The sboms in this directory were created with SwiftBom (<https://sbom.democert.org/sbom/>) based on the ‘single file view’ of the blinky application (<https://github.com/nerves-project/nerves_examples/blob/main/blinky/lib/blinky.ex> ) provided by the Plugfest organizers.

This tool requires manual input by the SBOM creator (in this case Duncan Sparrell).

The data chosen was:

* Main file
* Dependency on Logger
* Dependency on Nerves.Led

The files created were:

* CycloneDX-sfractal-blinky-0-1-1-1-4-2021-12-50.json
* CycloneDX-sfractal-blinky-0-1-1-1-4-2021-12-50.xml
* SPDX-sfractal-blinky-0-1-1-1-4-2021-12-50.spdx
* SWID-sfractal-blinky-0-1-1-1-4-2021-12-50.xml
* sfractal-blinky-0\_1\_1.png (as downloaded from the tool)
* ScreenShotGraph (screenshot with more info than download)

Questions raised:

1. Naming conventions? I just used what SwiftBom put out which hopefully are self-explanatory enough
2. I published all the formats swiftbom provided which is not all of them (eg only one of the 7 SPDX formats)
3. When using a package from a package manager (eg Logger from hex - see <https://hexdocs.pm/logger/Logger.html> ), what should be used for ‘organization’ name? Note Logger is an optional part of the Elixir programming language. The source is at <https://github.com/elixir-lang/elixir/blob/master/lib/logger/lib/logger.ex> but this could lead us down the rabbit hole of ‘trust’ of source to package manager etc. So I put ‘hex’ (ie the package manager) as the name
4. I did not put elixir itself as a dependency, yet it clearly is. I did not include because this is the ‘single file’ version that works on many Elixir versions on many platforms. My logic was this would be added by the ‘downstream’ user of the software. In my case I ran it on my mac laptop running interactive elixir ver 1.11.4 which in turn is dependent on erlang/OTP 23 (erts-11.1.8) but for ‘sf’ sbom I considered that unnecessary.