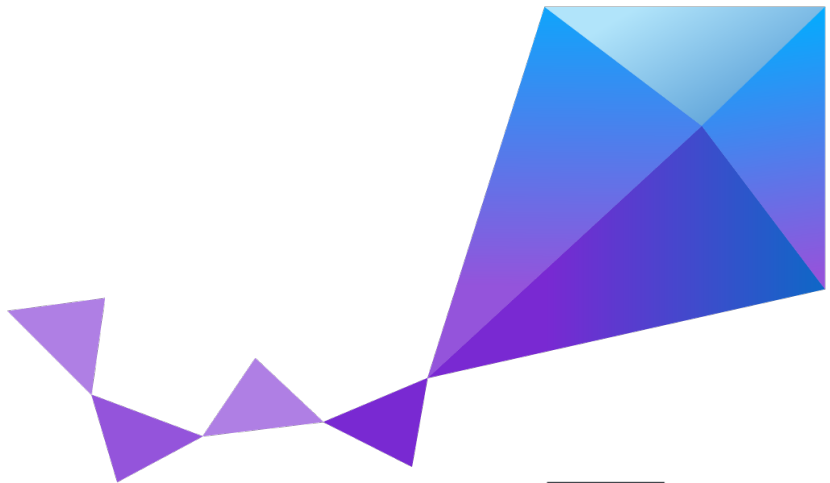
SBOMs for Embedded Firmware: The Zephyr RTOS Case Study

Benjamin Cabé
<benjamin@zephyrproject.org>



Zephyr® Project

A widely deployed, industrial-grade, real-time operating system


Zephyr RTOS
3rd Party Libraries
Application Services
OS Services
Kernel
HAL

SBOM for embedded products

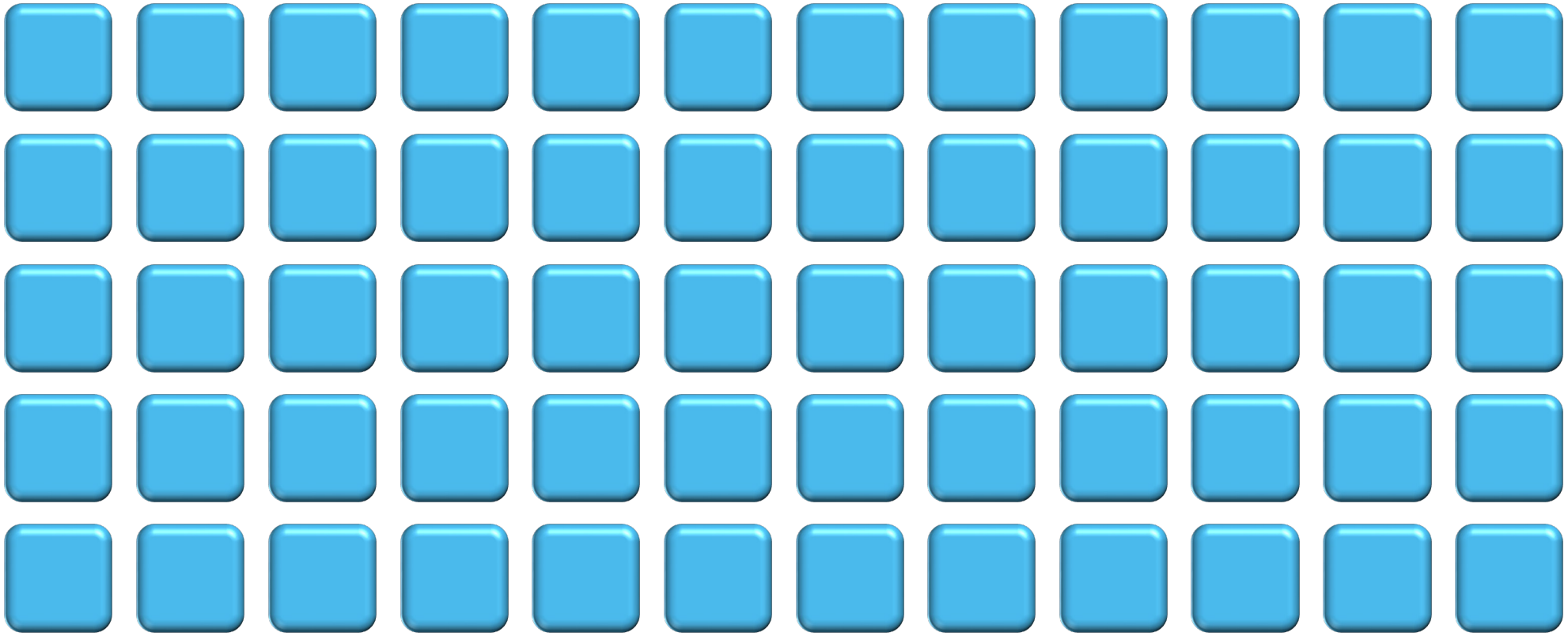
- Application code is only the tip of the iceberg
- RTOS itself
- Libraries
- HALs (Hardware Abstraction Layers)

SBOM for embedded products

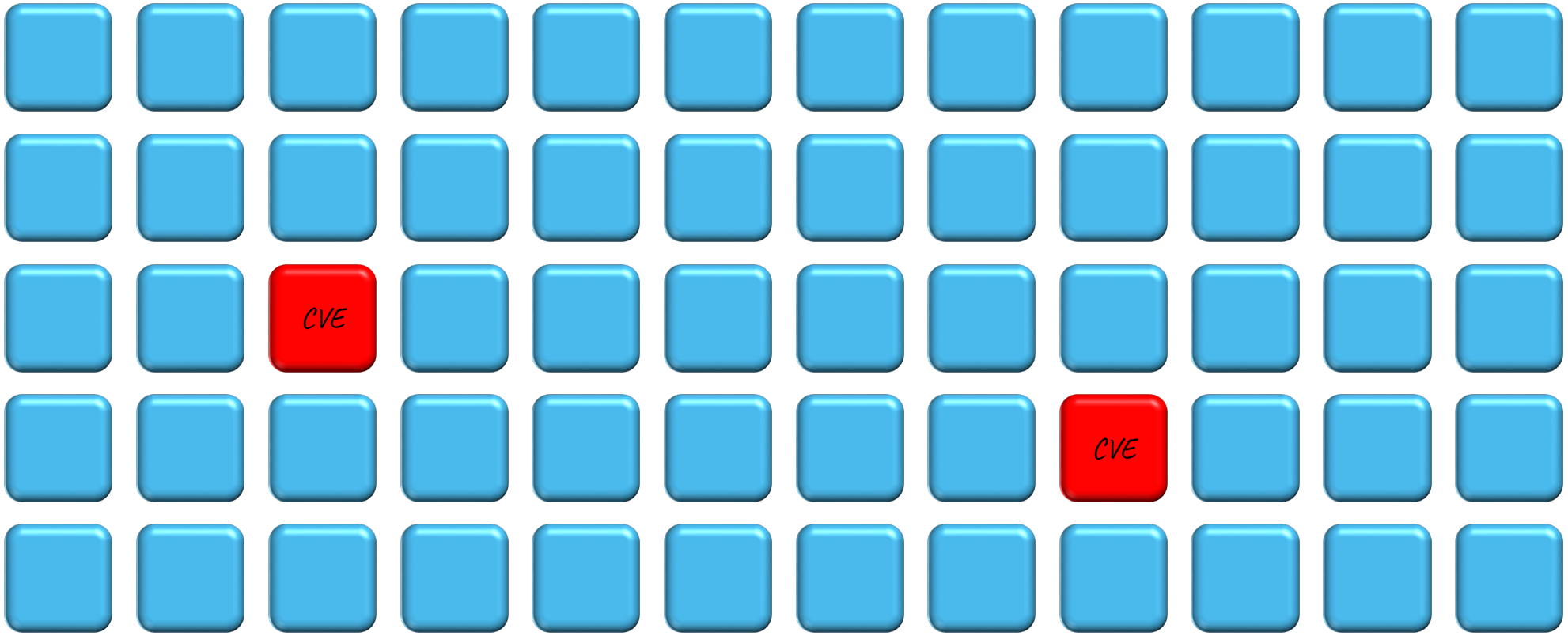
- Application code is only the tip of the iceberg
- RTOS itself
- Libraries
- HALs (Hardware Abstraction Layers)

… oh, and do I <u>really</u> pull in *all* this code?

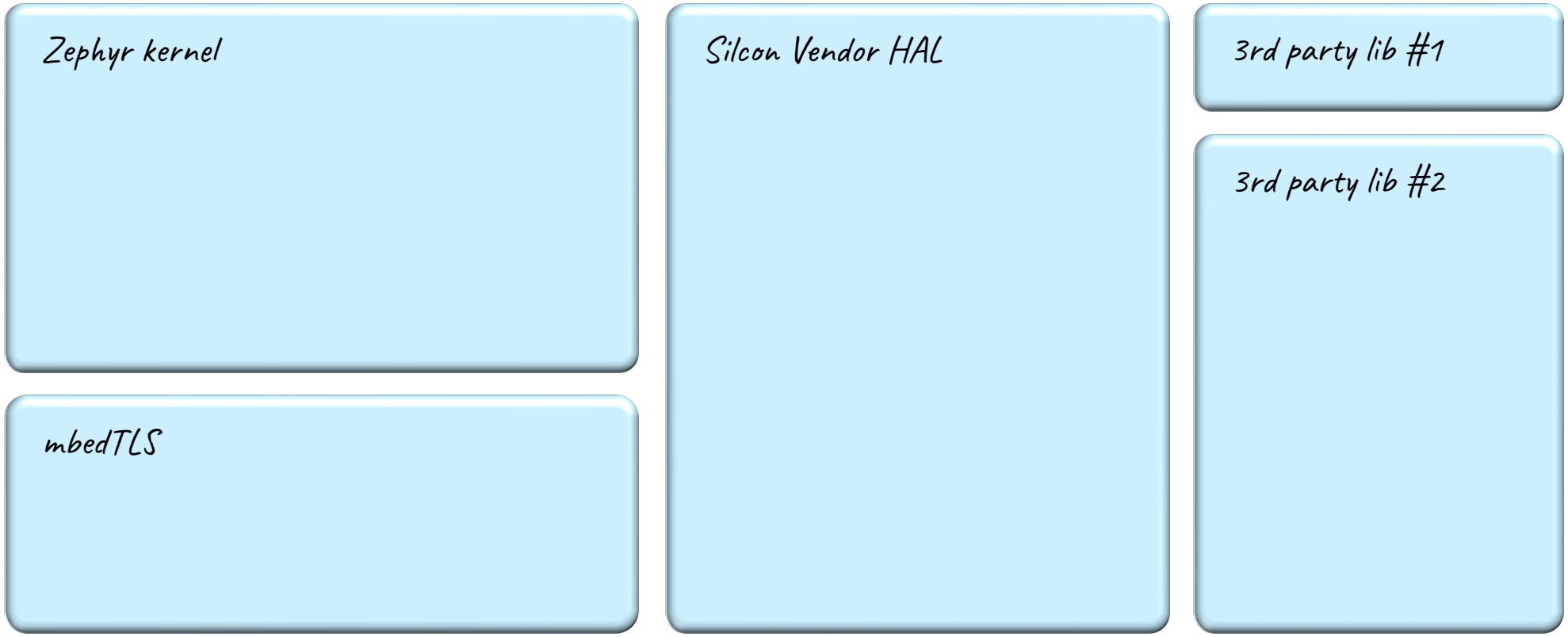
React.js application



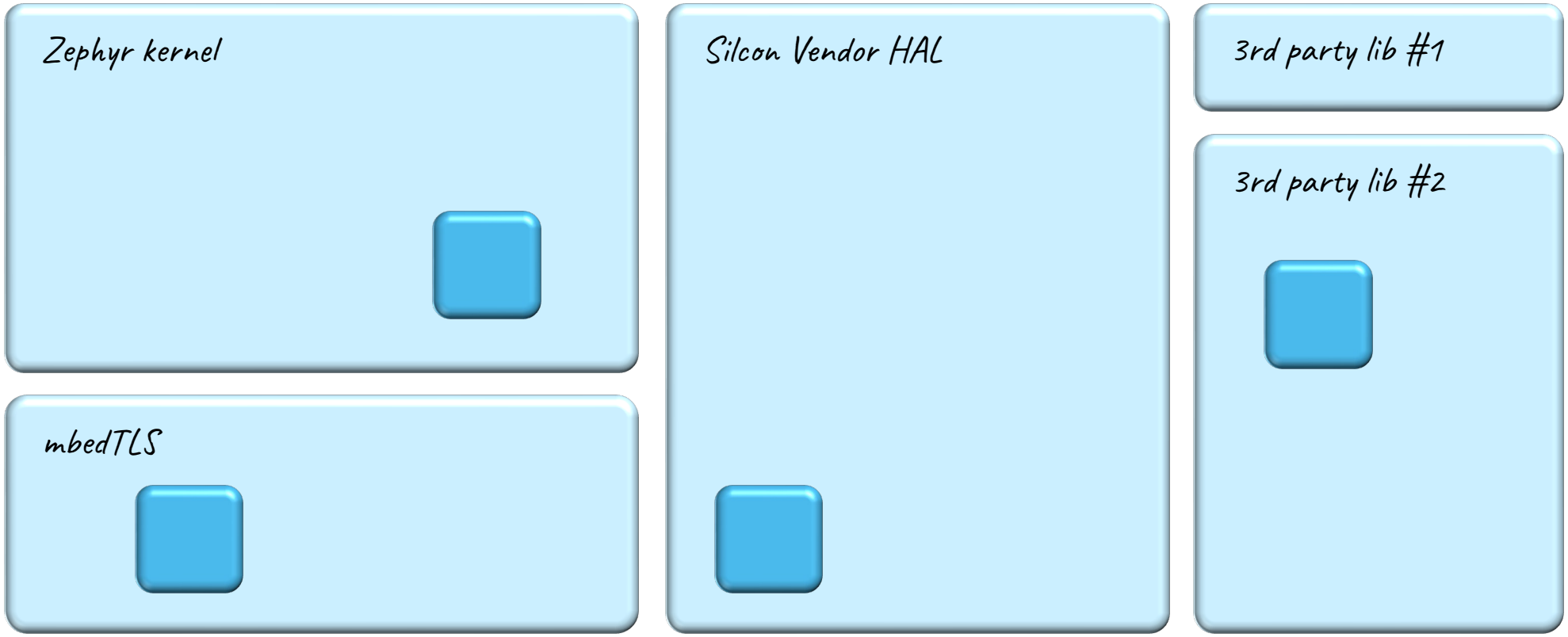
React.js application



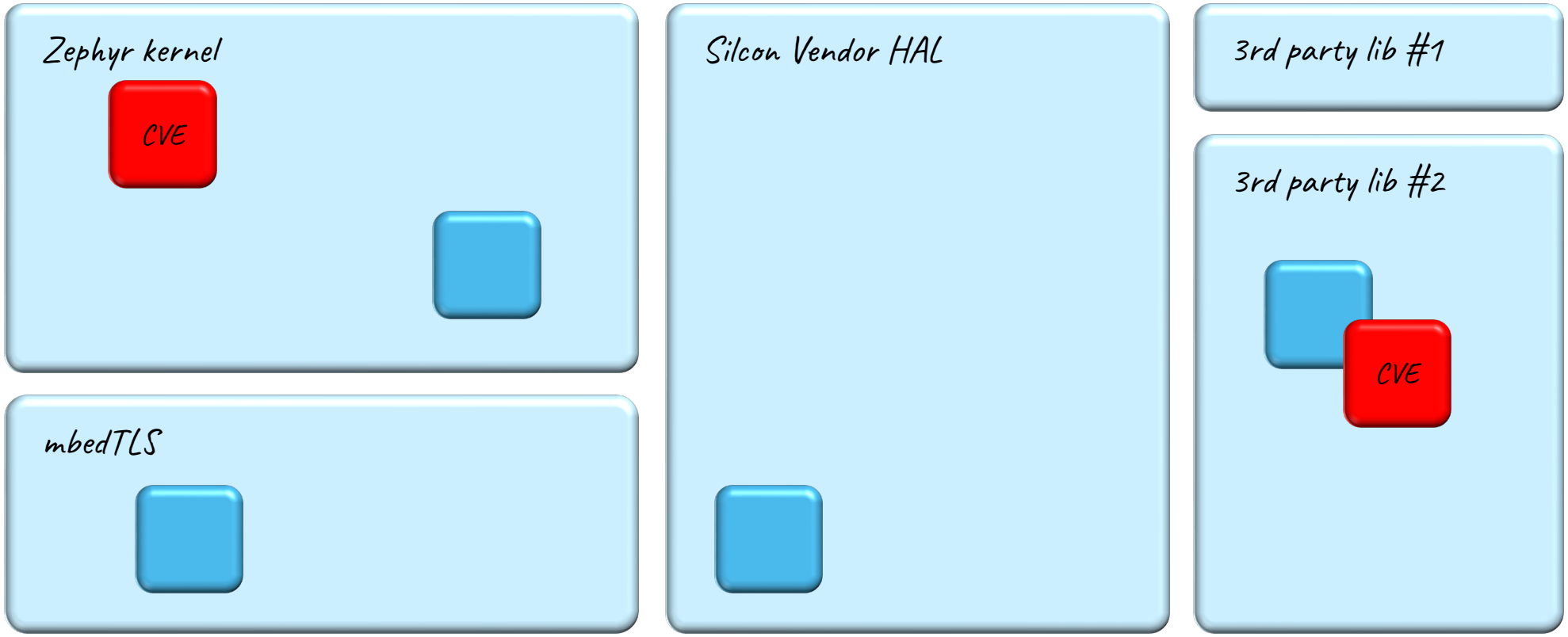
Zephyr application



Zephyr application



Zephyr application



From a Zephyr build to accurate SBOM(s)

CMake File API

- Capture dependencies between various build targets
- Target type (static library, executable, …)
- Compile flags

https://github.com/swinslow/cmake-spdx

Scan files

- Extract copyright headers (REUSE library)
- Extract license headers
- Generate fingerprints

“Zephyr pass”

- Identify modules
- Arrange into different SBOM documents (Zephyr sources, app sources, build files, SDK, …)

Zephyr modules

- Not everything lives in Zephyr upstream
- 1st and 3rd party modules can easily be pulled into a Zephyr manifest to add functionality...

  ... together with their CVEs?

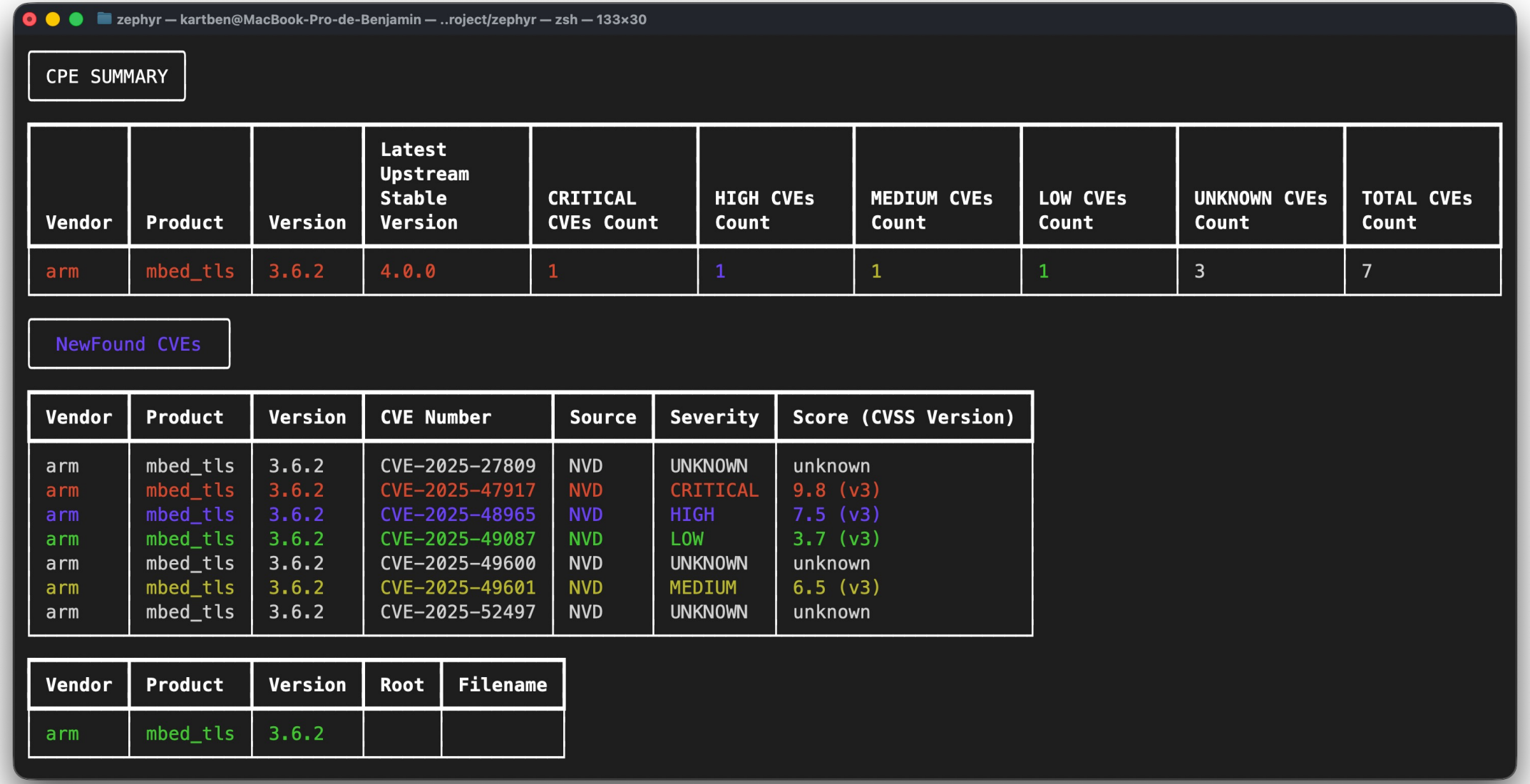
mbedtls/zephyr/module.yml

```
name: mbedtls
build:
  cmake-ext: True
  kconfig-ext: True
security:
  external-references:
    - cpe:2.3:a:arm:mbed_tls:3.6.5:*:*:*:*:*:*:*
    - pkg:github/Mbed-TLS/mbedtls@v3.6.5
```

```
...

##### Package: mbed-tls

PackageName: mbed_tls
SPDXID: SPDXRef-mbedtls-deps
PackageLicenseConcluded: NOASSERTION
PackageLicenseDeclared: NOASSERTION
PackageCopyrightText: NOASSERTION
PackageDownloadLocation: NOASSERTION
PackageVersion: 3.6.5
PackageSupplier: Organization: arm
ExternalRef: SECURITY cpe23Type
cpe:2.3:a:arm:mbed_tls:3.6.5:*:*:*:*:*:*:*
ExternalRef: PACKAGE-MANAGER purl pkg:github/Mbed-TLS/mbedtls@v3.6.5
FilesAnalyzed: false
PackageComment: Utility target; no files

...
```

```
cve-bin-tool  --sbom spdx
              --sbom-file build/spdx/modules-deps.spdx
```

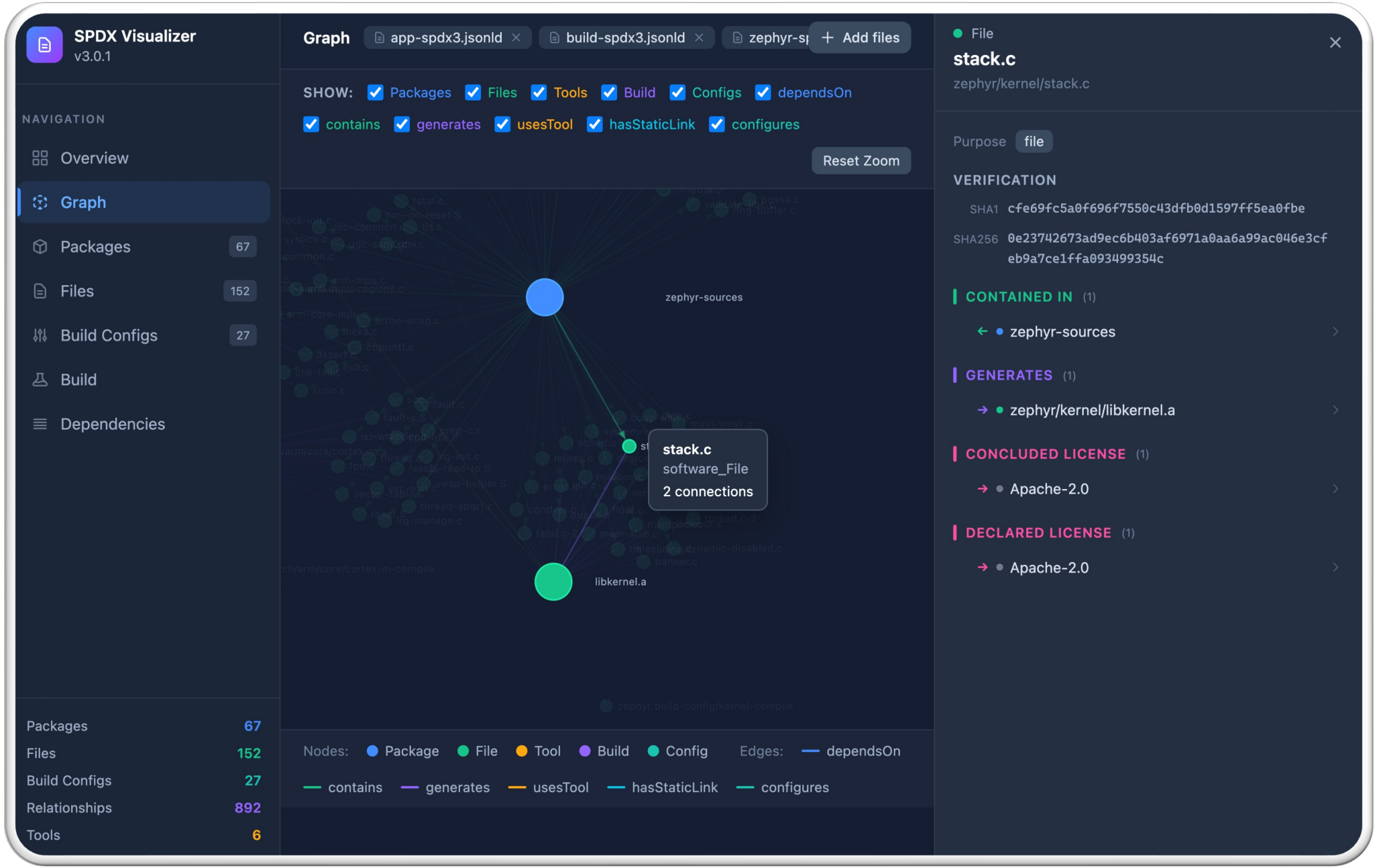
```
cve-bin-tool  --sbom spdx
              --sbom-file build/spdx/modules-deps.spdx
```

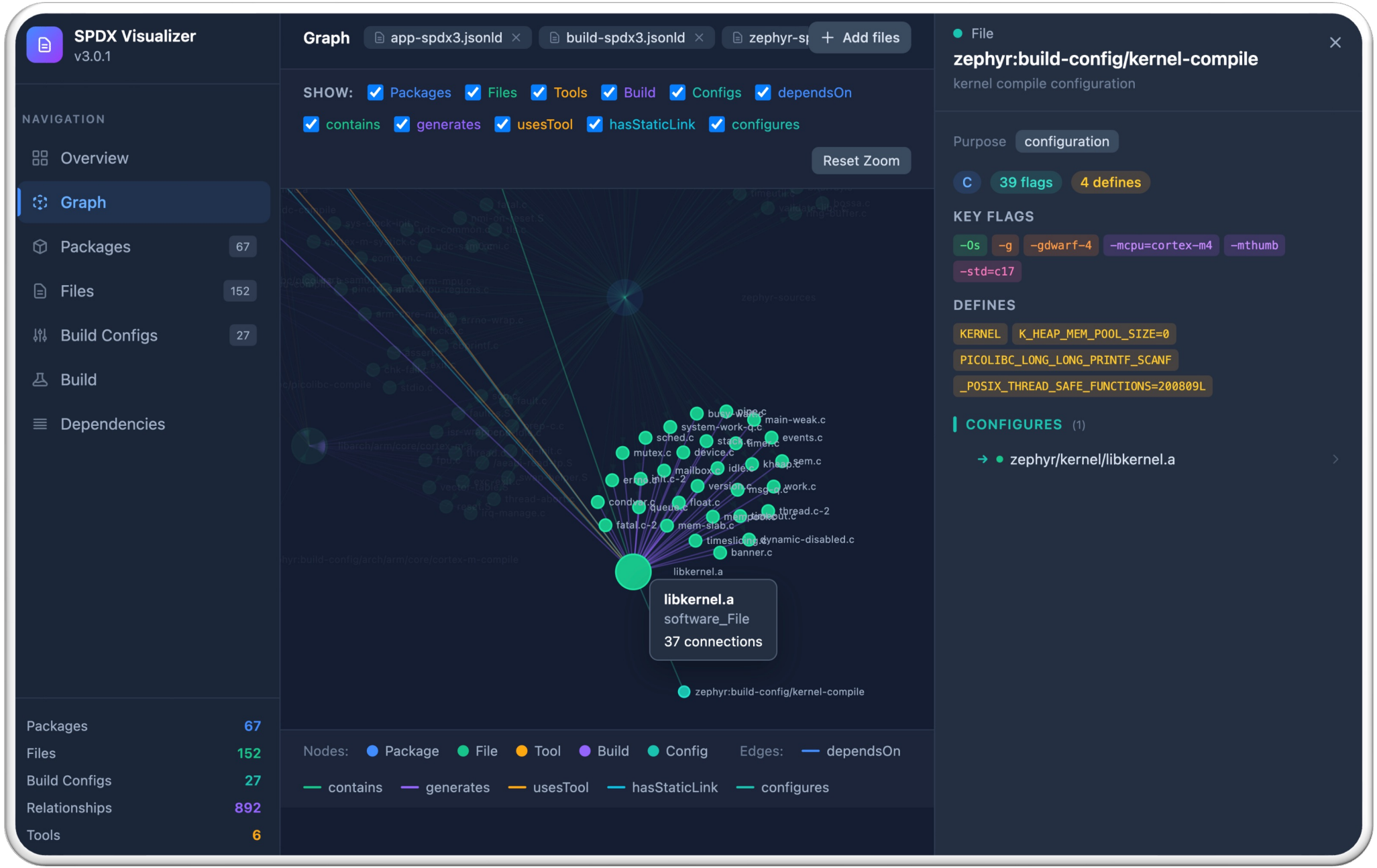


Towards SPDX 3 support

- SPDX 3.0 profiles (Software, Security, Licensing, Build, AI/ML, …) are very relevant for embedded
- Graph-oriented (JSON-LD)
  - Much easier to bake more ”Zephyr-specific” intelligence without being constrained by document-oriented serialization
- Richer semantics
  - e.g. `LifecycleScopedRelationship` for captured detailed information re: compilation process

DEMO


SPDX Visualizer
v3.0.1
NAVIGATION
Overview
Graph
Packages 67
Files 152
Build Configs 27
Build
Dependencies
Packages 67
Files 152
Build Configs 27
Relationships 892
Tools 6
Graph
app-spdx3.jsonld
build-spdx3.jsonld
zephyr-sp
Add files
SHOW:
Packages
Files
Tools
Build
Configs
dependsOn
contains
generates
usesTool
hasStaticLink
configures
Reset Zoom
zephyr-sources
stack.c
software_File
2 connections
libkernel.a
Nodes:
Package
File
Tool
Build
Config
Edges:
dependsOn
contains
generates
usesTool
hasStaticLink
configures
File
stack.c
zephyr/kernel/stack.c
Purpose
file
VERIFICATION
SHA1 cfe69fc5a0f696f7550c43dfb0d1597ff5ea0fbe
SHA256 0e23742673ad9ec6b403af6971a0aa6a99ac046e3cfeb9a7ce1ffa093499354c
CONTAINED IN (1)
zephyr-sources
GENERATES (1)
zephyr/kernel/libkernel.a
CONCLUDED LICENSE (1)
Apache-2.0
DECLARED LICENSE (1)
Apache-2.0


SPDX Visualizer
v3.0.1
NAVIGATION
Overview
Graph
Packages 67
Files 152
Build Configs 27
Build
Dependencies
Packages 67
Files 152
Build Configs 27
Relationships 892
Tools 6
Graph
app-spdx3.jsonld
build-spdx3.jsonld
zephyr-sp
Add files
SHOW:
Packages
Files
Tools
Build
Configs
dependsOn
contains
generates
usesTool
hasStaticLink
configures
Reset Zoom
libkernel.a
software_File
37 connections
zephyr:build-config/kernel-compile
Nodes:
Package
File
Tool
Build
Config
Edges:
dependsOn
contains
generates
usesTool
hasStaticLink
configures
File
zephyr:build-config/kernel-compile
kernel compile configuration
Purpose
configuration
C
39 flags
4 defines
KEY FLAGS
-Os
-g
-gdwarf-4
-mcpu=cortex-m4
-mthumb
-std=c17
DEFINES
KERNEL
K_HEAP_MEM_POOL_SIZE=0
PICOLIBC_LONG_LONG_PRINTF_SCANF
_POSIX_THREAD_SAFE_FUNCTIONS=200809L
CONFIGURES (1)
zephyr/kernel/libkernel.a

Towards SPDX 3 support – open questions

- Capturing **configuration** seems complicated, geared towards config “URIs” and not something that should live in the SBOM?
- “**`Tool`**” could probably allow to capture **more structured information** (e.g. version, …)

Wrapping up

- CMake file-based API FTW!
- Stay tuned for SPDX 3 support being merged in Zephyr ☺
- Next?
  - Tooling to help “diffing” against a given upstream reference? (typically a released LTS version).