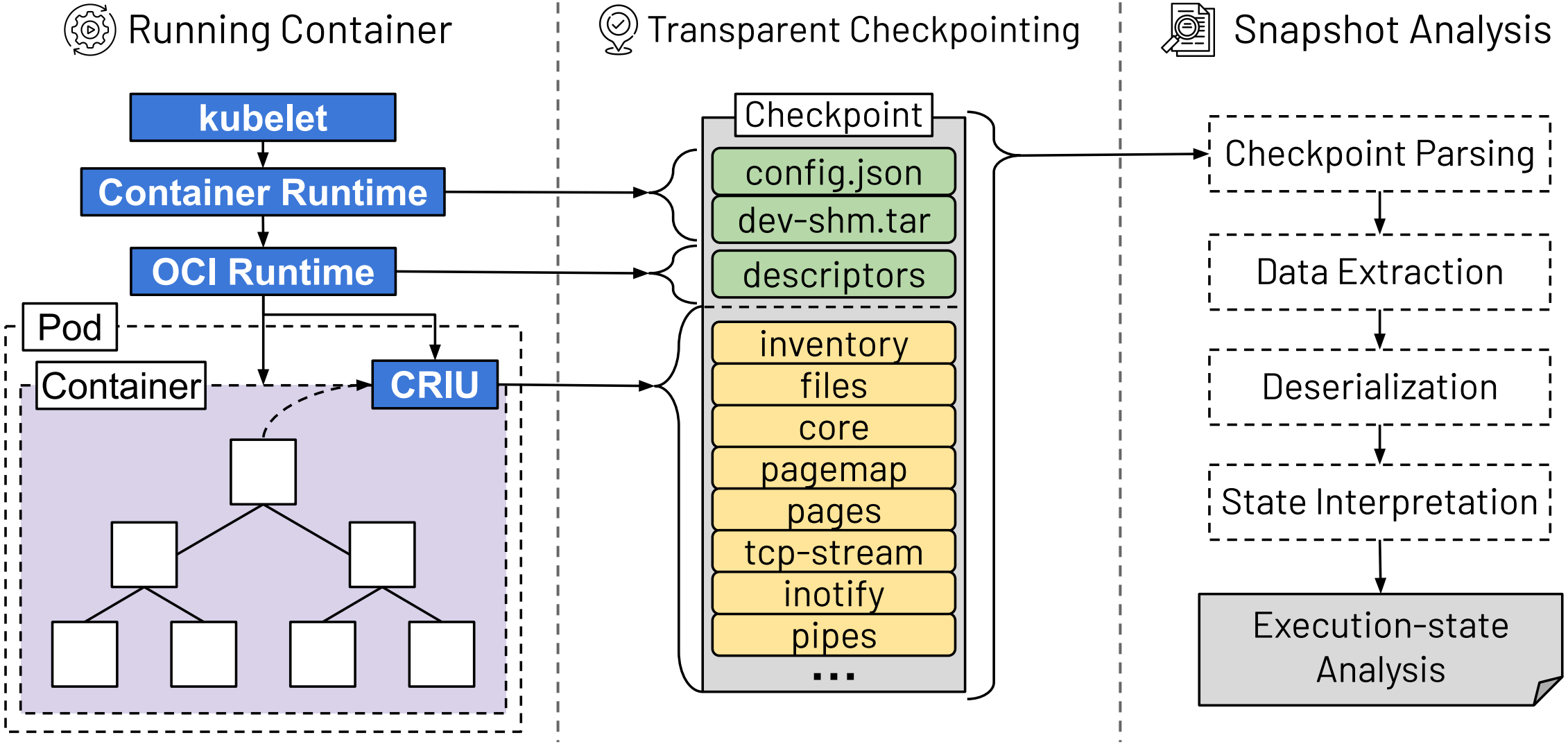
Threat Modeling



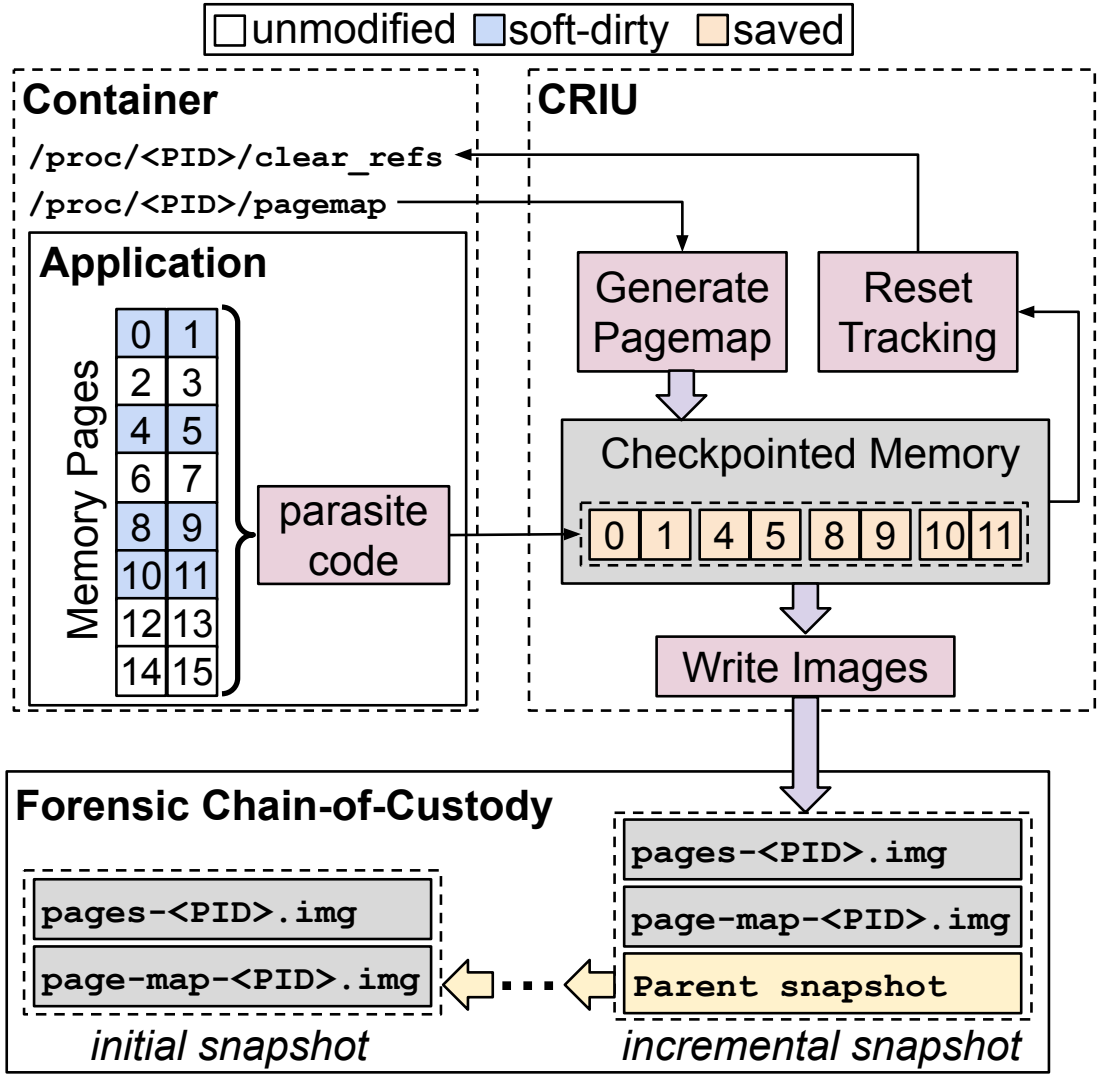
(a) Malicious Outsider (b) Uninformed Insider (c) Malicious Insider

Cloud Native Security Whitepaper (2022)

Snapshot Acquisition



Forensic Snapshot Chains



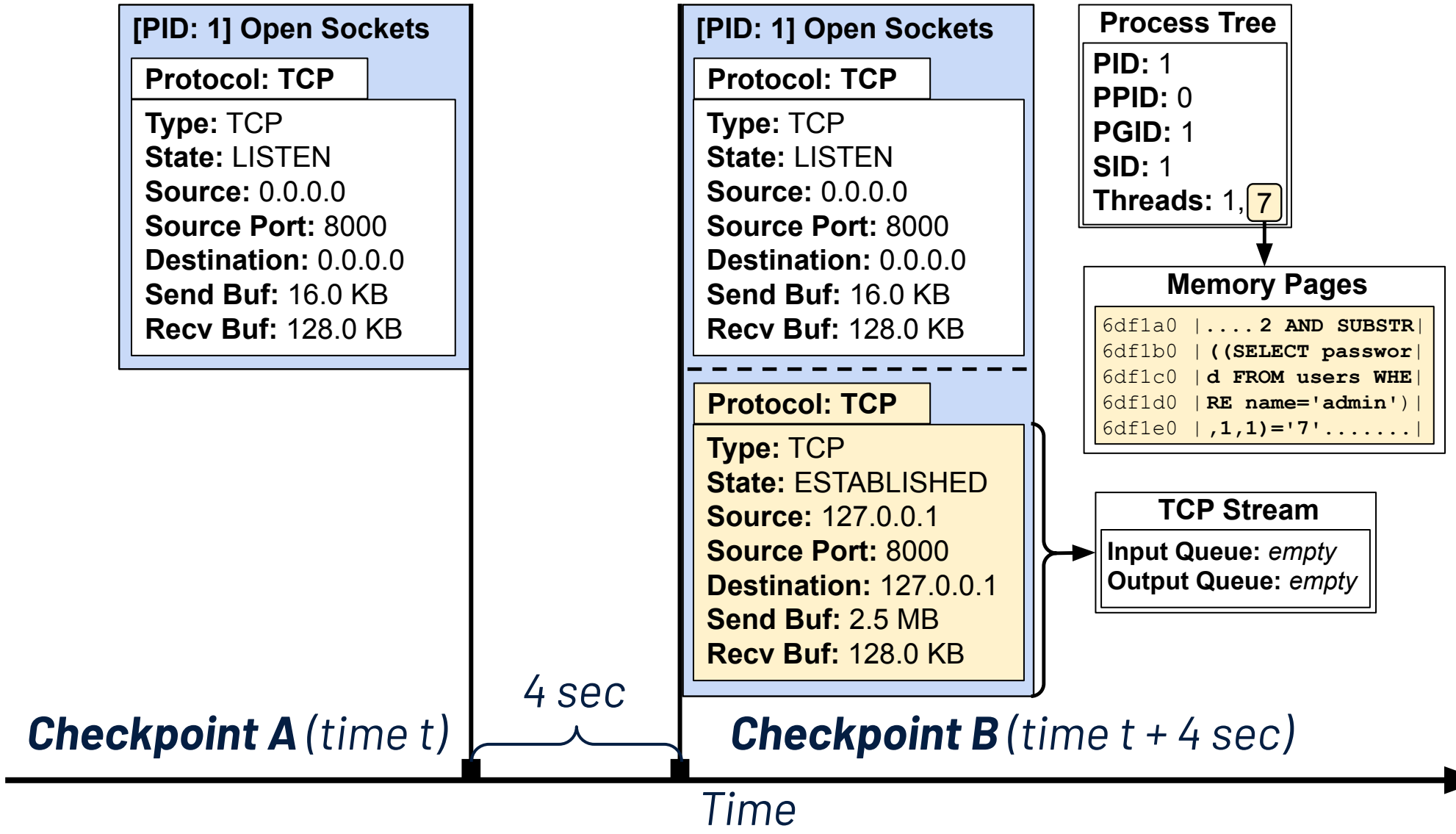
Checkpoints

- Immutable image digests
- Container IDs
- Pod UIDs
- Kubernetes Namespaces

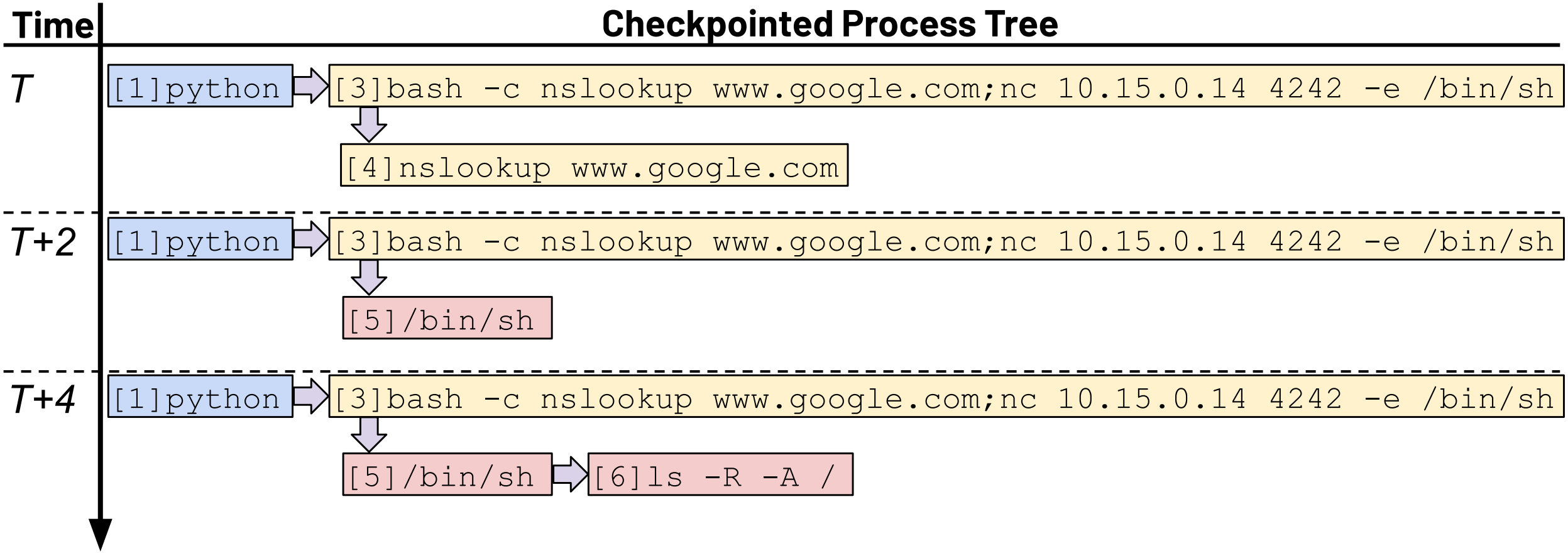
Timestamp Correlation

- Audit logs
- Checkpoint time
- Incident timeline

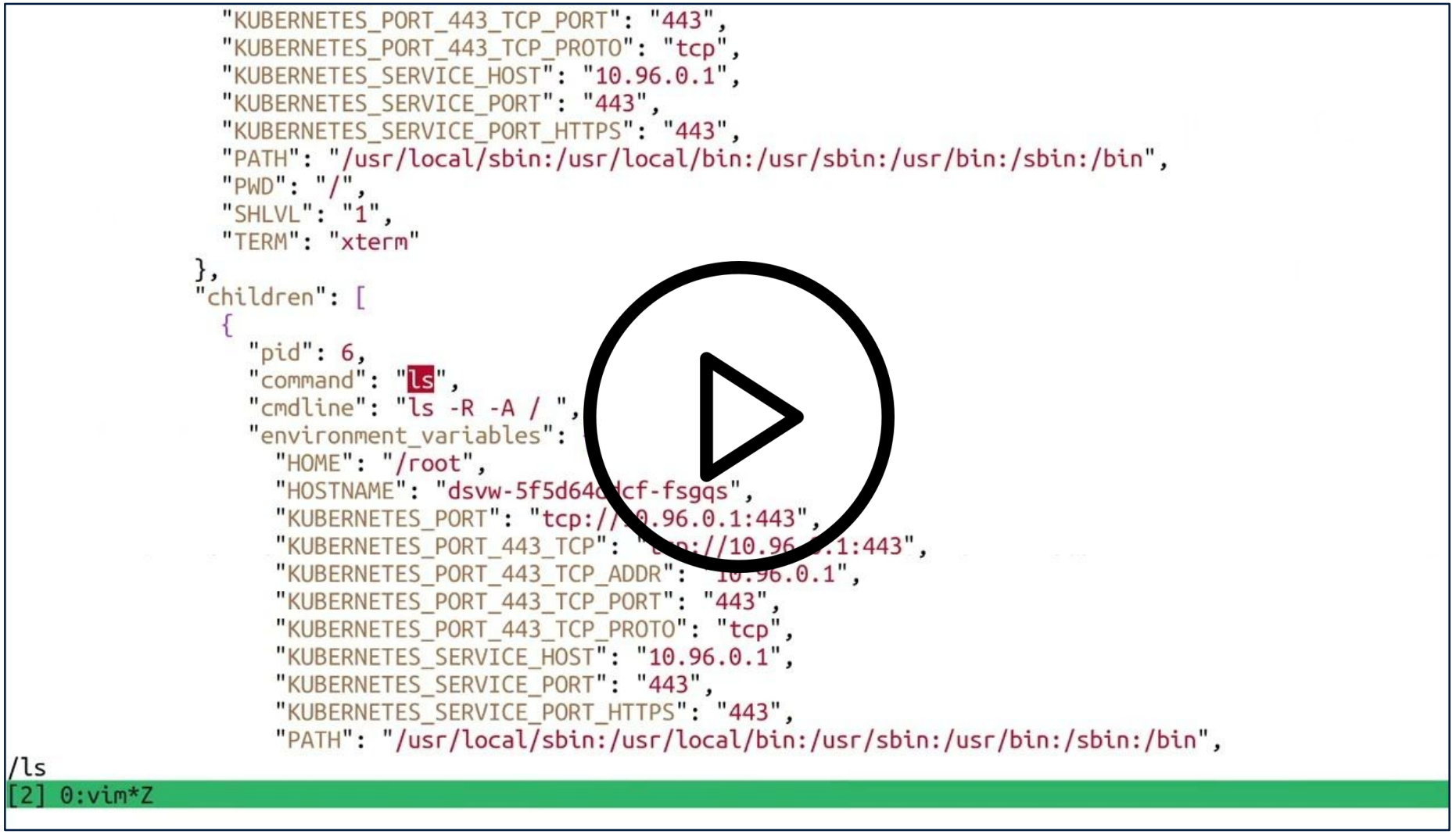
Analysis of SQL Injection Attack



Analysis of Command Injection Attack



Analysis of Command Injection Attack



Key Takeaways

- Detection ≠ Investigation
  - Security alerts detect incidents
  - Forensic investigations explain *what happened*, *how*, and *why*
- Traditional forensic techniques do not fit Kubernetes
  - Kubernetes = Ephemeral containers + dynamic state-reconciliation
  - Modern malware is memory-resident (fileless)
- Forensic snapshots preserve runtime evidence
  - Snapshots are taken without stopping workloads or alerting attackers
  - Capture memory, processes, and network state from live containers



github.com/checkpoint-restore/checkpointctl

criu.org/Kubernetes

Summary & Questions?

- Kubernetes attacks reside in the runtime state
- Alerts alone are not evidence
- Container snapshots preserve evidence that would otherwise be lost