

# Rust IN ACTION

T. S. McNamara

MEAP



MANNING



**MEAP Edition  
Manning Early Access Program  
Rust in Action  
Version 10**

Copyright 2019 Manning Publications

For more information on this and other Manning titles go to  
[manning.com](http://manning.com)

# welcome

---

Dear Reader,

Thanks for taking a chance and buying this early release book on the Rust programming language and the internals of computer systems. I hope that you'll be rewarded with a fun, informative read!

Part 1: Rust Language Distinctives will provide a quick-fire introduction to the Rust language by working through projects that begin to introduce concepts that are expanded upon later in the book, such as implementing a File API.

Part 2: Systems Programming from the Ground Up (Almost) will shift your focus towards the computer. You will learn how data is represented at various levels between the application, operating system and hardware. Rust language features will be introduced as required.

A note about Chapter 6: This chapter should be considered a work in progress. It covers lots of ground. Readers progress from learning what a pointer is to benchmarking memory allocations with system utilities for Linux. Some of the explanations are terse... perhaps too terse.

We believe that the content is interesting and relevant to professional programmers, but are considering how it should be expanded and refactored to be most relevant to the book's readers. The author and the editorial team are very interested in your views about what works and what needs more work.

Part 3: Concurrent and Parallel Programming will walk through the tools that computers offer to get work done in parallel. Its primary goal will be to explain how multiple threads can cooperate and coordinate. A large example—building a graph that can be distributed in multiple ways—will be extended throughout several chapters.

Finally, Part 4: Extending Applications Up and Out will show Rust being used to build up software components to extend large software projects. These projects demonstrate systems programming “with the system” rather than systems programming “of the system”. Part 4 will deal with the complexities of handling multiple CPU/OS pairs from the same code base.

As a MEAP reader, you have a unique opportunity to contribute to the book's development. All feedback is greatly received, but please remember that there will be a human receiving the message. The best channel is the Manning [liveBook's Discussion Forum](#). I'm also active on Twitter (@timClicks), Reddit (/u/timclicks) and the Rust Discourse forum (<https://users.rust-lang.org/u/timclicks>).

Thank you once again for choosing to purchase the book. It's a privilege to ride a short way with you along your computing journey.

—Tim McNamara

# *brief contents*

---

*1 Introducing Rust*

## **PART 1: RUST LANGUAGE DISTINCTIVES**

*2 Language Foundations*

*3 Compound Data Types*

*4 Lifetimes, Ownership and Borrowing*

## **PART 2: DEMYSTIFYING SYSTEMS PROGRAMMING**

*5 Data in Depth*

*6 Memory*

*7 Files and Storage*

*8 Networking*

*9 Time and Time Keeping*

*10 Threads, Processes & Containers*

*11 Kernel*

*12 Signals, Interrupts and Exceptions*

# Introducing Rust

## **This chapter covers:**

- Highlighting some great features of the language and its community
- Exposing you to Rust's syntax
- Introducing the goals of the project
- Discussing where Rust might be useful and when to avoid it
- Building your first Rust program
- Explaining how Rust compares to object-orientated and wider languages

Welcome to Rust, the programming language that rewards your curiosity. Once you scratch the surface, you will find a programming language with unparalleled speed and safety that is still comfortable to use. Learning the language can be challenging, but the rewards can be immense.

Rust has established a strong following. In Stack Overflow's annual developer survey, Rust has won “most loved programming language” in 2016, 2017, 2018 and 2019. The distinction is awarded to the language that has the highest proportion of current developers in the language who want to continue using it.

## **1.1 How is Rust used?**

The language has proven its ability to build powerful, reliable software.

Large technology leaders have adopted Rust:

- **Amazon Web Services** runs its serverless computing offerings, AWS Lambda

and AWS Fargate with Rust<sup>1</sup>

- **Dropbox** rebuilt its storage backend in Rust during 2015-2016, which manages exabytes of storage<sup>2</sup>
- **Cloudflare** develops many of its services with Rust, including its public DNS, serverless computing and packet inspection offerings<sup>3</sup>
- **Google** develops portions of the Chrome OS<sup>4</sup> and Fuchsia<sup>5</sup> operating systems in Rust.
- **Microsoft** writes components of its Azure platform in Rust, including a security daemon for its Internet of Things (IoT) service<sup>6</sup>
- **Mozilla** uses Rust to enhance the Firefox web browser. The browser project contains 15 million lines of code. Mozilla's first two Rust-in-Firefox projects, its MP4 metadata parser and text encoder/decoder have led to performance and stability improvements.
- **Samsung**, via its subsidiary SmartThings, uses Rust in its “Hub”. The Hub is the a smart devices firmware backend for its Internet of Things (IoT) service.
- **Oracle** has developed a container runtime in Rust, to overcome problems that they perceived with the Go reference implementation<sup>7</sup>

Rust is also productive enough for fast-moving startups to deploy it:

- **Sourcegraph** uses Rust to serve syntax highlighting across all of its languages<sup>8</sup>
- **Figma** employs Rust in the performance-critical components of its multi-player server<sup>9</sup>
- **Parity** develops its client to the Ethereum blockchain in Rust<sup>10</sup>

The language has also spawned lots of innovative projects. This includes operating systems, game engines, databases and drivers. Like its peer systems languages, it can be in micro-controllers through to supercomputers. Yet the language fee

Rust supports WebAssembly (WASM), a standard for deploying apps into browsers without JavaScript, as a first-class citizen. WASM allows you to compile and deploy your Rust project to the server, IoT devices, mobile devices and the browser.

## 1.2 What is it like to advocate for Rust at work?

This snippet from a 2017 discussing early Rust usage at Google for the Chrome OS project provides two anecdotes:

<sup>1</sup> Firecracker: Secure and fast microVMs for serverless computing [firecracker-microvm.github.io/](https://firecracker-microvm.github.io/)

<sup>2</sup> The Epic Story of Dropbox's Exodus From the Amazon Cloud Empire [www.wired.com/2016/03/epic-story-dropbox-exodus-amazon-cloud-empire/](http://www.wired.com/2016/03/epic-story-dropbox-exodus-amazon-cloud-empire/)

<sup>3</sup> Rust at Cloudflare [news.ycombinator.com/item?id=17077358](http://news.ycombinator.com/item?id=17077358)

<sup>4</sup> crosvm - The Chrome OS Virtual Machine Monitor [chromium.googlesource.com/chromiumos/platform/crosvm/](https://chromium.googlesource.com/chromiumos/platform/crosvm/)

<sup>5</sup> Fuchsia Rust Crates [fuchsia.googlesource.com/fuchsia/+/master/docs/development/languages/rust/crates.md](https://fuchsia.googlesource.com/fuchsia/+/master/docs/development/languages/rust/crates.md)

<sup>6</sup> [github.com/Azure/iotedge/tree/master/edgelet](https://github.com/Azure/iotedge/tree/master/edgelet)

<sup>7</sup> Building a Container Runtime in Rust [blogs.oracle.com/developers/building-a-container-runtime-in-rust](https://blogs.oracle.com/developers/building-a-container-runtime-in-rust)

<sup>8</sup> HTTP code syntax highlighting server written in Rust [github.com/sourcegraph/syntect\\_server](https://github.com/sourcegraph/syntect_server)

<sup>9</sup> Rust in Production at Figma [www.figma.com/blog/rust-in-production-at-figma/](http://www.figma.com/blog/rust-in-production-at-figma/)

<sup>10</sup> The fast, light, and robust EVM and WASM client [github.com/paritytech/parity-ethereum](https://github.com/paritytech/parity-ethereum)

**Listing 1.1. Excerpt from a the Hacker News comment thread discussing "``Chrome OS KVM - A component written in Rust''<sup>11</sup>**

indy on Sept 27, 2017

Is Rust an officially sanctioned language at Google?

zaxcellent on Sept 27, 2017

Author here: Rust is not officially sanctioned at Google, but there are pockets of folks using it here. The trick with using Rust in this component was convincing my coworkers that no other language was right for job, which I believe to be the case in this instance.

That being said, there was a ton of work getting Rust to play nice within the Chrome OS build environment. The Rust folks have been super helpful in answering my questions though.

ekidd on Sept 27, 2017

> The trick with using Rust in this component was convincing my coworkers that no other language was right for job, which I believe to be the case in this instance.

I ran into a similar use case in one of my own projects—a vobsub subtitle decoder, which parses complicated binary data, and which I someday want to run as web service. So obviously, I want to ensure that there are no vulnerabilities in my code.

I wrote the code in Rust, and then I used 'cargo fuzz' to try and find vulnerabilities. After running a billion(!) fuzz iterations, I found 5 bugs (see the 'vobsub' section of the trophy case for a list <https://github.com/rust-fuzz/trophy-case>).

Happily, not one of those bugs could actually be escalated into an actual exploit. In each case, Rust's various runtime checks successfully caught the problem and turned it into a controlled panic. (In practice, this would restart the web server cleanly.)

So my takeaway from this was that whenever I want a language (1) with no GC, but (2) which I can trust in a security-critical context, Rust is an excellent choice. The fact that I can statically link Linux binaries (like with Go) is a nice plus.

We can see that language adoption has been “bottom up” by engineers looking to overcome technical challenges. Skepticism from colleagues has been overcome with using Rust for internal side-projects, then gaining first-hand experience and measurable performance data. In the time since late 2017, Rust has continued to mature and strengthen.

### 1.3 What does Rust look and feel like?

Below at Listing 1.2 , you'll see an example of a JSON-based web service for

---

<sup>11</sup> [news.ycombinator.com/item?id=15346557](https://news.ycombinator.com/item?id=15346557)

providing the current time. It demonstrates a number of interesting features that help to produce effective software productively:

- High-level, expressive feel. Rust programs are able to feel ergonomic and yet achieve bare metal performance.
- No fuss type creation. Defining a new type doesn't require compulsory methods such as constructors, attribute accessors (get/set methods) or destructors to get off the ground (lines 14-17).
- Convenient method syntax. Rust is not an object-oriented language, but does include a few syntactic features to create readable/writable code (lines 32-34).
- The ability for library writers to tweak the compiler's behavior with plugins. In the example, the web framework asks the compiler to automatically create boilerplate code (lines 1-2) and generate a JSON representation of timestamps itself (line 15).

To see the web service in action, here are some instructions to get you started.

- Install Rust via [rustup.rs/](#)
- Open a console prompt and move to the `ch1-time-api` directory
- Execute `rustup install nightly`. This enables extra features, such as compiler-supported code generation, that are pending stabilization.
- Execute `rustup run nightly cargo run`. This tells Rust that we want to use the "nightly" channel that we've just installed to execute "cargo run", which will build and run the project.

All going well, after several lines describing compiling the code's dependencies, you'll see a report like this appear on your screen:

```
Compiling ch1-time-api v0.1.0 (file:///path/to/ch1-time-api)
Finished dev [unoptimized + debuginfo] target(s) in n.nn secs
  Running `target\debug\ch1-time-api.exe`
🔧 Configured for development.
=> address: localhost
=> port: 8000
=> log: normal
=> workers: 8
=> secret key: generated
=> limits: forms = 32KiB
=> tls: disabled
🔧 Mounting '/':
=> GET /
=> GET /time
🔧 Rocket has launched from http://localhost:8000
```

Here is the web service code itself:

**Listing 1.2. Example Rust Code - A Web API That Tells The Time (ch1-time-api/src/main.rs)**

```

#![feature(plugin)]          ①
#![plugin(rocket_codegen)]    ①

extern crate serde;           ②
extern crate chrono;          ②
extern crate rocket;          ②
extern crate rocket_contrib;   ②

#[macro_use]                  ③
extern crate serde_derive;

use chrono::prelude::*;

use rocket_contrib::Json;      ⑤

#[derive(Serialize)]          ⑥
struct Timestamp {
    time: String,
}

#[get("/")]
fn index() -> &'static str { ⑦
    "Hello, world!"           ⑨
}

#[get("/time")]
fn time_now() -> Json<Timestamp> {
    let now: DateTime<Utc> = Utc::now();
    let timestamp = Timestamp { time: now.to_rfc3339() };
    Json(timestamp)
}

fn main() {
    rocket::ignite()
        .mount("/", routes![index, time_now])
        .launch();
}

```

- ① Attributes, such as `#![feature(plugin)]` and `#[derive(Serialize)]`, customize behavior. `#[derive(Serialize)]` asks the compiler to create its own code for converting the `Timestamp` struct to a string, to be sent down the wire as JSON.
- ② `extern` brings external crates (packages) into local scope
- ③ Attribute to indicate that we want to import macros from another crate
- ④ `use` and an asterisk brings all exported members of `chrono::prelude` into local scope. This crate uses `DateTime` and `Utc`
- ⑤ `use` with curly braces brings only specified members into local scope. In this case, just the single member `Json`
- ⑥ `#[derive(Serialize)]` is provided by the `serde` crate and automatically generates a string representation of this struct (which will be used as JSON down the wire later on)

- ⑦ The `get` attribute is provided by the web framework. It tells Rust to generate code on our behalf for serving HTTP requests.
- ⑧ Define a function with no arguments. Its return type is a "static str", which can be thought of as a string type for string literals.
- ⑨ Rust returns the result of the final expression of a function. Using the `return` keyword at the end of a function is considered poor style

The preceding example was chosen as an attempt at packing as many representative features of the language into a single example as possible. Over the course of a few chapters, each of those features will be unpacked and examined. Until then, let's take a step back and consider some of the thinking behind the language and where it fits within the programming language ecosystem.

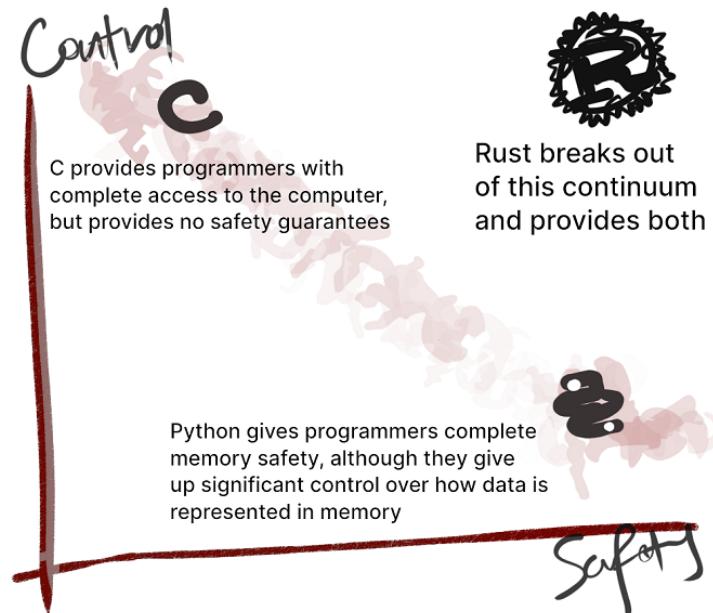
As you'll discover through the chapters ahead, many of its features are drawn from two programming sub-fields: systems programming and functional programming.

- From systems programming, Rust draws the notion of control and a willingness to strip back abstraction when required
- From functional programming, Rust provides efficient implementations of higher-order programming, an impressive type system, pattern matching and first class support for generics

The language's syntax is similar to programming languages from the C programming heritage. Yet the differences are sufficiently different to minimize issues that arise from switching between two almost-the-same languages.

## 1.4 What is Rust?

Rust's distinguishing feature—as a programming language—is its ability to analyse prevent invalid data access in your program at *compile time*. It guarantees that your program is *memory safe* without imposing any *run time* costs. Other languages provide safety by adding checks during your program's execution, thus slowing it down.



Rust's distinguishing feature—as a professional community—is the willingness to explicitly include values into its decision-making and process. Its compiler errors are ridiculously helpful. All interactions within the Rust community are governed by its code of conduct. And most visibly, its public messaging has changed.

Until late 2018, visitors to the Rust homepage with the technically-heavy message. At that point, the community implement a change to its wording to put its users (and its potential users) at the center.

**Table 1.1. Rust slogans over time. As Rust has developed in confidence, it has increasingly embraced the idea of acting as a facilitator and supporter of everyone wanting to achieve their programming aspirations.**

Until late 2018	From that point onwards
Rust is a systems programming language that runs blazingly fast, prevents segfaults and guarantees thread safety.	Empowering everyone to build reliable and efficient software.

Rust is labelled as a *systems programming language*, which tends to be seen as quite a specialized, almost esoteric, branch of programming. But those three ideas are widely applicable to software engineering projects in general. And so is Rust.

Let's flesh out three goals: safety, productivity and control.

### 1.4.1 Safety

Rust programs are free from:

- “dangling pointers” - live references to data that has become invalid over the course of the program
- “data races” - unable to determine how a program will behave from run to run because external factors are changing
- “buffer overflow” - attempting to access the 12th element of an array of only 6 elements
- “iterator invalidation” - an issue caused by something that is being iterated over being altered mid-way through

When programs are compiled in debug mode, Rust also protects against integer overflow. What is integer overflow? Well, as integers types have a fixed-width in memory, they are finite. Integer overflow is what happens when they hit their limit and flow over to the beginning again.

Knowing that a language is safe provides programmers with a degree of liberty. As they know that their program won’t implode, they become much more willing to experiment. Within the Rust community, this liberty has spawned the saying “fearless concurrency”.

Compile-time safety has other benefits. In the following snippet, the local variable `v` is a read-only reference to a vector of type `T`. The Rust compiler knows that read-only vectors will stay the same length for the whole function, thus the call to `len()` will never reach invalid memory. Thus the compiler can turn off runtime bounds checking for the `for..in` loop.

```
fn for_each(v: &Vec<T>) {    ①
    for item in 0..v.len() {    ②
        work(v[things]);
    }
}
```

① “`&Vec<T>`” reads as “a reference to a vector of type `T`”.

② `0..v.len()` returns an iterator from the

## 1.4.2 Productivity

When given a choice, Rust prefers the option that is easiest for the developer. Many of its subtler features are productivity boosts.

Programmer productivity is a difficult concept to demonstrate in a book example.

Let’s start with something that can snag beginners: using assignment (`=`) within an expression that should use an equality (`==`) test.

```
fn main() {
    let a = 10;

    if a = 10 {
        println!("a equals ten");
    }
}
```

```
}
```

In Rust, the preceding code would fail to compiler. The Rust 1.17 compiler generates the following message:

```
rustc 1.17.0 (56124baa9 2017-04-24)
error[E0308]: mismatched types
--> <anon>:4:8
 |
4 |     if a = 10 {
|         ^^^^^^ expected bool, found ()
|
= note: expected type `bool`
       found type `()`
```

**error: aborting due to previous error**

At first, "mismatched types" might feel like a strange error message. Surely variables can be tested for equality against integers. After some thought, it becomes apparent that the `if` test is being provided with the wrong type. It requires a boolean value and is instead receiving `()`. `()` is a placeholder value that will be discussed in more depth later.

Adding a second equals sign on line 4 results in a working program that prints `a equals ten`.

```
fn main() {
    let a = 10;

    if a == 10 {
        println!("a equals ten");
    }
}
```

Rust has many ergonomic features. It offers generics, sophisticated data types, pattern matching and closures.<sup>12</sup> Those who have worked with other ahead-of-time compilation languages are likely to appreciate Rust's build system and its comprehensive package manager: `cargo`.

### 1.4.3 Control

Control over memory access, memory layout and specific CPU instructions is very important when squeezing the best performance out of code. At times, it is imperative to manage how something is operating. It might matter that data is stored in the *stack*, rather than on the *heap*. At times, it might make sense to add reference counting to a shared value. Often, it makes sense to pass references to functions. Occasionally, it might be useful to create one's own type of pointer for a particular access pattern. Most of the time though, there are other things to worry about. And for the majority, Rust uses sensible defaults that align with its "zero cost abstractions" philosophy.

---

<sup>12</sup> If these terms are unfamiliar, do keep reading. They are explained throughout the book.

**NOTE**

If the terms such as *stack*, *heap* and *reference counting* are new to you, don't put the book down! We'll spend lots of the book explaining how they all work in the rest of the book.

The following code snippet prints out the line `a: 10, b: 20, c: 30, d: Mutex { data: 40 }`. Each representation is another way of storing an integer. As we progress through the next few chapters, the trade offs related to each level become apparent. For the moment, the important things to remember is that the menu is comprehensive and you are welcome to choose exactly what's right for your specific use case.

**Listing 1.3. A code example demonstrating multiple mechanisms for creating integer values. Each form provides differing semantics and run-time characteristics. Programmers retain full control of the trade offs that they wish to make.**

```
use std::rc::Rc;
use std::sync::{Arc, Mutex};

fn main() {
    let a = 10;                                ①

    let b = Box::new(20);                      ②

    let c = Rc::new(Box::new(30));              ③

    let d = Arc::new(Mutex::new(40));           ④

    println!("a: {:?}", a, b, c, d);
}
```

- ① An integer on the stack
- ② An integer on the heap, also known as a "boxed integer"
- ③ A boxed integer wrapped within a reference counter
- ④ An integer protected by a mutual exclusion lock, wrapped in an atomic reference counter

To understand why Rust is doing something the way it is, it can be helpful to refer back to these three principles:

- Data within Rust is immutable by default
- The language's first priority is safety
- Safety is almost always provided at compile time, without imposing runtime costs

## 1.5 Rust's Big Features

Our tools shape what we believe we can make. Rust seeks to enable you to build the software that you would like to, but were too scared to try. So what kind tool is Rust?

Flowing out from the three principles discussed in the last section are three overarching features of the language:

- Performance
- Concurrency
- Memory efficiency

### **1.5.1 Performance**

Svelte programs run fast. Yet the speed of the CPU is fixed. Thus, for software to run faster, it needs to do less. To achieve this, Rust pushes the burden of its high level features onto the compiler. Famously, Rust does not need a garbage collector to ensure safety.

Rust also has some less obvious tricks. An object's methods are always dispatched statically, unless dynamic dispatch is explicitly requested. This enables the compiler to heavily optimize code, sometimes to the point of eliminating the cost of the function call entirely.

### **1.5.2 Concurrency**

Asking a computer to do more than one thing at the same time has proven very difficult for software engineers to do. As far as an operating system is concerned, two independent threads of execution are at liberty to destroy each other if a programmer makes a serious mistake. Yet Rust has spawned the saying "fearless concurrency". Its emphasis on safety crosses the bounds of independent threads. There is no global interpreter lock (GIL) to constrain a thread's speed. We explore some of the implications of this in Part 2.

### **1.5.3 Memory Efficiency**

Rust enables you to create programs that require minimal memory. High-level constructs such as objects can be created with minimal overhead and may be optimized away.

## **1.6 Downsides of Rust**

It's easy to talk about this language as if it is the panacea of all software engineering. The (sometimes overstated) slogans are great. "High level syntax with low level performance!" "Concurrency without crashes!" "C with perfect safety!" For all of its merits, Rust does have disadvantages.

### **1.6.1 Compile Times**

Rust is slower at compiling code than its peer languages. It has a complex compiler toolchain that includes multiple intermediate representations and sending lots of code to LLVM. The "unit of compilation" for a Rust program is not an individual file, but a whole package (known affectionately as a "crate"). As crates can include multiple modules, they can be very large units of compilation. This enables whole-of-crate optimization, but requires whole-of-create compilation as well.

## 1.6.2 Strictness

Rust is a bit of a stickler. It's impossible—well, very difficult—to be lazy when programming with it. Programs won't compile until everything is just right.

Over time, it's likely that you'll come to appreciate this feature. If you've ever programmed in a dynamic language, then surely you would have encountered the frustration of your program crashing because of a misnamed variable. Rust brings that frustration sooner. But at least your users don't have to experience the frustration of things crashing.

## 1.6.3 Size of the Language

The language is large. It has a type system, multiple ways to gain access to values, an ownership system that is paired with enforced object lifetimes. The language is also comprehensive. The snippet below, seen before at Listing 1.3, probably caused a degree anxiety. It's fairly overwhelming.

```
use std::rc::Rc;
use std::sync::{Arc, Mutex};

fn main() {
    let a = 10;                                ①
    let b = Box::new(20);                      ②
    let c = Rc::new(Box::new(30));              ③
    let d = Arc::new(Mutex::new(40));           ④
    println!("a: {:?}", a, b, c, d);
}
```

- ① An integer on the stack
- ② An integer on the heap, also known as a "boxed integer"
- ③ A boxed integer wrapped within a reference counter
- ④ An integer protected by a mutual exclusion lock, wrapped in an atomic reference counter

The downside of allowing full control is that programmers have the burden of choice. Exactly which integer type you should choose depends on the problem at hand.

## 1.6.4 Hype

"Have you considered rewriting this in Rust?" The Rust community is very wary of growing too quickly and being consumed by hype. Yet, a number of software projects have encountered a question on their mailing list or issue tracker recommending a complete rewrite in a new language.

Software written in Rust is not immune to security problems. By 2015, as Rust gained prominence, implementations of SSL/TLS, namely OpenSSL and Apple's own fork, were found to have serious security holes. Known informally as "Heartbleed" and

"goto fail", both exploits provide opportunities to test Rust's claims of memory safety. Rust is likely to have helped in both cases, but it is still possible to write Rust code that suffers from similar issues.

### Heartbleed

Heartbleed was caused to the re-use of a buffer, i.e. an array of bytes set aside for taking input. Buffers are re-used to minimize the number of times an application must request memory from the operating system. We can create a similar situation fairly easily in Rust that leads to similar problems.

Imagine that we wished to store information from multiple User objects. We decide, for whatever reason, it re-use a single buffer through the course of the program. If we don't reset this buffer once we have made use of it, information from earlier calls leaks to the latter ones.

Here is a précis of a program that would encounter this error:

```
let buffer = &mut[0u8; 1024];    ①
read_secrets(&user1, buffer);  ②
store_secrets(buffer);

read_secrets(&user2, buffer);  ③
store_secrets(buffer);
```

- ① This reads "bind a reference (&) to a mutable (mut) array ([...]) that contains 1024 unsigned 8-bit integers (u8) initialized to 0 to the variable buffer."
- ② buffer is filled with bytes from the user1 object
- ③ buffer still contains data from user1 that may or may not be overwritten by user2

Rust does not protect you from logical errors. Rust ensures that your data is never able to be written in two places at the same time. It does not ensure that your program is free from all security issues.

### goto fail

The "goto fail" bug was caused by programmer error coupled with design issues with C and potentially its compilers for not pointing out the flaw. A function that was designed to verify a cryptographic key pair ended up skipping all checks. Here is a selected extract from the function at hand, with a fair amount of obfuscatory syntax retained.

```
static OSStatus
SSLVerifySignedServerKeyExchange(SSLContext *ctx, bool isRsa, SSLBuffer
signedParams,
                                uint8_t *signature, UInt16 signatureLen)
{
    OSStatus      err;    ①
```

```

...
if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)    ②
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
    goto fail;
    ③
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
    goto fail;

err = sslRawVerify(ctx,
                    ctx->peerPubKey,
                    dataToSign,           /* plaintext */
                    dataToSignLen,        /* plaintext length */
                    signature,
                    signatureLen);

if(err) {
    sslErrorLog("SSLDecodeSignedServerKeyExchange: sslRawVerify "
                "returned %d\n", (int)err);
    goto fail;
}

fail:
SSLFreeBuffer(&signedHashes);
SSLFreeBuffer(&hashCtx);
return err;   ④
}

```

- ① Initialization of the OSStatus object with a "pass" value, e.g. 0
- ② A series of defensive programming checks
- ③ Unconditional goto, meaning substantive check at `sslRawVerify()` is always skipped
- ④ Return the "pass" value of 0, even for inputs that should have failed the verification test

The issue lies between lines 11 & 13. In C, logical tests do not require brackets. C compilers interpret those three lines like this:

```

if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0) {
    goto fail;
}
goto fail;

```

Would Rust have helped? Probably. In this specific case, Rust's grammar would have caught the bug. It does not allow logical tests without parentheses. Rust also issues a warning when code is unreachable. But that doesn't mean the error is made impossible in Rust. Stressed programmers under tight deadlines make mistakes. In the general case, code would compile and run.

Code with caution.

## **1.7 Where does Rust fit best?**

Rust is a general purpose language that can be successfully deployed in many areas.

Its headline domain is *systems programming*, an area most prominently occupied by C & C++. Yet the boundary of that domain is quite porous. Historically, it would have covered software such as operating systems, compilers, interpreters, file systems and device drivers. Now, it would also include web browsers and other software, even if it are user-facing. With that in mind, where does Rust shine?

### **1.7.1 Data Processing**

Rust is extremely good at text processing and data wrangling. As of mid-2017, it touts the world's fastest regular expression engine. Its type system and memory control provide you with the ability to create high-throughput data pipelines with low and stable memory footprint. Small filter programs can be easily embedded into a larger framework via Apache Storm or Apache Kafka.

### **1.7.2 Extending an Application**

Rust is well suited for extending programs written in a dynamic language. This enables "Ruby gems in Rust", "Python C Extensions in Rust" or "Erlang/Elixir NIFs written in Rust". C extensions are typically a scary proposition. They tend to be quite tightly integrated with the runtime. Make a mistake and you could be looking at runaway memory consumption due to a memory leak or a complete crash. Rust takes away a lot of this fear.

### **1.7.3 Operating in Resource-constrained Environments**

C has been the domain of microcontrollers for decades. The Internet of Things is coming and that means many billions of insecure devices exposed to the network. Any input parsing code will be routinely probed for weaknesses, given how infrequently devices have their firmware updated. Rust can play an important role by adding a layer of safety without imposing runtime costs.

### **1.7.4 Applications**

There is nothing inherent in Rust's design that prevents it from being deployed to develop user-facing software. Servo, the web browser engine that acted as an incubator for Rust's early development, is a user-facing application.

#### **DESKTOP**

There is still a large space for applications to be written that live on people's computers. Desktop applications are often complex, difficult to engineer and difficult to support. With Rust's ergonomic approach to deployment, its rigor, it is likely to become many applications' secret sauce. To start, they will be built by small, indie developers. As Rust matures, so will the ecosystem.

## MOBILE

Android, macOS and other smart phone operating systems generally provide a blessed path for developers. In the case of Android, that path is Java. In the case of macOS, developers generally program in Swift. There is however, another way.

Both platforms provide the ability for "native applications" to run on the system. This is generally intended for applications written in C++, such as games, to be able to be deployed on people's phones. Rust is able to talk to the phone via the same interface with no additional runtime cost.

## WEB

As you'll be very aware, JavaScript is the language of the web. Over time though, this will change. Browser vendors are developing a standard called WebAssembly, which promises to be a compiler target for many languages. Rust is one of the first. Porting a Rust project to the browser requires two additional commands on the command line.

### **1.7.5 Systems Programming**

In some sense, systems programming is Rust's raison d'être. Many large programs have been implemented in Rust, including compilers (Rust itself), video game engines and operating systems. The Rust community includes writers of parser generators, databases and file formats. Rust has proven to be a productive environment for programmers who share Rust's goals.

## **1.8 Rust's hidden feature: its community**

It takes more than software to grow a programming language. One of the things that the Rust team has done extraordinarily well is to foster a positive and welcoming community around the language. Everywhere you go within the Rust world, you'll find that you'll be treated with courtesy and respect.

## **1.9 A Taste of the Language**

This section is a chance to experience Rust face to face. We start by understanding how to use the compiler, then move on to writing full programs.

### **1.9.1 Cheating Your Way To "Hello, world!"**

The first thing that most programmers will do when they reach for a new programming language is to learn how to print "Hello, world!" to the console. You'll do that too, but with flair. You'll be verifying that everything is in working order before you start encountering annoying syntax errors.

If you are on Windows, please open the Rust Command Prompt that is available in the Start menu after installing Rust. Please then execute the command:

```
C:\> cd %TMP%
```

If you are running Linux or OS X, please open a Terminal Window. Once open, please

enter the following:

```
$ cd /tmp
$
```

From this point onwards, the commands for all operating systems should be the same. If you have installed Rust correctly, the following three commands will produce "Hello, world!" on the screen (as well as a bunch of other output).

```
$ cargo new --bin hello
$ cd hello
$ cargo run
```

Here is an example of what the whole process looks like on Windows running Rust 1.12:

```
C:\> cd %TMP%
C:\Users\Tim\AppData\Local\Temp\> cargo new --bin hello
    Created binary (application) `hello` project
C:\Users\Tim\AppData\Local\Temp\> cd hello
C:\Users\Tim\AppData\Local\Temp\hello\> cargo run
    Compiling hello v0.1.0 (file:///C:/Users/Tim/AppData/Local/Temp/hello)
        Finished debug [unoptimized + debuginfo] target(s) in 2.36 secs
            Running `target\debug\hello.exe`
Hello, world!
```

If you have reached this far, fantastic! You have been able to run your first Rust code without needing to write any Rust.

Let's take a look at what's just happened. cargo a tool that provides both a build system and package manager. That is, cargo knows how to execute rustc (the Rust compiler) to convert your Rust code into executable binaries or shared libraries.

Cargo understands things such as the difference between debug build and a release build. It also knows how to manage 3rd party libraries, called crates in Rust. It can assist you to incorporate them into your project by automatically downloading the correct version from crates.io. One of its other miscellaneous tasks is to help you out when you create a new project by creating a boilerplate program.

The first line has four parts. The command "cargo", a subcommand "new", a parameter "hello" and an option "--bin". These four parts together should be read as, "cargo, please create a new project called hello I can run as a binary application".

```
[todo: hedgehog diagram]
cargo new --bin hello
|   |   \--> call the project "hello"
|   \-----> make this an executable binary
\-----> create a new project
```

Cargo then goes and creates a project for you that follows a standard template that all Rust crates follow. After completing the `cargo new` command, your directory structure will have been changed to something that looks like this:

```
$ tree hello
hello
├── Cargo.toml
└── src
    └── main.rs

1 directory, 2 files
```

All Rust crates have the same structure. In their base directory, a file called `Cargo.toml` describes the project's metadata, such as the project's name, its version and its dependencies. Source code appears in the `src/` directory. Rust source code files use the `.rs` file extension.

The next command that you executed was `cargo run`. This line is much simpler to grasp for you, but there was actually much more work being by cargo. You asked cargo to run the project. As there was nothing to actually run when you invoked the command, it decided to compile the code on your behalf in debug mode to provide maximal error information. As it happens, `src/main.rs` always includes a "Hello, world!" stub. The result of that compilation was a file called `hello` (or `hello.exe`). `hello` was executed and the result was printed to your screen.

For the curious, our project's directory structure has changed a great deal. We now have a `Cargo.lock` file in the base of our project and a `target/` directory. Both that file and the directory are cargo's domain. We won't need to touch them. They are artifacts of the compilation process. `Cargo.lock` is a file that specifies the exact version numbers of all the dependencies so that future builds are reliably built the same way until `Cargo.toml` is modified.

```
$ tree --dirsfirst hello
hello
├── src
│   └── main.rs
├── target
│   └── debug
│       ├── build
│       ├── deps
│       ├── examples
│       ├── native
│       └── hello
└── Cargo.lock
└── Cargo.toml
```

Well done for getting things up and running. Now that we've cheated our way to "Hello, World!", let's get there via the long way.

## 1.9.2 Your First Rust Program

We want to write a program that will output the following text:

```
Hello, world!
Grüß Gott!
ハロー・ワールド
```

You have probably seen the first line in your travels. The other two are there to highlight few of Rust's features: easy iteration and built-in support for Unicode.

We will use cargo, as in the previous section. To start, open a console window. Move into a temporary directory (`cd /tmp/` or `cd %TMP%` on Windows).

```
$ cargo new --bin hello2
$ cd hello2
```

Now open `hello2/src/main.rs` in a text editor. Replace the text with in that file with the following:

**Listing 1.4. Hello World In Three Languages (ch1-hello2.rs)**

```
fn greet_world() {
    println!("Hello, world!"); // our old friend. ①

    let southern_germany = "Grüß Gott!"; ②
    let japan = "ハロー・ワールド"; ③

    let regions = [southern_germany, japan]; ④

    for region in regions.iter() { ⑤
        println!("{}", &region);
    }
}

fn main() {
    greet_world();
}
```

① The exclamation mark here indicates the use of a macro, which we discuss shortly

② Assignment in Rust, more properly called variable binding, uses the `let` keyword

③ Unicode support out of the box

④ Array literals

⑤ "Borrow" the `region` variable by taking a reference, providing fast read-only access to its contents

Now that our code is updated, run `cargo run` from the `hello2/` directory. You should be presented with three greetings.

Let's take a few moments to touch on some of the elements Listing 1.4.

One of the first things that you are likely to notice is that strings in Rust are able to

include a wide range of characters. Strings are UTF-8. This means that you are able to use non-English languages with relative ease.

The one character that might look out of place is an exclamation mark after `println`. If you have programmed in Ruby, you may be used to thinking that it is used to signal a destructive operation. In Rust, it signals the use of a macro. Macros can be thought of as sort of fancy functions for now. They offer the ability to avoid boilerplate code. In the case of `println!`, there is a bunch of type detection going on under the hood so that arbitrary data types can be printed to the screen.

You are likely to have heard that Rust is a "systems" programming language. Typically defined, a systems programming language is "low level" and "close to the metal". Languages defined in these terms have tended to be fairly unwieldy, with the reward being that they're very powerful.

If you are familiar with the internals of programming languages such as Perl, Ruby, Python, Java and JavaScript, you may have come across the term "garbage collector". A garbage collector is a service that tells the operating system that one of your variables has left scope and the memory allocated to your program is able to be used by others.

Garbage collection is extremely convenient, but imposes a cost in that your programs must run more slowly as they are doing extra work to check which variables are still needed as your program runs. Rust has no garbage collector, but still offers the convenience of one.

One of the things that may be apparent if you have been reading about Rust for a long time is that we haven't added any type annotations to our example code. Rust is statically typed. That means, the behavior of all data is defined in advance of the program being run and that behavior is well specified. Yet, Rust has a very smart compiler. That compiler doesn't always need to be told about the data types that it encounters.

## 1.10 Rust phrase book



What do members of the Rust community mean when they use these terms?

### **Enabling Everyone**

All programmers, regardless of ability or background are welcome to participate. Programming, and particularly systems programming, should not be restricted to a blessed few.

### **Blazingly fast**

Rust is a fast programming language. You'll be able to write programs that match or exceed the performance of its peer languages, but you will have more safety guarantees.

### **Fearless concurrency**

Concurrent and parallel programming has always been seen as difficult. Rust frees you from whole classes of errors that have plagued its peer languages.

### **No Rust 2.0**

Code written today will always compile with a future Rust compiler. Rust is intended to be a reliable programming language that can be depended upon for decades to come. In accordance with *semantic versioning*, Rust will never be backwards incompatible, therefore will never release a new major version.

### **Zero-cost abstractions**

The features you gain from Rust impose no runtime cost. When you program in Rust, safety does not sacrifice speed.

## 1.11 Summary

This chapter you learned that:

- Many companies have successfully built large software projects in Rust.
- Software written in Rust can be compiled to the PC, the browser, the server, as well as mobile and IoT devices.
- The language is well loved by software developers. It has repeatedly won Stack Overflow's "most loved programming language" title.
- Rust allows you to experiment without fear. It provides correctness guarantees that other tools are unable to provide without imposing runtime costs.
- There are three main command line tools to learn:
  - `cargo`, which manages a whole crate
  - `rustup`, which manages Rust installations
  - `rustc`, which manages compilation of Rust source code
- Rust projects are not immune from all bugs.

# 2

## Language Foundations

### **This chapter covers:**

- Getting to grips with Rust syntax
- Learning the fundamental types and data structures
- Building command line utilities
- Compiling programs

This chapter introduces you to the fundamentals of Rust programming. By the end of the chapter, you will be able to create command line utilities and should be able to get the gist most Rust programs. We'll be working through most of the language's syntax, but deferring much of the detail about *why* things are how they are for later in the book.

This chapter is intended for programmers who have experience with another programming language. If you are an experienced Rust programmer, feel free to skim or skip this chapter.

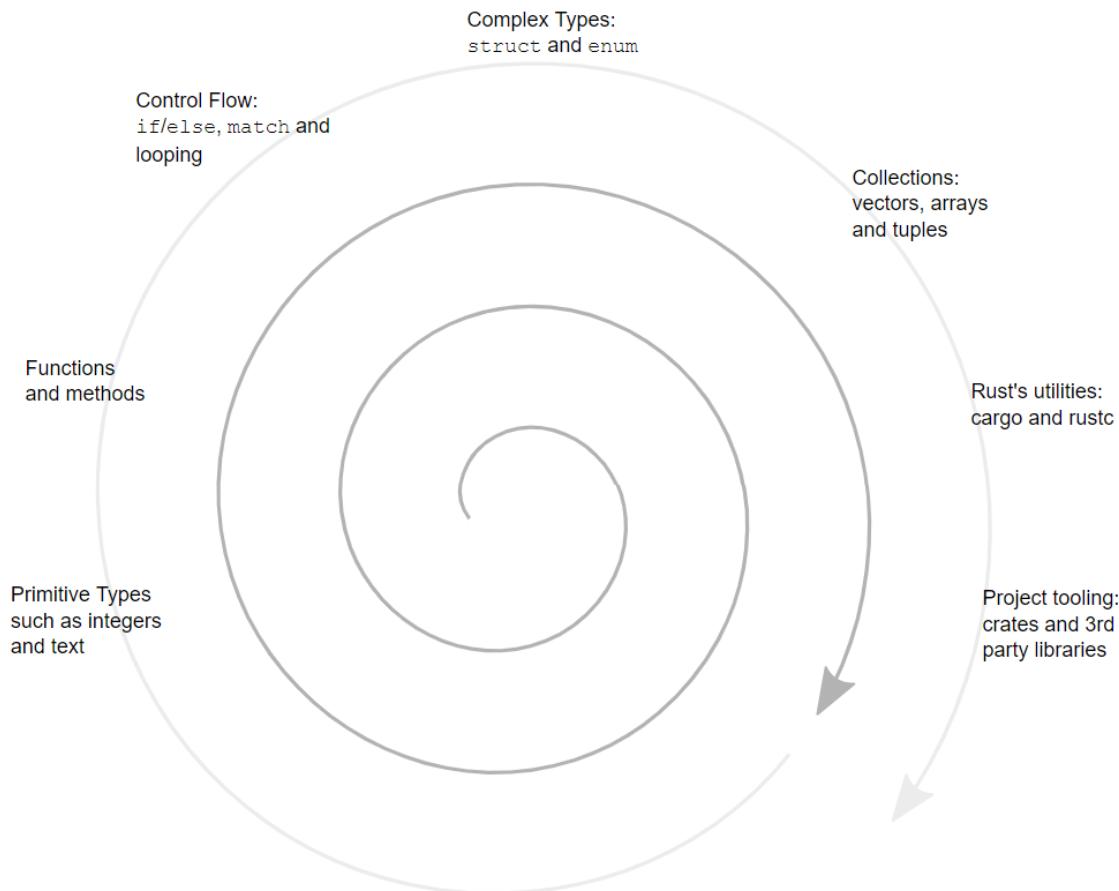
We will be building `grep-lite`, a much stripped down version of the ubiquitous `grep` utility. `grep-lite` looks for patterns within text, printing lines that match the pattern. The conceptual simplicity of this model will allow us to focus on the unique features of Rust.

**TIP****Beginners Are Welcome**

Rust's community strives to be welcome and responsive to newcomers. At times, you may strike a mental pothole when you encounter terms such as "lifetime elision", "hygienic macros" and "algebraic types" without context. Don't be afraid to ask for help. The community is much more welcoming than these helpful, yet opaque, documents may suggest.

The chapter takes a spiral approach to learning. A few concepts will be discussed multiple times. With each iteration, you will find yourself learning more. A completely unscientific map of the chapter is presented here:

**Figure 2.1. Chapter Topic Outline. Starting with Primitive Types, the chapter progresses through several concepts with increasing levels of depth.**



## 2.1 A Glance at Rust's Syntax

Rust tries to be boring and predictable where it can be. It has variables, numbers, functions and other familiar things that you would have seen in other languages. Its

blocks are delimited by curly brackets ({ and }), it uses a single equals sign as its assignment operator (=) and is whitespace agnostic.

## 2.2 A whole program with `main()`

Below is a short, yet complete Rust program. It prints `a + b = 30` to the console after guiding you through defining functions and using variables.

**Listing 2.1. Adding integers and using variables (ch2-first-steps.rs)**

```
fn main() {
    let a      = 10;          ①
    let b: i32 = 20;          ②

    let c = add(a, b);
    println!("a + b = {}", c);
}

fn add(i: i32, j: i32) -> i32 { ③
    i + j                  ④
}
```

- ① Types can be inferred by the compiler..
- ② ..or declared by the programmer when creating variables
- ③ Types are required when defining functions
- ④ Functions return the last expression's result, meaning `return` is not required (but be careful as adding a semi-colon to this line would change the semantics to `return ()` rather than `i32`)

Although only 11 lines of code, there is quite a lot packed into Listing 2.1. Here are some notes that should provide the gist of what's going on. We will cover the details in the rest of the chapter.

Line 1 (`fn main() {}`):

- The `fn` keyword begins a function definition.
- `main()` is the entrypoint to all Rust programs. It takes no arguments and returns no value.
- Code blocks, also known as *lexical scopes*, are defined with braces ({ & }).

Line 2 (`let a = 10;`):

- Use `let` to declare *variable bindings*. Variables are *immutable* by default, meaning that they are read-only rather than read/write.
- Statements are delimited with semi-colons ( ; ).

Line 3 (`let b: i32 = 20;`):

- You can designate a specific data type to the compiler. At times, this will be required as the compiler will be unable to deduce a unique type on your behalf.

Line 6 (`println!("a + b = {}", c);`):

- `println!()` is a *macro*. Macros are function-like, but return code rather than a value. In the case of printing, every data type has its own way of being converted to a string. `println!()` takes care of figuring out the exact methods to call on its arguments.
- Strings use double quotes ("") rather than single quotes ('')
- String formatting uses {} as a placeholder, rather than the C-like %s or other variants.

Line 9 (`fn add(...) → i32 {};`):

- Rust's syntax for defining functions should be legible to anyone who has worked with a typed programming before. Parameters are delimited by commas and types follow the variable names. The "dagger" or "thin arrow" syntax indicates return type, rather than the more traditional colon.

### **Compiling Code with `rustc`**

The Rust compiler `rustc` can be invoked to create a working executables from source code. To compile a single file of Rust code called `first-steps.rs` into a working program:

- Make sure that `first-steps.rs` includes a `main()` function
- Open a shell such as cmd.exe, bash or Terminal
- Move to the directory that includes `first-steps.rs`
- Execute the command `rustc first-steps.rs`

A file, `first-steps` (or `first-steps.exe`) has just been created. To execute it, enter `first-steps` on Windows or `./first-steps` on other operating systems.

Projects larger than a single file tend to be compiled with a higher-level tool called `cargo`. `cargo` understands whole crates and executes `rustc` on your behalf.

## **2.3 Starting out With Numbers**

Computers have been associated with numbers for longer than you have been able to say formula translator. Numeric literals for integers and floating point numbers are relatively straightforward.

The code below prints a single line to the console:

```
20; 21; 21; 1000000
```

### **Listing 2.2. Numeric Literals and Basic Operations in Rust (ch2-intro-to-numbers.rs)**

```
fn main() {
    let twenty = 20;                      ①
    let twenty_one: i32 = twenty + 1;      ②
    let floats_okay = 21.0;                ③
    let one_million = 1_000_000;           ④
```

```

    println!("{}; {}; {}; {}", twenty, twenty_one, floats_okay, one_million);
}

```

- ① Rust infers a type on your behalf if you don't supply one..
- ② ..which is done by adding type annotations (i32)
- ③ Floating point literals require no special syntax
- ④ Underscores can be used to increase readability and are ignored by the compiler

Rust also has built-in support for numeric literals that allow you to define literals in base 2 (binary), base 8 (octal) and base 16 (hexadecimal). This notation is also available within the formatting macros, such as `println!`. To demonstrate, the following output is produced by the code that follows.

```

3 30 300
11 11110 100101100
3 36 454
3 1e 12c

```

#### **Listing 2.3. Using Base 2, Base 8 and Base 16 Numeric Literals (ch2-non-base2.rs)**

```

fn main() {
    let three = 0b11;           ①
    let thirty = 0o36;          ②
    let three_hundred = 0x12C;   ③

    println!("{} {} {}", three, thirty, three_hundred);
    println!("{:b} {:b} {:b}", three, thirty, three_hundred);
    println!("{:o} {:o} {:o}", three, thirty, three_hundred);
    println!("{:x} {:x} {:x}", three, thirty, three_hundred);
}

```

- ① `0b` → **binary** (base 2)
- ② `0o` → **octal** (base 8)
- ③ `0x` → **hexidecimal** (base 16)

Rust contains a full complement of numeric types:

- `i8, i16, i32, i64` – signed integers ranging from 8-bit to 64-bit
- `u8, u16, u32, u64` – unsigned integers ranging from 8-bit to 64-bit
- `f32, f64` – floating point numbers in 32-bit and 64-bit variants
- `isize, usize` – integers that assume CPU's "native" width (e.g. in 64-bit CPUs, `usize` and `isize` will be 64 bits wide)

The number families are:

- signed integers (`i`) can represent negative as well as positive integers
- unsigned integer (`u`) can only represent positive integers but can count twice as high than their signed counterparts

- floating point (f) is able to represent real numbers and has special values for infinity, negative infinity and "not a number"

The widths are the number of bits that the type uses in RAM and in the CPU. Types that take up more space, such as `u32` vs `i8`, can represent more numbers at the expense of needing to store extra zeros for smaller numbers.

Number	Type	Bit Pattern in Memory
20	<code>u32</code>	<code>000000000000000000000000000010100</code>
20	<code>i8</code>	<code>0010100</code>

Although we've only touched on numbers, we nearly have enough exposure to Rust to create a prototype of our pattern matching program.

The listing below (which isn't yet runnable) will print 42 to the console when compiled. The syntax on line 6, e.g. `*item`, may be unfamiliar. `item` is a reference to some number within `haystack`. `*item == needle` asks Rust to compare the value referred to by `item` against `needle`. This is known as *de-referencing*.

#### Listing 2.4. Searching for an integer in an array of integers (ch2-needle-in-haystack.rs)

```
fn main() {
    let needle = 42;
    let haystack = [1, 1, 2, 5, 14, 42, 132, 429, 1430, 4862];      ①

    for reference in haystack.iter() {
        let item = *reference;
        if item == needle {                                         ②
            println!("{}: {}", item);                                ③
        }

        // if reference == &needle {                                ④
        //     println!("{}: {}", reference);
        // }
    }
}
```

- ① Array literal for a list of integers
- ② The `haystack.iter()` method returns an iterator over `haystack` that provides references to enabling access to individual elements
- ③ `item` is the value referred to by reference
- ④ This block provides an alternative form of the previous code. `reference == &needle` converts `needle` to a reference and compares against that.

This general pattern will come in handy as we look at more complex examples as the chapter progresses. Before looking at more complex types, let's take a moment to discuss one of Rust's more novel features - the `match` keyword.

## 2.4 Type-aware control flow with `match`

Let's say that we wanted to match against multiple patterns. While it's possible to use `if/else` blocks, these can become cumbersome and brittle. Rust's `match` keyword, analogous to other languages' `switch` keyword, can provide an alternative that is easier to read and more robust. Rust will ensure that you are testing against all possible values, meaning that corner cases do not occur. `match` returns when the first match is found.

The code below prints these two lines to the screen:

```
42: hit!
132: hit!
```

**Listing 2.5. Using the `match` keyword to match on multiple values (ch2-match-needles.rs)**

```
fn main() {
    // let needle = 42;           ①
    let haystack = [1, 1, 2, 5, 14, 42, 132, 429, 1430, 4862];

    for reference in haystack.iter() {
        let item = *reference;

        let result = match item {      ②
            42 | 132 => "hit!",     ③
            _ => "miss",           ④
        };

        if result == "hit!" {
            println!("{}: {}", item, result);
        }
    }
}
```

- ① The variable `needle` is now redundant
- ② `match` is an expression that returns a value that can be bound to a variable
- ③ `42 | 132` matches both `42` and `132`
- ④ `_` is a wildcard pattern that matches everything

`match` keyword plays an important role within the Rust language. Many control structures, such as looping, are defined in terms of `match` under the hood. They really shine when combined with the `Option` type that is discussed in depth next chapter.

Now that we have taken a good look at defining numbers and working with some of Rust's control flow mechanisms, let's move on to adding structure to programs with functions.

## 2.5 Getting Stuff Done With Functions

Since the introduction of structured programming, one of the fundamental abstractions

provided by programming languages has been the subroutine. In Rust, stand-alone subroutines are created as functions. Methods, that is functions tied directly to a specific object, also exist and will be discussed with `impl` (implementation) blocks.

Looking back to where the chapter begins, the snippet in Listing 2.1 contained a small function, `add()`. Repeated below, `add` takes two `i32` values and returns another:

**Listing 2.6. Extract of lines 9-11 from listing 2. 1.**

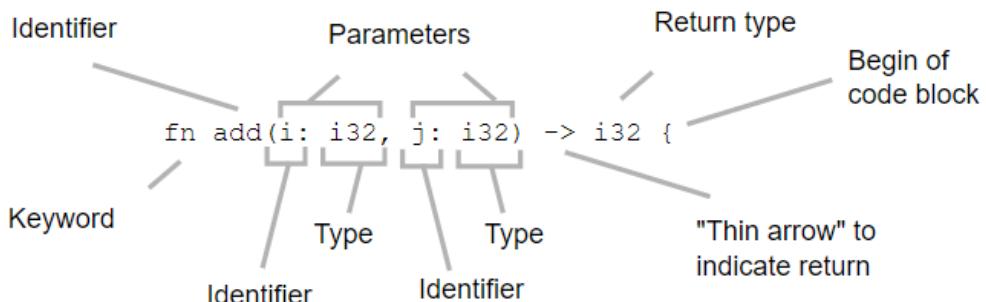
```
fn add(i: i32, j: i32) -> i32 {    ①
    i + j
}
```

- ① `add` takes two integer parameters and returns an integer. The two arguments will be bound to local variables `i` and `j`.

For the moment, let's concentrate on the syntax of each of the elements. As you will see shortly, Rust's function signatures can grow quite complex and therefore it pays to understand what's happening with simple ones. A visual picture of each of the pieces is provided below. Anyone who has programmed in a strongly typed programming language before should be able to squint their way through.

Rust's functions require that you specify your parameters' types and the function's return type.

**Figure 2.2. Rust's Function Definition Syntax**



### 2.5.1 Advanced Function Definitions

Rust's functions can also get somewhat scarier. To assist people who are reading more Rust source code than writing it, here is some extra content.

#### EXPLICIT LIFETIME ANNOTATIONS

As a bit of forewarning, allow me to introduce some more complicated notation. As you look through others' Rust code, you may encounter rune-like definitions like what happens:

**Listing 2.7. Type Signature of a function with lifetime explicit annotations**

```
add_with_lifetimes<'a, 'b>(i: &'a i32, j: &'b i32) -> i32 ① ②
```

① `<'a, 'b>` introduces the lifetimes `'a` and `'b` within the scope of `add_with_lifetimes()`

② `&'a i32` reads as "reference to an `i32` with lifetime `a`"

In general terms, this extra information is providing more specific information to the Rust compiler about data that lives outside the function. Functions that use references—denoted by the ampersands preceding the types—have data that exists outside of their scope.

Objects that live outside of a function are checked to make sure that accessing them is valid throughout that function. That is, Rust checks to make sure that all input data will live at least as long as the function that needs it. The details of what is happening is explained through the next few chapters, but here are some broad principles.

Underpinning Rust's safety checks is a *lifetime* system that tends to be able to work unaided. Usually, lifetime parameters do not need to be provided. Within the Rust community, this is known as *lifetime elision*. When they do—which is explained thoroughly in chapter 4—they appear within angle brackets: `<'a, 'b>`. The names `'a` and `'b` are arbitrary and local to this function. In essence, by saying that arguments `i` and `j` have lifetimes that are independent from one another.

Moving to the parameter list of `add_with_lifetimes()` on line 1, we see lots of noise. `i: &'a i32` reads as "variable `i` is a reference to a 32-bit integer with lifetime `'a`". At this stage, the we are actually describing to Rust where the lifetime parameters introduced in the angle brackets are actually used. Definitions can become more exotic with more parameters.

When used in complete example, as below, the you can see that no lifetime annotations are required when calling a function:

**Listing 2.8. Type Signature of a function with lifetime explicit annotations (ch2-add-with-lifetimes.rs)**

```
fn add_with_lifetimes<'a, 'b>(i: &'a i32, j: &'b i32) -> i32 {
    *i + *j ①
}

fn main() {
    let res = add_with_lifetimes(&10, &20); ② ③
    println!("{}", res);
}
```

① `*i + *j` indicates that we're adding the objects referred to by `i` and `j`, rather than adding the references directly

② `&10` and `&20` mean "reference to 10" and "reference to 20" respectively

③ No lifetime notation is required when calling a function

`*i + *j` on line 2 adds the dereferenced objects together, i.e. the referent values held by `i` and `j`. The use of references is an unfortunate necessity of introducing lifetimes, as lifetimes are not required for "normal" arguments.

## GENERIC FUNCTIONS

Another special case of function syntax appears when programmers write Rust functions to handle many possible input types. So far, we have seen functions that accept 32-bit integers (`i32`). Here is a function signature that can be called by many input types, as long as they are all the same:

### Listing 2.9. Type Signature of a Generic Function

```
fn add(i: T, j: T) -> T      ①
```

① `T` means for any type.

Capital letters in place of a type indicate a *generic* type. Conventionally, the variables `T`, `U` and `V` are used as placeholder values but this is arbitrary. `E` is often used to denote an error type. Generics enable significant code re-use and can greatly increase the usability of a strongly typed language.

Lastly, generic types can have some constraints placed on them. In our `add` example, we should ask the compiler to check that our input types support addition. To do that, programmers add *trait bounds* within angle brackets, before the parameter list.

### Listing 2.10. Type Signature of a Generic Function with Trait Bounds

```
fn add<T: Add<Output = T>>(i: T, j: T) -> T      ①
```

① `<T: Add<Output = T>>` requires that `T` must implement `Add` and that implementation outputs a value also of type `T`.

Trait bounds refer to *traits*. A trait is a language feature that is analogous to an interface or protocol in other domains. Traits are discussed in depth later on. For now, it will suffice to mention that traits enable commonality to exist between types.

A full example using the generic syntax, including trait bounds is provided in full below. The resulting executable prints out two lines to the screen:

```
1.2 + 3.4 = 4.6
10 + 20 = 30
```

### Listing 2.11. Full Example of Defining a Function with Generic Parameters and Trait Bounds

```
use std::ops::{Add};          ①

fn add<T: Add<Output = T>>(i: T, j: T) -> T {
    i + j
```

```

}

fn main() {
    let (a, b) = (1.2, 3.4);      ②
    let (x, y) = (10, 20);      ②

    let c = add(a,b);          ③
    let z = add(x,y);          ④

    println!("{} + {} = {}", a, b, c);
    println!("{} + {} = {}", x, y, z);
}

```

- ① Bring Add into scope
- ② Rust supports the ability to bind multiple variables to values via pattern matching
- ③ add() called with floating point values
- ④ add() called with integer values

As you can see, function signatures can become somewhat convoluted. Interpreting them can take some patience. Hopefully you now have the tools to break the pieces apart in case you get stuck down the track.

Here are a few principles that should assist:

- Terms in lower case (i, j) denote variables
- Single upper case letters (T) denote generic type variables
- Terms beginning with upper case (Add) are traits and specific types, such as `String`
- Labels ('a) denote lifetime parameters

## 2.6 *Creating grep-lite v1*

You don't have much exposure to the language yet. Still, it's probably enough to get through a simple example.

The code below is our first iteration of grep-lite. Its hard-coded parameters restrict its flexibility somewhat, but they are useful illustrations of string literals.

It prints a line to the console:

```
dark square is a picture feverishly turned--in search of what?
```

**Listing 2.12. Searching for a simple pattern within lines of a string (ch2-str-simple-pattern.rs)**

```

fn main() {
    let search_term = "picture";
    let quote = "Every face, every shop, bedroom window, public-house, and
dark square is a picture feverishly turned--in search of what?
It is the same with books. What do we seek through millions of pages?"; ①
}

```

```

for line in quote.lines() {    ②
    if line.contains(search_term) {
        println!("{}", line);
    }
}

```

- ① Multi-lined strings do not require special syntax
- ② Objects in Rust have methods; strings provide an iterator of lines

As you can see, Rust's strings can do quite a lot by themselves. Line 7 of Listing 2.12 demonstrates platform-independent line-by-line iteration. Line 8 demonstrates searching for text using method syntax. From here, let's expand the functionality of our proto-application.

### **Navigating Rust's Rich Collection of String Types**

Strings are somewhat complicated for newcomers to Rust. Implementation details tend to bubble up from below and cloud comprehension.

`String` and `str` both exist, yet are distinct types. Interacting with values from both types can be an annoying exercise at first, as different methods are required to perform similar actions. Prepare yourself for irritating type errors as your intuition develops.

`str` is a high-performance, relatively feature-poor type. Once created, `str` data is not copied when it is re-used. This minimizes the interaction between the program and the operating system, resulting in faster runtime performance. It is also the type of string literals.

A `String` is (probably) closest to what you know as a string type from other languages. It supports modification, including expanding and contraction over time. `String` is an *owned* type. This term has a particular meaning within Rust. Owned values are guaranteed to live as long as their sole owner. In essence, owners must live long enough to destroy their data when it is no longer needed such as when it falls out of scope.

`str` is usually seen in its referenced form `&str` and `&str` is referred to as a "string slice". The full type designation of is `'static &str`. The `'static` lifetime is somewhat special. It too owes its name to implementation details. Executable programs can contain a section of memory that is hard-coded with values. That section is known as static memory, as it is read-only during execution.

Some other types may be encountered in your travels:

- `char`: a single character, encoded as 4 bytes (equivalent to UTF-32). This differs from `&str` and `String`, which encodes single characters as UTF-8. Conversion does impose a penalty, but means that `char` values are of fixed-width and are therefore easier for the compiler to reason about. Characters encoded as UTF-8 can span 1-4 bytes.
- `[u8]`: a slice of raw bytes, usually found when dealing with streams of binary data.
- `std::ffi::OSString`: a platform-native string, very close in behavior to `String`, but without a guarantee that it's encoded as UTF-8 and won't contain the zero byte (`0x00`).

Fully understanding the distinction between `String` and `&str` requires knowledge of arrays and vectors. Textual data is very similar to these two types, with added convenience methods applied over the top.

Let's start adding functionality by printing out the line number, along with the match. This is equivalent to the `-n` option within the POSIX.1-2008 standard for the `grep` utility ([pubs.opengroup.org/onlinepubs/9699919799/utilities/grep.html](http://pubs.opengroup.org/onlinepubs/9699919799/utilities/grep.html)).

Adding a few lines to our previous example, we now see the following line printed to the screen:

```
2: dark square is a picture feverishly turned--in search of what?
```

**Listing 2.13. Searching for a pattern within a string and printing line numbers by manually incrementing a variable (ch2-simple-with-linenums.rs)**

```
fn main() {
    let search_term = "picture";
    let quote = "Every face, every shop, bedroom window, public-house, and
dark square is a picture feverishly turned--in search of what?
It is the same with books. What do we seek through millions of pages?";
    let mut line_num: usize = 1;                      ①

    for line in quote.lines() {
        if line.contains(search_term) {
            println!("{}: {}", line_num, line);      ②
        }
        line_num += 1;                           ③
    }
}
```

- ① We declare `line_num` as *mutable* via `let mut` and initialize it with 1
- ② Our `println!` macro is updated to allow for both values to be printed
- ③ Increment `line_num` in-place

Another approach to achieving this that demonstrates more of Rust's syntax follows. The output is the same, but here the code makes use of the `enumerate()` method and method chaining. `enumerate()` takes an iterator `I`, returning another `(N, I)`, where `N` is a number that starts at 0 and increments by 1 each iteration.

**Listing 2.14. Searching for a pattern within a string and printing line numbers by using the `enumerate()` method (ch2-simple-with-enumerate.rs)**

```
fn main() {
    let search_term = "picture";
    let quote = "Every face, every shop, bedroom window, public-house, and
dark square is a picture feverishly turned--in search of what?
It is the same with books. What do we seek through millions of pages?";

    for (idx, line) in quote.lines().enumerate() {      ①
        if line.contains(search_term) {
            let line_num = idx + 1;                     ②
            println!("{}: {}", line_num, line);
        }
    }
}
```

- ① As `lines()` returns an iterator, it can be chained with `enumerate()`

- ② To calculate the line number, we perform addition here avoiding calculations at every step

Another feature of grep that is extremely useful is to print out some context before and after the line that matches. In the GNU grep implementation, this is the `-C NUM` switch. To add support for that feature, we need to be able to create lists.

## 2.7 Making Lists of Things with Arrays, Slices and Vectors

Lists of things are incredibly common. The two types that you will be working with most often are arrays and vectors. Arrays are fixed-width and extremely lightweight. Vectors are growable, but incur a small runtime penalty because of extra bookkeeping that they do. As the underlying mechanisms with text data in Rust, it helps to have a cursory understanding of what is happening.

The goal of this section is to support printing out  $n$  lines of context that surround a match. To get there, we will need to segue somewhat and explain what *arrays*, *slices* and *vectors* are. The most useful type for this exercise is the vector. To learn about vectors though, we need to start by learning about its two simpler cousins.

### 2.7.1 Arrays

An array, at least as far as Rust is concerned, is a tightly packed collection of the same thing. It's possible to replace items within an array, but its size may not change. Because variable-length types such as `String` add a degree of complication, we'll revert back to discussing numbers for a little while.

Creating arrays takes two forms. We can provide a comma-delimited list within square brackets, e.g. `[1, 2, 3]`, or a *repeat expression*, e.g. `[0; 100]`, where you provide two values delimited by a semi-colon: the left value is repeated by the number of times on the right. Both variations support you providing an explicit type signature.

An example showing all four variations is provided below. It prints the following 4 lines to the console:

<code>[1, 2, 3]:</code>	<code>1 + 10 = 11</code>	<code>2 + 10 = 12</code>	<code>3 + 10 = 13</code>	<code>(Σ[1, 2, 3] = 6)</code>
<code>[1, 2, 3]:</code>	<code>1 + 10 = 11</code>	<code>2 + 10 = 12</code>	<code>3 + 10 = 13</code>	<code>(Σ[1, 2, 3] = 6)</code>
<code>[0, 0, 0]:</code>	<code>0 + 10 = 10</code>	<code>0 + 10 = 10</code>	<code>0 + 10 = 10</code>	<code>(Σ[0, 0, 0] = 0)</code>
<code>[0, 0, 0]:</code>	<code>0 + 10 = 10</code>	<code>0 + 10 = 10</code>	<code>0 + 10 = 10</code>	<code>(Σ[0, 0, 0] = 0)</code>

**Listing 2.15. Defining Arrays and Iterating Over Their Elements**

```
fn main() {
    let one          = [1,2,3];      ①
    let two: [u8; 3] = [1,2,3];    ②
    let blank1       = [0; 3];      ③
    let blank2: [u8; 3] = [0; 3];  ④

    let arrays = [one, two, blank1, blank2];
}
```

```

for a in &arrays {                      ⑤
    print!("{}: ", a);
    for n in a.iter() {                 ⑥
        print!("\t{} + 10 = {}", n, n+10);
    }

    let mut sum = 0;
    for i in 0..a.len() {               ⑦
        sum += a[i];
    }
    print!("\t(\u2211{} = {})", a, sum);
    println!("");
}
}

```

- ① [1,2,3] denotes an *array literal* and Rust infers its type itself (probably [i32; 3])
- ② [u8; 3] explicitly declares type of the array: 3 elements of u8
- ③ This form is known as a *repeat expression* ([0; 3]) that expects a constant (0) to be repeated  $n$  times.
- ④ Type signatures are also supported for repeat expressions
- ⑤ Taking a reference to an array returns a slice. Slices support iteration through arrays without needing to call `iter()`.
- ⑥ Arrays also have methods for iteration and manipulation
- ⑦ All array indexing is bounds checked. Requesting an item that's out of bounds will lead to a runtime panic.

Arrays are a simple data structure from the machine's point of view. They are a contiguous block of memory with elements of a uniform type.

The simplicity is still somewhat deceptive. Arrays can cause a few learning difficulties for newcomers.

- The notation can be confusing. [T; n] describes an array's type, where T is the elements' type and n is a non-negative integer. [f32; 12] denotes an array of 12 32-bit integers. It's easy to get confused with slices [T], which do not have a compile-time length.
- [u8; 3] is a different type than [u8; 4]. That is, the size of the array matters to the type system.
- In practice, most interaction with arrays occurs via another type called a *slice* ([T]) that is itself interacted with by reference (&[T]). And to add some linguistic confusion into the mix, both slices and references to slices are both called slices.

**NOTE**

For readers with a background in systems programming, Rust arrays are different from their C counterparts in important ways. Rust arrays are allocated on the stack like other value types. This means that Rust programmers access items directly, rather than via a pointer. There is no pointer arithmetic needed in your code. The compiler knows the size of an array's members and calculates memory offsets itself.

## 2.7.2 Slices

Slices are *dynamically sized* array-like objects. The term *dynamically sized* means that their size is not known at compile time. Yet, like arrays, they don't expand or contract. The use of the word *dynamic* in *dynamically sized* is closer in meaning to "dynamic typing" rather than movement. The lack of compile-time knowledge explains the distinction in the type signature between an array ( $[T; N]$ ) and a slice ( $[T]$ ).

Slices are important because it's easier to implement traits for slices than arrays. Traits are how Rust programmers add methods to objects. As  $[T; 1]$ ,  $[T; 2]$ , ...,  $[T; n]$  are all different types, implementing traits for arrays can become unwieldy. Creating a slice from an array is easy and cheap because it doesn't need to be tied to any specific size.

Another very important use for slices is their ability to act as a view on arrays (and other slices). The term "view" here is taken from database technology and means that slices can gain fast, read-only access of data without needing to copy anything around.

The rub with slices is that Rust wants to know the size of every object in your program and they're defined as not having a compile-time size. References to the rescue. As mentioned in the discussion about the use of the term *dynamically sized*, their size is fixed in memory. They're made up of two `usize` components (a pointer and a length). That's why you'll typically see slices referred to in their referenced form ( $\&[T]$ ), such as string slices that take the notation `&str`.

**NOTE**

**Don't worry too much about the distinctions between arrays and slices yet. In practice, it's not material. Each term is an artifact of implementation details. Those implementation details are important when dealing with performance-critical code, but not learning the basics of the language. Arrays are implemented as a reference and a length. A slice is similar to an array, but its length is not known at compile time.**

## 2.7.3 Vectors

Vectors (`Vec<T>`) are growable lists of  $T$ . Using vectors is extremely common in Rust code. They incur a small runtime penalty compared to arrays because of extra bookkeeping that they do to enable their size to change over time. But they often make up for it with their added flexibility.

The task at hand is to expand the feature set of the grep-lite utility. Specifically, we want the ability to store  $n$  lines of context around a match. Naturally, there are many ways to implement such a feature. To minimize code complexity, we'll use a two pass strategy. In the first pass, we'll tag lines that match. During the second pass, we'll collect lines that are within  $n$  lines of each of the tags.

The code example below is the longest you've seen so far. Take your time to digest the code. The most confusing syntax is probably `Vec<Vec<(usize, String)>>`, which appears on line 15. `Vec<Vec<(usize, String)>>` is a vector of vectors, e.g. `Vec<Vec<T>>` where `T` is of type `(usize, String)`. `(usize, String)` is a *tuple* and will be used to store line numbers along with the text that's near matches.

When the needle variable on line 4 is set to "oo", the following text is printed to the screen.

1: Every face, every shop,  
2: bedroom window, public-house, and  
3: dark square is a picture  
4: feverishly turned--in search of what?  
3: dark square is a picture  
4: feverishly turned--in search of what?  
5: It is the same with books.  
6: What do we seek  
7: through millions of pages?

## Listing 2.16. Enabling context lines to be printed out with a `Vec<Vec<T>>`, where `T` is a pair of values with line number and text (`usize, String`) (`ch2-introducing-vec.rs`)

```

// PASS 2
for (i, line) in haystack.lines().enumerate() {                      ⑦
    for (j, tag) in tags.iter().enumerate() {
        let lower_bound = tag.saturating_sub(context_lines);      ⑧
        let upper_bound = tag + context_lines;

        if (i >= lower_bound) && (i <= upper_bound) {
            let line_as_string = String::from(line);                ⑨
            let local_ctx = (i, line_as_string);
            ctx[j].push(local_ctx);
        }
    }
}

// OUTPUT
for local_ctx in ctx.iter() {
    for &(i, ref line) in local_ctx.iter() {                         ⑩
        let line_num = i + 1;
        println!("{}: {}", line_num, line);
    }
}
}

```

- ① `tags` holds line numbers where matches occur
- ② `ctx` contains a vector per match to hold that match's context lines
- ③ Iterate through the lines, recording line numbers where matches are encountered
- ④ `Vec::with\_capacity(n)` reserves space for  $n$  items
- ⑤ No explicit type signature is required here, as it can be inferred via the definition of `ctx` on line 15
- ⑥ When there are no matches, exit early
- ⑦ For each tag, at every line, check to see if we are nearby a match. When we are, add that line to the relevant `Vec<T>` within `ctx`.
- ⑧ `usize.saturating\_sub()` is subtraction that returns 0 on integer underflow rather than crashing the program (CPUs don't like attempting to send `usize` below zero)
- ⑨ Copy line into a new `String` and store that locally for each match
- ⑩ `ref line` informs the compiler that we wish to *borrow* this value, rather than *move* it. These two terms are explained fully later in later chapters.

`Vec<T>` will perform best when you can provide it with a size hint via `Vec::with_capacity()`. Providing an estimate minimizes the number of times that memory will need to be allocated from the operating systems.

**NOTE**

One thing to note when considering this approach in real text files is that encodings may cause issues. String is guaranteed to be UTF-8. Naïvely reading in a text file to a String will cause errors if invalid bytes are detected. A more robust approach is to read in data as [u8] (a slice of u8 values), then decode those bytes with help from your domain knowledge.

## 2.8 Including Third Party Code

Incorporating 3rd party code is essential to productive Rust programming. Rust's standard library tends to lack many things that other languages provide, such as random number generation and regular expression support.

To get your feet wet, you'll be including the regex crate into your program. Crates are the name the Rust community uses where others may use terms such as package, distribution or library. regex will provide you with the ability to match for regular expressions, rather than simply looking for exact matches.

To use 3rd party code, we'll rely on the cargo command line tool. Follow these instructions:

- Open a command prompt, using cmd.exe, bash, zsh or your own personal favorite
- cd /tmp (cd %TMP% on MS Windows)
- cargo new --bin grep-lite

You now should see the the following line appear:

```
Created binary (application) `grep-lite` project
```

Now, open the file /tmp/grep-lite/Cargo.toml in a text editor. The section [dependencies] should be updated to look like this:

```
[dependencies]
regex = "0.2.2"
```

We've now done all we need to do to enable cargo to pull down this code, all of its dependencies and have a working copy for our project. Open your command prompt again and execute these commands:

- cd /tmp/grep-lite (cd %TMP%\grep-lite on MS Windows)
- cargo build

You should see output fairly similar to this begin to appear:

```
Updating registry `https://github.com/rust-lang/crates.io-index`
Downloading regex v0.2.2
Downloading regex-syntax v0.4.1
Downloading libc v0.2.23
Downloading thread-id v3.1.0
  Compiling libc v0.2.23
  Compiling void v1.0.2
  Compiling regex-syntax v0.4.1
  Compiling utf8-ranges v1.0.0
```

```

Compiling unreachable v0.1.1
Compiling memchr v1.0.1
Compiling thread-id v3.1.0
Compiling thread_local v0.3.3
Compiling aho-corasick v0.6.3
Compiling regex v0.2.2
Compiling grep-lite v0.1.0 (file:///tmp/grep-lite)
    Finished dev [unoptimized + debuginfo] target(s) in 20.73 secs

```

Now that you have the crate installed and compiled, let's put it into action.

### 2.8.1 Adding Support for Regular Expressions

Regular expressions add great flexibility to the patterns that we are able to search for.

Here is a copy of an early example that we'll be modifying:

#### **Listing 2.17. Matching on exact strings**

```

fn main() {
    let search_term = "picture";
    let quote = "Every face, every shop, bedroom window, public-house, and
dark square is a picture feverishly turned--in search of what?
It is the same with books. What do we seek through millions of pages?";

    for line in quote.lines() {
        if line.contains(search_term) {
            println!("{}", line);
        }
    }
}

```

Make sure that you have updated `grep-lite/Cargo.toml` to include `regex` as a dependency as described in the previous section. Now, open `grep-lite/src/main.rs` in a text editor and fill it in with the following:

#### **Listing 2.18. Searching for patterns with regular expressions**

```

extern crate regex;      ①

use regex::Regex;        ②

fn main() {
    let re = Regex::new("picture").unwrap();    ③

    let quote = "Every face, every shop, bedroom window, public-house, and
dark square is a picture feverishly turned--in search of what?
It is the same with books. What do we seek through millions of pages?";

    for line in quote.lines() {
        match re.find(line) {                      ④
            Some(_) => println!("{}", line),      ⑤  ⑥
        }
    }
}

```

```
    None => (),
}
}
}
```

- ① Notify Rust to look outside of the standard library for this crate
  - ② Bring the `regex::Regex` type into local scope
  - ③ `unwrap()` "unwraps" a `Result`, crashing if an error occurs. Handling errors more robustly is discussed in depth later in the book.
  - ④ The `contains()` method has been replaced with a `match` block, which requires that we handle all possible cases
  - ⑤ `Some(T)` is the positive case of an `Option`. In this case means that `re.find()` has been successful.
  - ⑥ `_` is a wildcard, matching on all values
  - ⑦ `None` is the negative case of an `Option`
  - ⑧ `()` can be thought of as a null placeholder value here

Open a command prompt and move to the root directory of your grep-lite project. Executing `cargo run` should produce output similar to this:

**Listing 2.19. Output of cargo run**

```
$ cargo run
   Compiling grep-lite v0.1.0 (file:///tmp/grep-lite)
    Finished dev [unoptimized + debuginfo] target(s) in 1.38 secs
        Running `target/debug/grep-lite`
dark square is a picture feverishly turned--in search of what?
```

Admittedly, the code within Listing 2.18 hasn't taken significant advantage of its newfound regular expression capabilities. Hopefully you'll have the confidence to be able to slot them into some of the more complex examples.

### **2.8.2 Generating Crates' Documentation Locally**

Documentation for 3rd party crates is typically available online. Still, it can be useful to know how to generate a local copy in case the Internet fails you.

Move to the root of the project directory in a terminal, i.e. /tmp/grep-lite or %TMP%\grep-lite. Execute cargo doc.

**Listing 2.20. Output of cargo doc**

```
$ cargo doc
Documenting utf8-ranges v1.0.0
Documenting libc v0.2.23
Documenting regex-syntax v0.4.1
Documenting void v1.0.2
Documenting unreachable v0.1.1
Documenting memchr v1.0.1
Documenting thread-id v3.1.0
```

```
Documenting thread_local v0.3.3
Documenting aho-corasick v0.6.3
Documenting regex v0.2.2
Documenting grep-lite v0.1.0 (file:///tmp/grep-lite)
    Finished dev [unoptimized + debuginfo] target(s) in 10.0 secs
```

HTML documentation has now been created for you. By opening /tmp/grep-lite/target/doc/grep\_lite/index.html in a web browser (also try cargo doc --open), you'll be able to view the documentation for all crates that yours depends on. It's also possible to inspect the output directory to take a look at what is available to you:

```
$ tree -d -L 1 target/doc/
target/doc/
├── aho_corasick
├── grep_lite
├── implementors
├── libc
├── memchr
├── regex
├── regex_syntax
└── src
    ├── thread_id
    ├── thread_local
    ├── unreachable
    ├── utf8_ranges
    └── void
```

### 2.8.3 Managing Rust toolchains with rustup

`rustup` is another handy command line tool, along with `cargo`. Where `cargo` manages projects, `rustup` manages your Rust installation(s). `rustup` cares about "Rust toolchains" and enables you to move between versions of the compiler. This way it's possible to compile your projects for multiple platforms and experiment with nightly features of the compiler, while keeping the stable version nearby.

`rustup` simplifies the process for you to access Rust's documentation. Typing `rustup doc` will open your web browser to a local copy of Rust's standard library.

## 2.9 Supporting Command Line Arguments

Our program is rapidly increasing its feature count. Yet, there is no way for any options to be specified. To become an actual utility, `grep-lite` needs to be able to actually be able to interact with the world.

Sadly though, Rust has a fairly tight standard library. As with regular expressions, another area with relatively minimalist support is handling command line arguments. A nicer API is available through 3rd party crate called `clap` (among others). Now that we've seen how to bring in 3rd party code, let's take advantage of that to enable users of `grep-lite` to choose their own pattern. (We'll get to choosing their own input source in the next section.)

First, add `clap` as a dependency in your `Cargo.toml` file:

#### Listing 2.21. grep-lite/Cargo.toml

```
[package]
name = "grep-lite"
version = "0.1.0"
authors = ["Tim McNamara <code@timmcnamara.co.nz>"]

[dependencies]
regex = "0.2.2"
clap = "2.24.2"
```

Now, adjust `src/main.rs` to the following:

#### Listing 2.22. grep-lite/src/main.rs

```
extern crate clap;
extern crate regex;

use regex::Regex;
use clap::{App, Arg}; ①

fn main() {
    let args = App::new("grep-lite")
        .version("0.1")
        .about("searches for patterns")
        .arg(Arg::with_name("pattern")
            .help("The pattern to search for")
            .takes_value(true)
            .required(true))
        .get_matches();

    let pattern = args.value_of("pattern").unwrap(); ③
    let re = Regex::new(pattern).unwrap();

    let quote = "Every face, every shop, bedroom window, public-house, and
dark square is a picture feverishly turned--in search of what?
It is the same with books. What do we seek through millions of pages?";

    for line in quote.lines() {
        match re.find(line) {
            Some(_) => println!("{}", line),
            None => (),
        }
    }
}
```

① Bring the `clap::App` and `clap::Arg` objects into local scope

② Incrementally build up a command argument parser. Each argument takes an `Arg`. In our case we only need one.

- ③ Extract the pattern argument.

Running `cargo run` should set off a few lines in your console:

```
$ cargo run
    Finished dev [unoptimized + debuginfo] target(s) in 2.21 secs
      Running `target/debug/grep-lite`
error: The following required arguments were not provided:
  <pattern>

USAGE:
  grep-lite <pattern>

For more information try --help
```

The error is due to the fact that we haven't passed sufficient arguments through to our resulting executable. To pass arguments through, `cargo` supports some special syntax. Any arguments appearing after `--` are sent through to the result of the build.

```
$ cargo run -- picture
    Finished dev [unoptimized + debuginfo] target(s) in 0.0 secs
      Running `target/debug/grep-lite picture`
dark square is a picture feverishly turned--in search of what?
```

`clap` does more than provide parsing. It also generates usage documentation on your behalf. Running `grep-lite --help` provides an expanded view:

```
$ ./target/debug/grep-lite --help
grep-lite 0.1
searches for patterns

USAGE:
  grep-lite <pattern>

FLAGS:
  -h, --help      Prints help information
  -V, --version   Prints version information

ARGS:
  <pattern>      The pattern to search for
```

## 2.10 Reading From Files

Searching for text wouldn't be complete without being able to search within files. File I/O can be surprisingly finicky and so has been left until last.

Before adding the functionality to `grep-lite`, let's take a look at a standalone example. The general pattern is to open a `File` object, then wrap that in a `BufReader`. `BufReader` takes care of providing *buffered I/O*, which can reduce system calls to the operating system if the hard disk is congested.

**Listing 2.23. Reading a file line by line in Rust manually (ch2-read-file.rs)**

```
use std::fs::File;
use std::io::BufReader;
use std::io::prelude::*;

fn main() {
    let f = File::open("readme.md").unwrap();           ①
    let mut reader = BufReader::new(f);

    let mut line = String::new();                      ②
    loop {                                              ③
        let len = reader.read_line(&mut line).unwrap();  ④
        if len == 0 {
            break
        }

        println!("{} ({} bytes long)", line, len);

        line.truncate(0);                            ⑤
    }
}
```

- ① Creating a File requires a path argument and error handling in case the file does not exist. This program crashes if a "readme.txt" is not present.
- ② We'll re-use a single String object over the lifetime of the program
- ③ loop loops until the program encounters return, break or panics
- ④ Reading from disk can fail and we need to explicitly handle this. In our case, errors crash the program.
- ⑤ Shrink the String back to length 0, preventing lines from persisting into the following ones

Manually looping through a file can be cumbersome, despite its usefulness in some cases. For the common case of iterating through lines, Rust provides a helper iterator:

**Listing 2.24. Reading a file line by line via BufReader::lines() (ch2-bufreader-lines.rs)**

```
use std::fs::File;
use std::io::BufReader;
use std::io::prelude::*;

fn main() {
    let f = File::open("readme.md").unwrap();
    let reader = BufReader::new(f);

    for line_ in reader.lines() {          ①
        let line = line_.unwrap();         ②
        println!("{} ({} bytes long)", line, line.len());
    }
}
```

- ① There is a subtle behavior change here. `BufReader::lines()` removes the trailing newline character from each line
- ② Unwrapping the `Result` possible error at each line is still required, as with the manual version

We're now in a position to add reading from a file into 'grep-lite's feature list. The following listing creates a complete program that takes a regular expression pattern and an input file as arguments.

#### **Listing 2.25. grep-lite/src/main.rs**

```
extern crate clap;
extern crate regex;

use std::fs::File;
use std::io::BufReader;
use std::io::prelude::*;
use regex::Regex;
use clap::{App, Arg};

fn main() {
    let args = App::new("grep-lite")
        .version("0.1")
        .about("searches for patterns")
        .arg(Arg::with_name("pattern")
            .help("The pattern to search for")
            .takes_value(true)
            .required(true))
        .arg(Arg::with_name("input")
            .help("File to search")
            .takes_value(true)
            .required(true))
        .get_matches();

    let pattern = args.value_of("pattern").unwrap();
    let re = Regex::new(pattern).unwrap();

    let input = args.value_of("input").unwrap();
    let f = File::open(input).unwrap();
    let reader = BufReader::new(f);

    for line_ in reader.lines() {
        let line = line_.unwrap();
        match re.find(&line) { ①
            Some(_) => println!("{}", line),
            None => (),
        }
    }
}
```

① `line` is a `String` but `re.find()` takes `&str` as an argument

## 2.11 Reading from STDIN

A command line utility wouldn't be complete if it wasn't able to read from STDIN. Unfortunately for those readers who skimmed over earlier parts of this chapter, some of the syntax on line 11 might look quite unfamiliar. In short, rather than duplicate code within `main()`, we are using a generic function to abstract away the details of whether we are dealing with files or stdin.

```
extern crate clap;
extern crate regex;

use std::fs::File;
use std::io;
use std::io::BufReader;
use std::io::prelude::*;
use regex::Regex;
use clap::{App, Arg};

fn process_lines<T: BufRead + Sized>(reader: T, re: Regex) {
    for line_ in reader.lines() {
        let line = line_.unwrap();
        match re.find(&line) { ①
            Some(_) => println!("{}", line),
            None => (),
        }
    }
}

fn main() {
    let args = App::new("grep-lite")
        .version("0.1")
        .about("searches for patterns")
        .arg(Arg::with_name("pattern")
            .help("The pattern to search for")
            .takes_value(true)
            .required(true))
        .arg(Arg::with_name("input")
            .help("File to search")
            .takes_value(true)
            .required(false))
        .get_matches();

    let pattern = args.value_of("pattern").unwrap();
    let re = Regex::new(pattern).unwrap();

    let input = args.value_of("input").unwrap_or("-");

    if input == "-" {
        let stdin = io::stdin();
        let reader = stdin.lock();
        process_lines(reader, re);
    } else {

```

```
let f = File::open(input).unwrap();
let reader = BufReader::new(f);
process_lines(reader, re);
}
```

## 2.12 Summary

In this chapter you learned that:

- Rust has full support for primitive types, such as integers and floating point.
- Functions are strongly-typed and require both types for their parameters and return values
- List-like types are tailored to specific use cases. You will typically reach for `Vec<T>` first.
- All Rust programs have a single entry function: `main()`.
- Every crate has a `Cargo.toml` file that specifies its metadata.
- The `cargo` tool is able to compile your code and fetch its dependencies.
- `rustup` provides access to multiple compiler toolchains and to the language's documentation

# 3

# *Compound Data Types*

## **This chapter covers:**

- Composing data with structs
- Creating enumerated data types
- Add methods to types
- Handling errors in a type-safe manner
- Defining and implementing common behavior with traits
- Understanding how to keep implementation details private
- Using cargo to build documentation

Welcome to chapter 3. This chapter focuses on two key building blocks, `struct` and `enum`. It also discusses `impl` blocks (that are used to add methods to data) as well as its interface/protocol system: traits. If we spent the last chapter looking at Rust's atoms, this chapter is focused more on its molecules and perhaps its ions.

Throughout this chapter, you'll be working through how to represent files in code. Although conceptually simple—if you're reading this book, it's highly likely you've interacted with a file through code before—there are enough edge cases to make things interesting.

Our strategy will be to create mock version of everything using our own imaginary API. Towards the latter part of the chapter you'll learn how to interact with your actual operating system and file system(s).

### 3.1 Using plain functions to experiment with an API

To start us off, let's see how far we can get by making use of the tools that we've already know. Listing 3.1 lays out a few things that we would expect, such as opening and closing a "file". We'll use a rudimentary mock type to model one: a simple alias around `String` that holds a filename and little else.

To make things slightly more interesting than writing lots of boilerplate code, <<notquite-1>> does sprinkle in a few new concepts. They show you how to tame the compiler while you're experimenting with your design. Attributes are provided to relax compiler warnings and there the `read` function illustrates how to define a function that never returns. The code doesn't actually do anything, however. That will come very shortly.

**Listing 3.1. Using type aliases to stub out a type (ch3-not-quite-file-1.rs)**

```
#![allow(unused_variables)]                                     ①
type File = String;                                         ②
fn open(f: &mut File) -> bool {
    true                                                       ③
}
fn close(f: &mut File) -> bool {
    true                                                       ③
}
#[allow(dead_code)]
fn read(f: &mut File, save_to: &mut Vec<u8>) -> ! {        ④
    unimplemented!()                                         ⑤
}
fn main() {
    let mut f1 = File::from("f1.txt");                         ⑦
    open(&mut f1);                                           ⑧
    //read(f1, vec![]);
    close(&mut f1);
}
```

- ① Relax compiler warnings while working through ideas
- ② Create a type alias. The compiler won't distinguish between `String` & `File`, but your source code will.
- ③ Let's assume for the moment that these two functions always succeed
- ④ Relaxes a compiler warning about an unused function
- ⑤ Using `!` as a return type indicates to the Rust compiler that this function never returns
- ⑥ A macro that crashes the program if it is encountered
- ⑦ With the type declaration at line 3, `File` "inherits" all of `String`'s methods
- ⑧ There's little point in calling this method

There is *lots* that needs to be built upon from Listing 3.1.

- We haven't created a persistent object that could represent a file (there's only so much that can be encoded in a string)
- There was no attempt at implementing `read()` (and if we did, how would we handle the failure case?)
- `open()` and `close()` return `bool`; perhaps there is a way to provide a more sophisticated result type that might be able to contain an error message if the operating system reports one?
- None of our functions are methods. From a syntactic point of view, it might be nice to call `f.open()` rather than `open(f)`.

Let's begin at the top and work our way through this list. Brace yourself for a few scenic detours along the way as we encounter a few learning sideroads that will be profitable to explore.

## 3.2 Modeling Files With `struct`

We need something to represent the thing we're trying to model. `struct` allows you to create a composite type made up other types. Depending on your programming heritage, you may be more familiar with terms such as object or record.

We'll start with requiring that our files have a name and zero or more bytes of data.

Listing 3.2 prints the following two lines to the console:

```
File { name: "f1.txt", data: [] }
f1.txt is 0 bytes long
```

To represent data, the listing uses `Vec<u8>`. That is, a growable list of `u8` (single byte) values. The bulk of the `main()` function demonstrates usage, such as field access.

**Listing 3.2. Defining and Creating an Instance of a `struct` to Represent Files (ch3-mock-file.rs)**

```
##[derive(Debug)]                                     ①
struct File {
    name: String,
    data: Vec<u8>,                                ②
}

fn main() {
    let f1 = File {
        name: String::from("f1.txt"),            ③
        data: Vec::new(),                         ④
    };
    let f1_name = &f1.name;                      ⑤
    let f1_length = &f1.data.len();             ⑤
}
```

```

    println!("{}:?}", f1);
    println!("{} is {} bytes long", f1_name, f1_length);
}

```

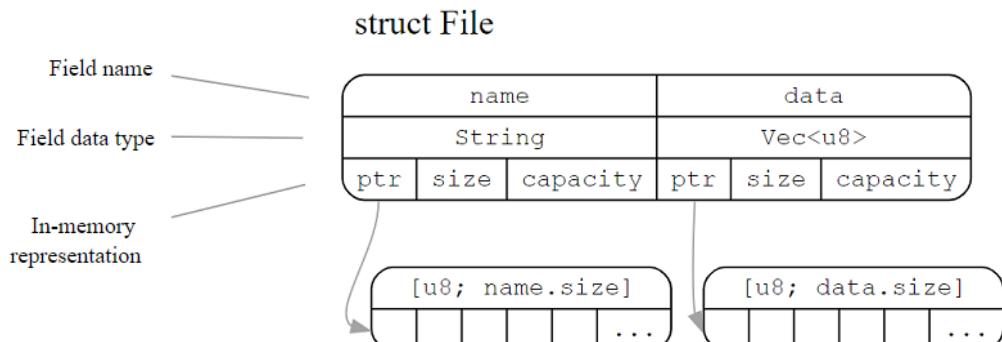
- ① Allows the `println!` macro to print `File`
- ② Using `Vec<u8>` provides access to some useful conveniences, such as dynamic sizing so that it will be possible to simulate writing to a file
- ③ `String::from` allows owned strings to be generated from string literals (which are slices)
- ④ We'll use the `vec!` macro to simulate an empty file
- ⑤ Accessing fields uses the "dot operator" (`.`); Accessing fields by reference prevents use after move issues.

Here is a detailed overview of Listing 3.2 :

- Lines 1-5 define the `File` struct. Definitions include fields and their associated types. They also include each field's lifetimes, which happened to be elided here. Explicit lifetimes are required when a field is a reference to another object.
- Lines 8-11 create our first instance of `File`. We use a literal syntax here, but typically structs in the wild will be created via a convenience method. `String::from()` is one of those convenience methods. It takes a value of another type, in this case a string slice (`&str`) and returns a `String` instance. `Vec::new()` is the more common case.
- Lines 13-17 demonstrate accessing our new instance's fields. We prepend an ampersand, indicating that we wish to access this data by reference. In Rust parlance, this means that the variables `f1_name` and `f1_length` are borrowing the data they refer to.

You have probably noticed that our `File` struct doesn't actually store anything to disk at all. That's actually okay for now. If you're interested in its internals, you are welcome to review Figure 3.1 . Its two fields (`name` and `data`) are themselves both created by structs. If you're unfamiliar with the term pointer (`ptr`), think of it as an address to some memory that we don't know beforehand. This topic is discussed in the chapter "Data in Depth".

**Figure 3.1. Inspecting the internals of the `File` struct**



We'll leave interacting with the hard disk drive or other persistent storage until later in the chapter. For the meantime, let's re-create Listing 3.1 with the `File` type that we have created.

### **The newtype pattern**

Sometimes, the `type` keyword is all that you need. But what about when you need to tell the compiler to treat your new "type" as a fully-fledged, distinct type, rather than just an alias? Enter "newtype".

The newtype pattern consists of wrapping a core type within a single-field `struct` or perhaps a `tuple`.

#### **Listing 3.3. Using the newtype pattern to distinguish URLs from ordinary strings (ch3-newtype-pattern.rs)**

```
##[derive(PartialEq)]           ①
struct Hostname(String);       ②

fn main() {
    let ordinary_string = String::from("localhost");
    let host = Hostname(ordinary_string.clone());
    if host == ordinary_string { ③
        println!("huh?");        ④
    };
}
```

① **PartialEq enables types to be compared for equality. It's called partial to enable certain types to describe situations where equality is not valid, such as floating point's "Not a Number" value.**

② **Hostname is our newtype**

③ **This line won't compile because the compiler understands that Hostname and String are distinct**

④ **Will never happen**

Here is the compiler output:

#### **Listing 3.4. Output from rustc when attempting to compile Listing 3.3**

```
error[E0308]: mismatched types
--> ch3-newtype-pattern.rs:7:16
|
7 |     if host == ordinary_string {      ①
|             ^^^^^^^^^^^^^^^^^ expected struct `Hostname`, found struct
`std::string::String`
|
= note: expected type `Hostname`
         found type `std::string::String`
```

error: aborting due to previous error

① **This line won't compile because the compiler understands that Hostname and String are distinct**

We can now add a little bit of functionality to the first listing of the chapter. Listing 3.5 adds the ability to "read" a file that has some data in it. All functions are assumed to always succeed and the code is still littered with hard-coded values. Still, the code finally prints something to the screen. Here is partially obscured output from the program:

```
File { name: "2.txt", data: [114, 117, 115, 116, 33] }
2.txt is 5 bytes long
***** ①
```

① Revealing this line would spoil all of the fun!

### **Listing 3.5. Using a struct to Mimic a File and Simulate Reading its Contents. Converts opaque data into a String. (ch3-not-quite-file-2.rs)**

```
#[allow(unused_variables)] ①
#[derive(Debug)]
struct File {
    name: String,
    data: Vec<u8>,
}

fn open(f: &mut File) -> bool { ③
    true
}

fn close(f: &mut File) -> bool { ③
    true
}

fn read(f: &File, save_to: &mut Vec<u8>) -> usize { ④
    let mut tmp = f.data.clone(); ⑤
    let read_length = tmp.len(); ⑥
    save_to.reserve(read_length); ⑥
    save_to.append(&mut tmp); ⑦
    read_length
}

fn main() {
    let mut f2 = File {
        name: String::from("2.txt"),
        data: vec![114, 117, 115, 116, 33],
    };

    let mut buffer: Vec<u8> = vec![];

    open(&mut f2); ⑧
    let f2_length = read(&f2, &mut buffer); ⑧
    close(&mut f2); ⑧
```

```

let text = String::from_utf8_lossy(&buffer);          ⑨

println!("{}:?", f2);
println!("{} is {} bytes long", &f2.name, f2_length);
println!("{}", text)                                ⑩
}

```

- ① Silences a warnings caused by open() and close() not making use of needing their argument
- ② This enables File to work with println! and its fmt! sibling macros, used at the bottom of the code listing
- ③ These two functions will remain inert for now
- ④ Return the "number of bytes read"
- ⑤ Make a copy of the data here, as save\_to.append() will shrink the input Vec<T>
- ⑥ Not strictly necessary, but useful to know about. Ensures that there is sufficient space to fit the incoming data and minimizes allocations when data is inserted byte-by-byte
- ⑦ Allocate sufficient data in the save\_to buffer to hold the contents of f
- ⑧ Do the hard work of interacting with the file.
- ⑨ Convert Vec<u8> to String. Any bytes that are not valid UTF-8 are replaced with
- ⑩ View the bytes 114, 117, 115, 116 & 33 as an actual word

The code so far has tackled 2 of the 4 issues raised at the end of Listing 3.1. Our File struct is a *bona fide* type. read() is implemented, albeit in a memory-inefficient manner. The last two points remain.

### 3.3 Adding Methods to a struct with impl

This section explains briefly what methods are and describes how to make use of them in Rust.

Methods are functions that are coupled to some object. From a syntactic point of view, they're just functions that don't need to specify one of their arguments. Rather than calling open() and passing a File object in as an argument (read(f, buffer)), methods allow the main object to be implicit in the function call (f.read(buffer)) using the dot operator.<sup>13</sup>

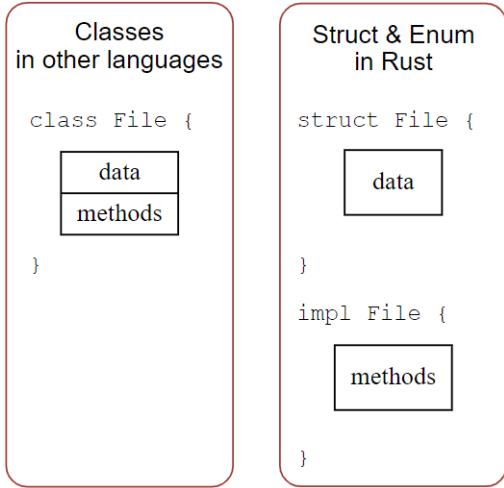
Rust is different than other languages that support methods. There is no "class" keyword. Its struct--and its enum types that are described further on--can both feel like classes at times, but as they don't support inheritance it's probably a good thing that they're named something different.

To define methods, Rust programmers use an `impl` block that are physically distinct in source code from the `struct` (and `enum`) blocks that you have already encountered.

---

<sup>13</sup> There are a number of theoretical differences between methods and functions relating to *purity*, but a detailed discussion of those differences is better placed elsewhere. Functions are regarded as *pure*, meaning their behavior is determined solely by their arguments. Methods are inherently impure, given that one of their arguments is effectively a side-effect. These are muddy waters though. Functions are perfectly capable of acting on side effects themselves. Moreover, methods are implemented with functions. And, to add an exception to an exception, objects are not always required for so called *static methods*.

**Figure 3.2. Illustrating syntactic differences between Rust and most object oriented languages.**  
**Within Rust, methods are defined separately from fields.**



### 3.3.1 Simplifying object creation by implementing a new() method

Creating objects with reasonable defaults is done through the `new()` method.

Every struct can be instantiated through a literal syntax. This is handy for getting started, but leads to unnecessary verbosity in most code.

Using `new()` is a convention within the Rust community. Unlike other languages, `new` is not a keyword and isn't given some sort of blessed status above other methods.

**Table 3.1. Comparing Rust's literal syntax for creating objects with the use of new() methods**

Current	With <code>File::new()</code>
<pre>File {   name: String::from("f1.txt"),   data: Vec::new(), };</pre>	<code>File::new("f1.txt", vec![]);</code>
<pre>File {   name: String::from("f2.txt"),   data: vec![114, 117, 115, 116, 33], };</pre>	<code>File::new("f2.txt", vec![114, 117, 115, 116, 33]);</code>

To enable these changes, you make use of an `impl` block, shown below in Listing 3.6 . The resulting executable should print out the same message as Listing 3.2 , substituting "f3.txt" for the original's "f1.txt".

**Listing 3.6. Using `impl` to add methods to a struct (ch3-defining-files-neatly.rs)**

```

#[derive(Debug)]
struct File {
    name: String,
    data: Vec<u8>,
}

impl File {
    fn new(name: &str) -> File {           ①
        File {
            name: String::from(name),      ②
            data: Vec::new(),             ②
        }
    }
}

fn main() {
    let f3 = File::new("f3.txt");

    let f3_name = &f3.name;           ③
    let f3_length = f3.data.len();

    println!("{}: {}", f3);
    println!("{} is {} bytes long", f3_name, f3_length);
}

```

- ① As `File::new()` is a completely normal function—rather than something blessed by the language—we need to tell Rust that it will be returning a `File` from this function
- ② `File::new()` does little more than encapsulate the object creation syntax. This is normal
- ③ Fields are private by default, but can be accessed within the module that defines the struct. The module system is discussed further on in the chapter

Creating `File::len()` successfully encapsulates the internal workings of the `File` struct. But now there's quite an irritating inconsistency when working with `&f1.name` and `f1.len()`. The next section resolves that inconsistency.

Merging this new knowledge with the example that we already have, Listing 3.7 is the result. It prints

```

File { name: "2.txt", data: [114, 117, 115, 116, 33] }
2.txt is 5 bytes long
***** ①

```

- ① Still hidden!

to the console.

**Listing 3.7. Using `impl` to improve the ergonomics of `File` (`ch3-defining-files-neatly.rs`)**

```

#[allow(unused_variables)]

#[derive(Debug)]
struct File {
    name: String,
    data: Vec<u8>,
}

impl File {
    fn new(name: &str) -> File {
        File {
            name: String::from(name),
            data: Vec::new(),
        }
    }

    fn new_with_data(name: &str, data: &Vec<u8>) -> File {      ①
        let mut f = File::new(name);
        f.data = data.clone();
        f
    }

    fn read(self: &File, save_to: &mut Vec<u8>) -> usize {      ②
        let mut tmp = self.data.clone();
        let read_length = tmp.len();
        save_to.reserve(read_length);
        save_to.append(&mut tmp);
        read_length
    }
}

fn open(f: &mut File) -> bool {                                ③
    true
}

fn close(f: &mut File) -> bool {                                ④
    true
}

fn main() {
    let f3_data: Vec<u8> = vec![114, 117, 115, 116, 33];      ⑤
    let mut f3 = File::new_with_data("2.txt", &f3_data);

    let mut buffer: Vec<u8> = Vec::new();

    open(&mut f3);
    let f3_length = f3.read(&mut buffer);                      ⑥
    close(&mut f3);

    let text = String::from_utf8_lossy(&buffer);
}

```

```

    println!("{:?}", f3);
    println!("{} is {} bytes long", &f3.name, f3_length);
    println!("{}", text);
}

```

- ① This method has snuck in to deal with cases where we want to simulate cases where a file has pre-existing data
- ② The `f` argument has been replaced with `self`
- ③ These two can remain as-is until we've looked at error handling
- ④ An explicit type needs to be provided, as `vec!` can't infer the necessary type through the function boundary
- ⑤ Here is the change in the calling code

## 3.4 Returning errors

Early on in the chapter, two points were raised discussing dissatisfaction with being unable to properly signify errors:

- There was no attempt at implementing `read()` (and if we did, how would we handle the failure case?)
- `open()` and `close()` return `bool`; perhaps there is a way to provide a more sophisticated result type that might be able to contain an error message if the operating system reports one?

The issue arises because dealing with hardware is unreliable. Even ignoring hardware faults, the disk may be full or the operating system may intervene and tell you that you don't have permission to delete a particular file. This section discusses different methods for signalling that an error has occurred, beginning with approaches common in other areas and finishing with idiomatic Rust.

### 3.4.1 Modifying a known global variable

One of the simplest methods for signalling that an error has occurred is by checking the value of a global variable. Although notoriously error prone, this is common idiom in systems programming. The C programmers are used to checking the value of `errno` once system calls have been returned. As an example, the `close()` system call closes a “file descriptor”—an integer representing a file, with numbers being relative to individual processes—and `errno` may be modified.

The section of POSIX standard discussing the `close()` system call includes this snippet:

*If `close()` is interrupted by a signal that is to be caught, it shall return -1 with `errno` set to `EINTR` and the state of `fd` [file descriptor] is unspecified. If an I/O error occurred while reading from or writing to the file system during `close()`, it may return -1 with `errno` set to `EIO`; if this error is returned, the state of `fd` is unspecified.*

-- close - close a file descriptor: The Open Group Base Specifications Issue 7  
<http://pubs.opengroup.org/onlinepubs/9699919799/functions/close.html>

Setting `errno` to either `EIO` or `EINTR` means to set it to some magical internal constant. The specific values are arbitrary and defined per operating system.

In Rust syntax, checking global variables would look something like this:

```
static mut ERROR: i32 = 0;      ①

// ...

fn main() {

    // ...
    read(f, buffer)

    unsafe {                      ②
        if ERROR != 0 {           ③
            panic!("An error has occurred")
        }
    }
}
```

- ① `static mut`, spoken as "mutable static", is a global variable with the '`static`' lifetime (that is, it's valid for the life of the program).
- ② Accessing and modifying `static mut` variables requires the use of an `unsafe` block. This is Rust's way of disclaiming all responsibility.
- ③ Checking the `ERROR` value happens here. Error checking relies on the convention that 0 means no error.

Here are the instructions to experiment with this pattern:

- Open a terminal
- Move to a scratch directory, such as `/tmp/`
- Execute `cargo new --bin --vcs none globalerror`
- Add the following dependency to the `globalerror/Cargo.toml` file:

```
[dependencies]
rand = "0.3"
```

- Replace the contents of `globalerror/src/main.rs` with the code in Listing 3.8
- Execute `cargo run`. You should see output like this:

```
$ cargo run
Compiling globalerror v0.1.0 (file:///path/to/globalerror)
  Finished dev [unoptimized + debuginfo] target(s) in 0.74 secs
    Running `target/debug/globalerror`
```

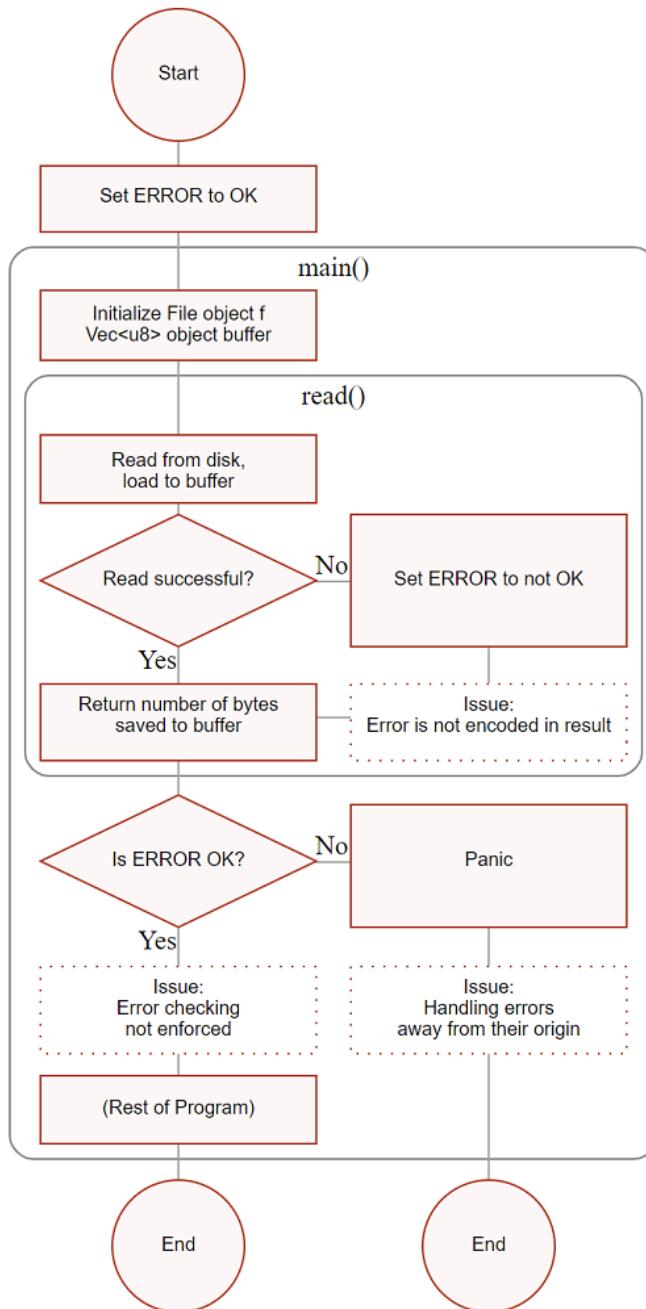
99,999/10,000 the program will not do anything. Occasionally—if the book has enough readers with sufficient motivation—it will print out the line: “An error has occurred!”

Listing 3.8, introduces some new syntax. The most significant is probably

the `unsafe` keyword The significance of this keyword will be discussed later in the book. In the meantime, consider `unsafe` to be a warning sign rather than an indicator that you're embarking on anything illegal. `Unsafe` means "the same level of safety offered by C at all times".

Mutable global variables are denoted with `static mut`. By convention, global variables in Rust use all caps. Rust includes a `const` keyword as well for values that may never change.

**Figure 3.3. A visual overview of Listing 3.8, including explanations of problems with using global error codes**



**Listing 3.8. Using global variables to propagate error information through a program  
(ch3/globalerror/src/main.rs)**

```

extern crate rand;          ①
use rand;                  ②

static mut ERROR: isize = 0; ③

struct File;               ④

#[allow(unused_variables)]
fn read(f: &File, save_to: Vec<u8>) -> usize {
    // "read from disk"
    if rand::thread_rng().gen_weighted_bool(10_000) { ⑤
        unsafe {
            ERROR = 1;                                ⑥
        }
    }

    0                                                 ⑦
}

#[allow(unused_mut)]
fn main() {                      ⑧
    let mut f = File;
    let mut buffer = vec![];

    read(&f, buffer);
    unsafe {
        if ERROR != 0 {                            ⑨
            panic!("An error has occurred!")
        }
    }
}

```

- ① Make an external crate available to our code
- ② Bring rand into local scope
- ③ Initialize ERROR to 0
- ④ Create a “unit type” with no fields to stand in for a real struct while we’re experimenting
- ⑤ Return true 1 in every  $n$  times this function is called, where  $n$  is 10,000
- ⑥ Set ERROR to 1, having the effect of notifying the rest of the system that an error has occurred
- ⑦ Always read() 0 bytes
- ⑧ Let’s keep buffer mutable for consistency with other code, even though it isn’t touched here
- ⑨ Accessing static mut variables is an unsafe operation

Experienced programmers will know that using the global variable `errno` is commonly adjusted by the operating system during syscalls.

This style of programming would typically be discouraged in Rust, as it omits both type safety (errors are encoded as plain integers) and can reward sloppy programmers with

unstable programs when they forget to check the `errno` value. However, it's an important style to be aware of because:

- Systems programmers may need to interact with operating system-defined global values
- Software that interacts with CPU registers and other low-level hardware will need to get used to inspecting flags to check that operations were completed successfully

### 3.4.2 Making use of the Result return type

Rust's approach to error handling is to use a type that stands for both the standard case and the error case. This type is known as `Result`. `Result` has two states, `Ok` and `Err`. This multi-headed hydra is versatile and is put to work all through the standard library. We'll consider *how* a single type can act as two later on. For the moment, let's just investigate the mechanics of working with it.

The example below at Listing 3.9 makes two major changes from previous iterations:

- Functions that interact with the file system return `Result<T, String>`, where `T` is the intended type. `String` will be used to report back error messages.
- When we call those functions, there is now an additional call to `unwrap()` which “unwraps” `Ok(T)` and produces `T`

There are some additional changes that may be useful to understand, but are not essential at this stage. `open()` and `close()` now take full *ownership* of their `File` arguments. While we'll defer a full explanation of the term ownership for now, it enables the `File` argument to be inserted into `Ok(T)` as `T` then returned. Associated with this change is that the variable `f4` is now re-bound multiple times with the results of function calls. Without this, we would run into issues with using data that is no longer valid. In a sense, re-assigning the value from the result of the calls to `open()` and `close()` allows the variable `f4` to re-claim ownership of its `File` value.

To run the code, follow these steps:

- Open a terminal
- Move to a scratch directory, such as `/tmp`/
- Execute `cargo new --bin --vcs none fileresult`
- Add the following dependency to the `fileresult/Cargo.toml` file:

```
[dependencies]
rand = "0.3"
```

- Replace the contents of `fileresult/src/main.rs` with the code in Listing 3.9
- Execute `cargo run`. You should see output like this:

```
$ cargo run
Compiling fileresult v0.1.0 (file:///path/to/fileresult)
Finished dev [unoptimized + debuginfo] target(s) in 1.04 secs
Running `target/debug/fileresult`
```

**Listing 3.9. Using Result to mark functions that are susceptible to file-system errors  
(ch3/fileresult/src/main.rs)**

```

extern crate rand;          ①
use rand::Rng;             ②

fn one_in(n: u32) -> bool {    ③
    rand::thread_rng().gen_weighted_bool(n)
}

#[derive(Debug)]
struct File {
    name: String,
    data: Vec<u8>,
}

impl File {
    fn new(name: &str) -> File {
        File { name: String::from(name), data: Vec::new() }           ④
    }

    fn new_with_data(name: &str, data: &Vec<u8>) -> File {
        let mut f = File::new(name);
        f.data = data.clone();
        f
    }

    fn read(self: &File, save_to: &mut Vec<u8>) -> Result<usize, String> {   ⑤
        let mut tmp = self.data.clone();
        let read_length = tmp.len();
        save_to.reserve(read_length);
        save_to.append(&mut tmp);
        Ok(read_length)           ⑥
    }
}

fn open(f: File) -> Result<File, String> {
    if one_in(10_000) {      ⑦
        let err_msg = String::from("Permission denied");
        return Err(err_msg);
    }
    Ok(f)
}

fn close(f: File) -> Result<File, String> {
    if one_in(100_000) {     ⑧
        let err_msg = String::from("Interrupted by signal!");
        return Err(err_msg);
    }
    Ok(f)
}

```

```

fn main() {
    let f4_data: Vec<u8> = vec![114, 117, 115, 116, 33];
    let mut f4 = File::new_with_data("4.txt", &f4_data);

    let mut buffer: Vec<u8> = vec![];

    f4 = open(f4).unwrap();                                     ⑨
    let f4_length = f4.read(&mut buffer).unwrap();             ⑨
    f4 = close(f4).unwrap();                                   ⑨

    let text = String::from_utf8_lossy(&buffer);

    println!("{}: {}", f4);
    println!("{} is {} bytes long", &f4.name, f4_length);
    println!("{}", text);
}

```

- ① Bring the rand crate into this crate's scope
- ② Bring the random number generator *trait* into scope
- ③ Helper function to enable us to trigger sporadic errors
- ④ Stylistic change to shorten the code block
- ⑤ First appearance of Result<T, E>, where T is an integer of type usize, and E is String.  
Using String allows us to provide arbitrary error messages.
- ⑥ In this code, read() never fails. But we are still wrapping read\_length in Ok because we're returning Result
- ⑦ Once in 10,000 executions, return an error.
- ⑧ Once in 100,000 executions, return an error.
- ⑨ "Unwrap" T from Ok, leaving T

**TIP**

**Calling Result.unwrap() is often considered poor style. It bludgeons the program into submission, effectively ignoring the possibility of errors.**

+ When Err(E) is returned, the whole program panics and shuts down. As the book progresses, we'll encounter more nuanced ways to handle the Err(E) case.

Using Result provides you with compiler-assisted code correctness: your code won't compile unless you've taken the time to handle the edge cases. This program will fail on error, but at least we have made this explicit.

So, what is a Result? Result is an enum defined in Rust's standard library. It has the same status as any other type, but is tied together with the rest of the language through strong community conventions. Wait.. what is an enum? I'm glad you asked. That's the topic of our next section.

## 3.5 Defining and making use of enum

An enum—enumeration in full—is a type that can represent multiple known variants. Classically, an enum would be used to represent several pre-defined known options, such as the suits of playing cards or planets in the solar system.

**Listing 3.10. Defining an enum that represents the suits of a French deck of playing cards**

```
enum Suit {
    Clubs,
    Spades,
    Diamonds,
    Hearts,
}
```

If you haven't programmed in a language that makes use of enums, understanding their value takes some effort. As you program with them for a while, you're likely to experience a minor epiphany. Consider creating some code that is parsing event logs. Each event has a name, perhaps "UPDATE" or "DELETE". Rather than storing those values as strings in your application, which can lead to subtle bugs later on when string comparisons become unwieldy, enums allow you to give the compiler some knowledge of the error codes. Later on, you'll be given warnings such as "Hi there, I see that you have considered the UPDATE case, but it looks like you've forgotten the DELETE case. You should fix that."

Listing 3.11 shows the beginnings of an application that parses text and emits structured data. When run, the program produces this output:

```
(Unknown, "BEGIN Transaction XK342")
(Update, "234:LS/32231 {"price": 31.00} -> {"price": 40.00}")
(Delete, "342:LO/22111")
```

**Listing 3.11. Defining an enum and making use of it to parse an event log (ch3-parse-log.rs)**

```
#[derive(Debug)]          ①
enum Event {
    Update,            ②
    Delete,            ②
    Unknown,           ②
}

type Message = String;    ③

fn parse_log(line: &'static str) -> (Event, Message) {      ④
    let parts: Vec<&str> = line.splitn(2, ' ').collect();    ⑤
    if parts.len() == 1 {          ⑥
        return (Event::Unknown, String::from(line))
    }

    let event = parts[0];          ⑦
    let rest = String::from(parts[1]);  ⑦

    match event {
        "UPDATE" | "update" => (Event::Update, rest),     ⑧
        "DELETE" | "delete" => (Event::Delete, rest),     ⑧
        _ => (Event::Unknown, String::from(line)),         ⑨
    }
}
```

```

}

fn main() {
    let log = "BEGIN Transaction XK342
UPDATE 234:LS/32231 {\"price\": 31.00} -> {\"price\": 40.00}
DELETE 342:LO/22111";

    for line in log.lines() {
        let parse_result = parse_log(line);
        println!("{}:?", parse_result);
    }
}

```

- ① Enable this enum to be printed to the screen via auto-generated code
- ② Create three variants of Event, including one value for unrecognized events
- ③ A convenient name for String for use in this crate's context
- ④ A function for parsing a line and converting it into semi-structured data
- ⑤ collect() consumes an iterator (returned from line.splitn()) and returns Vec<T>
- ⑥ If line.splitn() didn't split log into two parts, return an error
- ⑦ Assign each part of parts to a variable to ease future use
- ⑧ When we match a known event, return structured data
- ⑨ If we don't recognize the event type, return the whole line

Enums have a few tricks up their sleeves:

- They work together with Rust's pattern matching capabilities to help you build robust, readable code. This is visible on lines 19-23 of Listing 3.11 .
- Like struct, they support methods via `impl` blocks
- Rust's enums are more powerful than a set of constants. It's possible to include data within variants, granting them a struct-like persona:

```

enum Suit {
    Clubs,
    Spades,
    Diamonds,
    Hearts,          ①
}

enum Card {
    King(Suit),      ②
    Queen(Suit),     ②
    Jack(Suit)       ②
    Ace(Suit),       ②
    Pip(Suit, usize), ③
}

```

- ① The last element of enums also ends with a comma. This eases refactoring.
- ② Face cards have a suit
- ③ Pip cards have a suit and a rank

### 3.5.1 Using an enum to manage internal state

Now that you've seen how to define and use an enum, how would this be useful when applied to modelling files? We can expand our `File` type and allow it to change as it is opened and closed.

Listing 3.12 produces code that prints out a short alert to the console:

```
Error checking is working
File { name: "5.txt", data: [], state: Closed }
5.txt is 0 bytes long
```

**Listing 3.12. An enum that represents a File being open or closed (ch3-file-states.rs)**

```
#[derive(Debug,PartialEq)]
enum FileState {
    Open,
    Closed,
}

#[derive(Debug)]
struct File {
    name: String,
    data: Vec<u8>,
    state: FileState,
}

impl File {
    fn new(name: &str) -> File {
        File { name: String::from(name), data: Vec::new(), state: FileState::Closed }
    }

    fn read(self: &File, save_to: &mut Vec<u8>) -> Result<usize, String> {
        if self.state != FileState::Open {
            return Err(String::from("File must be open for reading"));
        }
        let mut tmp = self.data.clone();
        let read_length = tmp.len();
        save_to.reserve(read_length);
        save_to.append(&mut tmp);
        Ok(read_length)
    }
}

fn open(mut f: File) -> Result<File, String> {
    f.state = FileState::Open;
    Ok(f)
}

fn close(mut f: File) -> Result<File, String> {
    f.state = FileState::Closed;
    Ok(f)
}
```

```

fn main() {
    let mut f5 = File::new("5.txt");

    let mut buffer: Vec<u8> = vec![];

    if f5.read(&mut buffer).is_err() {
        println!("Error checking is working");
    }

    f5 = open(f5).unwrap();
    let f5_length = f5.read(&mut buffer).unwrap();
    f5 = close(f5).unwrap();

    let text = String::from_utf8_lossy(&buffer);

    println!("{}: {}", f5);
    println!("{} is {} bytes long", &f5.name, f5_length);
    println!("{}: {}", f5, text);
}

```

Enums can be a powerful aide in your quest to produce reliable, robust software. Consider it for your code whenever you discover yourself introducing stringly typed data such as messages codes.

## 3.6 Defining Common Behavior with Traits

A robust definition of the term “file” needs to be agnostic to storage medium. Files (at least) support *reading* and *writing*. Focusing on those two capabilities allows us to ignore where the reads and writes are actually taking place. They could be from a hard disk drive, an in-memory cache, over a network or via something more exotic.

Irrespective of whether a “file” is a network connection, a spinning metal platter or a superposition of an electron, it’s possible to define rules that say, “To call yourself a file, you must implement this”. Traits have close relatives in other languages. They’re often named interfaces, protocols or perhaps contracts.

You have already seen traits in action several times. Every time you’ve used `#[derive(Debug)]` in a type definition, you’ve implemented the `Debug` trait for that type. Traits permeate the Rust language. Let’s see how to create one.

### 3.6.1 Creating a Read trait

Traits enable the compiler (and other humans) to know that multiple types are attempting to perform the same task. Types that use `#[derive(Debug)]` are all able to be printed to the console via the `println!` macro and its relatives. Allowing multiple types to implement an `Read` trait enables code re-use and enables the Rust compiler to perform its “zero cost abstraction” wizardry.

For the sake of brevity, Listing 3.14 is a bare bones version of the code that we’ve already seen. When built with `rustc` and executed, Listing 3.14 prints the following

line to the console:

#### Listing 3.13. Output of Listing 3.14

```
0 byte(s) read from File
```

#### Listing 3.14. Defining the bare bones of a Read trait for File. Shows the distinction between the trait keyword which is used for definitions and the impl keyword for attaching a trait to a specific type. (ch3/ch3-skeleton-read-trait.rs)

```
#![allow(unused_variables)]      ①

#[derive(Debug)]
struct File;                  ②

trait Read {                   ③
    fn read(self: &Self, save_to: &mut Vec<u8>) -> Result<usize, String>;  ④
}

impl Read for File {
    fn read(self: &File, save_to: &mut Vec<u8>) -> Result<usize, String> {
        Ok(0)                      ⑤
    }
}

fn main() {
    let f = File{};
    let mut buffer = vec!();
    let n_bytes = f.read(&mut buffer).unwrap();
    println!("{} byte(s) read from {:?}", n_bytes, f);
}
```

- ① Silence any warnings relating to unused variables within functions
- ② Define a stub File type
- ③ Provide a specific name for the trait
- ④ A trait block includes the type signatures of functions that implementors must comply with. The pseudo-type Self is a placeholder for the type that will eventually be implementing Read.
- ⑤ A simple stub value that complies with the type signature required

Defining a trait and implementing it in on the same page can feel quite drawn out in small examples such as this. File is spread across three code blocks within Listing 3.14 . The flip side of this is that many common traits become second nature as your experience grows. Once you've learned what the PartialEq trait does for one type, you'll understand it for every other one. If you're wondering that implement PartialEq can be compared with the == operator. "Partial" allows for cases where two values that match exactly should not be treated as equals, such as the floating point's Not a Number value or SQL's NULL.

**TIP**

If you've spent some time looking through the Rust community's forums and documentation, you may noticed that they've formed their own variant of English grammar.

When you see a sentence with the following structure, "...T is Debug...", then they're saying that T implements the Debug trait.

### 3.6.2 *Implementing Display for your own types*

`println!` and a number of others live within a family of macros that all use the same underlying machinery. The macros `println!`, `print!`, `write!`, `writeln!` and `format!` all rely on the `Display` and `Debug` traits. That is, they rely on trait implementations provided by programmers to be able to convert from `{}` to what is printed to the console.

Looking a few pages back to Listing 3.12 , the `File` type was composed of a few fields and a custom subtype, `FileState`:

#### Listing 3.15. Snippet from Listing 3.12 illustrating the use of the Debug trait

```
#[derive(Debug, PartialEq)]
enum FileState {
    Open,
    Closed,
}

#[derive(Debug)]
struct File {
    name: String,
    data: Vec,
    state: FileState,
}

fn main() {
    let f5 = File::new("f5.txt");
    //...
    println!("{}:?", f5);      ①
}
```

- ① Debug relies on the question mark to work, which can be frustrating if other types implement `Display` and are happy to be printed via `{}`

It's possible to rely on the `Debug` trait auto-implementations as a crutch, but what should you do if you wanted to provide custom text? Searching through `rustdoc` documentation, `Display` requires that types implement a `fmt` method that returns `fmt::Result`.

#### Listing 3.16. Implementing Display for File and its associated type FileState

```
impl Display for FileState {
    fn fmt(&self, f: &mut fmt::Formatter) -> fmt::Result {
```

```

        match *self {
    }
}

impl Display for File {
    fn fmt(&self, f: &mut fmt::Formatter) -> fmt::Result {
        write!(f, "{}.{}.{}.{}", self.0, self.1, self.2, self.3)
    }
}

```

**Listing 3.17. Working code snippet to implement Display for a struct that includes fields that also need to implement Display (ch3/ch3-implementing-display.rs)**

```

#[allow(dead_code)]          ①

use std::fmt;               ②
use std::fmt::{Display};    ③

#[derive(Debug,PartialEq)]
enum FileState {
    Open,
    Closed,
}

#[derive(Debug)]
struct File {
    name: String,
    data: Vec<u8>,
    state: FileState,
}

impl Display for FileState {
    fn fmt(&self, f: &mut fmt::Formatter) -> fmt::Result {
        match *self {
            FileState::Open => write!(f, "OPEN"),           ④
            FileState::Closed => write!(f, "CLOSED"),        ④
        }
    }
}

impl Display for File {
    fn fmt(&self, f: &mut fmt::Formatter) -> fmt::Result {
        write!(f, "<{} ({})>", self.name, self.state)  ⑤
    }
}

impl File {
    fn new(name: &str) -> File {
        File {
            name: String::from(name),
            data: Vec::new(),
        }
    }
}

```

```

        state: FileState::Closed
    }
}
}

fn main() {
    let f6 = File::new("f6.txt");
    //...
    println!("{}:?", f6);      ⑥
    println!("{}:", f6);      ⑦
}

```

- ① Silence warnings related to FileState::Open not being used
- ② Bring the std::fmt crate into local scope, allowing us to make use of fmt::Result
- ③ Bring Display into local scope, avoiding the need for us to prefix it as fmt::Display in our code
- ④ Sneakily, we can make use of write! to do the grunt work for us. Strings already implement Display themselves, so there's very little left for us to do.
- ⑤ We can rely on the FileState Display implementation in our own code
- ⑥ The Debug implementation prints out a familiar message, in common with all other implementors of Debug, File { ... }
- ⑦ Our Display implementation follows its own rules, displaying itself as <f6.txt (CLOSED)>

We'll see many uses of traits throughout the course of the book. They underlie Rust's generics system and the language's robust type checking. With a little bit of abuse, they can also support a form of inheritance of the form that's common in most object oriented languages. For now though, the thing to remember is that traits are common behavior that types opt into via the syntax: `impl Trait for Type`.

## 3.7 Exposing your types to the world

Your crates will interact with others that you build up over time. You may wish to make that process easier for your future self by hiding internal details and documenting what's public. This section describes some of the tooling available within the language and cargo to make that process easier.

### 3.7.1 Protecting private data

Rust defaults to keeping things private. If you were to create a library with only the code that you have seen so far, importing your crate would provide no extra benefit. To remedy this, use the `pub` keyword to make things public.

Listing 3.19 provides a few examples of prefixing types and methods with `pub`. Its output is not exciting:

#### **Listing 3.18. Output of Listing 3.19**

```
File { name: "f7.txt", data: [], state: Closed }
```

**Listing 3.19. Making use of the pub keyword to mark the name and state fields of File to be public**

```

#[derive(Debug, PartialEq)]
pub enum FileState {    ①
    Open,
    Closed,
}

#[derive(Debug)]
pub struct File {
    pub name: String,
    data: Vec<u8>,      ②
    pub state: FileState,
}

impl File {
    pub fn new(name: &str) -> File {    ③
        File {
            name: String::from(name),
            data: Vec::new(),
            state: FileState::Closed
        }
    }
}

fn main() {
    let f7 = File::new("f7.txt");
    //...
    println!("{}: {:?}", f7);
}

```

- ① An enum's variants are assumed to be public if the overall type is made public
- ② File.data remains private if a third party were to import this crate via use
- ③ Even though the File struct is public, its methods must also be explicitly marked as such too

## 3.8 Creating In-line Documentation

When software systems become larger, it becomes more important to document one's progress. This section walks through adding documentation to your code and generating HTML versions of that content.

Below at Listing 3.20 , you'll see the familiar code with some added lines beginning with `///` or `!``. The first form is much more common. It generates documents that refer to the item that immediately follow. The second form refers to the current item, as the compiler scans the code. By convention, it is only used to annotate the current module but is available for other places as well.

**Listing 3.20. Adding Doc Comments to Code (ch3-file-doced.rs)**

```

///! Simulating files one step at a time.      ①

/// Represents a "file", which probably lives on a file system.      ②
#[derive(Debug)]
pub struct File {
    name: String,
    data: Vec<u8>,
}

impl File {
    /// New files are assumed to be empty, but a name is required.
    pub fn new(name: &str) -> File {
        File {
            name: String::from(name),
            data: Vec::new(),
        }
    }

    /// Returns the file's length in bytes.
    pub fn len(&self) -> usize {
        self.data.len()
    }

    /// Returns the file's name.
    pub fn name(&self) -> String {
        self.name.clone()
    }
}

fn main() {
    let f1 = File::new("f1.txt");

    let f1_name = f1.name();
    let f1_length = f1.len();

    println!("{}: {}", f1_name, f1_length);
    println!("{} is {} bytes long", f1_name, f1_length);
}

```

- ① The form `///!` is used to refer to the “current” item, the module that’s just been entered by the compiler  
 ② The form `///` annotates whatever is immediately following it

### **3.8.1 Using `rustdoc` to Render Docs For a Single Source File**

You may not know it, but you installed a command-line tool called `rustdoc` when you installed Rust. `rustdoc` is like a special-purpose Rust compiler. Instead of producing executable code, it produces HTML versions of your in-line documentation.

Here is how to use it. Assuming that you have the code at Listing 3.20 saved as `ch3-file-doced.rs`, follow these steps:

- Open a terminal
- Move to the location of your source file
- Execute `rustdoc ch3-file-doced.rs`
- Optional: Run `ls` (or `dir` on Windows).

You will notice that a directory (`doc/`) has been created for you. The documentation's entry point is actually within a sub-directory, `doc/ch3_file_doced/index.html`.

- Open a web browser, then navigate to [/path/to/doc/ch3\\_file\\_doced](#) and open a web browser (START / c [localhost](#) in Windows)

When your programs start to get larger and span multiple files, invoking `rustdoc` manually can become a bit of a pain. Thankfully, `cargo` can do the grunt work on your behalf. That's discussed later at ["Using cargo to Render Docs for a Crate and its Dependencies"](#).

### **3.8.2 Using cargo to Render Docs for a Crate and its Dependencies**

These comments can be rendered as rich text with `cargo`. `cargo` works with crates, rather than the individual files as we've been working with so far. To get around this, create a crate named `filebasics` by following these instructions:

- Open a terminal
- Move to a working directory, such as `/tmp/` (`cd %TEMP%` on MS Windows)
- Run `cargo new --bin filebasics`

You should end up with a project directory tree that looks like this:

```
filebasics
|---.gitignore
|---Cargo.toml
`---src
    `---main.rs      ①
```

① This file is what you will be editing in the following steps

- Save the source code from Listing 3.20 into `filebasics/src/main.rs`, overwriting the hello world boilerplate code that is already there

To build an HTML version of a crate's documentation:

- Move to the project's root directory (`filebasics/`) which includes the `Cargo.toml` file
- Run `cargo doc --open` and Rust will compile an HTML version of the documentation for your code.

You should see output similar to the following appear:

```
Documenting files v0.1.0 (file:///C:/Users/Tim/AppData/Local/Temp/files)
Finished dev [unoptimized + debuginfo] target(s) in 1.68 secs
Opening C:\Users\Tim\AppData\Local\Temp\files\target\doc\files\index.html
```

Launching cmd /C

Your default web browser will now be open and the documentation should be visible.

**TIP**

If you have lots of dependencies in your crate, the build process may take a while.

A useful flag is `cargo doc --no-deps`. Adding `--no-deps` can significantly restrict the work `rustdoc` has to do.

`rustdoc` supports rich text rendering text written in Markdown. That allows you to add headings, lists and links within your documentation. Code snippets that are wrapped in grave accent gates (``...``) are given syntax highlighting.

```
//! Simulating files one step at a time.

impl File {
    /// Creates a new, empty `File`.
    ///
    /// # Examples
    ///
    /// ```
    /// let f = File::new("f1.txt");
    /// ```
    pub fn new(name: &str) -> File {
        File {
            name: String::from(name),
            data: Vec::new(),
        }
    }
}
```

## 3.9 Summary

This chapter has packed a great deal of content into its pages. You have learned that:

- Struct is the foundational compound data type. Paired with traits, struct is the closest to “object” from other domains
- Enum is more powerful than a simple list. Enum’s strength lies in its ability to work with the compiler to consider all edge cases.
- Methods are added to types via `impl` blocks
- Global error codes can be used in Rust, but it can be cumbersome and would generally be frowned upon
- The `Result` type is the mechanism the Rust community prefers to use to signal the possibility of error
- Traits enable common behavior through Rust programs.
- Data and methods remain private until they’re declared public
- Cargo can be used to build the documentation of your crate and all of its dependencies

# *Lifetimes, Ownership and Borrowing*



## **This chapter covers:**

- discovering what the term “lifetime” means in the context of Rust programming
- working with the borrow checker rather than against it
- multiple tactics for dealing with issues when they crop up
- understanding what the responsibilities of an “owner” are
- learning how to “borrow” values that are owned elsewhere

This chapter attempts to explain one of the concepts that trips up most newcomers to Rust: its “borrow checker”. The borrow checker checks that all access to data is legal. Checking to see that all data access is legal allows Rust to prevent safety issues.

Learning how this system works will—at the very least—speed up your development time, by avoiding run ins with the compiler. More significantly though, learning to work with the borrow checker allows you to build larger software systems with confidence. It underpins the term “fearless concurrency”.

To explain how this system operates—and learn how to comply with it when an error is discovered—is this chapter’s role. It uses the somewhat lofty example of simulating a satellite constellation to explain the trade offs relating to different ways to provide shared access to data.

The details of borrow checking are thoroughly explored within the chapter. However, a few bullet points might be useful for readers wanting a quick gist:

Borrow checking relies on three inter-related concepts: lifetimes, ownership and borrowing.

- *ownership* is a stretched metaphor. There is no relationship to property rights. Within Rust, ownership relates to cleaning values up when they're no longer needed. For example, when a function returns, the memory holding its local variables needs to be freed. Owners cannot prevent other parts of the program from accessing their values or report data theft to some overarching Rust authority.
- A value's *lifetime* is the period when accessing that value is valid behavior. A function's local variables live until the function returns. Global variables might live for the life of the program.
- To *borrow* a value means to access it. This terminology is confusing, as there is no obligation to return the value back to its owner. It's used to emphasize that while values may have a single owner, it's possible for many parts of the program to share access to those values.

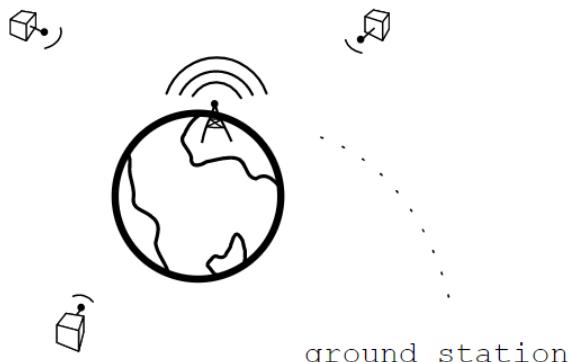
## 4.1 “Implementing” a Mock CubeSat Ground Station

Our strategy for this chapter will be to use an example that compiles, then make a minor change that will trigger an error that appears to emerge without any adjustment to the program's flow. Working through the fixes to those issues should make the concepts more complete.

The learning example for the chapter is a CubeSat constellation. If you've never encountered that phrase before, here are some definitions:

- CubeSats are miniature artificial satellites that are increasingly being used to increase the accessibility of space research.
- A ground station is an intermediary between the operators and the satellites themselves. It's listening on the radio, checking on the status of every satellite in the constellation and transmitting messages to and fro. When introduced in our code, it will act as the gateway between the user and the satellites.
- A constellation is the collective noun for satellites in orbit.

**Figure 4.1. CubeSats in Orbit**



In Figure 4.1, we have three CubeSats. To model this, we'll create a variable for each of them. They can happily be integers for the moment. We don't need to model the ground station explicitly yet, as we're not yet sending messages around the constellation, so we'll omit it for now.

```
let sat_a = 0;
let sat_b = 1;
let sat_c = 2;
```

To check on the status of each of our satellites, we'll use a stub function and an enum to represent potential error messages.

```
#[derive(Debug)]
enum StatusMessage {
    Ok,           ①
}

fn check_status(sat_id: u64) -> StatusMessage {
    StatusMessage::Ok ①
}
```

① For now, all of our CubeSats function perfectly all of the time

The `check_status()` function would be extremely complicated in a production system. For our purposes though, returning the same value every time is perfectly sufficient. Pulling these two snippets into a whole program that "checks" our satellites twice, we end up with something like this:

#### **Listing 4.1. Checking the status of our integer-based CubeSats (ch4/ch4-check-sats-1.rs)**

```
#![allow(unused_variables)]

#[derive(Debug)]
enum StatusMessage {
    Ok,
}

fn check_status(sat_id: u64) -> StatusMessage {
    StatusMessage::Ok
}

fn main () {
    let sat_a = 0;
    let sat_b = 1;
    let sat_c = 2;

    let a_status = check_status(sat_a);
    let b_status = check_status(sat_b);
    let c_status = check_status(sat_c);
    println!("a: {:?}", a_status, b_status, c_status);
}
```

```
// "waiting" ...
let a_status = check_status(sat_a);
let b_status = check_status(sat_b);
let c_status = check_status(sat_c);
println!("a: {:+?}, b: {:+?}, c: {:+?}", a_status, b_status, c_status);
}
```

Running Listing 4.1 should be fairly uneventful. The code compiles begrudgingly. We encounter the following output from our program:

#### **Listing 4.2. Output of Listing 4.1**

```
a: Ok, b: Ok, c: Ok
a: Ok, b: Ok, c: Ok
```

### **4.1.1 Encountering our first lifetime issue**

Let's move closer to idiomatic Rust by introducing type safety. Instead of integers, let's create a type to model our satellites. A real implementation of a CubeSat type would probably include lots of information about its position, its RF frequency band and more. We'll stick with only recording an identifier.

#### **Listing 4.3. Modelling a CubeSat as its own Type**

```
#[derive(Debug)]
struct CubeSat {
    id: u64;
}
```

Now that we have a `struct` definition, let's inject it into our code. Listing 4.4 will not compile. Understanding the details of why not is the task of much of this chapter.

#### **Listing 4.4. Checking the status of our integer-based CubeSats (ch4/ch4-check-sats-2.rs)**

```
#[derive(Debug)] ①
struct CubeSat {
    id: u64,
}

#[derive(Debug)]
enum StatusMessage {
    Ok,
}

fn check_status(sat_id: CubeSat) -> StatusMessage { ②
    StatusMessage::Ok
}

fn main() {
    let sat_a = CubeSat { id: 0 }; ③
    let sat_b = CubeSat { id: 1 }; ③
}
```

```

let sat_c = CubeSat { id: 2 };    ③

let a_status = check_status(sat_a);
let b_status = check_status(sat_b);
let c_status = check_status(sat_c);
println!("a: {:?}", a_status, b_status, c_status);

// "waiting" ...
let a_status = check_status(sat_a);
let b_status = check_status(sat_b);
let c_status = check_status(sat_c);
println!("a: {:?}", a_status, b_status, c_status);
}

```

- ① Modification 1: Add definition
- ② Modification 2: Use the new type within `check_status()`
- ③ Modification 3: Create three new instances

When you attempt to compile the code within Listing 4.4 , you will receive a message similar to the following (which has been edited for brevity):

#### **Listing 4.5. Error Message Produced When Attempting to Compile Listing 4.4**

```

error[E0382]: use of moved value: `sat_a`
--> code/ch4-check-sats-2.rs:26:31
 |
20 |     let a_status = check_status(sat_a);
 |                         ----- value moved here
...
26 |     let a_status = check_status(sat_a);
 |                         ^^^^^^ value used here after move
 |
= note: move occurs because `sat_a` has type `CubeSat`,
= which does not implement the `Copy` trait

...
error: aborting due to 3 previous errors

```

To trained eyes, the compiler's message is very helpful. It tells us exactly where the problem is and provides us with a recommendation on how to fix it. To less experienced eyes, it's significantly less useful. We are using a "moved" value and are fully advised to implement the `Copy` trait on `CubeSat`. Huh? Turns out, although it is written in English, the term "move" means something very specific within Rust. Nothing physically moves.

Movement within Rust code refers to movement of *ownership*, rather than movement of data. Ownership is a term used within the Rust community to refer to the compile-time process that checks that every use of a value is valid and that every value will be destroyed cleanly.

Every value in Rust is *owned*. In both Listing 4.1 `sat_a`, `sat_b` and `sat_c` *own* the data that they refer to. When calls to `check_status()` are made, ownership of the data moves from the variables in the scope of `main()` to the `sat_id` variable within the function. The significant difference is that the second example places that integer within a `CubeSat` struct.<sup>14</sup> This type change alters the semantics of how the program behaves.

Here is a stripped down version of the `main()` function from Listing 4.4 , focusing on `sat_a` and places where ownership moves:

#### **Listing 4.6. Extract of <<check-sats2>, focusing on the main() function**

```
fn main() {
    let sat_a = CubeSat { id: 0 };           ①
    let a_status = check_status(sat_a);       ②
    let a_status = check_status(sat_a);       ③
}
```

- ① Ownership originates here at the creation of the `CubeSat` object
- ② Ownership of the object moves to `check_status()`, but is not returned to `main()`
- ③ At this point, `sat_a` is no longer owner of the object, making access invalid

#### **Rebinding is legal when values are not borrowed**

If you have experience with programming languages such JavaScript (from 2015 onwards), you may have been surprised to see that the variables for each of the CubeSats were redefined in Listing 4.4 .

On line 20, `a_status` is assigned to the result of the first call to `check_status(sat_a)`. On line 26, it is reassigned to the result of the second call. The original value is overwritten.

This is legal Rust code, but one must be aware of ownership issues and lifetime here too. It's possible in this context because there are no live borrows to contend with. Attempting to overwrite a value that's still available from elsewhere in the program will cause the compiler to refuse to compile your program.

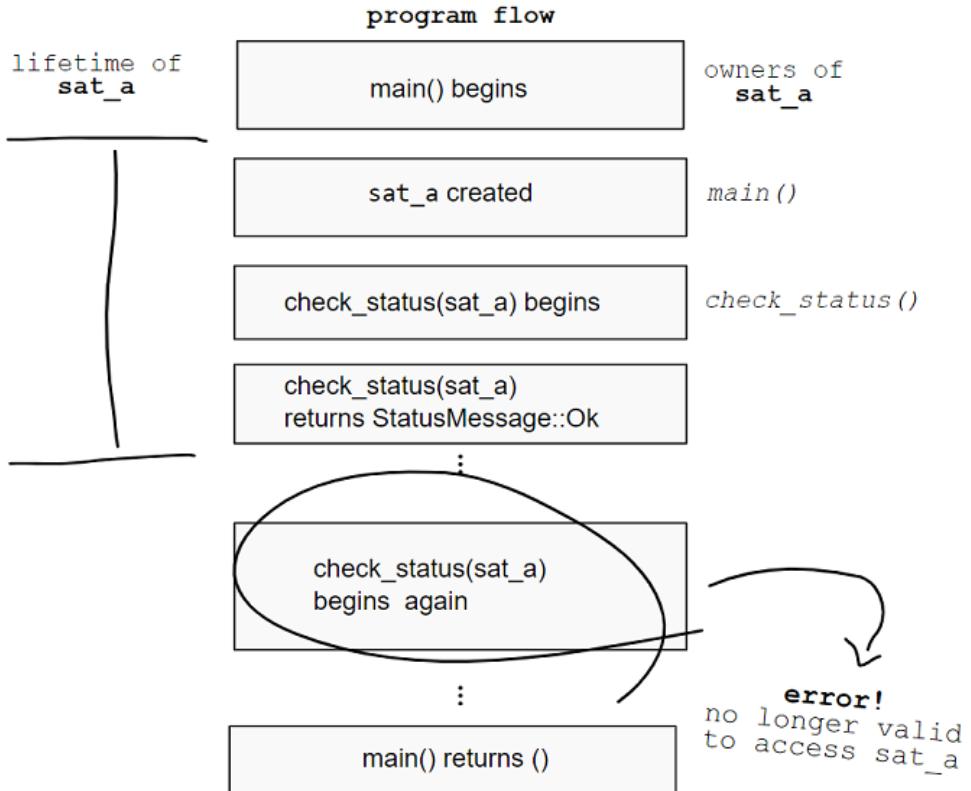
Figure 4.2 provides a visual walk-through of the inter-related processes of control flow, ownership and lifetimes. During the call to `check_status(sat_a)`, ownership *moves* to the `check_status()`function. When `check_status()` returns a `StatusMessage`, it drops the `sat_a` value. The *lifetime* of `sat_a` ends here. Yet, `sat_a` remains in the local scope of `main()` after the first call to `check_status()`. Attempting to access that variable will incur the wrath of the borrow checker.

The distinction between a value's lifetime and its scope—which is what many programmers are trained to rely on—can make things difficult to disentangle. Avoiding and overcoming this type of issue makes up the bulk of the chapter.

---

<sup>14</sup> Remember the phrase zero-cost abstractions? One of the ways this is manifest is by not adding extra data around values within structs.

**Figure 4.2. Visual Explanation of Rust Ownership Movement**



#### 4.1.2 Special behavior of primitive types

Before carrying on, it may be wise to explain why the first code snippet, that is Listing 4.1 , compiled at all. Indeed, the only change that we make at Listing 4.4 was to wrap our satellite variables in a custom type. As it happens, primitive types in Rust have special behavior. They implement the `Copy` trait.

Types implementing `Copy` are duplicated at times would otherwise be illegal. This provides some convenience day-to-day, at the expense of adding a trap for newcomers. As you grow out from toy programs using integers, your code suddenly breaks.

Formally, primitive types are said to possess *copy semantics*, whereas all other types have *move semantics*. Unfortunately for learners of Rust, that special case looks like the default case because they typically encounter primitive types first.

## 4.2 Guide to the figures in this chapter

The figures used in this chapter use a bespoke notation to illustrate the three interrelated concepts of scope, lifetimes and ownership.

**Figure 4.3. How to Interpret the Figures in This Chapter**

### Symbols

 sat\_a     base

 sat\_b     StatusMessage::Ok

 sat\_c     Console

### Actions

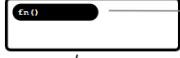
#### Create Value

 Symbol appears

#### Delete Value

 Symbol struck-through

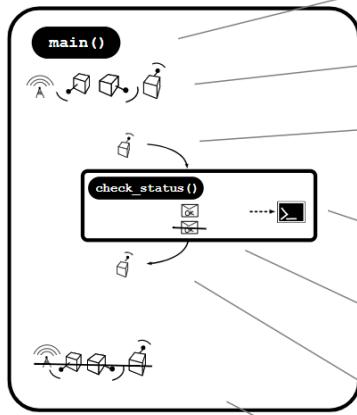
#### Function call

 Arguments  
Function name  
Return values

#### Print to console

..... 

### Example



main() is called

base, sat\_a, sat\_b and sat\_c are created

sat\_c is the sole argument to check\_status()

a message is printed to the console

a StatusMessage::Ok is created, then deleted

sat\_c is returned

base, sat\_a, sat\_b and sat\_c are deleted

## 4.3 What is an Owner? Does it Have any Responsibilities?

In the world of Rust, the notion of *ownership* is rather limited: An owner cleans up when its values' lifetimes end.

When values go out of scope or their lifetimes end for some other reason, their destructors are called. A destructor is a function that removes traces of the value from the program by deleting references and freeing memory. You won't find a call to any destructors in most Rust code. The compiler injects that code itself as part of the process of tracking every value's lifetime.

To provide a custom destructor for a type, implement `Drop`. This will typically be needed in cases where you have used `unsafe` blocks to allocate memory. `Drop` has one method, `drop(&mut self)` that you can use to conduct any necessary wind up activities.

An implication of this system is that values may not outlive their owner. This kind of situation can make data structures built with references, such as trees and graphs, feel slightly bureaucratic. If the root node of a tree is the owner of the whole tree, it can't be removed without taking ownership into account.

Finally, unlike the Lockean notion of personal property, ownership does not imply control or sovereignty. In fact, the "owners" of values do not even have special access to their owned data. Nor do they have an ability to restrict others from trespassing.

Owners don't get a say on other sections of code borrowing their values.

## 4.4 How Ownership Moves

There are two main ways to shift ownership from one variable to another within a Rust program. The first is through assignment.<sup>15</sup> The second is by passing data through a function barrier, either as an argument or a return value.

Revisiting our original code from Listing 4.4 , we can see that `sat_a` starts its life with ownership over a `CubeSat` object.

```
fn main() {
    let sat_a = CubeSat { id: 0 };
    ...
}
```

The `CubeSat` object is then passed into `check_status()` as an argument, moving ownership to the local variable `sat_id`.

```
fn main() {
    let sat_a = CubeSat { id: 0 };
    ...
    let a_status = check_status(sat_a);
    ...
}
```

Another possibility could have been that `sat_a` relinquishes its ownership within `main()` to another variable. That would look something like this:

```
fn main() {
    let sat_a = CubeSat { id: 0 };
    ...
    let new_sat_a = sat_a;
    ...
}
```

Lastly, were there to be a change in the `check_status()` function signature, it too could pass ownership of the `CubeSat` to a variable within the calling scope.

Here is our original function,

```
fn check_status(sat_id: CubeSat) -> StatusMessage {
    StatusMessage::Ok
}
```

and here is an adjusted function that achieves its message notification through a side-effect.

```
fn check_status(sat_id: CubeSat) -> CubeSat {
    println!("{}:{}: {}", sat_id, StatusMessage::Ok); ①
    sat_id ②
}
```

---

<sup>15</sup> Within Rust community, the term variable binding is preferred as is more technically correct.

- ① Use the Debug formatting syntax as our types have use #[derive(Debug)]
- ② Return a value by omitting the semi-colon at the end of the last line

When the adjusted `check_status()` function used in conjunction with a new `main()`, it's possible to see ownership of the `CubeSat` objects back to their original variables. The new code is:

**Listing 4.7. Returning ownership of objects back to their original variables via functions' return values (ch4/ch4-check-sats-3.rs)**

```
#![allow(unused_variables)]

#[derive(Debug)]
struct CubeSat {
    id: u64,
}

#[derive(Debug)]
enum StatusMessage {
    Ok,
}

fn check_status(sat_id: CubeSat) -> StatusMessage {
    println!("{}:{}: {}", sat_id, StatusMessage::Ok);
    StatusMessage::Ok
}

fn main () {
    let sat_a = CubeSat { id: 0 };
    let sat_b = CubeSat { id: 1 };
    let sat_c = CubeSat { id: 2 };

    let sat_a = check_status(sat_a);      ①
    let sat_b = check_status(sat_b);
    let sat_c = check_status(sat_c);

    // "waiting" ...
    let sat_a = check_status(sat_a);
    let sat_b = check_status(sat_b);
    let sat_c = check_status(sat_c);
}
```

- ① Now that the return value of `check_status()` is the original `sat_a`, the new `let` binding is "reset"

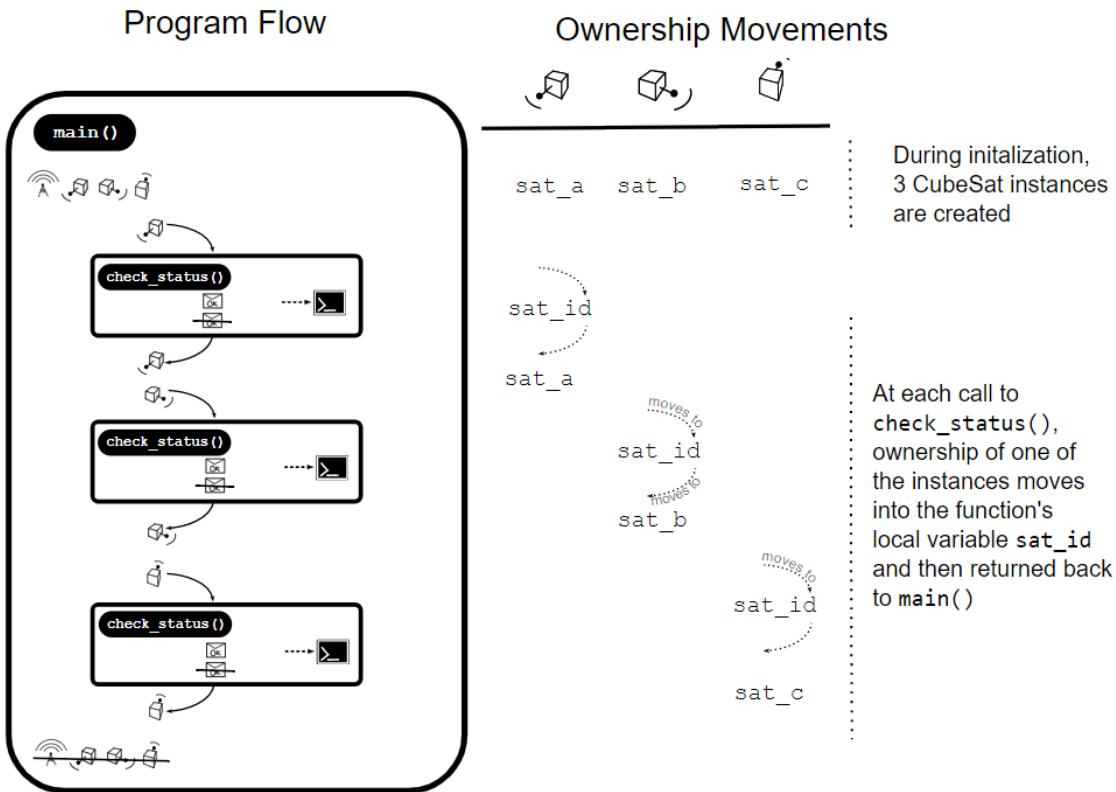
Printing to the console changes, this responsibility has been pushed into `check_status()`. The output from the new `main()` function looks like this:

**Listing 4.8. Output of Listing 4.7**

```
CubeSat { id: 0 }: Ok
```

```
CubeSat { id: 1 }: Ok
CubeSat { id: 2 }: Ok
CubeSat { id: 0 }: Ok
CubeSat { id: 1 }: Ok
CubeSat { id: 2 }: Ok
```

A visual overview of the ownership movements within Listing 4.7 is provided below.



## 4.5 Resolving Ownership Issues

Rust's ownership system is excellent. It provides a route to memory safety without needing a garbage collector. But there is a but. The ownership system can trip you up if you don't understand what's happening. This is particularly the case when you bring the programming style from your past experience to a new paradigm.

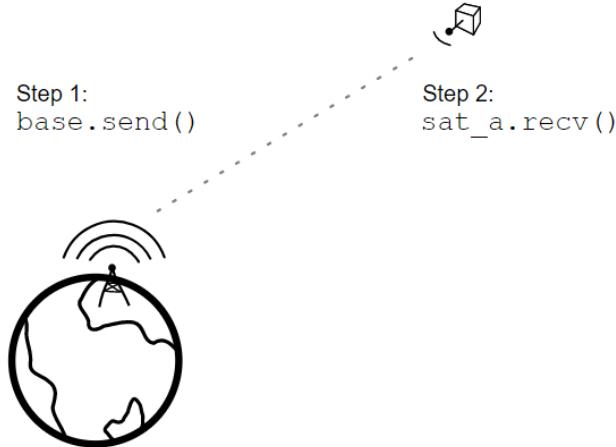
Four general strategies can help with ownership issues:

1. Use references where full ownership is not required
2. Duplicate the value
3. Refactoring code to reduce the number of long-lived objects
4. Wrap your data in a type designed to assist with movement issues

To examine each of these strategies, let's extend the capabilities of our satellite

network. Let's give the ground station and our satellites ability to send and receive messages.

**Figure 4.4. Gameplan: Sending Messages to Our Satellites**



Ignoring the details of implementing the methods, we want to avoid code that looks like this:

```
base.send(sat_a, "hello!"); ①
sat_a.recv();
```

- ① Moving ownership of `sat_a` to a local variable in `base.send()` will end up hurting us. That value will no longer be accessible for the rest of `main()`.

To get to a toy implementation, we will need a few more types to help us out somewhat. In Listing 4.9, a new field is added to `CubeSat`, `mailbox`. `CubeSat.mailbox` is a `Mailbox` struct that contains a vector of `Messages` within its `messages` field. We have aliased `String` to `Message`, giving us the functionality of the `String` type without needing to implement it ourselves.

**Listing 4.9. Adding a Mailbox Type to our System**

```
#[derive(Debug)]
struct CubeSat {
    id: u64,
    mailbox: Mailbox,
}

#[derive(Debug)]
enum StatusMessage {
    Ok,
}
```

```
#[derive(Debug)]
struct Mailbox {
    messages: Vec<Message>,
}

type Message = String
```

Creating a `CubeSat` instance has become slightly more complicated. To create one, we also need to create its associated `Mailbox` and the mailbox's associated `Vec<Message>`.

#### **Listing 4.10. Creating a new CubeSat with Mailbox**

```
CubeSat { id: 100, mailbox: Mailbox { messages: vec![] } }
```

Another type to add is to represent the ground station itself. We will use a bare struct for the moment. That will allow us to add methods to it and give us the option of adding a mailbox as a field later on also.

#### **Listing 4.11. Defining a struct to represent our ground station**

```
struct GroundStation;
```

Creating an instance of `GroundStation` should be trivial for you now.

#### **Listing 4.12. Creating a new ground station**

```
GroundStation {};
```

Now that we have our new types in place, let's put them to work.

### **4.5.1 Use references where full ownership is not required**

The most common change you will make to your code is to reduce the level of access you require. Instead of requesting ownership, use a borrow in your function definitions. For read-only access, use `& T`. For read/write access, use `&mut T`. Ownership might be needed in advanced cases, such as when functions wish to adjust the lifetime of their arguments.

Here is a comparison of the two different approaches.

Using ownership	Using a mutable reference
<pre><code>fn send(to: CubeSat, msg: Message) { ①     to.mailbox.messages.push(msg); }</code></pre> <p>① Moving ownership to the <code>to</code> variable.</p>	<pre><code>fn send(to: &amp;mut CubeSat, msg: Message) {     to.mailbox.messages.push(msg); }</code></pre>

Sending messages will eventually be wrapped up in a method, but in essence functions implementing it must modify the internal mailbox of the `CubeSat`. For simplicity's

sake, we'll return () and hope for the best in case of transmission difficulties caused by solar winds.

Here is the flow that we want to end up with. We send a message to `sat_a` and then receive it.

```
base.send(sat_a, "hello!".to_string());

let msg = sat_a.recv();
println!("sat_a received: {:?}", msg); // -> Option("hello!")
```

and implementations of those two methods.

#### **Listing 4.13. Adding `GroundStation.send()` and `SubeSat.recv()` methods**

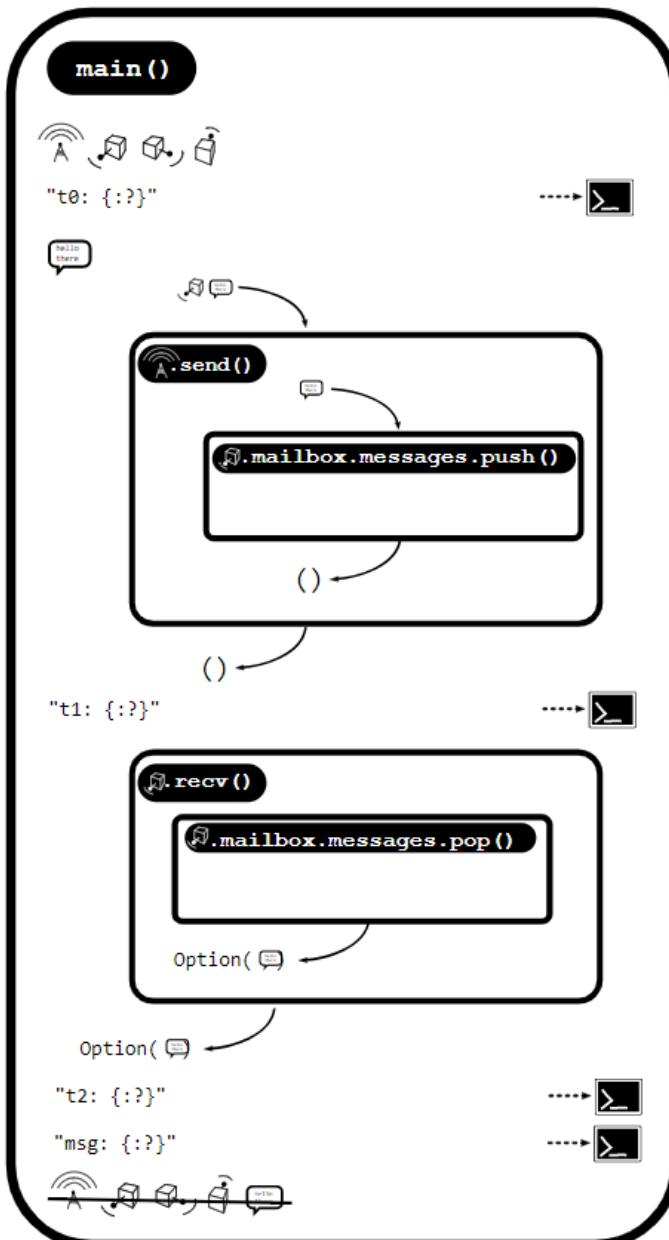
```
impl GroundStation {
    fn send(&self, to: &mut CubeSat, msg: Message) { ① ② ③
        to.mailbox.messages.push(msg); ④
    }
}

impl CubeSat {
    fn recv(&mut self) -> Option<Message> {
        self.mailbox.messages.pop()
    }
}
```

- ① `&self` indicates that `GroundStation.send()` only requires a read-only reference to `self`.
- ② The recipient `to` is taking a mutable borrow (`&mut`) of the `CubeSat` instance
- ③ The `msg` takes full ownership of its `Message` instance
- ④ Ownership of the `Message` instance transfers from `msg` into `messages.push()` as a local variable

Notice that both `GroundStation.send()` and `CubeSat.recv()` require mutable access to a `CubeSat` instance, as both methods are modifying the underlying `CubeSat.messages` vector. We move ownership of the message that we're sending into the `messages.push()`. This will provide us with some quality assurance later, notifying us if we were to access a message after it had already been sent.

**Figure 4.5. Gameplan: Pictorial View of "Avoiding Ownership Issues with References"**



The code listing Listing 4.14 brings together all of the code snippets in this section and prints out the following.

```
t0: CubeSat { id: 0, mailbox: Mailbox { messages: [] } } ①
```

```
t1: CubeSat { id: 0, mailbox: Mailbox { messages: ["hello there!"] } }
t2: CubeSat { id: 0, mailbox: Mailbox { messages: [] } }
msg: Some("hello there!")
```

- ① The output t0 - t2 are added to assist your understanding of how data is flowing through the program.

#### Listing 4.14. Avoiding Ownership Issues with References (ch4/ch4-sat-mailbox.rs)

```
#[derive(Debug)]
struct CubeSat {
    id: u64,
    mailbox: Mailbox,
}

#[derive(Debug)]
struct Mailbox {
    messages: Vec<Message>,
}

type Message = String;

struct GroundStation;

impl GroundStation {
    fn send(&self, to: &mut CubeSat, msg: Message) {
        to.mailbox.messages.push(msg);
    }
}

impl CubeSat {
    fn recv(&mut self) -> Option<Message> {
        self.mailbox.messages.pop()
    }
}

fn main() {
    let base = GroundStation {};
    let mut sat_a = CubeSat { id: 0, mailbox: Mailbox { messages: vec![] } };

    println!("t0: {:?}", sat_a);
    base.send(&mut sat_a, Message::from("hello there!")); ①

    println!("t1: {:?}", sat_a);

    let msg = sat_a.recv();
    println!("t2: {:?}", sat_a);

    println!("msg: {:?}", msg);
}
```

- ① We don't have a completely ergonomic way to create Message instances yet. Instead, we'll take advantage of the `String.from()` method, which converts from `&str` to `String` (aka `Message`).

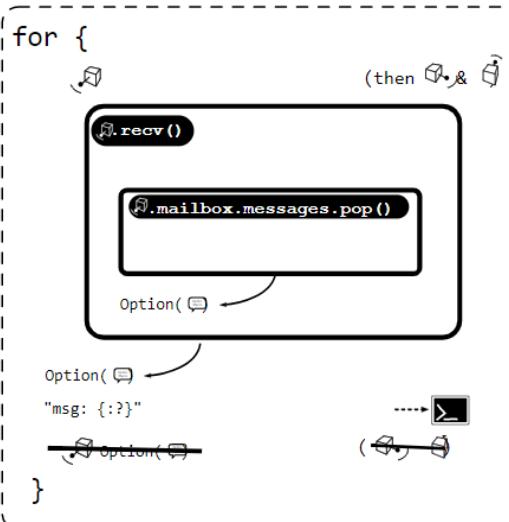
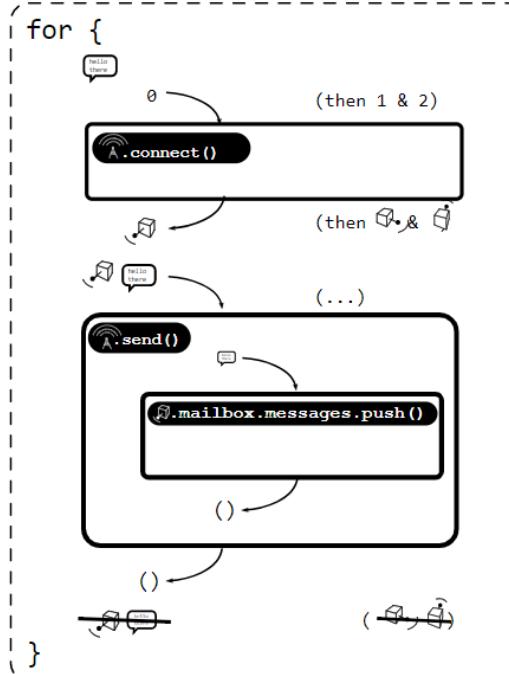
### 4.5.2 Use Fewer Long-Lived Values

If we have a large, long-standing object such as a global variable, it can be somewhat unwieldy to keep this around for every component of your program that needs it. Rather than using an approach of long-standing objects, consider making objects that are more discrete and ephemeral. Ownership issues can sometimes be resolved by considering the design of the overall program.

In our CubeSat case, we don't need to handle much complexity at all. Each of our four variables, `base`, `sat_a`, `sat_b` and `sat_c` live for the duration of `main()`. In a production system, there may be hundreds of different components and many thousands of interactions to manage. To increase the manageability of this kind of scenario, let's break things apart.

**Figure 4.6. Gameplan: Short-Lived Variables**





To implement this kind of strategy, we will create a function that returns CubeSat identifiers. That function is assumed to be a black box that's responsible for

communicating with some store of identifiers, such as a database. Whenever we need to communicate with a satellite, we'll create a new object. In this way, there is no requirement for us to maintain live objects for the whole of the program's duration. It also has the dual benefit that we can afford to transfer ownership of our short-lived variables to other functions.

```
fn fetch_sat_ids() -> Vec<u64> {    ①
    vec![1,2,3]
}
```

① Returns a vector of CubeSat IDs

We'll also create a method for `GroundStation` that allows us to create a `CubeSat` instance on demand once.

```
impl GroundStation {
    fn connect(&self, sat_id: u64) -> CubeSat {
        CubeSat { id: sat_id, mailbox: Mailbox { messages: vec![] } }
    }
}
```

Now we are now somewhat closer to our intended outcome. Our main function looks like the code snippet below. In effect, we've implemented the first half of Figure 4.6 .

```
fn main() {
    let base = GroundStation();

    let sat_ids = fetch_sat_ids();

    for sat_id in sat_ids {
        let mut sat = base.connect(sat_id);

        base.send(&mut sat, Message::from("hello"));
    }
}
```

But there's a problem. Our `CubeSat` instances die at the end of the `for` loop's scope, along with any messages that `base` sends them. To carry on our design decision of short-lived variables, the messages need to live somewhere outside of the `CubeSat` instances. In a real system, they would live on the RAM of a device in zero gravity. In our not-really-a-simulator, let's put them in a buffer object that lives for the duration of our program.

Our message store will be a `Vec<Message>`, aka our `Mailbox` type that we defined in one of the first code examples of this chapter. We'll change the `Message` struct to add a sender and recipient field. That way our now-proxy `CubeSat` instances can match against their id to receive messages.

```
#[derive(Debug)]
struct Mailbox {
    messages: Vec<Message>,
```

```

}

#[derive(Debug)]
struct Message {
    to: u64,
    content: String,
}

```

We also need to re-implement sending and receiving messages. Up until now, CubeSat objects have had access to their own mailbox object. The central GroundStation also had the ability to sneak into those mailboxes to send messages. That needs to change now, as only one mutable borrow may exist per object.

In the modifications below, the Mailbox instance is given the ability to modify its own messages vector. When any of the satellites transmit messages, they take a mutable borrow to the mailbox. They then defer the delivery to the mailbox object. According to this API, our satellites are able to call Mailbox methods, they are just not allowed to touch any internal Mailbox data themselves.

#### **Listing 4.15. Modifications to Mailbox and**

```

impl GroundStation {
    fn send(&self, mailbox: &mut Mailbox, to: &CubeSat, msg: Message) { ①
        mailbox.post(to, msg);
    }
}

impl CubeSat {
    fn recv(&self, mailbox: &mut Mailbox) -> Option<Message> { ②
        mailbox.deliver(&self)
    }
}

impl Mailbox {
    fn post(&mut self, msg: Message) { ③
        self.messages.push(msg);
    }

    fn deliver(&mut self, recipient: &CubeSat) -> Option<Message> { ④
        for i in 0..self.messages.len() {
            if self.messages[i].to == recipient.id { ⑤
                let msg = self.messages.remove(i); ⑥
                return Some(msg);
            }
        }
        None ⑦
    }
}

```

① Sending messages becomes a call to `Mailbox.post()`, yielding ownership of a `Message`

- ② Receiving messages becomes a call to `Mailbox.deliver()`, gaining ownership of a `Message`
- ③ `Mailbox.post()` requires mutable access to itself and ownership over a `Message`
- ④ `Mailbox.deliver()` requires a shared reference to a `CubeSat`, to pull out its `id` field
- ⑤ Astute readers will notice a strong anti-pattern here: mutating a collection while it is being iterated over. This is legal here because of the return on the next line. The compiler can prove that another iteration will not occur and allows this to go through.
- ⑥ When we find a message, return early with the `Message` wrapped in `Some`, per the `Option` type.
- ⑦ When no messages are found, return `None`

With that groundwork in place, we're now able to fully implement the strategy laid out in Figure 4.6 . The output from a compiled version of Listing 4.17 is below, followed by the listing.

#### **Listing 4.16. Output of Listing 4.17**

```
CubeSat { id: 1 }: Some(Message { to: 1, content: "hello" })
CubeSat { id: 2 }: Some(Message { to: 2, content: "hello" })
CubeSat { id: 3 }: Some(Message { to: 3, content: "hello" })
```

#### **Listing 4.17. Implementing the Short-Lived Variables Strategy (ch4/ch4-short-lived-strategy.rs)**

```
#[allow(unused_variables)]

#[derive(Debug)]
struct CubeSat {
    id: u64,
}

#[derive(Debug)]
struct Mailbox {
    messages: Vec<Message>,
}

#[derive(Debug)]
struct Message {
    to: u64,
    content: String,
}

struct GroundStation {}

impl Mailbox {
    fn post(&mut self, msg: Message) {
        self.messages.push(msg);
    }

    fn deliver(&mut self, recipient: &CubeSat) -> Option<Message> {
        for i in 0..self.messages.len() {
```

```

        if self.messages[i].to == recipient.id {
            let msg = self.messages.remove(i);
            return Some(msg);
        }
    }

    None
}
}

impl GroundStation {
    fn connect(&self, sat_id: u64) -> CubeSat {
        CubeSat {
            id: sat_id,
        }
    }

    fn send(&self, mailbox: &mut Mailbox, msg: Message) {
        mailbox.post(msg);
    }
}

impl CubeSat {
    fn recv(&self, mailbox: &mut Mailbox) -> Option<Message> {
        mailbox.deliver(&self)
    }
}

fn fetch_sat_ids() -> Vec<u64> {
    vec![1,2,3]
}

fn main() {
    let mut mail = Mailbox { messages: vec![] };

    let base = GroundStation {};

    let sat_ids = fetch_sat_ids();

    for sat_id in sat_ids {
        let sat = base.connect(sat_id);
        let msg = Message { to: sat_id, content: String::from("hello") };
        base.send(&mut mail, msg);
    }

    let sat_ids = fetch_sat_ids();

    for sat_id in sat_ids {
        let sat = base.connect(sat_id);

        let msg = sat.recv(&mut mail);
        println!("{}:{}: {}", sat_id, sat, msg);
    }
}

```

```

    }
}
```

### 4.5.3 Duplicate the value

Having a single owner for every object can mean significant up-front planning and/or refactoring of your software. As we saw in the previous section, it can be quite a lot of work to wriggle oneself out of an early design decision.

One alternative to refactoring is to simply copy values. Doing this often is typically frowned upon, but it can be useful at a pinch. Primitive types, such as integers, are a good example of that. Primitive types are cheap for a CPU to duplicate. So cheap in fact, that Rust always copies them if it would otherwise worry about ownership being moved.

Types can opt into two modes of being copied: `Clone` and `Copy`. `Copy` acts implicitly whenever ownership would otherwise be moved. The bits of object *a* are replicated to create object *b*. `Clone` acts explicitly. Types that implement `Clone` have a `.clone()` method that is permitted to do whatever it needs to create a new type.

**Table 4.1. Distinguishing Copy and Clone**

Copy	Clone
- always fast and cheap - implementation details are provided by the language—always a bit-for-bit exact copy of the value	- may potentially be expensive - implementation defined by the programmer in a type-specific manner

So why do Rust programmers not always use `Copy`? Well, to implement `Copy`, your types must consist of types that themselves implement `Copy`. Integers and floating point numbers implement `Copy`, but `String` and many other types such as `Vec<T>` do not. The reason `String` and friends do not implement `Copy` is that the types' internal pointers would be duplicated, not the data those pointers refer to. That could lead to multiple values pointing to the same data, leading to compiler confusion about which one is responsible for that data.

### IMPLEMENTING COPY

Let's go back to our original example (Listing 4.4) that caused the original movement issue. Here it is replicated for convenience, with `sat_b` and `sat_c` removed for brevity.

```

#[derive(Debug)]
struct CubeSat {
    id: u64,
}

#[derive(Debug)]
enum StatusMessage {
    Ok,
}
```

```

fn check_status(sat_id: CubeSat) -> StatusMessage {
    StatusMessage::Ok
}

fn main() {
    let sat_a = CubeSat { id: 0 };

    let a_status = check_status(sat_a);
    println!("a: {:?}", a_status);

    let a_status = check_status(sat_a); ①
    println!("a: {:?}", a_status);
}

```

① The second call to `check_status(sat_a)` is the location of error

At this stage, our program consisted of types that contain types that themselves implement `Copy`. That's good, as it means implementing it ourselves is fairly straightforward:

#### **Listing 4.18. Deriving Copy for Types That are Made Up of Types That Implement Copy Themselves**

```

#[derive(Copy,Clone,Debug)] ①
struct CubeSat {
    id: u64,
}

#[derive(Copy,Clone,Debug)] ①
enum StatusMessage {
    Ok,
}

```

① Adding `#[derive(Copy)]` tells the compiler to add an implementation itself

It's also possible to implement `Copy` manually. The `impl` blocks are impressively terse.

#### **Listing 4.19. Implementing Copy Manually**

```

impl Copy for CubeSat { }

impl Copy for StatusMessage { }

impl Clone for CubeSat { ①
    fn clone(&self) -> Self {
        CubeSat { id: self.id } ②
    }
}

impl Clone for StatusMessage {
}

```

```

fn clone(&self) -> Self {
    *self
}
}

```

- ① Implementing Copy requires an implementation of Clone
- ② If desired, we can write out the creation of a new object ourselves..
- ③ ..but often we can simply dereference self

## USING CLONE AND COPY

Now that we know how to implement them, let's put `Clone` and `Copy` to work.

We've discussed that `Copy` is implicit. Whenever ownership would otherwise move, such as during assignment and passing through function barriers, data is copied instead. `Clone` requires an explicit call to `.clone()`. That's a useful marker in non-trivial cases such as this example, because it warns the programmer that the process may be expensive.

**Listing 4.20. Using Clone and Copy (ch4/ch4-check-sats-clone-and-copy-traits.rs)**

```

#[derive(Debug,Clone,Copy)]    ①
struct CubeSat {
    id: u64,
}

#[derive(Debug,Clone,Copy)]    ①
enum StatusMessage {
    Ok,
}

fn check_status(sat_id: CubeSat) -> StatusMessage {
    StatusMessage::Ok
}

fn main () {
    let sat_a = CubeSat { id: 0 };

    let a_status = check_status(sat_a.clone());    ②
    println!("a: {:?}", a_status.clone());          ②

    let a_status = check_status(sat_a);            ③
    println!("a: {:?}", a_status);                  ③
}

```

- ① Copy implies `Clone`, so we can use either trait later on
- ② Cloning each object is as easy as calling `.clone()`
- ③ Copy works as expected

#### 4.5.4 Wrap Data Within Specialty Types

This chapter, we have been discussing Rust's ownership system and ways to navigate the constraints it imposes. A final strategy that is quite common is to use "wrapper" types that present a façade to the outside world of move semantics, but actually are doing something special under the hood.

**NOTE**

This section is merely a brief introduction. These wrapper types will be explained in much more detail in Part 2 of the book an beyond.

Rust allows programmers to opt-in to runtime garbage collection. To explain this, we'll need to introduce some new notation. `Rc<T>` means a "reference counted type `T``". We could wrap a single instance of `GroundStation` in a `Rc`, providing shared access to each of the satellites. Setting up that scenario involves a call to the `Rc::new()` static method.

**Listing 4.21. Wrapping a User-Defined Type in Rc (ch4/ch4-rc-groundstation.rs)**

```
use std::rc::Rc;      ①

#[derive(Debug)]
struct GroundStation {}

fn main() {
    let base: Rc<GroundStation> = Rc::new(GroundStation {});  ②

    println!("{:?}", base);
}
```

① The `use` keyword brings modules from the standard library into local scope

② "Wrapping" involves enclosing the `GroundStation` instance in a call to `Rc::new()`

`Rc<T>` implements `Clone`. Every call to `base.clone()` increments an internal counter. Every `Drop` decrements that counter. When the internal counter reaches zero, the original instance is freed.

`Rc<T>` does not allow mutation. To permit that, we need to wrap our wrapper. `Rc<RefCell<T>>` is a type that can be used to perform *interior mutability*. An object that has interior mutability presents an immutable façade, while internal values are being modified.

In the following example, the variable `base` is able to be modified despite being marked as an immutable variable. It's possible to visualize this by looking at the changes to the internal `base.radio_freq`.

```
base: RefCell { value: GroundStation { radio_freq: 87.65 } }
base_2: GroundStation { radio_freq: 75.31 }
base: RefCell { value: GroundStation { radio_freq: 75.31 } }
base: RefCell { value: "<borrowed>" }  ①
base_3: GroundStation { radio_freq: 118.52000000000001 }
```

- ① value: "borrowed" indicates that base has been mutably borrowed by somewhere else, and is no longer generally accessible

An important consideration to remember is that Rust's guarantees remain. They become enforced at runtime. It is certainly possible to cause runtime panics if you ignore the ownership and borrowing rules.

**Listing 4.22. Using Rc<RefCell<T>> to Permit Mutation Within an Object Marked Immutable**

```
use std::rc::Rc;
use std::cell::RefCell;

#[derive(Debug)]
struct GroundStation {
    radio_freq: f64 // MHz
}

fn main() {
    let base: Rc<RefCell<GroundStation>> = Rc::new(RefCell::new(
        GroundStation {
            radio_freq: 87.65
        }
    ));

    println!("base: {:?}", base);

    { // introduce a new scope
        let mut base_2 = base.borrow_mut();
        base_2.radio_freq -= 12.34;
        println!("base_2: {:?}", base_2);
    }

    println!("base: {:?}", base);

    let mut base_3 = base.borrow_mut();
    base_3.radio_freq += 43.21;

    println!("base: {:?}", base);
    println!("base_3: {:?}", base_3);
}
```

Adding more functionality—for example, reference counting semantics rather than move semantics—from types reduces their runtime performance. `Rc<T>` can be handy when implementing `Clone` would be prohibitively expensive.

**NOTE**

`Rc<T>` is not threadsafe. Replace `Rc<T>` with `Arc<T>` for atomic reference counter and `Rc<RefCell<T>>` with `Arc<Mutex<T>>`<sup>16</sup>.

## 4.6 Summary

In this chapter you learned that:

- A value's *owner* is responsible for cleaning up after that value when its lifetime ends.
- A value's *lifetime* is the period when accessing that value is valid behavior. Attempting to access a value after its lifetime has expired will lead to code that won't compile.
- To *borrow* a value means to access that value
- Several tactics are available to you if you find that the borrow checker won't allow your program to compile. This often means that you will need to rethink the design of your program.
- Use shorter-lived values, rather than values that stick around for a long time.
- Borrows may be read-only or read/write. Only one read/write borrow may exist at any one time.
- Duplicating a value can be a pragmatic way to break an impasse with the borrow checker. To duplicate a value, implement `Clone` or `Copy`.
- It's possible to opt-in to reference counting semantics through `Rc<T>`
- Rust supports a feature known as *interior mutability* that enables types to present themselves as immutable, even though their values can change over time

---

<sup>16</sup> Actually, Mutex is one of a number of options. Atomic operations are often also equally valid.



# 5

## Data in Depth

**This chapter covers:**

- Learn how data is represented in the computer
- Build a working CPU emulator
- Create your own a numeric data type
- Understand the inner workings of floating point numbers

This chapter is all about understanding how zeroes and ones can be built up to become much larger objects such text, images and sound. We will also touch upon how computers do computation. By the end of the chapter, you will have emulated a fully-functional computer with CPU, memory and user-defined functions. You will break apart floating point numbers to create a numeric data type of your own making that only takes up a single byte. The chapter introduces a number of terms that may not be familiar to programmers who have never done systems programming, such as *endianness* and *integer overflow*.

### 5.1 Bit Patterns and Types

A small but important lesson is that a single bit pattern can mean different things. The type system of a higher-level language, such as Rust, is just an artificial abstraction over reality. Understanding this becomes important as you begin to unravel some of that abstraction and to gain a deeper understanding of how computers work.

Listing 5.2 is an example that uses the same bit pattern to represent two different numbers. The type system—not the CPU—is what makes the distinction.

**Listing 5.1. Output of Listing 5.2**

```
a: 1100001111000011 50115
b: 1100001111000011 -15421
```

**Listing 5.2. Int vs Int (ch4-int-vs-int.rs)**

```
fn main() {
    let a: u16 = 50115;
    let b: i16 = -15421;

    println!("a: {:016b} {}", a, a);      ①
    println!("b: {:016b} {}", b, b);
}
```

① Note that these two values have the same bit pattern, but different types

The different mapping between bit strings and numbers explains part of the distinction between "binary" files and "text" files. Text files are just binary files that happen to follow a consistent mapping between bit strings and characters. This mapping is called an encoding. Arbitrary files don't describe their meaning to the outside world, which makes them very opaque.

We can take this process one step further. What happens if we ask Rust to treat a bit pattern produced by one type as another?

**Listing 5.3 Inspecting a Float's Bit String by Interpreting its bits as an Integer (ch5-f32-as-u32.rs)**

```
fn main() {
    let a: f32 = 42.42;
    let frankentype: u32 = unsafe {
        std::mem::transmute(a)           ①
    };

    println!("{:032b}", frankentype);   ②
}
```

① Note, no semi-colon here. We want the result of the expression to feed into the outer scope.

② The {:032b} syntax means format as a binary (via invoking the `fmt::Binary` trait) with zeros padded on the left to fill 32 places. Without 032, leftmost bits with a value of 0 would be truncated in the output.

To print a value as individual bits, the type of that value must implement `fmt::Display`. `f32` doesn't implement `fmt::Binary`, but integer types do. There are two integer types guaranteed to take up the same number of bits as `f32`, `i32` and `u32`. The decision is somewhat arbitrary.<sup>17</sup> [or even `[i16; 2]` for that matter.] Let's use `u32`. So, now we need a way to treat an `f32` as an `u32`, without affecting any

---

<sup>17</sup> Other options for the curious reader to explore are arrays, such as `[u8; 4]`

of the underlying bits. That's what `std::mem::transmute` does. It allows us to tell the compiler that we know best and to treat one value's data as if it is actually another type.

**TIP**

The keyword `unsafe` does not imply inherently dangerous. It is a marker to indicate that the programmer is fully responsible for maintaining the program's integrity.

Mixing data types underneath a program is inherently chaotic, so we need to wrap the operation within an `unsafe` block. `unsafe` tells the Rust compiler, "Stand back, I'll take care of things from here. I've got this.". Unsafe Rust is exactly the same language as safe Rust. It just does its work without the benefit of the compiler's guarantees. As we peek at and poke individual bytes during the course of the book, we'll be using `unsafe` sections of code.

When compiled and run, the code from Listing 5.3 produces the following output:

```
01000010001010011010111000010100
```

## 5.2 Life of an integer

During earlier chapters, we spent some time discussing what it means for an integer to be an `i32` or a `u8` or a `usize`.

Integers are like small, delicate fish. They do what they do remarkably well, but take them outside of their natural range and they die a quick, painful death.

Integers live within a fixed range. When represented inside the computer, they occupy a fixed number of bits per type. Unlike floating point numbers, they cannot sacrifice their precision to extend their bounds. Once those bits have been filled up with ones, the only way forward is back to all zeros.

A 16-bit integer can represent 65,535 unique numbers. What happens when you want to count to 65,536? Let's find out.

The technical term for the class of problem that we are investigating is *integer overflow*. One of the most innocuous ways of overflowing an integer is by incrementing forever. Listing 5.5 is a trivial example of this.

### **Listing 5.4. Output of Listing 5.5**

```
0...
1000..2000..3000..4000..5000..6000..7000..8000..9000..10000..
11000..12000..13000..14000..15000..16000..17000..18000..19000..20000..
21000..22000..23000..24000..25000..26000..27000..28000..29000..30000..
31000..32000..33000..34000..35000..36000..37000..38000..39000..40000..
41000..42000..43000..44000..45000..46000..47000..48000..49000..50000..
51000..52000..53000..54000..55000..56000..57000..58000..59000..60000..
thread 'main' panicked at 'attempt to add with overflow', ch5-to-oblivion.rs:5:7
note: Run with `RUST_BACKTRACE=1` for a backtrace.
61000..62000..63000..64000..65000..
```

**Listing 5.5. Incrementing an Integer Past its Range (ch4-to-oblivion-and-beyond.rs)**

```
fn main() {
    let mut i: u16 = 0;
    print!("{}..", i);

    loop {
        i += 1000;
        print!("{}..", i);
        if i % 10000 == 0 {
            print!("\n")
        }
    }
}
```

When we try to run Listing 5.5 , things don't end well for our program:

```
thread 'main' panicked at 'attempt to add with overflow', /path/to/ch4-u16-to-
oblivion-and-beyond.rs:6
note: Run with `RUST_BACKTRACE=1` for a backtrace.
```

A panicked program is a dead program. A panic means that the programmer has asked the program something that's impossible. It doesn't know what to do to proceed and shuts itself down.

To understand why this is such a critical class of bug, let's take a look at what's going on under the hood. Here is a program that prints out six numbers with their bit patterns laid out in literal form.

**TIP**

Try compiling the code with optimizations enabled via `rustc -O ch5-to-oblivion.rs` and running the resulting executable. The behavior is quite different.

When compiled, Listing 5.6 should print out the following short line:

```
0, 1, 2, ..., 65533, 65534, 65535
```

**Listing 5.6. u16 Bit Patterns**

```
fn main() {
    let zero: u16          = 0b0000_0000_0000_0000;
    let one: u16           = 0b0000_0000_0000_0001;
    let two: u16           = 0b0000_0000_0000_0010;
    // ...
    let sixtyfivethousand_533: u16 = 0b1111_1111_1111_1101;
    let sixtyfivethousand_534: u16 = 0b1111_1111_1111_1110;
    let sixtyfivethousand_535: u16 = 0b1111_1111_1111_1111; ①

    print!("{}{}, {}{}, {}, ...{}, {}, {}");
    println!("{}{}, {}{}, {}{}", sixty5_533, sixty5_534, sixty5_535);
}
```

① The problem we're interested in is what happens when there's no more space left.

There is another easy way to kill a program using a similar technique. In this case, we ask Rust to fit 400 into an u8, which can only count up to 255 values.

#### **Listing 5.7. Impossible Addition (ch5/ch5-impossible-addition.rs)**

```
fn main() {
    let (a, b) = (200, 200);
    let c: u8 = a + b;      ①
    println!("200 + 200 = {}", c);
}
```

① The type declaration is important here. Without it, your code will probably work just fine.

The code compiles, but one of two things happen:

- The program panics:

```
thread 'main' panicked at 'attempt to add with overflow', {chapter}-impossible-
add.rs:3:15
note: Run with `RUST_BACKTRACE=1` for a backtrace
```

**This behavior can be invoked via executing rustc with its default options: rustc ch5-
impossible-add.rs && ch5-impossible-add**

- The program gives you the wrong answer:

```
200 + 200 = 144
```

**This behavior can be invoked by executing rustc with the -O flag: rustc -O ch5-
impossible-add.rs && ch5-impossible-add**

There are two small lessons here.

- Rust programs can easily break
- It's important to understand the limitations of your types

Developing strategies for preventing integer overflow is one of the ways that systems programmers are distinguished from others. Programmers who only have experience with dynamic languages are extremely unlikely to encounter an integer overflow. Dynamic language runtimes will check to see that the result of integer expressions will be able to fit. When they can't, the variable that's receiving the result will be promoted to a wider integer type.

When developing performance critical code, you get to choose which parameters to adjust. If you use fixed-sized types, you gain speed and you need to accept some risk. To mitigate that risk, you can check to see that overflow won't occur at runtime. Imposing those checks will slow you down. Another, much more common option, is to sacrifice space by using a large integer type, such as i64. To go higher still, you'll need to move to arbitrary size integers, which come with their own costs.

### 5.2.1 Understanding Endianness

CPUs argue about which way round integers—actually all byte sequences—should be. Some prefer byte sequences to be from left-to-right and others prefer them right-to-left. This preference is known as a CPU’s *endianness*. The problem of endianness is one of the reasons why copying an executable file from one computer to another might not work.

Let’s consider a 32-bit integer that is representing the number made up of four bytes: AA, BB, CC and DD. Listing 5.8 , with the help of our friend `sys::mem::transmute`, demonstrates that byte order matters.

When compiled and executed, the code from Listing 5.8 will print out one of two things, depending on the endianness of your machine.

Most computers these days that people run for day-to-day work will print out

```
-573785174 vs -1430532899
```

but more exotic hardware swaps the two numbers around

```
-1430532899 vs -573785174
```

#### **Listing 5.8. Inspecting Endianness (ch5-endianness.rs)**

```
use std::mem;

fn main() {
    let big_endian: [u8; 4] = [
        0xAA, // 1101_1101
        0xBB, // 1100_1100
        0xCC, // 1011_1011
        0xDD, // 1010_1010
    ];

    let little_endian: [u8; 4] = [
        0xDD, // 1010_1010
        0xCC, // 1011_1011
        0xBB, // 1100_1100
        0xAA, // 1101_1101
    ];

    let (a,b): (i32, i32) = unsafe {
        (mem::transmute(big_endian), mem::transmute(little_endian))
    };

    println!("{} vs {}", a, b);
}
```

The terminology comes from the "significance" of the bytes in the sequence. To take you back to when you learned addition, we can factor the number 123 into three parts:

$100 \times 1$	100
$10 \times 2$	20
$1 \times 3$	3

Summing all of these parts gets us back to our original number. The first part, 100, is labelled as the "most significant". When written out in the conventional way, 123 as 123, we are writing in *big endian* format. Were we to invert that ordering, i.e. by writing 123 as 321, we would be writing in *little endian* format. Binary numbers work in a very similar way.

Each number part is a power of 2 ( $2^0, 2^1, 2^2, \dots, 2^n$ ), rather than a power of 10 ( $10^0, 10^1, 10^2, \dots, 10^n$ ).

Before the late-1990s, endianness was a very big issue, especially in the server market. Glossing over the fact that a number of processors can support bidirectional endianness, Sun Microsystems, Cray, Motorola and SGI went one way. Intel and ARM went the other way. The other way won. Integers are almost certainly stored in *little endian* format.

In addition to multi-byte sequences, there is a related problem within a byte. Should a u8 that represents 3 look like `0000_0011` or should it look like `1100_0000`? The computer's preference for layout of individual bits is known as its *bit numbering* or *bit endianness*. It's very unlikely that this internal ordering will affect your day-to-day programming. To investigate further, look for your platform's details on which end its *most significant bit* lies

**TIP**

The abbreviation **MSB** can be deceptive. Authors use the same abbreviation to refer to both **most significant bit** (bit numbering) and **most significant byte** (endianness).

## 5.3 Decimal Numbers

One of the claims made at the start of this chapter was that understanding more about bit patterns should enable you to compress your data. Let's put that into practice. In this section, you will learn how to pull bits out of a floating point number and injecting them into a single byte format of your own creation.

Here is some context for the problem at hand: Machine learning practitioners often need to store and distribute large models. A model, for our purposes here, is just a large array of numbers. The numbers within those models often fall within the ranges  $0..1$  or  $-1..1$ , depending on the application. Given we don't need the whole range that f32 or f64 support, why use all of their bytes? Let's see how far we can get with 1. Because there is a known limited range, it's possible to create a decimal number format that can model that range compactly.

To start, we're going to need to learn about how decimal numbers are represented inside today's computers. We're going to need to learn about the internals of floating point.

### 5.3.1 About Floating Point

Each floating point number is laid out in memory as scientific notation. If you're unfamiliar with scientific notation, here is a very quick primer. Scientists will describe the mass of Jupiter as “ $1.898 \times 10^{27}$  kg” and the mass of an ant as “ $3.801 \times 10^{-4}$  kg”. The key insight is that the same number of characters are used to describe vastly different scales. Computer scientists have taken advantage of that insight to create a fixed-width format that encodes a very wide range numbers.

Each position within a number in scientific notation is given a role:

- a sign, which is implied in our two examples, would be present for negative numbers (-)
- the *mantissa*, also known as the  *significand*, can be thought of as being the value in question (1.898 and 3.801)
- the *radix*, is the value that is raised to the power of the exponent (10 in both of our examples)
- the *exponent*, which describes the scale of the value (27 and -4)

This crosses over to floating point quite neatly. A floating point value is a container with three fields:

- a sign bit
- an exponent
- a mantissa

The radix is implied.

Our task is to extract each field from its container. This is slightly tricky, as they are not aligned at the edge of a byte. Therefore, we'll need to learn some bit manipulation techniques to get at them.

Each field requires a slightly different technique to extract the value. Listing 5.10 goes through the process of deconstructing and reconstructing the number 42.42. If you are familiar with bit manipulation, the code should be straightforward. If not, an extensive guide to what is going on follows the code.

The three main operations that are new are:

- “Right shift” (`n >> m`) where  $n$  and  $m$  are both integers. This operation moves bits towards the right and pads the now-empty left bits with zeros. The new value can now be interpreted as an integer in its own right. This technique is used to isolate the sign bit and the mantissa.
- “AND mask” (`n & m`). This operation is used as a filter. It allows you to selectively choose which bits to retain by adjusting  $m$  to suit.
- “Left shift” (`n << m`), with  $m$  typically being 1. This operation is used to create the  $m$  value for a subsequent AND mask. That is, we will be dynamically creating filters to isolate individual bits as the program progresses.

Those three operations are expanded upon after the code listing. When Listing 5.10 is run, its output is a visual marker of the process that it has undertaken:

### **Listing 5.9. Output from Listing 5.10**

```
42.42 -> [sign:0, exponent:32, mantissa:1.325625] -> 42.42
```

### **Listing 5.10. Deconstructing a Floating Point Value with Bit Manipulation Techniques**

```
const BIAS: i32 = 127;          ①
const RADIX: f32 = 2.0;         ①

fn main() {                      ②
    let n: f32 = 42.42;

    let (signbit, exponent, fraction) = deconstruct_f32(n);           ③
    let (sign, exponent, mantissa) = decode_f32_parts(signbit, exponent, fraction);
    ④
    let reconstituted_n = f32_from_parts(sign, exponent, mantissa);      ⑤

    println!("{} -> [sign:{}, exponent:{}, mantissa:{}{:?}] -> {}", n, signbit,
exponent, mantissa, reconstituted_n);
}

fn deconstruct_f32(n: f32) -> (u32, u32, u32) {
    let n_: u32 = unsafe { std::mem::transmute(n) };

    let sign      = (n_ >> 31) & 1;          ⑥
    let exponent = (n_ >> 23) & 0xff;        ⑦
    let fraction = 0b00000000_01111111_11111111_11111111 & n_;           ⑧

    (sign, exponent, fraction)           ⑨
}

fn decode_f32_parts(sign: u32, exponent: u32, fraction: u32) -> (f32, f32, f32) {
    let signed_1 = (-1.0_f32).powf(sign as f32);      ⑩

    let exponent = (exponent as i32) - BIAS;          ⑪
    let exponent = RADIX.powf(exponent as f32);        ⑪

    let mut mantissa: f32 = 1.0;           ⑫
    for i in 0..23_u32 {                  ⑬
        let one_at_bit_i = 1 << i;          ⑭
        if (one_at_bit_i & fraction) != 0 {   ⑮
            mantissa += 2_f32.powf((i as f32) - 23.0);  ⑯
        }
    }

    (signed_1, exponent, mantissa)
}
```

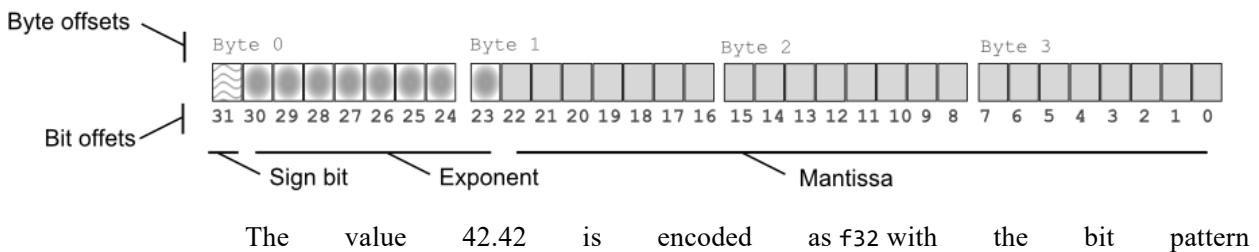
```
fn f32_from_parts(sign: f32, exponent: f32, mantissa: f32) -> f32 {    ⑯
    sign * exponent * mantissa
}
```

- ① Similar constants are accessible via the `std::f32` module
- ② `main()` can live happily at the beginning of a file
- ③ Here the three components of `n` are extracted, with each one being an untyped sequence of bits
- ④ Each component is interpreted according to the standard
- ⑤ The original value is produced from the three decoded components
- ⑥ Strip 31 unwanted bits away by shifting them into nowhere, leaving only the sign bit
- ⑦ Filter out the top bit with a logical AND mask, then strip 23 unwanted bits away
- ⑧ Only retain the 23 “least significant” bits via an AND mask
- ⑨ The mantissa part is called a fraction here, as it becomes the mantissa once it’s decoded
- ⑩ Convert the sign bit to 1.0 or -1.0. Parentheses are required around `-1.0_f32` to clarify operator precedence as method calls rank higher than unary minus.
- ⑪ We need to do a bit of a type dance here. `exponent` must become an `i32` in case subtracting the BIAS results in a negative number. Then it needs to be cast as a `f32`, so that it can be used for exponentiation.
- ⑫ We start by assuming that the implicit 24th bit is set. That has the upshot of defaulting the mantissa’s value as 1.
- ⑬ We provide a concrete type here to ensure that the bit patterns that are generated by the mask are defined
- ⑭ At each iteration, create an AND mask of a single bit in the position that we’re currently interested in.
- ⑮ Any non-zero result means that the bit is present within `fraction`
- ⑯ To arrive at the decimal value of the bit at `i`, we find  $2^{i-23}$ . -23 means that the result gets smaller when `i` is close to 0, as desired.
- ⑰ This code cheats a bit by using `f32` values in intermediate steps. Hopefully it is a forgivable offense.

Understanding how to unpack bits from bytes will mean that you’ll be in a much stronger position when you’re faced with interpreting untyped bytes flying in from the network.

### 5.3.2 Looking inside an `f32`

**Figure 5.1. An overview of the three components encoded within the bits of a floating point number. The layout corresponds to the `f32` type in Rust, called `binary32` within the IEEE 754-2008 standard and `single` by its predecessor IEE 754-1985.**



01000010001010011010111000010100. Here are the values of each of the three fields and what they represent:

**Table 5.1. The components of the f32 0x4229AE14**

Component name	Component in binary	Component as base-10 (u32)	Decoded Value
Sign bit	0	0	1
Exponent	10000100	132	5
Mantissa/Significand	1010011010111000010100	2,731,540	1.325625
Radix*			2
Exponent bias*			127

\* Defined by the standard

To convert the bit pattern to a decimal number, we follow the equation

$$n = -1^{sign\_bit} \times RADIX^{(exponent - EXPONENT\_BIAS)} \times mantissa$$

which looks like this with the values from Table 5.1:

$$42.42 = -1^1 \times 2^{(132 - 127)} \times 1.325625$$



## ABOUT THE SIGN BIT

The *sign bit* is a single bit that indicates which size of zero the decimal number lies on.

### Notes

1 represents negative numbers and 0 positive ones.

### Special Cases

- 0 and 0 have different bit patterns in memory, but compare as equal.

## HOW TO ISOLATE THE SIGN BIT

Shift the other bits out of the way. For f32, this involves a right shift 31 places (`>> 31`).

Steps:

- Cast f32 as u32 to allow for bit manipulation.

```
let n: u32 = unsafe { std::mem::transmute(42.42_f32) };
```



↖ The issue that needs to be resolved is the sign bit's position. Treated naïvely, it represents 4,294,967,296 ( $2^{32}$ ) or 0, rather than 1 ( $2^0$ ) or 0.

- Shift the bits within  $n$  31 places to the right.

```
let sign_bit = n >> 31;
```



↖ Sign bit has now been positioned in the "least significant" position.



## ABOUT THE EXPONENT

### Notes

To decode the exponent, treat bits as an integer then subtract 127 from the result. 127 is known as the “bias”.

### Special Cases

- 0x00 (0b00000000) indicates that the mantissa should be treated as a “subnormal number”. This increases how many decimal numbers near zero that can be represented.
- 0xFF (0b11111111) indicates that the decimal number is infinity ( $\infty$ ), negative infinity ( $-\infty$ ) or “Not a Number”. Not a Number values indicate special cases where the numeric result is mathematically undefined, such as  $0 \div 0$ , or that are otherwise invalid.

### How to Isolate the Exponent

Shift bits 31-22 rightwards to bit 0. Then strip away the sign bit with a AND mask. Interpret the remaining 8 bits as an integer, then remove the bias (127) to produce the actual exponent.

Steps:

1. Cast f32 as u32 to allow for bit manipulation

```
let n: u32 = unsafe { std::mem::transmute(42.42_f32) };
```



↖ Problem: Exponent bits are not aligned to the right.

2. Shift bits to the right

```
let exponent_: n >> 23;
```



Problem: Sign bit remains at bit 8.

- Filter the sign bit away with an AND mask. Only non-zero bits in the mask can pass through.

```
let exponent_: exponent_ & 0b00000000_00000000_00000000_11111111;
```



Sign bit has now been removed.

- Subtract the exponent bias, as defined by the standard.

```
let exponent: (exponent_ as i32) - 127; ①
```

① Casting the exponent bits an i32 allows a negative value to be represented.

## ABOUT THE MANTISSA

### Notes

Each bit represents a known value defined by the floating point standard. To calculate the mantissa, iterate through each bit  $i$ , adding  $2^{i-23}$  to a temporary variable when ' $i$ 'th bit equals 1. The bits represent 0.5 ( $2^{-1}$ ), 0.25 ( $2^{-2}$ ), through to 0.00000011920928955078125 ( $2^{-23}$ ). An implicit 24th bit that represents 1.0 ( $2^0$ ) is always on, except when special cases are triggered.

### Special Cases

The state of the exponent can trigger special treatment of the mantissa.

- When the exponent is 255 (0b11111111), infinity ( $\infty$ ) is represented by 0 in the mantissa and every other bit pattern represents Not a Number.
- When the exponent is 0 (0b00000000), zero is represented by 0 in the mantissa. Every non-zero bit pattern in the mantissa switches the implicit 24th to 0.0.

### How to Isolate the Mantissa

Iterate through the fractional bits of the mantissa, adding their value to a variable mantissa initialised with the value of the implicit 24th bit (1.0). Special cases are not handled in the steps below, but involve returning early with sentinel values for infinity/-infinity/Not a Number or subtracting 1.0 from the mantissa variable.

Steps:

- Cast f32 as u32 to allow for bit manipulation

```
let n: u32 = unsafe { std::mem::transmute(42.42_f32) };
```

2. Create a mutable f32 value initialized to 1.0 ( $2^0$ ).

```
let mut mantissa: f32 = 1.0;
```

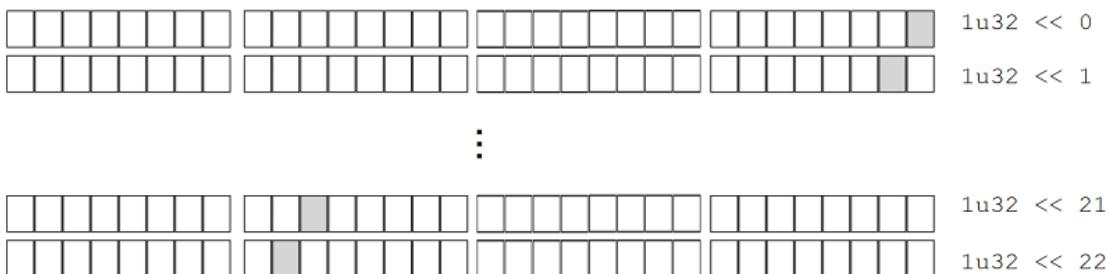
3. Iterate through the fractional bits of the mantissa, adding that bit's defined value to the mantissa variable.

```
for i in 0..23_u32 {
    let one_at_bit_i = 1 << i;
    if (one_at_bit_i & fraction) != 0 {
        let i_ = i as f32;
        mantissa += 2_f32.powf( i_ - 23.0 );
    }
}
```

- ① Specifying the type (u32) allows the bit shifting machinery to work by clarifying the intended number of bits.
- ② The syntax  $1 \ll i$  creates a bit pattern with a 1 at position  $i$  and zero everywhere else.  
When  $i$  equals 5, the bit pattern is `0b00000000_00000000_00000000_00100000`

**Figure 5.2. Illustrating how left shift works to isolate individual bits**

This figure shows the effect of left shifts on the integer 1 encoded as u32. White cells represent 0 bits, grey cells represent 1 bits. This technique enables the programmer to set any desired bit to be set to 1, independently of all others.



**TIP**

Rust's numbers have methods. While convenient, this can cause issues. Unary minus has lower precedence than method calls, meaning unexpected mathematical errors can occur.

The correct way to calculate  $-1^0$  is to use parentheses to make your intent clear to the compiler like

```
(-1.0_f32).powf(0.0)
```

rather than

```
-1.0_f32.powf(0.0)
```

which is interpreted as  $-(1^0)$ .

### 5.3.3 Representing decimal numbers in a single byte with a fixed-point number format

To represent numbers within a single byte, we'll use the “Q format”, developed by Texas Instruments for embedded computing devices. The Q format, is a fixed-point number<sup>18</sup>. Unlike floating point numbers, the decimal place does not move to dynamically accommodate different ranges.

The specific version of the Q format that we will be implementing is called Q7. This indicates that there is 7 bits available for the represented number, plus 1 sign bit. We'll disguise the decimal nature of the type by hiding the 7 bits within an `i8`. That will mean that the Rust compiler will be able to assist us to keep track of the value's sign. We will also be able to derive traits such as `PartialEq` and `Eq`, which provides comparison operators for our type for free.

#### Listing 5.15. Definition of the Q7 format (ch5/ch5-q/src/lib.rs)

```
#[derive(Debug, Clone, Copy, PartialEq, Eq)]
pub struct Q7(i8);    ①
```

① This form of a struct is known a “tuple struct” as it only has anonymous fields

Q7 is intended as a storage and data transfer type only. Its most important role is to be able to be converted to and from floating point types. Here is the conversion to `f64`:

#### Listing 5.16. Converting between f64 and Q7 (ch5/ch5-q/src/lib.rs)

```
impl From<f64> for Q7 { ①
    fn from(n: f64) -> Self {
        if n >= 1.0 { ②
            Q7(127)
        } else if n <= -1.0 {
            Q7(-128)
        } else {
            Q7((n * 128.0) as i8)
        }
    }
}

impl From<Q7> for f64 { ③
    fn from(n: Q7) -> f64 {
        (n.0 as f64) * 2f64.powf(-7.0) ④
    }
}
```

① Converting from `f64` to `Q7`

---

<sup>18</sup>  $\mathbb{Q}$ —often written as  $\mathbb{Q}$ —is the mathematical symbol for the set of rational numbers. Rational numbers are numbers on the number line—real numbers—excluding numbers such as  $\pi$ , which are irrational.

- ② Out of bounds numbers are coerced to the maximum of the Q7 range. This should never happen for the use cases that we are interested in.
- ③ Converting from Q7 to f64
- ④ This is mathematically equivalent to iterating through each of the bits and multiplying it to its weight, as was carried out earlier when decoding the floating point mantissa in the previous section

As there are also f32 values to convert between, let's make use of Rust's own machinery to do the hard work on our behalf:

#### **Listing 5.17. Converting between f32 and Q7 via f64 values (ch5/ch5-q/src/lib.rs)**

```
impl From<f32> for Q7 {
    fn from(n: f32) -> Self {
        Q7::from(n as f64)
    }
}

impl From<Q7> for f32 {
    fn from(n: Q7) -> f32 {
        f64::from(n) as f32
    }
}
```

Now both floating point types are covered. But how do we know that the code that what we've written actually does what we intended? How do we test what we've written? As it happens, Rust has excellent support for unit testing via cargo.

The Q7 code that you've seen is available as a complete listing at Listing 5.19 . To test the code, enter the root directory of the crate and run `cargo test`.

#### **Listing 5.18. Output of cargo test on code from Listing 5.19**

```
Compiling ch5-q v0.1.0 (file:///path/to/ch5/ch5-q)
Finished dev [unoptimized + debuginfo] target(s) in 2.86 secs
Running target\debug\deps\ch5_q-013c963f84b21f92

running 3 tests
test tests::f32_to_q7 ... ok
test tests::out_of_bounds ... ok
test tests::q7_to_f32 ... ok

test result: ok. 3 passed; 0 failed; 0 ignored; 0 measured; 0 filtered out

Doc-tests ch5-q

running 0 tests

test result: ok. 0 passed; 0 failed; 0 ignored; 0 measured; 0 filtered out
```

**Listing 5.19. Full code implementing the Q7 format and its conversion to and from f32 and f64 types (ch5/ch5-q/src/lib.rs)**

```

#[derive(Debug,Clone,Copy,PartialEq,Eq)]
pub struct Q7(i8);

impl From<f64> for Q7 {
    fn from (n: f64) -> Self {
        if n >= 1.0 {
            Q7(127)
        } else if n <= -1.0 {
            Q7(-128)
        } else {
            Q7((n * 128.0) as i8)
        }
    }
}

impl From<Q7> for f64 {
    fn from(n: Q7) -> f64 {
        (n.0 as f64) * 2f64.powf(-7.0)
    }
}

impl From<f32> for Q7 {
    fn from (n: f32) -> Self {
        Q7::from(n as f64)
    }
}

impl From<Q7> for f32 {
    fn from(n: Q7) -> f32 {
        f64::from(n) as f32
    }
}

#[cfg(test)]
mod tests {      ①
    use super::*;

    #[test]
    fn out_of_bounds() {
        assert_eq!(Q7::from(10.), Q7::from(1.));
        assert_eq!(Q7::from(-10.), Q7::from(-1.));
    }

    #[test]
    fn f32_to_q7() {
        let n1: f32 = 0.7;
        let q1 = Q7::from(n1);

        let n2 = -0.4;
    }
}

```

```

let q2 = Q7::from(n2);

let n3 = 123.0;
let q3 = Q7::from(n3);

assert_eq!(q1, Q7(89));
assert_eq!(q2, Q7(-51));
assert_eq!(q3, Q7(127));
}

#[test]
fn q7_to_f32() {
    let q1 = Q7::from(0.7);
    let n1 = f32::from(q1);
    assert_eq!(n1, 0.6953125);

    let q2 = Q7::from(n1);
    let n2 = f32::from(q2);
    assert_eq!(n1, n2);
}
}

```

- ① Define a sub-module within this file
- ② Bring the parent module within the sub-module's local scope

## 5.4 Generating *f32* values between 0 and 1 from random bytes

Here is an interesting exercise of the knowledge that you have developed over the proceeding pages. Imagine that you have a source of random bytes and you want to convert them into floating point values between 0 and 1. Naively interpreting the incoming bytes as f32/f64 would result in massive variations in scale. As divide is a slow operation, perhaps there is something faster than simply dividing by the largest value that a byte can represent, as per Listing 5.20

### **Listing 5.20. Generating a f32 that lies between 0 and 1 from an arbitrary input byte through division**

```

fn mock_rand(n: u8) -> f32 {
    (n as f32) / 255.0    ①
}

```

- ① 255 is the maximum value that u8 can represent

Perhaps it's possible to assume a constant exponent value, then shift the incoming bits into the mantissa, such that they would form a range between 0 and 1? [shiftbyte](#) is the best result that I could achieve. With an exponent of -1 (represented as 126/0b01111110), the source byte achieves a range of 0.5 to 0.998. That can be normalized to 0.0 to 0.996 with subtraction and multiplication. Is there a way to do better?

**shiftbyte**

```
fn mock_rand(n: u8) -> f32 {
    let base: u32 = 0b0_0111110_000000000000000000000000;
    let large_n = (n as u32) << 15;           ①
    let f32_bits = base | large_n;            ②
    let m = f32::from_bits(f32_bits);        ③
    2.0 * (m - 0.5)                         ④
}
```

- ① Underscores mark the sign/mantissa/exponent boundaries
- ② Align the input byte n to 32 bits, then increase its value by shifting its bits 15 places to the left
- ③ Take a bitwise OR, merging the base with the input byte
- ④ Interpret f32\_bits (which is type u32) as an f32
- ⑤ Normalize the output range

As a complete program, `mock_rand()` from [shiftbyte](#) can be incorporated into a test program fairly easily, as shown in Listing 5.22 .

**Listing 5.21. Output from Listing 5.22,**

```
max of input range: 11111111 -> 0.99609375
mid of input range: 01110111 -> 0.46484375
min of input range: 00000000 -> 0
```

**Listing 5.22. Generating a f32 that lies between 0 and 1 from an arbitrary input byte without division (ch5/ch5-u8-to-mock-rand.rs)**

```
fn mock_rand(n: u8) -> f32 {
    let base: u32 = 0b0_0111110_000000000000000000000000;
    let large_n = (n as u32) << 15;
    let f32_bits = base | large_n;
    let m = f32::from_bits(f32_bits);
    2.0 * (m - 0.5)
}

fn main() {
    println!("max of input range: {:08b} -> {:?}", 0xff, mock_rand(0xff));
    println!("mid of input range: {:08b} -> {:?}", 0x77, mock_rand(0x77));
    println!("min of input range: {:08b} -> {:?}", 0x00, mock_rand(0x00));
}
```

## 5.5 *Implementing a CPU in Software to Establish that Functions are also Data*

One of the fairly mundane, yet utterly intriguing, details about computing is that instructions are also just bytes of `usize`. Moreover, as a general computing device, your computer can emulate other computers' *instruction sets* by emulating them in software. That means that while we cannot pull apart a CPU to see how it works, we

can construct one with code.

Working through this section will teach you about how a computer operates at a fundamental level. It will show you how functions operate and what the term “pointer” means. We won’t have an assembly language, we’ll actually be programming directly in hex. It will also introduce you to other terms you may have heard of in passing, such as “the stack”.

We’ll implement a subset of a system that was available to consumers in the 1970s called CHIP-8. CHIP-8 was supported by a number of manufacturers, but was fairly primitive even the standards of the day. (It was created to write games, rather than for commercial or scientific applications.) One device was the COSMAC VIP. It had a single-color display with a resolution of 64x32 (0.0002 megapixels), 2KB RAM, 1.76 MHz CPU and was sold for USD275. Oh, and you needed to assemble the computer yourself. It also contained games programmed by the world’s first female game developer: Joyce Weisbecker.

### 5.5.1 CPU 1: “the Adder”

We’ll build up our understanding by starting with a minimal core. Let’s start by building an emulator that only supports a single instruction: addition.

To understand what’s happening within Listing 5.25 , there are three main things to learn:

- becoming familiar with new terminology
- How to interpret opcode
- Understanding the main loop

### GLOSSARY OF TERMS RELATED TO CPU EMULATION

Dealing with CPUs and emulation involves learning some terms that:

- an *operation* (often shortened to op) refers to procedures that are supported by the system natively. You may also encounter equivalent phrases such as “implemented in hardware”, “intrinsic operation” as you explore further.
- the *registers* are containers for data that CPU accesses directly. For most operations, operands must be moved to registers for the operation to function. For the CHIP-8, each register is a u8.
- an *opcode* is a number that maps to an operation. On the CHIP-8 platform, opcodes include both the operation and the operands’ registers.

Here is the CPU’s definition extracted from Listing 5.25:

#### **Listing 5.23. CPU Structure for CPU**

```
struct CPU {
    current_operation: u16,
    registers: [u8; 2],
}
```

When this “CPU” performs addition, the following steps need to be taken:

- Initialize a CPU object as `cpu`
- Load the operands into `cpu.registers`
- Load the addition opcode into `cpu.current_operation`

Once the data is in place, `cpu` will be able to execute the opcode. In a sense, CPU operations require both pre- and post-processing to actually work. Before an operation takes place, the registers must be loaded from memory correctly. Once an operation takes place, registers are downloaded into memory. At this stage, there is no memory. We will be directly injecting values into `cpu` from the host system.

## HOW TO INTERPRET CHIP-8 OPCODES

CHIP-8 opcodes are `u16` values that need to be decoded into one of three forms:

- The standard case divides the opcode into 4 parts: Operation group (`u8`), operation identifier within the group (`u8`), left register (`u8`) and right register (`u8`)
- To perform an operation with a constant, the opcode is divided into three parts: Operation identifier (`u8`), left operand (`u8`) and the constant (`u8`)
- An alternative case divides the opcode into 2 parts: Major operation group (`u8`), memory address (`u16`)

The standard case turns out to be a fairly intuitive division, as each part corresponds to a hexadecimal number.

**Table 5.2. How to read standard CHIP-8 opcodes**

As <code>u16</code>	As a ( <code>u8, u8, u8, u8</code> ) tuple
<code>0x71E4</code>	( <code>0x7, 0x1, 0xE, 0x4</code> )
<code>0x0222</code>	( <code>0x0, 0x1, 0x2, 0x3</code> )

Each part of the opcode has a role:

- The first (`0x7` and `0x0` in our examples) indicates which group of instructions the opcode refers to. Logical and arithmetic operations are in the group `0x8`, whereas control flow instructions are in the group `0x1`.
- The second and third parts are the register index of the two operands. There are no operations that are allowed to have more than two operands.
- The last part (`0x4` and `0x3`` in our examples) indicate which operation within the major group to perform. Each major group can support up to 16 operations within it. AS it happens, with just over 30 operations in total, none of the CHIP-8 major operation groupings uses all 16..

Here is the table of bit shifting operations needed to isolate each part.

**Table 5.3 Code to isolate each part of a CHIP-8 opcode 0x71E4 assigned to the variable op**

opcode	Rust Code	Decoded Field	Description
0x71E4	(op & 0xF000) >> 12	0x7	Filter the 4 desired bits with an AND mask, then shift them to the right-most position. The filtering step is not strictly necessary, but does help to indicate one's intentions.
0x71E4	(op & 0x0F00) >> 8	0x1	As above, but this time the filter is important. Without the mask, the first four bits would remain.
0x71E4	(op & 0x00F0) >> 4	0xE	As above, but with fewer positions to move.
0x71E4	op & 0x000F	0x4	Retain only the least 4 significant bits

The code within Listing 5.25 has a single opcode: 0x8010. Its decoded values are:

- major group 0x8, which happens to stand for arithmetic and logical instructions
- left operand 0x0, also known as register x, which represents `cpu.registers[0]`
- right operand 0x1, also known as register y, which represents `cpu.registers[1]`
- operation indicator 0x4, which is defined as “add register y to register x”

The alternative forms are somewhat simpler to decode, as they have fewer parts:

**Table 5.4. How to read CHIP-8 opcodes that refer to memory addresses**

As u16	As (u8, u16)
0x1BBC	(0x1, 0xBBBC)

This form of opcode will be described in more detail when we expand the capabilities of the emulator. One restriction of this format is that memory addresses must fit within 12 bits. That restricts the CHIP-8 platform’s total memory to 4096 bytes (0x000...0xFFFF).

## UNDERSTANDING THE EMULATOR’S MAIN LOOP

In Listing 5.25, `cpu.run()` performs the bulk of the program. It uses the following pattern:

- read instruction
- decode instruction
- match decoded instruction to known opcodes
- dispatch execution of the operation to a specific function

```
const ARITHMETIC_AND_LOGIC: u8 = 0x8;      ①
const ADD_XY: u8 = 0x4;                    ①

// ...

impl CPU {
    fn run(&mut self) {
```

```

let raw_op = self.current_operation;          ②
let op_major = ((raw_op & 0xF000) >> 12) as u8; ③
let x = ((raw_op & 0x0F00) >> 8) as u8;      ③
let y = ((raw_op & 0x00F0) >> 4) as u8;      ③
let op_minor = (raw_op & 0x000F) as u8;        ③

match (op_major, op_minor) {                ④
    (ARITHMETIC_AND_LOGIC, ADD_XY) => self.add_xy(x, y), ⑤
    _ => unimplemented!(),
}
}
//...
}

```

- ① Defined by the CHIP-8 documentation
- ② Assign the opcode to a local variable for convenience
- ③ Decode instruction into parts. While CHIP-8 has multiple decoding methods, we'll only implement one as we know that is what our instruction will be.
- ④ Match the decoded opcode parts against the known constants
- ⑤ Dispatch the operation to a method

### 5.5.2 First working emulator

Listing 5.25 is the full code of our proto-emulator: “the Adder”.

**Listing 5.24. Output of Listing 5.25**

```
5 + 10 = 15
```

**Listing 5.25. Implementing the beginnings of CHIP-8 emulator (ch5/ch5-cpu1/src/main.rs)**

```

const ADD_XY: u8 = 0x8;      ①

struct CPU {
    current_operation: u16,
    registers: [u8; 2],
}

impl CPU {
    fn run(&mut self) {
        let encoded_op = self.current_operation;
        let op = ((encoded_op & 0xF000) >> 12) as u8; ②
        let x = ((encoded_op & 0x0F00) >> 8) as u8; ②
        let y = ((encoded_op & 0x00F0) >> 4) as u8; ②

        match op {
            ADD_XY => {
                self.add_xy(x,y);
            },
            _ => unimplemented!(),
        }
    }
}

```

```

    }

    fn add_xy(&mut self, x: u8, y: u8) {
        self.registers[x as usize] += self.registers[y as usize];
    }
}

fn main() {
    let mut cpu = CPU {
        current_operation: 0x8014,
        registers: [0; 2],
    };

    cpu.registers[0] = 5;
    cpu.registers[1] = 10;
    cpu.run();

    assert_eq!(cpu.registers[0], 15);

    println!("5 + 10 = {}", cpu.registers[0]);
}

```

- ① Constant defined by the CHIP-8 documentation  
 ② Assign each bitfield to its own variable

### 5.5.3 CPU 2: “the Multi-Adder”

CPU 1 could execute a single instruction. CPU 2 is able to execute several instructions in sequence with the addition of a working main loop and a variable that we’ll call `position_in_memory`. `position_in_memory` holds the memory address of the CPU’s next instruction.

Listing 5.27 makes the following substantive changes to `cpul`:

- Inclusion of a fully-fledged main loop and stopping condition (Lines 14-31). At each step in the loop, memory at `position_in_memory` is accessed, decoded into an opcode, `position_in_memory` is then incremented to the next memory address and the opcode is executed. The CPU will continue to run forever until the stopping condition—an opcode of 0x0000—is encountered.
- Addition of 4kb of memory (Line 8).
- Removal of the `current_instruction` field of the CPU struct, which is replaced by a section of the main loop that decodes bytes from memory (Lines 15-17).
- Opcodes are written into memory (Lines 51-53).

#### **Listing 5.26. Output of Listing 5.27**

```
5 + 10 + 10 + 10 = 35
```

**Listing 5.27. Adding the ability for the emulator to process multiple instructions (ch5/ch5-cpu2/src/main.rs)**

```

const ARITHMETIC_AND_LOGIC: u8 = 0x8;
const HALT: u8 = 0x0;          ①
const ADD_XY: u8 = 0x4;

struct CPU {
    // current_operation: u16,      ②
    registers: [u8; 16],          ③
    position_in_memory: usize,    ④
    memory: [u8; 4096],           ⑤
}

impl CPU {
    fn run(&mut self) {
        loop {
            let op_byte1 = self.memory[self.position_in_memory] as u16;      ⑥
            let op_byte2 = self.memory[self.position_in_memory + 1] as u16;      ⑥
            let raw_op = op_byte1 << 8 | op_byte2;                            ⑦

            let op_major = ((raw_op & 0xF000) >> 12) as u8;
            let x = ((raw_op & 0x0F00) >> 8) as u8;
            let y = ((raw_op & 0x00F0) >> 4) as u8;
            let op_minor = (raw_op & 0x000F) as u8;

            self.position_in_memory += 2;                                      ⑧

            match (op_major, op_minor) {
                (HALT, HALT) => { return; },                                ⑨
                (ARITHMETIC_AND_LOGIC, ADD_XY) => self.add_xy(x, y),
                _ => unimplemented!("opcode {:04x}", raw_op),             ⑩
            }
        }
    }

    fn add_xy(&mut self, x: u8, y: u8) {
        self.registers[x as usize] += self.registers[y as usize];
    }
}

fn main() {
    let mut cpu = CPU {
        registers: [0; 16],
        memory: [0; 4096],
        position_in_memory: 0,
    };

    cpu.registers[0] = 5;
    cpu.registers[1] = 10;
    cpu.registers[2] = 10;      ⑪
    cpu.registers[3] = 10;      ⑪
}

```

```

cpu.memory[0] = 0x80; cpu.memory[1] = 0x14;      (12)
cpu.memory[2] = 0x80; cpu.memory[3] = 0x24;      (13)
cpu.memory[4] = 0x80; cpu.memory[5] = 0x34;      (14)

cpu.run();

assert_eq!(cpu.registers[0], 35);

println!("5 + 10 + 10 + 10 = {}", cpu.registers[0]);
}

```

- (1) Add a pattern to short circuit the program's execution. This is not part of the CHIP-8 specification but is useful for debugging.
- (2) No longer needed
- (3) Increase number of registers to 16 (0..F), as per the CHIP-8 specification
- (4) Add a variable that keeps track of where we currently are in the program. This is formally known as a *program counter*. Its type is `usize`, which simplifies the process of indexing the memory array.
- (5) Provide the system with 4kb memory
- (6) Access individual `u8` bytes, but interpret them as `u16` so that they can be joined together as a single opcode.
- (7) Shift `op_byte1` left to occupy the left-most bits of the `u16`
- (8) Increment `position_in_memory` to point to the next instruction.
- (9) Short circuit the function to terminate execution when the opcode `0x000` is encountered
- (10) This macro is useful when you are debugging, as it will promptly indicate that you have made a typo with any of the opcodes.
- (11) Initialise a few registers with values
- (12) Load the opcode `0x8014` to memory. `0x8014` means “add the value in register 1 to register 0”
- (13) Load the opcode `0x8024` to memory. `0x8024` means “add the value in register 2 to register 0”
- (14) Load the opcode `0x8034` to memory. `0x8014` means “add the value in register 3 to register 0”

#### 5.5.4 CPU 3: Adding functions

We have nearly built all of the emulator machinery. This section of the chapter demonstrates one of the assertions made at the start: functions are also data.

To build functions, we require some additional opcodes to be implemented:

- the CALL (0x2NNN where NNN is a memory address) opcode  
modifies `cpu.position_in_memory` to point to the address of the function
- RETURN modifies `cpu.position_in_memory` to the memory address of the previous CALL

To enable these two opcodes to work together, the CPU needs to have some specialised memory available for storing addresses. This is known as “the stack”. Each CALL adds an address to the stack, by incrementing the stack pointer and writing NNN to that position in the stack. Each RETURN removes the top address, by decrementing the stack pointer.

**Listing 5.28. Detail of the emulated CPU in Listing 5.30 to include a stack and stack pointer**

```
struct CPU {
    registers: [u8; 16],
    position_in_memory: usize,
    memory: [u8; 4096],
    stack: [u16; 16],           ①
    stack_pointer: usize,      ②
}
```

- ① The stack's maximum "height" is 16. After 16 nested function calls, the program will encounter a *stack overflow*.
- ② Giving the `stack_pointer` type `usize` makes it easier to be used to index values within stack

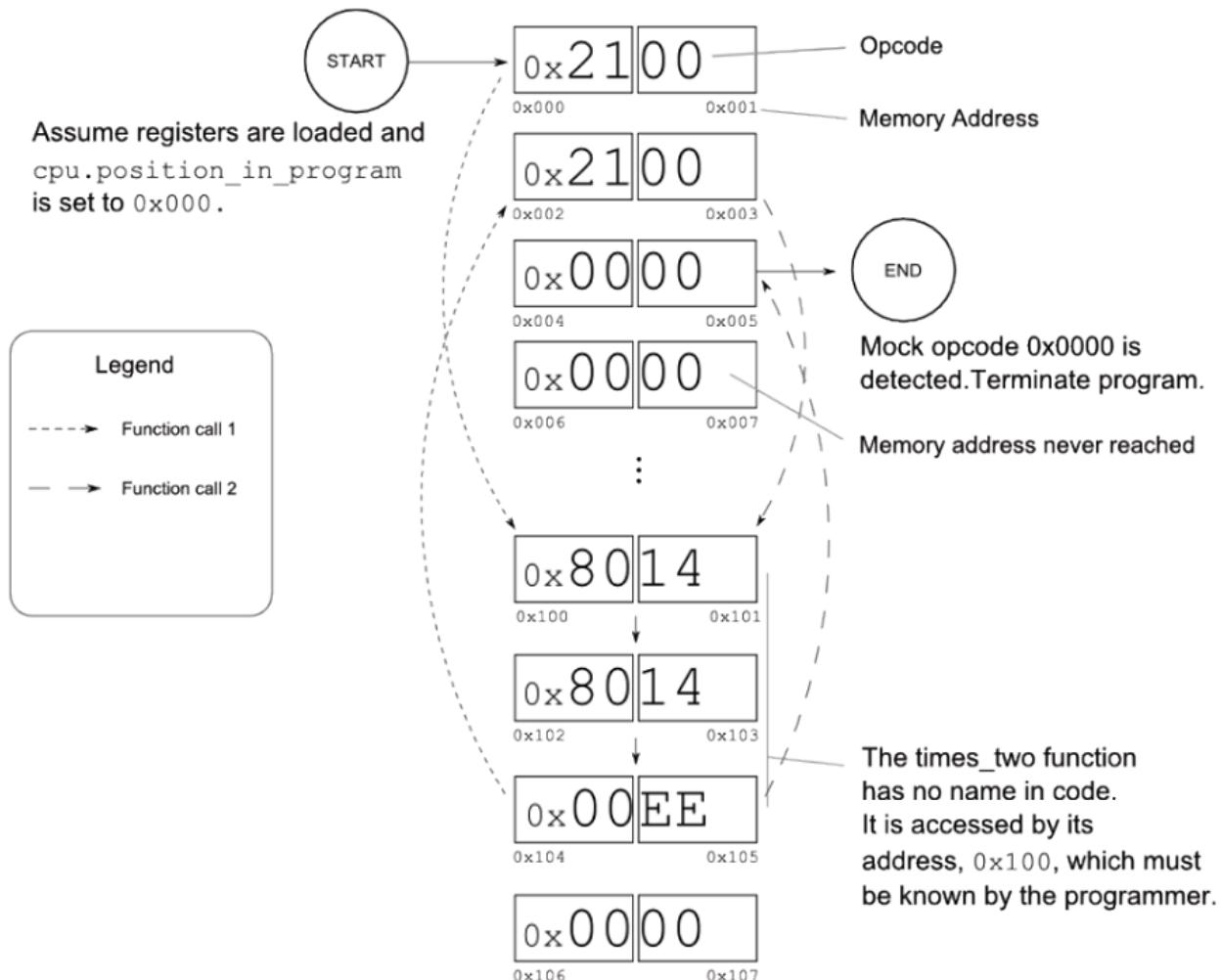
The function implemented within `main()` of Listing 5.30 acts like the Rust pseudo-code at [pseudo](#). Unfortunately, the function has neither a name, arguments, nor variables. Everything appears in hexadecimal numbers. To call a function written in CHIP-8, one must know its memory address (NNN) beforehand.

**pseudo**

```
fn times_two(register_1: u8, register_2: u8) {
    register_1 += register_2;
    register_1 += register_2;
}
```

An illustration of what is happening when `cpu.main()` is called at line 83 of Listing 5.30 is provided at Figure 5.3. The arrows reflect the state of the `cpu.position_in_memory` variable as it makes its way through the program.

**Figure 5.3. Illustrating the control flow of the function implemented within the emulated CPU from Listing 5.30**



#### **Listing 5.29. Output of Listing 5.30**

```
5 + (10 * 2) + (10 * 2) = 45
```

#### **Listing 5.30. Emulating a CPU that incorporates calling and returning from a user-defined function (ch5/ch5-cpu3/src/main.rs)**

```
struct CPU {
    registers: [u8; 16],
    position_in_memory: usize,
    memory: [u8; 4096],
```

```

        stack: [u16; 16],
        stack_pointer: usize,
    }

impl CPU {
    fn run(&mut self) {
        loop {
            let op_byte1 = self.memory[self.position_in_memory] as u16;
            let op_byte2 = self.memory[self.position_in_memory + 1] as u16;
            let opcode = op_byte1 << 8 | op_byte2;

            let x = ((opcode & 0x0F00) >> 8) as u8;
            let y = ((opcode & 0x00F0) >> 4) as u8;
            let op_minor = (opcode & 0x000F) as u8;
            let addr = opcode & 0xFFFF;

            self.position_in_memory += 2;

            match opcode {                                     ①
                0x0000 => { return; },
                0x00EE => { self.ret(); },
                0x2000...0x2FFF => { self.call(addr); },
                0x8000...0x8FFF => {
                    match op_minor {
                        4 => { self.add_xy(x, y); }
                        _ => { unimplemented!("opcode: {:04x}", opcode); }
                    }
                },
                _ => unimplemented!("opcode {:04x}", opcode),
            }
        }
    }

    fn call(&mut self, addr: u16) {
        let sp = self.stack_pointer;
        let stack = &mut self.stack;

        if sp > stack.len() {
            panic!("Stack overflow!")
        }

        stack[sp] = self.position_in_memory as u16;      ②
        self.stack_pointer += 1;                          ③
        self.position_in_memory = addr as usize;         ④
    }

    fn ret(&mut self) {
        if self.stack_pointer == 0 {
            panic!("Stack underflow");
        }

        self.stack_pointer -= 1;
        self.position_in_memory = self.stack[self.stack_pointer] as usize;  ⑤
    }
}

```

```

fn add_xy(&mut self, x: u8, y: u8) {
    self.registers[x as usize] += self.registers[y as usize];
}

fn main() {
    let mut cpu = CPU {
        registers: [0; 16],
        memory: [0; 4096],
        position_in_memory: 0,
        stack: [0; 16],
        stack_pointer: 0,
    };

    cpu.registers[0] = 5;
    cpu.registers[1] = 10;

    cpu.memory[0x000] = 0x21; cpu.memory[0x001] = 0x00;      ⑥
    cpu.memory[0x002] = 0x21; cpu.memory[0x003] = 0x00;      ⑦
    cpu.memory[0x100] = 0x80; cpu.memory[0x101] = 0x14;      ⑧
    cpu.memory[0x102] = 0x80; cpu.memory[0x103] = 0x14;      ⑨
    cpu.memory[0x104] = 0x00; cpu.memory[0x105] = 0xEE;      ⑩
    cpu.run();

    assert_eq!(cpu.registers[0], 45);
    println!("5 + (10 * 2) + (10 * 2) = {}", cpu.registers[0]);
}

```

- ① Use range matching against the opcode, rather than matching against tuples. It's now impossible to know whether to match against op\_minor, addr or another pattern before carrying out the match
- ② Add the "current" self.position\_in\_memory to the stack. As position\_in\_memory has been incremented by 2 on line 21, the "current" position is actually the next instruction after this call. This means that when the function returns, it will not be stuck in an infinite loop.
- ③ Increment self.stack\_pointer, preserving the self.position\_in\_memory until it needs to be accessed again in a subsequent return
- ④ Modifying self.position\_in\_memory has the effect of jumping to that address.
- ⑤ Jump to the position in memory where the call was made.
- ⑥ Opcode 0x2100: CALL the function at 0x100
- ⑦ Opcode 0x2100: CALL the function at 0x100
- ⑧ Opcode 0x0000: HALT execution
- ⑨ Opcode 0x8014: Add register 1's value to register 0
- ⑩ Opcode 0x8014: Add register 1's value to register 0
- ⑪ Opcode 00EE: RETURN

As you delve into systems documentation, you will find that real-life functions are more complicated than simply jumping to a pre-defined memory location. Operating systems and CPU architectures differ in calling conventions and their capabilities.

Sometimes operands will need to be added to the stack, sometimes inserted into defined registers. Still, while the specific mechanics may differ, the process will be roughly similar to what you have just encountered.

### 5.5.5 CPU 4: Adding the rest

With a few extra opcodes, it's possible to implement multiplication and many more functions within your inchoate CPU. Check the source code that comes along with the book (specifically the directory ch5/ch5-cpu4) for a mostly-complete fuller implementation of the CHIP-8 specification.

The last step in learning about CPUs and data is to understand how control flow works. Within CHIP-8, control flow works by comparing values in registers, then modifying `position_in_memory` depending on the outcome. There are no while loops or for loops within a CPU. Creating them in programming languages is the art of the compiler writer.

## 5.6 Summary

This has been a large, in-depth chapter. You have learned:

- How to treat a typed value as untyped bytes, then extract individual bits to produce new typed data
- How a CPU interprets instructions from memory, which are encoded as integers
- How a platform's endianness can invert the interpretation of the value that is being represented
- That the same bit pattern means different things, depending on its type
- How to navigate between base-2, base-10 and base-16 representations of integers
- How to write and run unit tests in your programs
- How to use left shift and right shift operations to single out individual bits



# 6

## Memory

### **This chapter covers:**

- What a pointer is and why some of them are “smart”
- What the terms “the stack” and “the heap” mean
- How a program views its memory and why that’s a lie

The chapter provides you with some of the tacit knowledge held by systems programmers about how the computer’s memory operates. It aims to be the most accessible guide to pointers and memory management available. You will be learning about how applications interact with an operating system. Programmers who understand these dynamics can use that knowledge to maximize their programs’ performance, while minimizing their memory footprint.

Memory is a shared resource and the operating system is an arbiter. To make its life easier, it lies to your program about how much memory is available and where it’s located. Revealing the truth behind those lies requires us to work through some prior knowledge. That is the work of the first two sections of the chapter. Each of the three sections builds on the previous one.

None of them assume that you’ve encountered the topic before. There is a fairly large body of theory to cover, but all of it is explained by example. Among other examples, you create your first graphical application in the book.

The chapter introduces little new Rust syntax, as the material is quite dense. You’ll learn how to construct pointers, how to interact with an operating system via its native API and how to interact with other programs through Rust’s foreign function interface.

## 6.1 Pointers

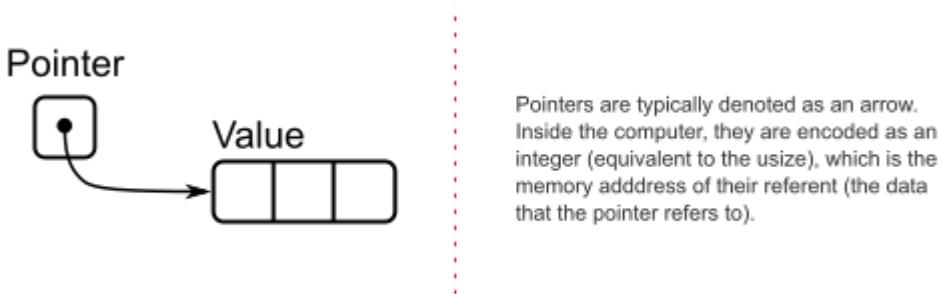
Pointers are how computers refer to data that isn't immediately accessible. The topic tends to have an aura of mystique to it. That's not necessary. If you've ever read a book's table of contents, then you've used a pointer. Pointers are just numbers that refer to somewhere else.

If you've never encountered systems programming before, there is lots of terminology to grapple with that is describing unfamiliar concepts. Thankfully though, what's sitting underneath the abstraction is not too difficult to understand. If you've used a table of contents, then you've used a pointer.

The first thing to understand is the notation. Figure 6.1 introduces 3 concepts:

- The arrow refers to some unknown location in memory
- Each box represents a block of memory. In this figure, each block refers to a `usize` width. Other figures use a byte, or perhaps even a bit, as the chunk of memory they're referring to.
- The rounded box underneath "Value" represents three blocks of memory that are next to each other

**Figure 6.1. Notation for illustrating a pointer. In Rust code, this is most frequently encountered as `&T` and `&mut T`, where `T` is the type of the value.**



Authors use the notation in Figure 6.1 to indicate that the two we don't know what the address held in the "Pointer" box will be, but they do want to demonstrate that "Pointer" and "Value" are connected.

For newcomers, pointers are scary and awe-inspiring. Their proper use requires you to know how exactly how your program is laid out in memory. Imagine reading a table of contents that says chapter 4 starts on page 97, but it actually starts on page 107. That will be frustrating, but at least you can cope with the mistake. A computer doesn't experience frustration. But it also lacks any intuition that it has been pointed to the wrong place. It will just keep working, correctly or incorrectly, as if it had been given the correct location. The fear of pointers is that you will introduce some impossible to debug error.

We can think of data stored within the program's memory as scattered around within physical RAM somewhere. To make use of that RAM, there needs to be some sort of retrieval system in place. An *address space* is that retrieval system. Pointers are encoded as memory *addresses*, which are represented as integers of type `usize`. An address points to somewhere within the address space. For the moment, think of the address space as all of your RAM laid out in a single line end to end.

Why are memory addresses encoded as `usize`? Surely there's no 64-bit computer with  $2^{64}$  bytes of RAM. The range of the address space is a façade provided by the operating system and the CPU. Programs only know an orderly series of bytes, irrespective of the amount of RAM is actually available in the system. We discuss how this works later in virtual memory section of this chapter.

**IMPORTANT**

Rust uses the same underlying representation in memory for multiple semantics. For example, `&T` and `&mut T` both look the same once your source code has been compiled. To reiterate, Rust's ownership rules and safety checks are invisible in the compiled binary file. This is a consequence of the *zero-cost abstractions* philosophy.

## 6.2 Exploring Rust's reference and pointer types

This section teaches you how to work with several of Rust's pointer types. *Rust in Action* tries to stick to the following guidelines:

- *reference* is used to signal that the Rust compiler will provide its safety guarantees
- *pointer* is used when referring to something more primitive, with an implication that we'll be responsible for maintaining safety. There is a connotation of being unsafe.
- *raw pointer* is used for types where it's important to make their unsafe nature explicit

**NOTE**

Dear MEAP reader, if you encounter any terminology that's difficult to understand, please add annotation in the liveBook version *Rust in Action* at [livebook.manning.com/#!/book/rust-in-action/](https://livebook.manning.com/#!/book/rust-in-action/).

Throughout this section, we'll be expanding on a common code fragment introduced by Listing 6.1 . A pictorial view of what's happening follows the code at Figure 6.2 .

**Listing 6.1. Mimicing pointers with references. Two global variables, B and C are pointed to by references. Those references hold addresses of B and C respectively.**

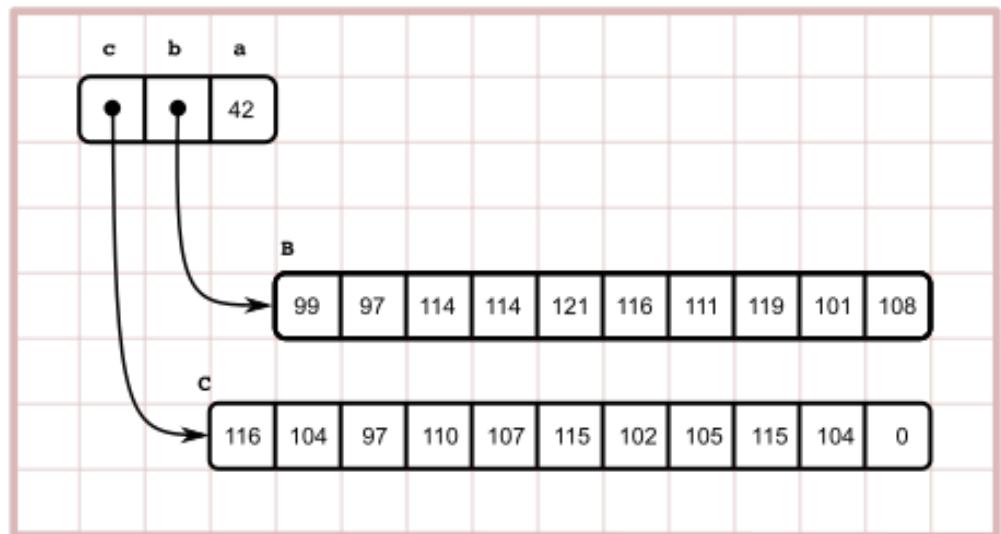
```
static B: [u8; 10] = [99, 97, 114, 114, 121, 116, 111, 119, 101, 108];
static C: [u8; 11] = [116, 104, 97, 110, 107, 115, 102, 105, 115, 104, 0];

fn main() {
    let a = 42;
    let b = &B;      ①
    let c = &C;      ①
}
```

```
    println!("a: {}, b: {:p}, c: {:p}");
}
```

- ① We use the same type of reference for this example for simplicity. Later examples distinguish *smart pointers* from *raw pointers* and require different types.
- ② The `{:p}` syntax asks Rust to format the variable as a pointer. That is, print out the memory address that the value is pointing to.

**Figure 6.2. An abstract view of how two pointers operate alongside a standard integer. The important lesson is that the programmer may not know the location of the referent data beforehand.**



Listing 6.1 has three variables within its `main()` function. `a` is rather trivial, it's just an integer. The two others are more interesting. `b` and `c` are references. They refer to two opaque arrays of data, `B` and `C`. For the moment, consider Rust references as equivalent to pointers.

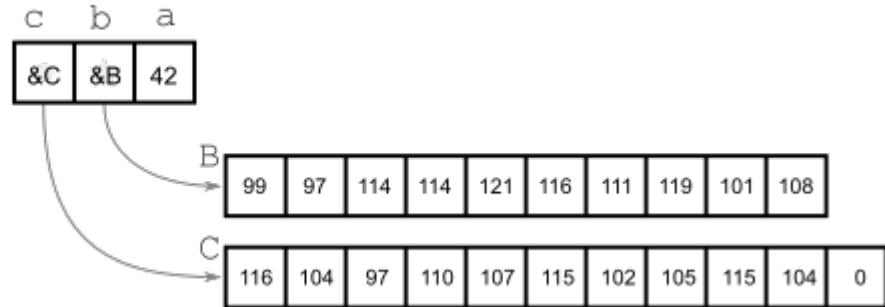
#### Listing 6.2. Output of Listing 6.1

```
a: 42, b: 0x556fd40eb480, c: 0x556fd40eb48a
```

- ① The exact memory addresses are likely to be different on your machine if you run the code

For slightly obscure technical reasons, variables are often loaded right-to-left within a computer.

This will be explained within the "Stack vs Heap" section of the chapter.



One problem with portraying pointers as arrows to disconnected arrays is that they de-emphasize that the address space is contiguous and shared between all variables.

Figure 6.3 provides a view of the same example into an imaginary address space of 49 bytes that has a pointer width of two bytes (16 bits). You'll notice that the variables b and c look different in memory, despite being the same type in Listing 6.1 . That's due to Listing 6.1 lying to you. The gritty details—and a code example that's closer to this diagram—are coming shortly.

**Figure 6.3. An illustrative address space of the program provided in Listing 6.1. It provides an illustration of the relationship between addresses (typically written in hexadecimal) and integers (typically written in decimal). White cells represent unused memory.**

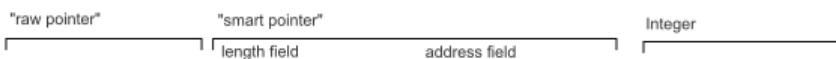
Variable

c

b

a

Abstract data type



Concrete representation



Memory layout

0x2A	0x2B	0x2C	0x2D	0x2E	0x2F	0x30	0x31
0	16	0	10	0	32	0	42
0x22	0x23	0x24	0x25	0x26	0x27	0x28	0x29
114	114	121	116	111	119	101	108
0x1A	0x1B	0x1C	0x1D	0x1E	0x1F	0x20	0x21
0						99	97
0x12	0x13	0x14	0x15	0x16	0x17	0x18	0x19
97	110	107	115	102	105	115	104
0xA	0xB	0xC	0xD	0xE	0xF	0x10	0x11
						116	104
0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8
0x0							

The NULL byte - a program's dead zone.  
If a pointer points to here and is then dereferenced, then the program will typically crash.

C

A "zero terminated buffer", which is the internal representation of strings in the C language.

Knowing how to convert these to Rust types is very useful for working with external code via its foreign function interface.

Together, c and C are a `CStr` in Rust's type system.

B

A "fixed width buffer" of length 10 that contains bytes without a terminator.

When used behind a pointer type, a buffer is often called the `Backing array`.

Together, b and B can almost create the `String` type in Rust, which also contains a capacity parameter.

For a more thorough examination of what is happening under the hood, Listing 6.4 produces much more output. It uses more sophisticated types instead of references to correlate more accurately with what is presented in Figure 6.3

**Listing 6.3. Output from Listing 6.4**

```

a:
location: 0x7ffe8f7ddfd0
size:     8 bytes
value:    42

b:
location: 0x7ffe8f7ddfd8
size:     8 bytes
points to: 0x55876090c830

c:
location: 0x7ffe8f7ddfe0
size:     16 bytes
points to: 0x558762130a40

B:
location: 0x55876090c830
size:     10 bytes
value:    [99, 97, 114, 114, 121, 116, 111, 119, 101, 108]

C:
location: 0x55876090c83a
size:     11 bytes
value:    [116, 104, 97, 110, 107, 115, 102, 105, 115, 104, 0]

```

**Listing 6.4. Using references and Box<T> to demonstrate the**

```

use std::mem::size_of;

static B: [u8; 10] = [99, 97, 114, 114, 121, 116, 111, 119, 101, 108];
static C: [u8; 11] = [116, 104, 97, 110, 107, 115, 102, 105, 115, 104, 0];

fn main() {
    let a: usize      = 42;
    let b: &[u8; 10] = &B;
    let c: Box<[u8]> = Box::new(C);

    println!("a:");
    println!(" location: {:p}", &a);
    println!(" size:   {:?} bytes", size_of::<usize>());
    println!(" value:   {:?}", a);
    println!();

    println!("b:");
    println!(" location: {:p}", &b);
    println!(" size:   {:?} bytes", size_of::<&[u8; 10]>());
    println!(" points to: {:p}", b);
    println!();

    println!("c:");
}

```

```

    println!(" location: {:p}", &c);
    println!(" size:     {:?} bytes", size_of::<Box<[u8]>>());
    println!(" points to: {:p}", c);
    println!();

    println!("B:");
    println!(" location: {:p}", &B);
    println!(" size:     {:?} bytes", size_of::<[u8; 10]>());
    println!(" value:    {:?}", B);
    println!();

    println!("C:");
    println!(" location: {:p}", &C);
    println!(" size:     {:?} bytes", size_of::<[u8; 11]>());
    println!(" value:    {:?}", C);
}

```

For readers who are interested in decoding the text within `B` and `C`, Listing 6.5 is a short program that matches Figure 6.3 more closely. It contains a number of new Rust features and some relatively archaic syntax that haven't been introduced yet. They'll be explained shortly.

**Listing 6.5. Using Rust's tools to print from strings provided by external sources. Almost creates a memory address layout that resembles Figure 6.3**

```

use std::borrow::Cow;          ①
use std::ffi::CStr;           ②
use std::os::raw::c_char;      ③

static B: [u8; 10] = [99, 97, 114, 114, 121, 116, 111, 119, 101, 108];
static C: [u8; 11] = [116, 104, 97, 110, 107, 115, 102, 105, 115, 104, 0];

fn main() {
    let a = 42;                ④
    let b: String;             ⑤
    let c: Cow<str>;          ⑥

    unsafe {
        let b_ptr = &B as *const u8 as *mut u8;          ⑦
        b = String::from_raw_parts(b_ptr, 10, 10);       ⑧

        let c_ptr = &C as *const u8 as *const c_char;    ⑨
        c = CStr::from_ptr(c_ptr).to_string_lossy();     ⑩
    }

    println!("a: {}, b: {}, c: {}", a, b, c);
}

```

① `Cow` stands for "copy on write". It is a smart pointer type that is able to read from its pointer location without needing to copy it first. This is handy when a buffer is provided to you from an external source. Avoiding copies increases runtime performance.

- ② `CStr` is a C-like string type from the foreign function interface module of the Rust standard library (`std::ffi`). It allows Rust to read in 0-terminated strings.
- ③ This is not strictly needed, but does make the code's intent clear. `c_char` is almost certainly a type alias for Rust's `i8` type, with the possibility of a platform-specific nuances. C does not define the width of its `char` type in its standard, although it's one byte wide in practice. Retrieving the type alias from the `std::os::raw` module allows for differences.
- ④ Each of the variables are introduced here, so that they're accessible from `println!` later. If we created `b` and `c` within the `unsafe` block, they would be out of scope later on.
- ⑤ `String`, as it happens, is a smart pointer type. It holds a pointer to a backing array and a field to store the size.
- ⑥ `Cow` accepts a type parameter for the data it points to. `str` is the type returned by `CStr.to_string_lossy()` and so is appropriate here.
- ⑦ References cannot be cast directly to `*mut T`, which is the type required by `String::from_raw_parts()`. Thankfully `*const T` can be cast to `*mut T`, leading to the this double cast syntax.
- ⑧ `String::from_raw_parts()` accepts a pointer (`*mut T`) to an array of bytes, a size and a capacity parameter.
- ⑨ Here we convert a `*const u8` to a `*const i8`, aliased to `c_char`. The conversion to `i8` works sucessfully because we remain under 128, following the ASCII standard.
- ⑩ Conceptually, `CStr::from_ptr()` takes responsibility for reading the pointer until it reaches a 0 and then generates a `Cow<str>` from that result.

To understand the code in Listing 6.5 , there is quite a bit of ground to cover. We first need to work through what a “raw pointer” is, then discuss a number of feature-rich alternatives that have been built around them.

### 6.2.1 Raw pointers in Rust

A “raw” pointer is a pointer is there a.

If you'll forgive the syntax, the Rust types for raw pointers are denoted as `*const T` and `*mut T` for immutable and mutable variants respectively. That is, even though each is a single type, they contains three tokens:

- A raw pointer to a `String` looks like `*const String`.
- A raw pointer to an `i32` is written as `*mut i32`.

Before we put pointers into practice, here are two other things that are useful to know:

- The difference between a `*mut T` and a `*const T` is minimal. They can be freely cast between one another and tend to be used interchangeably. They act as in-source documentation.
- Rust references (`&mut T` and `&T`) compile down to raw pointers. That means that it's possible to access the performance of raw pointers without needing to venture into `unsafe` blocks.

Here is a small example that creates a raw pointer from an `i64` value. It then prints the value and its address in memory via the `{:p}` syntax.

**Listing 6.6. Creating a raw pointer by casting a reference to a value as \*const T**

```
fn main() {
    let a: i64 = 42;
    let a_ptr = &a as *const i64;           ①

    println!("a: {} ({:p})", a, a_ptr);    ②
}
```

- ① Cast a reference to a (`&a`) to a constant raw pointer to an `i64` (`*const i64`)  
 ② Print the value of the variable `a` (42) and its address in memory (`0x7ff...`)

The terms pointer and address are sometimes used interchangeably. There is one important difference. A pointer knows its referent's width in bytes. An `i64` is 8 bytes wide (64 bits ÷ 8 bits per byte). Therefore, if an `i64` is stored at address `0x7ffd`, then each of the bytes between `0x7ffd..0x8004` must be fetched from RAM to recreate the integer's value.

**Listing 6.7. Identifying a value's address by casting a reference to it as a raw pointer via std::mem::transmute**

```
fn main() {
    let a: i64 = 42;
    let a_ptr = &a as *const i64;
    let a_addr: usize = unsafe { std::mem::transmute(a_ptr) };    ①

    println!("a: {} ({:p}...0x{:x})", a, a_ptr, a_addr + 7);
}
```

- ① `transmute()` interprets the bytes at the location as another type. Using `transmute()` here is considered unidiomatic Rust, but allows us to postpone introducing more syntax.

Under the hood, references (`&T` and `&mut T`) are implemented as raw pointers. But they come with extra guarantees and should always be preferred. Accessing the value of a raw pointer is always `unsafe`.

Using raw pointers in Rust code is like working with pyrotechnics. Usually the results are fantastic, sometimes they're painful and very occasionally they're tragic. Raw pointers should be considered an intermediary step between receiving something from the operating system or another programming language and into a reference.

To demonstrate their volatility, let's work through a quick example with Rust's raw pointers. Creating a pointer of arbitrary types with from any integer is perfectly legal. Dereferencing that pointer must occur within an `unsafe` block, implying that the programmer takes full responsibility for any consequences.

```
fn main() {
    let ptr = 42 as *const Vec<String>;    ①
```

```

unsafe {
    let new_addr = ptr.offset(4);
    println!("{:p} -> {:p}", ptr, new_addr);
}

```

- ① Pointers can be created from any integral value safely. An `i32` is not a `Vec<String>`, but Rust is quite comfortable to ignore that here.

To reiterate - raw pointers are not safe. They have a number of properties that mean that their use is strongly discouraged within day-to-day Rust code.

- They do not own their values. The Rust compiler does not check that the referent data is still valid when they're accessed
- Multiple raw pointers to the same data is allowed. Every raw pointer can have write read/write access to that data. This means that there is no time when Rust can guarantee that the shared data is valid.

Notwithstanding those warnings, there are a small number of valid reasons to make use of raw pointers.

- It's unavoidable. Perhaps some operating system call or 3rd party code requires a raw pointer. Raw pointers are very common with C code that provides an external interface.
- Shared access to something is essential and runtime performance is paramount. Perhaps multiple components within your application require equal access to some expensive-to-compute variable. If you're willing to take on the risk of one of those components poisoning every other component with some silly mistake, then raw pointers are an option of last resort.

## 6.2.2 Rust's pointer ecosystem

Given that raw pointers are unsafe, what is the safer alternative? The alternative is to use *smart pointers*. In the Rust community, a smart pointer is some pointer type that has some kind of super power, over and above the ability to deference a memory address. You will probably encounter the term *wrapper type* as well. Rust's smart pointer types tend to wrap raw pointers and bestow them with added semantics.

A narrower definition of “smart pointer” is common in the C communities. There, authors (generally) imply that the term smart pointer means the C equivalents of Rust's `core::ptr::Unique`, `core::ptr::Shared` and `std::rc::Weak` types. You will be introduced to those four types shortly.

**NOTE**

The term **fat pointer** refers to memory layout. Thin pointers, such as raw pointers, are a single `usize` wide. Fat pointers are usually two `usize` wide. Occasionally more.

Rust has an extensive set of pointer (and pointer-like) types in its standard library. Each has their own role, strengths and weaknesses. Given their unique properties, rather than writing them out as a list, let's model them as characters in a card-based

role playing game.

Raw Pointer	Box<T>	Rc<T>												
 <p>The cousins <code>*mut T</code> and <code>*const T</code> are the free radicals of the pointer world. Lightning fast, but wildly unsafe.</p> <table border="0"> <tr> <td><b>Powers</b></td><td><b>Weaknesses</b></td></tr> <tr> <td> <ul style="list-style-type: none"> <li>• Speed</li> <li>• Can interact with outside world</li> </ul> </td><td> <ul style="list-style-type: none"> <li>• Unsafe</li> </ul> </td></tr> </table> <p><small>Image: Detail of <i>Acrobats Beneath Cherry Trees: Spinning Tops and Balancing</i> by Utagawa Yoshikazu</small></p>	<b>Powers</b>	<b>Weaknesses</b>	<ul style="list-style-type: none"> <li>• Speed</li> <li>• Can interact with outside world</li> </ul>	<ul style="list-style-type: none"> <li>• Unsafe</li> </ul>	 <p>Store anything in a box. Accepts almost any type for long term storage. The workhorse of a new, safe programming era.</p> <table border="0"> <tr> <td><b>Powers</b></td><td><b>Weaknesses</b></td></tr> <tr> <td> <ul style="list-style-type: none"> <li>• Store a value in central storage, in a location called "the heap"</li> </ul> </td><td> <ul style="list-style-type: none"> <li>• Size increase</li> </ul> </td></tr> </table> <p><small>Image: Detail from 15th edition of <i>Caesar's Column: A Story of the Twentieth Century</i> by Ignatius Donnelly</small></p>	<b>Powers</b>	<b>Weaknesses</b>	<ul style="list-style-type: none"> <li>• Store a value in central storage, in a location called "the heap"</li> </ul>	<ul style="list-style-type: none"> <li>• Size increase</li> </ul>	 <p>The reference counted pointer, <code>Rc&lt;T&gt;</code> is Rust's competent, yet miserly bookkeeper. It knows who has borrowed what and when.</p> <table border="0"> <tr> <td><b>Powers</b></td><td><b>Weaknesses</b></td></tr> <tr> <td> <ul style="list-style-type: none"> <li>• Shared access to values</li> </ul> </td><td> <ul style="list-style-type: none"> <li>• Size increase</li> <li>• Runtime cost</li> <li>• Not threadsafe</li> </ul> </td></tr> </table> <p><small>Image: Detail of <i>The Miser</i>, from <i>The Dance of Death</i> by Wenceslaus Hollar</small></p>	<b>Powers</b>	<b>Weaknesses</b>	<ul style="list-style-type: none"> <li>• Shared access to values</li> </ul>	<ul style="list-style-type: none"> <li>• Size increase</li> <li>• Runtime cost</li> <li>• Not threadsafe</li> </ul>
<b>Powers</b>	<b>Weaknesses</b>													
<ul style="list-style-type: none"> <li>• Speed</li> <li>• Can interact with outside world</li> </ul>	<ul style="list-style-type: none"> <li>• Unsafe</li> </ul>													
<b>Powers</b>	<b>Weaknesses</b>													
<ul style="list-style-type: none"> <li>• Store a value in central storage, in a location called "the heap"</li> </ul>	<ul style="list-style-type: none"> <li>• Size increase</li> </ul>													
<b>Powers</b>	<b>Weaknesses</b>													
<ul style="list-style-type: none"> <li>• Shared access to values</li> </ul>	<ul style="list-style-type: none"> <li>• Size increase</li> <li>• Runtime cost</li> <li>• Not threadsafe</li> </ul>													
Arc<T>	Cell<T>	RefCell<T>												
 <p><code>Arc&lt;T&gt;</code> is Rust's ambassador. It can share values across threads, guaranteeing that they will not interfere with each other.</p> <table border="0"> <tr> <td><b>Powers</b></td><td><b>Weaknesses</b></td></tr> <tr> <td> <ul style="list-style-type: none"> <li>• Shared access to values</li> <li>• Threadsafe</li> </ul> </td><td> <ul style="list-style-type: none"> <li>• Size increase</li> <li>• Runtime cost</li> </ul> </td></tr> </table> <p><small>Image: Detail of <i>The Grand Vizir giving Audience to the English Ambassador</i> by Robert Prisker</small></p>	<b>Powers</b>	<b>Weaknesses</b>	<ul style="list-style-type: none"> <li>• Shared access to values</li> <li>• Threadsafe</li> </ul>	<ul style="list-style-type: none"> <li>• Size increase</li> <li>• Runtime cost</li> </ul>	 <p>An expert in metamorphosis, Cell confers the ability to mutate immutable values.</p> <table border="0"> <tr> <td><b>Powers</b></td><td><b>Weaknesses</b></td></tr> <tr> <td> <ul style="list-style-type: none"> <li>• Interior mutability</li> </ul> </td><td> <ul style="list-style-type: none"> <li>• Size increase</li> <li>• Performance</li> </ul> </td></tr> </table> <p><small>Image: Detail from <i>On the Disposition of Iron in Variegated Strata</i> by George Mew</small></p>	<b>Powers</b>	<b>Weaknesses</b>	<ul style="list-style-type: none"> <li>• Interior mutability</li> </ul>	<ul style="list-style-type: none"> <li>• Size increase</li> <li>• Performance</li> </ul>	 <p>Perform mutation on immutable references with <code>RefCell&lt;T&gt;</code>. Its mind-bending powers come with some costs.</p> <table border="0"> <tr> <td><b>Powers</b></td><td><b>Weaknesses</b></td></tr> <tr> <td> <ul style="list-style-type: none"> <li>• Interior mutability</li> <li>• Can be nested within Rc and Arc, which only accept immutable refs</li> </ul> </td><td> <ul style="list-style-type: none"> <li>• Size increase</li> <li>• Runtime speed</li> <li>• Lack of compile-time guarantees</li> </ul> </td></tr> </table> <p><small>Image: Detail of figure 187 from <i>The Principles of Light and Color</i> by Edwin Abbott</small></p>	<b>Powers</b>	<b>Weaknesses</b>	<ul style="list-style-type: none"> <li>• Interior mutability</li> <li>• Can be nested within Rc and Arc, which only accept immutable refs</li> </ul>	<ul style="list-style-type: none"> <li>• Size increase</li> <li>• Runtime speed</li> <li>• Lack of compile-time guarantees</li> </ul>
<b>Powers</b>	<b>Weaknesses</b>													
<ul style="list-style-type: none"> <li>• Shared access to values</li> <li>• Threadsafe</li> </ul>	<ul style="list-style-type: none"> <li>• Size increase</li> <li>• Runtime cost</li> </ul>													
<b>Powers</b>	<b>Weaknesses</b>													
<ul style="list-style-type: none"> <li>• Interior mutability</li> </ul>	<ul style="list-style-type: none"> <li>• Size increase</li> <li>• Performance</li> </ul>													
<b>Powers</b>	<b>Weaknesses</b>													
<ul style="list-style-type: none"> <li>• Interior mutability</li> <li>• Can be nested within Rc and Arc, which only accept immutable refs</li> </ul>	<ul style="list-style-type: none"> <li>• Size increase</li> <li>• Runtime speed</li> <li>• Lack of compile-time guarantees</li> </ul>													

<p><b>Cow&lt;T&gt;</b></p>  <p>Why write something down when you only need to read it? Perhaps if you want to make modifications. This is the role of Cow (copy on write).</p> <table border="0"> <tr> <td><b>Powers</b></td> <td><b>Weaknesses</b></td> </tr> <tr> <td>• Avoids writes when only read access is used</td> <td>• Possible size increase</td> </tr> </table> <p><small>Image: Detail of Lessons for the flute alone as written by Thomas Britten</small></p>	<b>Powers</b>	<b>Weaknesses</b>	• Avoids writes when only read access is used	• Possible size increase	<p><b>String</b></p>  <p>Acting as a guide on how to deal with the uncertainties of user input, String shows us how to build safe abstractions.</p> <table border="0"> <tr> <td><b>Powers</b></td> <td><b>Weaknesses</b></td> </tr> <tr> <td>• Grows dynamically as required</td> <td>• Size, can over-allocate</td> </tr> <tr> <td>• Guarantees correct encoding at runtime</td> <td></td> </tr> </table> <p><small>Image: Detail from Remarks on the Abracadabra of the Nineteenth Century by William Leo-Wolf</small></p>	<b>Powers</b>	<b>Weaknesses</b>	• Grows dynamically as required	• Size, can over-allocate	• Guarantees correct encoding at runtime		<p><b>Vec&lt;T&gt;</b></p>  <p>The bedrock of dynamically sized types within Rust, Vec&lt;T&gt; understands how to provide a home for your data as needed.</p> <table border="0"> <tr> <td><b>Powers</b></td> <td><b>Weaknesses</b></td> </tr> <tr> <td>• Grows dynamically as required</td> <td>• Size, can over-allocate</td> </tr> </table> <p><small>Image: Detail from Chronologischer Raupenkalender, oder, Naturgeschichte der europäischen Raupen by Christian Friedrich Vogel</small></p>	<b>Powers</b>	<b>Weaknesses</b>	• Grows dynamically as required	• Size, can over-allocate		
<b>Powers</b>	<b>Weaknesses</b>																	
• Avoids writes when only read access is used	• Possible size increase																	
<b>Powers</b>	<b>Weaknesses</b>																	
• Grows dynamically as required	• Size, can over-allocate																	
• Guarantees correct encoding at runtime																		
<b>Powers</b>	<b>Weaknesses</b>																	
• Grows dynamically as required	• Size, can over-allocate																	
<p><b>RawVec&lt;T&gt;</b></p>  <p>The bedrock of Vec&lt;T&gt; and other dynamically sized types. Understands how to provide a home for your data as needed.</p> <table border="0"> <tr> <td><b>Powers</b></td> <td><b>Weaknesses</b></td> </tr> <tr> <td>• Grows dynamically as required</td> <td>• Not directly applicable from your code</td> </tr> <tr> <td>• Works with the memory allocator to find space</td> <td></td> </tr> </table> <p><small>Image: Detail from Chronologischer Raupenkalender, oder, Naturgeschichte der europäischen Raupen by Christian Friedrich Vogel</small></p>	<b>Powers</b>	<b>Weaknesses</b>	• Grows dynamically as required	• Not directly applicable from your code	• Works with the memory allocator to find space		<p><b>Unique&lt;T&gt;</b></p>  <p>Sole owner of a value, a unique pointer is guaranteed to possess full control.</p> <table border="0"> <tr> <td><b>Powers</b></td> <td><b>Weaknesses</b></td> </tr> <tr> <td>• Base for types requiring exclusive possession of values, such as String</td> <td>• Not appropriate for application code directly</td> </tr> </table> <p><small>Image: Detail from illustrations from From Earth to the Moon by Emile-Antoine Bayard</small></p>	<b>Powers</b>	<b>Weaknesses</b>	• Base for types requiring exclusive possession of values, such as String	• Not appropriate for application code directly	<p><b>Shared&lt;T&gt;</b></p>  <p>Sharing ownership is hard. Shared&lt;T&gt; makes life a little bit easier.</p> <table border="0"> <tr> <td><b>Powers</b></td> <td><b>Weaknesses</b></td> </tr> <tr> <td>• Shared ownership</td> <td>• Not appropriate for application code directly</td> </tr> <tr> <td>• Can align memory to T's width, even when empty</td> <td></td> </tr> </table> <p><small>Image: Detail from New Pictures in Old Frames: being a book of verse for girls and boys, written in old French forms, etc by Gertrude Bradley</small></p>	<b>Powers</b>	<b>Weaknesses</b>	• Shared ownership	• Not appropriate for application code directly	• Can align memory to T's width, even when empty	
<b>Powers</b>	<b>Weaknesses</b>																	
• Grows dynamically as required	• Not directly applicable from your code																	
• Works with the memory allocator to find space																		
<b>Powers</b>	<b>Weaknesses</b>																	
• Base for types requiring exclusive possession of values, such as String	• Not appropriate for application code directly																	
<b>Powers</b>	<b>Weaknesses</b>																	
• Shared ownership	• Not appropriate for application code directly																	
• Can align memory to T's width, even when empty																		

Each of the pointer types introduced here will be used extensively throughout the book. As such, we'll give them fuller treatment when they're needed. For now, the two novel attributes that appear within the "powers" section of some of these cards are *interior mutability* and *shared ownership*. They warrant some discussion:

### Interior mutability

You may wish to provide an argument to a method that takes a immutable values, yet you need to retain mutability. If you're willing to pay the runtime performance cost, it's possible to fake immutability. If the method requires an owned value, wrap the argument in `Cell<T>`. References can be wrapped in `RefCell<T>`. It is common when using reference counted types `Rc<T>` and `Arc<T>`, which only accept immutable arguments, to also be wrapped in `Cell<T>` or `RefCell<T>`. The resulting type might look like `Rc<RefCell<T>>`. This means that you pay the runtime cost twice, but with significantly more flexibility.

### Shared ownership

Some objects, such as network connections or access to some operating system service perhaps, are difficult to mould into the pattern of having a single place with read/write access at any given time. Code might be simplified if two parts of the program can share access to that single resource. Rust will allow you to do this, but at the expense of a runtime cost.

#### 6.2.3 Smart pointer building blocks

You may arise at a situation when you wish to build your own smart pointer type with its own semantics. Perhaps a new research paper has been released and you wish to incorporate its results into your own work. Perhaps you're conducting the research! Regardless, it might be useful to note that Rust's pointer types are extensible. That is, they're designed with extension in mind.

All of the programmer-facing pointer types, such as `Box<T>`, are built from more primitive types that live deeper within Rust, often in its `core` or `alloc` modules.

The C++ smart pointer types have Rust counterparts:

Here are some useful sarting points for when you investigate building your own smart pointer types:

- `core::ptr::Unique` is the basis for types such as `String`, `Box<T>` and the pointer field of `Vec<T>`
- `core::ptr::Shared` is the basis for `Rc<T>` and `Arc<T>`. It can handle situations where shared access is desired.

In addition, the following tools can also be very handy in certain situations.

- Deeply inter-linked data structures may benefit from `std::rc::Weak` and `std::arc::Weak` for single and multi-threaded programs respectively. They allow access to data within an `Rc/Arc` without incrementing its reference count. This can prevent never-ending cycles of pointers.
- `alloc::raw_vec::RawVec` supports `Vec<T>` and `VecDeq<T>` (an expandable, double-ended queue that hasn't appeared in the book so far). It understands how to allocate and deallocate memory in a smart way for any given type.
- `std::cell::UnsafeCell` sits behind both `Cell<T>` and `RefCell<T>`. If you would like to provide interior mutability to your types, its implementation is worth investigating.

A full treatment of building new safe pointers touches on some of Rust's internals. These building blocks have their own building blocks. Unfortunately, explaining every detail will diverge too far from our goals for this chapter.

### 6.3 Providing programs with memory for their data

This section attempt to demystify the terms: “the stack” and “the heap”. They often appear in contexts that pre-suppose you already know what they mean. That isn’t the

case here. We'll cover the details of what they are, why they are and how to make use of that knowledge to make your programs leaner and faster.

Some people hate wading through the details though. For those readers, here is salient difference between the stack and the heap:

- the stack is fast
- the heap is slow

That difference leads to the following axiom: “when in doubt, prefer the stack”. To place data onto the stack, the compiler must know the type’s size at compile time. Translated to Rust, that means “when in doubt, use types that implement `Sized`”.

Now that you've got the gist, it's time to learn when to take the slow path and how to avoid it when you want to go faster.

### 6.3.1 The stack

The stack is often described by analogy: think of a stack of dinner plates waiting in the cupboard of a commercial kitchen. Cooks are taking plates off the stack to serve food, lowly dishwashers are placing new plates on the top.

The unit—the plate—of a computing stack is the *stack frame*, also known as the *allocation record*. You are probably used to think of This is a group of variables and other data.

Like many descriptions in computing, “the stack” and “the heap” are analogies that only partially fit. If you are learning about them for the first time, you may need to detangle yourself from the mental picture of them created by its name.

The stack is often described by analogy to a stack of dinner plates waiting in the cupboard. Unfortunately, that mental picture is inaccurate. Here are some differences:

- the stack actually contains two levels of “objects”: *stack frames* and data
- the stack grants programmers with access to multiple elements stored within it, rather than the top item only.
- the stack can include elements of arbitrary size, where the implication of the dinner plate analogy is that all elements must be the same size.
- as an implementation detail, items within the stack are not necessarily removed from RAM when they are inaccessible from code. When dinner plates are picked up, they've really gone. Instead, some designated machinery within the CPU marks the location of the new top.

So why is the stack called the stack? Because of the usage pattern. Entries on the stack are made in a Last In, First Out (LIFO) manner.

The entries in the stack are called *stack frames*. Stack frames are created as function calls are made. As a program makes progress, a cursor within the CPU updates to reflect the current address of the current stack frame. The cursor is known as the *stack pointer*. As functions are called within functions, the stack pointer decreases in value

as the stack grows. When a function returns, the stack pointer increases.

Stack frames contain a function's state during the call. When a function is called within a function, the older function's values are effectively frozen in time. They are also known as a *activation frames*, and less commonly *allocation records*.<sup>19</sup> Unlike dinner plates, every stack frame is a different size. The stack frame contains space for its function's arguments, a pointer to the original call site and local variables (except the data which is allocated on the heap).

**TIP** If you are unfamiliar with what the term “call site” means, refer to the CPU emulation section of chapter 5.

To understand what is happening more fully, let's consider a thought experiment. Imagine a diligent, yet absurdly single-minded cook in a commercial kitchen. The cook takes each table's docket and places them in a queue. The cook has a fairly bad memory, so she writes down what her current order is in her own notebook. As new orders come in, she updates her notebook to refer to the new order. As she completes orders, her notebook is changed to the next item on the queue. Unfortunately for customers in this restaurant, the book operated in a last in, first out manner. Hopefully, you will not be one of the early orders during tomorrow's lunch rush. In this experiment, her notebook plays the role of the stack pointer. The stack itself is comprised of variable-length dockets, representing stack frames.

Like stack frames, restaurant dockets contain some metadata. The table number can act as the return address.

The stack's primary role is to make space for local variables. Why is the stack fast? All of a function's variables are side-by-side in memory. That speeds up access.

### ***Improving the ergonomics of functions that accept can only accept String or &str***

As a library author, it can simplify downstream application code if you could accept both `&str` and `String` types to your functions. Unfortunately, they're two types have very different representations in memory. One is allocated on the stack, the other is allocated on the heap.

Consider the example of validating a password. For the purposes of the example, a strong password is one that's at least 6 characters long.

#### ***Listing 6.8. Validating a password by checking its length***

```
fn is_strong(password: String) -> bool {
    password.len() > 5
}
```

`password_is_strong` can only accept `String`. That means that the following code won't work:

---

<sup>19</sup> To be precise, the activation frame is called a stack frame when allocated on the stack.

```
let pw = "justok";
let is_strong = is_strong(pw);
Generic code can help.
```

In cases where read-only access is required, use functions with the type signature `fn x<T: AsRef<str>> (a: T) rather than fn x(a: String)`. The fairly unwieldy type signature reads as "function x takes an argument password of type T, where T implements pass:[AsRef<str>]" Implementors of `AsRef<str>` behave as a reference to `str`, even when they're not.

Here is the code snippet again, now with the new signature in place:

#### **Listing 6.9. Accepting any type T that implements AsRef<str>. AsRef<str> means that it can behave as a reference to str.**

```
fn is_strong<T: AsRef<str>>(password: T) -> bool {    ①
    password.as_ref().len() > 5
}
```

① Calling code can provide a String or a &str as password.

When read/write access to the argument is required, normally you can make use of `AsRef<T>`'s sibling trait `AsMut<T>`. Unfortunately for this example, `& static str` cannot become mutable and so another strategy can be deployed: implicit conversion. It's possible to ask Rust to accept only those types which can be converted to `String`. We'll then perform that conversion within the function and apply any required business logic to that newly created `String`.

#### **Listing 6.10. Accepting any type T that can be converted to a String. This can circumvent the issue that &str is an immutable value.**

```
fn is_strong<T: Into<String>>(password: T) -> bool {
    pw.into().len() > 5
}
```

This implicit conversion strategy does have significant risks though. If a `String`-ified version of the `password` variable needs to be created multiple times in the pipeline, it would be much more efficient to require an explicit conversion within the calling application. That way the `String` will be created once and reused.

### **6.3.2 The heap**

This section introduces “the heap”. The heap is an area of a program’s memory for types that do not have sizes known at compile time.

What does it mean to have no known size at compile time? In Rust, there are two senses of this word. Some types grow and shrink over time as required. Obvious cases are `String` and `Vec<T>`. Other types, even though they don’t change size at runtime, are unable to tell the Rust compiler how much memory to allocate. These are known as *dynamically sized types*. Slices (`[T]`) are the commonly cited example. Slices have no compile-time length. Internally, they’re a pointer to some part of an array. But slices actually represent some number of elements within that array. Another example is

a *trait object*, which haven't been described in this book so far. Trait objects allow Rust programmers to mimic some features of dynamic languages, by allowing multiple types to be wedged into the same container.

## WHAT IS THE HEAP?

You will gain a fuller understanding of *what* the heap is once you work through the next section on virtual memory. For now, let's concentrate on what it is *not*. Once those points are clarified, we'll then work back towards some form of truth.

The word “heap” implies disorganisation. A closer analogy would be warehouse space in some medium-sized business. As deliveries arrive (as variables are created), the warehouse makes space available. As the business carries out its work, those materials are used and the warehouse space can now be made available for new deliveries. At times, there are gaps and perhaps a bit of clutter is left around over time. But overall, there is a good sense of order.

Another mistake that the “heap” has no relation to the data structure known as “a heap”. That data structure is often used to create priority queues. It's an incredibly clever tool in its own right, but right now it's a complete distraction. The heap is not a data structure. It's an area of memory.

Now that those two distinctions are made, let's inch towards an explanation. The critical difference from a usage point of view is that variables on the heap must be accessed via a pointer, whereas this is not required variables accessed on the stack.

Although it's a trivial example, let's consider two variables `a` and `b`. They're both representing integers, 40 and 60 respectively. In one of those cases though, the integer happens to live on the heap.

```
let a: i32 = 40;
let b: Box<i32> = Box::new(60);
```

Now, let's demonstrate that critical difference. The following code won't compile:

```
let result = a + b;
```

The boxed value assigned to `b` is only accessible via a pointer. To access that value, we need to *dereference* it. The *dereference operator* is a unary `*`, which prefixes the variable name:

```
let result = a + *b;
```

This syntax can be difficult to follow at first, as the symbol is also used for multiplication, but it does become more natural over time. Listing 6.11 is a complete example.

**Listing 6.11. Creating variables on the heap implies creating that variable via a pointer type, such as `Box<T>`.**

```
fn main() {
    let a: i32 = 40;      ①
    let b: Box<i32> = Box::new(60);    ②

    println!("{} + {} = {}", a, b, a + *b);  ③
}
```

- ① 40 lives on the stack
- ② 60 lives on the heap
- ③ To access the 60, we need to dereference it.

To get a feel for what the heap is and what is happening within memory as a program is running, let's consider a tiny example. All we will be doing is creating some numbers “on the heap”, then adding their values together.

A further introduction to using the heap is provided by the larger Listing 6.13 When run, the program produces some fairly trivial output: two 3s. Still, it's really the internals of the program's memory that are important here, not its results. A pictorial view of the program's memory as it runs follows the code at Figure 6.4, .

**Listing 6.12. Output from Listing 6.13**

3 3

**Listing 6.13. Allocating and de-allocating memory on the heap via `Box<T>` (`ch6/ch6-heap-via-box/src/main.rs`)**

```
use std::mem::drop;          ①

fn main() {
    let a = Box::new(1);      ②
    let b = Box::new(1);      ②
    let c = Box::new(1);      ②

    let result1 = *a + *b + *c;  ③

    drop(a);                ④
    let d = Box::new(1);
    let result2 = *b + *c + *d;

    println!("{} {}", result1, result2);
}
```

- ① Bring manual `drop()` into local scope
- ② Allocate values “on the heap”

- ③ The unary `*` is called the dereference operator. It returns the value within the box. `result1` holds the value 3.
- ④ Invoke `drop()`, freeing up memory for other uses

Listing 6.13 places four values “on the heap” and removes one. It contains some new—or at least less familiar—syntax that might be worthwhile to cover and/or recap:

- `Box::new(T)` allocates `T` on the heap. “Box” is term that can be deceptive if you don’t share its intuition. Something that has been “boxed” lives on the heap, with a pointer to it on the stack. This is demonstrated in the first column of Figure 6.4 , where the number `0x100` at address `0xffff` points to the value 1, at address `0x100`. However, there is no actual “box” of bytes enclosing a value. Nor is the value hidden or concealed in some way.
- `std::mem::drop` brings the function `drop()` into local scope. `drop()` is used to delete objects before their scope ends. Types that implement `Drop`, have a `drop()` method, but explicitly calling it is illegal within user code. `std::mem::drop` is an escape hatch from that rule.
- Asterisks next to variables (`*a, *b, *c, *d`) are unary operators. This is the *dereference operator*. Dereferencing a `Box::(T)` returns `T`. In our case, the variables `a, b, c` and `d` are references that refer to integers.

Each column illustrates what is happening inside memory at 6 lines of code. The stack appears as the boxes along the top, and the heap appears along the bottom. The figure omits several details, but should help you gain an intuition of the relationship between the stack and the heap.

**NOTE**

If you have experience with a debugger and wish to explore what is happening, be sure to compile your code with no optimizations. Compile your code with `cargo build` (or `cargo run`), rather than `cargo build --release`. Using the `--release` flag actually ends up optimizing all of the allocations and arithmetic away. If you are invoking `rustc` manually, the command to `rustc --codegen opt-level=0` if you are invoking `rustc` manually.

**Figure 6.4. A view into a program's memory during Listing 6.13**

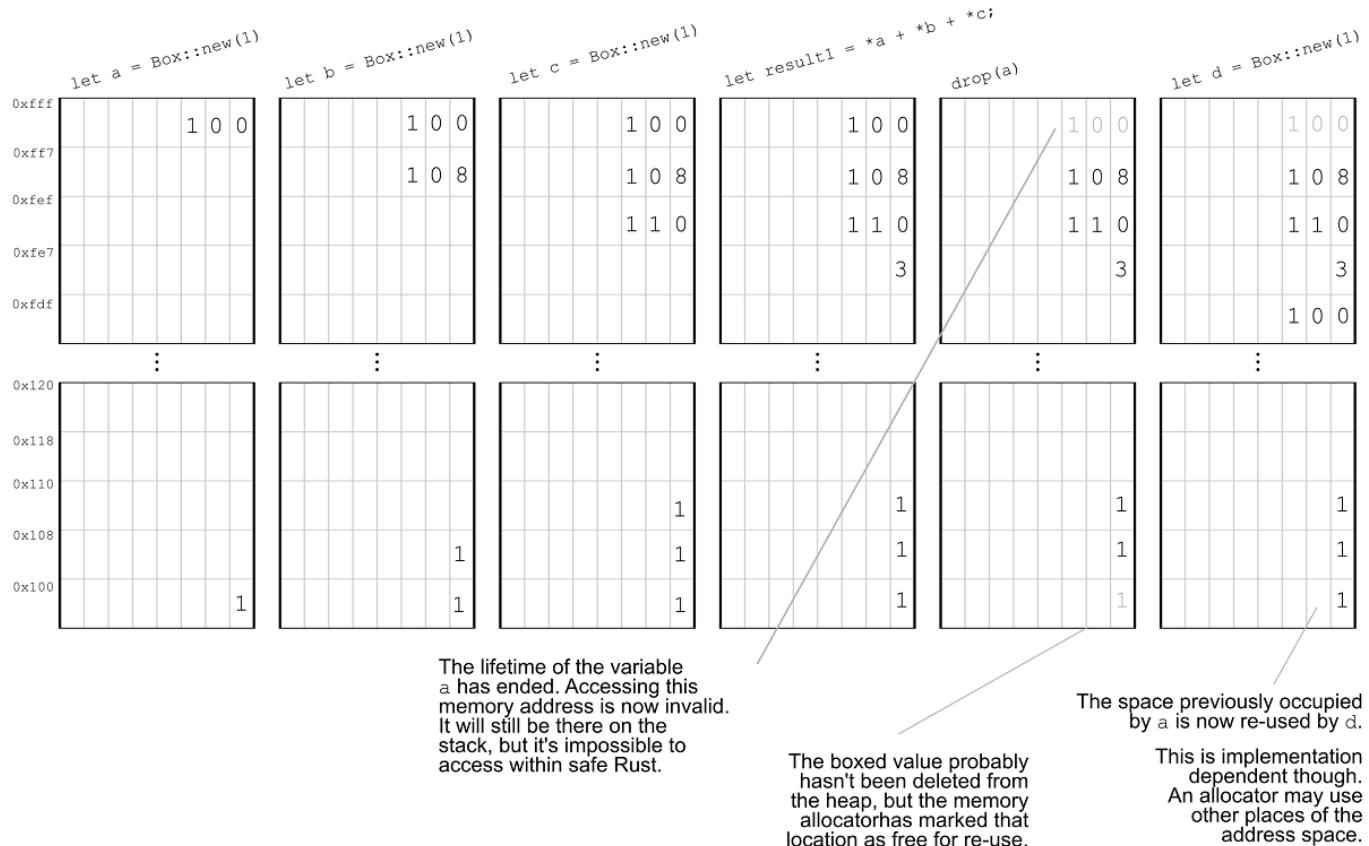
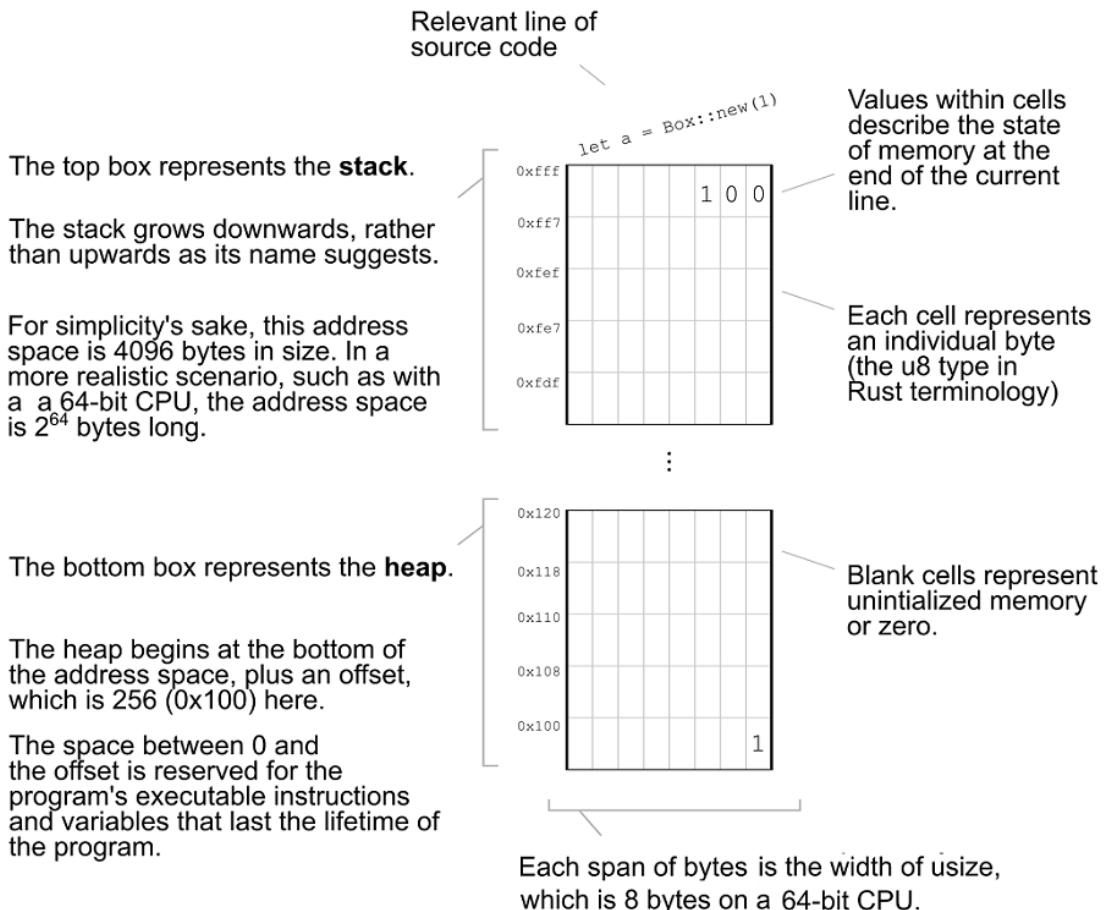


Figure 6.4 packs quite a lot of information into a small space. The following figure provides a short guide to interpreting it:

**Figure 6.5. How to Interpret Figure 6.4**



### 6.3.3 What is dynamic memory allocation?

At any given time, a running program has a fixed number of bytes to get its work done in. When it would like more, it needs to ask for it from the operating system. This is known as *dynamic memory allocation*.

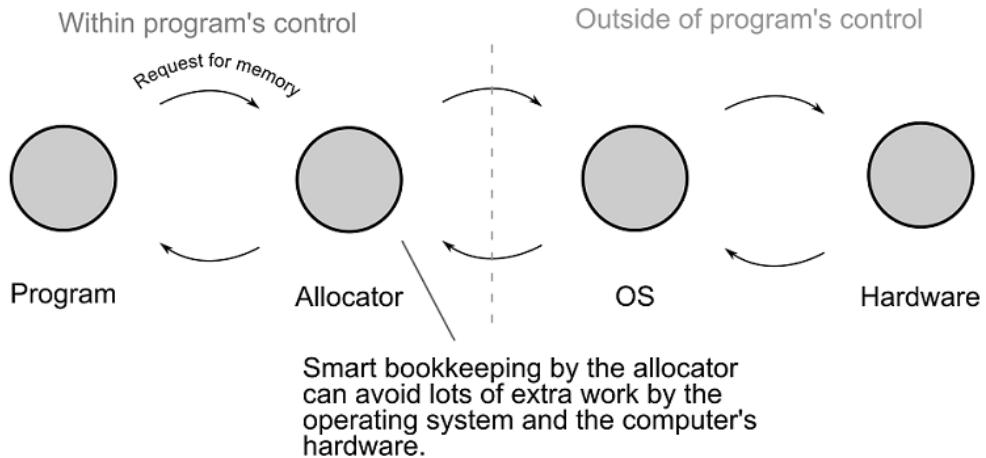
Dynamic memory allocation is usually discussed as a three step process:

- Step 1: Request memory from the operating system via `alloc()` (or, in MS Windows, via `HeapAlloc()`).
- Step 2: Make use of the allocated memory in the program.
- Step 3: Release memory that isn't needed back to the operating system via `free()` (or `HeapFree()`)

As it turns out, there is an intermediary between the program and the operating system: the allocator. The allocator—a specialist sub-program that is embedded into yours

behind the scenes—can perform optimizations that avoid lots of work within the operating system and CPU.

**Figure 6.6. Conceptual view of dynamic memory allocation.** Requests for memory originate and terminate at the program, but involve several other components. At each stage, the components may short-circuit the process and return quickly.



When can the allocator boost a program’s speed? Let’s consider the case of allocating and freeing memory for integers that are being created and destroyed over the lifetime of the program. A naïve allocator would request new memory from the operating system every time some new data is created. That allocator would release the memory back to the operating system immediately upon `Drop`. A smarter allocator holds onto memory that is available upon `Drop` for some future value that might need the space. Because integers are the same width in bytes, applying this caching logic can avoid lengthy trips to the operating system.

Listing 6.15 provides a trivial example.

When run, the program produces some fairly trivial output: two 3s. However, it’s actually the internal side-effects that wish to examine. They’re detailed within Figure 6.4 .

#### **Listing 6.14. Output from Listing 6.15**

```
3 3
```

#### **Listing 6.15. Allocating and de-allocating memory on the heap via `Box<T>` (`ch6/ch6-heap-via-box/src/main.rs`)**

```
use std::mem::drop;      ①
fn main() {
```

```

let a = Box::new(1);
let b = Box::new(1);
let c = Box::new(1);

let result1 = *a + *b + *c;      ②

drop(a);      ③
let d = Box::new(1);
let result2 = *b + *c + *d;

println!("{} {}", result1, result2);
}

```

- ① Bring manual drop() into local scope
- ② Use the variables so that they're not optimized away by the compiler. The unary \* operator is called the dereference operator. It returns the value within the box.
- ③ The memory holding a is now available for other allocations

Now that you we have some idea of what the heap's role is, let's examine its performance impact and strategies to reduce that impact. Before starting, let's recap why there's a performance difference. The stack enables very fast access to functions' local variables because they reside next to each other within RAM. Variables allocated on the heap could be anywhere.

To quantify this impact, we need to learn how to measure the cost. To get a large number of measurements, we need a program that creates and destroys many values. Let's create a toy program: a 2D particle fountain. Imagine looking top-down from a water jet, watching droplets fall to the ground. In our example, particles emerge from the center of the screen at an initial velocity and then a force slows the particle down.

This section of the chapter might be quite a lot to take in. Depending on your experience level, it's possible that there are some new layers of complexity that you'll need to absorb:

- New tools. We'll be creating logs from the Linux administration tool strace. strace allows you to trace system calls. To drive stract we'll be working with a command line shell, which itself may be new to some readers.
- New abstractions. The code introduces the concept of a "closure". While intuitive to those who already understand what's happening, they can be a mental barrier to those who haven't encountered them before.
- New terminology.

Despite the possibility of mental potholes, let's press on.

Listing 6.18 is centered around two main structs, `World` and `Shape`. `World` creates and destroys `Shape` instances over time, according to a sine wave pattern. Repeated creation and destruction allows us to examine the effect of memory allocation and deallocation. While running, the app spins in a main loop. At each iteration, the `World` has a update step and a render step. During the update step, the shapes are

repositioned. During the render, they're created on screen via some magic provided by the Piston game engine. Piston is a dependency that enables us to forget about how the rendering process works.

**NOTE**

Dear MEAP readers, unfortunately Listing 6.18 does not compile reliably with optimized code enabled (e.g. via `cargo run --release`) due to breakage released in a downstream release shortly before this chapter was released. Please compile it with `cargo run`. As changes are made downstream, they will make it in to updated dependencies in further editions of the MEAP.

**Screenshots from the result of running Listing 6.18**

After building Listing 6.18, you should see a window appear on your screen filled with a white background. Pulses of gray particles should start flowing from the centre.

**Listing 6.17. Build dependencies for Listing 6.18 (ch6/ch6-particles/Cargo.toml)**

```
[package]
name = "ch6-particles"
version = "0.1.0"
authors = ["TS McNamara <code@timmcnamara.co.nz>"]

[dependencies]
piston_window = "0.73"          ①
piston2d-graphics = "0.23"       ②
rand = "0.3"                     ③
```

- ① piston\_window provides a wrapper around the core functionality of the piston game engine. This will allow us to easily draw things on screen, largely irrespective of host environment.
- ② piston2d-graphics provides vector mathematics, which is important to simulate movement.
- ③ rand provides random number generators and associated functionality.

**Listing 6.18. A graphical application that creates and destroys many heap-allocated objects (ch6/ch6-particles/main.rs)**

```
extern crate graphics;           ①
extern crate piston_window;      ①
extern crate rand;               ①

use graphics::math::{ Vec2d, add, mul_scalar };           ②
use rand::distributions::{IndependentSample, Range};      ②

type RGBA = [f32; 4];           ③
const WHITE: RGBA = [1.0; 4];
const GRAY: RGBA = [0.7, 0.7, 0.7, 0.3];
const N_PARTICLES: usize = 500;  ④

struct World {                  ⑤
    current_turn: usize,
    shapes: Vec<Box<Shape>>,
    height: u32,
    width: u32,
}

struct Shape {                  ⑥
    height: f64,
    width: f64,
    position: Vec2d<f64>,
    velocity: Vec2d<f64>,
    acceleration: Vec2d<f64>,
    color: RGBA,
}

impl Shape {
    fn new(x: f64, y: f64) -> Self {           ⑦
        let mut rng = rand::thread_rng();          ⑧
    }
}
```

```

let legal_range = Range::new(-5_f64, 5_f64);

let x_speed = legal_range.ind_sample(&mut rng);
let y_speed = legal_range.ind_sample(&mut rng);
let x_accel = 0.1 * legal_range.ind_sample(&mut rng);
let y_accel = 0.1 * legal_range.ind_sample(&mut rng);

Shape {
    height: 10.0,
    width: 10.0,
    position: [x, y],
    velocity: [x_speed, y_speed],
    acceleration: [x_accel, y_accel],
    color: GRAY,
}
}

fn update(&mut self) {                                     ⑨
    self.velocity = add(self.velocity, self.acceleration); ⑩
    self.position = add(self.position, self.velocity);
    self.acceleration = mul_scalar(self.acceleration, 0.7); ⑪
    self.color[3] *= 0.97;                                ⑫
}
}

impl World {
    fn new(width: u32, height: u32) -> World {           ⑬
        World {
            current_turn: 0,
            shapes: Vec::<Box<Shape>>::new(),
            height: height,
            width: width,
        }
    }

    fn add_shapes(&mut self, n: usize) {                   ⑭
        let x = (self.width / 2) as f64;
        let y = (self.height / 2) as f64;

        for _ in 0..n {
            self.shapes.push(Box::new(Shape::new(x, y))); ⑮
        };
    }

    fn remove_shapes(&mut self, n: usize) {                ⑯
        let n_shapes = self.shapes.len();

        let to_remove = if n > n_shapes {
            n_shapes
        } else {
            n
        };
    }
}

```

```

        for _ in 0..to_remove {                                ⑯
            self.shapes.remove(0);                            ⑯
        }

        self.shapes.shrink_to_fit();                        ⑯
    }

fn calc_population_change(&self) -> isize {          ⑯
    const N: f64 = N_PARTICLES as f64;                  ⑯
    const MAX: f64 = N*0.5;                            ⑯
    const MIN: f64 = -N*0.5;                           ⑯
    let x: f64 = self.current_turn as f64;

    let n = 0.4*N*(0.1*x).sin() + 0.1*N*x.sin();      ⑯
    n.max(MIN).min(MAX).round() as isize               ⑯
}

fn update(&mut self) {
    let n = self.calc_population_change();

    if n > 0 {
        self.add_shapes(n as usize);
    } else {
        self.remove_shapes(n.abs() as usize);
    }

    self.current_turn += 1;
}
}

fn main() {
    let (width, height) = (640, 480);                  ⑯
    let mut window: PistonWindow =                   ⑯
        WindowSettings::new("particles", [width, height])
            .exit_on_esc(true)
            .build()
            .expect("Could not create a window.");

    let mut world = World::new(width, height);         ⑯
    world.add_shapes(N_PARTICLES);                     ⑯

    while let Some(event) = window.next() {           ⑯
        for shape in &mut world.shapes {              ⑯
            shape.update();                          ⑯
        }
        world.update();                            ⑯

        window.draw_2d(&event, |ctx, renderer| {      ⑯
            clear(WHITE, renderer);
            for s in &mut world.shapes {
                let rect = [s.position[0], s.position[1], s.width, s.height]; ⑯
            }
        });
    }
}

```

```
        let transformation_matrix = ctx.transform;
        rectangle(s.color, rect, transformation_matrix, renderer);
    }
});
```

- ① With `extern`, we bring external crates into the local crate's namespace.
  - ② With `use`, we are able to pull other functions from other modules into our own. That avoids needing to use the full path later on in our application.
  - ③ `RGBA` is a type alias that refers to a particular method of encoding color: Red, Green, Blue, Alpha (which controls transparency)
  - ④ Provides the starting number of shapes that will be generated when the program starts up
  - ⑤ `World` maintains the state of the whole scene, such as the window dimensions and a container of `Box<Shape>` instances
  - ⑥ Data contained within `Shape` relates to its movement over time (position, velocity and acceleration) and rendering (height, width and color).
  - ⑦ New `Shape` instances are created with random acceleration and velocity, albeit within a defined range of  $[-0.5, 0.5]$
  - ⑧ Random number generator instances must be created as mutable, as their internal values change during each call
  - ⑨ `Shape` updates itself by changing its position and increasing its transparency at each step.
  - ⑩ There is no matrix/vector math operators within the language. `graphics::math` is providing this functionality for us.
  - ⑪ Slow down the shape's movement
  - ⑫ Dim the shape, by reducing its alpha channel, which increases its transparency when rendered
  - ⑬ New `World` instances are created with no shapes. Later in the `main()` function, shapes are added before the first screen is rendered.
  - ⑭ `add_shapes()` creates `Shape` instances in the middle of the `World`
  - ⑮ Here we force the `Shape` instances to be allocated on the heap via `Box<T>`
  - ⑯ `remove_shapes()` deletes `Shape` instances from the `World`. To avoid crashes at runtime, it first checks to see that there are enough `Shape` instances to delete.
  - ⑰ Remove the oldest particle. This is quite an inefficient operation, as all remaining particles are shifted to fill the now-empty slot. A smarter strategy would be to use `std::collections::VecDeque`, which supports removing from the front without needing to shift data around afterwards.
  - ⑱ `shrink_to_fit()` will help to force a re-allocation later when shapes are added.
  - ⑲ `calc_population_change()` indicates to `World` whether it should add or delete `Shape` instances this turn. Using sine functions creates pulses of particles, but isn't entirely cache friendly.
  - ⑳ Define `N` as a shorter alias for `N_PARTICLES`
  - ㉑ Limit range of growth/death then convert to `isize`
  - ㉒ Define window width and height
  - ㉓ Create an OS-native application window
  - ㉔ Initialize the world with particles

- ㉕ This is Piston's "main loop". `window.next()` will iterate forever, or until the ESC key is pressed, whichever is first. The event objects that `window.next()` generates are important to Piston, but are not immediately interesting to us here.
- ㉖ The update step. Each of the objects that we have created so far will have their `update()` methods called on them.
- ㉗ The render step. The `|ctx, renderer| { ... }` syntax is our first encounter with a closure in Rust. This is a function defined in-line that is repeatedly called each step. This is part of the `piston_window` public API and is explained in more depth shortly. The `clear()` and `rectangle()` functions are provided by Piston. A transformation matrix is a matrix used heavily to optimize rendering speed (that we don't make any use of here!)

Listing 6.18, is a fairly long code example, but hopefully it does not contain any code that's too alien from what you've already seen. Towards the end, the code example introduces Rust's closure syntax. If you look at the call to `window.draw_2d()`, it has a second argument with vertical bars surrounding two variable names (`|ctx, renderer| { ... }`). Those vertical bars provide space for the closure's arguments and the curly braces are its body.

A closure is a function that is defined in-line and can access variables from its surrounding scope. They're often called a *anonymous* or *lambda* functions.

Closures a common feature within idiomatic Rust code. They will be explained in detail as the book covers concurrency. They have been deliberately kept out of examples so far as there has been so much other new content to grasp. For the moment though, let's provide some evidence that allocating on the heap (many millions of times) can have a performance impact on your code.

Linux-based operating systems often come equipped with the `ltrace` utility. `ltrace` stands for "library trace". It allows us to inspect what our program and its dependencies are doing when accessing other code. As well as detecting *what* the program is doing calling functions from external libraries, it allows us to see exactly *how long* each of those functions took before they returned.

To begin, the project needs to be set up:

- Open a terminal window
- Move to a scratch directory, perhaps `/tmp/`
- Execute `cargo new --bin --vcs none particles`
- Copy the code from Listing 6.18 into the `./particles/src/main.rs` file, replacing the `main()` function created by `cargo`
- Execute `cargo run`. A graphical window should appear filled with grey rectangles.

To run our program under tracing, follow these steps:

- Execute `cargo build` to confirm that the executable is available for tracing.
- Execute `pass:[timeout 20 ltrace -T -o trace.txt -e - *+malloc+free+realloc ./target/release/particles]`. This creates a log file

of activities written to `trace.txt`. The argument `pass:[-e - *+malloc+free+realloc]` says “record only calls to `malloc`, `free` and `realloc`”.

- Executing pass:[`sed 's/->/ /' trace.txt | sed 's/, /|/' | tr '()'>=' '=' | column -t | tr -s ' ' '\t'` > trace.tsv]

formats trace.txt to create a tab-delimited file that can be interpreted by the plotting tool gnuplot.

With `trace.txt` and `trace.tsv` available, we can begin to perform some performance tuning. For example, we can use the command line to print out a list of the most common requests for memory via the shell command `grep malloc trace.txt | cut -d ' ' -f 1 | sort | uniq -c | sort -rn | head -n 10`. That line (very approximately) reads as, “search `trace.txt` for the term `malloc`, reformat the results, find the unique lines and their counts, then print out the top 10”.

139472	gallium_dri.so->malloc(72)	(1)
32545	particles->malloc(96)	(2)
1815	libstdc++.so.6->malloc(24)	
1814	libxcb.so.1->malloc(16)	
1034	libX11.so.6->malloc(16)	
958	libX11.so.6->malloc(72)	
944	libxcb.so.1->malloc(76)	
921	libX11.so.6->malloc(40)	
901	libstdc++.so.6->malloc(16)	
690	libX11.so.6->malloc(208)	

- ① A very large number of small allocations are requested by the `gallium_dri.so` library—part of the Mesa 3D graphics library—that we're unable to influence directly.
  - ② This is the line that interests us most. Our program makes 32k requests for memory of the same size. This provides indication that allocating a large array to hold multiple objects will be more time efficient over the life of the program.

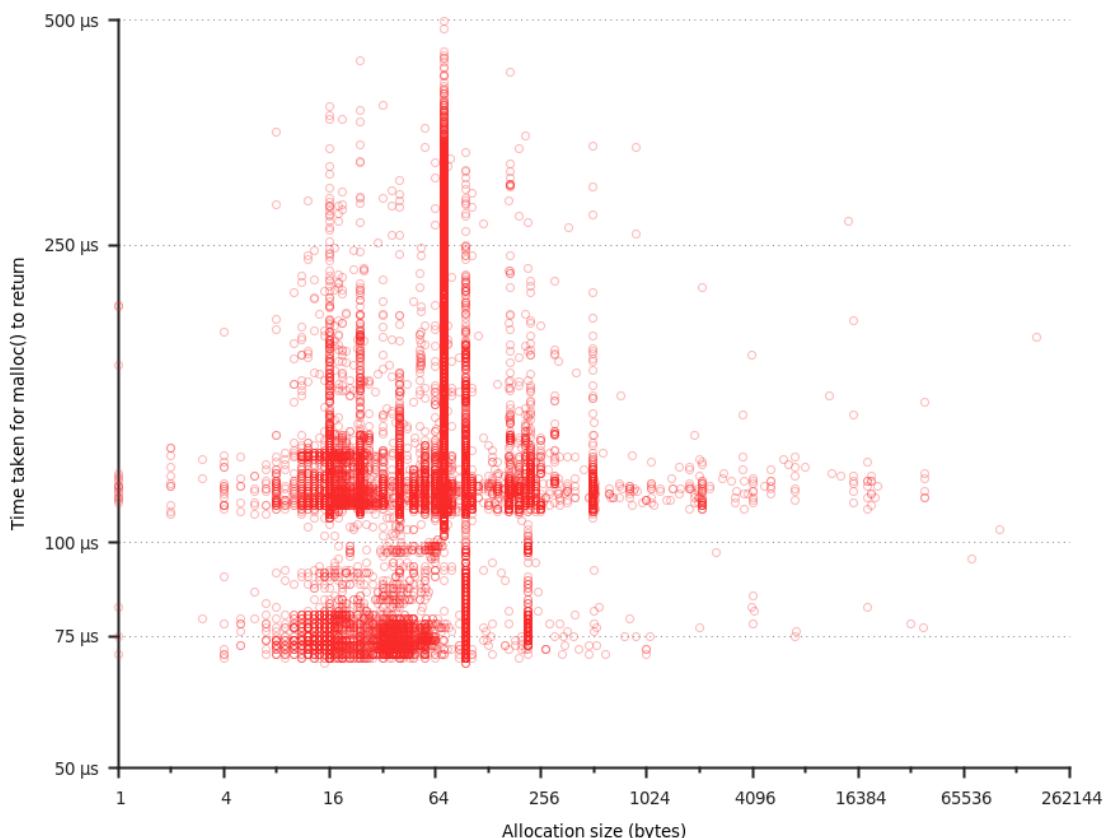
`trace.txt` is a raw extract from `ltrace`. Each line represents a call to a function and has the following signature: "caller→function(arg, ...) = return value <duration (secs)>". From this snippet, we can see that the calls to `malloc()` take an integer as an argument and returns a memory address. Conversely, `free()` takes a memory address as an argument and returns `<void>`, aka `NULL`.

**Listing 6.19. A formatted extract from the output of ltrace on the particles executable produced by Listing 6.18 (ch6/ch6-tracing-output/trace.txt)**

- ① A request for 4 bytes (`particles->malloc(4)`) takes 0.00009 seconds, whereas a request for 10x more memory (`particles->malloc(40)`) takes less time (0.00008 seconds).

One interesting aspect from this short extract is that memory allocation speed is not correlated with allocation size. When every heap allocation is plotted, this becomes even clearer:

**Figure 6.7. Plotting heap allocation times against allocation size shows that there is no clear relationship. The time taken to allocate memory is essentially unpredictable, even when requesting the same amount of memory multiple times.**



To generate your own version of Figure 6.7 , the following gnuplot script can be tweaked as desired.

**Listing 6.20. Script used to generate Figure 6.7 with gnuplot**

```
# GENERAL SETTINGS
set key off
set rmargin 5
```

```

set grid ytics noxtics nocbtics back
set border 3 back lw 2 lc rgbcolor "#222222"

# X AXIS
set xlabel "Allocation size (bytes)"
set logscale x 2
set xtics nomirror out

# Y AXIS
set ylabel "Time taken for malloc() to return"
set logscale y
set yrange [0.00005 to 0.0005]
set ytics ( \
    "50 {/Symbol m}s" 0.00005, \
    "75 {/Symbol m}s" 0.000075, \
    "100 {/Symbol m}s" 0.0001, \
    "250 {/Symbol m}s" 0.00025, \
    "500 {/Symbol m}s" 0.0005, \
)
# "
# "750 {/Symbol m}s" 0.00075, \
# "1000 {/Symbol m}s" 0.001, \
# "2500 {/Symbol m}s" 0.0025, \
# "5000 {/Symbol m}s" 0.005 \
# )
set ytics nomirror out

plot "allocs.tsv" with points pointtype 6 linecolor rgbcolor "#aaafa2a2a"
print "done"

```

The unstable dynamics of the time to return from `malloc()` might justify the time to investigate some alternatives. Perhaps those hundreds of microseconds really do count for your application.

Some general strategies include:

- Using arrays of uninitialized objects. Instead of creating objects from scratch as required, create a bulk lot of them with zeroed values. When the time comes to activate one of those objects, set its values to non-zero. This can be a very dangerous strategy, as you're circumventing Rust's lifetime checks.
- Using an alternative allocator. Memory allocators are often sensitive to the sizes where they perform best at.
- Investigate `arena::Arena` and `arena::TypedArena`. They allow objects to be created on-the-fly, but `alloc()` and `free()` are only called when the arena is created and destroyed.

## 6.4 Virtual Memory

This section explains what the term *virtual memory* means and why it exists. You will be able to use this knowledge to speed up your programs, by building software that “goes with the grain”. CPUs can compute faster when they’re able to access memory

quickly. Understanding some of the dynamics of the computer architecture can help to provide CPUs with memory efficiently.

### 6.4.1 Background

I have spent far too much of my life playing computer games. As enjoyable and challenging as I've found them, I've often wondered about whether I would have been better off spending my teenage years doing something more productive. Still, it's left me with plenty of memories. Some of those memories still leave a bitter taste. Occasionally, someone would enter the game and obliterate everyone with near perfect aim and seemingly impossibly high health ratings. Other players would decry "cheater!" but were more-or-less helpless in defeat. While waiting in in-game purgatory, I would sit wondering: "How is that possible? How are those tweaks to the game actually made?"

By working through this section's examples, you would have built the core of a tool that's capable of inspecting and modifying values of a running program.

#### **Glossary of terms related to virtual memory**

Terminology within this area is particularly arcane. It is often tied to decisions made many decades ago when the earliest computers were being designed. Here is a quick reference of some of the most important terms:

##### **Page**

Fixed-size block of words of *real memory*. Typically 4kb in size for 64-bit operating systems.

##### **Word**

Any type that is size of a pointer. This corresponds to the width of the CPU's registers. In Rust, `usize` and `isize` are word-length types.

##### **Page fault**

An error raised by the CPU when a valid memory address is requested that is not currently in physical RAM. Signals to the operating system that at least one page must be swapped back in to memory.

##### **Swapping**

Migrating a page of memory stored temporarily on disk from main memory upon request.

##### **Virtual memory**

The program's view of its memory. All data accessible to a program is provided in its address space by the operating system.

##### **Real memory**

The operating system's view of the physical memory available on the system. In many technical texts, real memory is defined independently from real memory, which becomes much more of an electrical engineering term.

##### **Page table**

The data structure maintained by the operating system to manage translating from virtual to real memory.

##### **Segment**

A segment is a block within virtual memory. Virtual memory is divided into blocks to minimize the space required to translate between virtual and physical addresses.

##### **Segmentation fault**

An error raised by the CPU when an illegal memory address is requested.

**MMU:** A component of the CPU that manages memory address translation. Maintains a cache of recently-translated addresses called the TLB, which stands for the translation lookaside buffer although that terminology has fallen from fashion.

**Note:** One term that has not been defined in any technical sense so far in this book is “process”. If you’ve encountered it before and have been wondering why it has been omitted, it will be introduced properly when concurrency is introduced. For now, consider the terms “process” and its peer “operating system process” to refer to a running program.

## 6.4.2 Step 1: Having a Process Scan Its Own Memory

Intuitively, a program’s memory is a series of bytes that starts at location 0 and ends at location  $n$ . If a program reports 100kB of RAM usage, it would seem that  $n$  would be somewhere near 100,000. Let’s test that intuition.

We’ll create a small command-line program that looks through memory, starting at location 0 and ending at 10,000. As it’s a small program, it shouldn’t occupy more than 10,000 bytes.

When executed, the program will not perform as intended. Sadly, it will crash. You’ll learn why why the crash occurs as your follow through this section.

**Listing 6.21. Attempting to scan through a running program’s memory byte by byte, starting at zero. This listing introduces the syntax for creating raw pointers and dereferencing (reading) them. (ch6/ch6-memscan-1/src/main.rs)**

```
fn main() {
    let mut n_nonzero = 0;

    for i in 0..10000 {
        let ptr = i as *const u8;          ①
        let byte_at_addr = unsafe { *ptr }; ②

        if byte_at_addr != 0 {
            n_nonzero += 1;
        }
    }

    println!("non-zero bytes in memory: {}", n_nonzero);
}
```

- ① Convert `i` to a `*const T`, a “raw pointer” of type `u8`. Raw pointers allow programmers to inspect raw memory addresses. We treat every address as a unit, ignoring the fact that most values span multiple bytes.
- ② Dereference the pointer. That is, read the value at address `i`. Another way of saying this is read the value being pointed to.

Listing 6.21 crashes because it is attempting to dereference a NULL pointer.

When `i` equals `0`, `ptr` can't really be dereferenced. Incidentally, this is why all raw pointer dereferences must occur within an `unsafe` block. How about we attempt to start from a non-zero memory address? Given that the program is executable code, there should be several thousand bytes of non-zero data to iterate through at least.

**Listing 6.22. Scanning a process's memory, starting from 1 to avoid dereferencing a NULL pointer**

```
fn main() {
    let mut n_nonzero = 0;

    for i in 1..10000 {      ①
        let ptr = i as *const u8;
        let byte_at_addr = unsafe { *ptr };

        if byte_at_addr != 0 {
            n_nonzero += 1;
        }
    }

    println!("non-zero bytes in memory: {}", n_nonzero);
}
```

① Start at 1 rather than 0 to avoid NULL pointer exception

This unfortunately does not solve the issue completely. Listing 6.22 still crashes upon execution and the number of non-zero bytes is never printed to the console. This is due to what's known as a *segmentation fault*.

Segmentation faults are generated when the CPU and operating system detect that your program is attempting to access memory regions that it isn't entitled to. Memory regions are divided into segments. That explains the name.

Let's try a different approach. Rather than attempting to scan through bytes, let's look for the addresses of things that we know exist. We've spent lots of time learning about pointers, let's put that to use. Listing 6.24 creates several values, examining their addresses.

Every run of Listing 6.24 will (probably) generate unique values. Here is the output of one run:

**Listing 6.23. Output from Listing 6.24**

```
GLOBAL:      0x7ff6d6ec9310
local_str:  0x7ff6d6ec9314
local_int:   0x23d492f91c
boxed_int:   0x18361b78320
boxed_str:   0x18361b78070
fn_int:     0x23d492f8ec
```

As you can see, values appear to be scattered across a very wide range. So despite your program (hopefully) only needing a few kilobytes of RAM, a few variables live in giant locations. These are *virtual addresses*. As explained in the heap vs stack section, the stack starts at the top of the address space and the heap near the bottom. In this run, the highest value is `0x7ff6d6ec9314`. That's approximately  $2^{64} \div 2$ . That number is due to the operating system reserving half of the address space for itself.

**Listing 6.24. Printing out the address of several variables within a program to examine its address space (ch6/ch6-memscan-3/src/main.rs)**

```
static GLOBAL: i32 = 1000;          ①

fn noop() -> *const i32 {
    let noop_local = 12345;        ②
    &noop_local as *const i32     ③
}

fn main() {
    let local_str = "a";          ④
    let local_int = 123;          ④
    let boxed_str = Box::new('b'); ④
    let boxed_int = Box::new(789); ④
    let fn_int = noop();         ④

    println!("GLOBAL: {:p}", &GLOBAL as *const i32);      ⑤
    println!("local_str: {:p}", local_str as *const str);  ⑤
    println!("local_int: {:p}", &local_int as *const i32);   ⑤
    println!("boxed_int: {:p}", Box::into_raw(boxed_int)); ⑤
    println!("boxed_str: {:p}", Box::into_raw(boxed_str)); ⑤
    println!("fn_int: {:p}", fn_int);                      ⑤
}
```

- ① Create a global static, which is a global variable in Rust programs
- ② Create a local variable within `noop()` so that something is from outside of `main()` has a memory address
- ③ Return the address of `noop_local` as a raw pointer
- ④ Create various values of several types, including values on the heap.
- ⑤ Print out the values' addresses

By now, you'll be pretty good at being able to access addresses of stored values. There are actually two small lessons that you also picked up on:

- Some memory addresses are illegal. The operating system will shut your program down if it attempts to access memory that is out of bounds.
- Memory addresses are not arbitrary. Although they seem to be spread quite far apart within the address space, values are clustered together within pockets.

Before pressing on with the cheat program, let's step back and look at the system that's operating behind the scenes to translate these virtual addresses to real memory.

### 6.4.3 Translating virtual addresses to physical addresses

Accessing data in a program requires virtual addresses—the only addresses that the program itself has access to—gets translated into physical addressed. This process involves a dance between the program, the operating system, the CPU, the RAM hardware and occasionally hard drives and other devices.

The CPU is responsible for performing this translation, but the operating system stores the instructions. CPUs contain a *memory management unit* (MMU) that is designed for this one job. For every running program, every virtual address is mapped to a physical address. Those instructions are stored in memory too (at a pre-defined address). That means, in the worst case, every attempt at accessing memory addresses incurs two memory lookups.

The worst case is possible to avoid. The CPU maintains a cache of recently translated addresses. That is, the CPU has its own (fast) memory to speed up accessing memory. For historic reasons, this cache is known as the *translation lookaside buffer*, often abbreviated as TLB. For programmers optimizing for performance, keep your data structures lean and avoid deeply nested structures. Reaching the capacity of the TLB (typically around 100 for x86 processors) can be costly.

Looking into how the translation system operates reveals more, often quite complex, details. Virtual addresses are grouped into blocks called *pages*, which are typically 4kb in size. This practice avoids needing to store a translation mapping for every single variable in every single program. Having a uniform size for each page also assists to avoid a phenomenon known as *memory fragmentation*, where pockets of empty, yet unusable, space appear within available RAM.

**NOTE**

This is a general guide only. The details of how the OS and CPU cooperate to manage memory differs significantly in some environments. In particular, constrained environments such as microcontrollers may use real addressing. For those interested in learning more, the research field is known as *computer architecture*.

The operating system and CPU can play some interesting tricks when data lives within pages of virtual memory:

- Having a virtual address space allows the operating system to overallocate. Programs that ask for more memory than the machine can physically provide are able to be accommodated.
- Inactive pages of memory can be swapped to disk in a byte-for-byte manner until its requested by the active program. Swapping is often used in periods of high contention for memory, but can be used more generally depending on an operating system's whims.
- Other size optimizations can be performed, such as compression. A program will see its memory intact. Behind the scenes, the operating system has compressed the program's wasteful data usage.
- Programs are able to share data quickly. If your program requests a large block of zeroes, say for a newly-created array, the operating system might point you

towards a page filled with zeroes that is currently being used by three other programs. None of the programs are aware that the others are looking at the same physical memory and the zeroes have different positions within their virtual address space.

- Paging can speed up the loading of shared libraries. As a special case of the previous bullet point, if a shared library has already been loaded by another program, the operating system can avoid loading it into memory twice by pointing the new program to the old data.
- Paging adds security between programs. As you discovered earlier in the section, some parts of the address space are illegal to access. The operating system has other attributes that it can add. If an attempt is made to write to a read only page, the program will be terminated by the operating system.

Making effective use of the virtual memory system in day-to-day programs requires thinking about how data is represented in RAM. Here are some guidelines:

- Keep hot working portions of your program within 4kb of size. This will maintain very fast lookups.
- If 4kb is unreasonable for your application, then the next target to keep under is 4kb\*100. That rough guide should mean that the CPU can maintain its translation cache (the TLB) in good order to support your program.
- Avoid deeply nested data structures with pointer spaghetti. If a pointer points to another page, then performance will suffer.
- Test the ordering of your nested loops. CPUs read small blocks of bytes from the RAM hardware, known as a *cache line*. When processing an array, you can take advantage of this by investigating whether you are doing column-wise operations or row-wise operations.

One thing to note: virtualization makes this situation worse. If you’re running an app inside a virtual machine, the hypervisor must also translate addresses for its guest operating systems. This is why many CPUs ship with “virtualization support”, which can reduce this extra overhead. Running containers within virtual machines adds another layer of indirection and therefore latency. For bare metal performance, run apps on bare metal.

### **How does an executable file turn into a program’s virtual address space?**

The layout of executable files (aka binaries) have many similarities to the address space diagram that we saw earlier in the heap vs stack section of the chapter.

While the exact process is dependent on the operating system and file format, here is a representative example. Each of the segments of the address space that we have been discussing are described by binary files. When the executable is started, the operating system loads the right bytes into the right places. Once the virtual address space is created, the CPU can be told to jump to the start of the .text segment and the program begins executing.

## Executable File (ELF)

### File Header

Describes the file type.

### Program Header

Describes the memory segments used by the program and their attributes.

### Common Segments

#### .bss

Historic name, originally stood for "Block Started by Symbol". Location for uninitialized static variables. Takes up very little space in the file, typically only a length of needed bytes.

#### .rodata

Stands for "Read only data". Location for initialized immutable values with a, static lifetime such as string literals (static T).

#### .data

Location for initialized mutable global variables with a static lifetime (static mut T).

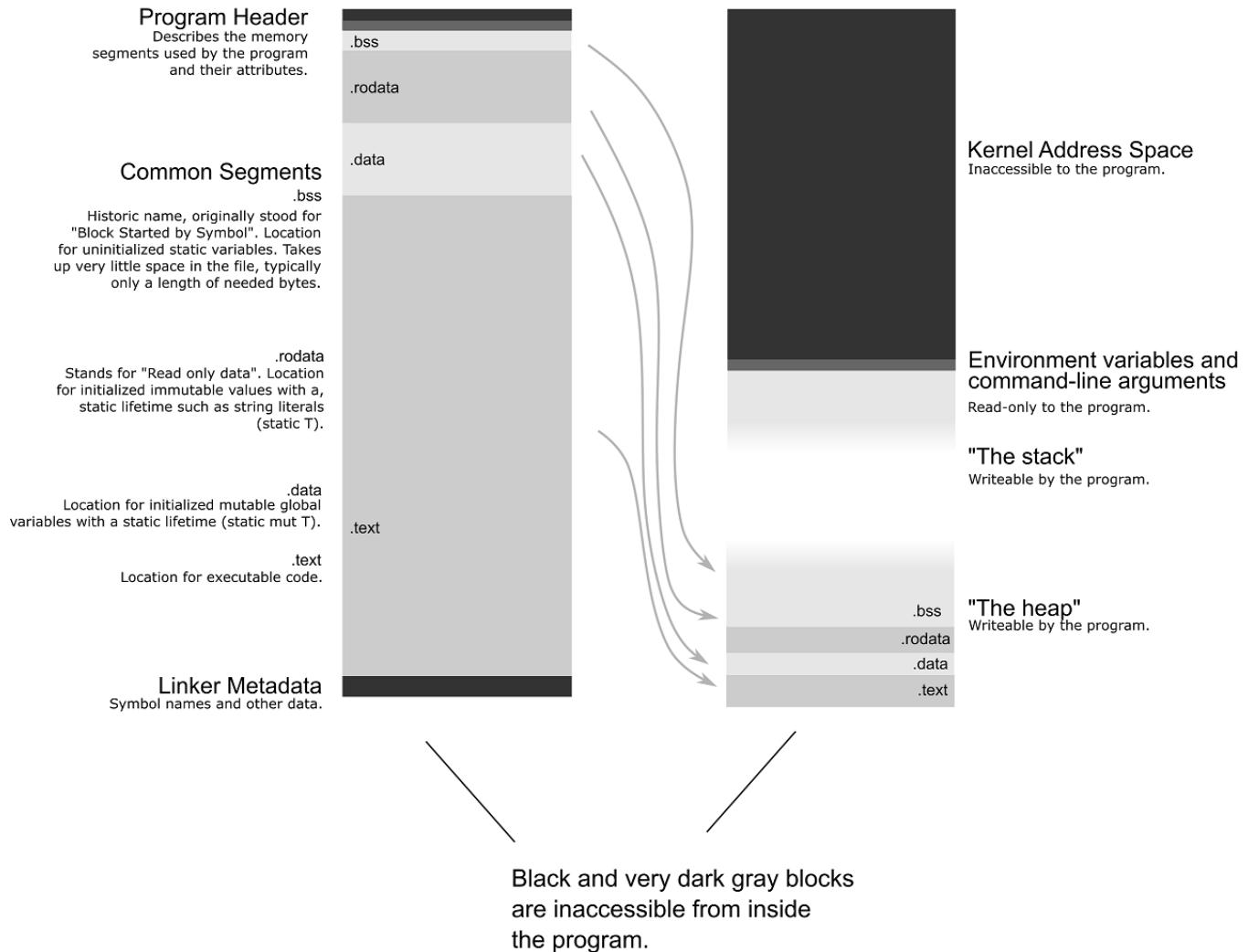
#### .text

Location for executable code.

### Linker Metadata

Symbol names and other data.

## Virtual Address Space



### 6.4.4 Step 2: Working with the operating system to scan an address space

Our task is to scan our program's memory while it's running. As we've discovered, the operating system maintains the instructions for mapping between a virtual address and a physical address. Perhaps we can ask the operating system to tell us what is happening?

Operating systems provide an interface for programs to be able to make requests,

known as *system calls*. Within Windows, the KERNEL.DLL provides the necessary functionality to be able to inspect and manipulate memory of a running process.

**NOTE**

Why Windows? Well, many Rust programmers use MS Windows as a platform. Also, its functions are quite well named and don't require as much prior knowledge as the POSIX API.

When you run Listing 6.27 , you should see lots of output with many sections similiar to the following:

**Listing 6.25. Output from Listing 6.27**

```
MEMORY_BASIC_INFORMATION {           ①
    BaseAddress: 0x00007ffbe8d9b000,
    AllocationBase: 0x0000000000000000,
    AllocationProtect: 0,             ②
    RegionSize: 17568124928,
    State: 65536,                  ②
    Protect: 1,                     ②
    Type: 0                         ②
}
MEMORY_BASIC_INFORMATION {
    BaseAddress: 0x00007fffffe0000,
    AllocationBase: 0x00007fffffe0000,
    AllocationProtect: 2,
    RegionSize: 65536,
    State: 8192,
    Protect: 1,
    Type: 131072
```

- ① MEMORY\_BASIC\_INFORMATION is a struct defined within the Windows API.
- ② These fields are the integer representations of enums defined within the Windows API. It's possible to decode these to the enum variant names, but this isn't available without adding extra code to the listing.

**Listing 6.26. Dependencies for Listing 6.27 (ch6/ch6-meminfo-win/Cargo.toml)**

```
[package]
name = "meminfo"
version = "0.1.0"
authors = ["Tim McNamara <code@timmcnamara.co.nz>"]

[dependencies]
winapi = "0.2"          ①
kernel32-sys = "0.2"     ②
```

- ① Defines some useful type aliases
- ② Provides interaction with KERNEL.DLL from the Windows API

**Listing 6.27. Inspecting a program's memory via the Windows API**

```

extern crate kernel32;
extern crate winapi;

use winapi::{
    DWORD,          ①
    HANDLE,         ②
    LPVOID,         ②
    PVOID,          ③
    SIZE_T,         ④
    LPSYSTEM_INFO,  ⑤
    SYSTEM_INFO,    ⑥
    MEMORY_BASIC_INFORMATION, ⑥
};

fn main() {
    let this_pid: DWORD;                      ⑦
    let this_proc: HANDLE;                    ⑦
    let min_app_addr: LPVOID;                 ⑦
    let max_app_addr: LPVOID;                 ⑦
    let mut base_addr: PVOID;                ⑦
    let mut proc_info: SYSTEM_INFO;           ⑦
    let mut mem_info: MEMORY_BASIC_INFORMATION; ⑦

    const MEMINFO_SIZE: usize = std::mem::size_of::<MEMORY_BASIC_INFORMATION>();

    unsafe { ⑧
        base_addr = std::mem::zeroed();
        proc_info = std::mem::zeroed();
        mem_info = std::mem::zeroed();
    }

    unsafe { ⑨
        this_pid = kernel32::GetCurrentProcessId();
        this_proc = kernel32::GetCurrentProcess();
        kernel32::GetSystemInfo(&mut proc_info as LPSYSTEM_INFO); ⑩
    };

    min_app_addr = proc_info.lpMinimumApplicationAddress; ⑪
    max_app_addr = proc_info.lpMaximumApplicationAddress; ⑪

    println!("{} @ {}", this_pid, this_proc);
    println!("{}", proc_info);
    println!("min: {}, max: {}", min_app_addr, max_app_addr);

    loop { ⑫
        let rc: SIZE_T = unsafe {
            kernel32::VirtualQueryEx(
                this_proc, base_addr,
                &mut mem_info, MEMINFO_SIZE as SIZE_T) ⑬
        };
    }
}

```

```

    };

    if rc == 0 {
        break
    }

    println!("{:#?}", mem_info);
    base_addr = ((base_addr as u64) + mem_info.RegionSize) as PVOID;
}
}

```

- ① u32
- ② Pointer types for various internal APIs without an associated type. In Rust, “void pointers” are defined in `std::os::raw::c_void`. A HANDLE is a pointer to some opaque resource within Windows.
- ③ In Windows, data type names are often prefixed with a shorthand for their type. P stands for pointer. LP stands for long pointer, e.g. 64 bit.
- ④ u64 (usize on this machine)
- ⑤ A pointer to a SYSTEM\_INFO struct
- ⑥ Some structs defined by Windows internally
- ⑦ These variables will be initialized from within unsafe blocks. To make them accessible in the outer scope, they need to be defined here.
- ⑧ This block guarantees that all memory is initialized
- ⑨ This block of code is where system calls are made
- ⑩ Rather than use a return value, this function makes use of a C idiom to provide its result to the caller. We provide a pointer to some pre-defined struct, then read that struct’s new values once the function has returned to see the results.
- ⑪ Renaming these variables for convenience.
- ⑫ This loop does the work of scanning through the address space
- ⑬ This system call provides information about a specific segment of the running program’s memory address space, starting at `base_addr`.

Finally we have been able to explore an address space without the operating system killing our program. Now the question remains, how do we inspect individual variables and modify them?

#### 6.4.5 Step 3: reading and writing bytes to processes’ memory

Operating systems provide tools to read and write memory, even in other programs. This is essential for Just-In-Time compilers (JITs), debuggers and programs to help people cheat at games to work.

On Windows, the general process looks something like this in Rust-like pseudo-code:

```

let pid = some_process_id;
OpenProcess(pid);

loop address space {
    call VirtualQueryEx() to access the next memory segment
    scan the segment by calling ReadProcessMemory(), looking for a selected pattern
}

```

```
    call WriteProcessMemory() with the desired value  
}
```

Linux provides an even simpler API via `process_vm_readv()` and `process_vm_writev()`. They're analogous to `ReadProcessMemory()` and `WriteProcessMemory()` in Windows.

## 6.5 Wrap up

Memory management is a complicated area with many levels of abstraction to uncover. This chapter has tried to focus on those elements that are most salient to your work as a programmer. Now when you read your next blog post on some low-level coding technique, you should be much more able to follow along with the terminology.

You have learned:

- What a pointer is and what distinguishes pointers from memory addresses
- What a smart pointer is and that the term has a wider meaning in the Rust community than it does in the C++ community
- That there is a family of smart pointer types that can be used to suit your application's requirements
- That the standard library's smart pointer types are built from building blocks that you can also use to define your own smart pointers if required
- What the heap and stack are
- Why using the stack is faster
- How the memory allocation process operates
- How an operating system, the CPU and the program cooperate to fetch and modify your program's data
- How your program can customize its performance via altering its allocation strategy
- How to trace a program's memory allocations
- What a syscall is and how to make one on Linux and Windows



# 7 *Files & Storage*

## **This chapter covers:**

- Learn how data is represented on physical storage devices
- Write your own data structures to your preferred file format
- Build a tool to read from files and inspect their contents
- Create a working key-value store that's immune from becoming corrupt

Storing data permanently on digital media is trickier than it looks. This chapter takes you through some of that detail. To transfer information held by ephemeral electrical charges in RAM to (semi-)permanent storage media—and then to be able to retrieve it again later—takes several layers of software indirection.

The chapter introduces some new concepts for Rust developers, such as how to structure projects into library crates. This is needed because one of the projects is ambitious. By the end of the chapter, you would have built a working key-value store that's guaranteed to be durable to hardware failure at any stage.

During the chapter, we'll work through a small number of side quests. For example, we implement parity bit checking and explore what it means "to hash" a value. To start with however, let's see if we can create patterns from the raw byte sequence within files.

## **7.1 What is a file format?**

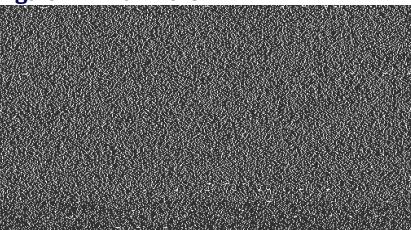
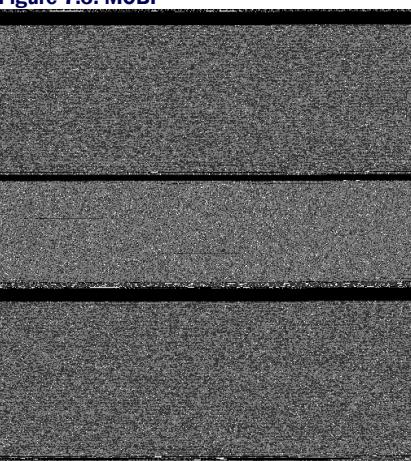
File formats are standards for working with data as a single, ordered sequence of bytes. Storage media, such as hard disk drives, can only work with data in serial. In contrast, data that's accessed purely-in memory is hierarchical. Pointers—which

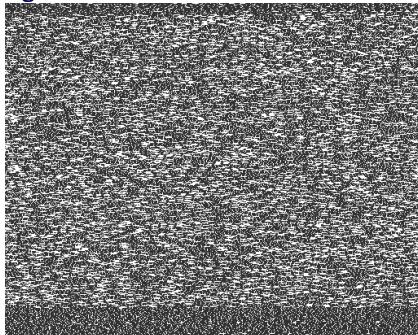
underlie Rust's references—are common and supported by the hardware (the CPU). The CPU doesn't have an intrinsic notion of a allow different components of data structure to live in different regions.

File formats live in a large design space with trade offs in performance, human-readability and portability. Some formats are highly portable and self-describing. Others are restrict themselves a single environment and are unable to be read by third party tools.

Table 7.1 illustrates some of the design space. Each row reveals the file format's internal patterns, which are generated from the same source text. By color-coding each byte within the file, it's possible to see structural differences between each representation.

**Table 7.1. Internals of four digital versions of William Shakespeare's *Much Ado About Nothing* produced by Project Gutenberg.**

<b>Figure 7.1. Plain Text</b> 	<p>The plain text version of the play contains printable characters only. They are indicated by dark grey for letters and punctuation, and white for whitespace. Visually, the image appears to be very noisy. It lacks internal structure. That's due to the variation in length of the natural language that the file is representing. A file with regular, repeating structures, such as a file format designed to hold arrays of floating point numbers, tends to look quite different.</p>
<b>Figure 7.2. EPUB</b> 	<p>The EPUB format is actually a compressed ZIP archive with a bespoke file extension. There are many bytes within the file that fall out of the range of "printable" category , as indicated by the mid-grey pixels.</p>
<b>Figure 7.3. MOBI</b> 	<p>Includes four bands of NUL bytes (0x00), represented as black pixels. These bands probably represent the result of an engineering trade off. In some sense, these empty bytes are wasted space. But they're probably added as padding so that the file's sections are very easy to parse later on.</p> <p>//// None of the three major sections look like they are human readable. As the intended deployment platform is the Amazon Kindle device, that's probably intended. ////</p> <p>The other feature of this file is its size. It's larger than the other versions of the play. That might imply that the file is harboring more data than just the text. Candidates include display elements like fonts through to encryption keys to enforce anti-copying restrictions within the file.</p>

**Figure 7.4. HTML**

The HTML file contains a very high proportion of whitespace characters. They are indicated by white pixels. Markup languages like HTML tend to add whitespace to aid readability.

## 7.2 Creating your own file formats for data storage with `serde`

When working with data that needs to be stored over a long time, the proper thing to do is to use a battle-tested database. Despite this, many systems use plain text files for data storage. Configuration files are common candidates.

The Rust ecosystem has excellent support for converting data to many on-disk formats.

### 7.2.1 Writing data to disk with `serde` & the `bincode` format

`serde` is a crate that `*ser*`ializes and `*de*`serializes Rust values to and from many formats. Each format has its own strengths, many are human-readable, while others prefer to be compact so that they can be speedily sent across the network.

Using `serde` takes surprisingly little ceremony. As an example, let's use `find` statistics about the Nigerian city of Calabar and store them in multiple output formats.

To start, let's assume that our code contains a `City` struct:

```
#[derive(Serialize, Deserialize)]      ①
struct City {
    name: String,
    population: usize,
    latitude: f64,
    longitude: f64,
}
```

- ① The `Serialize` and `Deserialize` traits are provided by the `serde` crate. Most code implements them with this `derive` annotation. They provide the tooling to enable many external formats to interact with Rust code.

Populating that struct with data about Calabar is straightforward:

```
let calabar = City {
    name: String::from("Calabar"),
    population: 470_000,
    latitude: 4.95,
```

```
    longitude: 8.33,  
};
```

Now to convert that calabar variable into JSON, it's one line of code:

```
let as_json = serde_json::to_string(&calabar).unwrap();
```

serde speaks much more than JSON though. The code at Listing 7.3 also provides similar examples for two lesser-known formats, CBOR and bincode. CBOR and bincode are more compact than JSON, at the expense of being machine-readable only. Here is a view of that `calabar` variable in several variants:

**Listing 7.1.** Output of Listing 7.3 demonstrating the different distributions of the bytes present in each format. JSON is readable as-is, but CBOR and bincode contain NUL bytes that require escaping.

To generate that output, compile the code at Listing 7.3 using `serde-eg-toml` as the crate's TOML file.

## **Listing 7.2. Declaring the dependencies and setting other crate metadata for Listing 7.3**

(ch7/ch7-serde-eg/Cargo.toml)

```
[package]
name = "ch7-serde-eg"
version = "0.1.0"
authors = ["Tim McNamara <code@timmcnamara.co.nz>"]

[dependencies]
bincode = "1"
serde = "1"
serde_cbor = "0.8"
serde_derive = "1"
```

```
serde_json = "1"
```

**Listing 7.3. Converting a Rust struct to three different file formats with serde (ch7/ch7-  
serde-eg/src/main.rs)**

```
#[macro_use]
extern crate serde_derive;

extern crate serde;
extern crate serde_cbor;
extern crate serde_json;
extern crate bincode;

#[derive(Serialize, Deserialize)]      ①
struct City {
    name: String,
    population: usize,
    latitude: f64,
    longitude: f64,
}

fn main() {
    let calabar = City {
        name: String::from("Calabar"),
        population: 470_000,
        latitude: 4.95,
        longitude: 8.33,
    };

    let as_json = serde_json::to_string(&calabar).unwrap();          ②
    let as_cbor = serde_cbor::to_vec(&calabar).unwrap();            ②
    let as_bincode = bincode::serialize(&calabar).unwrap();         ②

    println!("json: {}", &as_json);
    println!("cbor: {:?}", &as_cbor);
    println!("cbor (as UTF-8): {:?}", String::from_utf8_lossy(&as_cbor));
    println!("bincode: {:?}", &as_bincode);
    println!("bincode (as UTF-8): {:?}", String::from_utf8_lossy(&as_bincode));
}
```

- ① The `#derive` attribute (`#[derive(Serialize, Deserialize)]`) is added to the `City` struct definition. This instructs the `serde_derive` crate to write the necessary code that will carry out the conversion between an in-memory `City` and an on-disk `City`.
- ② Unfortunately, formats can have differing APIs. Each crate is maintained independently from the `serde` core. In a sense, that's why a library like `serde` is so useful. It provides a common framework for implementing serializers and deserializers for any new format independently from one another.

### 7.3 Implementing a hexdump Clone

A very handy utility for inspecting files' contents is `hexdump`. `hexdump` takes a stream of bytes, often from a file, then outputs those bytes in pairs of hexadecimal numbers. Table 7.2 provides an example. As you'll know from previous chapters, two hexadecimal numbers can represent all digits from 0 to 255, which is the number of bit patterns representable within a single byte. We'll call our clone `fview`, short for file view.

**Table 7.2. `fview` in operation**

<code>fview input</code>	<pre>fn main() {     println!("Hello, world!") }</pre>
<code>fview output</code>	<pre>[0x00000000] 0a 66 6e 20 6d 61 69 6e 28 29 20 7b 0a 20 20 20 [0x00000010] 20 70 72 69 6e 74 6c 6e 21 28 22 48 65 6c 6c 6f [0x00000020] 2c 20 77 6f 72 6c 64 21 29 0a 7d</pre>

Unless you're familiar with hexadecimal notation, the output from `fview` can be fairly opaque. If you're experienced at looking at similar output, you may notice that there are no bytes above `0x7e` (127). There are also very few bytes less than `0x21` (33), with the exception of `0x0a` (10). `0x0a` represents the newline character ('`\n`'). These byte patterns are markers that we're dealing with a plain text input source.

The source code that builds the complete `fview` is provided at Listing 7.5 . Because a few new features of Rust need to be introduced, we'll take a few steps to get to the full program. We'll start with [fview-nofile](#) that uses a string literal as input and produces the output in Table 7.2 .

**Listing 7.4. A hexdump clone with a hard-coded input that mocks file I/O. Demonstrates the use of multi-string literals and importing the `std::io` traits via `std::io::prelude`. This enables `&[u8]` types to be read as files, via the `std::io::Read` trait. (ch7/ch7-fview-str/src/main.rs)**

```
use std::io::prelude::*;

const BYTES_PER_LINE: usize = 16;
const INPUT: &'static [u8] = br#"
fn main() {
    println!("Hello, world!")
}#;

fn main() -> std::io::Result<()> {
    let mut buffer: Vec<u8> = vec!();
    INPUT.read_to_end(&mut buffer)?;                                ③
    ④

    let mut position_in_input = 0;
    for line in buffer.chunks(BYTES_PER_LINE) {                  ⑤
        print!("[0x{:08x}] ", position_in_input);
        for byte in line {
```

```

        print!("{:02x} ", byte);
    }
    println!();                                ⑥
    position_in_input += BYTES_PER_LINE;
}

Ok(())
}

```

- ① The "prelude" imports traits that are heavily used in I/O operations, such as `Read` and `Write`. It's possible to include the traits manually, but they're so common that the standard library provides this convenience line to help keep your code compact.
- ② Multi-line string literals don't need their double-quotes escaped when built with *raw string literals*. Notice the `r` prefix and the `#` delimiters. The additional `b` prefix indicates that this should be treated as bytes (`&[u8]`), not as UTF-8 text (`&str`).
- ③ Make space for the program's input with an internal buffer.
- ④ "Read" our input and insert it into our internal buffer.
- ⑤ Write out the current position with up to 8 left-padded zeros.
- ⑥ Shortcut for printing a newline to stdout.

Now that we have seen the intended operation of `fview`, let's extend its capabilities to read real files.

**Listing 7.5. A basic hexdump clone that demonstrates how to open a file in Rust and iterate through its contents (ch7/ch7-fview/src/main.rs)**

```

use std::fs::File;                                ①
use std::io::prelude::*;

const BYTES_PER_LINE: usize = 16;                  ④

fn main() {
    let arg1 = env::args().nth(1);                  ⑤
    let fname = arg1.expect("usage: fview FILENAME"); ⑥

    let mut f = File::open(&fname).expect("Unable to open file."); ⑦
    let mut pos = 0;
    let mut buffer = [0; BYTES_PER_LINE];

    while let Ok(_) = f.read_exact(&mut buffer) {      ⑧
        print!("[0x{:08x}] ", pos);
        for byte in &buffer {
            match *byte {
                0x00 => print!("."),
                0xff => print!("## "),
                _ => print!("{:02x} ", byte),
            }
        }
    }
}

```

```

        println!("");
        pos += BYTES_PER_LINE;
    }
}

```

- ① Import the standard library's `File` type into local scope
- ② The prelude imports lots of common functionality for convenience.
- ③ `std::env` provides fairly low-level access to the program's environment. We're not building a complicated app, so we don't need to worry about anything more fully-featured.
- ④ Changing this constant can change the effects that are generated by the program.
- ⑤ Rust iterators provide a `nth()` method that allows you to extract single values. Using to extract an argument from `env::args()` means that the argument won't be validated, but that will suffice for now.
- ⑥ Using `nth()` does however incur some cost: it mandates that you consider an error case. It returns a `Result`. `expect()` prints the usage error message is printed to the screen when there are no command-line arguments provided or some other issue arises.
- ⑦ The calls to `expect()` should be considered a friendlier version of `unwrap()`. `unwrap()` panics abruptly on error. `expect()` panics with an error message.
- ⑧ Rather than calling `chunks()` on the input iterator, we explicitly provide a buffer to fill to `read_exact()`.

Listing 7.5 introduces from new Rust:

- `while let Ok(_) { ... }` is a control flow structure. The program will continue to loop until `f.read_exact()` returns `Err`, which occurs when it has run out of bytes to read.
- `f.read_exact()` comes from the `Read` trait. The method transfers data from the source, in our case `f`, to the buffer provided as an argument and stops when that buffer is full. It provides greater control to you as a programmer for managing memory, than the `chunks()` option used in Listing 7.4 but does come with some quirks. If the buffer is longer than the number of available bytes to read, the file will return an error and the state of the buffer is undefined.'

## 7.4 File operations in Rust

So far in this chapter, we have invested a lot of time considering how data is translated into sequences of bytes. Let's spend some time considering another level of abstraction, the file.

Previous chapters have covered basic operations, such as opening and reading from a file. This section contains some other helpful techniques, which provide more granular control.

### 7.4.1 Opening a file in Rust and controlling its file mode

Files are an abstraction that's maintained by the operating system. It presents a façade of names and hierarchy above a nest of raw bytes.

Files also provide a layer of security. They have permissions attached to them that the

operating system will enforce. This—in principle, at least—is what prevents a web server running under its own user account from reading files owned by others.

`std::fs::File` is the primary type for interacting with the file system. There are two default methods available for creating a

**Table 7.3. Creating File values in Rust code and their effects on the underlying file system**

Method	Return value when the file already exists	Effect on underlying file	Return value when no file exists
<code>File::open</code>	<code>Ok(File)*</code>	Opened in read-only mode, as is	<code>Err</code>
<code>File::create</code>	<code>Ok(File)*</code>	All existing bytes are truncated, and the file is opened at	<code>Ok(File)*</code>

\* Assuming the user account has sufficient permission.

When more control over is required over the file mode, `std::fs::OpenOptions` is available. It provides the necessary knobs to turn for any intended application. Listing 7.19 provides a good example of a case where an “append” mode is requested. The application requires writeable file that is also readable and will be created if it doesn’t already exist.

**Listing 7.6. Excerpt of Listing 7.19 demonstrating the use of `std::fs::OpenOptions` to create an writeable file that will not be truncated when it’s opened**

```
let f = OpenOptions::new()
    .read(true)          ①
    .write(true)         ②
    .create(true)        ③
    .append(true)        ④
    .open(path)?;        ⑤
                        ⑥
```

- ① An example of the “Builder” pattern. Each method returns a new instance of the `OpenOptions` struct with the relevant option set.
- ② Open the file for reading
- ③ Enable writing. This line is not strictly necessary, as it’s implied by `append`.
- ④ Create a file at `path` if it doesn’t already exist
- ⑤ Don’t delete any content that’s already been written to disk.
- ⑥ Open the file at `path` after unwrapping the intermediate `Result`

#### **7.4.2 Interacting with the file system in a type-safe manner with `std::fs::Path`**

Rust provides type-safe variant of `str` and `String` in its standard library: `std::path::Path` and `std::path::PathBuf`. They can be used to unambiguously work with path separators in a cross-platform way. `Path` can address

files, directories and related abstractions, such as symbolic links.

Creating one is relatively straight-forward:

```
let hello = PathBuf::from("/tmp/hello.txt")
```

From there, interacting with them reveals methods that specific to paths:

```
hello.extension() ①
```

① Returns Some("txt")

The full API is straight-forward for anyone who has used code to manipulate paths with code before, so it won't be fleshed out here. Still, it may be worth discussing why it's included within the language as many languages omit this.

#### TIP

As an implementation detail, `std::fs::Path` and `std::fs::PathBuf` are implemented on top of `std::ffi::OsStr` and `std::ffi::OsString` respectively. This means that `Path` and `PathBuf` are not guaranteed to be UTF-8.

Why use `Path`, rather than manipulating strings directly?

#### Clearer intent

`Path` provides useful methods, such as `set_extension()` that describe the intended outcome. This can assist programmers who later read the code. Manipulating strings manner doesn't provide that level of self-documentation.

#### Portability

Some operating systems treat file system paths as case insensitive. Others don't. Using one operating system's conventions may result in issues later on when users end up expecting their host system's conventions will be followed. Additionally, path separators are specific to operating systems and thus can differ. This means that using raw strings can lead to portability issues. Comparisons require exact matches.

#### Easier debugging

If you're attempting to extract `/tmp` from the path `/tmp/hello.txt`, doing it manually can introduce subtle bugs that may only appear at runtime. Mis-counting the correct number index values after splitting the string on `/` introduces a bug that can't be caught at compile time.

To illustrate the subtle errors, consider the case of separators. Slashes are common in today's operating systems, but those conventions took some time to become established.

- `\` is commonly used on MS Windows
- `/` is the convention for UNIX-like operating systems
- `:` was the path separator of the classic Mac OS

- → is used in the Stratus VOC operating system

**Table 7.4. Comparing std::String and std::path::Path to extract a file's parent directory**

<pre>fn main() {     let hello = String::from("/tmp/hello.txt");     let tmp_dir = hello.split("/").nth(0);     println!("{}:", tmp_dir); }</pre>	<pre>use std::path::PathBuf;  fn main() {     let mut hello = PathBuf::from("/tmp/hello.txt");     hello.pop();                                ①     println!("{}:", hello.display());            ② }</pre>
<p>① Split hello at its backslashes, then take the zeroith element of the resulting Vec&lt;String&gt;</p> <p>② Mistake! Prints Some("") .</p>	<p>① Truncates hello in place</p> <p>② Success! Prints "/tmp".</p>
<p>The plain String code enables you to use familiar methods, but can introduce subtle bugs that are difficult to detect at compile time. In this instance, we've used the wrong index number to access the parent directory (/tmp).</p>	<p>Using path::Path does not make your code immune to subtle errors, but can certainly help to minimize their likelihood. Path provides dedicated methods for common operations, such as setting a file's extension.</p>

## 7.5 Implementing a key-value store with a log-structured, append-only storage architecture

It's time to tackle something larger. Let's begin to lift the lid on database technology.

Along the way, we'll learn the internal architecture of a family of database systems using the "log-structured, append-only" model. They're significant as case studies because they are both designed for extremely high resilience and high performance. Despite storing data on fickle media such as flash storage or a spinning hard disk drive, databases using this model are able to guarantee that a) data will never be lost and b) that their backing data files will never be corrupted.

### 7.5.1 The key-value model

actionkv is a *key-value store*. That means that it can store and retrieve sequences bytes ([u8]) of arbitrary length. Each sequence has two parts. The first is a key, and the second is a value. As the &str type is represented as [u8] internally, Table 7.5 uses the plain text notation, rather than the binary equivalent that's used prominently earlier in "[Writing data to disk with serde & the bincode format](#)".

**Table 7.5. Illustrating keys and values by matching countries with their capital cities**

Key	Value
"Cook Islands"	"Avarua"
"Fiji"	"Suva"
"Kiribati"	"South Tarawa"
"Niue"	"Alofi"

The key-value model enables simple queries such as "what is the capital city of Fiji?" but doesn't support asking broader queries, such as "what is the list of capital cities for all Pacific Island states?".

## 7.5.2 Introducing actionkv v0.1: an in-memory key-value store with a command line interface

The first version of our key-value store, `actionkv` exposes us to the API that we'll use and introduces the main library code. The library code won't change, as the subsequent two systems are built on top of it. Before we get to that code though, there are some pre-requisites that need to be covered.

Unlike other projects in this book, this one uses the "library" template to start with (`cargo new --lib actionkv`) It has the following structure:

```
actionkv
└── src
    └── akv_mem.rs
    └── lib.rs
└── Cargo.toml
```

Using a library crate allows programmers to build re-usable abstractions within their projects. For our purposes, we'll use the same `lib.rs` for multiple executables.

This means that we declare the location of executable binaries produced by the project by providing a section within the project's `Cargo.toml` file. See

**Listing 7.7. Defining dependencies and other metadata (ch7/ch7-actionkv1/Cargo.toml)**

```
[package]
name = "actionkv"
version = "0.1.0"
authors = ["Tim McNamara <code@timmcnamara.co.nz>"]

[dependencies]
byteorder = "1.2"          ①
crc = "1.7"                ②

[lib]                      ③
name = "libactionkv"        ③
path = "src/lib.rs"         ③

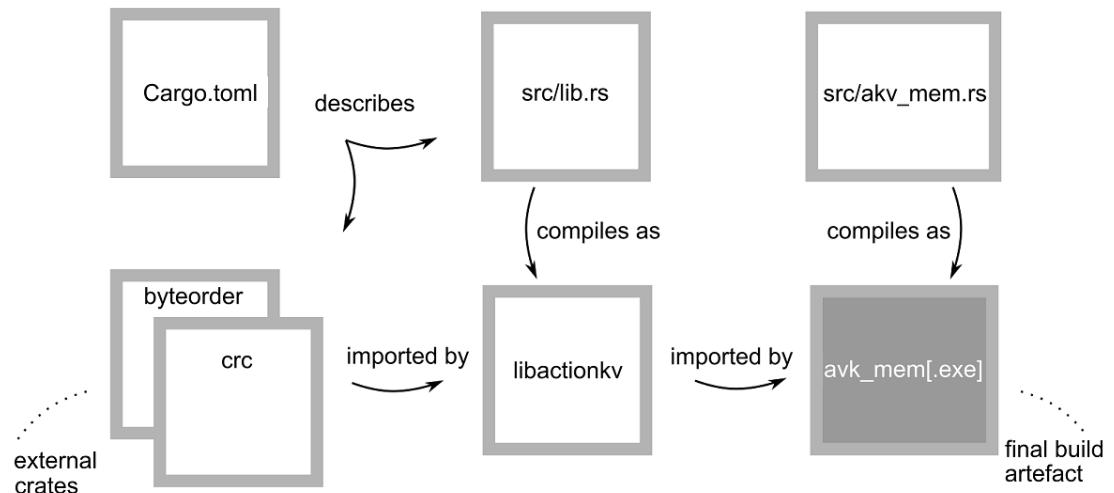
[[bin]]                    ④
name = "akv_mem"
path = "src/akv_mem.rs"
```

- ① The `byteorder` crate extends many Rust types with extra traits that enable them to be written to disk and read back into a program in a repeatable, easy-to-use way
- ② The `crc` crate provides the checksum functionality that we want to include
- ③ A `[lib]` section of `Cargo.toml` lets you define your own name for the library that you're building. A crate may only have one library.

- ④ A `pass: [[ [bin]]]` section—of which there may be many—of `Cargo.toml` defines an executable file that will be built from this crate. The double-square bracket syntax (`pass: [[[]]]`) is required because it unambiguously describes `bin` as being part of 1 or more elements.

The project will end up with several files. Figure 7.5 illustrates the relationships and how they work together to build the `akv_mem` executable that's referred to within the `[[bin]]` section of the project's `Cargo.toml` file.

**Figure 7.5. An outline of how the different files within the ActionKV project and their dependencies work together. The project's `Cargo.toml` coordinates lots of activity that will ultimately result in an executable being built.**



## 7.6 `actionkv v0.1 front-end code`

The public API of `actionkv` is comprised of four operations: “get”, “delete”, “insert” and “update”.

**Table 7.6. Operations supported by `actionkv`**

Command	Description
<code>get &lt;key&gt;</code>	retrieves the value at key from the store
<code>insert &lt;key&gt; &lt;value&gt;</code>	adds a key/value pair to the store
<code>delete &lt;key&gt;</code>	removes a key/value pair from the store
<code>update &lt;key&gt; &lt;value&gt;</code>	replace an old value with a new one

### Naming is difficult

To access stored key-value pairs, should the API provide “get”, “retrieve” or perhaps “fetch”? Should setting values be “insert”, “store” or “set”?

actionkv to say neutral to these decisions by deferring to the API provided by std::collections::HashMap.

We use Rust’s matching facilities to efficiently work with the command-line arguments and dispatch to the correct internal function:

#### **Listing 7.8. Excerpt from Listing 7.9 demonstrating the public API**

```

match action {
    "get" => {
        match store.get(key).unwrap() {
            None => eprintln!("{} not found", key),
            Some(value) => println!("{}: {}", key, value),      ②
        }
    },
    "delete" => store.delete(key).unwrap(),
    "insert" => {
        let value = maybe_value.expect(&USAGE).as_ref();      ③
        store.insert(key, value).unwrap()
    },
    "update" => {
        let value = maybe_value.expect(&USAGE).as_ref();
        store.update(key, value).unwrap()
    },
    _ => eprintln!("{}: {}", key, &USAGE),
}

```

- ① action is a command-line argument, and has the type &str
- ② println! needs to use Debug syntax ({:?}) as [u8] is arbitrary bytes and therefore does not implement Display.
- ③ A future update that could be added for compatibility with Rust’s HashMap would be for insert to return the old value, if it exists

In full, the code for actionkv v0.1 is presented as Listing 7.9 . Notice that the heavy lifting of interacting with the file system is delegated to an instance of ActionKV called store. How ActionKVoperates is explained in [“Understanding the core of actionkv: the libactionkv crate”](#).

#### **Listing 7.9. In-memory key-value store command line application (ch7/ch7-actionkv1/src/akv\_mem.rs)**

```

extern crate libactionkv;                      ①
use libactionkv::ActionKV;                     ①

```

```

#[cfg(target_os = "windows")]
const USAGE: &'static str = "
Usage:
    akv_mem.exe FILE get KEY
    akv_mem.exe FILE delete KEY
    akv_mem.exe FILE insert KEY VALUE
    akv_mem.exe FILE update KEY VALUE
";

#[cfg(not(target_os = "windows"))]
const USAGE: &'static str = "
Usage:
    akv_mem FILE get KEY
    akv_mem FILE delete KEY
    akv_mem FILE insert KEY VALUE
    akv_mem FILE update KEY VALUE
";

fn main() {
    let args: Vec<String> = std::env::args().collect();
    let fname = args.get(1).expect(&USAGE);
    let action = args.get(2).expect(&USAGE).as_ref();
    let key = args.get(3).expect(&USAGE).as_ref();
    let maybe_value = args.get(4);

    let path = std::path::Path::new(&fname);
    let mut store = ActionKV::open(path).expect("unable to open file");
    store.load().expect("unable to load data");

    match action {
        "get" => {
            match store.get(key).unwrap() {
                None => eprintln!("{} not found", key),
                Some(value) => println!("{}: {}", key, value),
            }
        },
        "delete" => store.delete(key).unwrap(),
        "insert" => {
            let value = maybe_value.expect(&USAGE).as_ref();
            store.insert(key, value).unwrap()
        },
        "update" => {
            let value = maybe_value.expect(&USAGE).as_ref();
            store.update(key, value).unwrap()
        },
        _ => eprintln!("{}: {}", &USAGE),
    }
}

```

- ① Although `src/lib.rs` exists within our project, it's treated the same as any other crate within our project's `src/bin.rs` file

- ② The `cfg` attribute allows MS Windows users will see the correct file extension in their help documentation. This attribute is explained at [“Tailoring what is compiled with conditional compilation”](#).

### 7.6.1 Tailoring what is compiled with conditional compilation

Rust provides excellent facilities for altering what is compiled depending on the *compiler target architecture*. Generally, this is the target’s operating system, but may be facilities provided by its CPU. Changing what is compiled depending on some compile-time condition is known as *conditional compilation*.

To add conditional compilation to your project, annotate your source code with `cfg` attributes. `crg` works in conjunction with the `target` parameter provided to `rustc` during compilation.

Listing 7.9 provides a usage string—common as quick documentation for command-line utilities—for multiple operating systems. It’s replicated here. When the project is built for Windows, the usage string contains a `.exe` file extension. The resulting binary files only include the data that is relevant for their target.

**Listing 7.10. Excerpt from Listing 7.9 demonstrating the use of conditional compilation to provide two definitions of `const USAGE` in the source code**

```
#[cfg(target_os = "windows")]
const USAGE: &'static str = "
Usage:
    akv_mem.exe FILE get KEY
    akv_mem.exe FILE delete KEY
    akv_mem.exe FILE insert KEY VALUE
    akv_mem.exe FILE update KEY VALUE
";

#[cfg(not(target_os = "windows"))]
const USAGE: &'static str = "
Usage:
    akv_mem FILE get KEY
    akv_mem FILE delete KEY
    akv_mem FILE insert KEY VALUE
    akv_mem FILE update KEY VALUE
";
```

There is no negation operator for these matches. That is, `#[cfg(target_os != "windows")]` does not work. Instead, there is a function-like syntax for specifying matches. Use `#[cfg(not(...))]` for negation. `#[cfg(all(...))]` and `#[cfg(any(...))]` are also available to match on elements of a list.

The list of conditions that may trigger compilation changes is extensive:

**Table 7.7. Options available to match against in cfg attributes**

Attribute	Valid options	Notes
target_arch	"aarch64" "arm" "mips" "powerpc" "powerpc64" "x86" "x86_64"	Not an exclusive list of options.
target_os	"android" "bitrig" "dragonfly" "freebsd" "haiku" "ios" "linux" "macos" "netbsd" "redox" "openbsd" "windows"	Not an exclusive list of options.
target_family	"unix" "windows"	
target_env	"" "gnu" "msvc" "musl"	This will often be an empty string ("").
target_endian	"big" "little"	Useful for when bit-shifting operators such as << and & are used in code to prevent unintentional errors.
target_pointer_width	"32" "64"	The size (in bits) of the target architecture's pointer size. Used for <code>isize</code> , <code>usize</code> * <code>const</code> and * <code>mut</code> types.
target_has_atomic	"8" "16" "32" "64" "ptr"	Integer sizes that have support for atomic operations. See chapter XX for an overview.
target_vendor	"apple" "pc" "unknown"	
test		No options, just uses a simple Boolean check
debug_assertions		No options, just uses a simple Boolean check. This attribute is present for non-optimized builds and supports the <code>debug_assert!</code> macro.

Lastly, it's possible to tweak `cfg` attributes when invoking `cargo/rustc` via the `--cfg ATTRIBUTE command-line argument.`

## 7.7 ***Understanding the core of actionkv: the libactionkv crate***

The command line application built in [“actionkv v0.1 front-end code”](#) dispatches its work to `libactionkv::ActionKV`. The responsibilities of the `ActionKV` struct are a) to manage interactions with the file system and b) to encode and decode data from the on-disk format.

**Figure 7.6. Relationship between libactionkv and other components of the project**



### 7.7.1 Initializing the ActionKV struct

To create an instance of `libactionkv::ActionKV`, there are two steps: 1) pointing to the file where the data is stored and 2) loading an in-memory index from the data within that file.

#### Listing 7.11. Excerpt of Listing 7.9 demonstrating the initialization process

`of libactionkv::ActionKV`

```
let mut store = ActionKV::open(path).expect("unable to open file");      ①
store.load().expect("unable to load data");    ②
```

① Step 1: open the file at path

② Step 2: create an in-memory index by loading the data from path

Both steps return `Result`, which is why the calls to `.expect()` are also present.

Let's look inside the code of `ActionKV::open()` and `ActionKV::load()`. `open()` opens the file from disk, `load()` loads the offsets of any pre-existing data into an in-memory index.

The code uses two type aliases, `ByteStr` and `ByteString`:

```
type ByteStr = [u8];
```

We'll use the `ByteStr` type alias for data that tends to be used as a string, but happens to be in a binary (raw bytes) form. Its text-based peer is the built-in `str`. Both `str` and `ByteStr` are seen in the wild as `&str` and `&ByteStr` are they are both slices.

```
pass:[type ByteString = Vec<u8>;]
```

The alias `ByteString` will be the workhorse used when we want to use a type that behaves like a `String`, but is binary data.

#### **Listing 7.12. Excerpt from Listing 7.19 demonstrating the use of `ActionKV::open()`**

```
type ByteString = Vec<u8>;                                ①
type ByteStr = [u8];                                     ②

#[derive(Debug, Serialize, Deserialize)]                  ③
pub struct KeyValuePair {
    pub key: ByteString,
    pub value: ByteString,
}

#[derive(Debug)]
pub struct ActionKV {
    f: File,
    pub index: HashMap<ByteString, u64>,                ④
}

impl ActionKV {
    pub fn open(path: &Path) -> io::Result<Self> {
        let f = OpenOptions::new()
            .read(true)
            .write(true)
            .create(true)
            .append(true)
            .open(path)?;
        Ok(ActionKV { f: f, index: HashMap::new() })
    }

    pub fn load(&mut self) -> io::Result<()> {
        let mut f = BufReader::new(&mut self.f);

        loop {
```

```

        let current_position = f.seek(SeekFrom::Current(0))?;

        let maybe_kv = ActionKV::process_record(&mut f);
        let kv = match maybe_kv {
            Ok(kv) => kv,
            Err(err) => {
                match err.kind() {
                    io::ErrorKind::UnexpectedEof => {
                        break;
                    },
                    _ => return Err(err),
                }
            },
        };

        self.index.insert(kv.key, current_position);
    }

    Ok(())
}

```

- ① This code will be processing lots of `Vec<u8>` data. Because they'll be used in the same way as `String` tends to be used, `ByteString` is a useful alias.
- ② `ByteStr` is to `&str` what `ByteString` is to `Vec<u8>`
- ③ `Serialize` and `Deserialize` are explained later in the chapter at ["Writing data to disk with serde & the bincode format"](#). They instruct the compiler to generate `serialization` code to enable writing `KeyValuePair` data to disk via.
- ④ Maintains a mapping between keys and file locations.
- ⑤ The role of the `ActionKV::load()` method is to populate the index of the `ActionKV` struct, mapping keys to file positions
- ⑥ We use the `File::seek()` method to return the number of bytes from the start of the file. This becomes the value of the index.
- ⑦ `ActionKV::process_record()` reads a record in the file at its current position
- ⑧ "Unexpected" is relative. The application may not have expect to encounter the end of the file, but we expect files to be finite and so we deal with that eventuality.

## What is EOF?

File operations in Rust might return an error of type `std::io::ErrorKind::UnexpectedEof`. What is "Eof"?

End of File (EOF) is a *convention* that operating systems provide to applications. There is no special marker or delimiter at the end of a file, within the file itself.

EOF is a zero byte (`0u8`). When reading from a file, the operating system tells the application how many bytes were successfully read from storage. If no bytes were successfully read from disk, yet no error condition was detected, then the operating system and therefore the application assume that EOF has been reached.

This works because the operating system has the responsibility for interacting with physical devices. When a file is read by an application, the application notifies the operating system that it would like to access the disk.

### **7.7.2 Processing an individual record**

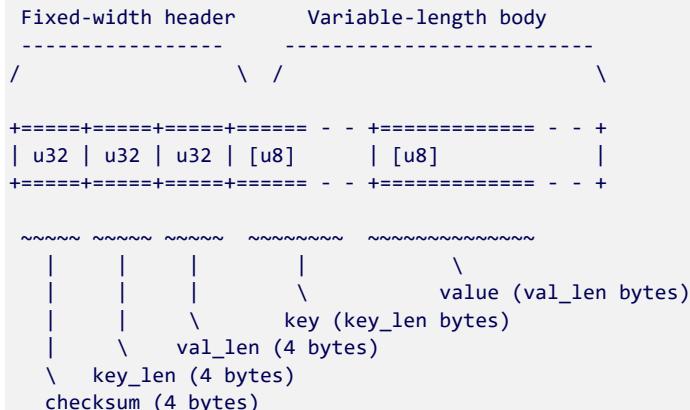
`actionkv` uses a published standard for its on-disk representation. It is an implementation of the "Bitcast" storage backend that was developed for the original implementation of the Riak database. "Bitcast" belongs to a family of file formats known in the literature as "Log-Structured Hash Tables".

## **What is "Riak"?**

Riak is a database. It was developed during the height of the NoSQL movement and competed against similar systems MongoDB, Apache CouchDB and Toyko Tyrant. It distinguished itself with its emphasis on resilience to failure. Although it was slower than its peers, it made a guarantee that it will never lose data. That guarantee was enabled in part because of its smart choice of data format.

Bitcast lays every record in a prescribed manner:

**Listing 7.13.** Illustration of a single record in the the Bitcast file format. To parse a record, read the header information, then use that information to read the body. Lastly verify the body's contents with the checksum provided in the header.



Every key-value pair is prefixed by 12 bytes. Those bytes describe its length (key len + val len) and its content (checksum)

`process_record()` is the function that does the processing for this within `actionkv`. It begins by reading twelve bytes that represent three integers: a checksum, the length of the key and the length of the value. Those values are then used to read the rest of the data from disk and verify that is what's intended.

**Listing 7.14. Extract from 7.19 focusing on the ActionKV::process\_record() method**

```
fn process_record<R: Read>(f: &mut R) -> io::Result<KeyValuePair> {  
    let saved_checksum = f.read_u32::<LittleEndian>()?;
    let key_len = f.read_u32::<LittleEndian>()?;
    (1)  
    (2)  
    (2)
```

```

let val_len = f.read_u32::<LittleEndian>()?;
let data_len = key_len + val_len;                                ②

let mut data = ByteString::with_capacity(data_len as usize);

{
    f.by_ref()                                                 ③
        .take(data_len as u64)
        .read_to_end(&mut data)?;
}

debug_assert_eq!(data.len(), data_len as usize);                  ④

let checksum = crc32::checksum_ieee(&data);
if checksum != saved_checksum {                                    ⑤
    panic!("data corruption encountered ({:08x} != {:08x})", checksum,
           saved_checksum);
}

let val = data.split_off(key_len as usize);                        ⑥
let key = data;

Ok( KeyValuePair { key: key, value: val } )
}

```

- ① The `f` argument accepts any type that implements `Read`. This is generally expected to be files, but `&[u8]` is another type that's acceptable here.
- ② The `byteorder` crate allows on-disk integers to be read in a deterministic manner, as discussed at [“Writing multi-byte binary data to disk in a guaranteed byte order”](#).
- ③ `f.by_ref()` is required because `take(n)` creates a new `Read` value. Using a reference within this short-lived block allows us to sidestep ownership issues.
- ④ `debug_assert!` tests are disabled in optimized builds, enabling debug builds to have more runtime checks.
- ⑤ A “checksum” is a number that can be used to verify that the bytes read from disk are the same as what was intended. This process is discussed at [“Validating I/O errors with checksums”](#).
- ⑥ The `split_off(n)` method splits a `Vec<T>` in two at `n`.

### 7.7.3 Writing multi-byte binary data to disk in a guaranteed byte order

One challenge that our code faces is that it needs to be able to store multi-byte data to disk in a deterministic way. This sounds easy, but computing platforms differ as to how they read numbers. Some read the four bytes of an `i32` from left-to-right, others read right-to-left. That could potentially be a problem if the program is designed to be written by one computer and loaded by another.

The Rust ecosystem provides some support here to minimize the chance of getting things wrong via the `byteorder` crate. `byteorder` takes care of the heavy lifting by extending types that implement the standard library’s `Read` and `Write` traits. `Read` and `Write` are the main traits related to file I/O operations. They’re most commonly associated with `std::io::File`, but are also implemented by other types, such as `[u8]`.

To follow what's going on with our key-value store code at `akv_mem`, it will help to have an understanding how of `byteorder` works. Listing 7.16 is a toy application that demonstrates the core functionality. Lines 11-23 show how to write to a file and lines 28-35 show how to read from one.

The two key lines are:

```
use byteorder::{LittleEndian};
use byteorder::{ReadBytesExt, WriteBytesExt};
```

`byteorder::littleEndian`—and its peers `BigEndian` and `NativeEndian` that are not used in Listing 7.16—are types that declare how multi-byte data is written to and read to disk. `byteorder::ReadBytesExt` and `byteorder::WriteBytesExt` are traits. In some sense, they're invisible within the code. They add methods to primitive types, such as `f32` and `i16`, but there is no “ignition” or “activate” syntax that. Bringing them into scope with a `use` statement immediately adds powers to the types that are implemented within the source of `byteorder`. In practice, that means primitive types. Rust, as a statically-typed language, makes this transformation at compile-time. From the running program's point of view, integers always had the ability to write themselves to disk in a pre-defined order.

When executed, Listing 7.16 produces a visualisation of the byte patterns that are created by writing `1_u32`, `2_i8` and `3.0_f32` out in little-endian order:

```
[1, 0, 0, 0]
[1, 0, 0, 0, 2]
[1, 0, 0, 0, 2, 0, 0, 0, 0, 0, 0, 8, 64]
```

#### Listing 7.15. Metadata for the project at Listing 7.16 (ch7/ch7-write123/Cargo.toml)

```
[package]
name = "write123"
version = "0.1.0"
authors = ["Tim McNamara <code@timmcnamara.co.nz>"]

[dependencies]
byteorder = "1.2"
```

#### Listing 7.16. Writing integers to disk (ch7/ch7-write123/src/main.rs)

```
extern crate byteorder;

use std::io::Cursor;
use byteorder::{LittleEndian}; ①
use byteorder::{ReadBytesExt, WriteBytesExt}; ② ③

fn write_numbers_to_file() -> (u32, i8, f64) {
    let mut w = vec![]; ④

    let one: u32    = 1;
```

```

let two: i8    = 2;
let three: f64 = 3.0;

w.write_u32::<LittleEndian>(one).unwrap();          ⑤
println!("{:?}", &w);

w.write_i8(two).unwrap();                           ⑥
println!("{:?}", &w);

w.write_f64::<LittleEndian>(three).unwrap();          ⑤
println!("{:?}", &w);

(one, two, three)
}

fn read_numbers_from_file() -> (u32, i8, f64) {
    let mut r = Cursor::new(vec![1, 0, 0, 0, 2, 0, 0, 0, 0, 0, 0, 8, 64]);      ⑧
    let one_ = r.read_u32::<LittleEndian>().unwrap();
    let two_ = r.read_i8().unwrap();
    let three_ = r.read_f64::<LittleEndian>().unwrap();

    (one_, two_, three_)
}

fn main() {
    let (one, two, three) = write_numbers_to_file();
    let (one_, two_, three_) = read_numbers_from_file();

    assert_eq!(one, one_);
    assert_eq!(two, two_);
    assert_eq!(three, three_);
}

```

- ① As files support the ability to seek(), that is to move backwards and forwards to different positions, something is necessary to enable a `Vec<T>` to mock being a file. `io::Cursor` plays that role, enabling an in-memory `Vec<T>` to be file-like.
- ② Used as a type argument for various `read_*`() and `write_*`() methods that are used in the program.
- ③ Traits that provide `read_*`() and `write_*`()
- ④ The variable name `w` stands for “writer”
- ⑤ Write values “to disk”. These methods return `io::Result`, which we swallow here as they won’t fail unless something is seriously wrong with the computer that is running the program.
- ⑥ Single byte types `i8` and `u8` don’t take an endianness parameter

#### 7.7.4 Validating I/O errors with checksums

`actionkv` has no method of validating what it has read from disk is what was written to disk. Perhaps something was interrupted during the original write? While we may not be able to recover the original data if this were the case, if we could recognize the issue then we would be in a position to alert the user.

A well-worn path to overcome this problem is to use a technique called a *checksum*.

Here's how it works:

### Saving to disk

- Before data is written to disk, a checking function (there are many options as to which function) is applied to those bytes
- The result of the checking function (the checksum) is written alongside the original data.

No checksum is calculated for the bytes of the checksum. If something breaks while writing the checksum's own bytes to disk, this will also be noticed later on as an error.

### Reading from disk

- Read the data and the saved checksum.
- Apply the checking function to the data.
- Compare the results of the two checking functions. If the two results do not match, an error must have occurred and the data should be considered corrupted.

Which checking function should you use? Like many things in computer science, it depends. An ideal checksum function would a) return the same result for the same input, b) always return a different result for different inputs, c) be fast and d) be easy to implement.

**Table 7.8. A simplistic evaluation of different checksum functions**

Checksum Technique	Size of Result	Simplicity	Speed	Reliability
Parity bit	1 bit	★★★★★	★★★★★	★★☆☆☆
CRC32	32 bits	★★★★☆☆	★★★★☆	★★★☆☆
cryptographic hash function	128-512 bits (or more)	★☆☆☆☆☆	★☆☆☆☆	★★★★★

Functions that you might see in the wild will depend on your application domain. More traditional areas might see the use of simpler systems, such as “parity bit” or “CRC32”.

- The parity bit is easy and fast, but is somewhat prone to error.
- CRC32 (cyclic redundancy check, returning 32 bits) is much more complex, but its results are more trustworthy.
- Cryptographic hash functions are much more complex still while also being significantly slower, yet provide very high levels of assurance.

### IMPLEMENTING PARITY BIT CHECKING

This section here implements one of the simpler checksum schemes: parity checking. Parity checks count the number of 1s within a bitstream. They store a bit that indicates whether the count was even or odd.

Parity bits have traditionally been used for error detection within noisy communication systems, such as transmitting data over analog systems such as radio waves. For example, the ASCII encoding of text has a particular property that makes it quite

convenient for this scheme. Its 128 only require 7 bits of storage ( $128 = 2^7$ ). That leaves one bit spare in every byte.

Systems can also include parity bits in larger streams of bytes. Listing 7.18 presents (an overly chatty) implementation. The `parity_bit()` function in lines 1-10 that takes an arbitrary stream of bytes and returns a `u8` indicating whether the count of the input's bits was even or odd.

When executed, Listing 7.18 produces the following output:

#### Listing 7.17. Output from Listing 7.18

```
input: [97, 98, 99]          ①
97 (0b01100001) has 3 one bits
98 (0b01100010) has 3 one bits
99 (0b01100011) has 4 one bits
output: 00000001

input: [97, 98, 99, 100]      ②
97 (0b01100001) has 3 one bits
98 (0b01100010) has 3 one bits
99 (0b01100011) has 4 one bits
100 (0b01100100) has 3 one bits
result: 00000000
```

① `[97, 98, 99]` represents `b"abc"` as seen by the internals of the Rust compiler.

② `[97, 98, 99, 100]` represents `b"abcd"`

#### Listing 7.18. Implementing parity bit checking (ch7/ch7-paritybit/src/main.rs)

```
fn parity_bit(bytes: &[u8]) -> u8 {                                ①
    let mut n_ones: u32 = 0;

    for byte in bytes {
        let ones = byte.count_ones();                                ②
        n_ones += ones;
        println!("{} (0b{:08b}) has {} one bits", byte, byte, ones);
    }
    (n_ones % 2 == 0) as u8                                       ③
}

fn main() {
    let abc = b"abc";
    println!("input: {:?}", abc);
    println!("output: {:08x}", parity_bit(abc));
    println!();
    let abcd = b"abcd";
    println!("input: {:?}", abcd);
    println!("result: {:08x}", parity_bit(abcd))
}
```

- ① Take a byte slice as argument bytes and return a single byte as output. This function could have easily returned a bool value, but returning u8 allows the result to be shifted into some future desired position later on.
- ② All of Rust's integer types come equipped with count\_ones() and count\_zeros() methods.
- ③ There are plenty of methods to optimize this function. One fairly simple approach would be to hard code a const [u8; 256] array of zeros and ones corresponding to the intended result, then index that array with each byte.

### 7.7.5 Inserting a new key-value pair into an existing database

As discussed during [“actionkv v0.1 front-end code”](#), there are four operations that our code needs to support: insert, get, update and delete. We’re using an append-only design, which means that the last two can be implemented as variants of insert. You may have noticed that during load(), the inner loop continues until the end of the file. This allows more-recent updates to overwrite stale data, including deletions.

Inserting a new record is almost the inverse of process\_record() described at [“Processing an individual record”](#).

```
pub fn insert(&mut self, key: &ByteStr, value: &ByteStr) -> io::Result<()> {
    let position = self.insert_but_ignore_index(key, value)?;

    self.index.insert(key.to_vec(), position);                                ①
    Ok(())
}

pub fn insert_but_ignore_index(&mut self, key: &ByteStr, value: &ByteStr) ->
io::Result<u64> {
    let mut f = BufWriter::new(&mut self.f);                                ②

    let key_len = key.len();
    let val_len = value.len();
    let mut tmp = ByteString::with_capacity(key_len + val_len);

    for byte in key {                                                        ③
        tmp.push(*byte);
    }

    for byte in value {                                                     ③
        tmp.push(*byte);
    }

    let checksum = crc32::checksum_ieee(&tmp);                                ③

    let next_byte = SeekFrom::End(0);
    let current_position = f.seek(SeekFrom::Current(0))?;
    f.seek(next_byte)?;
    f.write_u32::<LittleEndian>(checksum)?;
    f.write_u32::<LittleEndian>(key_len as u32)?;
    f.write_u32::<LittleEndian>(val_len as u32)?;
    f.write_all(&mut tmp)?;
```

```
    Ok(current_position)
}
```

- ① `key.to_vec()` converts the `&ByteStr` to a `ByteString`.
- ② `std::io::BufWriter` is a type that batches multiple short `write()` calls into fewer actual disk operations single one. This increases throughput while keeping the application code neater.
- ③ Iterating through one collection to populate another is slightly awkward, but the job gets done.

### 7.7.6 libactionkv full code listing

`libactionkv` performs the heavy lifting in our key-value stores. You have already explored much of it during “[Initializing the ActionKV struct](#)”, “[Processing an individual record](#)”, and “[Inserting a new key-value pair into an existing database](#)”.

Here is the code in full:

**Listing 7.19. libactionkv (ch7/ch7-actionkv1/src/lib.rs)**

```
#[macro_use]
extern crate serde_derive;

extern crate byteorder;
extern crate crc;

use std::collections::HashMap;
use std::io;
use std::io::prelude::*;
use std::io::{SeekFrom, BufReader, BufWriter};
use std::fs::{File, OpenOptions};
use std::path::{Path};
use byteorder::{LittleEndian, ReadBytesExt, WriteBytesExt};
use crc::crc32;

type ByteString = Vec;
type ByteStr = [u8];

#[derive(Debug, Serialize, Deserialize)]
pub struct KeyValuePair {
    pub key: ByteString,
    pub value: ByteString,
}

#[derive(Debug)]
pub struct ActionKV {
    f: File,
    pub index: HashMap<ByteString, u64>,
}

impl ActionKV {
    pub fn open(path: &Path) -> io::Result<Self> {
        let f = OpenOptions::new()
            .read(true)
            .write(true)
            .create(true)
            .open(path).expect("Failed to open file");
        return Ok(Self { f });
    }

    pub fn insert(&mut self, key: ByteString, value: ByteString) {
        let mut writer = BufWriter::new(self.f);
        writer.write_all(key.as_slice()).expect("Failed to write key");
        writer.write_all(value.as_slice()).expect("Failed to write value");
        writer.flush().expect("Failed to flush writer");
    }

    pub fn get(&self, key: ByteString) -> Option<ByteString> {
        let mut reader = BufReader::new(self.f);
        let mut buffer = [0; 1024];
        let mut pos = 0;
        let mut offset = 0;
        let mut found = false;
        while !found && pos < self.index.len() {
            let size = self.index.get(&key).unwrap();
            let mut current_pos = offset + pos * 1024;
            let mut current_size = 1024;
            if current_pos + current_size > self.index.len() {
                current_size = self.index.len() - current_pos;
            }
            reader.read_exact(&buffer[0..current_size]).expect("Failed to read buffer");
            for i in 0..current_size {
                if buffer[i] == 0 {
                    break;
                }
                if buffer[i] == key[pos] {
                    found = true;
                    break;
                }
            }
            pos += 1;
        }
        if found {
            let mut current_pos = offset + pos * 1024;
            let mut current_size = 1024;
            if current_pos + current_size > self.index.len() {
                current_size = self.index.len() - current_pos;
            }
            reader.read_exact(&buffer[0..current_size]).expect("Failed to read buffer");
            let mut value = ByteString::new();
            for i in 0..current_size {
                if buffer[i] == 0 {
                    break;
                }
                value.push(buffer[i]);
            }
            return Some(value);
        }
        None
    }

    pub fn remove(&mut self, key: ByteString) {
        let mut writer = BufWriter::new(self.f);
        writer.write_all(key.as_slice()).expect("Failed to write key");
        writer.write_all([0].as_slice()).expect("Failed to write zero");
        writer.flush().expect("Failed to flush writer");
    }
}
```

```

        .read(true)
        .write(true)
        .create(true)
        .append(true)
        .open(path)?;
    Ok(ActionKV { f: f, index: HashMap::new() })
}

pub fn load(&mut self) -> io::Result<()> {
    let mut f = BufReader::new(&mut self.f);

    loop {
        let current_position = f.seek(SeekFrom::Current(0))?;

        let maybe_kv = ActionKV::process_record(&mut f);
        let kv = match maybe_kv {
            Ok(kv) => kv,
            Err(err) => {
                match err.kind() {
                    io::ErrorKind::UnexpectedEof => {
                        break;
                    },
                    _ => return Err(err),
                }
            },
        };
        self.index.insert(kv.key, current_position);
    }

    Ok(())
}

fn process_record<R: Read>(f: &mut R) -> io::Result<KeyValuePair> { ①
    let saved_checksum = f.read_u32::<LittleEndian>()?;
    let key_len = f.read_u32::<LittleEndian>()?;
    let val_len = f.read_u32::<LittleEndian>()?;
    let data_len = key_len + val_len;

    let mut data = ByteString::with_capacity(data_len as usize);

    {
        f.by_ref()
            .take(data_len as u64)
            .read_to_end(&mut data)?;
    }
    debug_assert_eq!(data.len(), data_len as usize);

    let checksum = crc32::checksum_ieee(&data);
    if checksum != saved_checksum {
        panic!("data corruption encountered ({:08x} != {:08x})", checksum,
               saved_checksum);
    }
}

```

```

let val = data.split_off(key_len as usize);
let key = data;

Ok( KeyValuePair { key: key, value: val } )
}

pub fn seek_to_end(&mut self) -> io::Result<u64> {
    self.f.seek(SeekFrom::End(0))
}

pub fn get(&mut self, key: &ByteStr) -> io::Result<Option<ByteString>> { ②
    let position = match self.index.get(key) {
        None => return Ok(None),
        Some(position) => *position,
    };

    let kv = self.get_at(position)?;

    Ok(Some(ByteString::from(kv.value)))
}

pub fn get_at(&mut self, position: u64) -> io::Result<KeyValuePair> {
    let mut f = BufReader::new(&mut self.f);
    f.seek(SeekFrom::Start(position))?;
    let kv = ActionKV::process_record(&mut f)?;

    Ok(kv)
}

pub fn find(&mut self, target: &ByteStr) -> io::Result<Option<(u64, ByteString)>> {
    let mut f = BufReader::new(&mut self.f);

    let mut found : Option<(u64, ByteString)> = None;

    loop {
        let position = f.seek(SeekFrom::Current(0))?;

        let maybe_kv = ActionKV::process_record(&mut f);
        let kv = match maybe_kv {
            Ok(kv) => kv,
            Err(err) => {
                match err.kind() {
                    io::ErrorKind::UnexpectedEof => {
                        break;
                    },
                    _ => return Err(err),
                }
            },
        };

        if kv.key == target {
    
```

```

        found = Some((position, kv.value));
    }

    // important to keep looping until the end of the file,
    // in case the key has been overwritten
}

Ok(found)
}

pub fn insert(&mut self, key: &ByteStr, value: &ByteStr) -> io::Result<()> {
    let position = self.insert_but_ignore_index(key, value)?;

    self.index.insert(key.to_vec(), position);
    Ok(())
}

pub fn insert_but_ignore_index(&mut self, key: &ByteStr, value: &ByteStr) ->
io::Result<u64> {
    let mut f = BufWriter::new(&mut self.f);

    let key_len = key.len();
    let val_len = value.len();
    let mut tmp = ByteString::with_capacity(key_len + val_len);

    for byte in key {
        tmp.push(*byte);
    }

    for byte in value {
        tmp.push(*byte);
    }

    let checksum = crc32::checksum_ieee(&tmp);

    let next_byte = SeekFrom::End(0);
    let current_position = f.seek(SeekFrom::Current(0))?;
    f.seek(next_byte)?;
    f.write_u32::<LittleEndian>(checksum)?;
    f.write_u32::<LittleEndian>(key_len as u32)?;
    f.write_u32::<LittleEndian>(val_len as u32)?;
    f.write_all(&mut tmp)?;

    Ok(current_position)
}

#[inline]
pub fn update(&mut self, key: &ByteStr, value: &ByteStr) -> io::Result<()> {
    self.insert(key, value)
}

#[inline]
pub fn delete(&mut self, key: &ByteStr) -> io::Result<()> {
}

```

```

        self.insert(key, b"""
    }
}

```

- ① `process_record()` assumes that `f` is already at the right place in the file
- ② We need to wrap `Option` within `Result` to allow for the possibilities of I/O errors as well as missing values occurring
- ③ "Unexpected" is relative. The application may not have expected it, but we expect files to be finite.

If you've made it this far, you should congratulate yourself. You've implemented a key value store that will happily store and retrieve whatever you have to throw at it.

### 7.7.7 Working with keys and values with `HashMap` and `BTreeMap`

Working with key-value pairs happens in almost every programming language. For the tremendous benefit of learners everywhere, this task, and the data structures that support it, have many names.

You might encounter someone with a computer science background preferring to use the term *hash table*. Perl and Ruby strip that off and call them *hashes*. Lua does the opposite and uses the term *table*. Many communities name the structure after a metaphor, such as a *dictionary* (one term is being associated with a “definition”) or a *map* (programmers, following mathematicians, are mapping from one value to another). Other communities prefer naming based on the role that the structure plays. PHP describes them as *associative arrays*. JavaScript’s objects tend to be implemented as a key/value pair collection and so generic term *object* suffices. Static languages tend to name them according to how they are implemented. C++ and Java distinguish between a *hash map* and a *tree map*.

Rust uses the terms `HashMap` and `BTreeMap` to define two implementations of the same abstract data type. Rust is closest to C++ and Java in this regard.

In this book, the terms “collection of key/value pairs” and “associative array” refer to the abstract data type. “Hash table” refers to associative arrays implemented with a hash table. `HashMap` prefers to Rust’s implementation of hash tables.

#### **What is a hash? What is hashing?**

If you’ve ever been confused by the term “hash”, it may help to understand that this relates to an implementation decision made to enable non-integer keys to map to values.

`HashMap` is implemented with a *hash function*. Computer scientists will understand that this implies a certain behavior pattern in common cases. They have a “constant time lookup” in general. (Although their performance can suffer in some pathological cases, as we’ll see shortly).

A *hash function* maps between values of variable-length to fixed-length values. In practice, the return value of a hash function is an integer. That fixed-width value can then be used to build a very efficient lookup table. This internal lookup table is known as a *hash table*.

Listing 7.20 is a very basic hash function for `&str` that simply interprets the first character of a string as an unsigned integer:

**Listing 7.20. Implementing a basic hash function for &str that uses the first character of the string as an integer value**

```
fn basic_hash(key: &str) -> u32 {
    let first = key.chars()          ①
        .next()                      ②
        .unwrap_or('\'0');           ③

    unsafe {                         ④
        std::mem::transmute::<char, u32>(first) ④
    }                                ④
}

① The .chars() iterator converts the string into a series of char values, which are each 4 bytes long
② .next() returns an Option, which will be either Some(char) or None for empty strings
③ In the case of an empty string, provide NULL as the default. unwrap_or() behaves as unwrap(),
but will provide a value rather than panicing when None is encountered.
④ Interpret the memory of first as a u32, even though its type is char.
```

`basic_hash` can take any string as input—an infinite set of possible inputs—and return a fixed-width result for all of them in a deterministic manner. Great!

`basic_hash` is very fast, but has some large faults. If multiple inputs start with the same character (perhaps “Tonga” and “Tuvalu”), they will result in the same output. This happens in every instance when a infinite input space is mapped into a finite space, but it’s particularly bad here. Natural language text is not uniformly distributed.

Hash tables, including Rust’s `HashMap` deal with this phenomenon, called a *hash collision*, by providing a backup location for keys with the same hash value. That secondary storage is typically a `Vec<T>` that we’ll call the collision store. When collisions occur, the collision store is scanned from front to back whenever it is accessed. That linear scan takes longer and longer to run as the store’s size increases. Attackers can make use of this characteristic to overload the computer that is performing the hash function.

In very general terms, faster hash functions do less work to avoid being attacked. They will also perform best when their inputs will be within a defined range.

Fully understanding the internals of how hash tables are implemented is too much detail for here. It’s a fascinating topic for programmers who wish to extract optimum performance and memory usage from their programs.

## 7.7.8 Creating a `HashMap` and populating it with values

Listing 7.21 provides a collection of key-value pairs encoded as JSON.

**Listing 7.21. Using some polynesian island nations and their capital cities to demonstrate the use of an associative array in JSON notation**

```
{
    "Cook Islands": "Avarua",
    "Fiji": "Suva",
    "Kiribati": "South Tarawa",
    "Niue": "Alofi",
```

```

    "Tonga": "Nuku'alofa",
    "Tuvalu": "Funafuti"
}

```

Rust does not provide a literal syntax for `HashMap` within the standard library. To insert items into and get them out again, follow the example provided at Listing 7.22 .

When executed, Listing 7.22 produces the following line in the console:

```
Capital of Tonga is: Nuku'alofa
```

### **Listing 7.22. An example of the basic operations of `HashMap` (ch7/ch7-pacific-basic/src/main.rs)**

```

use std::collections::HashMap;

fn main() {
    let mut capitals = HashMap::new(); ①

    capitals.insert("Cook Islands", "Avarua");
    capitals.insert("Fiji", "Suva");
    capitals.insert("Kiribati", "South Tarawa");
    capitals.insert("Niue", "Alofi");
    capitals.insert("Tonga", "Nuku'alofa");
    capitals.insert("Tuvalu", "Funafuti");

    println!("Capital of Tonga is: {}", capitals["Tonga"]); ②
}

```

- ① Type declarations of the keys and values are not required here as they are inferred by the Rust compiler
- ② `HashMap` implements `Index`, which allows for values to be retrieved via the square bracket indexing style

Writing everything out as method calls can feel needlessly verbose at times. With some support from the wider Rust ecosystem, it's possible to inject JSON string literals into Rust code. What's best is that the conversion is done at compile time, meaning no loss of runtime performance.

The output of Listing 7.23 is also a single line:

```
Capital of Tonga is: "Nuku'alofa" ①
```

- ① The double quotes are also included as the `json!` macro returns a wrapper around `String` and this is its default representation.

### **Listing 7.23. Using `serde-json` crate to include JSON literals within your Rust source code (ch7/ch7-pacific-json/src/main.rs)**

```
#[macro_use] ①
```

```
extern crate serde_json;          ①

fn main() {
    let capitals = json!({
        "Cook Islands": "Avarua",
        "Fiji": "Suva",
        "Kiribati": "South Tarawa",
        "Niue": "Alofi",
        "Tonga": "Nuku'alofa",
        "Tuvalu": "Funafuti"
    });

    println!("Capital of Tonga is: {}", capitals["Tonga"])
}
```

- ① Incorporate the `serde_json` crate into this one and make use of its macros. This brings the `json!` macro into scope.
- ② `json!` takes a JSON literal—and also Rust expressions that implement `String` values—and converts it into a Rust value of type `serde_json::Value`. `serde_json::Value` is an enum that can represent every type within the JSON specification.

### 7.7.9 Retrieving values from `HashMap` and `BTreeMap`

The main operation that a key-value store provides is the ability to access its values. There are two ways to achieve this. To demonstrate them, let's assume that we have initialized `capitals` from Listing 7.23 .

The approach already demonstrated is to access values via square brackets:

```
capitals["Tonga"] ①
```

- ① Returns "Nuku'alofa"

This approach will return a read-only reference the value (which is deceptive when dealing with examples containing string literals, as their status as references is somewhat disguised). In the syntax used by Rust's documentation, this is described as `&V`, where `&` denotes a read-only reference and `V` is the type of the value. If the key is not present, the program will panic.

**NOTE**

Index notation is supported by all types that implement the `Index` trait.

Accessing `capitals["Tonga"]` is syntactic sugar for `capitals.index("Tonga")`.

Secondly, it's possible to use the `.get()` method on `HashMap`. This returns an `Option<&V>`, providing the opportunity to recover from cases where values are missing.

```
capitals.get("Tonga") ①
```

- ① Returns `Some("Nuku'alofa")`

Other important operations supported by `HashMap` are:

- Deleting key-value pairs with the `.remove()` method
- Iterating over keys, values and key-value pairs with the `.keys()`, `.values()` and `.iter()` methods respectively as well as their read/write variants (`.keys_mut()`, `.values_mut()` and `.iter_mut()`).

There is no method for iterating through a subset of the data. For that, `BTreeMap` is needed.

### 7.7.10 How to decide between `HashMap` and `BTreeMap`

If you're wondering about which backing data structure to choose, here is a simple guideline: Use `HashMap` unless you have a good reason to use `BTreeMap`.

`BTreeMap` is faster when there is a natural ordering between the keys, and your application makes use of that ordering. Specifically:

- you wish to process values in order
- you wish to select for a range of keys

Let's demonstrate these two use cases with a small example from Europe. The Dutch East India Company, known as VOC after the initials of its Dutch name *Vereenigde Oostindische Compagnie* was an extremely powerful economic and political force at its peak.

For two centuries, VOC was a dominant trader between Asia and Europe. It had its own navy, currency and established its own colonies (called trading posts). It was also the first company to issue bonds. In the beginning, investors from six business chambers (kamers) provided capital for the business.

Let's use these investments as key-value pairs. Code is available at Listing 7.25 . When compiled, it produces an executable that generates the following output:

#### Listing 7.24. Output from Listing 7.25

```
chamber Rotterdam invested 173000
chamber Hoorn invested 266868
chamber Delft invested 469400
chamber Enkhuizen invested 540000
chamber Middelburg invested 1300405
chamber Amsterdam invested 3697915
smaller chambers: Rotterdam Hoorn Delft
```

#### Listing 7.25. Demonstrating range queries and ordered iteration of the `BTreeMap`

```
use std::collections::BTreeMap;

fn main() {
    let mut voc = BTreeMap::new();
```

```

voc.insert(3_697_915, "Amsterdam");
voc.insert(1_300_405, "Middelburg");
voc.insert( 540_000, "Enkhuizen");
voc.insert( 469_400, "Delft");
voc.insert( 266_868, "Hoorn");
voc.insert( 173_000, "Rotterdam");

for (guilders,kamer) in &voc {
    println!("chamber {} invested {}", kamer, guilders);      ①
}

print!("smaller chambers: ");
for (_guilders,kamer) in voc.range(0..500_000) {            ②
    print!("{} ", kamer);
}
println!("");
}

```

① Prints in sorted order. With integers, this means starting at the lowest value.

② BTreemap allows you to select a portion of the keys that will be iterated through with the range syntax

**Table 7.9. Considerations for deciding on which implementation to use to map keys to values**

std::collections::HashMap with default hash function (known as SipHash in the literature)	cryptographically secure and resistant to denial of service attacks, but slower than alternative hash functions
std::collections::BTreemap	useful for keys with an inherent ordering where cache-coherence may provide a speed boost

### 7.7.11 Adding database index to action\_kv v0.2

Databases and file systems are much larger pieces of software than single files. There is a very large design space involved with storage and retrieval systems, which is why new ones are always being developed. Common to all of those systems however will be a component that is the real smarts behind the database

actionkv v0.1, built in “[Introducing actionkv v0.1: an in-memory key-value store with a command line interface](#)”, contains a major issue that prevents it from having a decent start-up time. Every time it’s run, it needs to re-build its index of where keys are stored every time it runs.

Let’s add the ability for actionkv to store its own data that index *within* the same file that is being used to store application data.

It will be easier than it sounds. No changes to libactionkv are necessary. And the front-end code only requires minor additions.

The project folder now has a new structure with an extra file:

**Listing 7.26. ActionKV v0.2: updated project structure**

```

actionkv
└── src
    ├── akv_disk.rs      ①
    ├── akv_mem.rs
    └── lib.rs
    └── Cargo.toml ②

```

- ① New file included in the the project
- ② Two updates are required here to add a new binary and dependencies

The project's `Cargo.toml` adds some new dependencies along with a second "[[bin]]" entry:

**Listing 7.27. ActionKV v0.2: updated `Cargo.toml` file (ch7/ch7-actionkv2/Cargo.toml)**

```

[package]
name = "actionkv"
version = "0.2.0"
authors = ["Tim McNamara <code@timmcnamara.co.nz>"]

[dependencies]
bincode = "1.0"          ①
byteorder = "1.2"
crc = "1.7"
serde = "1.0"            ①
serde_derive = "1.0"      ①

[lib]
name = "libactionkv"
path = "src/lib.rs"

[[bin]]
name = "akv_mem"
path = "src/akv_mem.rs"

[[bin]]
name = "akv_disk"        ②
path = "src/akv_disk.rs"  ②

```

- ① New dependencies to assist with writing the index to disk
- ② New executable definition

When a key is accessed, we convert load the index on-disk representation to its in-memory form.

**Listing 7.28. Excerpt from Listing 7.29 highlighting the main change from Listing 7.9**

```
match action {
```

```

    "get" => {
①        let index_as_bytes = a.get(INDEX_KEY).unwrap().unwrap();
②        let index: HashMap<ByteString, u64> =
bincode::deserialize(&index_as_bytes).unwrap();      ③

        match index.get(key) {                         ④
            None => eprintln!("{} not found", key),   ④
            Some(idx) => {                           ⑤
                let kv = a.get_at(idx).unwrap();
                println!("{}:", kv.value),           ⑤
            }
        }
    },
},

```

- ① Nothing changes for the end-user
- ② INDEX\_KEY is the “name” of the index within the database. Two unwrap() calls are required because a.index is a HashMap that returns Option and values themselves are stored within an Option to facilitate possible future deletes.
- ③ Convert the on-disk representation to an in-memory representation.
- ④ Has the key that’s been requested actually been stored?
- ⑤ Yes! Great, now fetch that KeyValuePair from disk

**Listing 7.29. A key-value store that persists its index data between runs (ch7/ch7-actionkv2/src/akv\_disk.rs)**

```

extern crate bincode;
extern crate libactionkv;

use std::collections::HashMap;
use libactionkv::ActionKV;

#[cfg(target_os = "windows")]
const USAGE: &'static str = "
Usage:
    akv_disk.exe FILE get KEY
    akv_disk.exe FILE delete KEY
    akv_disk.exe FILE insert KEY VALUE
    akv_disk.exe FILE update KEY VALUE
";

#[cfg(not(target_os = "windows"))]
const USAGE: &'static str = "
Usage:
    akv_disk FILE get KEY
    akv_disk FILE delete KEY
    akv_disk FILE insert KEY VALUE
    akv_disk FILE update KEY VALUE
";

```

```

type ByteStr = [u8];
type ByteString = Vec<u8>;

fn store_index_on_disk(a: &mut ActionKV, index_key: &ByteStr) {
    a.index.remove(index_key);
    let index_as_bytes = bincode::serialize(&a.index).unwrap();
    a.index = std::collections::HashMap::new();
    a.insert(index_key, &index_as_bytes).unwrap();
}

fn main() {
    const INDEX_KEY: &ByteStr = b"+index";

    let args: Vec<String> = std::env::args().collect();
    let fname = args.get(1).expect(&USAGE);
    let action = args.get(2).expect(&USAGE).as_ref();
    let key = args.get(3).expect(&USAGE).as_ref();
    let maybe_value = args.get(4);

    let path = std::path::Path::new(&fname);
    let mut a = ActionKV::open(path).expect("unable to open file");

    a.load().expect("unable to load data");
    store_index_on_disk(&mut a, INDEX_KEY);

    match action {
        "get" => {
            let index_as_bytes = a.get(&INDEX_KEY).unwrap().unwrap();
            let index: HashMap<ByteString, u64> =
bincode::deserialize(&index_as_bytes).unwrap();

            match index.get(key) {
                None => eprintln!("{} not found", key),
                Some(value) => println!("{}: {}", key, value), // needs to use Debug as
[u8] is arbitrary bytes
            }
        },
        "delete" => a.delete(key).unwrap(),
        "insert" => {
            let value = maybe_value.expect(&USAGE).as_ref();
            a.insert(key, value).unwrap()
        },
        "update" => {
            let value = maybe_value.expect(&USAGE).as_ref();
            a.update(key, value).unwrap()
        },
        _ => eprintln!("{}: {}", key, &USAGE),
    }
}

```

## 7.8 Summary

This chapter has covered lots of ground. Hopefully you have a newfound appreciation

for some of the difficulties that arise from trying to do something as easy as storing information.

You have learned:

- presenting binary data as text with hexadecimal notation by implementing a `hexdump` clone
- translating between Rust data structures and on-disk file formats, such as JSON, with `serde` and its related crates
- reading and writing multi-byte binary data with a defined endianness
- verifying data that's sent across fallible channels via checksums and parity bits
- managing complex software projects by writing library crates
- adding multiple binaries to a project with `cargo`
- using a `lib.rs` file to build a crate and import it with a project's `main()` function, within `src.rs`
- working with key value pairs
- the internals of parity bit checking and other forms of checksum
- printing errors to `stderr` with the `eprintln!` macro



# Networking

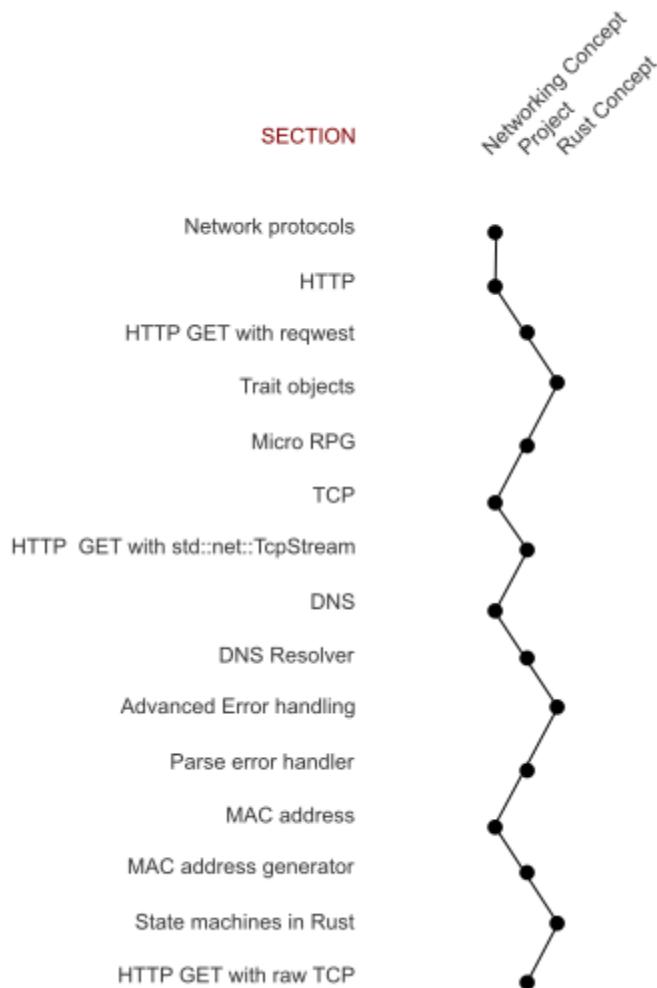
This chapter implements making HTTP requests multiple times, stripping away a layer of abstraction each time. We start by using a user-friendly library, then boil that away until we're left with manipulating raw TCP packets. Impress your friends your ability to distinguish an IP address from a MAC address. And learn why we went straight from IPv4 to IPv6.

You'll also be learning lots of Rust in this chapter, most of it related to advanced error handling techniques which become essential for incorporating upstream crates. Several pages are devoted to error handling. This includes a through introduction to *trait objects*.

Networking is a difficult subject to cover in a single chapter. Each layer is a fractal of complexity. Networking experts will hopefully be kind of my lack of depth in my treatment of their topic of interest!

Figure 8.1 provides an overview of the topics that the chapter covers. Some of the projects that we cover include implementing DNS resolution, generating standards-compliant MAC addresses and multiple examples of generating HTTP requests.. A hint of a role-playing game is added for light relief.

**Figure 8.1. Networking chapter map. The chapter incorporates a healthy mix of theory and practical exercises.**



## 8.1 Just enough HTTP

Rather than trying to learn the whole networking stack, let's focus on something that's of practical use. Most readers of this book will have encountered web programming. Most web programming involves interacting with some sort of framework. Let's look there.

HTTP is the protocol that web frameworks understand. Learning more about HTTP enables us to extract the most performance out of our web frameworks. It can also help us to more easily diagnose any problems that are occurring.

**Figure 8.2. Several layers of networking protocols involved with delivering content over the Internet. Includes comparisons with 2 other common models, the 7 layer OSI model and the 4 layer TCP/IP model.**

## How computers talk to each other

### ABOUT

A view of the networking stack. Each layer relies upon the layers below it.

Occasionally layers bleed together. For example, HTML files can include directives that overwrite those provided by HTTP.

For a message to be received, each layer must be traversed from bottom to top. To send messages, the steps are reversed.

### HOW TO READ

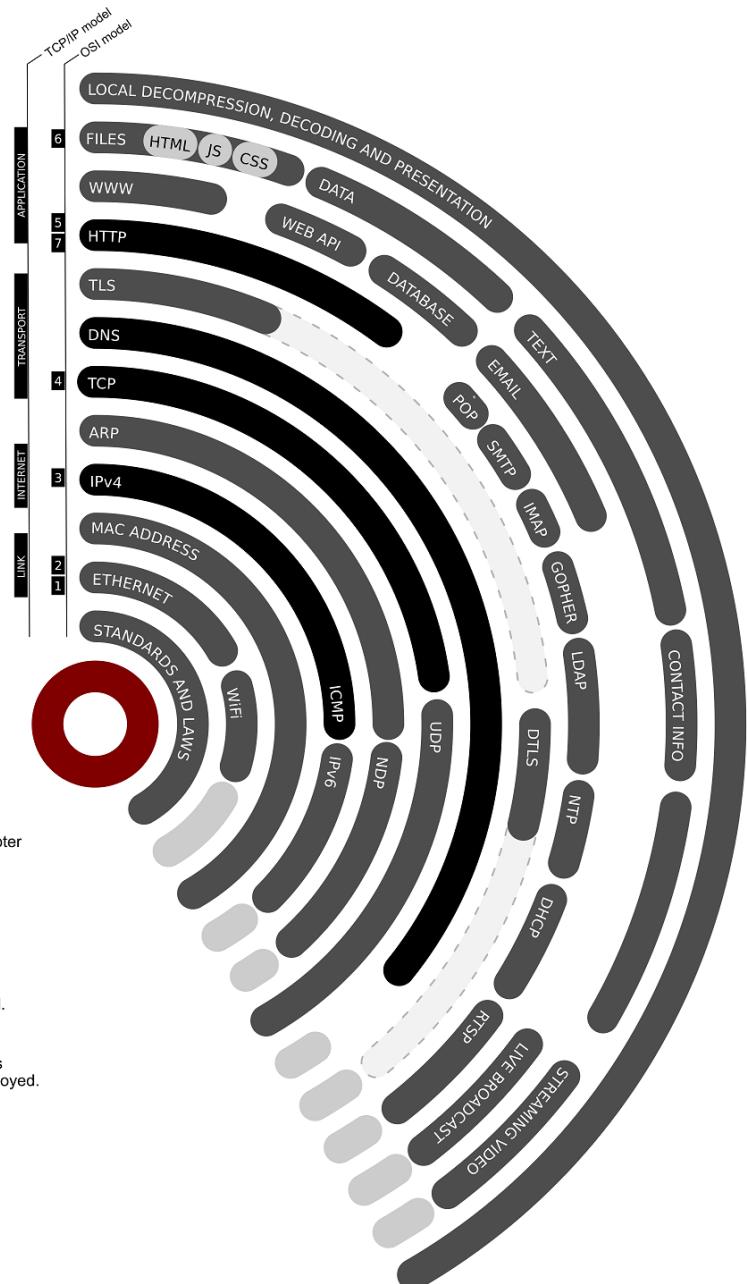
Vertical positioning typically indicates that two levels interact at that location.

Exceptions include encryption provided by TLS, Network addressing can be provided by either IPv4 or IPv6 and virtual layers are largely ignorant of physical links. (Shadows from physics do appear on upper layers in the form of latency and reliability.)

Gaps indicate that a higher level can pass directly through to the level below. A domain name or TLS security is not necessary for HTTP to function, for example.

### LEGEND

-  Protocol discussed in this chapter
-  Protocol in use at this level
-  Represents hundreds of other protocols that exist at this level.
-  Represents that this protocol is available, but may not be deployed.



Networking is comprised of layers. If you’re new to the field, don’t be intimidated by the flood of acronyms. The most important thing to remember is that lower levels are unaware of what’s happening above them and higher levels are agnostic to what’s happening below them. Lower levels receive a stream of bytes and pass it on. Higher levels don’t care how messages are sent, they just want them to be sent.

HTTP is known as an application-level protocol. It relies on *TLS* (Transport Layer Security), which has replaced the better known *SSL* (Secure Socket Layer). TLS sits on top of TCP. On top of HTTP sit HTML, CSS, JavaScript, WebAssembly modules, images, video and other files. These layers do bleed together slightly though. HTTP will often redundantly include information provided at the TCP layer. HTML includes a mechanism to supplement or overwrite directives omitted or specified within HTTP.

Figure 8.2 provides one view of the networking stack. Even that complicated picture is highly simplified. Listing 8.3 and its output at Listing 8.4

#### **Listing 8.1. Generating a HTTP message to [www.manning.com](https://www.manning.com/books/rust-in-action)**

```
curl \1
  --include \2
  --head \3
  https://www.manning.com/books/rust-in-action
```

- ① curl is a command-line utility for making requests over the Internet, especially HTTP
- ② Include the HTTP response codes
- ③ Use the HEAD method, which omits the message body. This shortens the length of the response, making it easier to show in [Listing 8.2](#) .

#### **Listing 8.2. Contents of an HTTP message**

```
HTTP/1.1 200 \1
Server: nginx/1.16.0
Date: Sun, 26 May 2019 04:26:26 GMT
Content-Type: text/html; charset=UTF-8 \2
Connection: keep-alive \3
X-Application-Context: application:production \4
Content-Language: en-US
X-Frame-Options: Deny
Content-Security-Policy: frame-ancestors 'none'
```

- ① This server supports version 1.1 of the HTTP protocol and this message has the 200 response code, which means everything went smoothly.
- ② The Content-Type header describes the format—and in this case the encoding—of the message body.
- ③ The Connection header relates to the underlying TCP/TLS connection. It’s telling the client (curl) that it should hold the connection open if there are more requests to be made.
- ④ The host system has defined a custom header that has been passed along from whatever has generated the page.

In Listing 8.1 , we’re only seeing what’s happening at the HTTP layer. It’s possible to ask for more output. That’ll help identify what was actually sent.

**Listing 8.3. Making an HTTP request to `www.manning.com` with the `curl` command-line utility, requesting verbose output.**

```
curl -vI https://www.manning.com/books/rust-in-action
```

**Listing 8.4. Example output from Listing 8.3 . Actual output will differ between `curl` versions, depending on how your `curl` was compiled and the details of Manning’s hosting environment.**

```
* Trying 35.166.24.88...                                         1
* TCP_NODELAY set                                              2
* Connected to www.manning.com (35.166.24.88) port 443 (#0)  3
* ALPN, offering h2                                              4
* ALPN, offering http/1.1                                         4
* successfully set certificate verify locations:
*   CAfile: none                                                 5
*   CApath: /etc/ssl/certs
* TLSv1.3 (OUT), TLS handshake, Client hello (1):               6
* TLSv1.3 (IN), TLS handshake, Server hello (2):                6
* TLSv1.2 (IN), TLS handshake, Certificate (11):                6
* TLSv1.2 (IN), TLS handshake, Server key exchange (12):        6
* TLSv1.2 (IN), TLS handshake, Server finished (14):             6
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):        6
* TLSv1.2 (OUT), TLS change cipher, Client hello (1):            6
* TLSv1.2 (OUT), TLS handshake, Finished (20):                   6
* TLSv1.2 (IN), TLS handshake, Finished (20):                   6
* SSL connection using TLSv1.2 / ECDHE-RSA-AES256-GCM-SHA384    6
* ALPN, server accepted to use http/1.1                         7
* Server certificate:
*   subject: OU=Domain Control Validated; CN=*.manning.com      8
*   start date: May 25 00:46:15 2019 GMT
*   expire date: May 25 00:46:15 2020 GMT
*   subjectAltName: host "www.manning.com" matched cert's "*.manning.com"
*   issuer: C=US; ST=Arizona; L=Scottsdale; O=GoDaddy.com, Inc.;
OU=http://certs.godaddy.com/repository/; CN=Go Daddy Secure Certificate Authority - G2
*   SSL certificate verify ok.                                     9
> HEAD /books/rust-in-action HTTP/1.1                           10
> Host: www.manning.com
> User-Agent: curl/7.61.0
> Accept: */*
>
< HTTP/1.1 200
HTTP/1.1 200
< Server: nginx/1.16.0
Server: nginx/1.16.0
< Date: Sun, 26 May 2019 04:41:58 GMT
Date: Sun, 26 May 2019 04:41:58 GMT
```

```

< Content-Type: text/html; charset=UTF-8
Content-Type: text/html; charset=UTF-8
< Connection: keep-alive
Connection: keep-alive
< X-Application-Context: application:production
X-Application-Context: application:production
< Content-Language: en-US
Content-Language: en-US
< X-Frame-Options: Deny
X-Frame-Options: Deny
< Content-Security-Policy: frame-ancestors 'none'
Content-Security-Policy: frame-ancestors 'none'

<
* Connection #0 to host www.manning.com left intact

```

- ➊ DNS has resolved the `www.manning.com` host to the IP address `35.166.24.88` (DNS)
- ➋ TCP connection parameters being used by `curl` (Internal)
- ➌ TCP connection is established, using the conventional port 443 for HTTPS (TCP)
- ➍ ALPN parameters being used by `curl`. ALPN is an extension to TLS (Internal)
- ➎ The location of SSL certificates that my computer, and by extension `curl`, trusts (Internal)
- ➏ TLS negotiation process, where the two sides are attempting to decide which version of TLS and the encryption ciphers to use (TLS)
- ➐ ALPN negotiation results (Internal)
- ➑ Details from the SSL certificate (Internal)
- ➒ Verification of the server's SSL certificate against the certificates that my computer has stored (Internal)
- ➓ Data sent by `curl` to the server (HTTP)
- ➔ Response back to `curl` (HTTP)

HTTPS sits on top of TLS, which sits on top of TCP. One thing to note is that the web server itself is somewhat ignorant that content is being delivered over TLS. On lines 32 and 33 of Listing 8.4, the server responds with the string "HTTP/1.1 200". The encryption is wrapped around this content. As discussed earlier, the lower level (TLS) is ignorant of what it's dealing with and the higher level (HTTP) doesn't care about how it is being transported to the recipient.

Protocols don't necessarily carry all of the semantics of their underlying layers with them, although shadows do tend to linger. For example, HTTP is a connectionless protocol, but it's implemented upon TCP, which sets up a persistent connection between two computers. TCP is used by HTTP because it also provides reliability and in-order delivery of messages.

## 8.2 Generating an HTTP GET request with `reqwest`

Our first implementation will be with a high-level library that is focused on HTTP. We'll be using `reqwest`, as its focus is primarily on making it easy for Rust programmers to create an HTTP request.

Although it's the shortest, the `reqwest` implementation is the most feature complete. As well as being able to correctly interpret HTTP headers, it will also handle cases such as content redirects. Most importantly though, it understands how to handle TLS properly. In addition to expanded networking capabilities, `reqwest` also validates the content's encoding and ensures that it is sent to your application as a valid `String`. None of our lower-level implementations do any of that.

#### **Listing 8.5. Project structure for Listing 8.7**

```
ch8-simple/
└── src
    └── main.rs
Cargo.toml
```

#### **Listing 8.6. Crate metadata for Listing 8.7 (ch8/ch8-simple/Cargo.toml)**

```
[package]
name = "ch8-simple"
version = "0.1.0"
authors = ["Tim McNamara <code@timmcnamara.co.nz>"]
edition = "2018"

[dependencies]
reqwest = "0.9"
```

#### **Listing 8.7. Making an HTTP request with the reqwest library (ch8/ch8-simple/src/main.rs)**

```
extern crate reqwest;

fn main() -> Result<(), Box<dyn std::error::Error>> { ❶
    let url = "http://www.rustinaction.com/";
    let mut response = reqwest::get(url)?;

    let content = response.text()?;
    print!("{}", content);

    Ok(())
}
```

❶ The syntax for `Box<dyn std::error::Error>` is new. It represents a *trait object*.

If you've ever done any web programming, Listing 8.7 should be straight forward. `reqwest::get()` issues an HTTP GET request to the URL represented by `url`. The `response` variable holds a struct representing the server's response. The `response.text()` method returns a `Result` that provides access to the HTTP body, after validating that the contents are a legal `String`.

One question though - what on earth is the error side of the `Result` return type `Box<dyn std::error::Error>?` This is an example of a *trait object*, which enables Rust to

support *polymorphism* at runtime. Trait objects are proxies for concrete types. The syntax `Box<dyn std::error::Error>` means a `Box`, a pointer, to any type that implements `'std::error::Error'`'s

Using a library that knows about HTTP allows our programs to omit many details:

- Knowing when to close the connection. HTTP has rules for telling each of the parties when the connection has ended. This isn't available to us when making requests by hand. Instead, we keep the connection open for as long as possible, and hope that the server will close
- Converting the byte stream to content. Rules for translating the message body from `[u8]` to `String` (or perhaps an image, video or some other content) are handled as part of the protocol. This can be tedious to handle by hand, as HTTP allows content to be compressed in several methods and encoded in several plain text formats.
- TCP port numbers. HTTP defaults to port 80. A library that is tailored for HTTP, such as `reqwest` can omit it. When we're building requests by hand with generic TCP crates, we need to be explicit.
- IP addresses. The TCP protocol doesn't actually know about domain names like `www.rustinaction.com`. The library is resolving the IP address for `www.rustinaction.com` on our behalf.

## 8.3 Trait Objects

This section describes *trait objects* in detail. If you would like to focus on networking, feel free to skip ahead to “[TCP](#)”. There is a reasonable amount of jargon in the next several paragraphs. Brace yourself. You'll do fine.

Let's start by introducing trait objects by what they achieve and what they do, rather than focusing on what they are. Trait objects are similar to generics, but they're more flexible. An example might be useful to illustrate this.

One irritating aspect of Rust's `Vec<T>` is that it can only hold contain elements of the same type. Trait objects can allow you to do so.

You're developing the world's next best-selling fantasy role-playing game. Although players may choose different races, and each race is defined in its own `struct`, you want them to be able to treat them as a unit. A `Vec<T>` won't work here, because we can't easily have types `T`, `U` and `V` wedged into `Vec<T>` without introducing some type of wrapper object. Through some pointer trickery, trait objects can enable this. Trait objects have a common representation to the compiler.

Trait objects have three forms of syntax: `&dyn Trait`, `&Trait`, and `Box<Trait>`.

- `&dyn Trait`
- `&Trait`
- `Box<Trait>`

Listing 8.9 is the start of your game. Characters in the game can be one of three races:

humans, elves and dwarves. They're represented by the `Human`, `Elf` and `Dwarf` structs respectively. Characters interact with things. Things are represented by the `Thing` type<sup>20</sup>. `Thing` is an enum that currently represents swords and trinkets. There's only one form of interaction right now: enchantment.

Enchanting a thing looks like this:

```
character.enchant(&mut thing)
```

Enchantment doesn't actually do anything, unless a mistake is made. When a mistake occurs, `thing` is transformed into a trinket. As a friend of mine regularly says: life is pain.

Within Listing 8.9, we create a party of characters with the following syntax:

```
let d = Dwarf {};
let e = Elf {};
let h = Human {};

let party: Vec<&dyn Enchanter> = vec![&d, &h, &e]; ❶
```

- ❶ Although `d`, `e` and `h` are different types, using the type hint `&dyn Enchanter` tells the compiler to treat each value as a trait object. They now all have the same type.

Actually casting the spell involves choosing a spellcaster. We make use of the `rand` crate for that.

```
let spellcaster = party.choose(&mut rand::thread_rng()).unwrap();
spellcaster.enchant(&mut it)
```

The `choose` method originates from the `rand::seq::SliceRandom` trait that is brought into scope in line 2. One of the party is chosen at random. She then attempts to enchant the object `it`.

Compiling and running Listing 8.9 results in a variation of this:

```
Elf mutters incoherently. The Sword fizzes, then turns into a worthless trinket.
```

#### **Listing 8.8. Crate metadata for the rpg project (ch8/ch8-rpg/Cargo.toml)**

```
[package]
name = "rpg"
version = "0.1.0"
authors = ["Tim McNamara <code@timmcnamara.co.nz>"]
edition = "2018"

[dependencies]
rand = "0.7"
```

---

<sup>20</sup> Naming is hard.

**Listing 8.9. Example of a using a trait object, &Enchanter to enable a container to hold several types (ch8/ch8-rpg/src/main.rs)**

```
use rand;
use rand::seq::SliceRandom;
use rand::Rng;

#[derive(Debug)]
struct Dwarf {}

#[derive(Debug)]
struct Elf {}

#[derive(Debug)]
struct Human {}

#[derive(Debug)]
enum Thing {
    Sword,
    Trinket,
}

trait Enchanter: std::fmt::Debug {
    fn competency(&self) -> f64;

    fn enchant(&self, thing: &mut Thing) {
        print!("{} mutters incoherently. ", self);
        if rand::thread_rng().gen_bool(self.competency()) {
            println!("The {} glows brightly.", thing);
            return;
        }
        println!("The {} fizzes, then turns into a worthless trinket.", thing);
        *thing = Thing::Trinket {};
    }
}

impl Enchanter for Dwarf {
    fn competency(&self) -> f64 {
        0.5
    }
}
impl Enchanter for Elf {
    fn competency(&self) -> f64 {
        0.95
    }
}
impl Enchanter for Human {
    fn competency(&self) -> f64 {
        0.8
    }
}
```

```

fn main() {
    let mut it = Thing::Sword;

    let d = Dwarf {};
    let e = Elf {};
    let h = Human {};

    let party: Vec<&Enchanter> = vec![&d, &h, &e];
    let spellcaster = party.choose(&mut rand::thread_rng()).unwrap();

    spellcaster.enchant(&mut it)
}

```

Trait objects are a powerful construct in the language. In a sense, they provide a way to navigate Rust's rigid type system. As you learn about this feature in more detail, you will encounter some jargon. Trait objects are a form of *type erasure*. The compiler does not have access to the original type during the call to `enchant()`.

### *&Trait vs &Type*

One of the frustrating things about Rust's syntax for beginners is that traits objects and type parameters look very similar.

For example, consider these two lines:

```

use rand::Rng;
use rand::rngs::ThreadRng;

```

Although they both have something to do with random number generators, they're quite different. `rand::Rng` is a trait, `rand::rngs::ThreadRng` is a struct.

Trait objects make this distinction harder. When used as a function argument and similar places, the form `&Rng` is "a reference to something that implements `Rng`", whereas `&ThreadRng` reads as "a reference a `ThreadRng`".

With time, the distinction between traits and types becomes easier to grasp. Types and traits are used in different places.

Common use cases for trait objects:

- creating collections of heterogeneous objects
- as a return value, they can enable functions to returning multiple concrete types
- supporting *dynamic dispatch*, whereby the function that is called is determined at run-time, rather than compile time

Trait objects are not objects in the sense that an object-oriented programmer would understand. They're perhaps closer to a mixin class. Trait objects don't exist on their own. They're agents of some other type.

An alternative analogy would be a singleton object that is delegated with some authority by another concrete type. In Listing 8.9, the `&Enchanter` is delegated to act on behalf of three concrete types.

## 8.4 TCP

Dropping down from HTTP, we encounter TCP. Rust's standard library provides us with cross-platform tools for making TCP requests. Let's use them.

### Listing 8.10. Project structure for Listing 8.12

```
ch8-stdlib
├── src
│   └── main.rs
└── Cargo.toml
```

### Listing 8.11. Project metadata for Listing 8.12 (ch8/ch8-stdlib/Cargo.toml)

```
[package]
name = "ch8-stdlib"
version = "0.1.0"
authors = ["Tim McNamara <paperless@timmcnamara.co.nz>"]
edition = "2018"

[dependencies]
```

### Listing 8.12. Using the Rust standard library to construct an HTTP GET request

#### using std::net::TcpStream (ch8/ch8-stdlib/src/main.rs)

```
use std::io::prelude::*;
use std::net::TcpStream;

fn main() -> std::io::Result<()> {
    let mut connection = TcpStream::connect("www.rustinaction.com:80")?; ①

    connection.write_all(b"GET / HTTP/1.0")?; ②
    connection.write_all(b"\r\n")?; ③
    connection.write_all(b"Host: www.rustinaction.com")?; ④
    connection.write_all(b"\r\n\r\n")?; ⑤

    std::io::copy(&mut connection, &mut std::io::stdout())?; ⑥

    Ok(())
}
```

- ➊ We need to specify the port (80) explicitly, TcpStream does not know that this will become a HTTP request.
- ➋ GET is the HTTP method, / is the resource we're attempting to access and HTTP/1.0 is the protocol version we're requesting. Why 1.0? It does not support "keep alive" requests, which will allow our stream to close without difficulty.
- ➌ In many networking protocols, \r\n is how a new line is signified.
- ➍ The hostname provided on line 5 is actually discarded once it is converted to an IP address. The Host HTTP header allows the server to know which host we're connecting to.

- 5 Two blank lines signifies that we've finished the request.
- 6 `std::io::copy()` streams bytes from a Reader to a Writer.

### 8.4.1 What is a “port number”?

Port numbers are purely virtual. They are simply `u16` values. Port numbers allow a single IP address to host multiple services.

### 8.4.2 Converting a hostname to an IP address

So far, we've been providing the hostname `www.rustinaction.com` to Rust. But, to send messages over the Internet, the Internet Protocol requires IP addresses. TCP knows nothing about domain names. To convert a domain name to an IP address, we rely on the Domain Name System (DNS) and its process called *domain name resolution*.

We're able to resolve names by asking a server. They're able to recursively ask other servers. Requests can be made over TCP, including encrypted with TLS, but are also sent over UDP. We'll be using that here, because it's more useful for learning purposes.

To explain how the translating from a domain name to an IP address works, we'll create a small application that does the translation. It's called `resolve`, for which Listing 8.16 lists its source code. `resolve` makes use of public DNS services, but you are able to add your own easily with the `-s` argument.

#### **Public DNS providers**

At the time of writing, several companies provide DNS servers for public use. Any of the IP addresses listed here should offer roughly equivalent service.

- 1.1.1.1 and 1.0.0.1 by Cloudflare
- 8.8.8.8 and 8.8.4.4. by Google
- 9.9.9.9 by Quad9, founded by IBM
- 64.6.64.6 and 64.6.65.6 by VeriSign

Domain name resolution takes place in the *domain name system* (DNS). DNS is primarily delivered over UDP, but also makes use of UDP for long messages and an extension called DNSSEC. `resolve` only understands a small portion of DNS and therefore only requires DNS messages.

The project makes uses of an external crate, `trust-dns`, to perform the hard work. `trust-dns` implements the RFC 1035—which defines DNS—and several later RFCs quite faithfully and uses terminology derived from it.

Some of the terms that are useful to understand are outlined in Table 8.1.

**Table 8.1. Terms that are used in RFC 1035, the `trust_dns` crate and Listing 8.16 and how they interlink**

Term	Definition	Representation in Code
<b>Domain Name</b>	A domain name is almost what you probably think of when you use the term “domain name” in everyday language. The technical definition includes some special cases, such as the “root” domain which is encoded as a single dot and domain names needing to be case-insensitive.	Defined in <code>trust_dns::domain::Name</code> <pre>pub struct Name {     is_fqdn: bool, ❶     labels: Vec&lt;Label&gt;, }</pre> <p>❶ “fqdn” stands for “fully-qualified domain name”</p>
<b>Message</b>	A <code>Message</code> is a container format for both requests to DNS servers (called <i>queries</i> ) and responses back to clients (called <i>answers</i> ). Messages must contain a header, but other fields are not required. <code>Message</code> represents this with several <code>Vec&lt;T&gt;</code> fields. They do not need to be wrapped in <code>Option</code> to represent missing values as their length can be 0.	Defined in <code>trust_dns::domain::Name</code> <pre>struct Message {     header: Header,     queries: Vec&lt;Query&gt;,     answers: Vec&lt;Record&gt;,     name_servers: Vec&lt;Record&gt;,     additional: Vec&lt;Record&gt;,     sig0: Vec&lt;Record&gt;, ❶     edns: Option&lt;Edns&gt;, ❷ }</pre> <p>❶ “sig0” is a cryptographically signed record used for verifying the message’s integrity. It is defined in RFC 2535.</p> <p>❷ “edns” indicates whether the message includes “Extended DNS”</p>
<b>Message Type</b>	A message type identifies the message as a query or an answer. Queries can also be updates, which is functionality that our code ignores.	Defined in <code>trust_dns::op::MessageType</code> <pre>pub enum MessageType {     Query,     Response, }</pre>
<b>Message ID</b>	A number that is used for senders to link queries and answers.	<code>u16</code>
<b>Resource Record Type</b>	The resource record type refers to the DNS codes that you’ve probably encountered if you’ve ever configured a domain name. Of note is how <code>trust_dns</code> handles invalid codes. The <code>RecordType</code> enum contains an <code>Unknown(u16)</code> variant that can be used for codes that it doesn’t understand.	Defined in <code>trust_dns::rr::record_type::RecordType</code> <pre>pub enum RecordType {     A,     AAAA,     ANAME,     ANY,     // ...     Unknown(u16),     ZERO, }</pre>
<b>Query</b>	A <code>Query</code> holds the domain name and the record type that we’re seeking the DNS details for. They also describe the DNS class, allows	Defined in <code>trust_dns::op::Query</code> <pre>pub struct Query {     name: Name,     query_type: RecordType,</pre>

	queries to distinguish between messages sent over the Internet from other transport protocols.	query_class: DNSClass, }
Op Code	An OpCode is, in some sense, a subtype of <code>MessageType</code> . This is an extensibility mechanism that allows future functionality. For example, RFC 1035 defines the "Query" and "Status" op codes but others were defined later. "Notify" and "Update" are defined by RFC 1996 and RFC 2136, respectively.	Defined in <code>trust_dns::op::OpCode</code> <code>pub enum OpCode {</code> <code>Query,</code> <code>Status,</code> <code>Notify,</code> <code>Update,</code> }

An unfortunate consequence of the protocol—which is a consequence of reality, I suppose—is that there are many options, types and sub-types involved. The process of constructing a message that asks, “Dear DNS server, what is the IPv4 address for `domain_name`?", is shown in Listing 8.13.

**Listing 8.13. Constructing a DNS message in Rust with `trust-dns` to request an IPv4 address for `domain_name`. (Excerpt from Listing 8.16 )**

```
let mut msg = Message::new();  
①  
msg  
    .set_id(rand::random::<u16>())  
    .set_message_type(MessageType::Query)  
    .set_op_code(OpCode::Query)  
    .add_query(Query::query(domain_name, RecordType::A))  
    .set_recursion_desired(true);  
②  
③  
④
```

- ① A Message has little content of its own, its main role is to be a container for the query that we're adding a few lines down.
- ② We'll just use a random number as our message ID. The expression `rand::random::<u16>()` can be read as “call `random()` from the `rand` crate, returning a `u16` value”.
- ③ To ask for multiple record types, such as AAAA for IPv6 addresses, add extra queries.
- ④ Request that the DNS server asks DNS servers for us on our behalf if it doesn't know the answer.

We're now in a position where we can meaningfully inspect the code. It has the following structure: parse command line arguments, build a DNS message using `trust_dns` types, convert the structured data into a stream of bytes and then send those bytes across the wire. Then we need to accept the response from the server, decode the incoming bytes and print out the result.

The error handling is relatively ugly, with many calls to `unwrap()` and `expect()`. We'll address that problem shortly during [“Ergonomic Error Handling for Libraries”](#).

The end process is a command-line application that's quite simple. Running `resolve` involves very little ceremony. Given a domain name, `resolve` provides an IP address:

```
$ resolve www.rustinaction.com  
35.185.44.232
```

Listing 8.14 outlines the layout of the files required to build `resolve`. The listings Listing 8.15 and Listing 8.16 are the project's source code.

While you are experimenting with the project, you may wish to use some features of `cargo run` to speed up your process:

```
$ cargo run -q -- www.rustinaction.com ①
35.185.44.232
```

- ① `cargo` sends any arguments to the right of `--` to the executable that it is compiling. The `-q` option mutes any intermediate output.

#### **Listing 8.14. Crate structure for `resolve`**

```
ch8/ch8-resolve
└── Cargo.toml
└── src
    └── main.rs
```

#### **Listing 8.15. Crate metadata for `resolve` (ch8/ch8-resolve/Cargo.toml)**

```
[package]
name = "resolve"
version = "0.1.0"
authors = ["Tim McNamara <paperless@timmcnamara.co.nz>"]
edition = "2018"

[dependencies]
rand = "0.6"
clap = "2.33"

[dependencies.trust-dns]
version = "0.16"
default_features = false
```

#### **Listing 8.16. `resolve`: a simple DNS command-line utility that can resolve the IP address for domain names (ch8/ch8-resolve/src/main.rs)**

```
extern crate clap;

use std::net::{SocketAddr, UdpSocket};
use std::time::Duration;

use clap::{App, Arg};
use rand;
use trust_dns::op::{Message, MessageType, OpCode, Query};
use trust_dns::rr::domain::Name;
use trust_dns::rr::record_type::RecordType;
use trust_dns::serialize::binary::*;

fn main() {
```

```

let app = App::new("resolve")
    .about("A simple to use DNS resolver")
    .arg(Arg::with_name("dns-server").short("s").default_value("1.1.1.1"))
    .arg(Arg::with_name("domain-name").required(true))
    .get_matches();

let domain_name_raw = app.value_of("domain-name").unwrap();
let dns_server_raw = app.value_of("dns-server").unwrap();

let mut request_as_bytes: Vec<u8> = Vec::with_capacity(512); ①
let mut response_as_bytes: [u8; 512] = [0; 512]; ②

let domain_name = Name::from_ascii(&domain_name_raw).unwrap(); ③
let mut msg = Message::new(); ④
msg
    .set_id(rand::random::<u16>())
    .set_message_type(MessageType::Query) ⑤
    .add_query(Query::query(domain_name, RecordType::A))
    .set_op_code(OpCode::Query)
    .set_recursion_desired(true); ⑥

let mut encoder = BinEncoder::new(&mut request_as_bytes); ⑦
msg.emit(&mut encoder).unwrap(); ⑦

let localhost = UdpSocket::bind("0.0.0.0:0").expect("cannot bind to local
socket"); ⑧
let timeout = Duration::from_secs(3);
localhost.set_read_timeout(Some(timeout)).unwrap();
localhost.set_nonblocking(false).unwrap();

let dns_server: SocketAddr = format!("{}:53",
dns_server_raw).parse().expect("invalid address");
let _amt = localhost.send_to(&request_as_bytes, dns_server).expect("socket
misconfigured");

let (_amt, _remote) = localhost.recv_from(&mut response_as_bytes).expect("timeout
reached");

let dns_message = Message::from_vec(&response_as_bytes).expect("unable to parse
response");

for answer in dns_message.answers() {
    if answer.record_type() == RecordType::A {
        let resource = answer.rdata();
        let ip = resource.to_ip_addr().expect("invalid IP address received");
        println!("{}: {}", ip.to_string());
    }
}
}

```

① We allocate 512 bytes, even though this isn't strictly necessary. 512 is the number of bytes specified by DNS when messages are sent over UDP.

- ② An implementation detail of `recv_from()` (called later on) is that it relies on the length of the buffer provided to indicate how many bytes to read from the network. `Vec<T>` created with `with_capacity()` has a length of 0, leading to an early return.
- ③ Convert the string to a data type the represents domain names
- ④ A `Message` represents a DNS message, which is a container for queries (and other information, such as answers)
- ⑤ Specify that this is a DNS query, not a DNS answer (they both have the same representation over the wire)
- ⑥ Ask the DNS server to query any DNS servers that it knows about if it doesn't know the answer itself.
- ⑦ Convert the `Message` type into raw bytes with the `BinEncoder`.
- ⑧ 0.0.0.0:0 means "listen to all addresses on a random port", and the actual port will be selected by the operating system.

### **UDP “connections”**

UDP does not have a notion of a long-lived connection. Put another another way, UDP does not have duplex communication. That means to ask a question of a DNS server, both parties must act as clients and servers from the point of view of UDP.

Time to recap. Our overall task is to make HTTP requests. HTTP is built on TCP. But we only have a domain name (`www.rustinction.com`) when we’re making the request, so we need to use DNS. But DNS is primarily delivered over UDP. So we’ve needed to take a diversion and learn about UDP. Now it’s time to return to TCP. Before we’re able to though, we need to learn how to combine error types that emerge from multiple dependencies.

## **8.5 Ergonomic Error Handling for Libraries**

Rust’s error handling is safe and sophisticated. However, it offers a few challenges. When a function incorporates `Result` types from two upstream crates, the `? operator` no longer works because it can only understand a single type. This will prove to be important when we refactor our domain resolution code to work alongside our TCP code. This section discusses some of those challenges and some strategies for managing them.

### **8.5.1 Issue: unable to return multiple error types**

Returning a `Result<T, E>` works great when there is a single error type `E`. But things become more complicated when we want to work with multiple error types.

**TIP**

For single-file examples, compile the code with `rustc <filename>`, rather than using cargo build.

If an example is named `io-error.rs`, then the shell command is: `rustc io-error.rs && ./io-error[.exe]`

To start with, let’s look at a small example that covers the easy case of a single error type. We’ll try to open a file that does not exist.

When run, Listing 8.17 prints out a short message in Rust syntax:

```
Error: Os { code: 2, kind: NotFound, message: "No such file or directory" }
```

We won't win any awards for user experience here, but we get a chance to learn a new language feature.

#### **Listing 8.17. A Rust program that always produces an I/O error (ch8/misc/io-error.rs)**

```
use std::fs::File;

fn main() -> Result<(), std::io::Error> {
    let _f = File::open("invisible.txt")?;

    Ok(())
}
```

Now let's introduce another error type into `main()`. This will produce a compiler error. We'll then work through some options to get the code to compile.

#### **Listing 8.18. A function that attempts to return multiple Result types**

**(ch8/misc/multierror.rs)**

```
use std::fs::File;
use std::net::Ipv6Addr;

fn main() -> Result<(), std::io::Error> {
    let _f = File::open("invisible.txt")?; ①
    let _localhost = ":".parse::<Ipv6Addr>()?; ②

    Ok(())
}
```

① `File::open()` returns `Result<(), std::io::Error>`

② `".".parse::<Ipv6Addr>()` returns `Result<Ipv6Addr, std::net::AddrParseError>`

Compiling Listing 8.18 (use `rustc multierror.rs`) produces quite a stern error message:

```
error[E0277]: the trait bound `std::io::Error: std::convert::From<std::net::AddrParseError>` is not satisfied
--> multierror.rs:6:22
  |
6 |     let _localhost = ":".parse::<Ipv6Addr>()?;
  |     ^^^^^^^^^^^^^^^^^^^^^^^^^^ the trait
`std::convert::From<std::net::AddrParseError>` is not implemented for
`std::io::Error`
  |
= help: the following implementations were found:
  <std::io::Error as std::convert::From<std::ffi::NulError>>
```

```

        <std::io::Error as std::convert::From<std::io::ErrorKind>>
        <std::io::Error as std::convert::From<std::io::IntoInnerError<W>>>
= note: required by `std::convert::From::from`  

  
error: aborting due to previous error
  
For more information about this error, try `rustc --explain E0277`.
```

The error message can be difficult to interpret if you don't know what the question mark operator (?) is doing. What are there multiple messages about `std::convert::From`? The ? operator is syntactic sugar for the `try!` macro. `try!` performs two functions. When it detects `Ok(value)`, the expression evaluates to `value`. When `Err(err)` occurs, `try!/?` returns early after attempting to convert `err` to the error type defined in the calling function.

In Rust-like pseudo-code, the `try!` macro could be defined as:

```
macro try {
    match expression {
        Result::Ok(val) => val,                      ①
        Result::Err(err) => {
            let converted = convert::From::from(err);   ②
            return Result::Err(converted);              ③
        }
    );
}
```

- ① When an expression matches `Result::Ok(val)`, use `val`
- ② When it matches `Result::Err(err)`, convert it to the outer function's error type and then return early.
- ③ This return returns from the calling function, not the `try!` macro itself.

Looking at Listing 8.18 again, we can see the macro in action.

```
fn main() -> Result<(), std::io::Error> {
    let _f = File::open("invisible.txt")?;           ①
    let _localhost = "::1".parse::<Ipv6Addr>()?;  ②

    Ok(())
}
```

- ① `File::open` could evaluate `std::io::Error`, so no conversion is necessary.
- ② `"::1".parse()` presents ? with a `std::net::AddrParseError`. We don't define how to convert `std::net::AddrParseError` to `std::io::Error`, so program fails to compile.

As well as saving you from needing to use explicit pattern matching to extract the value or return an error, the ? operator also attempts to convert its argument into an error type if required. Because the signature of `main` is `main() -> Result<(), std::io::Error>`, Rust is attempting to convert the `std::net::AddrParseError` produced by `parse::<Ipv6Addr>()` into a `std::io::Error`. Don't worry though, we can fix this!

Earlier in the chapter at “Trait Objects”, we introduced trait objects. Now we’ll be able to put them to good use. Using `Box<Error>` as the error variant in the `main()` function allows us to progress.

#### **Listing 8.19. Output from Listing 8.20**

```
Error: Os { code: 2, kind: NotFound, message: "No such file or directory" }
```

I suppose it’s a limited form of progress. We’ve circled around to the error that we started with. But we’ve passed through the compiler error, which is what we wanted. Onwards.

#### **Listing 8.20. Using a trait object in a return value to simplify error handling when errors originate from multiple upstream crates. (ch8/misc/traiterror.rs)**

```
use std::fs::File;
use std::error::Error;
use std::net::Ipv6Addr;

fn main() -> Result<(), Box<Error>> {           ①
    let _f = File::open("invisible.txt")?;          ②
    let _localhost: Ipv6Addr = "::1".parse()?;       ③

    Ok(())
}
```

① `Box<Error>` is a trait object, which represents any type that implements `Error`.

Wrapping trait objects in `Box` is necessary because their size (in bytes on the stack) is unknown at compile-time. In the case of Listing 8.20, the trait object might originate from either `File::open()` or `"::1".parse()`. What actually happens depends on the circumstances encountered at runtime. A `Box` has a known size on the stack. Its raison d’être is to point to things that don’t, such as trait objects.

### **8.5.2 Wrapping downstream errors by defining our own error type**

The problem that we are attempting to solve is that each of our dependencies defines its own error type. Multiple error types in one function prevent returning `Result`. The first strategy we looked at was to use trait objects. But trait objects have a potentially significant downside.

Using trait objects is also known as *type erasure*. Rust is no longer able to know that an error has originated upstream. Using `Box<Error>` as the error variant of a `Result` means that the upstream error types are, in a sense, lost. The original errors are now converted to exactly the same type.

It is possible to retain the upstream errors, but requires some more work on our behalf. We need to bundle upstream errors in our own type. When the upstream errors are needed later, say for reporting errors to the user, it’s possible to extract them with

pattern matching.

Here is the outline:

- Define an enum that includes the upstream errors as variants
- Annotate the enum with `#[derive(Debug)]`
- Implement `Display`
- Implement `Error`, which almost comes for free because we have implemented `Debug` and `Display`
- Use `map_err()` in your code to convert the upstream error to your omnibus error type. `map_err()` isn't function that you have encountered before. We'll explain what it does when we get there.

It's possible to stop there, but there's an optional extra step that improves the ergonomics:

- Implement `std::convert::From` to remove the need to call `map_err()`

To begin, let's start back with the code that we know fails from Listing 8.18 .

```
use std::fs::File;
use std::net::Ipv6Addr;

fn main() -> Result<(), std::io::Error> {
    let _f = File::open("invisible.txt")?;
    let _localhost = ":".parse::<Ipv6Addr>()?;
    Ok(())
}
```

This fails because `".parse::<Ipv6Addr>()` does not return a `std::io::Error`. What we want to end up with is code that looks a little more like Listing 8.21:

#### **Listing 8.21. Hypothetical example of the kind of code that we would like to write**

```
use std::fs::File;
use std::io::Error; ①
use std::net::AddrParseError; ②
use std::net::Ipv6Addr;

enum UpstreamError{
    IO(std::io::Error),
    Parsing(AddrParseError),
}

fn main() -> Result<(), UpstreamError> {
    let _f = File::open("invisible.txt")?.maybe_convert_to(UpstreamError);
    let _localhost = ":".parse::<Ipv6Addr>()?.maybe_convert_to(UpstreamError);

    Ok(())
}
```

- ➊ Bring upstream errors into local scope.

## DEFINE AN ENUM THAT INCLUDES THE UPSTREAM ERRORS AS VARIANTS

The first thing to do is to return a type that can hold the upstream error types. In Rust, an enum works well. Listing 8.21 does not compile, but does do this step. We'll tidy up the imports slightly.

```
use std::io;
use std::net;

enum UpstreamError{
    IO(io::Error),
    Parsing(net::AddrParseError),
}
```

Let's proceed.

### ANNOTATE THE ENUM WITH #[DERIVE(DEBUG)]

Easy. That's a single line change. We add `#[derive(Debug)]` to line 4. The best kind of change.

```
use std::io;
use std::net;

#[derive(Debug)]
enum UpstreamError{
    IO(io::Error),
    Parsing(net::AddrParseError),
}
```

### IMPLEMENT STD::FMT::DISPLAY

We'll cheat slightly and implement `Display` by simply using `Debug`. We know that this is available to us, because errors must define `Debug`.

```
use std::fmt;
use std::io;
use std::net;

#[derive(Debug)]
enum UpstreamError{
    IO(io::Error),
    Parsing(net::AddrParseError),
}

impl fmt::Display for UpstreamError {
    fn fmt(&self, f: &mut fmt::Formatter<'_>) -> fmt::Result { ➊
        write!(f, "{}", self)
    }
}
```

- ➊ Implement `Display` in terms of `Debug` via the "`{:?}`" syntax.

## IMPLEMENT `STD::ERROR::ERROR`

Another easy change. Excellent.

```
use std::error; ➊
use std::fmt;
use std::io;
use std::net;

#[derive(Debug)]
enum UpstreamError{
    IO(io::Error),
    Parsing(net::AddrParseError),
}

impl fmt::Display for UpstreamError {
    fn fmt(&self, f: &mut fmt::Formatter<'_>) -> fmt::Result {
        write!(f, "{:?}", self)
    }
}

impl error::Error for UpstreamError { } ➋
```

- ➊ Bring the `std::error::Error` trait into local scope  
➋ Defer to default method implementations. The compiler will fill in the blanks.

The `impl` block is especially terse. There are default implementations of every method defined by `std::error::Error`, so we're asking the compiler to do all of the work for us.

## USE `MAP_ERR()` IN YOUR CODE TO CONVERT THE UPSTREAM ERROR TO YOUR OMNIBUS ERROR TYPE

Back at Listing 8.21 , we wanted to have a `main()` that looks like this:

```
fn main() -> Result<(), UpstreamError> {
    let _f = File::open("invisible.txt")?.maybe_convert_to(UpstreamError);
    let _localhost = ":1".parse::<Ipv6Addr>()?.maybe_convert_to(UpstreamError);

    Ok(())
}
```

I can't offer you that, but I can give you this:

```
fn main() -> Result<(), UpstreamError> {
    let _f = File::open("invisible.txt").map_err(UpstreamError::IO)?;
    let _localhost = ":1".parse::<Ipv6Addr>().map_err(UpstreamError::Parsing)?;

    Ok(())
}
```

This new code works! Here's how. The `map_err()` function maps an error to a function. Variants of our `UpstreamError` enum can be used as functions here. The `?` operator needs to be at the end. Otherwise the function may have returned before the code has a chance to convert the error.

Listing 8.23 provides the new code. When run, it produces this message to the console:

#### **Listing 8.22. Output from Listing 8.23**

```
----. Error: IO(Os { code: 2, kind: NotFound, message: "No such file or directory"
}) ----.
```

#### **Listing 8.23. Wrapping upstream errors in our own type to retain type safety (ch8/misc/wraperror.rs)**

```
use std::io;
use std::fmt;
use std::net;
use std::fs::File;
use std::net::Ipv6Addr;

#[derive(Debug)]
enum UpstreamError{
    IO(io::Error),
    Parsing(net::AddrParseError),
}

impl fmt::Display for UpstreamError {
    fn fmt(&self, f: &mut fmt::Formatter<'_>) -> fmt::Result {
        write!(f, "{}", self)
    }
}

impl error::Error for UpstreamError { }

fn main() -> Result<(), UpstreamError> {
    let _f = File::open("invisible.txt").map_err(UpstreamError::IO)?;
    let _localhost = ":".parse::<Ipv6Addr>().map_err(UpstreamError::Parsing)?;

    Ok(())
}
```

It's also possible to remove the calls to `map_error()`. To enable that, we need to implement `From`.

#### **IMPLEMENT STD::CONVERT::FROM TO REMOVE THE NEED TO CALL MAP\_ERR()**

The `std::convert::From` trait has a single required method, `from()`. We need two `impl` blocks to enable our two upstream error types to be convertible.

```

impl From<io::Error> for UpstreamError {
    fn from(error: io::Error) -> Self {
        UpstreamError::IO(error)
    }
}

impl From<net::AddrParseError> for UpstreamError {
    fn from(error: net::AddrParseError) -> Self {
        UpstreamError::Parsing(error)
    }
}

```

Now the `main()` returns to a simple form of itself:

```

fn main() -> Result<(), UpstreamError> {
    let _f = File::open("invisible.txt")?;
    let _localhost = ":1".parse::<Ipv6Addr>()?;
    Ok(())
}

```

The full code listing is provided by Listing 8.24 . Implementing `From` places the burden of extra syntax on the library writer. It results in a much easier experience for people using your crate.

**Listing 8.24. Implementing `std::convert::From` for our wrapper error type to simplify its use by downstream programmers (ch8/misc/wraperror2.rs)**

```

use std::io;
use std::fmt;
use std::net;
use std::fs::File;
use std::net::Ipv6Addr;

#[derive(Debug)]
enum UpstreamError{
    IO(io::Error),
    Parsing(net::AddrParseError),
}

impl fmt::Display for UpstreamError {
    fn fmt(&self, f: &mut fmt::Formatter<'_>) -> fmt::Result {
        write!(f, "{:?}", self) // <1> Implement Display in terms of Debug
    }
}

impl error::Error for UpstreamError { }

impl From<io::Error> for UpstreamError {
    fn from(error: io::Error) -> Self {
        UpstreamError::IO(error)
    }
}

```

```

}

impl From<net::AddrParseError> for UpstreamError {
    fn from(error: net::AddrParseError) -> Self {
        UpstreamError::Parsing(error)
    }
}

fn main() -> Result<(), UpstreamError> {
    let _f = File::open("invisible.txt").map_err(UpstreamError::IO)?;
    let _localhost = ":1".parse::<Ipv6Addr>().map_err(UpstreamError::Parsing)?;

    Ok(())
}

```

### 8.5.3 Cheat with unwrap() and expect()

The final approach for dealing with multiple error types is to use `unwrap()` and `expect()`. This is a reasonable approach when writing a `main()` function, but isn't recommended for library authors. Your users don't want their programs to crash because of things outside of their control.

Now that we have the tools to handle multiple error types in a function, we can continue our journey.

## 8.6 MAC addresses

Several pages ago now in Listing 8.16 , you implemented a DNS resolver. That enables conversions from a host name, such as `www.rustinaction.com`, to an IP address. Now that we have an IP address to connect to, we want to connect to it.

The Internet Protocol enables devices to contact each other via their IP addresses. But that's not sufficient. Networking using the Ethernet standards—which, almost everything developed since 1998 or so uses-- a unique identifier for every piece of hardware that's connected.

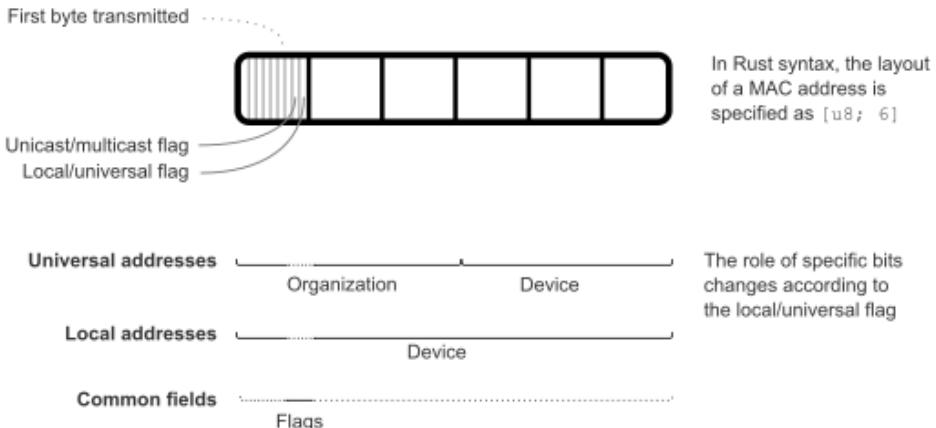
Why a second number? The answer is partially technical and partially historic. Ethernet networking and the Internet started life independently. Ethernet's focus was local area networks. The Internet was developed to enable communication between networks. Ethenet is the addressing system understood by devices that share a physical link. Or a radio link, in the case of WiFi, Bluetooth and other wireless technologies. Perhaps a better way to express this is that MAC addresses are used by devices that share electrons.

IP addresses are hierarchical, but MAC addresses are not. Addresses appearing close together numerically are not close together physically or organizationally.

MAC addresses are 48 bits (6 bytes) wide. IP addresses are 32 bits (4 bytes) for IPv4 and 128 bits (16 bytes) for IPv6.

**Figure 8.3. MAC address in-memory layout**

## MAC Address Layout



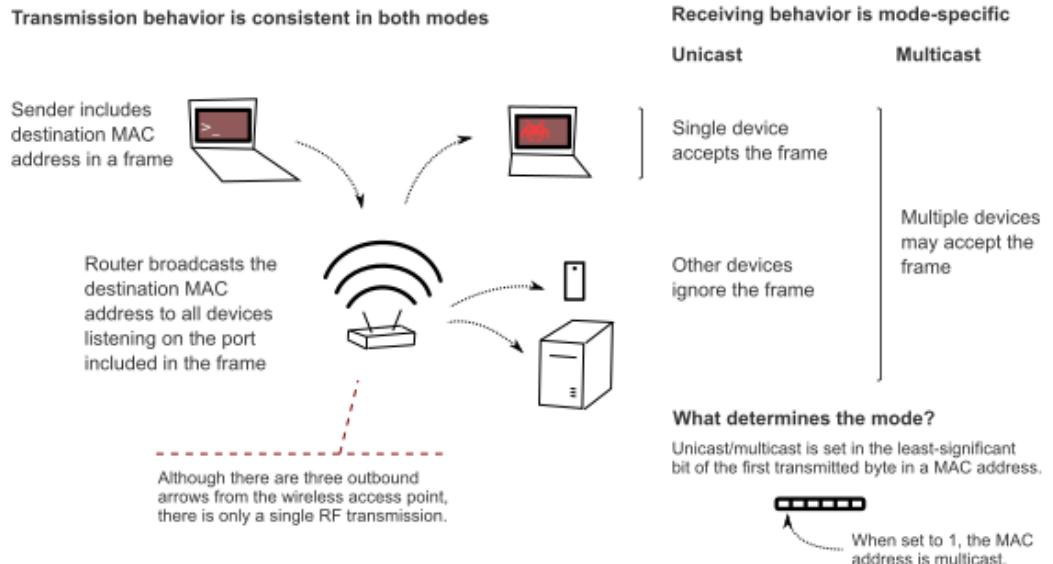
There are 2 forms of MAC address:

- *universally administered addresses* or *universal* are set when devices are manufactured. Manufacturers use a prefix that they are assigned by the IEEE Registration Authority and a scheme of their choosing for the remaining bits
- *locally administered addresses* or *local* allow devices to create their own MAC address without registration. When setting a device's MAC address yourself in software, you should make sure that your address is set to this

MAC addresses have two modes: *unicast* and *multicast*. Their transmission behavior is identical. The distinction is made when a device makes a decision whether to accept a *frame*. A frame is a term used by the Ethernet protocol for a byte slice at this level. Analogies to frame include the terms packet, wrapper and envelope.

**Figure 8.4. The differences between multicast and unicast MAC addresses**

## Unicast vs Multicast MAC Addresses



Unicast addresses are intended to transport information between two points that are in direct contact, say between a laptop and a router. Wireless access points complicate matters somewhat, but don't change the the fundamentals. A multicast address can be accepted

The term *unicast* is somewhat misleading. There is be a broadcast step. Unicast addresses differ in which devices take action on them, not which data is transmitted over the wire (or through the radio waves).

### 8.6.1 Generating MAC addresses

When we begin talking raw TCP later at Listing 8.36 , we'll be creating a virtual hardware device. To convince anything to talk to us, we need to learn how to assign our virtual device a MAC address. The `macgen` project at Listing 8.26 generates MAC addresses.

**Listing 8.25. Crate metadata for macgen (ch8/ch8-mac/Cargo.toml)**

```
[package]
name = "ch8-macgen"
version = "0.1.0"
authors = ["Tim McNamara <paperless@timmcnamara.co.nz>"]
edition = "2018"

[dependencies]
```

```
rand = "0.7"
```

**Listing 8.26. macgen, a MAC address generator (ch8/ch8-mac/src/main.rs)**

```
extern crate rand;

use rand::RngCore;
use std::fmt;
use std::fmt::Display;

#[derive(Debug)]
struct MacAddress([u8; 6]);
```

1

```
impl Display for MacAddress {
    fn fmt(&self, f: &mut fmt::Formatter<'_>) -> fmt::Result {
        let octet = &self.0;
        write!(f,
               "{:02x}:{:02x}:{:02x}:{:02x}:{:02x}:{:02x}",
               octet[0], octet[1], octet[2], octet[3], octet[4], octet[5])
        2
    }
}
```

2

```
}
```

```
impl MacAddress {
    fn new() -> MacAddress {
        let mut octets: [u8; 6] = [0; 6];
        rand::thread_rng().fill_bytes(&mut octets);
        octets[0] |= 0b_0000_0011;
        MacAddress { 0: octets }
    }

    fn is_local(&self) -> bool {
        (self.0[0] & 0b_0000_0010) == 0b_0000_0010
    }

    fn is_unicast(&self) -> bool {
        (self.0[0] & 0b_0000_0001) == 0b_0000_0001
    }
}

fn main() {
    let mac = MacAddress::new();
    assert!(mac.is_local());
    assert!(mac.is_unicast());
    println!("mac: {}", mac);
}
```

3

① Use the newtype pattern to wrap a bare array without any extra overhead

② Convert each byte to hexadecimal notation

③ Force MAC to be locally assigned and unicast by setting the two least-significant bits to 1 with the *bitwise OR assignment operator*

The code from Listing 8.26 should feel legible. Line 25 contains some relatively obscure syntax though. `octets[0] |= 0b_0000_0011` coerces the two flag bits described at Figure 8.3 to the 1 state. That designates every MAC address we generate as locally assigned and unicast.

## 8.7 **Implementing state machines with Rust's enums**

Another pre-requisite for handling network messages is being able to define a state machine. Our code need needs to adapt to changes in connectivity.

Listing 8.36 contains a state machine, implemented with a loop, a `match` and a Rust enum. Because of Rust's expression-based nature, control flow operators also return values. Every time around the loop, the state is mutated in place.

**Listing 8.27. Pseudo-code state machine implementation with a repeated `match` on a enum work together**

```
enum HttpState {
    Connect,
    Request,
    Response,
}

loop {
    state = match state {
        HttpState::Connect if !socket.is_active() => {
            socket.connect();
            HttpState::Request
        }
        HttpState::Request if socket.may_send() => {
            socket.send(data);
            HttpState::Response
        }
        HttpState::Response if socket.can_recv() => {
            received = socket.recv();
            HttpState::Response
        }
        HttpState::Response if !socket.may_recv() => {
            break;
        }
        _ => state,
    }
}
```

More advanced methods to implement finite state machines do exist. This is the simplest, however. We'll be making use of it in Listing 8.36. The best enable the transitions to become part of the type system itself.

## 8.8 Raw TCP

But we're still far too high level! To dig deeper though, we're going to need to get some assistance from the operating system.

Integrating with the raw TCP packets typically requires root/superuser access. The operating system starts to get quite grumpy when an unauthorized user asks to make raw network requests. We can get around this (on Linux) by creating a proxy device that non-super users are allowed to communicate with directly.

### ***Don't have Linux?***

If you're running another operating system, there are many virtualization options available.

- The Multipass project provides very fast Ubuntu virtual machines on macOS and Windows hosts
- On Windows, another option to look into is “WSL”, the “Windows Subsystem for Linux”
- Oracle VirtualBox is an open source project with excellent support for many host operating systems

## 8.9 *Creating a virtual networking device*

The `ip` utility can create TUN/TAP devices. The higher level `tunctl` utility may also be useful here. To create a device called `tap-rust`, execute the command in Listing 8.28 in your Linux console:

### ***Listing 8.28. Command to create a TAP device on Linux 2.2 and above***

```
sudo \          1
ip tuntap \
    add \
        mode tap \
            name tap-rust \
                user $USER      6
```

- ➊ Execute as the root user
- ➋ Tell `ip` that we're managing TUN/TAP devices
- ➌ Use the "add" sub-command
- ➍ Use the "TUN" tunnelling mode
- ➎ Give your device a unique name
- ➏ Grant access to your non-root user account

When successful, `ip` prints no output. To confirm that `tap-rust` has been added, we can use the `ip tuntap list` sub-command.

**Listing 8.29. Command to list TUN/TAP devices**

```
ip tuntap list
```

When executed, you should see the `tap-rust` device in the list of devices in the output.

```
$ ip tuntap list
tap-rust: tap persist user 1000
```

Now that we have created a networking device, we also need to allocate it an IP address and tell our system to forward packets to it.

**Listing 8.30. Commands to enable tap-rust to access the Internet**

```
sudo ip link set tap-rust up
sudo ip addr add 192.168.42.100/24 dev tap-rust

sudo iptables -t nat -A POSTROUTING -s 192.168.42.0/24 -j MASQUERADE
sudo sysctl net.ipv4.ip_forward=1
```

To remove the device once you have completed this chapter, use "del" rather than "add".

**Listing 8.31. Removing the rust TUN device created earlier (ch8/ch8-mget/teardown.sh)**

```
sudo ip tuntap del mode tun name rust
```

## 8.10 “Raw” HTTP

**WARNING**

Large, complicated example ahead. If you're reading the MEAP and feel like it's too long and too complicated, please let me know!

We should now have all the knowledge we need to take on the challenge of using HTTP at the TCP level. The `mget` project (`mget` is short for “**m**anual **g**et”) spans Listing 8.34 and Listing 8.37 .

Each file provides a different role:

- `main.rs` (Listing 8.34 ) handles command-line parsing and weaves together the functionality provided by its peer files. This is where error types are combined using the process outlined at “[Wrapping downstream errors by defining our own error type](#)”.
- `ethernet.rs` (Listing 8.35 ) generates MAC address using the logic from Listing 8.26 and converts between MAC address types defined by `smoltcp` and our own.
- `http.rs` (Listing 8.36) does most of the work. It carries out the work of interacting with the server to make the HTTP request.
- `dns.rs` (Listing 8.37 ) performs DNS resolution using the structure provided earlier

**TIP** The source code for every code listing is available from [www.manning.com/books/rust-in-action](http://www.manning.com/books/rust-in-action).

**NOTE** Important acknowledgement: Listing 8.36 was derived from the HTTP client example within the smoltcp crate itself. whitequark has built an absolutely fantastic networking library.

#### Listing 8.32. File structure for the mget project

```
ch8-mget
├── src
│   ├── main.rs
│   ├── http.rs
│   ├── ethernet.rs
│   └── dns.rs
└── Cargo.toml
```

#### Listing 8.33. Crate metadata for mget (ch8/ch8-mget/Cargo.toml)

```
[package]
name = "mget"
version = "0.1.0"
authors = ["Tim McNamara <paperless@timmcnamara.co.nz>"]
edition = "2018"

[dependencies]
clap = "2.33"
rand = "0.7"
url = "2.0.0"
log = "0.4"
env_logger = "0.6"

[dependencies.trust-dns]
version = "0.16"
default_features = false

[dependencies.smoltcp]
version = "0.5"
default_features = true
features = ["proto-igmp", "proto-ipv4", "verbose", "log"]
```

#### Listing 8.34. mget command line parsing and overall coordination (ch8/ch8-mget/src/main.rs)

```
extern crate log;
extern crate clap;
extern crate env_logger;
extern crate rand;
extern crate smoltcp;
extern crate url;
```

```

use clap::{App, Arg};
use url::Url;
use smoltcp::phy::TapInterface;

mod dns;
mod http;
mod ethernet;

fn main() {
    let app = App::new("mget")
        .about("GET a webpage, manually")
        .arg(Arg::with_name("url").required(true))
        .arg(Arg::with_name("tap-device").required(true))
        .arg(Arg::with_name("dns-server").short("s").default_value("1.1.1.1"))
        .get_matches();

    // read raw values from command-line
    let url_text = app.value_of("url").unwrap();
    let dns_server_text = app.value_of("dns-server").unwrap();
    let tap_text = app.value_of("tap-device").unwrap();

    let url = Url::parse(url_text).expect("unable to parse <url> as a URL");
    if url.scheme() != "http" {
        eprintln!("only HTTP protocol supported");
        return;
    }
    let domain_name = url.host_str().expect("domain name required");

    let _dns_server: std::net::Ipv4Addr = dns_server_text
        .parse()
        .expect("unable to parse <dns-server> as an IPv4 address");

    let tap = TapInterface::new(&tap_text).expect("unable to use <tap-device> as a
network interface");

    let addr = dns::resolve(dns_server_text, domain_name).unwrap().unwrap();

    let mac = ethernet::MacAddress::new().into();

    http::get(tap, mac, addr, url).unwrap();
}

```

**Listing 8.35. Ethernet type conversion and MAC address generation (ch8/ch8-mget/src/ethernet.rs)**

```

extern crate rand;

use std::fmt;
use std::fmt::Display;

use rand::RngCore;

```

```

use smoltcp::wire;

#[derive(Debug)]
pub struct MacAddress([u8; 6]);

impl Display for MacAddress {
    fn fmt(&self, f: &mut fmt::Formatter<'_>) -> fmt::Result {
        let octet = &self.0;
        write!(f, "{:02x}:{:02x}:{:02x}:{:02x}:{:02x}:{:02x}",
            octet[0], octet[1], octet[2], octet[3], octet[4], octet[5]
        )
    }
}

impl MacAddress {
    pub fn new() -> MacAddress {
        let mut octets: [u8; 6] = [0; 6];
        rand::thread_rng().fill_bytes(&mut octets);
        octets[0] |= 0b_0000_0011;
        MacAddress { 0: octets }
    }
}

impl Into<wire::EthernetAddress> for MacAddress {
    fn into(self) -> wire::EthernetAddress {
        wire::EthernetAddress { 0: self.0 }
    }
}

```

**Listing 8.36. Manually creating an HTTP request, using TCP primitives (ch8/ch8-mget/src/http.rs)**

```

use std::collections::BTreeMap;
use std::fmt;
use std::net::IpAddr;
use std::os::unix::io::AsRawFd;

use smoltcp::iface::{EthernetInterfaceBuilder, NeighborCache, Routes};
use smoltcp::phy::TapInterface;
use smoltcp::phy::wait as phy_wait;
use smoltcp::socket::{SocketSet, TcpSocket, TcpSocketBuffer};
use smoltcp::time::Instant;
use smoltcp::wire::{EthernetAddress, IpAddress, IpCidr, Ipv4Address};
use url::Url;

#[derive(Debug)]
enum HttpState {
    Connect,
    Request,
    Response,
}

```

```

#[derive(Debug)]
pub enum UpstreamError {
    Network(smoltcp::Error),
    InvalidUrl,
    Content(std::str::Utf8Error),
}

impl fmt::Display for UpstreamError {
    fn fmt(&self, f: &mut fmt::Formatter<'_>) -> fmt::Result {
        write!(f, "{}", self)
    }
}

impl From<smoltcp::Error> for UpstreamError {
    fn from(error: smoltcp::Error) -> Self {
        UpstreamError::Network(error)
    }
}

impl From<std::str::Utf8Error> for UpstreamError {
    fn from(error: std::str::Utf8Error) -> Self {
        UpstreamError::Content(error)
    }
}

fn random_port() -> u16 {
    49152 + rand::random::<u16>() % 16384
}

pub fn get(tap: TapInterface, mac: EthernetAddress, addr: IpAddr, url: Url) ->
Result<(), UpstreamError> {
    let domain_name = url.host_str().ok_or(UpstreamError::InvalidUrl)?;

    let neighbor_cache = NeighborCache::new(BTreeMap::new());

    let tcp_rx_buffer = TcpSocketBuffer::new(vec![0; 1024]);
    let tcp_tx_buffer = TcpSocketBuffer::new(vec![0; 1024]);
    let tcp_socket = TcpSocket::new(tcp_rx_buffer, tcp_tx_buffer);

    let ip_addrs = [
        IpCidr::new(IpAddress::v4(192, 168, 42, 1), 24),
    ];

    let fd = tap.as_raw_fd();
    let mut routes = Routes::new(BTreeMap::new());
    let default_gateway = Ipv4Address::new(192, 168, 20, 1);
    routes.add_default_ipv4_route(default_gateway).unwrap();
    let mut iface = EthernetInterfaceBuilder::new(tap)
        .ethernet_addr(mac)
        .neighbor_cache(neighbor_cache)
        .ip_addrs(ip_addrs)
        .routes(routes)
        .finalize();
}

```

```

let mut sockets = SocketSet::new(vec![]);
let tcp_handle = sockets.add(tcp_socket);

let http_header = format!(
    "GET {} HTTP/1.0\r\nHost: {}\r\nConnection: close\r\n\r\n",
    url.path(),
    domain_name,
);
}

let mut state = HttpState::Connect;
'http: loop {
    let timestamp = Instant::now();
    match iface.poll(&mut sockets, timestamp) {
        Ok(_) => {}
        Err(e) => { // 
            eprintln!("error: {:?}", e);
        }
    }
}

{
    let mut socket = sockets.get::<TcpSocket>(tcp_handle);

    state = match state {
        HttpState::Connect if !socket.is_active() => {
            eprintln!("connecting");
            socket.connect((addr, 80), random_port())?;
            HttpState::Request
        }
        HttpState::Request if socket.may_send() => {
            eprintln!("sending request");
            socket.send_slice(http_header.as_ref())?;
            HttpState::Response
        }
        HttpState::Response if socket.can_recv() => {
            socket.recv(|raw_data| {
                let output = String::from_utf8_lossy(raw_data);
                println!("{}: {}", raw_data.len(), output);
            })?;
            HttpState::Response
        }
        HttpState::Response if !socket.may_recv() => {
            eprintln!("received complete response");
            break 'http;
        }
        _ => state,
    }
}

phy_wait(fd, iface.poll_delay(&sockets, timestamp)).expect("wait error");
}

```

```
    Ok(())
}
```

**Listing 8.37. Creating DNS queries to translate domain names to IP addresses (ch8/ch8-mget/src/dns.rs)**

```
use std::error::Error;
use std::net::{SocketAddr, UdpSocket};
use std::time::Duration;

use trust_dns::op::{Message, MessageType, OpCode, Query};
use trust_dns::proto::error::ProtoError;
use trust_dns::rr::domain::Name;
use trust_dns::rr::record_type::RecordType;
use trust_dns::serialize::binary::*;

fn message_id() -> u16 {
    let candidate = rand::random();
    if candidate == 0 {
        return message_id();
    }
    candidate
}

#[derive(Debug)]
pub enum DnsError {
    ParseDomainName(ProtoError),
    ParseDnsServerAddress(std::net::AddrParseError),
    Encoding(ProtoError),
    Decoding(ProtoError),
    Network(std::io::Error),
    Sending(std::io::Error),
    Receiving(std::io::Error),
}

impl std::fmt::Display for DnsError {
    fn fmt(&self, f: &mut std::fmt::Formatter) -> std::fmt::Result {
        write!(f, "{:#?}", self)
    }
}

impl std::error::Error for DnsError {
    // use default methods
}

pub fn resolve(dns_server_address: &str, domain_name: &str) -> Result<Option<std::net::IpAddr>, Box<Error>> {
    // input parsing
    let domain_name =
        Name::from_ascii(domain_name).map_err(DnsError::ParseDomainName)?;
    let dns_server_address = format!("{}:53", dns_server_address);
    let dns_server: SocketAddr =
```

```

dns_server_address.parse().map_err(DnsError::ParseDnsServerAddress)?;

// allocate buffers
let mut request_buffer: Vec<u8> = Vec::with_capacity(50);
let mut response_buffer: [u8; 512] = [0; 512]; ❶

let mut request = Message::new();
request.add_query(Query::query(domain_name, RecordType::A)); ❷
request
    .set_id(message_id())
    .set_message_type(MessageType::Query)
    .set_op_code(OpCode::Query)
    .set_recursion_desired(true); ❸

let timeout = Duration::from_secs(5);
let localhost = UdpSocket::bind("0.0.0.0:0").map_err(DnsError::Network)?; ❹
localhost.set_read_timeout(Some(timeout)).map_err(DnsError::Network)?;
localhost.set_nonblocking(false).map_err(DnsError::Network)?;

let mut encoder = BinEncoder::new(&mut request_buffer);
request.emit(&mut encoder).map_err(DnsError::Encoding)?;

let _n_bytes_sent = localhost
    .send_to(&request_buffer, dns_server)
    .map_err(DnsError::Sending)?;

loop { ❺
    let (_n_bytes_recv, remote_port) = localhost.recv_from(&mut
response_buffer).map_err(DnsError::Receiving)?;
    if remote_port == dns_server {
        break;
    }
}

let response = Message::from_vec(&response_buffer).map_err(DnsError::Decoding)?;
for answer in response.answers() {
    if answer.record_type() == RecordType::A {
        let resource = answer.rdata();
        let server_ip = resource.to_ip_addr().expect("invalid IP address received");
        return Ok(Some(server_ip));
    }
}

Ok(None)
}

```

- ❶ DNS over UDP uses a maximum packet size of 512 bytes
- ❷ DNS messages can hold multiple queries, but here we're only using a single one
- ❸ Ask the DNS server that we're connecting to make requests on our behalf if it doesn't know the answer
- ❹ Binding to port 0 asks the operating system to allocate a port on our behalf

- 5 There is a minuscule chance another UDP message will be received on our port from some unknown sender. To avoid that, we ignore packets from IP addresses that we don't expect.

`mget` is an ambitious project. It brings together all the threads from the chapter, is dozens of lines long and yet is less capable than `request::get(url)` call we made at Listing 8.7 . Hopefully it's revealed several interesting avenues for you to explore. Perhaps surprisingly, there are several more networking layers to unwrap.

## 8.11 Wrapping Up

Well done for making your way through a lengthy and challenging chapter.

You have learned:

- implementing `std::fmt::Display` with little fuss in terms of `std::fmt::Debug`
- resolving domain names to IP addresses
- parsing input to your Rust programs safely, such as creating type-safe IP addresses from raw strings with `"127.0.0.1".parse::<Ipv4Addr>()`.
- generating valid MAC addresses
- what the question mark operator (the `try!` macro) is doing under the hood and why compile errors mention conversion traits
- using a `loop` and `match` with an `enum` to implement a simple finite state machine
- creating wrapper error types with an `enum`, then implementing `std::convert::Format` on the upstream errors to enable your `enum` to work with the `?` operator
- implementing the `std::error::Error` trait by implementing `std::fmt::Display` and `std::fmt::Debug`, then using default implementations of the required methods
- using trait objects to create a collection of heterogeneous objects



# *Time and Time Keeping*

***This chapter covers:***

- how a computer keeps time
- how operating systems represent timestamps
- synchronize with the world's atomic clocks with the Network Time Protocol (NTP)

During this chapter, you'll be producing an NTP client that can request the current time from the world's network of public time servers. It's a fully-functioning client that can be included into your own computer's boot process to keep it in sync with the world.

Understanding of how time works within computers supports your efforts to build resilient applications. The system's clock jumps both backwards and forwards in time. Knowing why this happens will allow you to anticipate and prepare for that eventuality.

Your computer also contains multiple physical and virtual clocks. It takes some knowledge to understand the limitations of each and when they're appropriate. Understanding the limitations of each should foster a healthy skepticism of micro benchmarks and other time-sensitive code.

Some of the hardest software engineering involves distributed systems that need to agree on what the time is. If you have the resources of Google, then you're able to maintain a network atomic clocks that provide a worldwide time synchronization of 7ms. The closest open source alternative is CockroachDB. It relies on the Network Time Protocol (NTP), which may have a (worldwide) latency of approximately dozens of milliseconds. But that doesn't make it useless. When deployed within a local network, NTP allows computers to agree on the time to within a few milliseconds or

less.

On the Rust side of the equation, this chapter invests lots of time interacting with the operating system internals. You'll become more confident with unsafe blocks and using raw pointers. Readers will become familiar with `chrono`, the *de facto* standard crate for high-level time and clock operations.

## 9.1 Background

It's easy to think that a day has 86,400 seconds.  $60 \text{ seconds} \times 60 \text{ minutes} \times 24 \text{ hours} = 86400$ . But the Earth's rotation isn't quite that perfect. The length of each day fluctuates due to tidal friction with the moon and other effects such as torque at the boundary of the Earth's core and its mantle.

Software does not tolerate these imperfections. Most systems assume that most seconds have an equal duration. The mismatch presents several problems. In 2012, a large number of services—including high profile sites such as Reddit and Mozilla's Hadoop infrastructure—running stopped functioning after a leap second was added to their clocks. And at times, clocks can go back in time too. Few software systems are prepared for the same timestamp to appear twice. That makes it very difficult to debug the logs.

There are two options for resolving this impasse:

- keep the length of each second fixed—which is good for computers, while being irritating for humans. Over time, “midday” will drift towards sunset or sunrise.
- adjust the length of each year to keep the sun's position relative to noon in the same place from year to year—good for humans, but sometimes highly irritating for computers

In practice, both options have been chosen. The world's atomic clocks use their own time zone with fixed-length seconds called TAI. Everything else uses time zones that are periodically adjusted called UTC.

TAI is spoken by the world's atomic clocks and they maintain a fixed-length year. UTC adds leap seconds to IAT about once every 18 months. In 1972, IAT and UTC were 10 seconds apart. By 2016, they had drifted to 36 seconds apart.

As well as the issues with Earth's fickle rotational speed, the physics of your own computer make it very challenging to keep accurate time. There are also (at least) two clocks running on your system. One is a battery-powered device called the real-time clock. The other one is known as *system time*. System time increments itself based on *hardware interrupts* provided by the computer's motherboard. Somewhere in your system, a quartz crystal is oscillating rapidly.

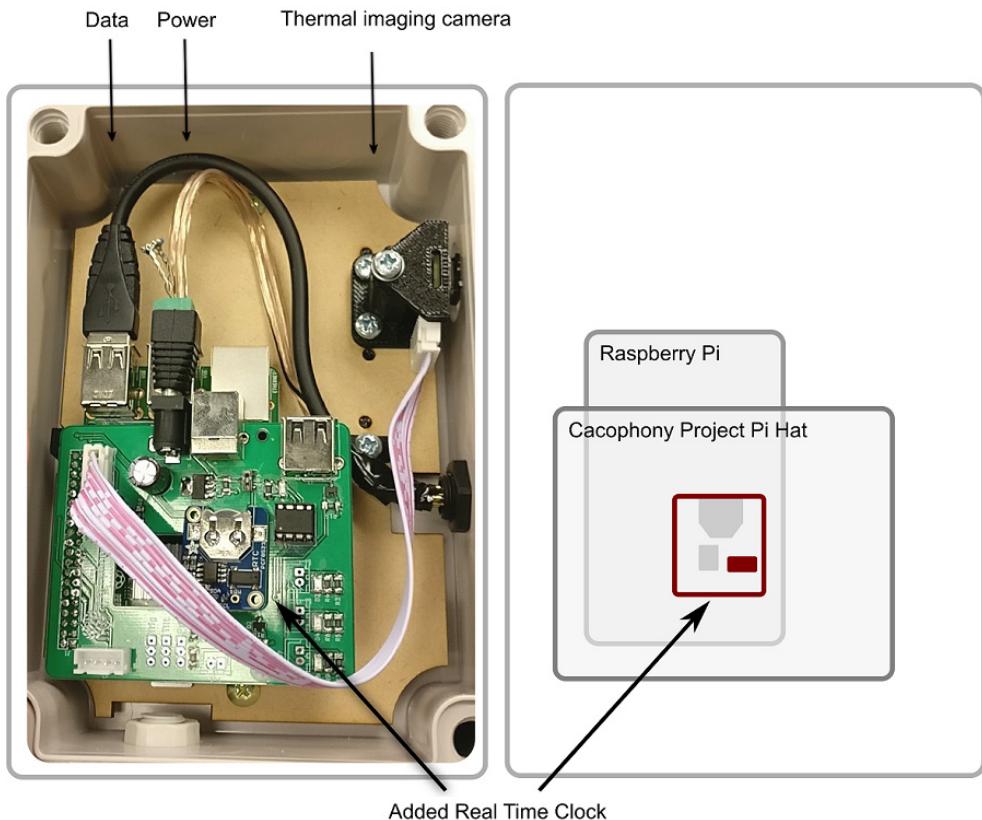
### **Dealing with hardware platforms without a real-time clock**

The Raspberry Pi does not include a battery-supported real-time clock. When the computer turns on, the system clock is set to the epoch time. During boot, it uses the network time protocol (NTP) to identify the current time.

What about situations where there is no network connection? This is the situation faced by the Cacophony Project, which develops devices to support New Zealand's native bird species by applying computer vision to accurately identify pest species.

The main sensor of the device is a thermal imaging camera. Footage needs to be annotated with accurate timestamps. To enable this, the Cacophony Project team decided to add an additional real-time clock to their custom board, known as a "Raspberry Pi Hat"

**Figure 9.1. Viewing the internals of a prototype for the Cacophony Project's automated pest detection system**



## 9.2 Sources of Time

Computers can't look at the clock on the wall to determine what time it is. They need to figure it out by themselves. To explain how this happens, let's consider how digital clocks operate generally, then consider how computer systems operate given some difficult constraints, such as operating without power.

Digital clocks consist of two main parts. The first part is some component that ticks at regular intervals. The second part is a pair of counters. One counter increments as ticks

occur. The other increments as seconds occur.

Determining "now" within digital clocks means comparing up the number of seconds against some pre-determined starting point. The starting point is known as the *epoch*.

Embedded hardware aside, when your computer is turned off, a small battery-powered clock is running. Its electric charge causes a quartz crystal to oscillate rapidly. The clock measures those oscillations and updates its internal counters.

In a running computer, the CPU clock frequency becomes the source of regular ticks. A CPU core operates at a fixed frequency.<sup>21</sup> Inside the hardware, a counter can be accessed via CPU instructions<sup>22</sup> and/or by accessing pre-defined CPU registers.

Relying on a CPU's clock can actually cause problems in niche scientific and other high-accuracy domains, such as profiling an application's behaviour. When computers use multiple CPUs, which is especially common in high performance computing, each CPU has a slightly different clock rate. Moreover, CPUs perform out-of-order execution. This means that it's impossible for someone creating a benchmarking/profilling software suite to deterministically know long a function has taken between two timestamps. The CPU instructions requesting the current timestamp may have been shifted around.

### 9.3 Definitions

Unfortunately, this chapter needs to introduce some jargon that will be important to be able to refer to for anyone looking deeply into the subject matter.

#### `absolute time`

A term to describe the time that you would tell someone if they were to ask for the time. Also referred to as *wall clock* time and *calendar time*.

#### `realtime clock`

The *realtime clock* is a physical clock that's embedded into the computer's motherboard that keeps time when power is off. Also known as the *CMOS clock*.

#### `system clock`

The operating system's view of the time is known as the *system clock*. Upon boot, the operating system takes over timekeeping duties from the realtime clock. All applications derive their idea of the time from the system time. The *system clock* experiences jumps, as it can be manually set to a different position. This can jumpiness can confuse some applications.

#### `monotonically increasing`

A *monotonically increasing* clock never provides the same time twice. This is a useful property for a computer application, as log messages will never have a

<sup>21</sup> Dynamic adjustments to a CPU's clock speed do occur in many processors to conserve power, but they happen infrequently enough from the point of view of the clock that they're insignificant.

<sup>22</sup> For example, Intel-based processors support the RDTSC instruction, which stands for "Read Time Stamp Counter".

repeated timestamp among other advantages. Unfortunately, preventing time adjustments means being permanently bound to the local clock's skew. The *system clock* is not monotonically increasing.

#### **steady clock**

A *steady clock* provides two guarantees: 1) its seconds are all equal length, and 2) it is *monotonically increasing*. Values from steady clocks are unlikely to align to the *system clock* time or absolute time. They typically start at 0 when computers boot up, then count upwards as an internal counter progresses. Although potentially useless for knowing the absolute time, they are very handy calculating the duration between two points in time.

#### **high accuracy**

A clock is highly accurate if the length of its seconds are regular. The difference between two clocks is known as *skew*. Accurate clocks have very little skew against the atomic clocks that are humanity's best engineering effort at keeping accurate time.

#### **high resolution**

A *high resolution* clock is able to give accuracy down to 10 nanoseconds, or perhaps below. High resolution clocks are typically implemented within CPU chips, as there are few devices that can maintain time at such high frequency. CPUs are able to do this, because their units of work are measured in cycles and cycles have the same duration. A 1Ghz CPU core takes 1 nanosecond to compute 1 cycle.

#### **fast clock**

A *fast clock* takes very little time to read the time. Fast clocks sacrifice accuracy and precision for speed.

## **9.4 Encoding Time**

There are many ways to represent time within a computer. The typical approach is use a pair of 32-bit integers. The first counts the number of seconds that have elapsed. The second represents a fraction of a second. The precision of the fractional part depends on the device in question.

The starting point is arbitrary. The most common epoch in UNIX-based systems is 1 Jan 1970 UTC. Alternatives include 1 Jan 1900 (which happens to be used by NTP), 1 Jan 2000 for more recent applications and 1 Jan 1601, which is the beginning of the Gregorian calendar.

Using fixed-width integers presents two main advantages and two main challenges:

- Advantages
  - simplicity: it's very easy to understand the format
  - efficiency: integer arithmetic is the CPU's favorite activity

- Disadvantages
  - fixed-range: all fixed-integer types are finite, implying that time will eventually wrap around to 0 again
  - imprecise: integers are discrete, while time is continuous. Different systems make different trade offs relating to sub-second accuracy, leading to rounding errors.

It's also important to note that the general approach is inconsistently implemented. Here are some things seen in the wild to represent the seconds component:

- UNIX timestamps - 32 bit integer - milliseconds since “epoch”, e.g. 1 Jan 1970.
- MS Windows FILETIME structures (since Windows 2000) - 64bit unsigned integer - 100 nanosecond increments since 1 Jan 1601 (UTC)
- Rust community's `chronos` crate - 32 bit signed integer - used to implement the `NaiveTime`, alongside an enum to represent timezones where appropriate. Has relatively few quirks. One of which is sneaking leap seconds into the nanoseconds field.
- `time_t` (meaning “time type”, but also called simple time or calendar time) within the C standard library (`libc`)
  - Dinkumware's `libc` - `unsigned long int`, e.g. a 32-bit unsigned integer
  - GNU `libc` - `long int`, e.g. a 32-bit signed integer
  - AVR `libc` - uses a 32-bit unsigned integer, and its epoch begins on Midnight, 1 January 2000 UTC ([www.nongnu.org/avr-libc/user-manual/time\\_8h\\_source.html](http://www.nongnu.org/avr-libc/user-manual/time_8h_source.html))

Fractional parts tend to use the same type as their whole-second counterparts, but this isn't guaranteed.

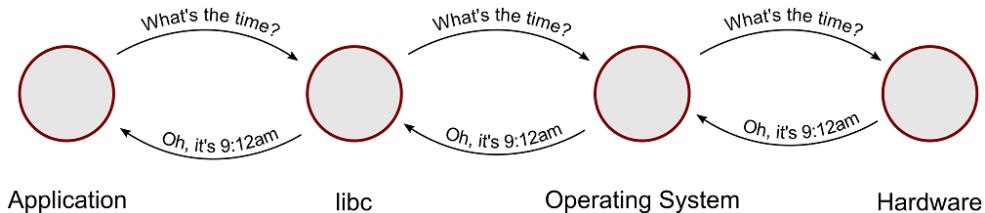
#### **9.4.1 Representing time zones**

Time zones are political divisions, rather than technical ones. A soft consensus appears to have been formed around storing another integer that represents the number of seconds offset from UTC.

### **9.5 *clock v0.1.0: Teaching an application how to tell the time***

To begin coding our NTP client, let's start by learning how to read the time.

**Figure 9.2. How an application tells time time. It gets this information from the operating system, usually via functionality provided by the system's libc implementation.**



Listing 9.2 might almost feel too small to be a fully-fledged example. Running the code will result in the current timestamp formatted according to the ISO 8601 standard.

**Listing 9.1. Crate configuration for Listing 9.2 (ch9/ch9-clock0/Cargo.toml)**

```

[package]
name = "clock"
version = "0.1.0"
authors = ["Tim McNamara <code@timmcnamara.co.nz>"]

[dependencies]
chrono = "0.4"
  
```

**Listing 9.2. Reading the system time in the local time zone and printin it to the screen  
(ch9/ch9-clock0/src/main.rs)**

```

extern crate chrono;          ①
use chrono::Local;            ②

fn main() {
    let now = Local::now();
    println!("{}", now);
}
  
```

① Mark the chrono crate as visible from within this one.

② Bring chrono::Local into local scope. Local is a type that understand's the local system's time zone.

There is lots of complexity being hidden by these 8 lines of code. Much of it will be peeled away during the course of the chapter.

The magic is provided by chrono::Local. It returns a typed value that contains a time zone. Attempts to interact with timestamps that don't include time zones, or to perform other forms of illegal time arithmetic, result in the program refusing to compile.

## 9.6 *clock v0.1.1: Formatting timestamps to comply with ISO 8601 and email standards*

The application that we'll be creating is called `clock`. `clock` reports the current time. During the chapter, it will be incrementally enhanced to support setting the time manually and via NTP.

For the moment, compiling the code from Listing 9.9 and sending the `--use-standard timestamp` flag should produce something like the following output:

**Listing 9.3. Output from compiling and running the code of `clock v0.1.1`, provided at Listing 9.9**

```
$ cd path/to/ch9/ch9-clock1
$ cargo run -- --use-standard timestamp
...
Compiling clock v0.1.1 (file:///path/to/ch9/ch9-clock1)
warning: method is never used: `set`  

--> src\main.rs:15:5
|
15 |     fn set() -> ! {
|     ^^^^^^^^^^
|
= note: #[warn(dead_code)] on by default

    Finished dev [unoptimized + debuginfo] target(s) in 1m 10s
        Running `target/debug/clock --use-standard timestamp`
1529190417
```

- ① Two dashes after a `cargo` command send the remaining arguments to the application that's being built
- ② Listing 9.9, includes a placeholder function that is not implemented.
- ③ This integer is the timestamp provided by `clock`.

### 9.6.1 *Refactoring the `clock v0.1.0` code to support wider architecture*

It makes sense to spend a short period of time creating a scaffold for the larger application that `clock` will become.

Within `clock`, we'll make a small cosmetic change. Rather than using functions to read the time and adjust it, we'll use static methods of a struct `Clock`.

**Listing 9.4. Excerpt from Listing 9.9 showing the change from Listing 9.2 relating to how the time is read from the local system clock**

```
use chrono::DateTime;
use chrono::Local;

struct Clock;
```

```
impl Clock {
    fn get() -> DateTime<Local> {      ①
        Local::now()
    }

    fn set() -> ! {
        unimplemented!()
    }
}
```

① `DateTime<Local>` is a Datetime with the Local timezone information

`Clock` is purely acting as a namespace at this stage. Adding a struct in now provides some extensibility later on. As the application grows, it might become useful for `Clock` to contain some state between calls or implement some trait to support some new functionality.

**TIP** A struct with no fields is known as a "zero sized" type. It will not occupy any memory in the resulting application and is purely a compile-time construct.

## 9.6.2 Formatting the time as a UNIX timestamp or a formatted string according to ISO 8601, RFC 2822, and RFC 3339

Timestamps that will be sent to out-bound to `stdout` are produced using functionality provided by `chrono`:

**Listing 9.5. Excerpt from Listing 9.9 showing the methods used to format dates**

```
let now = Clock::get();
match std {
    "timestamp" => println!("{}", now.timestamp()),
    "rfc2822"   => println!("{}", now.to_rfc2822()),
    "rfc3339"   => println!("{}", now.to_rfc3339()),
    _ => unreachable!(),
}
```

`clock` (thanks to `chrono`) supports three time formats. ISO 8601 support is provided by the RFC 3339, which is a slightly stricter standard. Every RFC 3339-compliant timestamp is an ISO 8601-compliant timestamp, but the inverse is not true.

Here is an excerpt from a command-line session that demonstrates each of the options:

```
$ cargo run -q          ①
2018-06-17T11:25:19.467585800+12:00 ②

$ cargo run -q --use-standard rfc2822
Sun, 17 Jun 2018 11:23:18 +1200

$ cargo run -q --use-standard rfc3339
2018-06-17T11:23:52.865697400+12:00
```

```
$ cargo run -q --use-standard timestamp
1529191458
```

- ① Passing `-q` (for “quiet”), silences intermediate output from cargo
- ② RFC 3339 / ISO 8601 is the default output format

### 9.6.3 Providing a full command-line interface

Command line arguments are part of the environment provided to an application from its operating system when it’s established. They’re raw strings.

Rust provides some support for accessing the raw `Vec<String>` via `std::env::args`, but it can be tedious to develop lots of parsing logic for moderately sized applications. Our code wants to be able to validate certain input—for example that the desired output format is one that `clock` actually supports—and validating input tends to be irritatingly complex. To avoid this frustration, `clock` makes use of the `clap` crate.

`clap` provides facilities for constructing command line **applications**. In particular, it makes the task of interpreting command-line arguments and providing help documentation. There are two main types that are useful for getting started: `clap::App` and `clap::Arg`. Each `clap::Arg` represents a command-line argument and the options that it can represent. `clap::App` collects them into a single application.

To support the public API at Table 9.1, the code at Listing 9.6 uses three `Arg` structs that are wrapped together within a single `App`:

**Table 9.1. Usage examples for executing `clock` application from the command-line, each of which need to be supported by our parser**

Usage	Description	Example output
<code>clock</code>	Default usage. Print the current time.	2018-06-17T11:25:19.467585800+12:00
<code>clock get</code>	Provide “get” action explicitly with default formatting.	2018-06-17T11:25:19.467585800+12:00
<code>clock get --use-standard timestamp</code>	Provide “get” action and a formatting standard.	1529191458
<code>clock get -s timestamp</code>	Provide “get” action and a formatting standard using shorter notation.	1529191458
<code>clock set &lt;datetime&gt;</code>	Provide “set” action explicitly with default parsing rules.	
<code>clock set --use-standard timestamp &lt;datetime&gt;</code>	Provide “set” action explicitly and indicate that the input will be a UNIX timestamp.	

**Listing 9.6. Excerpt from Listing 9.9, demonstrating the use of clap to parse command-line arguments**

```
let app = App::new("clock")
    .version("0.1.1")
    .about("Gets and sets (aspirationally) the time.")
    .arg(Arg::with_name("action")
        .takes_value(true)
        .possible_values(&["get", "set"])
        .default_value("get"))
    .arg(Arg::with_name("std")
        .short("s")
        .long("use-standard")
        .takes_value(true)
        .possible_values(&["rfc2822", "rfc3339", "timestamp"])
        .default_value("rfc3339"))
    .arg(Arg::with_name("datetime")
        .help("When <action> is 'set', apply <datetime>. Otherwise, ignore."));

let args = app.get_matches();
```

clap creates some usage documentation on your behalf. This can be read from the project's root directory:

**Listing 9.7. Reviewing the automatically generated usage documentation for clock**

```
$ cd /path/to/ch9/ch9-clock1
$ cargo run -q -- --help
clock 0.1
①
Gets and sets (aspirationally) the time.

USAGE:
  clock.exe [OPTIONS] [ARGS]

FLAGS:
  -h, --help      Prints help information
  -V, --version   Prints version information

OPTIONS:
  -s, --use-standard <std>      [default: rfc3339]  [possible values: rfc2822,
  rfc3339, timestamp]

ARGS:
  <action>       [default: get]  [possible values: get, set]
  <datetime>     When <action> is 'set', apply <datetime>. Otherwise, ignore.
```

① Execute cargo run "quietly" (with -q) and send --help to the resulting binary

**Listing 9.8. Crate configuration for Listing 9.9 (ch9/ch9-clock1/Cargo.toml)**

```
[package]
name = "clock"
version = "0.1.1"                                     ①
authors = ["Tim McNamara <code@timmcnamara.co.nz>"]

[dependencies]
chrono = "0.4"
clap = "2"                                         ②
```

① The version number has been incremented by 0.0.1.

② A new dependency has been added. We'll pin to the major version of the clap crate.

#### **9.6.4 The full clock v0.1.1 code listing**

With the pre-requisite knowledge covered, let's move to seeing everything in a single place.

**Listing 9.9. Producing formatted dates from the command line (ch9/ch9-clock1/src/main.rs)**

```
extern crate chrono;
extern crate clap;

use clap::{App, Arg};
use chrono::DateTime;
use chrono::Local;

struct Clock;

impl Clock {
    fn get() -> DateTime<Local> {
        Local::now()
    }

    fn set() -> ! {
        unimplemented!()
    }
}

fn main() {
    let app = App::new("clock")
        .version("0.1.1")
        .about("Gets and sets (aspirationally) the time.")
        .arg(Arg::with_name("action")
            .takes_value(true)
            .possible_values(&["get", "set"])
            .default_value("get"))
        .arg(Arg::with_name("std")
            .short("s"))
```

```

    .long("use-standard")
    .takes_value(true)
    .possible_values(&["rfc2822", "rfc3339", "timestamp"])
    .default_value("rfc3339"))
    .arg(Arg::with_name("datetime")
        .help("When <action> is 'set', apply <datetime>. Otherwise, ignore."));

let args = app.get_matches();

let action = args.value_of("std").unwrap();                      ①
let std = args.value_of("std").unwrap();                          ①

if action == "set"
    unimplemented!()                                              ②
}

let now = Clock::get();
match std {
    "timestamp" => println!("{}", now.timestamp()),
    "rfc2822"   => println!("{}", now.to_rfc2822()),
    "rfc3339"   => println!("{}", now.to_rfc3339()),
    _            => unreachable!(),
}
}
}

```

① A default value has been supplied to each of these arguments, so it's safe to unwrap() here.

② Abort early as we're not ready for setting the time yet.

## 9.7 *clock v0.1.2: Setting the time*

Setting the time is complicated by the fact that each operating system has its own mechanism for doing so. This requires that we use operating system-specific conditional compilation to create a cross-portable tool.

### 9.7.1 *Common behavior*

Listing 9.13 provides two implementations of setting the time. They both follow a common pattern:

1. Parse a command-line argument to create a `DateTime<FixedOffset>` value. The `FixedOffset` timezone is provided by `chrono` as a proxy for “whichever timezone is provided by the user”. `chronocan't` know at compile-time which timezone will be selected.
2. Convert the `DateTime<FixedOffset>` to a `DateTime<Local>` to enable timezone comparisons.
3. Instantiate an operating system-specific struct that's used as an argument for the necessary *system call* (system calls are function calls provided by the operating system)
4. Set the system's time within an `unsafe` block. Unsafety is required because responsibility is delegated to the operating system.

5. Print the updated time.

**TIP**

This code uses functions to teleport the system's clock to a different time. This jumpiness can cause issues for applications that expect monotonically increasing time. A smarter (and more complex) approach is to adjust the length of a second for  $n$  seconds until the desired time is reached.

Functionality is implemented within the `Clock` struct that was introduced at [“Refactoring the clock v0.1.0 code to support wider architecture”](#).

### **9.7.2 Setting the time in operating systems that use libc**

POSIX-compliant operating systems can have their time set via a call to `settimeofday()`, which is provided by `libc`. `libc` is the “C Standard Library” and has lots of historic connections with UNIX operating systems. The C language was developed to write UNIX. Even today, interacting with a UNIX derivative involves using the tools provided by the C language.

There are two mental hurdles required for Rust programmers to understand this code:

1. the arcane types provided by `libc`
2. the unfamiliarity of providing arguments as pointers

Let's address both.

#### **LIBC IS TYPE-HEAVY AS IT USES MANY ALIASES**

Dealing with the time APIs within `libc` means dealing with many types and type aliases. The code is intended to be easy to implement, which means providing local implementors (hardware designers) the opportunity to change aspects as their platforms require. The way this is done is to use type aliases everywhere, rather than sticking to a defined integer type.

Near the start of Listing 9.10 , you will encounter the line

```
libc::time::{timeval,time_t,suseconds_t};
```

which represents two type aliases and a struct definition. In Rust syntax, they're defined like this:

```
type time_t = i64;
type suseconds_t = i64;

pub struct timeval {
    pub tv_sec: time_t,
    pub tv_usec: suseconds_t,
}
```

`time_t` represents the seconds that have elapsed since “the Epoch”. `suseconds_t` represents the fractional component of the current second.

## NON-WINDOWS CLOCK CODE

libc provides a handy function, `settimeofday`. The project's `Cargo.toml` file requires two extra lines to bring `libc` bindings into the crate:

```
[target.'cfg(not(windows))'.dependencies] ①
libc = "0.2"
```

① These two lines can be added to the end of the file

### Listing 9.10. Setting the time in a `libc` environment, such as Linux and BSD operating systems

```
#[cfg(not(windows))]
fn set<Tz: TimeZone>(t: DateTime<Tz>) -> () { ①
    use libc::settimeofday;
    use libc::{suseconds_t, time_t, timeval, timezone}; ②

    let t = t.with_timezone(&Local); // variable names indicate the data's
progression
    let mut u: timeval = unsafe { zeroed() }; // through the function

    u.tv_sec = t.timestamp() as time_t;
    u.tv_usec = t.timestamp_subsec_micros() as suseconds_t;

    unsafe { ③
        let mock_tz: *const timezone = std::ptr::null();
        gettimeofday(&u as *const timeval, mock_tz);
    }
}
```

- ① `t` is sourced from the command line and has already been parsed.
- ② Operating system-specific imports are made within the function, to avoid polluting the global scope. `libc::settimeofday` is a function that modifies the system clock. `suseconds_t`, `time_t`, `timeval`, and `timezone` are all types that are used interact with it.
- ③ The `timezone` parameter of `settimeofday()` appears to be some historic accident. Non-null values generate an error.

This code cheekily, and probably perilously, avoids checking whether the `settimeofday` function was successful. It's very possible that it didn't. That will be remedied in the next iteration of `clock`.

### 9.7.3 Setting the time on MS Windows

The code for MS Windows is similar to its `libc` peers. It is somewhat wordier, as the struct that sets the time has more fields than the second and subsecond part.

The rough equivalent of `libc` is called `kernel32.dll`, which is accessible after also including the `winapi` crate.

## WINDOWS API INTEGER TYPES

Windows provides its own take on what to call integral types. This code only makes use of the WORD type, but it can be useful to remember two other common types that have emerged since computers used 16-bit CPUs.

Windows Type	Rust Type	Remarks
WORD	u16	Refers to the width of a CPU “word”, as it was when Windows was initially created.
DWORD	u32	“Double word”
QWORD	u64	“Quadruple word”
LARGE_INTEGER	i64	A type defined as a crutch to enable 32-bit and 64-bit platforms to share code.
ULARGE_INTEGER	u64	An unsigned version of LARGE_INTEGER

## REPRESENTING THE TIME IN WINDOWS

Windows provides multiple time types. Within `clock` however, we’re mostly interested in `SYSTEMTIME`. Another type that is provided is `FILETIME`, described here to avoid confusion.

Windows Type	Rust Type	Remarks
SYSTEMTIME	winapi::SYSTEMTIME	Contains fields for the year, month, day of the week, day of the month, hour, minute, second and millisecond.
FILETIME	winapi::FILETIME	Analogous to <code>libc::timeval</code> Contains second and millisecond fields. Microsoft’s documentation warns that on 64-bit platforms, its use can cause irritating overflow bugs without finicky type casting, which is why it’s not employed here.

## WINDOWS CLOCK CODE

As the `SYSTEMTIME` struct contains many fields, generating one takes a little bit longer.

### Listing 9.11. Setting the time using the Windows kernel.dll API

```
#[cfg(windows)]
fn set(<Tz: TimeZone>(t: DateTime<Tz>) -> () {
    use winapi::{SYSTEMTIME, WORD};
    use kernel32::{GetSystemTime, SetSystemTime};

    let t = t.with_timezone(&Local);

    let mut systime: SYSTEMTIME = unsafe { zeroed() } ;

    let dow = match t.weekday() {
        Weekday::Mon => 1,
        Weekday::Tue => 2,
        Weekday::Wed => 3,
        Weekday::Thu => 4,
        Weekday::Fri => 5,
        Weekday::Sat => 6,
        Weekday::Sun => 7,
    };
    systime.wDay = dow;
    systime.wMonth = t.month();
    systime.wYear = t.year();
    systime.wHour = t.hour();
    systime.wMinute = t.minute();
    systime.wSecond = t.second();
    systime.wMilliseconds = t.nanosecond() / 1_000_000;
}
```

(1)  
(1)  
(1)

```

Weekday::Wed => 3,                                ①
Weekday::Thu => 4,                                ①
Weekday::Fri => 5,                                ①
Weekday::Sat => 6,                                ①
Weekday::Sun => 0,                                ①
};

let mut ns = t.nanosecond();                         ②
let mut leap_second = 0;                            ②
let is_leap = ns > 1_000_000_000;                  ②
                                                    ②
if is_leap {                                       ②
    ns -= 1_000_000_000;                          ②
    leap_second += 1;                           ②
}

systime.wYear = t.year() as WORD;
systime.wMonth = t.month() as WORD;
systime.wDayOfWeek = dow as WORD;
systime.wDay = t.day() as WORD;
systime.wHour = t.hour() as WORD;
systime.wMinute = t.minute() as WORD;
systime.wSecond = (leap_second + t.second()) as WORD; ③
systime.wMilliseconds = (ns / 1_000_000) as WORD;

let systime_ptr = &systime as *const SYSTEMTIME;

unsafe {
    SetSystemTime(systime_ptr);
}
}

```

- ① The chrono::Datelike trait provides the weekday() method. Microsoft's developer documentation provides the conversion table.
- ② As an implementation detail, chrono represents leap seconds by adding an extra second within the nanoseconds field. To convert the nanoseconds to milliseconds, as required by Windows, we need to account for this.
- ③ See the warning below.

**WARNING**

Note to MEAP readers—I need to check how Windows handles leap seconds more thoroughly. The documentation for SYSTEMTIME ([msdn.microsoft.com/en-us/library/windows/desktop/ms724950\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/ms724950(v=vs.85).aspx)) does not mention them. This implies that the seconds field must remain 0..=59.

### 9.7.4 *clock v0.1.2 Full code listing*

Listing 9.12 provide the full source listing for *clock v0.1.2*.

**Listing 9.12. Crate configuration for Listing 9.13 (ch9/ch9-clock0/Cargo.toml)**

```
[package]
name = "clock"
version = "0.1.2"
authors = ["Tim McNamara <code@timmcnamara.co.nz>"]

[dependencies]
chrono = "0.4"
clap = "2.32"

[target.'cfg(windows)'.dependencies]
winapi = "0.2"
kernel32-sys = "0.2"

[target.'cfg(not(windows))'.dependencies]
libc = "0.2"
```

**Listing 9.13. Cross-portable code for setting of the system time**

```
extern crate chrono;
extern crate clap;
#[cfg(windows)] extern crate winapi;
#[cfg(windows)] extern crate kernel32;
#[cfg(not(windows))] extern crate libc;

use clap::{App, Arg};
use chrono::DateTime;
use chrono::{Local, FixedOffset};
use std::mem::zeroed;
struct Clock;

impl Clock {
    fn get() -> DateTime<Local> {
        Local::now()
    }

    #[cfg(windows)]
    fn set<Tz: TimeZone>(t: DateTime<Tz>) -> () {
        use chrono::Weekday;
        use kernel32::SetSystemTime;
        use winapi::{SYSTEMTIME, WORD};

        let t = t.with_timezone(&Local);

        let mut systime: SYSTEMTIME = unsafe { zeroed() };

        let dow = match t.weekday() {
            Weekday::Mon => 1,
            Weekday::Tue => 2,
            Weekday::Wed => 3,
            Weekday::Thu => 4,
```

```

        Weekday::Fri => 5,
        Weekday::Sat => 6,
        Weekday::Sun => 0,
    };

    let mut ns = t.nanosecond();
    let is_leap_second = ns > 1_000_000_000;

    if is_leap_second {
        ns -= 1_000_000_000;
    }

    systime.wYear = t.year() as WORD;
    systime.wMonth = t.month() as WORD;
    systime.wDayOfWeek = dow as WORD;
    systime.wDay = t.day() as WORD;
    systime.wHour = t.hour() as WORD;
    systime.wMinute = t.minute() as WORD;
    systime.wSecond = t.second() as WORD;
    systime.wMilliseconds = (ns / 1_000_000) as WORD;

    let systime_ptr = &systime as *const SYSTEMTIME; // as *mut SYSTEMTIME; //
convert to a pointer, then change its mutability

    unsafe {
        SetSystemTime(systime_ptr); // giving a pointer to a value to something
outside of Rust's control is unsafe
    }
}

#[cfg(not(windows))]
fn set<Tz: TimeZone>(t: DateTime<Tz>) -> () {
    use libc::settimeofday;
    use libc::{suseconds_t, time_t, timeval, timezone};

    let t = t.with_timezone(&Local); // variable names indicate the data's
progression
    let mut u: timeval = unsafe { zeroed() }; // through the function

    u.tv_sec = t.timestamp() as time_t;
    u.tv_usec = t.timestamp_subsec_micros() as suseconds_t;

    unsafe {
        let mock_tz: *const timezone = std::ptr::null();
        gettimeofday(&u as *const timeval, mock_tz);
    }
}

fn main() {
    let app = App::new("clock")
        .version("0.1")
        .about("Gets and sets (aspirationally) the time.")
}

```

```

    .after_help("Note: UNIX timestamps are parsed as whole seconds since 1st
January 1970 0:00:00 UTC. For more accuracy, use another format.")
    .arg(Arg::with_name("action")
        .takes_value(true)
        .possible_values(&["get", "set"])
        .default_value("get"))
    .arg(Arg::with_name("std")
        .short("s")
        .long("use-standard")
        .takes_value(true)
        .possible_values(&["rfc2822", "rfc3339", "timestamp"])
        .default_value("rfc3339"))
    .arg(Arg::with_name("datetime")
        .help("When <action> is 'set', apply <datetime>. Otherwise, ignore."))
        .help("When <action> is 'set', apply <datetime>. Otherwise, ignore."));

let args = app.get_matches();

let action = args.value_of("action").unwrap();
let std = args.value_of("std").unwrap();

if action == "set" {
    let t_ = args.value_of("datetime").unwrap();

    let parser = match std {
        "rfc2822" => DateTime::parse_from_rfc2822,
        "rfc3339" => DateTime::parse_from_rfc3339,
        _ => unimplemented!(),
    };

    let err_msg = format!("Unable to parse {} according to {}", t_, std);
    let t = parser(t_).expect(&err_msg);

    Clock::set(t)
}

let now = Clock::get();

match std {
    "timestamp" => println!("{}", now.timestamp()),
    "rfc2822"   => println!("{}", now.to_rfc2822()),
    "rfc3339"   => println!("{}", now.to_rfc3339()),
    _ => unreachable!(),
}
}

```

## 9.8 Improving error handling

Those readers who have dealt with operating systems before will probably be dismayed at some of the code within “[clock v0.1.2: Setting the time](#)”. It doesn’t check to see whether the calls to `settimeofday()` and `SetSystemTime()` were actually successful.

There are multiple reasons why setting the time might fail. The most obvious one is that the user who is attempting to set the time lacks permission to do so.

The robust approach is to have `Clock::set(t)` return `Result`. As that will require modifying two functions that we have already spent some time explaining in-depth, let's introduce a workaround that makes use of the operating system's error reporting instead.

```
fn main() {
    // ...
    if action == "set" {
        // ...

        Clock::set(t);

        let maybe_error = std::io::Error::last_os_error();           ①
        let os_error_code = &maybe_error.raw_os_error();           ①
        match os_error_code {
            Some(0) => (),
            None => (),
            _ => eprintln!("Unable to set the time: {:?}", maybe_error), ②
        }
    }
}
```

- ① `maybe_error` is a Rust type that we can deconstruct to convert it into a raw `i32` value that's easy to match on.
- ② Matching on a raw integer saves importing an enum, but sacrifices type safety. Production-ready code shouldn't cheat in this way.

After calls to `Clock::set(t)`, Rust will happy talk to the operating system via `std::io::Error::last_os_error()` to see if an error code has been generated.

## 9.9 *clock v0.1.3 Resolving differences between clocks with the Network Time Protocol (NTP)*

Resolving disputes about what time it is known formally *clock synchronisation*. There are multiple international standards for synchronizing clocks. This section focuses on the most prominent one: the Network Time Protocol (NTP). NTP has existed since the mid-1980s and has proven to be very stable. Its on-wire format has not changed in the first four revisions of the protocol, with backwards compatibility retained the entire time.

NTP operates in two modes that can loosely be described as “always on” and “request/response”.

The “always on” mode allows multiple computers to work in a peer to peer fashion to converge on an agreed definition of “now”. It requires a software daemon/service to be running constantly on each device but can achieve very tight synchronization within local networks.

The “request/response” mode is much simpler. Local clients request the time via a

single message and then parse the response. Keeping track of the elapsed time on the client and comparing timestamps

NTP allows clients to request the time from computers who are closer to atomic clocks. But that only gets us part of the way. Let's say that your computer asks 10 computers what they think the time is. Now we have 10 assertions about the time, and the network lag will differ for each source.

### **9.9.1 Sending NTP requests and interpreting responses**

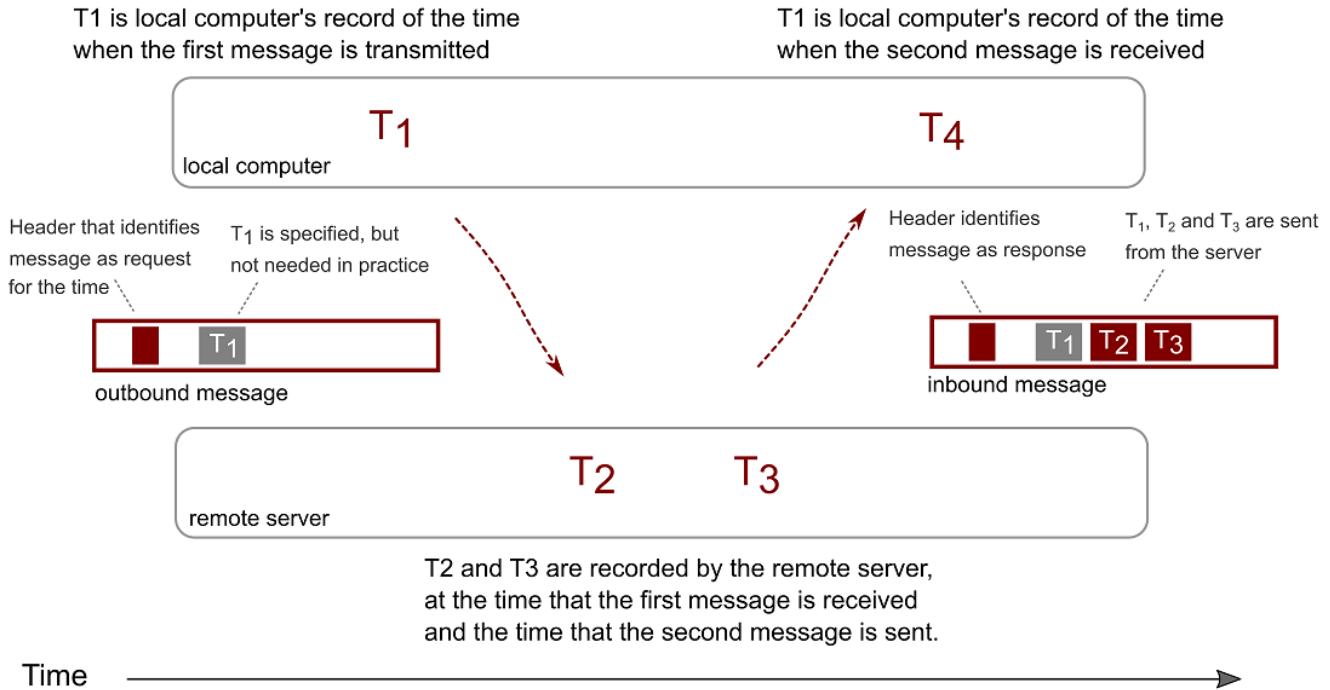
Let's consider the client-server situation where your computer wants to correct its own time. For every computer that you check with — let's call them *time servers* — there are two messages:

- The message from your computer to each time server is the *request*
- The reply is known as the *response*

These two messages generate four time points. They occur in serial, and their names are designated by the specification (RFC 2030):

- $T_1$ : the client's timestamp of when the request was sent. Referred to as  $t_1$  in code.
- $T_2$ : the time server's timestamp when the request was received. Referred to as  $t_2$  in code.
- $T_3$ : the time server's timestamp of when it sends its response. Referred to as  $t_3$  in code.
- $T_4$ : the client's timestamp of when the response was received. Referred to as  $t_4$  in code.

**Figure 9.3. Timestamps that are defined within the Network Time Protocol**



To see what this means in code, spend a few moments looking through Listing 9.14 . Lines 2-12 deal with establishing a connection. Lines 14-21 produce T<sub>1</sub> to T<sub>4</sub>. Lines 2-12 deal with establishing a connection. Lines 14-21 produce T<sub>1</sub> to T<sub>4</sub>.

#### **Listing 9.14. Defining a function that sends NTP messages**

```
fn ntp_roundtrip(host: &str, port: u16) -> Result<NTPResult, std::io::Error> {
    let destination = format!("{}:{}", host, port);
    let timeout = Duration::from_secs(1);

    let request = NTPMessage::client();
    let mut response = NTPMessage::new();

    let message = request.data;

    let mut udp = UdpSocket::bind(LOCAL_ADDR)?;
    udp.connect(&destination).expect("unable to connect");

    let t1 = Utc::now();                                ①
    udp.send(&message)?;                            ②
    udp.set_read_timeout(Some(timeout));
    udp.recv_from(&mut response.data)?;            ③
    let t4 = Utc::now();
```

```

let t2: DateTime<Utc> = response.rx_time().unwrap().into();      ④
let t3: DateTime<Utc> = response.tx_time().unwrap().into();      ⑤

Ok(NTPResult {
    t1: t1,
    t2: t2,
    t3: t3,
    t4: t4,
})
}

```

- ① This code cheats slightly by not even bothering to encode `t1` in the outbound message. In practice, this works perfectly well and requires fractionally less work.
- ② Send a request payload (which is defined elsewhere) to the server.
- ③ This call will *block* the application until data is ready to be received.
- ④ `rx_time()` stands for received timestamp and is the time that the server received the client's message.
- ⑤ `tx_time()` stands for transmitted timestamp and is the time that the server sent the reply

$T_1$  to  $T_4$ , encapsulated in Listing 9.14 as `NTPResult`, are all that's required to judge whether the local time matches the servers. The protocol contains some more sophistication relating to error handling, but that's avoided here for simplicity. Otherwise, it's a perfectly capable NTP client.

## 9.9.2 Adjusting the local time as a result of the server's response

Given that our client has received at least one (and hopefully a few more) NTP responses, all that's left to do is to calculate the “right” time. But wait, which time is “right”? All we have are relative timestamps. There is still no universal truth that we've been given access to.

The NTP documentation provides two equations to help resolve the situation. For those readers who don't enjoy Greek letters, feel free to skim or even skip the next few paragraphs.

Our aim is to calculate two values:

3. the *time offset* is what we're ultimately interested in. It is denoted as  $\theta$  (theta) by the official documentation. When  $\theta$  is a positive number, our clock is fast. When it is negative, our clock is slow.
4. the *delay* caused by network congestion, latency and other noise. This is denoted as  $\delta$  (delta). A large  $\delta$  implies that the reading is less reliable. Our code will use this value to prefer to follow servers that respond quickly.

**Table 9.2. How to calculate  $\delta$  and  $\theta$  in NTP**

$\delta = (T_4 - T_1) - (T_3 - T_2)$	( $T_4 - T_1$ ) calculates the total time spent on the client's side. ( $T_3 - T_2$ ) calculates the total time spent on the server's side. The difference between the two differences, e.g. $\delta$ , is an estimate of the difference between the clocks, plus a delay caused because of network traffic and processing.
$\theta = ((T_2 - T_1) + (T_4 - T_3)) / 2$	We take the average of the two pairs of timestamps.

The mathematics can be deceptively confusing because there is always an innate desire to know what the time *actually is*. That's impossible to know. All we have are assertions.

NTP is designed to operate multiple times per day, with participants nudging their clocks incrementally over time. Given sufficient adjustments,  $\theta$  tends to 0 while  $\delta$  remains relatively stable.

The standard is quite prescriptive about the formula to do carry out the adjustments. For example, the reference implementation of NTP includes some useful filtering to limit the effect of bad actors and other spurious results.

We're going to cheat. We'll just take a mean of the differences, weighted by  $1/\theta^2$ . This aggressively penalizes slow servers.

To minimize the likelihood of any negative outcomes:

- We're checking the time with “known good” actors. In particular, we'll use time servers hosted by major operating system vendors and other reliable sources to minimize the chances of someone sending us a questionable result.
- No single result will affect the result too much. We'll cap any adjustments we make to the local time to 200ms.

**Listing 9.15. Adjusting the time according to the responses from of multiple time servers**

```
fn check_time() -> Result<f64, std::io::Error> {
    const NTP_PORT: u16 = 123;

    let servers = [
        "time.nist.gov",
        "time.apple.com",
        "time.euro.apple.com",
        "time.google.com",           ①
        "time2.google.com",          ①
        // "time.windows.com",       ②
    ];
    let mut times = Vec::with_capacity(servers.len());
    for &server in servers.iter() {
        print!("{} =>", server);
        let mut reader = TcpReader::new(server, NTP_PORT);
        let mut writer = TcpWriter::new(reader);
        writer.write(&NTPMessage::Request).await?;
        let response = reader.read().await?;
        times.push(response.time);
    }
    let delta = (times[1] - times[0]) - (times[2] - times[1]);
    let theta = (times[1] + times[2]) / 2;
    let adjustment = (1.0 / theta.pow(2)) * delta;
    if adjustment.abs() > 200.0 {
        adjustment = 200.0;
    }
    let now = SystemTime::now();
    let offset = now.duration_since(UNIX_EPOCH).unwrap();
    let timestamp = offset.as_secs_f64() + adjustment;
    let mut writer = TcpWriter::new(TcpReader::new("localhost", 123));
    writer.write(&NTPMessage::Response { timestamp }).await?;
}
```

```

let calc = ntp_roundtrip(&server, NTP_PORT);

match calc {
    Ok(time) => {
        println!(" {}ms away from local system time", time.offset());
        times.push(time);
    },
    Err(_) => println!(" ? [response took too long]"),
};

let mut offsets = Vec::with_capacity(servers.len());
let mut offset_weights = Vec::with_capacity(servers.len());

for time in &times {
    let offset = time.offset() as f64;
    let delay = time.delay() as f64;

    let weight = 1_000_000.0 / (delay*delay); ③
    if weight.is_finite() {
        offsets.push(offset);
        offset_weights.push(weight);
    }
}

let avg_offset = weighted_mean(&offsets, &offset_weights);

Ok(avg_offset)
}

```

- ① Google's time servers implement leap seconds by expanding the length of a second, rather than adding an extra second. Thus, for one day approximately every 18 months, this server may report a different time than the others.
- ② At the time of writing, Microsoft's time server appeared to be providing a time that was 15 seconds ahead of its peers.
- ③ Penalize slow servers by substantially decreasing their relative weights

### 9.9.3 Converting between time representations that use different precisions and epochs

chrono represents the fractional part of a second down to nanosecond precision, whereas NTP can represent times that differ between approximately 250 picoseconds. That's roughly 4 times more precise. The different internal representations used imply that some accuracy is likely to be lost during conversions.

The mechanism for telling Rust that two types can be converted is the `From` trait. `From` provides the `from()` method, which is encountered early on in one's Rust career in example such as `String::from("Hello, world!")`.

Listing 9.16 provides implementations of `From` and `Into` that allow explicit type conversion. This code allows the line `response.rx_time().unwrap().into()`;

within Listing 9.14 to work.

#### Listing 9.16. Converting between chrono::DateTime and NTP timestamps

```
##[derive(Default,Debug,Copy,Clone)]
struct NTPTimestamp {
    seconds: u32,                                ①
    fraction: u32,                                ①
}
impl From<NTPTimestamp> for DateTime<Utc> {
    fn from(ntp: NTPTimestamp) -> Self {
        let secs = ntp.seconds as i64 - NTP_TO_UNIX_SECONDS;      ②
        let mut nanos = ntp.fraction as f64;
        nanos *= 1e9;
        nanos /= 2_f64.powi(32);                      ③
        Utc.timestamp(secs, nanos as u32)
    }
}

impl From<DateTime<Utc>> for NTPTimestamp {
    fn from(utc: DateTime<Utc>) -> Self {
        let secs = utc.timestamp() + NTP_TO_UNIX_SECONDS;
        let mut fraction = utc.nanosecond() as f64;
        fraction *= 2_f64.powi(32);
        fraction /= 1e9;

        NTPTimestamp {
            seconds: secs as u32,
            fraction: fraction as u32,
        }
    }
}
```

- ① Our internal type to represent a NTP timestamp
- ② Defined as 2\_08\_988\_800, which is the number of seconds between 1 Jan 1900 (the NTP epoch) and 1 Jan 1970 (the UNIX epoch).
- ③ These conversions can be implemented using bit shift operations, at the expense of even less readability.

`From` has a reciprocal peer, `Into`. Implementing `From` will allow Rust to automatically generate an `Into` implementation on its own, except in advanced cases. In those advanced cases, it's likely that developers already posses the knowledge required to implement `Into` manually and so probably don't need assistance here.

#### 9.9.4 *clock v0.1.3 full code listing*

The whole code listing for `clock` is presented in `clock-v013`.

Taken in its full glory, the whole of `clock` can look quite large and imposing.

Hopefully there is nothing new within Listing 9.17 .

### **Listing 9.17. Command-line NTP client**

```
extern crate byteorder;
extern crate chrono;
extern crate clap;
#[cfg(not(windows))] extern crate libc;
#[cfg(windows)] extern crate kernel32;
#[cfg(windows)] extern crate winapi;

use byteorder::{BigEndian, ReadBytesExt};
use chrono::DateTime;
use chrono::Duration as ChronoDuration;
use chrono::{Datelike, TimeZone, Timelike};
use chrono::{Local, Utc};
use clap::{App, Arg};
use std::mem::zeroed;
use std::net::UdpSocket;
use std::time::Duration;

const NTP_MESSAGE_LENGTH: usize = 48; // 12*4 bytes
const NTP_TO_UNIX_SECONDS: i64 = 2_208_988_800;
const LOCAL_ADDR: &'static str = "0.0.0.0:12300";

#[derive(Default, Debug, Copy, Clone)]
struct NTPTimestamp {
    seconds: u32,
    fraction: u32,
}

struct NTPMessage {
    data: [u8; NTP_MESSAGE_LENGTH],
}

#[derive(Debug)]
struct NTPResult {
    t1: DateTime<Utc>,
    t2: DateTime<Utc>,
    t3: DateTime<Utc>,
    t4: DateTime<Utc>,
}
}

impl NTPResult {
    fn offset(&self) -> i64 {
        let duration = (self.t2 - self.t1) + (self.t3 - self.t4);
        duration.num_milliseconds() / 2
    }

    fn delay(&self) -> i64 {
        let duration = (self.t4 - self.t1) - (self.t3 - self.t2);
        duration.num_milliseconds()
    }
}
```

```

    }
}

impl From<NTPTimestamp> for DateTime<Utc> {
    fn from(ntp: NTPTimestamp) -> Self {
        let secs = ntp.seconds as i64 - NTP_TO_UNIX_SECONDS;
        let mut nanos = ntp.fraction as f64;
        nanos *= 1e9;
        nanos /= 2_f64.powi(32);

        Utc.timestamp(secs, nanos as u32)
    }
}

impl From<DateTime<Utc>> for NTPTimestamp {
    fn from(utc: DateTime<Utc>) -> Self {
        let secs = utc.timestamp() + NTP_TO_UNIX_SECONDS;
        let mut fraction = utc.nanosecond() as f64;
        fraction *= 2_f64.powi(32);
        fraction /= 1e9;

        NTPTimestamp {
            seconds: secs as u32,
            fraction: fraction as u32,
        }
    }
}

impl NTPMessage {
    fn new() -> Self {
        NTPMessage {
            data: [0; NTP_MESSAGE_LENGTH],
        }
    }

    fn client() -> Self {
        const VERSION: u8 = 3;
        const MODE: u8 = 3;

        let mut msg = NTPMessage::new();

        // the first byte of every NTP message contains three fields,
        // but we only need to set two of them
        msg.data[0] |= VERSION << 3;
        msg.data[0] |= MODE;
        msg
    }
}

fn parse_timestamp(&self, i: usize) -> Result<NTPTimestamp, std::io::Error> {
    let mut reader = &self.data[i..i + 8];
    let seconds = reader.read_u32::<BigEndian>()?;
    let fraction = reader.read_u32::<BigEndian>()?;
}

```

```

Ok(NTPTimestamp {
    seconds: seconds,
    fraction: fraction,
})
}

fn rx_time(&self) -> Result<NTPTimestamp, std::io::Error> {
    self.parse_timestamp(32)
}

fn tx_time(&self) -> Result<NTPTimestamp, std::io::Error> {
    self.parse_timestamp(40)
}
}

fn weighted_mean(values: &[f64], weights: &[f64]) -> f64 {
    let mut result = 0.0;
    let mut sum_of_weights = 0.0;

    for (v, w) in values.iter().zip(weights) {
        result += v * w;
        sum_of_weights += w;
    }

    result / sum_of_weights
}

fn ntp_roundtrip(host: &str, port: u16) -> Result<NTPResult, std::io::Error> {
    let destination = format!("{}:{}", host, port);
    let timeout = Duration::from_secs(1);

    let request = NTPMessage::client();
    let mut response = NTPMessage::new();

    let message = request.data;

    let udp = UdpSocket::bind(LOCAL_ADDR)?;
    udp.connect(&destination).expect("unable to connect");

    let t1 = Utc::now();
    udp.send(&message)?;
    udp.set_read_timeout(Some(timeout))?;
    udp.recv_from(&mut response.data)?;
    let t4 = Utc::now();

    let t2: DateTime<Utc> = response.rx_time().unwrap().into();
    let t3: DateTime<Utc> = response.tx_time().unwrap().into();

    Ok(NTPResult {
        t1: t1,
        t2: t2,
        t3: t3,
        t4: t4,
    })
}

```

```

        })
}

fn check_time() -> Result<f64, std::io::Error> {
    const NTP_PORT: u16 = 123;

    let servers = [
        "time.nist.gov",
        "time.apple.com",
        "time.euro.apple.com",
        "time.google.com",
        "time2.google.com",
        // "time.windows.com",
    ];
}

let mut times = Vec::with_capacity(servers.len());

for &server in servers.iter() {
    print!("{} =>", server);

    let calc = ntp_roundtrip(&server, NTP_PORT);

    match calc {
        Ok(time) => {
            println!(" {}ms away from local system time", time.offset());
            times.push(time);
        }
        Err(_) => println!(" ? [response took too long]"),
    };
}

let mut offsets = Vec::with_capacity(servers.len());
let mut offset_weights = Vec::with_capacity(servers.len());

for time in &times {
    let offset = time.offset() as f64;
    let delay = time.delay() as f64;

    let weight = 1_000_000.0 / (delay * delay);      ①
    if weight.is_finite() {
        offsets.push(offset);
        offset_weights.push(weight);
    }
}

let avg_offset = weighted_mean(&offsets, &offset_weights);

Ok(avg_offset)
}

struct Clock;

impl Clock {

```

```

fn get() -> DateTime<Local> {
    Local::now()
}

#[cfg(windows)]
fn set<Tz: TimeZone>(t: DateTime<Tz>) -> () {
    use chrono::Weekday;
    use kernel32::SetSystemTime;
    use winapi::{SYSTEMTIME, WORD};

    let t = t.with_timezone(&Local);

    let mut systime: SYSTEMTIME = unsafe { zeroed() };

    let dow = match t.weekday() {
        Weekday::Mon => 1,
        Weekday::Tue => 2,
        Weekday::Wed => 3,
        Weekday::Thu => 4,
        Weekday::Fri => 5,
        Weekday::Sat => 6,
        Weekday::Sun => 0,
    };

    let mut ns = t.nanosecond();
    let is_leap_second = ns > 1_000_000_000;

    if is_leap_second {
        ns -= 1_000_000_000;
    }

    systime.wYear = t.year() as WORD;
    systime.wMonth = t.month() as WORD;
    systime.wDayOfWeek = dow as WORD;
    systime.wDay = t.day() as WORD;
    systime.wHour = t.hour() as WORD;
    systime.wMinute = t.minute() as WORD;
    systime.wSecond = t.second() as WORD;
    systime.wMilliseconds = (ns / 1_000_000) as WORD;

    let systime_ptr = &systime as *const SYSTEMTIME;

    unsafe {
        SetSystemTime(systime_ptr);
    }
}

#[cfg(not(windows))]
fn set<Tz: TimeZone>(t: DateTime<Tz>) -> () {
    use libc::settimeofday;
    use libc::{suseconds_t, time_t, timeval, timezone};

    let t = t.with_timezone(&Local); // variable names indicate the data's

```

```

progression
    let mut u: timeval = unsafe { zeroed() }; // through the function

    u.tv_sec = t.timestamp() as time_t;
    u.tv_usec = t.timestamp_subsec_micros() as suseconds_t;

    unsafe {
        let mock_tz: *const timezone = std::ptr::null();
        settimeofday(&u as *const timeval, mock_tz);
    }
}

fn main() {
    let app = App::new("clock")
        .version("0.1.3")
        .about("Gets and sets the time.")
        .after_help("Note: UNIX timestamps are parsed as whole seconds since 1st
January 1970 0:00:00 UTC. For more accuracy, use another format.")
        .arg(Arg::with_name("action")
            .takes_value(true)
            .possible_values(&["get", "set", "check-ntp"])
            .default_value("get"))
        .arg(Arg::with_name("std")
            .short("s")
            .long("use-standard")
            .takes_value(true)
            .possible_values(&["rfc2822", "rfc3339", "timestamp"])
            .default_value("rfc3339"))
        .arg(Arg::with_name("datetime")
            .help("When <action> is 'set', apply <datetime>. Otherwise, ignore."));
}

let args = app.get_matches();

let action = args.value_of("action").unwrap(); // default_value() has been
supplied,
let std = args.value_of("std").unwrap(); // so it's safe to use .unwrap()

if action == "set" {
    let t_ = args.value_of("datetime").unwrap();

    let parser = match std {
        "rfc2822" => DateTime::parse_from_rfc2822,
        "rfc3339" => DateTime::parse_from_rfc3339,
        _ => unimplemented!(),
    };

    let err_msg = format!("Unable to parse {} according to {}", t_, std);
    let t = parser(t_).expect(&err_msg);

    Clock::set(t);
} else if action == "check-ntp" {
    let offset = check_time().unwrap() as isize;
}

```

```

let adjust_ms = offset.signum() * offset.abs().min(200) / 5;
let adjust_ms_ = ChronoDuration::milliseconds(adjust_ms as i64);
let now: DateTime<Utc> = Utc::now() + adjust_ms_;
Clock::set(now);
}

let maybe_error = std::io::Error::last_os_error();
let os_error_code = &maybe_error.raw_os_error();
match os_error_code {
    Some(0) => (),
    None => (),
    _ => eprintln!("Unable to set the time: {:?}", maybe_error),
}
}

let now = Clock::get();

match std {
    "timestamp" => println!("{}", now.timestamp()),
    "rfc2822" => println!("{}", now.to_rfc2822()),
    "rfc3339" => println!("{}", now.to_rfc3339()),
    _ => unreachable!(),
}
}

```

## 9.10 Summary

In this chapter, you have learned

- Different strategies for handling the imperfect nature of the Earth's rotation around the Sun
- Parsing timestamps from strings into Rust objects via the `chrono` crate
- Interacting with `libc`, including accessing type aliases and calling functions via `unsafe` blocks
- Using system calls to set the system clock
- Accessing error codes provided by the operating system
- Dealing with precision differences between internal representations
- Converting between types by implementing `From`
- Silencing intermediate output from `cargo` via the `-q` option

# 12

## *Signals, Interrupts and Exceptions*

### **This chapter covers:**

- Learn how the outside world, such as the network and the keyboard, lets an application know that it has data ready for processing
- Disambiguating between the terms interrupt, exception, trap and fault
- Send and receive signals between running applications

This chapter describes the process by which the outside world communicates with your operating system. Programs' execution is constantly being interrupted by the network when bytes are ready to be delivered. That is, after connecting to a database—or at any other time—the operating system could demand that your application deals with a message. This chapter describes how this process operates and how to prepare your programs for it.

In the last chapter, you learned a digital clock is periodically notifying the operating system that time has progressed. This chapter explains how those notifications occur. It also introduces the concept of multiple applications running at the same time via the concept of signals.

Signals emerged as part of the UNIX operating system tradition and can be used to send messages between different running programs.

We'll be addressing both concepts—signals and interrupts—together as the programming model is similar but it's simpler to get started with signals.

This chapter tends to focus on the Linux operating system running on x86 CPUs. That's not to say that users of other operating systems are unable to do follow along.

## 12.1 Disambiguating several related terms

This computing sub-field contains related terms. For newcomers, they all look similar and it's not helped that they are used interchangeably. Examples of confusing terms include:

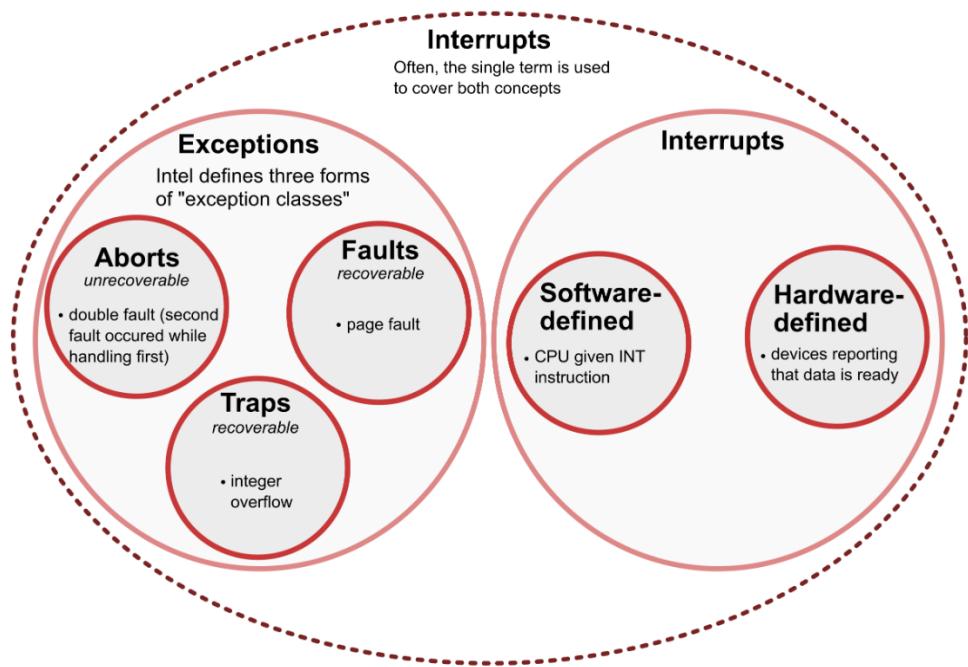
- Trap
- Exception
- Signal
- Fault
- Interrupt
- Hardware
- Software interrupt

The two concepts that are most important to distinguish are *signals* and *interrupts*. A signal is a software-level abstraction that is associated with an operating system. An interrupt is a CPU-related abstraction and is closely associated with the system's hardware.

Signals are a form of limited inter-process communication. They don't contain content, but their presence indicates something. They're analogous to a physical, audible buzzer. The buzzer isn't providing any content, but the person who set the alarm still knows what's intended when it's making noise. To add confusion to the mix, signals are often described as software interrupts, although this chapter will attempt to avoid the use of the term interrupt to refer to a signal.

There are two forms of interrupts, which differ in their origin. One form of interrupts occur within the CPU during its processing. They are the result of attempting to process illegal instructions and attempting to access invalid memory addresses. This first form is known technically as *synchronous interrupts*, but you will tend to hear them referred to by their more common name: *exceptions*. The second form of interrupts are generated by hardware devices, such as keyboards and accelerometers. They are what's commonly implied by the term interrupt. They can occur at any time and are formally known as *asynchronous interrupts*. Just like signals, they're also able to be generated within software. Figure 12.1 illustrates how they inter-relate.

**Figure 12.1. A visual taxonomy of how the terms interrupt, exception, trap and fault interact within Intel CPUs.**



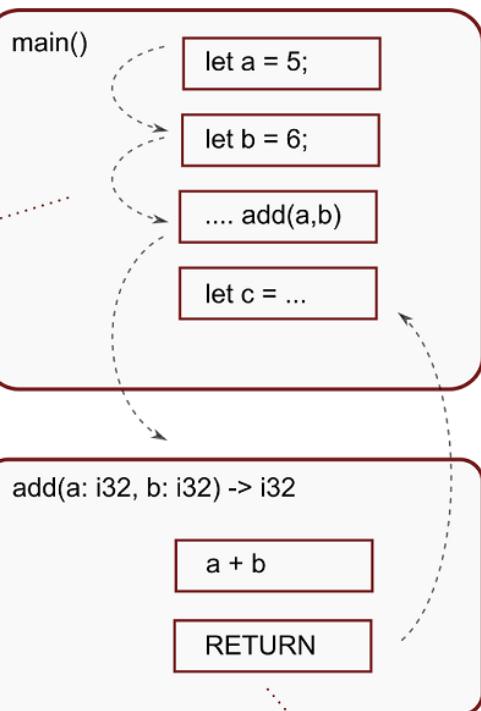
Interrupts can be specialized. A *trap* is an error detected by the CPU that it gives the operating system a chance to recover from. A *fault* is another form of recoverable problem. If the CPU is given a memory address that it can't read from, it notifies the operating system and asks for an updated address.

Interrupts will force an application's control flow to change, whereas many signals can be ignored when desired. Upon receiving an interrupt, the CPU will jump to handler code, irrespective of the current state of the program. The location of the handler code is pre-defined by the BIOS and operating system during a system's bootup process.

**Figure 12.2. Using addition to demonstrate signal handling control flow**

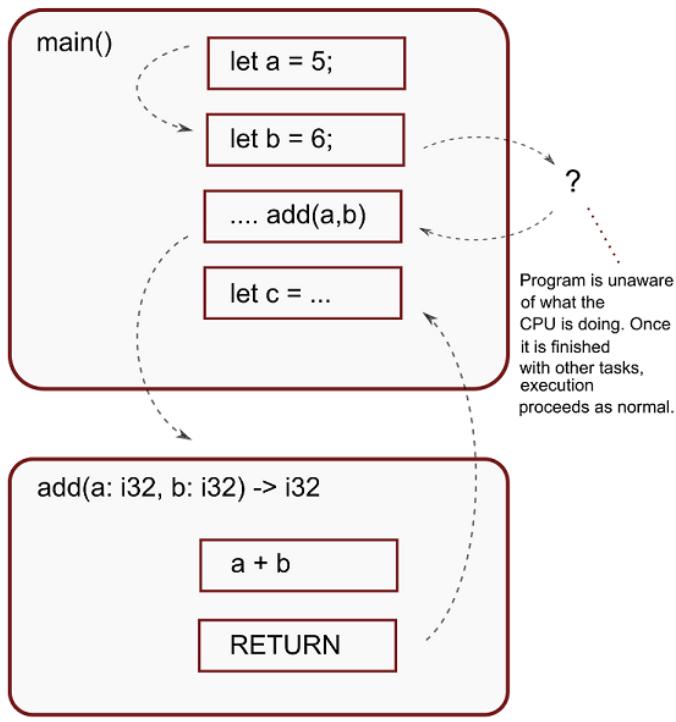
### Normal Program Execution

Control flow in the normal case operates in a linear sequence of instructions. Function calls and return statements do jump a CPU around in memory, but the order of events can be pre-determined.



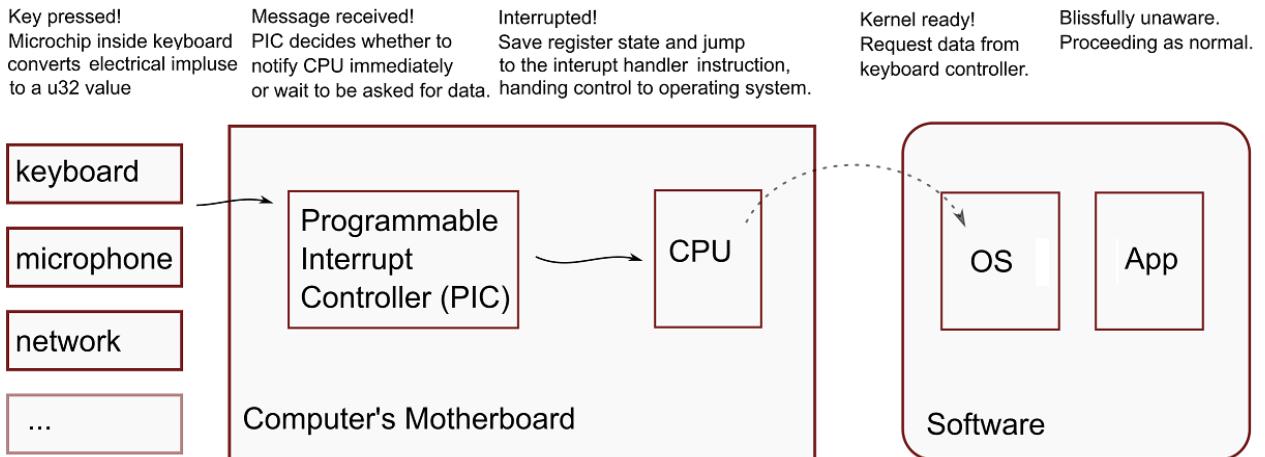
### Interrupted Program Execution

When a hardware interrupt occurs, the program is not unaffected directly, although there may be a negligible performance impact as the operating system must deal with the hardware.



Return instruction is implicit in Rust.

**Figure 12.3. Lifetime of an interrupt generated from a hardware device. Once the operating system has been notified that data is ready, it will then communicate with the device (in this case, the keyboard) directly to read the data into its own memory.**



To make things more difficult for learners, applications tend to be notified of interrupts as signals. This makes it even easier to conflate the two.

#### **Listing 12.1. Source code for Figure 12.2**

```
fn add(a: i32, b:i32) -> i32 {
    a + b
}

fn main() {
    let a = 5;
    let b = 6;
    let c = add(a,b);
}
```

#### **Treating Signals as Interrupts**

Handling interrupts directly means manipulating the operating system kernel. Because we would prefer not to do that in a learning environment, we'll play fast and loose with the terminology. For the rest of this chapter, treats signals as if they are interrupts.

Why simplify things? Writing operating system components involves tweaking the kernel. Breaking things there means that our system could become completely unresponsive without a clear way to fix things.

From a more pragmatic perspective, avoiding tweaks to the kernel means that we can avoid learning a whole new compiler toolchain.

We also have the advantage that the programming model is quite similar between signal handling and interrupt handling. That allows to keep any errors within our code to be constrained to our application, rather than risk bringing the whole system down.

The general pattern:

- Model your application's standard control flow
- Model the interrupted control flow — identify resources that would need to be cleanly shut down if required

- Write the interrupt/signal handler – be fast, update some state and return quickly. You will typically delegate time-consuming operations by only modifying a global variable that is regularly checked by the main loop of the program
- Modify your application’s standard control flow to look for the GO/NO GO flag that may have been modified by a signal handler

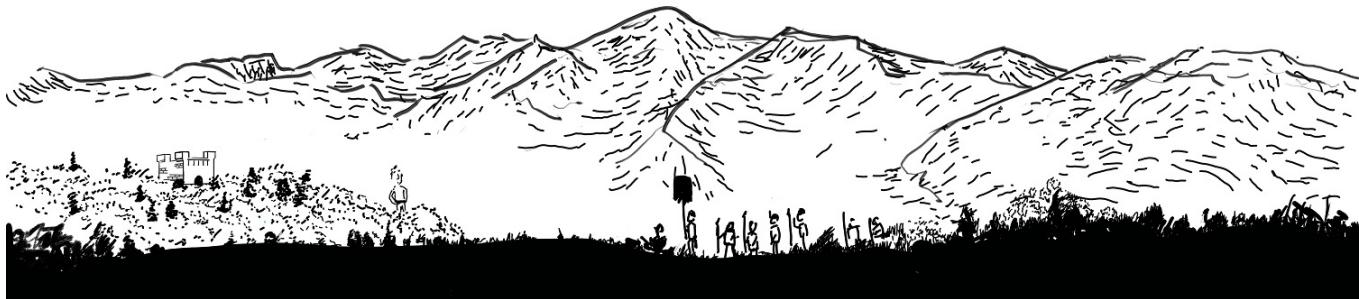
## **12.2 Avoiding writing code by relying on the default signal handling behavior**

Sometimes the best approach is to let the system’s defaults do the work. Code that you don’t need to write is code that’s free from bugs that you’ve caused.

The default behavior for most signals is shutting down the application. When an application does not provide a special handler function—we’ll learn how to do that in this chapter—the operating system considers the signal to be an abnormal condition. When an operating system detects an abnormal condition within an application, things don’t end well for the application. It terminates the application.

**Figure 12.4. An application defending itself from maulauding hoards of unwanted signals.**

**Signal handlers are the friendly giants of the computing world. They stay out of the way, but are there when your application needs to defend its castle. Although not part of everyday control-flow, they’re extremely useful when the time is right. Note: Not all signals can be handled. SIGKILL is particularly vicious.**



Here are three common signals that your application may receive and their intended action:

**SIGINT**

Terminate the program, usually generated by person.

**SIGTERM**

Terminate the program, usually generated by another program.

**SIGKILL**

Immediately terminate the program, without the ability to recover.

There are many others. A fuller list is provided at Listing 12.5 . You’ll notice that these three examples are heavily associated with terminating a running program. That’s not necessarily the case.

### **12.2.1 Using SIGSTOP and SIGCONT to suspend and resume a program’s operation**

In the case of the `SIGSTOP` signal, the application is suspended until it receives `SIGCONT`. This is used by UNIX systems for job control. It’s also useful to know about if you wish to manually intervene and halt a running application, but would like the ability to recover some time in the future.

Listing 12.4 is a minimal environment that allows us to invoke this stop, then continue functionality. What Rust will you learn? You’ll discover the “inclusive range” syntax.

#### **Listing 12.2. Overview of the files within the ch12-sixty project**

```
ch12-sixty
├── src
│   └── main.rs
└── Cargo.lock
```

#### **Listing 12.3. Package description file (ch12/ch12-sixty/Cargo.toml)**

```
[package]
name = "ch12-sixty"
version = "0.1.0"
authors = ["Tim McNamara <code@timmcnamara.co.nz>"]

[dependencies]
```

#### **Listing 12.4. Basic application that lives for 60 seconds, printing out its progress along the way. Happ to receive signals SIGSTOP and SIGCONT. (ch12/ch12-sixty/src/main.rs)**

```
use std::time;
use std::process;
use std::thread::{sleep};

fn main() {
    let delay = time::Duration::from_secs(1); (1)

    let pid = process::id();
    println!("{}: pid", pid);

    for i in 1..=60 { (2)
        sleep(delay);
        println!(". {}", i);
    }
}
```

- ① This application is intended to be run in conjunction with second terminal that is generating signals.
- ② The ..= syntax is an inclusive range. 1..60 counts from 1 to 59, 1..=60 counts from 1 to 60.

Once the code from Listing 12.4 is saved to disk, open two consoles. In the first, execute `cargo run`. A 3-5 digit number will appear, followed by a counter incrementing per second. The first line's number is the “pid”, or *process id*.

<b>Console 1: Compiles and executes ch12-sixty</b>	<b>Console 2: Sends signals to the ch12-sixty</b>	<b>Comments</b>
\$ cd ch12/ch12-sixty \$ cargo run 23221 . 1 . 2 . 3 . 4		23221 appears as output because it is the <i>process identifier</i> (pid) for this invocation of <code>ch10-sixty</code> .
	\$ kill -SIGSTOP 23221	If you are unfamiliar with the shell command <code>kill</code> , its role is to send signals. It's named after its most common role, to send <code>SIGTERM</code> .
[1]+ Stopped cargo run \$		This console window will be returned to the prompt, as there is no longer anything running in the foreground.
	\$ kill -SIGCONT 23221	
. 5 . 6 . 7 . 8		

The default handling of `SIGSTOP` and `SIGCONT` provides utility without further tweaks. So what are the other signals and what are their default handlers?

### 12.2.2 Listing all signals supported by the operating system

We can ask `kill` for that information:

**Listing 12.5. Generating a list of signals that are supported on your operating system with the `kill` command**

```
$ kill -1 ①
 1) SIGHUP      2) SIGINT      3) SIGQUIT      4) SIGILL      5) SIGTRAP
 6) SIGABRT     7) SIGEMT      8) SIGFPE       9) SIGKILL     10) SIGBUS
11) SIGSEGV    12) SIGSYS     13) SIGPIPE     14) SIGALRM     15) SIGTERM
16) SIGURG     17) SIGSTOP     18) SIGSTP      19) SIGCONT     20) SIGCHLD
21) SIGTTIN    22) SIGTTOUT   23) SIGIO       24) SIGXCPU     25) SIGXFSZ
26) SIGVTALRM  27) SIGPROF    28) SIGWINCH   29) SIGPWR      30) SIGUSR1
31) SIGUSR2    32) SIGRTMAX
```

① -l stands for “list”

That’s a lot, Linux! To make matters worse, few signals have standardized behavior.

Thankfully, most applications don’t need to worry about setting handlers for many of them (if any). Here is a much tighter list of signals that are more likely to be encountered in day-to-day programming:

**Table 12.1. List of common signals, their default actions and tips for sending them from the command line**

Signal	Read as	Default Action	Comment	Shortcut
SIGHUP	Hung Up	Terminate	Its origins are from dialup modems. Now often sent to background applications (daemons/services) to request that they re-read their configuration files. Sent to running programs when you logout from a shell.	<b>CTRL + D</b>
SIGINT	Interrupt (or perhaps interactive)	Terminate	User-generated signal to terminate a running application.	<b>CTRL + C</b>
SIGTERM	Terminate	Terminate	Asks application to “gracefully” terminate.	
SIGKILL	Kill	Terminate (unstoppable)		
SIGQUIT	Quit	Write memory to disk as a <i>core dump</i> , then terminate.		<b>CTRL + \</b>
SIGTSTP	Terminal Stop	Pause execution	Application was requested to stop from the terminal	<b>CTRL + Z</b>
SIGSTOP	Stop	Pause execution (unstoppable)		
SIGCONT	Continue	Resume execution when paused		

Looking at the “Default Action” column, we can see that SIGKILL and SIGSTOP have special status. Programs are able to avoid the others. Those two cannot be handled or blocked by the application.

### 12.3 Handling signals with custom actions

The default actions for signals are fairly limited. Receiving a signal tends to end badly for applications by default. If external resources, such as a database connection, are left open, they might not be cleaned up properly when the application ends.

The most common use case for signal handlers is to allow an application to cleanly shutdown. Some common tasks that might be necessary when an application shuts

down:

- flushing the hard disk drive to ensure that pending data has been written to disk
- closing any network connections
- de-registering from any distributed scheduler or work queue

To stop the current workload and shut down, a signal handler is required. To set up a signal handler, we need to create a function with the signature `f(i32) → ()`. That is, the function needs to accept an `i32` integer as its sole argument and return no value.

This poses some software engineering issues. The signal handler isn't able to access any information from the application, except which signal was sent. Therefore it doesn't know what state anything is in and so can't know what needs shutting down beforehand.

There are some additional constraints, in addition to the architectural one. Signal handlers must also act very quickly, with a subset of functionality available to general code. They're constrained in time and scope.

Signal handlers must act quickly for two main reasons:

1. They're blocking other signals of the same type from being handled
2. Moving fast reduces the likelihood that they are operating alongside another signal handler of another type

Signal handlers have reduced scope in what they're permitted to do. For example, they must avoid executing any code that might itself generate signals.

To wriggle out of this constrained environment, the ordinary approach to this is to use a Boolean flag as a global variable that is regularly checked during a program's execution.

If the flag is set, then call a function to cleanly shutdown the application within the context of the application.

For this pattern to work, there are two requirements:

- the signal handler's sole responsibility is to mutate the flag
- the application's `main()` function regularly checks the flag to detect whether the flag has been modified

### **12.3.1 Global variables in Rust**

Rust facilitates global variables (variables accessible anywhere within the program) by declaring a variable with the `static` keyword in global scope. Suppose we wanted to create a global value `SHUT_DOWN` that we set to `true` when a signal handler believes it's time to urgently shut down. We use this declaration:

```
static mut SHUT_DOWN: bool = false;
```

`static mut` is read as “mutable static”, irrespective of how grammatically contorted that is.

Global variables presents an issue for Rust programmers. Accessing them—even for reading only—is `unsafe`. That can mean that the code can become quite cluttered, as it’s wrapped in `unsafe` blocks. This ugliness is a signal—avoid global state where possible.

Listing 12.8, presents a toy example of reading from (line 12) and writing to (lines 7–9) a `static mut` variable. The call to `rand::random()` on line 8 produces Boolean values. Output is a series of dots. 50%<sup>23</sup> of the time, you’ll receive an output that looks like this:

#### **Listing 12.6. Typical output produced by Listing 12.8**

.

#### **Listing 12.7. Crate metadata for Listing 12.8 (ch12/ch12-toy-global/Cargo.toml)**

```
[package]
name = "ch12-toy-global"
version = "0.1.0"
authors = ["Tim McNamara <tim.mcnamara@canonical.com>"]
edition = "2018"

[dependencies]
rand = "0.6"
```

#### **Listing 12.8. Accessing global variables (mutable statics) in Rust (ch12/ch12-toy-global/src/main.rs)**

```
use rand;

static mut SHUT_DOWN: bool = false;

fn main() {
    loop {
        unsafe {           ①
            SHUT_DOWN = rand::random(); ②
        }
        print!(".");

        if unsafe { SHUT_DOWN } {      ③
            break
        };
    }
    println!()
}
```

① Reading from and writing to a `static mut` variable requires an `unsafe` block

---

<sup>23</sup> Assuming a fair random number generator, which Rust uses by default. This assumption holds as long as you trust your operating system’s random number generator.

- ② `rand::random()` is a short-cut that calls `rand::thread_rng().gen()` to produce a random value.  
The required type is inferred from the type of `SHUT_DOWN`.
- ③ Because blocks evaluate to their last result, it's possible to use a block within

### 12.3.2 Using a global variable to indicate that shutdown has been initiated

Given that signal handlers must be quick and simple, we'll do the minimal work possible. We'll set a variable to indicate that the program needs to shut down. This technique is demonstrated by Listing 12.11

Listing 12.11 is structured into three functions:

`register_signal_handlers()`

Communicates to the operating system (via `libc`) what the signal handler for each signal is. This function makes use of a *function pointer*, which treats a function as data. Function pointers are explained at “[Understanding function pointers and their syntax](#)”.

`handle_signals()`

Handles incoming signals. This function is agnostic as to which signal is sent, although we'll only be dealing with `SIGTERM`.

`main()`

Initializes the program and iterates through a “main loop”.

When run, the resulting executable produces a trace of where it is:

#### Listing 12.9. Intended output from Listing 12.11

```

1
SIGUSR1
2
SIGUSR1
3
SIGTERM
4
*   ①

```

① I hope that you will forgive the cheap ASCII art explosion.

**NOTE**

If the signal handler was not correctly registered, the word “Terminated” may appear. Make sure that you've added a call to `register_signal_handler()` early within `main()`. Listing 12.11 does this on line 38.

#### Listing 12.10. Crate setup for Listing 12.11 (ch12/ch12-basic-handler/Cargo.toml)

```

[package]
name = "ch12-handler"

```

```

version = "0.1.0"
authors = ["Tim McNamara <code@timmcnamara.co.nz>"]

[dependencies]
libc = "0.2"

```

**Listing 12.11. Creating an basic signal handler that modifies a global variable when executed (ch12/ch12-basic-handler/src/main.rs)**

```

#![cfg(not(windows))]                                     ①

extern crate libc;                                       ②

use std::time;
use std::thread::{sleep};
use libc::{SIGTERM, SIGUSR1};                            ③
                                                        ④
                                                        ⑤

static mut SHUT_DOWN: bool = false;                      ⑥

fn main() {
    register_signal_handlers();

    let delay = time::Duration::from_secs(1);

    for i in 1_usize.. {                                ⑦
        println!("{}", i);
        unsafe {
            if SHUT_DOWN {
                println!("*");
                return;
            }
        }

        sleep(delay);

        let signal = if i > 2 {
            SIGTERM
        } else {
            SIGUSR1
        };
        unsafe {
            libc::raise(signal);
        }
    }
    unreachable!();
}

fn register_signal_handlers() {
    unsafe {
        libc::signal(SIGTERM, handle_sigterm as usize);  ⑦
        libc::signal(SIGUSR1, handle_sigusr1 as usize);   ⑧
    }
}

```

```

}

#[allow(dead_code)]
fn handle_sigterm(_signal: i32) {
    register_signal_handlers();

    println!("SIGTERM");

    unsafe {
        SHUT_DOWN = true;
    }
}

#[allow(dead_code)]
fn handle_sigusr1(_signal: i32) {
    register_signal_handlers();

    println!("SIGUSR1");
}

```

- ① Indicates to cargo/rustc that this code won't run on MS Windows.
- ② Imports the libc crate, enabling access to the kernel's functionality, such as signals.
- ③ Brings the Duration type into scope, enabling us to represent spans of time.
- ④ Enables our program to pause its execution.
- ⑤ Brings the two signal constants into local scope.
- ⑥ Initialize a Boolean mutable static to false.
- ⑦ Calling functions within libc requires an unsafe block, as it's outside of Rust's control.
- ⑧ `libc::signal` takes a signal name (technically, an integer) and an address of a function (a *function pointer*, albeit untyped) as arguments and associates the signal with the function
- ⑨ Why `usize? libc::signal()` requires an integer as its second argument. As *function pointers*, `handle_sigterm` and `handle_sigusr1` have the type `fn(i32) → ()`.
- ⑩ Without this attribute, rustc warns that this function is never run.

### ***Understanding the difference between const and static***

Static and constant seem similar. Here is the main difference:

- `static` values appear in a single location in memory
- `const` values may be duplicated in locations where they're accessed

Duplicating `const` values can be a CPU-friendly optimization. It allows for data locality and improved cache performance.

Why use confusingly similar names for two different things? It could be considered a historical accident.

The word `static` refers to the segment of the address space that the variables live in. `static` values live outside of the stack space. They live within the region where string literals are held, near the bottom of the address space. That means, accessing a `static` variable almost certainly implies a dereferencing a pointer.

The constant in `const` values refers to the value itself. When accessed from code, the data might get duplicated to every location that it's needed, if the compiler believes that will result in faster access.

## 12.4 Sending application-defined signals

Signals can be used as a limited form of messaging. Within your business rules, create definitions for `SIGUSR1` and `SIGUSR2`. They're unallocated by design. In Listing 12.11 , we use `SIGUSR1` to do very little work.

### 12.4.1 Understanding function pointers and their syntax

Listing 12.11 includes some syntax that might be confusing:

```
handle_sigterm as usize
```

What is happening here? The address that the function is stored at is being converted to an integer. In Rust, the `fn` keyword creates a *function pointer*.

Readers who have worked through chapter 5 will understand that functions are just data. That is to say they're sequences of bytes that make sense to the CPU. A function pointer is a pointer to the start of that sequence.

A pointer is a data type that acts as a stand-in for its referent. Within an application's source code, pointers contain both the address of the value referred to as well as its type. The type information is something that's stripped away in the compiled binary. Their internal representation is an integer of `usize`. That makes pointers very cheap to pass around. In C, making use of function pointers can feel like arcane magic. In Rust, they're hiding in plain sight.

Every `fn` declaration is actually a function pointer. That means, that Listing 12.13 is legal code and should print out something similar to the following line:

#### Listing 12.12. Expected output from Listing 12.13

```
noop as usize: 0x5620bb4af530 ①
```

① `0x5620bb4af530` is the memory address (in hexadecimal notation) of the start of the `noop()` function. This number will be different on your machine.

#### Listing 12.13. Casting a function to usize to demonstrate that it is being used as a function pointer.

```
fn noop() {}

fn main() {
    let fn_ptr = noop as usize;

    println!("noop as usize: 0x{:x}", fn_ptr);
}
```

But what is the type of the function pointer created from `fn noop()`? To describe

function pointers, Rust re-uses its function signature syntax. In the case of `fn noop()`, the type is `*const fn() -> ()`. This type is read as “a const pointer to a function that takes no arguments and returns unit”. A *const pointer* is immutable and *unit* is Rust’s stand-in value for nothingness.

Listing 12.15 adds a second type cast. Its output should two lines that should be mostly identical:

#### **Listing 12.14. Exepected output from Listing 12.15**

```
noop as usize: 0x55ab3fdb05c0 ①
noop as *const T: 0x55ab3fdb05c0 ①
```

- ① These two numbers will be different on your machine, but they should match each other.

#### **Listing 12.15. Casting a function to usize to demonstrate that it is being used as a function pointer.**

```
fn noop() {}

fn main() {
    let fn_ptr = noop as usize;
    let typed_fn_ptr = noop as *const fn() -> ();

    println!("noop as usize: 0x{:x}", fn_ptr);
    println!("noop as *const T: {:p}", typed_fn_ptr); ①
}
```

- ① Note the use of the pointer format modifier `:p`

## **12.5 Ignoring signals**

As illustrated earlier by Table 12.1 , most signals terminate the running program by default. This can be somewhat disheartening for the running program attempting to get its work done. Sometimes the application knows best. For those cases, many signals can be ignored.

`SIGSTOP` and `SIGKILL` aside, the constant `SIG_IGN` can be provided to `libc::signal()`, instead of a function pointer. An example of its usage is provided by Listing 12.17 , which prints the following line to the console:

#### **Listing 12.16. Output from Listing 12.17**

```
ok
```

**Listing 12.17. Ignoring signals with libc::SIG\_IGN, then resetting them to their default handling behavior.**

```
extern crate libc;

use libc::{signal,raise};
use libc::{SIG_DFL, SIG_IGN, SIGTERM};

fn main() {
    unsafe {                                     ①
        signal(SIGTERM, SIG_IGN);               ②
        raise(SIGTERM);                         ③
    }
    println!("ok");

    unsafe {                                     ④
        signal(SIGTERM, SIG_DFL);               ⑤
        raise(SIGTERM);                         ⑥
    }
    println!("not ok");
}
```

- ① An unsafe block is required because Rust does not control what happens beyond the function boundaries.
- ② Set the SIGTERM signal to ignore.
- ③ `libc::raise()` allows code to make a signal, in this case to itself.
- ④ Reset the SIGTERM signal to its default.
- ⑤ Program terminates here.
- ⑥ This code is never reached, and therefore this string is never printed.

## 12.6 Shutting down from deeply nested call stacks

What if our program is deep in the middle of a call stack and can't afford to unwind? When receiving a signal, the program might want to execute some clean up code before terminating (or being forcefully terminated). This is sometimes referred to as *nonlocal control transfer*.

UNIX-based operating systems provide some tooling to enable you to make use of that machinery via two system calls: `setjmp` and `longjmp`.

- `setjmp` sets a marker location
- `longjmp` jumps back to the previously marked location

Why bother with such programming gymnastics? Sometimes using low-level techniques like these is the only way out of a tight spot. They approach the Dark Arts of systems programming. To quote the manpage:

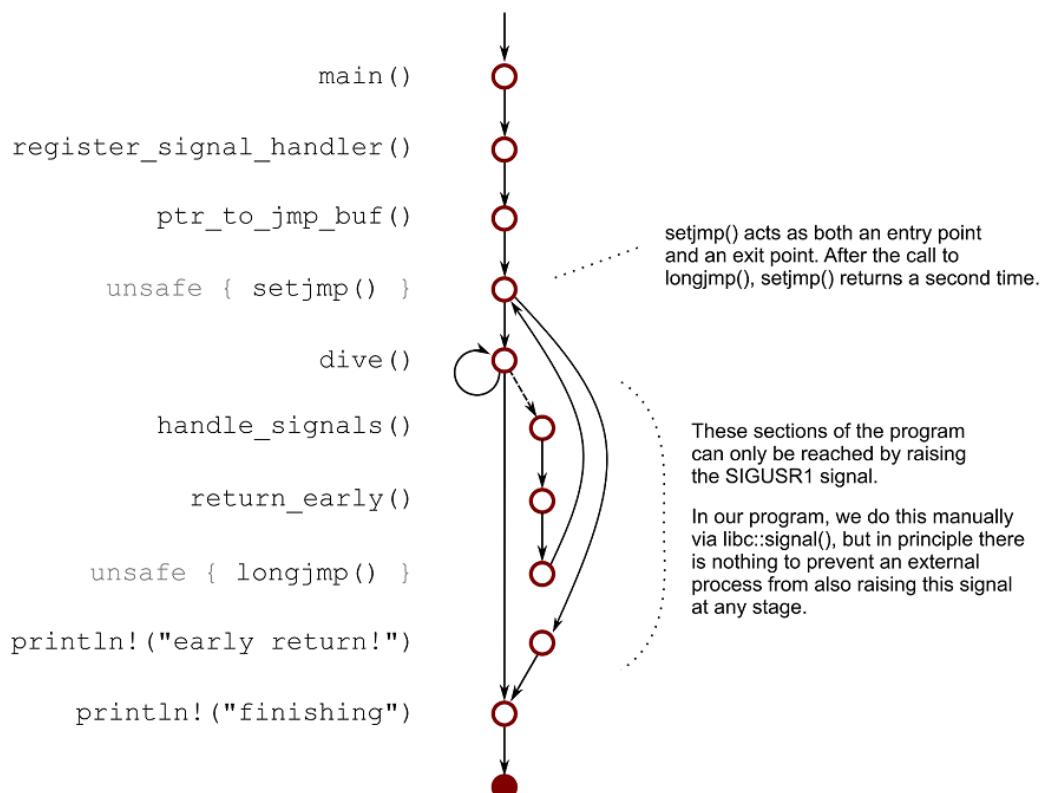
*setjmp() and longjmp() are useful for dealing with errors and interrupts encountered in a low-level subroutine of a program.*

-- Linux Documentation Project: setjmp(3)

These two tools circumvents normal control flow and allow programs to teleport themselves through the code. Occasionally an error occurs deep within a call stack. If our program takes too long to respond to the error, the operating system may simply abort the program and the program's data may be left in an inconsistent state. To avoid this, `longjmp` can be used to shift control directly to the error-handling code.

To understand what significance of this is, consider what happens in an ordinary program's callstack during several calls to a recursive function as shown in Listing 12.18 . Each call to `dive()` adds another place that control will eventually return to. `longjmp` is used to bypass them.

**Figure 12.5. Control flow graph of the code from Listing 12.23 . The program's control flow can be intercepted via a signal and then resume from point of setjmp()**



**Table 12.2. Comparing the intended output from Listing 12.18 and Listing 12.23 .**

<p>Listing 12.18 produces a symmetrical pattern. Each level is caused by a nested call to <code>dive()</code>, which is removed when the calls return.</p> <pre># ## ### #### ##### ##### #### ### #</pre>	<p>Listing 12.23 produces a much different pattern. After a few calls to <code>dive()</code>, control teleports back to <code>main()</code> without the calls to <code>dive()</code> returning.</p> <pre># ## ### early return! finishing!</pre>
--	--

On the right-hand side, the code jumps directly from the third call to the top to the call stack.

**Listing 12.18. Illustrating how the callstack operates by printing its progress as the program executes (ch10/ch10-callstack/src/main.rs)**

```
fn print_depth(depth: usize) {
    for _ in 0..depth {
        print!("#");
    }
    println!("");
}

fn dive(depth: usize, max_depth: usize) {
    print_depth(depth);
    if depth >= max_depth {
        return;
    } else {
        dive(depth+1, max_depth);
    }
    print_depth(depth);
}

fn main() {
    dive(0, 5);
}
```

Now... there's a lots of work to do to make this work.

The Rust language itself doesn't have the tools to enable this control flow trickery. It needs to access some provided by its compiler toolchain. Compilers provide special functions known as *intrinsics* to application programs. Using an *intrinsic function* from Rust takes some ceremony to set up, but operates a standard function once that set up is in-place.

### 12.6.1 Setting up intrinsics in a program

Listing 12.23 uses two intrinsics, `setjmp()` and `longjmp()`. To enable them in our programs, the crate must be annotated with the following attribute:

**Listing 12.19. Crate-level attribute required in `main.rs` (ch12/ch12-sjlj/src/main.rs)**

```
#![feature(link_llvm_intrinsics)]
```

This raises two immediate questions that will be answered fully shortly:

1. What is an intrinsic function?
2. What is LLVM?

Additionally, we need to tell Rust about the functions that are being provided by LLVM. Rust won't know anything about them apart from their type signatures, which means that any use of them must occur within an `unsafe` block.

**Listing 12.20. Declaring the LLVM intrinsic functions within Listing 12.23 (ch12/ch12-sjlj/src/main.rs)**

```
#![allow(non_camel_case_types)]  
extern "C" {  
    #[link_name = "llvm.setjmp"]  
    pub fn setjmp(a: *mut i8) -> i32;  
  
    #[link_name = "llvm.longjmp"]  
    pub fn longjmp(a: *mut i8, b: i32) -> ();  
}
```

(1)

(1) Used to silence a warning provided by `rustc`

This small section of code contains a fair amount of complexity.

- `extern "C"` means, "this block of code should obey C's conventions, rather than Rust's own ones
- The `link_name` attribute tells the linker where to find the two functions that we're declaring
- `*mut i8` is a pointer to a signed byte. For those with C programming experience, you may recognize this as the pointer to the beginning of a string, e.g. a `*char` type.

## WHAT IS AN INTRINSIC FUNCTION?

Intrinsic functions, generally referred to as *intrinsics*, are functions made available via the compiler, rather than as part of the language. The compiler has greater access to the environment and can therefore . For example, a compiler understands the characteristics of the CPU that the to-be-compiled program will run on.

Intrinsic functions generally take one of two forms:

## Access to specialized instructions

Many CPUs provide specialist instructions for optimized certain workloads. For example, the CPU may guarantee that updating an integer is an *atomic operation*. Atomic here is meant in the sense of being indivisible. This can be extremely important when dealing with concurrent code.

## Access to CPU-specific error handling

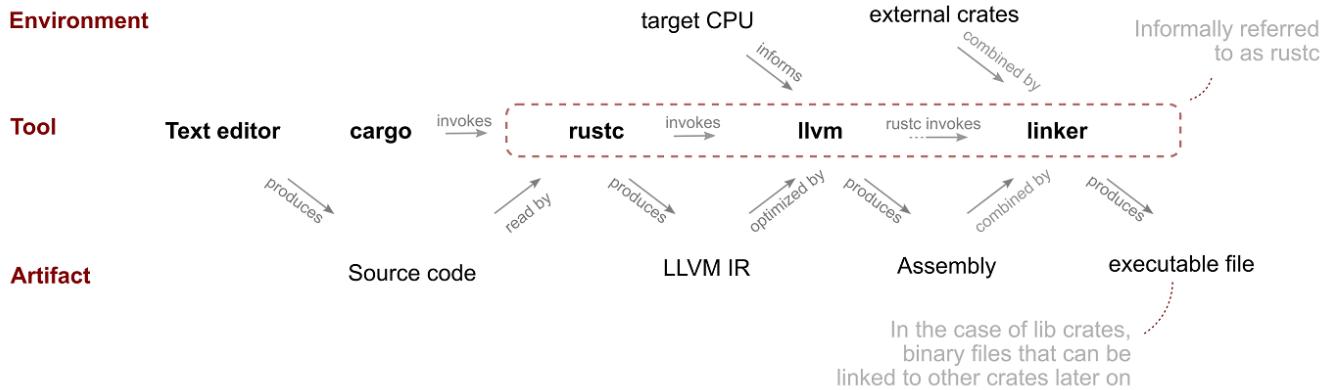
The facilities provided by CPUs for managing exceptions differ products. `setjmp` and `longjmp` fall into this camp.

## WHAT IS LLVM?

From the point of view of Rust programmers, LLVM can be considered as a subcomponent of `rustc`, the Rust compiler. It's an external tool that's bundled with `rustc`. Rust programmers can draw from tools that it provides. One set of tools that LLVM provides is intrinsic functions.

LLVM is itself a compiler. Its role is illustrated at Figure 12.6 .

**Figure 12.6. Some of the major steps required to generate an executable from Rust source code. LLVM is an essentialy part of the process, but one that is not user-facing.**



It translates code produced by `rustc`, which produces LLVM IR (intermediate language), into machine-readable assembly language. To make matters more complicated, another tool, called a linker, is required to stitch multiple crates together. On MS Windows, Rust uses `link.exe`, a program provided by Microsoft, as its linker. On other operating systems, the GNU linker `ld` is used.

Understanding more detail about LLVM implies learning more about `rustc` and compilation in general. Like many things, getting closer to the truth requires perserving through a fractal-like domain. Learning every sub-system seems to require learning about another set of sub-systems. Explaining more here would be a fascinating—but ultimately distracting—diversion.

## 12.6.2 Casting a pointer to another type

One of the more arcane parts of Rust's syntax is how to cast between pointer types. You'll encounter this as you make your way through Listing 12.23 . Problems arise because of the type signature of `setjmp()` and `longjmp()`:

```
extern "C" {
    #[link_name = "llvm.setjmp"]
    pub fn setjmp(a: *mut i8) -> i32;

    #[link_name = "llvm.longjmp"]
    pub fn longjmp(a: *mut i8, b: i32) -> ();
}
```

`setjmp()` and `longjmp()` both require a `*mut i8` as an input argument, yet the type that our Rust code is working with is `&jmp_buf`<sup>24</sup>. The `jmp_buf` type is defined like this:

```
const JMP_BUF_WIDTH: usize = mem::size_of::<usize>() * 8;      ①
type jmp_buf = [i8; JMP_BUF_WIDTH];                            ②
```

- ① This constant will be 64 bits (8 bytes) in 64-bit machines and 32 bits (4 bytes) on 32-bit machines.
- ② We need enough storage available to store 8 or so integers. These bytes will be enough to for `setjmp()` to store a snapshot of the program's current state.

There is only 1 `jmp_buf` value within our program, a global mutable static called `RETURN_HERE`:

```
static mut RETURN_HERE: jmp_buf = [0; JMP_BUF_WIDTH];
```

Thus arises our requirement to learn how to cast pointer types. Within the Rust code, we refer to `RETURN_HERE` as a reference, e.g. `&RETURN_HERE`. LLVM expects those bytes to be presented as a `*mut i8`.

To perform the conversion, there are multiple steps:

```
unsafe { &RETURN_HERE as *const i8 as *mut i8 }
```

Unpacking the conversion steps leads to this sequence:

- Start with `&RETURN_HERE`, a read-only reference to a global static variable of type `[i8; 8]` (or `[i8; 4]` on 32-bit machines)
- Convert that reference to a `*const i8`. Casting between pointer types is considered safe Rust, but dereferencing that pointer requires an `unsafe` block.
- Convert the `*const i8` to a `*mut i8`. This declares the memory as mutable (read/write).
- Wrap the conversion in an `unsafe` block, because it is dealing with access to a global variable

---

<sup>24</sup> `jmp_buf` is the conventional name for this buffer, which might be useful for any readers who wish to dive deeper themselves.

Why not use something like `&mut RETURN_HERE as *mut i8?` The Rust compiler becomes quite concerned about giving LLVM access to its data. The approach provided here, starting with a read-only reference, puts it at ease.

### **12.6.3 Running the Linux-specific code from Listing 12.23 in other operating systems via Docker**

**INFO**
**Note to MEAP readers:**

Docker installation instructions will appear within the book's appendices. Please use the book's forum ([forums.manning.com/forums/rust-in-action](https://forums.manning.com/forums/rust-in-action)) if you require any assistance before the appendix is available.

The code in Listing 12.23 does not run on MS Windows. To minimize this issue, we can use virtualization. Docker is a virtualization technology for Linux that enables you to create isolated environments. Docker Inc. also provides interfaces to enable macOS and MS Windows users to make use of Docker from within host operating system.

Listing 12.21 provides a fairly complex Dockerfile. Docker will use it to create two Docker containers that result in a static binary that can be copied into any Linux-based operating system.

**Listing 12.21. Dockerfile for Listing 12.23 (ch12/ch12-sj1j/Dockerfile)**

```
FROM rust:latest as intermediate
RUN rustup toolchain install nightly
RUN rustup default nightly
RUN rustup target add x86_64-unknown-linux-musl

ENV PATH $PATH:/root/.cargo/bin
ENV PKG_CONFIG_ALLOW_CROSS=1

# fetch dependencies using a minimal project,
# enabling the docker image to be cached with dependencies installed
RUN USER=root cargo new --bin project
WORKDIR /project

COPY ./Cargo.lock ./Cargo.lock
COPY ./Cargo.toml ./Cargo.toml

# build actual project
COPY ./src ./src
RUN cargo +nightly -v check
RUN cargo +nightly -v build --target x86_64-unknown-linux-musl
RUN ls -R /project/target

FROM alpine
COPY --from=intermediate /project/target/x86_64-unknown-linux-musl/debug/ch12-sj1j /
CMD /ch12-sj1j
```

## 12.6.4 Compiling the code

We're now in a position where possible points of confusion within Listing 12.23 should be minor. As it has been several pages, here again is the behavior that we're attempting to replicate:

### Listing 12.22. Expected output from Listing 12.23

```
#  
##  
###  
early return!  
finishing!
```

One final note. Listing 12.23 requires that `rustc` is on the nightly channel to compile correctly. If you encounter the following error, use `rustup` via the command line to install it `rustup install nightly`.

```
error[E0554]: #![feature] may not be used on the stable release channel  
--> src/main.rs:1:1  
|  
1 | #![feature(link_llvm_intrinsics)]  
| ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^  
  
error: aborting due to previous error  
  
For more information about this error, try `rustc --explain E0554`.
```

Once installed, you can request that `cargo` invokes the nightly compiler by adding `+nightly` to your command line scripts, e.g. `cargo +nightly build` and `cargo +nightly run`.

### Listing 12.23. Using LLVM's internal compiler machinery (“intrinsics”) to access the operating system's `longjmp` facilities. `longjmp` allows programs to escape their stack frame and jump anywhere within their address space. (ch12/ch12-sjlj/src/main.rs)

```
#![feature(link_llvm_intrinsics)]  
#![allow(non_camel_case_types)]  
#![cfg(not(windows))]  
  
extern crate libc;  
  
use libc::{SIGUSR1, SIGALRM, SIGHUP, SIGQUIT, SIGTERM};  
use std::mem;  
  
const JMP_BUF_WIDTH: usize = mem::size_of::<usize>() * 8;  
type jmp_buf = [i8; JMP_BUF_WIDTH];  
  
static mut SHUT_DOWN: bool = false;  
static mut RETURN_HERE: jmp_buf = [0; JMP_BUF_WIDTH];
```

```

const MOCK_SIGNAL_AT: usize = 3;                                ⑤

extern "C" {
    #[link_name = "llvm.setjmp"]
    pub fn setjmp(a: *mut i8) -> i32;

    #[link_name = "llvm.longjmp"]
    pub fn longjmp(a: *mut i8, b: i32) -> ();
}

#[inline]                                                       ⑥
fn ptr_to_jmp_buf() -> *mut i8 {
    unsafe { &RETURN_HERE as *const i8 as *mut i8 }
}

#[inline]                                                       ⑥
fn return_early() {
    let franken_pointer = ptr_to_jmp_buf();
    unsafe { longjmp(franken_pointer, 1) };                      ⑦
}

fn register_signal_handler() {                                  ⑧
    unsafe {                                                     ⑦
        libc::signal(SIGUSR1, handle_signals as usize);          ⑨
    }
}

#[allow(dead_code)]                                         ⑩
fn handle_signals(_signal: i32) {                           ⑪
    register_signal_handler();

    unsafe {
        SHUT_DOWN = true;
    }

    return_early();
}

fn print_depth(depth: usize) {
    for _ in 0..depth {
        print!("#");
    }
    println!("");
}

fn dive(depth: usize, max_depth: usize) {                    ⑫
    unsafe {
        if SHUT_DOWN == true {
            println!("!");
            return;
        }
    }
    print_depth(depth);
}

```

```

if depth >= max_depth {
    return;
} else if depth == MOCK_SIGNAL_AT {
    unsafe {
        libc::raise(SIGUSR1);
    }
} else {
    dive(depth + 1, max_depth);
}
print_depth(depth);
}

fn main() {
    const JUMP_SET: i32 = 0;

    register_signal_handler();

    let return_point = ptr_to_jmp_buf();
    let rc = unsafe { setjmp(return_point) };
    if rc == JUMP_SET {
        dive(0, 10);
    } else {
        println!("early return!");
    }

    println!("finishing!")
}

```

- ① This attribute prevents the code from compiling on MS Windows, which has different low-level internals. If you're using an MS Windows machine, then consider using the Docker route outlined at [12.6.3](#).
- ② Our code only uses a single signal, SIGUSR1, but it's possible to write a signal handler that handles more than one. Bringing them into scope aids readability later on.
- ③ When this flag is true, the program will initiate its shut down code.
- ④ A buffer to hold a checkpoint of the program's current register state when `setjmp()` is called
- ⑤ Only allow a recursion depth of 3
- ⑥ An `#[inline]` attribute marks the function as being available for *inlining*, which is a compiler optimization technique for eliminating the cost of function calls.
- ⑦ Calling LLVM intrinsics requires an unsafe block. Rust can't make any guarantees about what happens on the other side of the function barrier.
- ⑧ This function only registers one of the many signals that have been pulled into local scope for brevity
- ⑨ Ask libc to associate the `handle_signals` function with the SIGUSR1 signal.
- ⑩ `#[allow(dead_code)]` silences a warning from the Rust compiler. During normal operation, a signal handler would never be reached and so Rust marks it as unreachable.
- ⑪ Immediately re-register signal handlers minimizes the chances of a missing a signal while handling this one.
- ⑫ A recursive function that returns once `max_depth` (or `MOCK_SIGNAL_AT`) has been reached.

## 12.7 A note on applying these techniques to platforms without signals

Signals are a UNIX-ism. In other platforms, messages from the operating system are handled differently.

On MS Windows, for example, command-line applications need to provide a handler function via `SetConsoleCtrlHandler` to the kernel. That handler function is then invoked from a when a “signal” is sent to the application.

Regardless of the specific mechanism, the high-level approach demonstrated in this chapter should be fairly portable.

Here is the pattern:

- Your CPU generates interrupts that it requires the operating system to respond to
- Operating systems often delegate responsibility for handling interrupts via some sort of callback system
- A callback system means creating function pointer

## 12.8 Revising exceptions

At the start of the chapter, we discussed the distinction between signals, interrupts and exceptions. There has been very little coverage of exceptions directly. We have treated them as a special class of interrupts. Interrupts themselves have been modelled as signals.

## 12.9 Summary

On the Rust side, we have spent lots of time interacting with `libc` and unsafe blocks, unpacking function pointers, tweaking global variables and beginning to explore some of the features available in `rustc` and LLVM. The bulk of the chapter though has been utilising these features to work with signals. Within Linux, signals are the main mechanism that the operating system communicates with applications.

You have learned:

- the differences between traps, exceptions and interrupts are
- that hardware devices, such as the network, notify applications about data to be processed via interrupting the CPU
- what a signal is
- what the effects of delegating signal handling to the system’s defaults are
- how to set up a signal handler
- how UNIX manages job control via `SIGSTOP` and `SIGCONT`
- what a function pointer is and how they can be defined and shared
- how to ignore signals
- how to escape the general function call/return procedure via `setjmp` and `longjmp`
- what LLVM is and how the Rust compiler uses it to build software