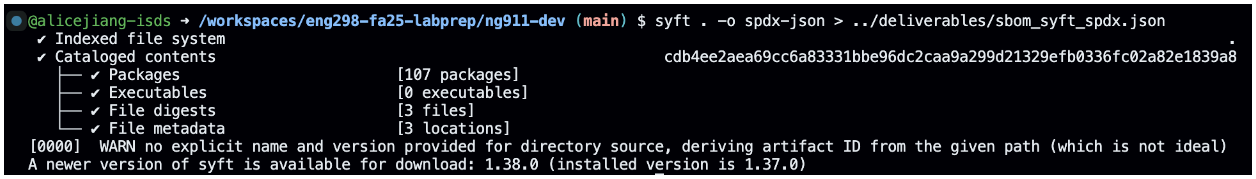
Alice Jiang
Foundational Technical & Organizational Concepts & Practices in Cybersecurity 298
Professor O'Brien
12/08/25

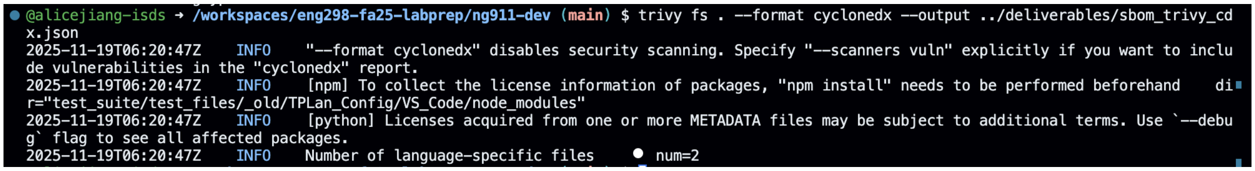
Module 7: Assignment: Secure Software Supply Chain with SBOMs

1. How many components each tool reported (Syft vs. Trivy)
    a. For Syft, it has 107 packages, making it 107 components



```
● @alicejiang-isds → /workspaces/eng298-fa25-labprep/ng911-dev (main) $ syft . -o spdx-json > ../deliverables/sbom_syft_spdx.json
  ✔ Indexed file system                                                                                        .
  ✔ Cataloged contents                                                cdb4ee2aea69cc6a83331bbe96dc2caa9a299d21329efb0336fc02a82e1839a8
     ├── ✔ Packages                        [107 packages]
     ├── ✔ Executables                     [0 executables]
     ├── ✔ File digests                    [3 files]
     └── ✔ File metadata                   [3 locations]
 [0000]  WARN no explicit name and version provided for directory source, deriving artifact ID from the given path (which is not ideal)
 A newer version of syft is available for download: 1.38.0 (installed version is 1.37.0)
```

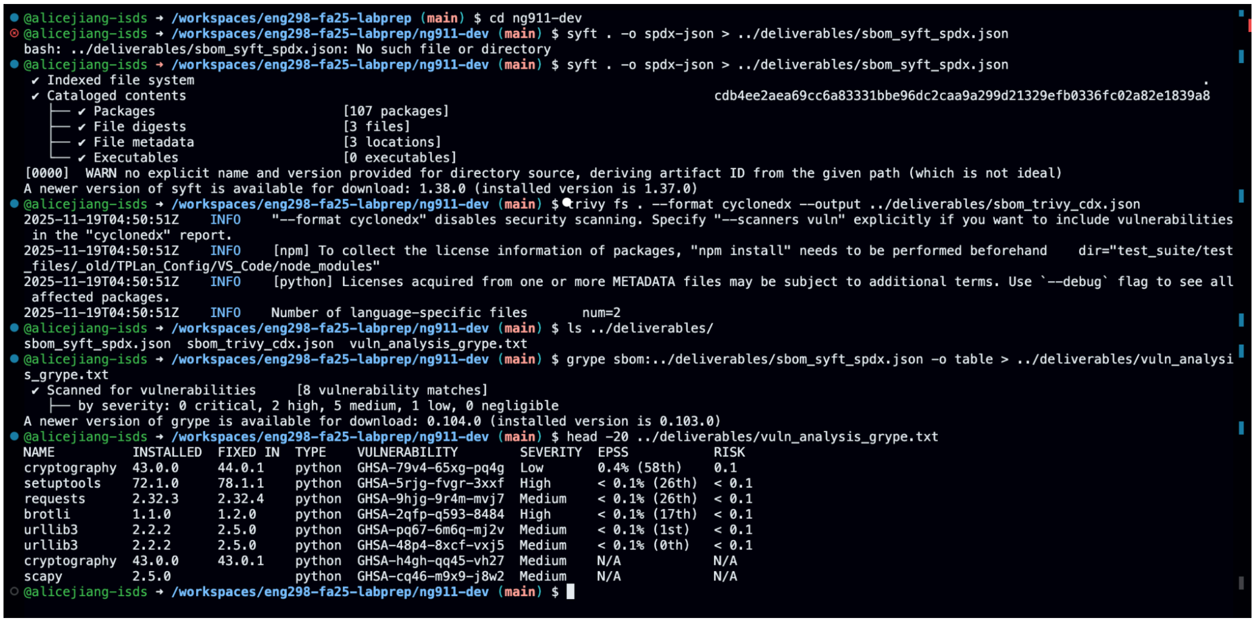
    b. For Trivy, there's 2 language-specific files, making it 2 components



```
● @alicejiang-isds → /workspaces/eng298-fa25-labprep/ng911-dev (main) $ trivy fs . --format cyclonedx --output ../deliverables/sbom_trivy_cd
  x.json
  2025-11-19T06:20:47Z    INFO    "--format cyclonedx" disables security scanning. Specify "--scanners vuln" explicitly if you want to inclu
  de vulnerabilities in the "cyclonedx" report.
  2025-11-19T06:20:47Z    INFO    [npm] To collect the license information of packages, "npm install" needs to be performed beforehand    di
  r="test_suite/test_files/_old/TPLan_Config/VS_Code/node_modules"
  2025-11-19T06:20:47Z    INFO    [python] Licenses acquired from one or more METADATA files may be subject to additional terms. Use `--debu
  g` flag to see all affected packages.
  2025-11-19T06:20:47Z    INFO    Number of language-specific files    ● num=2
```

2. One difference you notice between the SPDX SBOM and the CycloneDX SBOM (format, fields, component count, etc.)
    a. One difference I notice between SPDX SBOM and the CycloneDX SBOM is that the SPDX SBOM is more organized in the format, it tells you the number of packages, file digests, file metadata, and executables there are, and the count is shown on the right side. While for CycloneDX SBOM, it's more compact in the format, there's no table-like field, instead it's separated into lines, but it shows the count, just within a line.

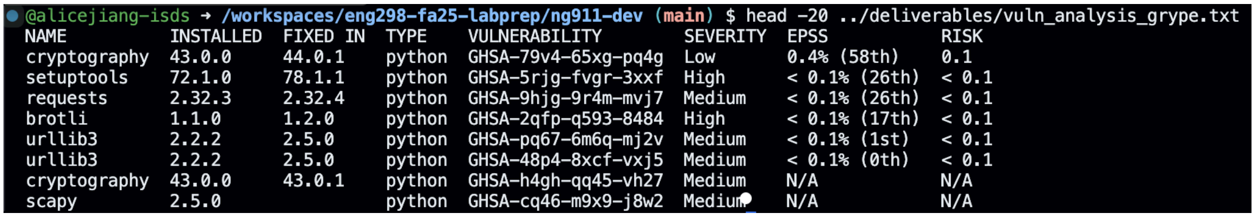
Here is the screenshot of the whole code for the labs:



```
● @alicejiang-isds → /workspaces/eng298-fa25-labprep (main) $ cd ng911-dev
⊗ @alicejiang-isds → /workspaces/eng298-fa25-labprep/ng911-dev (main) $ syft . -o spdx-json > ../deliverables/sbom_syft_spdx.json
  bash: ../deliverables/sbom_syft_spdx.json: No such file or directory
● @alicejiang-isds → /workspaces/eng298-fa25-labprep/ng911-dev (main) $ syft . -o spdx-json > ../deliverables/sbom_syft_spdx.json
   ✔ Indexed file system                                                                                     .
   ✔ Cataloged contents                                                    cdb4ee2aea69cc6a83331bbe96dc2caa9a299d21329efb0336fc02a82e1839a8
      ├── ✔ Packages                        [107 packages]
      ├── ✔ File digests                    [3 files]
      ├── ✔ File metadata                   [3 locations]
      └── ✔ Executables                     [0 executables]
  [0000]  WARN no explicit name and version provided for directory source, deriving artifact ID from the given path (which is not ideal)
  A newer version of syft is available for download: 1.38.0 (installed version is 1.37.0)
● @alicejiang-isds → /workspaces/eng298-fa25-labprep/ng911-dev (main) $ trivy fs . --format cyclonedx --output ../deliverables/sbom_trivy_cdx.json
  2025-11-19T04:50:51Z    INFO    "--format cyclonedx" disables security scanning. Specify "--scanners vuln" explicitly if you want to include vulnerabilities
   in the "cyclonedx" report.
  2025-11-19T04:50:51Z    INFO    [npm] To collect the license information of packages, "npm install" needs to be performed beforehand    dir="test_suite/test
  _files/_old/TPLan_Config/VS_Code/node_modules"
  2025-11-19T04:50:51Z    INFO    [python] Licenses acquired from one or more METADATA files may be subject to additional terms. Use `--debug` flag to see all
   affected packages.
  2025-11-19T04:50:51Z    INFO    Number of language-specific files       num=2
● @alicejiang-isds → /workspaces/eng298-fa25-labprep/ng911-dev (main) $ ls ../deliverables/
  sbom_syft_spdx.json  sbom_trivy_cdx.json  vuln_analysis_grype.txt
● @alicejiang-isds → /workspaces/eng298-fa25-labprep/ng911-dev (main) $ grype sbom:../deliverables/sbom_syft_spdx.json -o table > ../deliverables/vuln_analysi
  s_grype.txt
   ✔ Scanned for vulnerabilities     [8 vulnerability matches]
     ├── by severity: 0 critical, 2 high, 5 medium, 1 low, 0 negligible
  A newer version of grype is available for download: 0.104.0 (installed version is 0.103.0)
● @alicejiang-isds → /workspaces/eng298-fa25-labprep/ng911-dev (main) $ head -20 ../deliverables/vuln_analysis_grype.txt
  NAME          INSTALLED  FIXED IN  TYPE    VULNERABILITY        SEVERITY  EPSS           RISK
  cryptography  43.0.0     44.0.1    python  GHSA-79v4-65xg-pq4g  Low       0.4% (58th)    0.1
  setuptools    72.1.0     78.1.1    python  GHSA-5rjg-fvgr-3xxf  High      < 0.1% (26th)  < 0.1
  requests      2.32.3     2.32.4    python  GHSA-9hjg-9r4m-mvj7  Medium    < 0.1% (26th)  < 0.1
  brotli        1.1.0      1.2.0     python  GHSA-2qfp-q593-8484  High      < 0.1% (17th)  < 0.1
  urllib3       2.2.2      2.5.0     python  GHSA-pq67-6m6q-mj2v  Medium    < 0.1% (1st)   < 0.1
  urllib3       2.2.2      2.5.0     python  GHSA-48p4-8xcf-vxj5  Medium    < 0.1% (0th)   < 0.1
  cryptography  43.0.0     43.0.1    python  GHSA-h4gh-qq45-vh27  Medium    N/A            N/A
  scapy         2.5.0                python  GHSA-cq46-m9x9-j8w2  Medium    N/A            N/A
○ @alicejiang-isds → /workspaces/eng298-fa25-labprep/ng911-dev (main) $ 
```

(NOTE: my terminal got resetted due to my github codespace being inactive, so it doesn't show the `git clone https://github.com/tamu-edu/ng911-dev.git`)

3. Copy the top 5 rows into your report table. Then select one CVE, locate it in the NVD Database, and summarize its cause or impact in one sentence.



```
● @alicejiang-isds → /workspaces/eng298-fa25-labprep/ng911-dev (main) $ head -20 ../deliverables/vuln_analysis_grype.txt
  NAME          INSTALLED  FIXED IN  TYPE    VULNERABILITY        SEVERITY  EPSS           RISK
  cryptography  43.0.0     44.0.1    python  GHSA-79v4-65xg-pq4g  Low       0.4% (58th)    0.1
  setuptools    72.1.0     78.1.1    python  GHSA-5rjg-fvgr-3xxf  High      < 0.1% (26th)  < 0.1
  requests      2.32.3     2.32.4    python  GHSA-9hjg-9r4m-mvj7  Medium    < 0.1% (26th)  < 0.1
  brotli        1.1.0      1.2.0     python  GHSA-2qfp-q593-8484  High      < 0.1% (17th)  < 0.1
  urllib3       2.2.2      2.5.0     python  GHSA-pq67-6m6q-mj2v  Medium    < 0.1% (1st)   < 0.1
  urllib3       2.2.2      2.5.0     python  GHSA-48p4-8xcf-vxj5  Medium    < 0.1% (0th)   < 0.1
  cryptography  43.0.0     43.0.1    python  GHSA-h4gh-qq45-vh27  Medium    N/A            N/A
  scapy         2.5.0                python  GHSA-cq46-m9x9-j8w2  Medium    N/A            N/A
```

NAME	INSTALLED	FIXED IN	TYPE	VULNERABILITY	SEVERITY	EPSS	RISK
cryptography	43.0.0	44.0.1	python	GHSA-79v4-65xg-pq4g	Low	0.4% (58th)	0.1
setuptools	72.1.0	78.1.1	python	GHSA-5rjg-fvgr-3xxf	High	< 0.1% (26th)	< 0.1
requests	2.32.3	2.32.4	python	GHSA-9hjg-9r4m-mvj7	Medium	< 0.1% (26th)	< 0.1
brotli	1.1.0	1.2.0	python	GHSA-2qfp-q593-8484	High	< 0.1% (17th)	< 0.1
urllib3	2.2.2	2.5.0	python	GHSA-pq67-6m6q-mj2v	Medium	< 0.1% (1st)	< 0.1

NAME	INSTALLED	FIXED IN	TYPE	VULERNRABILITY	SEVERITY	EPSS	RISK
cryptography	43.0.0	44.0.1	python	GHSA-79v4-65xg-pq4g	Low	0.4% (58th)	0.1
setuptools	72.1.0	78.1.1	python	GHSA-5rjg-fvgr-3xxf	High	< 0.1% (26th)	< 0.1

requests	2.32.3	2.32.4	python	GHSA-9hjg-9r4m-mvj7	Medium	< 0.1% (26th)	< 0.1
brotli	1.1.0	1.2.0	python	GHSA-2qfp-q593-8484	High	< 0.1% (17th)	< 0.1
urlib3	2.2.2	2.5.0	python	GHSA-pq67-6m6q-mj2v	Medium	< 0.1% (1st)	< 0.1

I had to use this website to translate the GHSA IDs to CVE: https://github.com/advisories ↴

NAME	INSTALLED	FIXED IN	TYPE	CVE	SEVERITY	EPSS	RISK
cryptography	43.0.0	44.0.1	python	CVE-2024-12797	Low	0.4% (58th)	0.1
setuptools	72.1.0	78.1.1	python	CVE-2025-47273	High	< 0.1% (26th)	< 0.1
requests	2.32.3	2.32.4	python	CVE-2024-47081	Medium	< 0.1% (26th)	< 0.1
brotli	1.1.0	1.2.0	python	CVE-2025-6176	High	< 0.1% (17th)	< 0.1
urlib3	2.2.2	2.5.0	python	CVE-2025-c	Medium	< 0.1% (1st)	< 0.1

The CVE I chose is this: CVE-2025-47273
The impact of this specific CVE is that there was a path traversal vulnerability in PackageIndex of the package setuptools, where attackers can write files to arbitrary locations on the filesystem with permission on Python code, which means they can do remote code execution——luckily this got fixed in version 78.1.1.