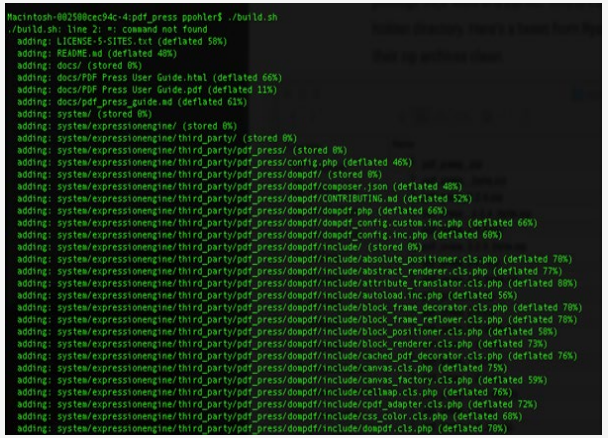
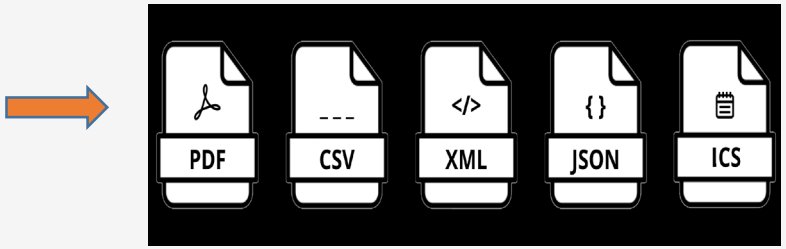
SBOM – POC Manufacturer Perspective

POC lessons and challenges

Steps in SBOM POC

1. Information Gathering
2. Generating machine/human readable document
3. Distributing/Sharing SBOM

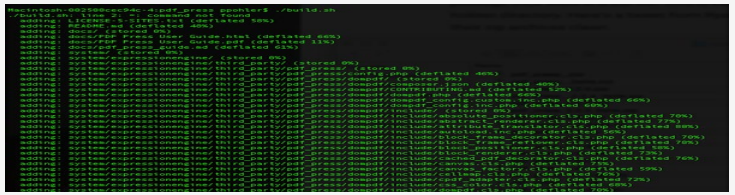




Steps in SBOM POC

1 Information Gathering

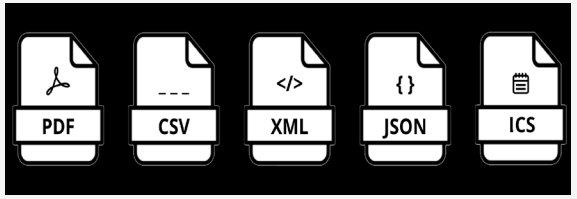
- Application Components
- Platform Components



Product Team	SCA Tools	License Clearance Team	Manual Inventory List	SW Build Team (CI)	Vulnerability Monitoring
- WMI and Powershell ○ Too much of unwanted data! ○ Missing non-installable components	- Open source and commercial SCA ○ Most are good in identifying open source or COTS components ○ Missing some custom built components	- Licensing components list ○ Not able to get complete list of components	- MDM inventory of product's components ○ Use Excel macro to create SBOM ○ Webform data entry	- Export build script ○ Missing Platform components ○ Missing manufacture's name	- 3rd Components monitoring ○ Has all information for SBOM and VEX ○ Need to ensure Data completeness

Steps in SBOM POC

2 Generating machine/human readable document



- Content
  - Baseline elements established by the Framing Working Group
- Formats
  - SPDX, SWID and CycloneDX
  - POC has established SPDX and SWID
  - SPDX and CycloneDX have tool support
- Tools
  - Custom Excel script files
  - Web based data entry form
  - Manufacturer custom tools
  - SCA tools generate SPDX or custom format
- Challenges
  - Component ID
    - Software Identity
    - purl, CPE names
  - Component patch information in SBOM
  - Missing SBOM from supply chain
  - Linking Primary SBOM, and Medical device for better asset management
  - SBOM Verification - Is SBOM complete?

Steps in SBOM POC

3 Distribution/Sharing SBOM

- BOX folder with Excel registry for now
- Future thoughts…
  - Host in common public domain
  - Authenticated common domain
  - Manufacture specific domain
  - Provided by Medical Device, when applicable

? Guidance/playbook document in progress