

U.S. Patent No. 7,784,058 (“’058 Patent”)

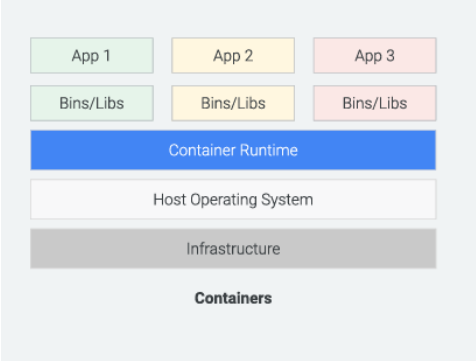
Formatted: Indent: Left: 1", First line: 0.5"

Accused Instrumentalities: Google products and services using secure containerized applications, including without limitation Google Kubernetes Engine, Cloud Run, and Migrate to Containers, and all versions and variations thereof since the issuance of the asserted patent.

Each Accused Instrumentality infringes the claims in substantially the same way, and the evidence shown in this chart is similarly applicable to each Accused Instrumentality. Each claim limitation is literally infringed by each Accused Instrumentality. However, to the extent any claim limitation is not met literally, it is nonetheless met under the doctrine of equivalents because the differences between the claim limitation and each Accused Instrumentality would be insubstantial, and each Accused Instrumentality performs substantially the same function, in substantially the same way, to achieve the same result as the claimed invention. Notably, Defendant has not yet articulated which, if any, particular claim limitations it believes are not met by the Accused Instrumentalities.

Claim 1

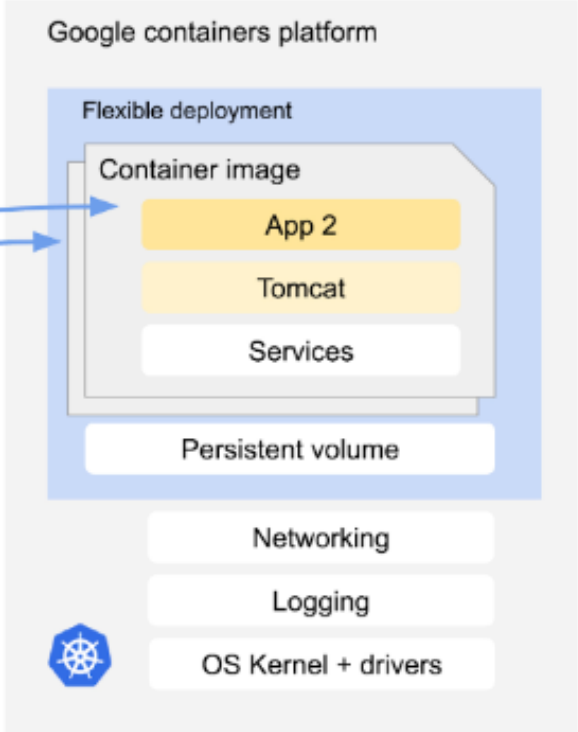
Claim 1	Accused Instrumentalities
<p>[1pre] 1. A computing system for executing a plurality of software applications comprising:</p>	<p>To the extent the preamble is limiting, each Accused Instrumentality comprises or constitutes a computing system for executing a plurality of software applications as claimed.</p> <p><i>See claim limitations below.</i></p> <p><i>See also, e.g.:</i></p> <p>Google Kubernetes Engine (GKE) clusters provide secured and managed Kubernetes services with autoscaling and multi-cluster support. GKE lets you deploy, manage, and scale containerized applications on Kubernetes, powered by Google Cloud.</p> <p>https://cloud.google.com/migrate/containers/docs/getting-started</p> <p>Use Migrate to Containers to modernize traditional applications away from virtual machine (VM) instances and into native containers that run on Google Kubernetes Engine (GKE), GKE Enterprise clusters, or Cloud Run platform. You can migrate workloads from VMs that run on VMware or Compute Engine, giving you the flexibility to containerize your existing workloads with ease. Migrate to Containers supports modernization of IBM WebSphere, JBoss, Apache, Tomcat, WordPress, Windows IIS applications, as well as containerisation of Linux-based applications.</p> <p>https://cloud.google.com/migrate/containers/docs/getting-started.</p>

Claim 1	Accused Instrumentalities
	<p data-bbox="541 386 1482 526">A container is a way of packaging a given application's code and dependencies so that the application will run easily in any computing environment. This solves the common problem of</p>  <p data-bbox="506 548 978 906">The diagram illustrates the container architecture stack. At the top, three application boxes labeled 'App 1' (green), 'App 2' (yellow), and 'App 3' (pink) are shown. Below each app is a corresponding 'Bins/Libs' box in the same color. These three pairs are stacked on top of a blue 'Container Runtime' box. Below the runtime is a light gray 'Host Operating System' box, and at the bottom is a dark gray 'Infrastructure' box. The entire stack is labeled 'Containers' at the bottom.</p> <p data-bbox="506 927 1293 954">https://services.google.com/fh/files/misc/why_container_security_matters.pdf</p>

Claim 1	Accused Instrumentalities
	<p>Containers can run virtually anywhere, greatly easing development and deployment: on Linux, Windows, and Mac operating systems; on virtual machines or on physical servers; on a developer's machine or in data centers on-premises; and of course, in the public cloud.</p> <p>Containers are lightweight packages of your application code together with dependencies such as specific versions of programming language runtimes and libraries required to run your software services.</p> <p>https://cloud.google.com/learn/what-are-containers</p>
[1a] a) a processor;	<p>Each Accused Instrumentality comprises a processor.</p> <p>For example, each node/host contains at least one CPU.</p> <p><i>See, e.g.:</i></p>

Claim 1	Accused Instrumentalities
	<p data-bbox="520 367 1094 659">Containers virtualize CPU, memory, storage, and network resources at the operating system level, providing developers with a view of the OS logically isolated from other applications.</p> <p data-bbox="504 708 1020 732">https://cloud.google.com/learn/what-are-containers</p> <ul data-bbox="533 764 1495 954" style="list-style-type: none"> • Higher utilization and density, leveraging automatic bin-packing and auto-scaling capabilities, Kubernetes places containers optimally in nodes based on required resources while scaling as needed, without impairing availability. In addition, unlike VMs, all containers on a single node share one copy of the operating system and don't each require their own OS image and vCPU, resulting in a much smaller memory footprint and CPU needs. This means more workloads running on fewer compute resources. <p data-bbox="504 967 1491 1019">https://cloud.google.com/blog/products/containers-kubernetes/how-migrate-for-anthos-improves-vm-to-container-migration</p> <p data-bbox="520 1057 1507 1198">Containers use specific features of the Linux kernel that "trick" individual applications into thinking they're in their own unique environment, even though multiple applications share the same host kernel. (If you're not familiar with the Linux kernel, it's a part of the operating system that communicates between processes--requests that do user tasks like opening a file, running a program-- and the hardware. It manages resources like memory and CPU to meet these requests).</p> <p data-bbox="504 1214 1293 1239">https://services.google.com/fh/files/misc/why_container_security_matters.pdf</p>

Claim 1	Accused Instrumentalities
<p>[1b] b) an operating system having an operating system kernel having OS critical system elements (OSCSEs) for running in kernel mode using said processor; and,</p>	<p>Each Accused Instrumentality comprises an operating system having an operating system kernel having OS critical system elements (OSCSEs) for running in kernel mode using said processor.</p> <p>For example, the OSCSEs include kernel-mode functions similar to the functionalities provided by user-space libraries such as glibc. These are implemented in kernel-space to handle tasks such as (without limitation) memory management (kmalloc(), kfree(), etc.) at kernel level.</p> <p><i>See, e.g.:</i></p> <ul style="list-style-type: none"> • Containers are much more lightweight than VMs • Containers virtualize at the OS level while VMs virtualize at the hardware level • Containers share the OS kernel and use a fraction of the memory VMs require <p>https://cloud.google.com/learn/what-are-containers</p> <p>Kernel mode</p> <p>Kernel mode refers to the processor mode that enables software to have full and unrestricted access to the system and its resources. The OS kernel and kernel drivers, such as the file system driver, are loaded into protected memory space and operate in this highly privileged kernel mode.</p> <p>https://www.techtarget.com/searchdatacenter/definition/kernel</p>

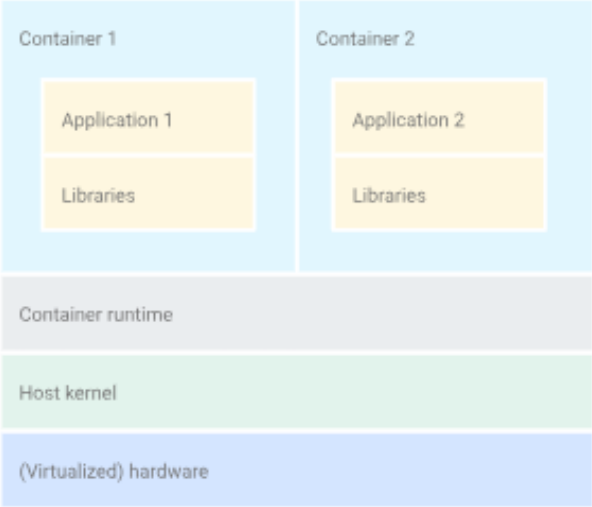
Claim 1	Accused Instrumentalities
	 <p>The diagram illustrates the Google containers platform architecture. It is structured as follows:</p> <ul style="list-style-type: none"> Google containers platform (outermost layer) Flexible deployment (blue box containing): <ul style="list-style-type: none"> Container image (grey box containing): <ul style="list-style-type: none"> App 2 (yellow box) Tomcat (yellow box) Services (white box) Persistent volume (white box) Networking (white box) Logging (white box) OS Kernel + drivers (white box, with a Docker logo icon to its left) <p>Two blue arrows point from the left towards the 'Container image' box, indicating input or interaction.</p> <p>https://cloud.google.com/blog/products/application-modernization/shift-your-apps-to-container-based-workloads-on-the-command-line</p>

Claim 1	Accused Instrumentalities
	<p>The migration prerequisites are dependent on your specific migration environment. Confirm that your workloads' OS and source platform are compatible for migration by reviewing the prerequisites for your specific migration environment:</p> <p>https://cloud.google.com/migrate/containers/docs/setting-up-overview</p> <p>Containers use specific features of the Linux kernel that “trick” individual applications into thinking they’re in their own unique environment, even though multiple applications share the same host kernel. (If you’re not familiar with the Linux kernel, it’s a part of the operating system that communicates between processes--requests that do user tasks like opening a file, running a program-- and the hardware. It manages resources like memory and CPU to meet these requests).</p> <p>https://services.google.com/fh/files/misc/why_container_security_matters.pdf</p> <p>The GNU C Library, commonly known as glibc, is the GNU Project implementation of the C standard library. It is a wrapper around the system calls of the Linux kernel for application use. Despite its name, it now also directly supports C++ (and, indirectly, other programming languages). It was started in the 1980s by the Free Software Foundation (FSF) for the GNU operating system.</p> <p>https://en.wikipedia.org/wiki/Glibc</p>
<p>[1c] c) a shared library having shared library critical system elements (SLCSEs) stored therein for use by the plurality of software applications in user mode and</p>	<p>Each Accused Instrumentality comprises a shared library having shared library critical system elements (SLCSEs) stored therein for use by the plurality of software applications in user mode.</p> <p>For example, the shared library with SLCSEs include the runtime environment, system tools, and dependencies, such as the glibc library and other libraries that replicate OSCSEs, included in the container image (including without limitation in a base image that is included within the container image).</p> <p><i>See, e.g.:</i></p>

Claim 1	Accused Instrumentalities
	<p data-bbox="522 367 978 711">A “container image” is your application and its dependencies, and uses a “base image” as the basis for the container image</p> <p data-bbox="522 769 1486 1094">The container image specifies the container’s file system. For example, if you’re running a Node.js application, the container image would contain your app, Node.js, and other dependencies like Linux system libraries (except the kernel). A container image usually extends a base operating system image, or base image. This base image is the basis of your container, so you’ll want to ensure that it’s properly patched and free from known vulnerabilities.</p> <p data-bbox="504 1133 1293 1159">https://services.google.com/fh/files/misc/why_container_security_matters.pdf</p>

Claim 1	Accused Instrumentalities
	<p>A base image is the starting point for most container-based development workflows. Developers start with a base image and layer on top of it the necessary libraries, binaries, and configuration files used to run their application.</p> <p>Many base images are basic or minimal Linux distributions: Debian, Ubuntu, Red Hat Enterprise Linux (RHEL), Rocky Linux, or Alpine. Developers can consume these images directly from Docker Hub or other sources. There are official providers along with a wide variety of other downstream repackagers that layer software to meet customer needs.</p> <p>Google maintains base images for building its own applications. These images are built from the same source that Docker Hub uses. Therefore, they match the images you would get from Docker Hub.</p> <p>https://cloud.google.com/software-supply-chain-security/docs/base-images</p> <p>The preconfigured base images provided by Cloud Workstations contain only a minimal environment with IDE, basic Linux terminal and language tools and a <code>sshd</code> server. To expedite the environment setup of specific development use cases, you can create custom container images that extend these base images to pre-install tools and dependencies and that run automation scripts.</p> <p>For custom container images, we recommend setting up a pipeline to automatically rebuild these images when the Cloud Workstations base image is updated, in addition to running a container scanning tool such as Artifact Analysis to inspect any additional dependencies you added. You're responsible for maintaining and updating custom packages and dependencies added to custom images.</p> <p>https://cloud.google.com/workstations/docs/customize-container-images</p>

Claim 1	Accused Instrumentalities
	<p>A container is a way of packaging a given application's code and dependencies so that the application will run easily in any computing environment. This solves the common problem of</p> <p>Containers solve the portability problem by isolating the application and its dependencies so they can be moved seamlessly between machines. A process running in a container lives isolated from the underlying environment. You control what it can see and what resources it can access. This helps you use resources more efficiently and not worry about the underlying infrastructure.</p> <p>One of the primary reasons to adopt containers is for your applications to be decoupled from the underlying environment and support higher resource utilization by "bin packing" multiple workloads onto each server. As such, the architecture of containers means that they're deployed with multiple containers sharing the same kernel.</p> <p>The core components of the Linux kernel that are used for containers are cgroups – control groups, which define the resources like CPU and memory which are available to a given process – and namespaces, which are a way of separating processes by restricting what each process can see, so that system resources "appear" isolated to the process.</p> <p>https://services.google.com/fh/files/misc/why_container_security_matters.pdf</p>

Claim 1	Accused Instrumentalities
	 <p>The diagram illustrates a container architecture stack. At the top, two containers are shown side-by-side: 'Container 1' and 'Container 2'. Each container contains an 'Application' (Application 1 and Application 2 respectively) and 'Libraries'. Below the containers is a 'Container runtime' layer, followed by the 'Host kernel', and finally '(Virtualized) hardware' at the base.</p> <p>https://cloud.google.com/architecture/best-practices-for-operating-containers</p> <p>For example, Migrate to Containers automatically generates a container image, a Dockerfile for day-2 image updates and application revisions, Kubernetes deployment YAMLs and (where relevant) a persistent data volume onto which the application data files and persistent state are copied. This automated, intelligent extraction is https://cloud.google.com/blog/products/containers-kubernetes/how-migrate-for-anthos-improves-vm-to-container-migration</p>

Claim 1	Accused Instrumentalities
	<p>Containers are lightweight packages of your application code together with dependencies such as specific versions of programming language runtimes and libraries required to run your software services.</p> <p>https://cloud.google.com/learn/what-are-containers</p> <h2>About storage drivers</h2> <p>To use storage drivers effectively, it's important to know how Docker builds and stores images, and how these images are used by containers. You can use this information to make informed choices about the best way to persist data from your applications and avoid performance problems along the way.</p> <h2>Storage drivers versus Docker volumes</h2> <p>Docker uses storage drivers to store image layers, and to store data in the writable layer of a container. The container's writable layer doesn't persist after the container is deleted, but is suitable for storing ephemeral data that is generated at runtime. Storage drivers are optimized for space efficiency, but (depending on the storage driver) write speeds are lower than native file system performance, especially for storage drivers that use a copy-on-write filesystem. Write-intensive applications, such as database storage, are impacted by a performance overhead, particularly if pre-existing data exists in the read-only layer.</p> <p>Use Docker volumes for write-intensive data, data that must persist beyond the container's lifespan, and data that must be shared between containers. Refer to the volumes section to learn how to use volumes to persist data and improve performance.</p> <p>https://docs.docker.com/storage/storagedriver/</p>

Claim 1**Accused Instrumentalities**

Images and layers

A Docker image is built up from a series of layers. Each layer represents an instruction in the image's Dockerfile. Each layer except the very last one is read-only. Consider the following Dockerfile:

```
# syntax=docker/dockerfile:1

FROM ubuntu:22.04
LABEL org.opencontainers.image.authors="org@example.com"
COPY . /app
RUN make /app
RUN rm -r $HOME/.cache
CMD python /app/app.py
```

This Dockerfile contains four commands. Commands that modify the filesystem create a layer. The `FROM` statement starts out by creating a layer from the `ubuntu:22.04` image. The `LABEL` command only modifies the image's metadata, and doesn't produce a new layer. The `COPY` command adds some files from your Docker client's current directory. The first `RUN` command builds your application using the `make` command, and writes the result to a new layer. The second `RUN` command removes a cache directory, and writes the result to a new layer. Finally, the `CMD` instruction specifies what command to run within the container, which only modifies the image's metadata, which doesn't produce an image layer.

<https://docs.docker.com/storage/storagedriver/>

Claim 1	Accused Instrumentalities
	<p>Each layer is only a set of differences from the layer before it. Note that both <i>adding</i>, and <i>removing</i> files will result in a new layer. In the example above, the <code>\$HOME/.cache</code> directory is removed, but will still be available in the previous layer and add up to the image's total size. Refer to the Best practices for writing Dockerfiles and use multi-stage builds sections to learn how to optimize your Dockerfiles for efficient images.</p> <p>The layers are stacked on top of each other. When you create a new container, you add a new writable layer on top of the underlying layers. This layer is often called the "container layer". All changes made to the running container, such as writing new files, modifying existing files, and deleting files, are written to this thin writable container layer. The diagram below shows a container based on an <code>ubuntu:15.04</code> image.</p> <div data-bbox="726 756 1325 1235" data-label="Diagram"> <p>The diagram illustrates the layer structure of a Docker container. At the top is a dashed box labeled "Thin R/W layer" with an arrow pointing to it from the label "Container layer". Below this are four solid blue boxes representing "Image Layers (R/O)", each with a unique ID and size: <ul style="list-style-type: none"> 91e54dfb1179 (0 B) d74508fb6632 (1.895 KB) c22013c84729 (194.5 KB) d3a1f33e8a5a (188.1 MB) A padlock icon is positioned to the right of these layers, indicating they are read-only. The entire stack is labeled "ubuntu:15.04" and "Container (based on ubuntu:15.04 image)". </p> </div> <p>https://docs.docker.com/storage/storagedriver/</p>

Claim 1	Accused Instrumentalities
	<h2 data-bbox="520 370 730 423">Volumes</h2> <p data-bbox="520 467 1514 570">Volumes are the preferred mechanism for persisting data generated by and used by Docker containers. While bind mounts are dependent on the directory structure and OS of the host machine, volumes are completely managed by Docker. Volumes have several advantages over bind mounts:</p> <p data-bbox="504 586 1041 613">https://kubernetes.io/docs/concepts/storage/volumes/</p> <h2 data-bbox="520 651 974 695">Container environment</h2> <p data-bbox="520 721 1171 776">The Kubernetes Container environment provides several important resources to Containers:</p> <ul data-bbox="554 802 1150 932" style="list-style-type: none">• A filesystem, which is a combination of an image and one or more volumes.• Information about the Container itself.• Information about other objects in the cluster. <p data-bbox="504 959 1213 987">https://kubernetes.io/docs/concepts/containers/container-environment/</p>

Claim 1	Accused Instrumentalities
	<h2 data-bbox="520 367 699 415">Images</h2> <p data-bbox="520 443 1209 565">A container image represents binary data that encapsulates an application and all its software dependencies. Container images are executable software bundles that can run standalone and that make very well defined assumptions about their runtime environment.</p> <p data-bbox="520 592 1215 651">You typically create a container image of your application and push it to a registry before referring to it in a <code>Pod</code>.</p> <p data-bbox="504 670 1058 698">https://kubernetes.io/docs/concepts/containers/images/</p> <h2 data-bbox="520 732 730 781">Volumes</h2> <p data-bbox="520 808 1178 899">On-disk files in a container are ephemeral, which presents some problems for non-trivial applications when running in containers. One problem occurs when a container crashes or is stopped.</p> <p data-bbox="520 907 1215 1162">Container state is not saved so all of the files that were created or modified during the lifetime of the container are lost. During a crash, kubelet restarts the container with a clean state. Another problem occurs when multiple containers are running in a <code>Pod</code> and need to share files. It can be challenging to setup and access a shared filesystem across all of the containers. The Kubernetes <code>volume</code> abstraction solves both of these problems. Familiarity with <code>Pods</code> is suggested.</p> <p data-bbox="504 1182 1041 1209">https://kubernetes.io/docs/concepts/storage/volumes/</p>

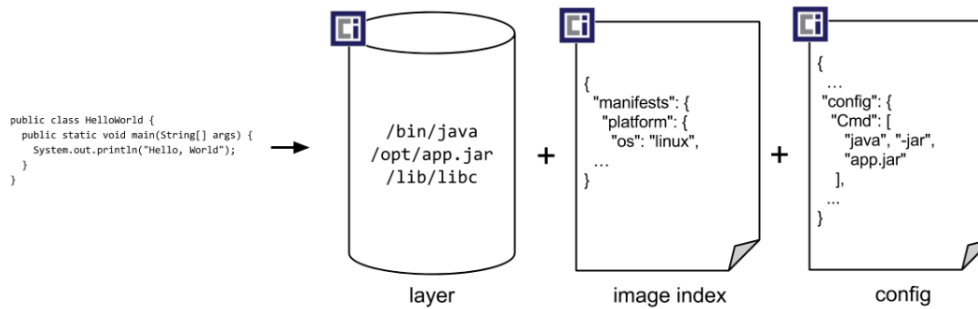
Claim 1	Accused Instrumentalities
	<p data-bbox="533 370 1031 415">Open Container Initiative</p> <hr/> <p data-bbox="533 467 940 503">Image Format Specification</p> <hr/> <p data-bbox="533 540 1503 602">This specification defines an OCI Image, consisting of an image manifest, an image index (optional), a set of filesystem layers, and a configuration.</p> <p data-bbox="533 630 1509 686">The goal of this specification is to enable the creation of interoperable tools for building, transporting, and preparing a container image to run.</p> <p data-bbox="501 711 1178 764">https://github.com/opencontainers/image-spec/blob/a6af2b480dfc001ba975f44de53001c873cb0ef/spec.md</p>

Claim 1

Accused Instrumentalities

Overview

At a high level the image manifest contains metadata about the contents and dependencies of the image including the content-addressable identity of one or more [filesystem layer changeset](#) archives that will be unpacked to make up the final runnable filesystem. The image configuration includes information such as application arguments, environments, etc. The image index is a higher-level manifest which points to a list of manifests and descriptors. Typically, these manifests may provide different implementations of the image, possibly varying by platform or other attributes.

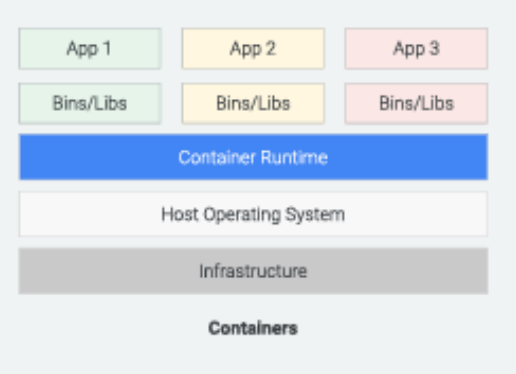


<https://github.com/opencontainers/image-spec/blob/a6af2b480dcfc001ba975f44de53001c873cb0ef/spec.md>


Claim 1	Accused Instrumentalities
	<h2 data-bbox="520 363 1031 407">OCI Image Configuration</h2> <p data-bbox="520 451 1524 581">An OCI <i>Image</i> is an ordered collection of root filesystem changes and the corresponding execution parameters for use within a container runtime. This specification outlines the JSON format describing images for use with a container runtime and execution tool and its relationship to filesystem changesets, described in Layers.</p> <p data-bbox="520 610 1318 638">This section defines the <code>application/vnd.oci.image.config.v1+json</code> media type.</p> <p data-bbox="504 662 1199 719">https://github.com/opencontainers/image-spec/blob/a6af2b480dcf001ba975f44de53001c873cb0ef/config.md</p>


Claim 1	Accused Instrumentalities
	<p>Layer</p> <ul style="list-style-type: none"> • Image filesystems are composed of <i>layers</i>. • Each layer represents a set of filesystem changes in a tar-based layer format, recording files to be added, changed, or deleted relative to its parent layer. • Layers do not have configuration metadata such as environment variables or default arguments - these are properties of the image as a whole rather than any particular layer. • Using a layer-based or union filesystem such as AUFS, or by computing the diff from filesystem snapshots, the filesystem changeset can be used to present a series of image layers as if they were one cohesive filesystem. <p>Image JSON</p> <ul style="list-style-type: none"> • Each image has an associated JSON structure which describes some basic information about the image such as date created, author, as well as execution/runtime configuration like its entrypoint, default arguments, networking, and volumes. • The JSON structure also references a cryptographic hash of each layer used by the image, and provides history information for those layers. • This JSON is considered to be immutable, because changing it would change the computed ImageID. • Changing it means creating a new derived image, instead of changing the existing image. <p>https://github.com/opencontainers/image-spec/blob/a6af2b480dcfc001ba975f44de53001c873cb0ef/config.md</p>
[1d] i) wherein some of the SLCSEs stored in the shared library are functional replicas of OSCSEs and are accessible	In each Accused Instrumentality, some of the SLCSEs stored in the shared library are functional replicas of OSCSEs and are accessible to some of the plurality of software applications and when

Claim 1	Accused Instrumentalities
<p>to some of the plurality of software applications and when one of the SLCSEs is accessed by one or more of the plurality of software applications it forms a part of the one or more of the plurality of software applications,</p>	<p>one of the SLCSEs is accessed by one or more of the plurality of software applications it forms a part of the one or more of the plurality of software applications.</p> <p>For example, a base image serves as a self-contained unit that encompasses all the necessary components for an application to run, including the application code, runtime environment, system tools, and dependencies (i.e., SLCSEs). The images are based on existing Linux distributions, such as Debian and Ubuntu, including essential system elements (i.e., functional replicas of OSCSEs). Each container image is based on a specific base image, which contains the application code, and dependencies, including system libraries or shared library critical system elements (SLCSEs). The base image forms a part of the container image according to the “layer” model described in the documentation below. When the container runs the image, it creates a runtime instance of that container image. In turn, when one or more applications executes within the container runtime environment, it dynamically links to the SLCSEs stored in the runtime environment, which thereby become a part of the application(s).</p> <p><i>See, e.g.:</i></p> <p>Many base images are basic or minimal Linux distributions: Debian, Ubuntu, Red Hat Enterprise Linux (RHEL), Rocky Linux, or Alpine. Developers can consume these images directly from Docker Hub or other sources. There are official providers along with a wide variety of other downstream repackagers that layer software to meet customer needs.</p> <p>https://cloud.google.com/software-supply-chain-security/docs/base-images</p> <p>A container is a way of packaging a given application’s code and dependencies so that the application will run easily in any computing environment. This solves the common problem of</p>

Claim 1	Accused Instrumentalities
	<p data-bbox="512 358 806 581">A “container image” is your application and its dependencies, and uses a “base image” as the basis for the container image</p>  <p>The diagram illustrates the layers of container architecture. At the top, three application boxes labeled 'App 1' (green), 'App 2' (yellow), and 'App 3' (pink) are shown. Below each app is a corresponding 'Bins/Libs' box in the same color. These three pairs sit on a blue 'Container Runtime' bar. This bar sits on a white 'Host Operating System' bar, which in turn sits on a grey 'Infrastructure' bar. The entire stack is labeled 'Containers' at the bottom.</p>

Claim 1	Accused Instrumentalities																								
	<p>The container image specifies the container's file system. For example, if you're running a Node.js application, the container image would contain your app, Node.js, and other dependencies like Linux system libraries (except the kernel). A container image usually extends a base operating system image, or base image. This base image is the basis of your container, so you'll want to ensure that it's properly patched and free from known vulnerabilities.</p> <p>https://services.google.com/fh/files/misc/why_container_security_matters.pdf</p> <table border="1" data-bbox="514 665 1514 1027"> <thead> <tr> <th data-bbox="514 665 724 722">OS</th> <th data-bbox="724 665 1207 722">Repository path</th> <th data-bbox="1207 665 1514 722">Google Cloud Marketplace listing</th> </tr> </thead> <tbody> <tr> <td data-bbox="514 722 724 763">Debian 10 "Buster"</td> <td data-bbox="724 722 1207 763">marketplace.gcr.io/google/debian10</td> <td data-bbox="1207 722 1514 763">Google Cloud Marketplace</td> </tr> <tr> <td data-bbox="514 763 724 803">Debian 11 "Bullseye"</td> <td data-bbox="724 763 1207 803">marketplace.gcr.io/google/debian11</td> <td data-bbox="1207 763 1514 803">Google Cloud Marketplace</td> </tr> <tr> <td data-bbox="514 803 724 844">Debian 12 "Bookworm"</td> <td data-bbox="724 803 1207 844">marketplace.gcr.io/google/debian12</td> <td data-bbox="1207 803 1514 844">Google Cloud Marketplace</td> </tr> <tr> <td data-bbox="514 844 724 885">Rocky Linux 8</td> <td data-bbox="724 844 1207 885">marketplace.gcr.io/google/rockylinux8</td> <td data-bbox="1207 844 1514 885">Google Cloud Marketplace</td> </tr> <tr> <td data-bbox="514 885 724 925">Rocky Linux 9</td> <td data-bbox="724 885 1207 925">marketplace.gcr.io/google/rockylinux9</td> <td data-bbox="1207 885 1514 925">Google Cloud Marketplace</td> </tr> <tr> <td data-bbox="514 925 724 966">Ubuntu 20.04</td> <td data-bbox="724 925 1207 966">marketplace.gcr.io/google/ubuntu2004</td> <td data-bbox="1207 925 1514 966">Google Cloud Marketplace</td> </tr> <tr> <td data-bbox="514 966 724 1027">Ubuntu 22.04</td> <td data-bbox="724 966 1207 1027">marketplace.gcr.io/google/ubuntu2204</td> <td data-bbox="1207 966 1514 1027">Google Cloud Marketplace</td> </tr> </tbody> </table> <p>https://cloud.google.com/software-supply-chain-security/docs/base-images</p>	OS	Repository path	Google Cloud Marketplace listing	Debian 10 "Buster"	marketplace.gcr.io/google/debian10	Google Cloud Marketplace	Debian 11 "Bullseye"	marketplace.gcr.io/google/debian11	Google Cloud Marketplace	Debian 12 "Bookworm"	marketplace.gcr.io/google/debian12	Google Cloud Marketplace	Rocky Linux 8	marketplace.gcr.io/google/rockylinux8	Google Cloud Marketplace	Rocky Linux 9	marketplace.gcr.io/google/rockylinux9	Google Cloud Marketplace	Ubuntu 20.04	marketplace.gcr.io/google/ubuntu2004	Google Cloud Marketplace	Ubuntu 22.04	marketplace.gcr.io/google/ubuntu2204	Google Cloud Marketplace
OS	Repository path	Google Cloud Marketplace listing																							
Debian 10 "Buster"	marketplace.gcr.io/google/debian10	Google Cloud Marketplace																							
Debian 11 "Bullseye"	marketplace.gcr.io/google/debian11	Google Cloud Marketplace																							
Debian 12 "Bookworm"	marketplace.gcr.io/google/debian12	Google Cloud Marketplace																							
Rocky Linux 8	marketplace.gcr.io/google/rockylinux8	Google Cloud Marketplace																							
Rocky Linux 9	marketplace.gcr.io/google/rockylinux9	Google Cloud Marketplace																							
Ubuntu 20.04	marketplace.gcr.io/google/ubuntu2004	Google Cloud Marketplace																							
Ubuntu 22.04	marketplace.gcr.io/google/ubuntu2204	Google Cloud Marketplace																							

Claim 1	Accused Instrumentalities
	 <p data-bbox="548 469 812 503">Debian 10 "Buster"</p> <p data-bbox="548 516 961 550">Google Click to Deploy containers</p> <p data-bbox="548 583 747 617">Open source OS</p>

Claim 1	Accused Instrumentalities
	<div data-bbox="541 386 611 451"></div> <p data-bbox="541 467 957 548">Ubuntu 20.04 Google Click to Deploy containers</p> <p data-bbox="499 854 1360 883">https://console.cloud.google.com/marketplace/browse?filter=solution-type:container</p>

Claim 1	Accused Instrumentalities
	<h2 data-bbox="512 363 1012 415">About storage drivers</h2> <p data-bbox="512 454 1486 552">To use storage drivers effectively, it's important to know how Docker builds and stores images, and how these images are used by containers. You can use this information to make informed choices about the best way to persist data from your applications and avoid performance problems along the way.</p> <h2 data-bbox="512 607 1243 652">Storage drivers versus Docker volumes</h2> <p data-bbox="512 682 1520 893">Docker uses storage drivers to store image layers, and to store data in the writable layer of a container. The container's writable layer doesn't persist after the container is deleted, but is suitable for storing ephemeral data that is generated at runtime. Storage drivers are optimized for space efficiency, but (depending on the storage driver) write speeds are lower than native file system performance, especially for storage drivers that use a copy-on-write filesystem. Write-intensive applications, such as database storage, are impacted by a performance overhead, particularly if pre-existing data exists in the read-only layer.</p> <p data-bbox="512 935 1512 1032">Use Docker volumes for write-intensive data, data that must persist beyond the container's lifespan, and data that must be shared between containers. Refer to the volumes section to learn how to use volumes to persist data and improve performance.</p> <p data-bbox="512 1055 974 1081">https://docs.docker.com/storage/storagedriver/</p>

Claim 1**Accused Instrumentalities**

Images and layers

A Docker image is built up from a series of layers. Each layer represents an instruction in the image's Dockerfile. Each layer except the very last one is read-only. Consider the following Dockerfile:

```
# syntax=docker/dockerfile:1

FROM ubuntu:22.04
LABEL org.opencontainers.image.authors="org@example.com"
COPY . /app
RUN make /app
RUN rm -r $HOME/.cache
CMD python /app/app.py
```

This Dockerfile contains four commands. Commands that modify the filesystem create a layer. The `FROM` statement starts out by creating a layer from the `ubuntu:22.04` image. The `LABEL` command only modifies the image's metadata, and doesn't produce a new layer. The `COPY` command adds some files from your Docker client's current directory. The first `RUN` command builds your application using the `make` command, and writes the result to a new layer. The second `RUN` command removes a cache directory, and writes the result to a new layer. Finally, the `CMD` instruction specifies what command to run within the container, which only modifies the image's metadata, which doesn't produce an image layer.

<https://docs.docker.com/storage/storagedriver/>

Claim 1	Accused Instrumentalities
	<p>Each layer is only a set of differences from the layer before it. Note that both <i>adding</i>, and <i>removing</i> files will result in a new layer. In the example above, the <code>\$HOME/.cache</code> directory is removed, but will still be available in the previous layer and add up to the image's total size. Refer to the Best practices for writing Dockerfiles and use multi-stage builds sections to learn how to optimize your Dockerfiles for efficient images.</p> <p>The layers are stacked on top of each other. When you create a new container, you add a new writable layer on top of the underlying layers. This layer is often called the "container layer". All changes made to the running container, such as writing new files, modifying existing files, and deleting files, are written to this thin writable container layer. The diagram below shows a container based on an <code>ubuntu:15.04</code> image.</p> <div data-bbox="726 756 1325 1235" data-label="Diagram"> <p>The diagram illustrates the layer structure of a Docker container. At the top is a dashed box labeled "Thin R/W layer" with an arrow pointing to it from the label "Container layer". Below this are four solid blue boxes representing "Image Layers (R/O)", each with a unique ID and a size: <ul style="list-style-type: none"> 91e54dfb1179 (0 B) d74508fb6632 (1.895 KB) c22013c84729 (194.5 KB) d3a1f33e8a5a (188.1 MB) A padlock icon is positioned to the right of these layers, indicating they are read-only. The entire stack is labeled "ubuntu:15.04" and "Container (based on ubuntu:15.04 image)". </p> </div> <p>https://docs.docker.com/storage/storagedriver/</p>

Claim 1	Accused Instrumentalities
	<h2 data-bbox="520 370 730 423">Volumes</h2> <p data-bbox="520 467 1514 570">Volumes are the preferred mechanism for persisting data generated by and used by Docker containers. While bind mounts are dependent on the directory structure and OS of the host machine, volumes are completely managed by Docker. Volumes have several advantages over bind mounts:</p> <p data-bbox="504 589 1041 613">https://kubernetes.io/docs/concepts/storage/volumes/</p> <h2 data-bbox="520 651 974 695">Container environment</h2> <p data-bbox="520 721 1171 776">The Kubernetes Container environment provides several important resources to Containers:</p> <ul data-bbox="554 805 1150 932" style="list-style-type: none"><li data-bbox="554 805 1150 862">• A filesystem, which is a combination of an image and one or more volumes.<li data-bbox="554 870 947 894">• Information about the Container itself.<li data-bbox="554 902 1020 932">• Information about other objects in the cluster. <p data-bbox="504 959 1213 984">https://kubernetes.io/docs/concepts/containers/container-environment/</p>

Claim 1	Accused Instrumentalities
	<h2 data-bbox="520 367 699 415">Images</h2> <p data-bbox="520 443 1209 565">A container image represents binary data that encapsulates an application and all its software dependencies. Container images are executable software bundles that can run standalone and that make very well defined assumptions about their runtime environment.</p> <p data-bbox="520 592 1215 651">You typically create a container image of your application and push it to a registry before referring to it in a <u>Pod</u>.</p> <p data-bbox="504 670 1058 698">https://kubernetes.io/docs/concepts/containers/images/</p> <h2 data-bbox="520 732 732 781">Volumes</h2> <p data-bbox="520 808 1178 899">On-disk files in a container are ephemeral, which presents some problems for non-trivial applications when running in containers. One problem occurs when a container crashes or is stopped.</p> <p data-bbox="520 907 1215 1162">Container state is not saved so all of the files that were created or modified during the lifetime of the container are lost. During a crash, kubelet restarts the container with a clean state. Another problem occurs when multiple containers are running in a <u>Pod</u> and need to share files. It can be challenging to setup and access a shared filesystem across all of the containers. The Kubernetes <u>volume</u> abstraction solves both of these problems. Familiarity with <u>Pods</u> is suggested.</p> <p data-bbox="504 1182 1041 1209">https://kubernetes.io/docs/concepts/storage/volumes/</p>

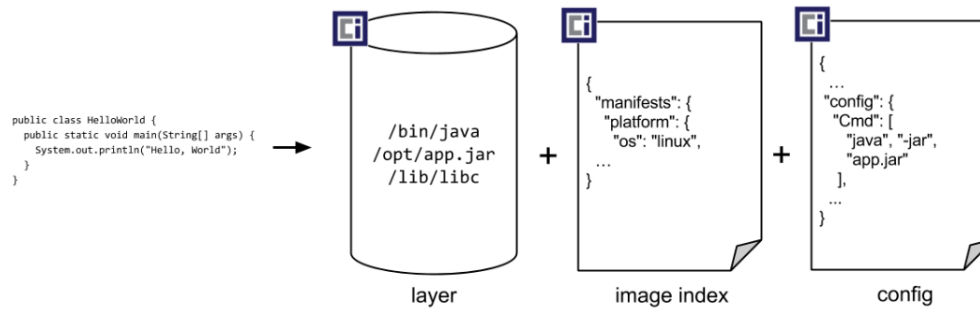
Claim 1	Accused Instrumentalities
	<p data-bbox="533 370 1031 415">Open Container Initiative</p> <hr/> <p data-bbox="533 467 940 503">Image Format Specification</p> <hr/> <p data-bbox="533 542 1503 600">This specification defines an OCI Image, consisting of an image manifest, an image index (optional), a set of filesystem layers, and a configuration.</p> <p data-bbox="533 630 1509 688">The goal of this specification is to enable the creation of interoperable tools for building, transporting, and preparing a container image to run.</p> <p data-bbox="501 711 1176 769">https://github.com/opencontainers/image-spec/blob/a6af2b480dfc001ba975f44de53001c873cb0ef/spec.md</p>

Claim 1

Accused Instrumentalities

Overview

At a high level the image manifest contains metadata about the contents and dependencies of the image including the content-addressable identity of one or more [filesystem layer changeset](#) archives that will be unpacked to make up the final runnable filesystem. The image configuration includes information such as application arguments, environments, etc. The image index is a higher-level manifest which points to a list of manifests and descriptors. Typically, these manifests may provide different implementations of the image, possibly varying by platform or other attributes.



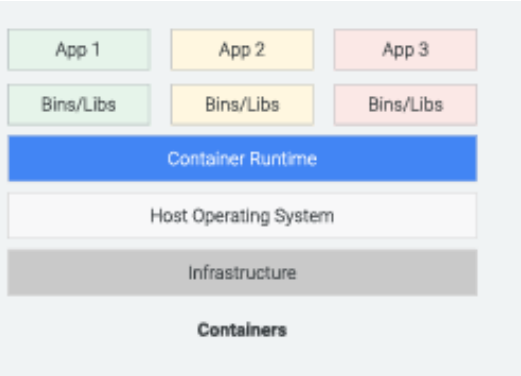
<https://github.com/opencontainers/image-spec/blob/a6af2b480dcfc001ba975f44de53001c873cb0ef/spec.md>

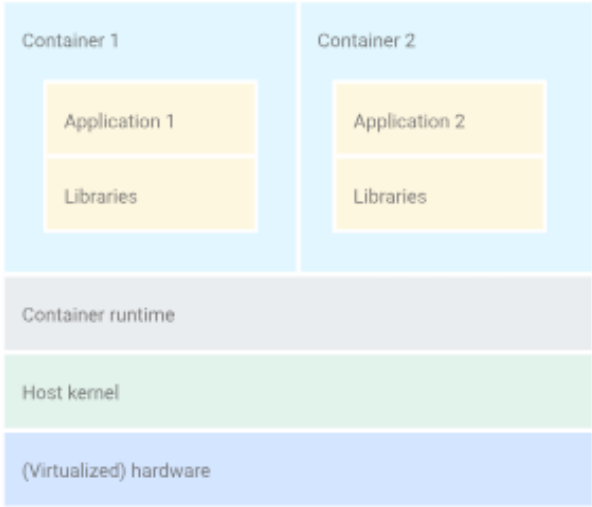
Claim 1	Accused Instrumentalities
	<h2 data-bbox="520 363 1031 407">OCI Image Configuration</h2> <p data-bbox="520 451 1524 578">An OCI <i>Image</i> is an ordered collection of root filesystem changes and the corresponding execution parameters for use within a container runtime. This specification outlines the JSON format describing images for use with a container runtime and execution tool and its relationship to filesystem changesets, described in Layers.</p> <p data-bbox="520 610 1318 638">This section defines the <code>application/vnd.oci.image.config.v1+json</code> media type.</p> <p data-bbox="504 662 1199 716">https://github.com/opencontainers/image-spec/blob/a6af2b480dcf001ba975f44de53001c873cb0ef/config.md</p>

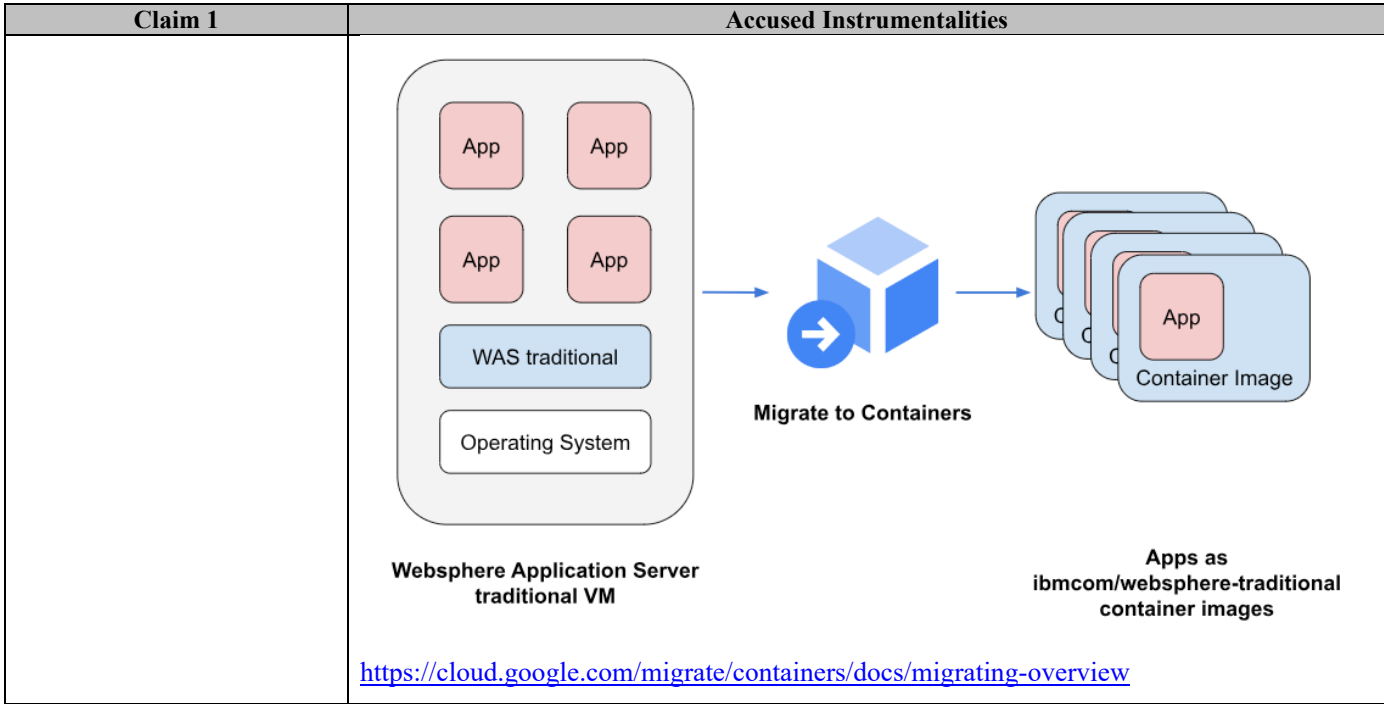
Claim 1	Accused Instrumentalities
	<p data-bbox="527 367 596 394">Layer</p> <ul data-bbox="548 427 1526 703" style="list-style-type: none"> <li data-bbox="548 427 989 451">• Image filesystems are composed of <i>layers</i>. <li data-bbox="548 464 1526 524">• Each layer represents a set of filesystem changes in a tar-based layer format, recording files to be added, changed, or deleted relative to its parent layer. <li data-bbox="548 537 1526 597">• Layers do not have configuration metadata such as environment variables or default arguments - these are properties of the image as a whole rather than any particular layer. <li data-bbox="548 610 1526 703">• Using a layer-based or union filesystem such as AUFS, or by computing the diff from filesystem snapshots, the filesystem changeset can be used to present a series of image layers as if they were one cohesive filesystem. <p data-bbox="527 740 684 768">Image JSON</p> <ul data-bbox="548 800 1526 1076" style="list-style-type: none"> <li data-bbox="548 800 1526 893">• Each image has an associated JSON structure which describes some basic information about the image such as date created, author, as well as execution/runtime configuration like its entrypoint, default arguments, networking, and volumes. <li data-bbox="548 906 1526 966">• The JSON structure also references a cryptographic hash of each layer used by the image, and provides history information for those layers. <li data-bbox="548 979 1526 1039">• This JSON is considered to be immutable, because changing it would change the computed ImageID. <li data-bbox="548 1052 1451 1076">• Changing it means creating a new derived image, instead of changing the existing image. <p data-bbox="506 1097 1199 1157">https://github.com/opencontainers/image-spec/blob/a6af2b480dcfc001ba975f44de53001c873cb0ef/config.md</p>

Claim 1	Accused Instrumentalities
	<p>DESCRIPTION top</p> <p>The programs ld.so and ld-linux.so* find and load the shared objects (shared libraries) needed by a program, prepare the program to run, and then run it.</p> <hr/> <p>https://man7.org/linux/man-pages/man8/ld.so.8.html</p>
<p>[1e] ii) wherein an instance of a SLCSE provided to at least a first of the plurality of software applications from the shared library is run in a context of said at least first of the plurality of software applications without being shared with other of the plurality of software applications and where at least a second of the plurality of software applications running under the operating system have use of a unique instance of a corresponding critical system element for performing same function, and</p>	<p>In each Accused Instrumentality, an instance of a SLCSE provided to at least a first of the plurality of software applications from the shared library is run in a context of said at least first of the plurality of software applications without being shared with other of the plurality of software applications and where at least a second of the plurality of software applications running under the operating system have use of a unique instance of a corresponding critical system element for performing same function.</p> <p>When a Docker or Kubernetes image is used to create a container, it creates a separate and isolated instance of a runtime environment which is independent of other containers running on the same host. Each container has its own instance of base images and its own data. The containers run in isolation, ensuring that the SLCSEs stored in the shared library are accessible to the software applications running in their respective containers. The image includes essential system files, libraries, and dependencies required to run the software application within the container. The containers can share common dependencies and components using layered images. This means that multiple containers utilize the same base image to create an instance. When an instance of SLCSE is provided from the base image (i.e., from the shared library) to an individual container including application software, it operates in isolation and runs its own instance of the software application without sharing resources or critical system elements with other containers. This ensures that each container has its own isolated context. Docker or Kubernetes containers can share common dependencies and components using layered images. This means that multiple containers can utilize the same base image. Therefore, each container, containing the application software running under the operating system, utilizes a unique instance of the corresponding critical system element to execute the respective application software for performing a same or a different function.</p> <p><i>See, e.g.:</i></p>

Claim 1	Accused Instrumentalities
	<p>A container is a way of packaging a given application's code and dependencies so that the application will run easily in any computing environment. This solves the common problem of</p> <p>https://services.google.com/fh/files/misc/why_container_security_matters.pdf</p>

Claim 1	Accused Instrumentalities
	<p>Containers solve the portability problem by isolating the application and its dependencies so they can be moved seamlessly between machines. A process running in a container lives isolated from the underlying environment. You control what it can see and what resources it can access. This helps you use resources more efficiently and not worry about the underlying infrastructure.</p> <p>The container image specifies the container's file system. For example, if you're running a Node.js application, the container image would contain your app, Node.js, and other dependencies like Linux system libraries (except the kernel). A container image usually extends a base operating system image, or base image. This base image is the basis of your container, so you'll want to ensure that it's properly patched and free from known vulnerabilities.</p>  <p>https://services.google.com/fh/files/misc/why_container_security_matters.pdf</p>

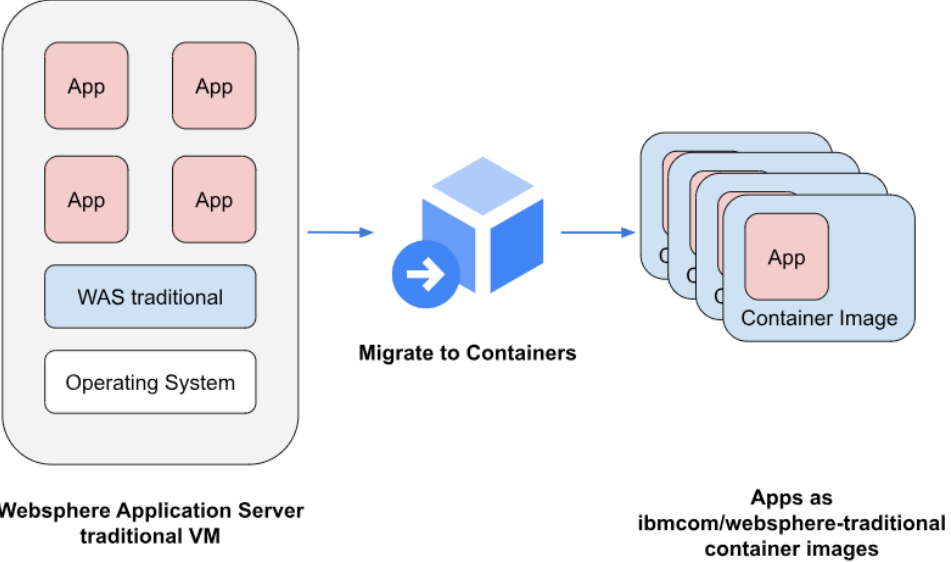
Claim 1	Accused Instrumentalities
	 <p>The diagram illustrates a container architecture stack. At the top, two containers are shown side-by-side: 'Container 1' and 'Container 2'. Each container contains an 'Application' (Application 1 and Application 2 respectively) and 'Libraries'. Below the containers is a 'Container runtime' layer, followed by the 'Host kernel', and finally '(Virtualized) hardware' at the base.</p> <p>https://cloud.google.com/architecture/best-practices-for-operating-containers</p>



Claim 1	Accused Instrumentalities
	<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> <p>Dockerfile App 1</p> <pre style="background-color: #f8d7da; padding: 5px;">FROM node:19.7.0</pre> <pre style="background-color: #d4edda; padding: 5px;">ADD src_app1 /src/</pre> <pre style="background-color: #d4edda; padding: 5px;">RUN cd /src && \ npm install</pre> </div> <div style="text-align: center;"> <p>Dockerfile App 2</p> <pre style="background-color: #f8d7da; padding: 5px;">FROM node:19.7.0</pre> <pre style="background-color: #d4edda; padding: 5px;">ADD src_app2 /src/</pre> <pre style="background-color: #d4edda; padding: 5px;">RUN cd /src && \ npm install</pre> </div> </div> <div style="margin-top: 10px;"> <p> Common layers, downloaded only once</p> <p> Layers unique to each image</p> </div> <p>https://cloud.google.com/architecture/best-practices-for-building-containers</p> <p>One method of packaging an application into a container is with the use of a Dockerfile. The Dockerfile is similar to a script which instructs the daemon on how to assemble the container image. See the Dockerfile reference documentation for more information.</p> <p>Using the Dockerfile method to build a container requires direct knowledge about the application in order to assemble the container. The first step to creating a Dockerfile is selecting an image that will be used as the basis of your image. This image should be a parent or base image maintained and published by a trusted source, usually your company.</p> <p>https://codelabs.developers.google.com/developing-containers-with-dockerfiles#2</p>

Claim 1	Accused Instrumentalities
<p>[1f] iii) wherein a SLCSE related to a predetermined function is provided to the first of the plurality of software applications for running a first instance of the SLCSE, and wherein a SLCSE for performing a same function is provided to the second of the plurality of software applications for running a second instance of the SLCSE simultaneously.</p>	<p>In each Accused Instrumentality, a SLCSE related to a predetermined function is provided to the first of the plurality of software applications for running a first instance of the SLCSE, and wherein a SLCSE for performing a same function is provided to the second of the plurality of software applications for running a second instance of the SLCSE simultaneously.</p> <p>For example, in Docker or Kubernetes containers, each container operates independently, and a base image includes essential system files, libraries, and dependencies (i.e., SLCSEs) required to run the software application within the container. Based on information and belief, each element, such as system files, libraries, and dependencies (i.e., SLCSE) is associated with an execution of a predetermined function related to the application. When an image is used to create a container in the Accused Instrumentality, an instance of the SLCSE is provided to a software application. Therefore, different instances of the SLCSE are provided to different applications for performing either a same or a different function, simultaneously.</p> <p><i>See, e.g.:</i></p> <p>Containers solve the portability problem by isolating the application and its dependencies so they can be moved seamlessly between machines. A process running in a container lives isolated from the underlying environment. You control what it can see and what resources it can access. This helps you use resources more efficiently and not worry about the underlying infrastructure.</p> <p>The container image specifies the container's file system. For example, if you're running a Node.js application, the container image would contain your app, Node.js, and other dependencies like Linux system libraries (except the kernel). A container image usually extends a base operating system image, or base image. This base image is the basis of your container, so you'll want to ensure that it's properly patched and free from known vulnerabilities.</p> <p>https://services.google.com/fh/files/misc/why_container_security_matters.pdf</p>

Claim 1	Accused Instrumentalities
	<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> <p>Dockerfile App 1</p> <pre style="background-color: #f8d7da; padding: 5px;">FROM node:19.7.0</pre> <pre style="background-color: #d4edda; padding: 5px;">ADD src_app1 /src/</pre> <pre style="background-color: #d4edda; padding: 5px;">RUN cd /src && \ npm install</pre> </div> <div style="text-align: center;"> <p>Dockerfile App 2</p> <pre style="background-color: #f8d7da; padding: 5px;">FROM node:19.7.0</pre> <pre style="background-color: #d4edda; padding: 5px;">ADD src_app2 /src/</pre> <pre style="background-color: #d4edda; padding: 5px;">RUN cd /src && \ npm install</pre> </div> </div> <p style="margin-top: 20px;"> Common layers, downloaded only once Layers unique to each image </p> <p>https://cloud.google.com/architecture/best-practices-for-building-containers</p>

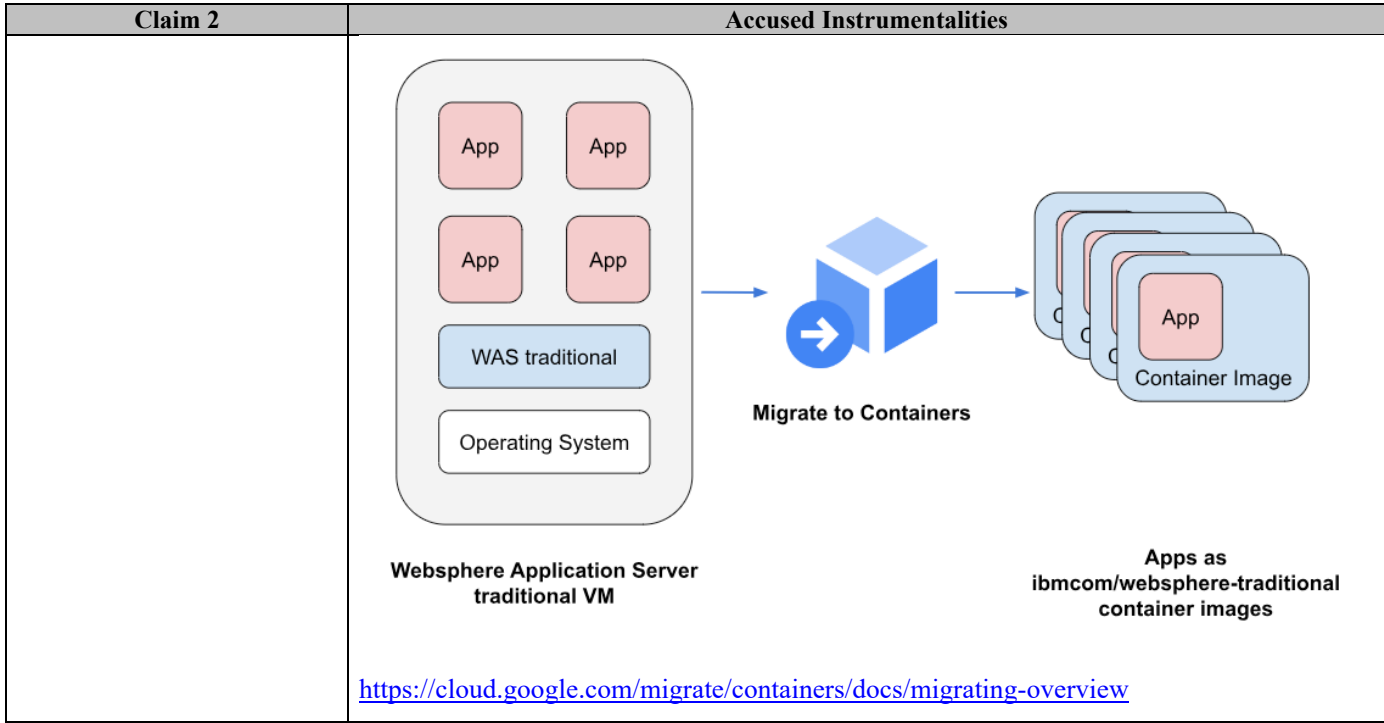
Claim 1	Accused Instrumentalities
	 <p data-bbox="533 870 844 919">Websphere Application Server traditional VM</p> <p data-bbox="1171 862 1482 933">Apps as ibmcom/websphere-traditional container images</p> <p data-bbox="894 712 1115 737">Migrate to Containers</p> <p data-bbox="504 987 1272 1011">https://cloud.google.com/migrate/containers/docs/migrating-overview</p>

Claim 2

Claim 2	Accused Instrumentalities
<p data-bbox="161 1154 472 1295">2. A computing system as defined in claim 1, wherein in operation, multiple instances of an SLCSE stored in the shared library run</p>	<p data-bbox="504 1154 1493 1239">Each Accused Instrumentality comprises or constitutes a computing system as defined in claim 1, wherein in operation, multiple instances of an SLCSE stored in the shared library run simultaneously within the operating system.</p>

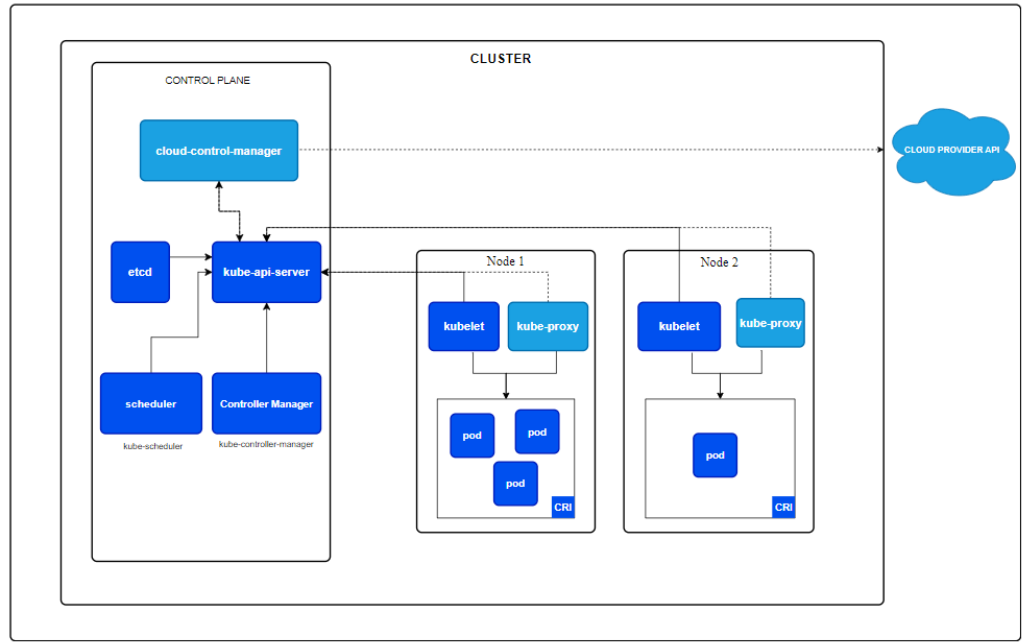
Claim 2	Accused Instrumentalities
<p>simultaneously within the operating system.</p>	<p>For example, an individual host/node runs multiple containers and/or pods simultaneously, each of which has an instance of an SLCSE. When the multiple containers and/or pods run simultaneously, the multiple instances of the SLCSE stored in the shared library run simultaneously.</p> <p><i>See, e.g.:</i></p> <p>Containers solve the portability problem by isolating the application and its dependencies so they can be moved seamlessly between machines. A process running in a container lives isolated from the underlying environment. You control what it can see and what resources it can access. This helps you use resources more efficiently and not worry about the underlying infrastructure.</p> <p>The container image specifies the container's file system. For example, if you're running a Node.js application, the container image would contain your app, Node.js, and other dependencies like Linux system libraries (except the kernel). A container image usually extends a base operating system image, or base image. This base image is the basis of your container, so you'll want to ensure that it's properly patched and free from known vulnerabilities.</p> <p>https://services.google.com/fh/files/misc/why_container_security_matters.pdf</p>

Claim 2	Accused Instrumentalities
	<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> <p>Dockerfile App 1</p> <pre style="background-color: #f8d7da; padding: 5px;">FROM node:19.7.0</pre> <pre style="background-color: #d4edda; padding: 5px;">ADD src_app1 /src/</pre> <pre style="background-color: #d4edda; padding: 5px;">RUN cd /src && \ npm install</pre> </div> <div style="text-align: center;"> <p>Dockerfile App 2</p> <pre style="background-color: #f8d7da; padding: 5px;">FROM node:19.7.0</pre> <pre style="background-color: #d4edda; padding: 5px;">ADD src_app2 /src/</pre> <pre style="background-color: #d4edda; padding: 5px;">RUN cd /src && \ npm install</pre> </div> </div> <p style="margin-top: 20px;"> Common layers, downloaded only once Layers unique to each image </p> <p>https://cloud.google.com/architecture/best-practices-for-building-containers</p>



Claim 2

Accused Instrumentalities



Kubernetes cluster architecture

<https://kubernetes.io/docs/concepts/architecture/>

Claim 2	Accused Instrumentalities
	<h2 data-bbox="516 375 894 435">Containers</h2> <p data-bbox="516 483 1514 607">Each container that you run is repeatable; the standardization from having dependencies included means that you get the same behavior wherever you run it.</p> <p data-bbox="516 656 1514 776">Containers decouple applications from the underlying host infrastructure. This makes deployment easier in different cloud or OS environments.</p> <p data-bbox="516 824 1493 948">Each <u>node</u> in a Kubernetes cluster runs the containers that form the Pods assigned to that node. Containers in a Pod are co-located and co-scheduled to run on the same node.</p> <p data-bbox="516 992 978 1016">https://kubernetes.io/docs/concepts/containers/</p>

Kubernetes Scheduler

In Kubernetes, *scheduling* refers to making sure that Pods are matched to Nodes so that Kubelet can run them.

Scheduling overview

A scheduler watches for newly created Pods that have no Node assigned. For every Pod that the scheduler discovers, the scheduler becomes responsible for finding the best Node for that Pod to run on. The scheduler reaches this placement decision taking into account the scheduling principles described below.

If you want to understand why Pods are placed onto a particular Node, or if you're planning to implement a custom scheduler yourself, this page will help you learn about scheduling.

<https://kubernetes.io/docs/concepts/scheduling-eviction/kube-scheduler/>

Claim 2	Accused Instrumentalities
	<p data-bbox="512 367 961 415">Running containers</p> <p data-bbox="512 456 1514 553">Docker runs processes in isolated containers. A container is a process which runs on a host. The host may be local or remote. When you execute <code>docker run</code>, the container process that runs is isolated in that it has its own file system, its own networking, and its own isolated process tree separate from the host.</p> <p data-bbox="504 586 968 610">https://docs.docker.com/engine/reference/run/</p>

Claim 3

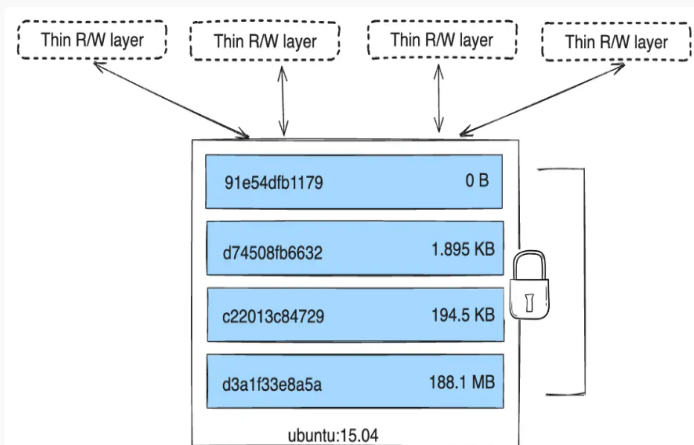
Claim 3	Accused Instrumentalities
<p data-bbox="163 751 478 946">3. A computing system according to claim 1 wherein OSCSEs corresponding to and capable of performing the same function as SLCSEs remain in the operating system kernel.</p>	<p data-bbox="504 751 1514 833">Each Accused Instrumentality comprises or constitutes a computing system according to claim 1 wherein OSCSEs corresponding to and capable of performing the same function as SLCSEs remain in the operating system kernel.</p> <p data-bbox="504 854 1472 935">For example, both Docker and Kubernetes systems preserve the host kernel substantially unchanged; therefore the OSCSEs corresponding to the SLCSEs remain in the operating system kernel.</p> <p data-bbox="504 959 596 984"><i>See, e.g.:</i></p> <p data-bbox="504 1008 1136 1114">Most base images are basic or minimal Linux distributions: Debian, Ubuntu, Redhat, Centos, or Alpine. Developers usually consume these images directly from Docker Hub, or other sources. There are official providers along with a wide variety of other downstream repackagers that layer software to meet customer needs.</p> <p data-bbox="504 1114 1262 1138">https://cloud.google.com/software-supply-chain-security/docs/base-images</p>

Claim 3**Accused Instrumentalities**

[Container image files](#) are complete, static and executable versions of an application or service and differ from one technology to another. [Docker images](#) are made up of multiple layers, which start with a base image that includes all of the dependencies needed to execute code in a container. Each image has a readable/writable layer on top of static unchanging layers. Because each container has its own specific container layer that customizes that specific container, underlying image layers can be saved and reused in multiple containers. An Open Container Initiative ([OCI](#))

<https://www.techtarget.com/searchitoperations/definition/container-containerization-or-container-based-virtualization>

Because each container has its own writable container layer, and all changes are stored in this container layer, multiple containers can share access to the same underlying image and yet have their own data state. The diagram below shows multiple containers sharing the same Ubuntu 15.04 image.



<https://docs.docker.com/storage/storagedriver/>

Claim 4

Claim 4	Accused Instrumentalities
<p>4. A computing system according to claim 1 wherein the one or more SLCSEs provided to one of the plurality of software applications having exclusive use thereof, use system calls to access services in the operating system kernel.</p>	<p>Each Accused Instrumentality comprises or constitutes a computing system according to claim 1 wherein the one or more SLCSEs provided to one of the plurality of software applications having exclusive use thereof, use system calls to access services in the operating system kernel.</p> <p>For example, the SLCSEs in a container use system calls to access services in the operating system kernel. For example, the glibc library (or other similar library) in the container uses system calls to interface with the host Linux kernel. In general, system calls can be observed using a tool such as strace.</p> <p><i>See, e.g.:</i></p> <p>The GNU C Library, commonly known as glibc, is the GNU Project implementation of the C standard library. It is a wrapper around the system calls of the Linux kernel for application use. Despite its name, it now also directly supports C++ (and, indirectly, other programming languages). It was started in the 1980s by the Free Software Foundation (FSF) for the GNU operating system.</p> <p>https://en.wikipedia.org/wiki/Glibc</p>

We can now get the process id directly from the cgroup. It will be located in the cgroup.procs file.

```
### Terminal 2 - Worker Node ###

# Get the process id
$ cat cri-containerd-ceeeef06afe89c8223d33b11e8d9e0b207118ac4dac3af826687668ee1ee
16254

# Validate what is running under the process
$ ps aux | grep 16254
azureus+ 16254 0.0 0.1 713972 10476 ?        Ssl 15:04  0:00 ./faultyapp
azureus+ 94806 0.0 0.0 7004 2168 pts/0    S+  16:22  0:00 grep --color=
```

Got it! With that, we can try to find out what is going out inside the app. Lets try to run strace to get some more insight.

```
### Terminal 2 - Worker Node ###

$ sudo strace -p 16254 -f
...
# The app is trying to read a file port.txt
[pid 16269] openat(AT_FDCWD, "port.txt", O_RDONLY|O_CLOEXEC <unfinished ...>
[pid 16254] epoll_pwait(5, <unfinished ...>
# The file does not exist
[pid 16269] <... openat resumed>          = -1 ENOENT (No such file or directory)
[pid 16254] <... epoll_pwait resumed>[], 128, 0, NULL, 0) = 0
[pid 16269] write(1, "Something went wrong...\n", 24 <unfinished ...>
```

After filtering the output, we can see the application is trying to read a text file called port.txt, and a few lines later, there is a message stating ENOENT (No such file or directory). Let's create that file.

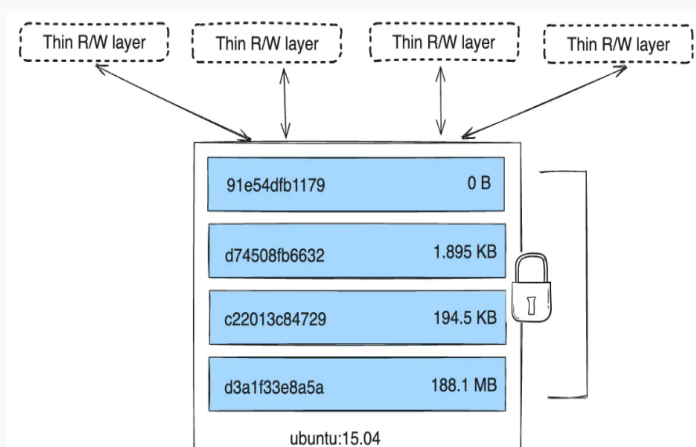
<https://www.berops.com/blog/a-different-method-to-debug-kubernetes-pods>

Claim 5

Claim 5	Accused Instrumentalities
<p>5. A computing system according to claim 1 wherein the operating system kernel comprises a kernel module adapted to serve as an interface between an SLCSE in the context of an application program and a device driver.</p>	<p>Each Accused Instrumentality comprises or constitutes a computing system according to claim 1 wherein the operating system kernel comprises a kernel module adapted to serve as an interface between an SLCSE in the context of an application program and a device driver.</p> <p>For example, the server (node) includes an operating system having a kernel. The kernel comprises a kernel module which enables applications (including their libraries) to have access to system resources such as storage, <i>i.e.</i>, acts as an interface between applications/libraries and OS libraries or drivers</p> <p><i>See, e.g.:</i></p> <h2 data-bbox="533 704 846 748">Container images</h2> <p data-bbox="533 776 1125 894">A container image is a ready-to-run software package containing everything needed to run an application: the code and any runtime it requires, application and system libraries, and default values for any essential settings.</p> <p data-bbox="501 915 978 943">https://kubernetes.io/docs/concepts/containers/</p> <p data-bbox="512 984 1346 1117">Docker is used to create, run and deploy applications in containers. A Docker image contains application code, libraries, tools, dependencies and other files needed to make an application run. When a user runs an image, it can become one or many instances of a container.</p> <p data-bbox="501 1136 1220 1164">https://www.techtarget.com/searchitoperations/definition/Docker-image</p>

Claim 5**Accused Instrumentalities**

Because each container has its own writable container layer, and all changes are stored in this container layer, multiple containers can share access to the same underlying image and yet have their own data state. The diagram below shows multiple containers sharing the same Ubuntu 15.04 image.



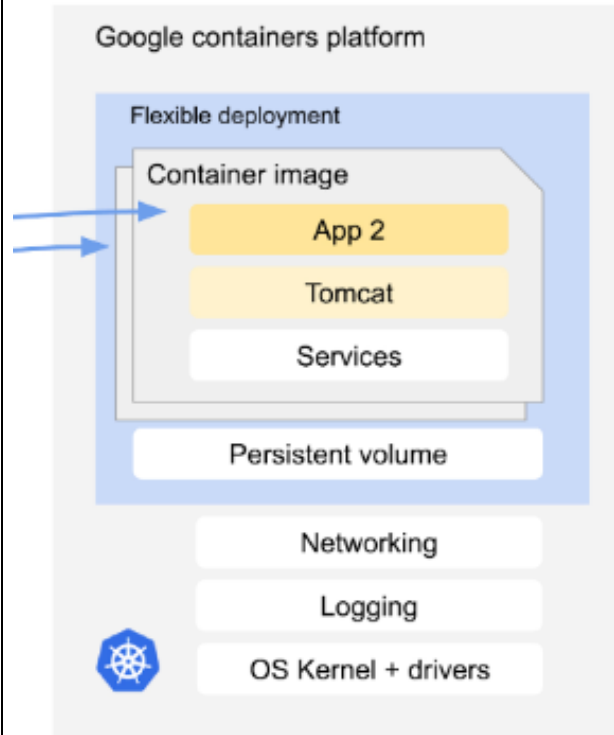
<https://docs.docker.com/storage/storagedriver/>

Containers use specific features of the Linux kernel that “trick” individual applications into thinking they’re in their own unique environment, even though multiple applications share the same host kernel. (If you’re not familiar with the Linux kernel, it’s a part of the operating system that communicates between processes--requests that do user tasks like opening a file, running a program-- and the hardware. It manages resources like memory and CPU to meet these requests).

https://services.google.com/fh/files/misc/why_container_security_matters.pdf

Claim 5

Accused Instrumentalities



<https://cloud.google.com/blog/products/application-modernization/shift-your-apps-to-container-based-workloads-on-the-command-line>

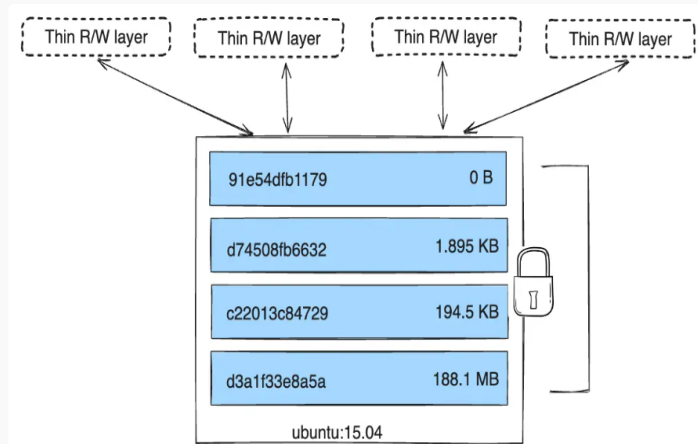
Claim 10

Claim 10	Accused Instrumentalities
<p>10. A computing system according to claim 2 wherein SLCSEs stored in the shared library are linked to particular software applications of the plurality of software applications as the particular software applications are loaded such that the particular software applications have a link that provides unique access to a unique instance of a CSE.</p>	<p>Each Accused Instrumentality comprises or constitutes a computing system according to claim 2 wherein SLCSEs stored in the shared library are linked to particular software applications of the plurality of software applications as the particular software applications are loaded such that the particular software applications have a link that provides unique access to a unique instance of a CSE.</p> <p>For example, the containers can share common dependencies and components using layered images, and multiple containers can use the same base image. Therefore, each container, containing the application software running under the operating system of the server hosting GKE, uses a unique instance of the corresponding critical system element to execute the respective application software and has a link to that unique instance. The software applications dynamically link to the SLCSEs using, e.g., ld.so.</p> <p><i>See, e.g.:</i></p> <h3>Container images</h3> <p>A container image is a ready-to-run software package containing everything needed to run an application: the code and any runtime it requires, application and system libraries, and default values for any essential settings.</p> <p>https://kubernetes.io/docs/concepts/containers/</p> <p>Docker is used to create, run and deploy applications in containers. A Docker image contains application code, libraries, tools, dependencies and other files needed to make an application run. When a user runs an image, it can become one or many instances of a container.</p> <p>https://www.techtarget.com/searchitoperations/definition/Docker-image</p>

Claim 10

Accused Instrumentalities

Because each container has its own writable container layer, and all changes are stored in this container layer, multiple containers can share access to the same underlying image and yet have their own data state. The diagram below shows multiple containers sharing the same Ubuntu 15.04 image.



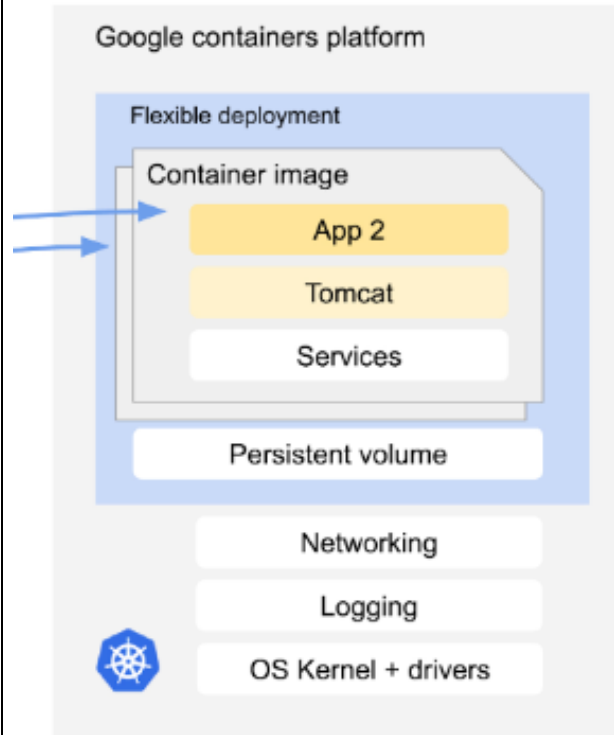
<https://docs.docker.com/storage/storagedriver/>

Containers use specific features of the Linux kernel that “trick” individual applications into thinking they’re in their own unique environment, even though multiple applications share the same host kernel. (If you’re not familiar with the Linux kernel, it’s a part of the operating system that communicates between processes--requests that do user tasks like opening a file, running a program-- and the hardware. It manages resources like memory and CPU to meet these requests).

https://services.google.com/fh/files/misc/why_container_security_matters.pdf

Claim 10

Accused Instrumentalities



<https://cloud.google.com/blog/products/application-modernization/shift-your-apps-to-container-based-workloads-on-the-command-line>

Claim 10	Accused Instrumentalities
	<p>Containers solve the portability problem by isolating the application and its dependencies so they can be moved seamlessly between machines. A process running in a container lives isolated from the underlying environment. You control what it can see and what resources it can access. This helps you use resources more efficiently and not worry about the underlying infrastructure.</p> <p>The container image specifies the container's file system. For example, if you're running a Node.js application, the container image would contain your app, Node.js, and other dependencies like Linux system libraries (except the kernel). A container image usually extends a base operating system image, or base image. This base image is the basis of your container, so you'll want to ensure that it's properly patched and free from known vulnerabilities.</p> <p>https://services.google.com/fh/files/misc/why_container_security_matters.pdf</p>

Claim 10	Accused Instrumentalities
	<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> <p>Dockerfile App 1</p> <pre style="background-color: #f8d7da; padding: 5px;">FROM node:19.7.0</pre> <pre style="background-color: #d4edda; padding: 5px;">ADD src_app1 /src/</pre> <pre style="background-color: #d4edda; padding: 5px;">RUN cd /src && \ npm install</pre> </div> <div style="text-align: center;"> <p>Dockerfile App 2</p> <pre style="background-color: #f8d7da; padding: 5px;">FROM node:19.7.0</pre> <pre style="background-color: #d4edda; padding: 5px;">ADD src_app2 /src/</pre> <pre style="background-color: #d4edda; padding: 5px;">RUN cd /src && \ npm install</pre> </div> </div> <p style="margin-top: 10px;"> Common layers, downloaded only once Layers unique to each image </p> <p style="margin-top: 10px;"> https://cloud.google.com/architecture/best-practices-for-building-containers </p> <p>DESCRIPTION top</p> <p>The programs ld.so and ld-linux.so* find and load the shared objects (shared libraries) needed by a program, prepare the program to run, and then run it.</p> <p>https://man7.org/linux/man-pages/man8/ld.so.8.html</p>

Claim 18

Claim 18	Accused Instrumentalities
<p>18. A computer system as defined in claim 2 wherein SLCSEs are not copies of OSCSEs.</p>	<p>Each Accused Instrumentality comprises or constitutes a computer system as defined in claim 2 wherein SLCSEs are not copies of OSCSEs.</p> <p>For example, in a typical case the SLCSEs come from a Linux distribution independent of the host operating system, and thus are not identical to the OSCSEs. For another example, the SLCSEs are provided to the computer system through a separate process than the process by which the OSCSEs are provided to the computer system, and thus are not copied from the OSCSEs.</p> <p><i>See, e.g.:</i></p> <h3>Container images</h3> <p>A container image is a ready-to-run software package containing everything needed to run an application: the code and any runtime it requires, application and system libraries, and default values for any essential settings.</p> <p>https://kubernetes.io/docs/concepts/containers/</p> <p>Docker is used to create, run and deploy applications in containers. A Docker image contains application code, libraries, tools, dependencies and other files needed to make an application run. When a user runs an image, it can become one or many instances of a container.</p> <p>https://www.techtarget.com/searchitoperations/definition/Docker-image</p>

Claim 18	Accused Instrumentalities
	<p data-bbox="512 363 1503 467">Because each container has its own writable container layer, and all changes are stored in this container layer, multiple containers can share access to the same underlying image and yet have their own data state. The diagram below shows multiple containers sharing the same Ubuntu 15.04 image.</p> <div data-bbox="680 521 1377 959" style="text-align: center;"> <p>The diagram illustrates a shared storage architecture. At the top, four dashed boxes labeled 'Thin R/W layer' are arranged horizontally. Below them is a central box representing the 'ubuntu:15.04' image. This image is composed of four stacked layers, each with a unique ID and size: <ul style="list-style-type: none"> 91e54dfb1179: 0 B d74508fb6632: 1.895 KB c22013c84729: 194.5 KB d3a1f33e8a5a: 188.1 MB A padlock icon is positioned to the right of the image stack, indicating it is read-only. Arrows show that each 'Thin R/W layer' is linked to the top layer of the image stack, and bidirectional arrows connect the layers within the image stack.</p> </div> <p data-bbox="504 979 974 1003">https://docs.docker.com/storage/storagedriver/</p>