Binutils

Igor Półchłopek

Plan Prezentacji(system x86_64-linux-gnu – Ubuntu 18.04 (bionic))

1. Przedstawienie czym są narzędzia Binutils i do czego służą.
2. Biblioteka BFD
3. Jak działa kompilacja na przykładzie g++
4. Narzędzie as - GNU assembler
5. Narzędzie ld - GNU linker
6. Narzędzie ar/ranlib – GNU Archive Command
7. Inne narzędzia binutils

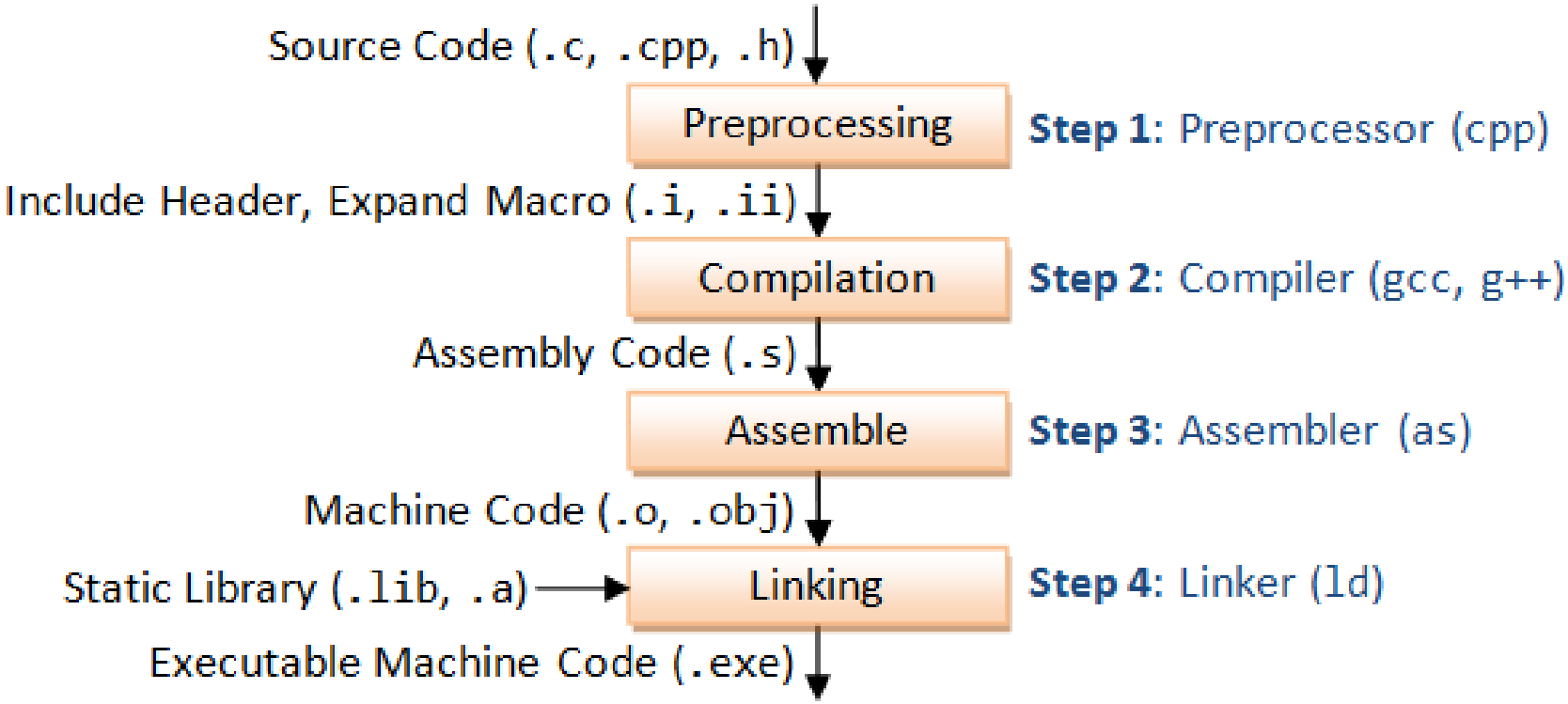
Czym są Binutils? Jakie mają zastosowanie?

ld	as	addr2line
ar	c++filt	dlltool
gold	gprof	nlmconv
nm	objcopy	objdump
ranlib	readelf	size
strings	strip	windmc
	windres	

Biblioteka BFD

- BFD - Binary File Descriptor
- Język programowania - C
- Autor - Cygnus Solutions
- Główny mechanizm Projekt`u GNU
- Wspiera ponad 50 formatów plików oraz ponad 25 modeli programowych procesora(architektur procesora)
- Korzystają z niej narzędzia Binutils

Kompilacja g++



as - GNU assembler

- Znany również pod nazwą gas
- Tworzy z plików assemblera pliki objektowe
- Tworzone są pliki w formacie ELF

ld - GNU linker

- Służy do połączenia plików obiektowych oraz archiwalne(biblioteczne)
- Rozwiązuję symbole
- Jest to ostatni etap kompilacji
- Zachowanie komendy ld opisuje linker script(jeśli nie utworzymy generowany jest automatycznie)

ar/ranlib - GNU Archive Command

- Służy do generowania i manipulowania archiwami
- Archiwum jest to pojedynczy plik, zawierający zbiór innych plików.
- Struktura archiwów umożliwia wyciągnięcie z niego oryginalnych plików

Biblioteka dynamiczna – shared library, rodzaj biblioteki, która łączona jest z programem wykonywalnym dopiero w momencie jego wykonania. Dane z bibliotek dynamicznych mogą być współdzielone przez różne programy jednocześnie. Biblioteki są ładowane do pamięci tylko raz, nawet jeśli są równocześnie współużytkowane.

nm

- Wypisuje symbole zawarte w plikach
- Wypisuje adres, typ oraz nazwę każdego symbolu
- Rozróżnia symbole lokalne oraz globalne poprzez zapis symbolu małą bądź wielką literą

nm – lista symboli

- A : Global absolute symbol.
- a : Local absolute symbol.
- B : Global bss symbol.
- b : Local bss symbol.
- D : Global data symbol.
- d : Local data symbol.
- f : Source file name symbol.
- L : Global thread-local symbol (TLS).
- l : Static thread-local symbol (TLS).
- T : Global text symbol.
- t : Local text symbol.
- U : Undefined symbol.

objdump

- Wyświetla informacje z plików obiektowych
- Dzięki wielu opcjom możemy wyświetlić tylko interesującą nas część informacji
- Może być użyte do deasemblacji

objcopy

- Kopiuje zawartość pliku obiektowego
- Potrafi utworzyć plik docelowy w innym formacie niż plik źródłowy
- Nie potrafi zmienić kolejności bajtów(byte order, endianness)

strip

- Służy do usuwania zbędnych symboli z pliku
- Może zmniejszyć rozmiar pliku oraz przyśpieszyć działanie programu

strings

- Wyświetla wszystkie możliwe do odczytania sekwencje charów(składające się z przynajmniej 4 znaków)
- Domyślnie szuka tylko w sekcji .data
- Użyty na pliku wykonywalnych wyświetla dodatkowo informacje dodane podczas linkowania

size

- Wyświetla rozmiar poszczególnych sekcji
- Działa tylko na plikach objektowych i wykonywalnych

c++filt

- Wspiera przeciążanie, które pozwala funkcji o takiej samej nazwie przyjąć inny rodzaj bądź inną ilość argumentów
- Wykorzystuje dekorowanie nazw(mangling)

Dziękuję za uwagę!!