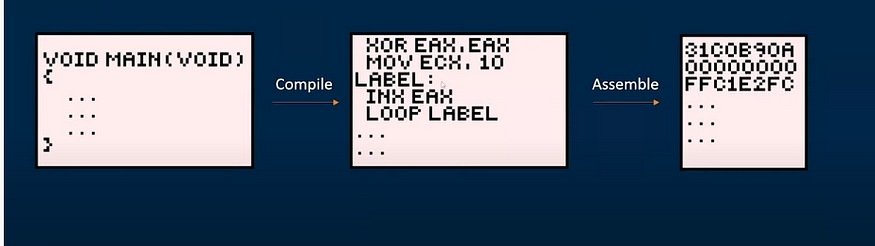
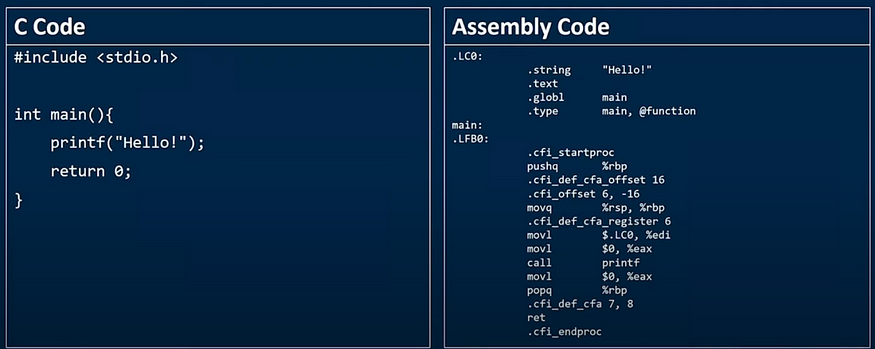
Ghidra , ücretsiz bir tersine mühendislik aracıdır. Tersine mühendislik araçları yürütülebilir hale getirilmiş kodları(genelde asm kodları) kaynak koda dönüştürerek kullanıcıların kodların nasıl çalıştığını anlamasını sağlar.

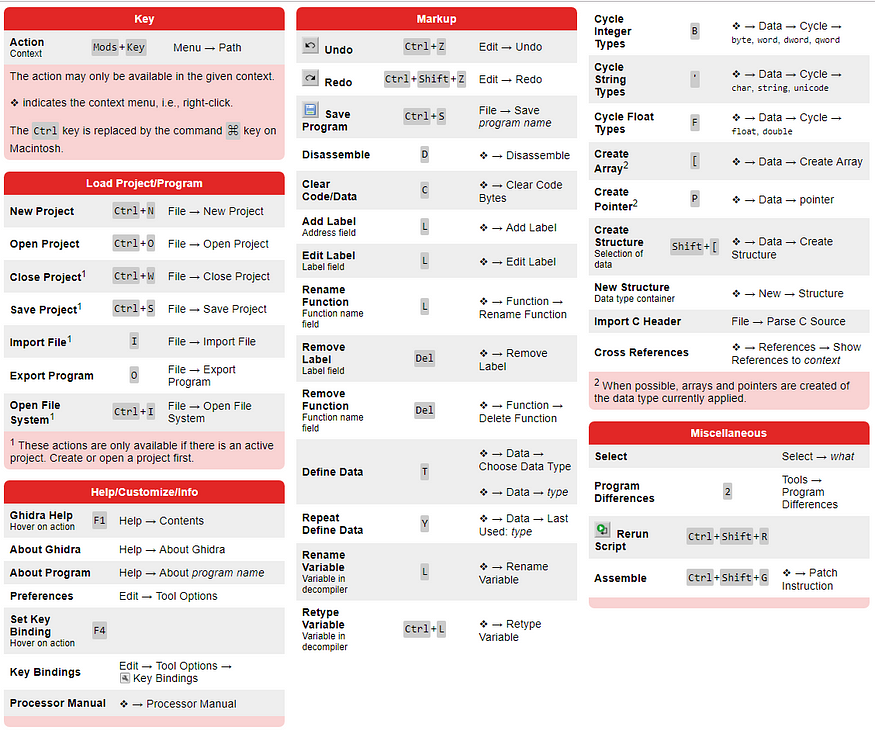
C programlama veya biraz assembly bilginiz varsa, çok seveceğinize eminim.

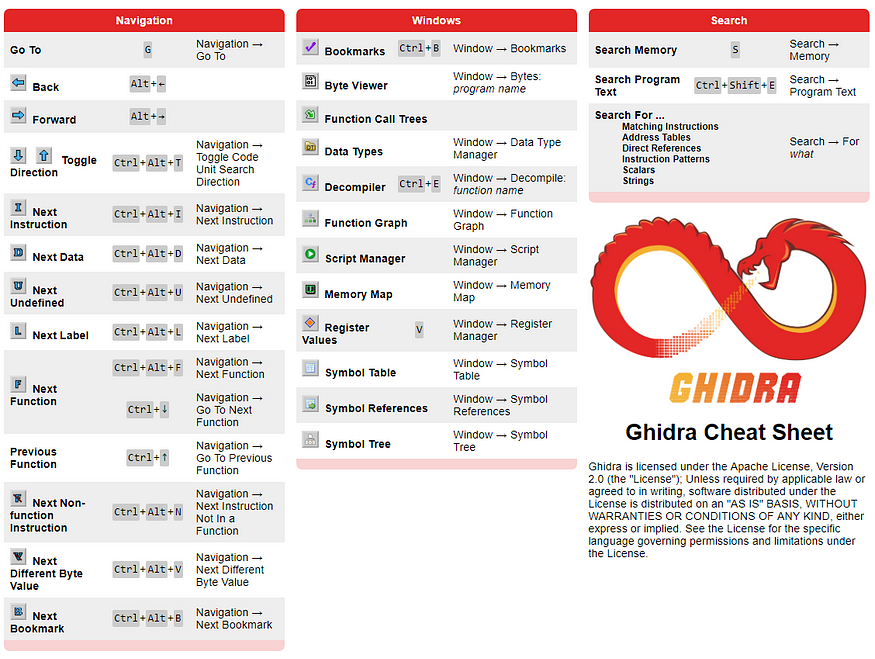
Aslında burada amaç aşagıda gösterilen sağdaki kodu soldaki gibi analiz etmeye çalışmaktır.





**Ghidra Cheat Sheet:**





Derleme işleminin çıktısı birçok şekilde olabilir.

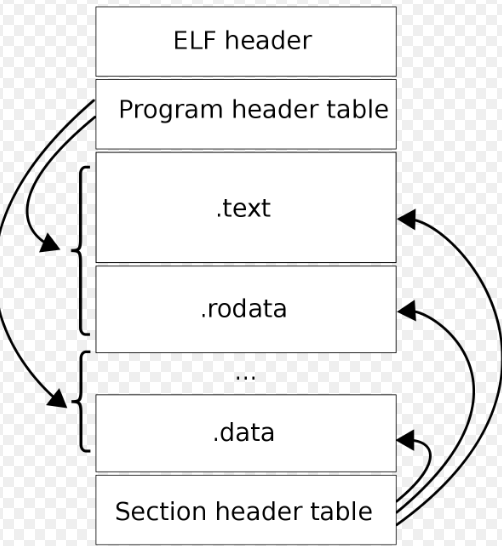
*PE(windows)*

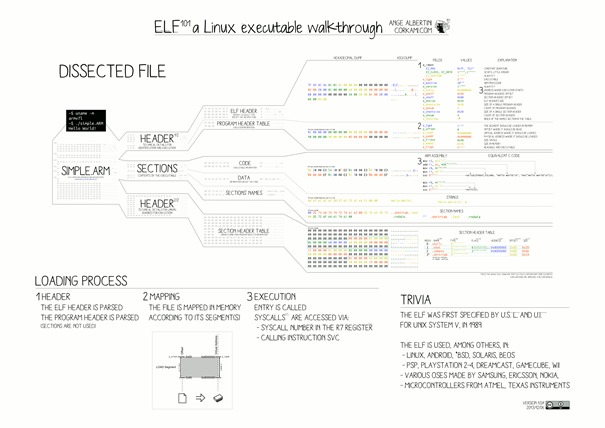
*ELF(Linux)*

*COFF/ECOFF*

ELF (Executable and Linkable Format File)ELF dosyaları, işletim sistemi tarafından yürütülmesi için gereken bilgileri sağlar.üç bileşene ayrılır :

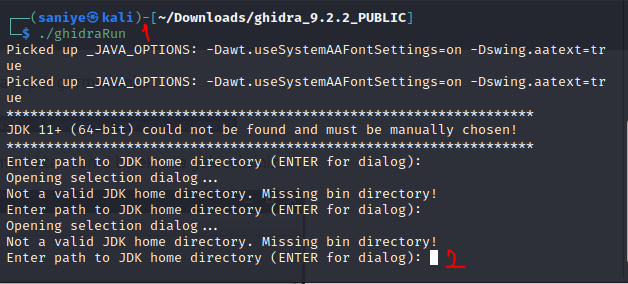
ELF Header , Sections , segments





Ghidra kurmaya başlayalım :

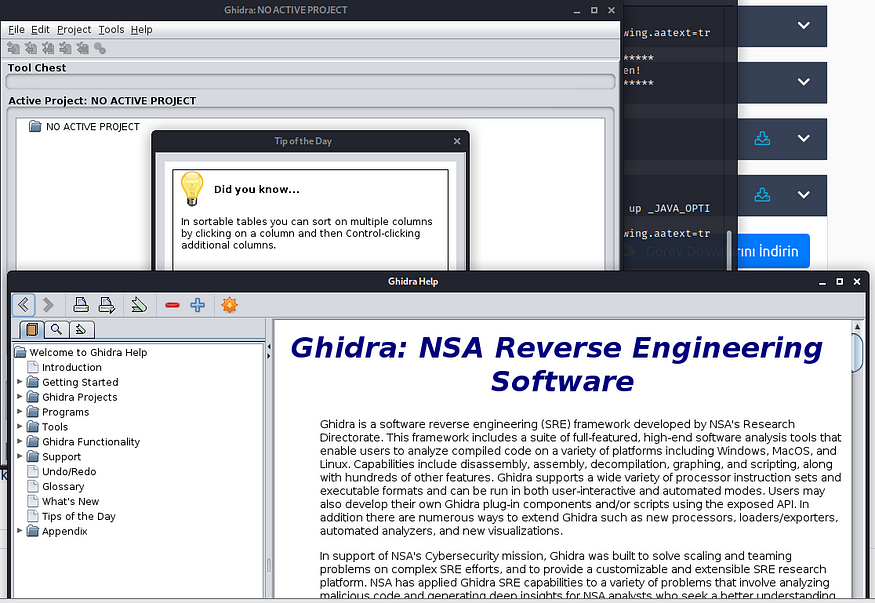
önce buradan indirelim . (Jre veya jdk olmadan açamayacaksınız)

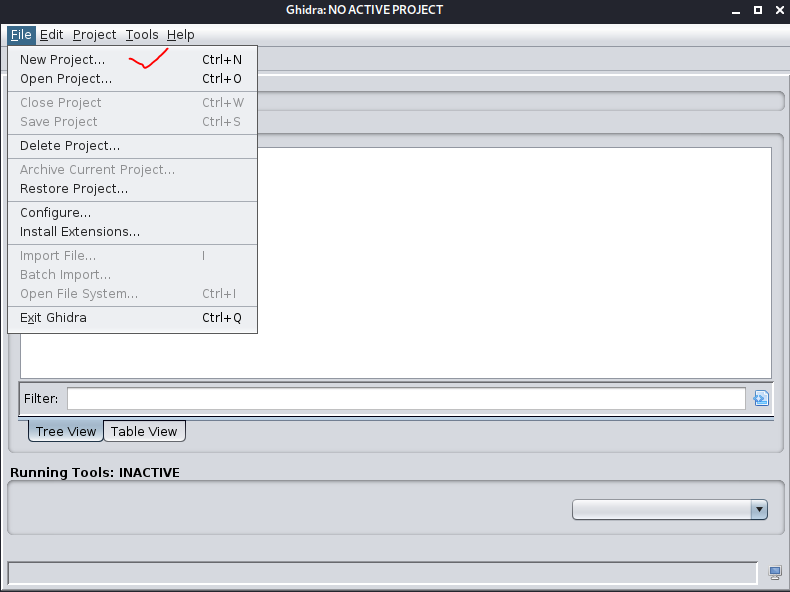


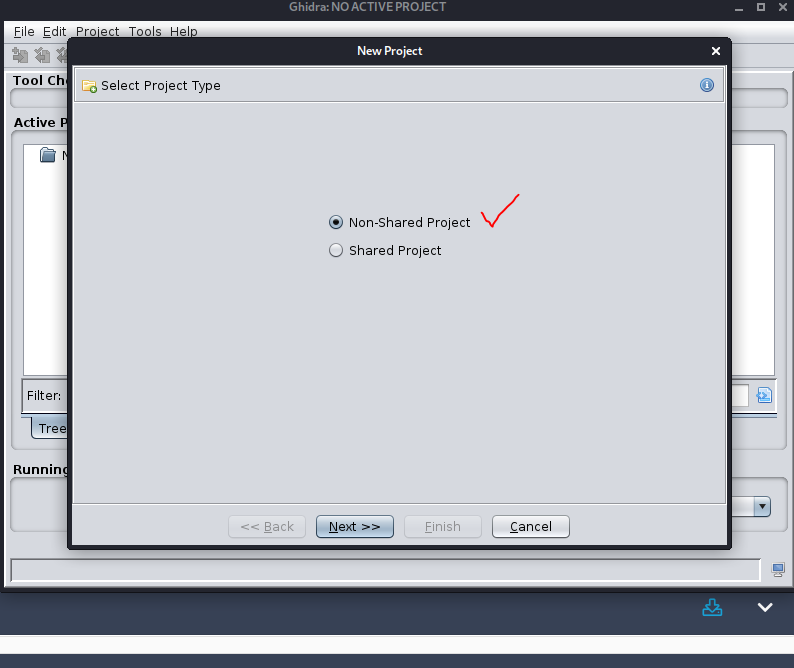
jdk kurulum :

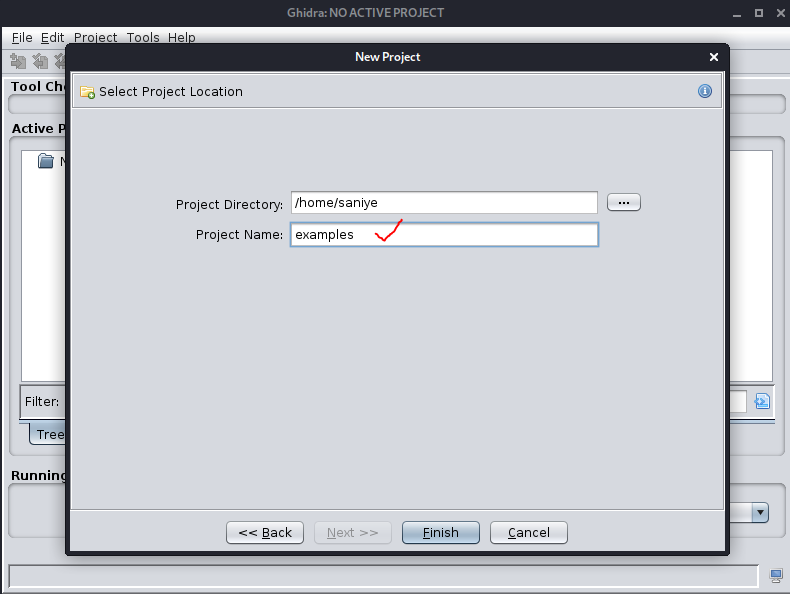
*sudo apt install -y default-jdk*

jdk kurulumundan sonra yukarıda yarım kalan enter for dialog kısmına tıklayarak işleme devam edelim ghidra otomatik açılıyor:

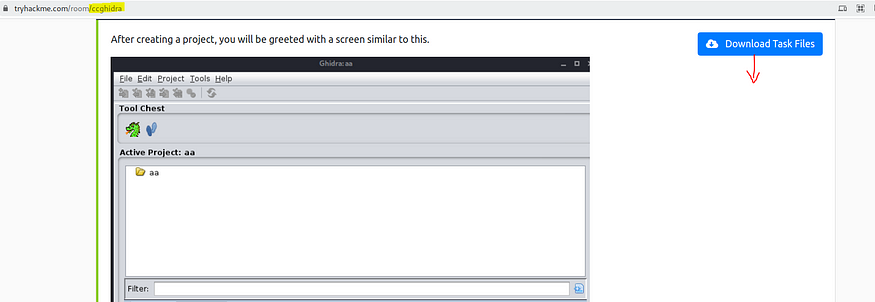




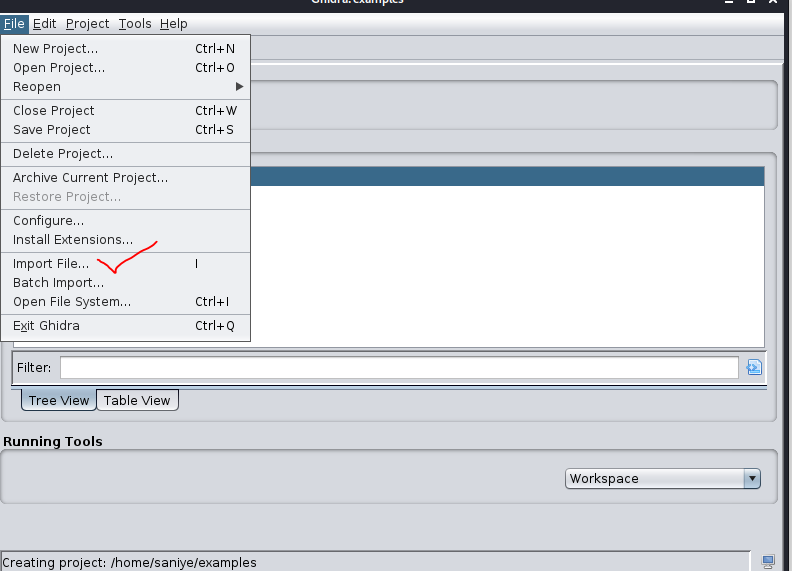


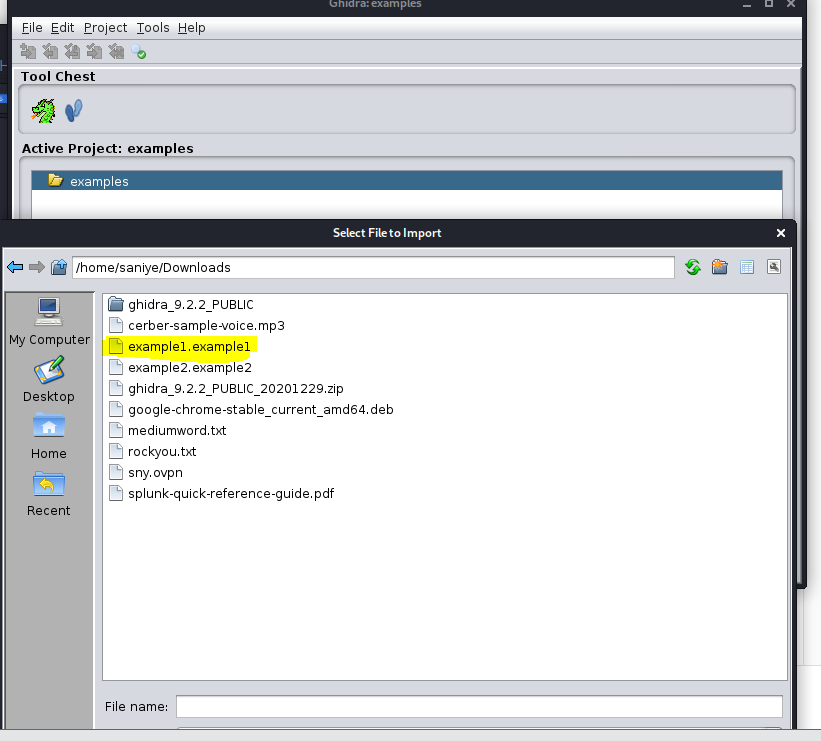


İndirdiğimiz örnekler üzerinden incelemeye başlayalım :

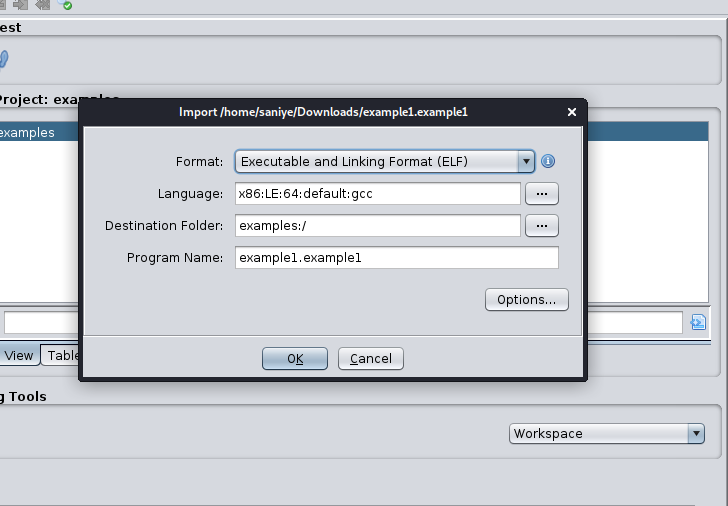


proje oluşturduktan sonra import file diyelim :



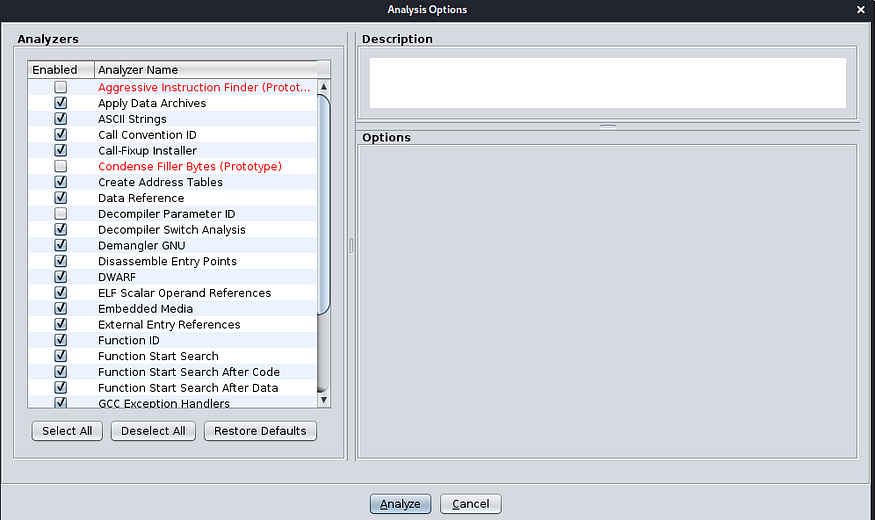


İndirdiğimiz ilk örneği seçelim.select file to import diyelim

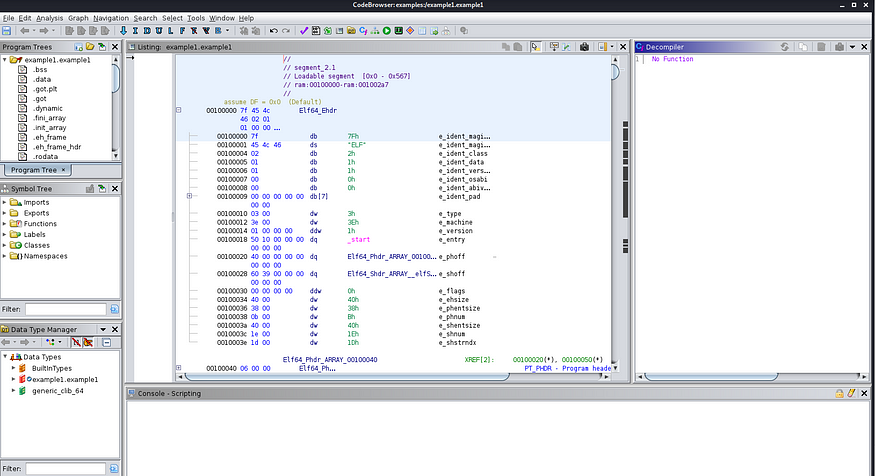




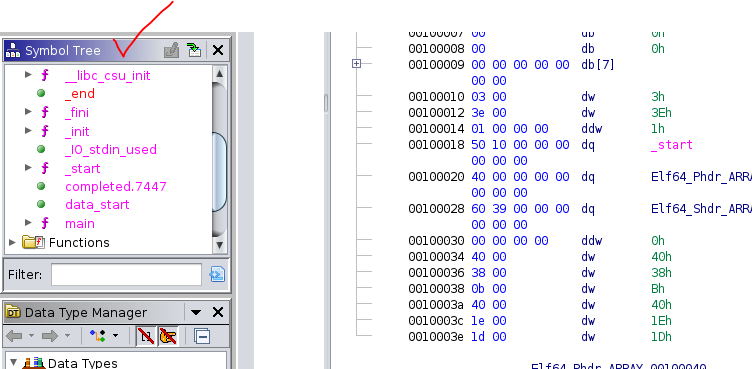
Analiz etmek istediğiniz ekstra seçenekleri buradan işaretleyebilirsiniz :



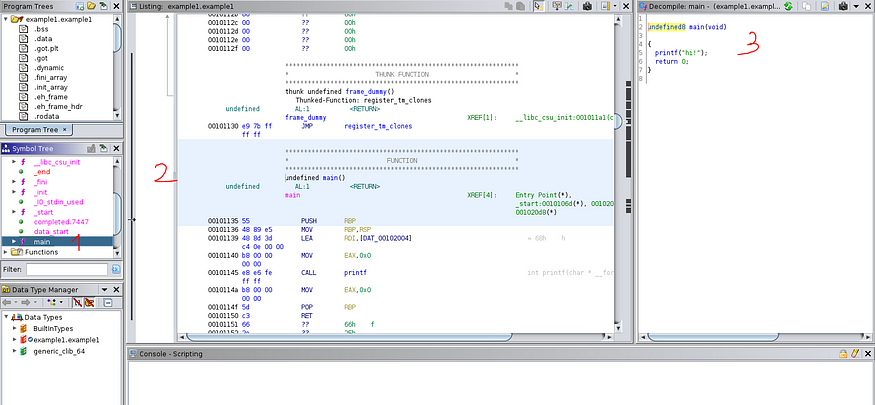
Şimdi analiz edeceğimiz example1 karşımızda :



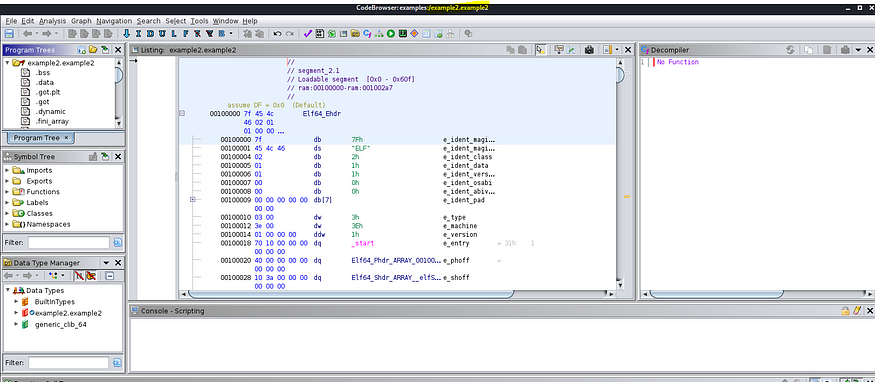
Burada ilk olarak bize pratiklik sağlayacak en önemli kısım symbol tree kısmıdır :



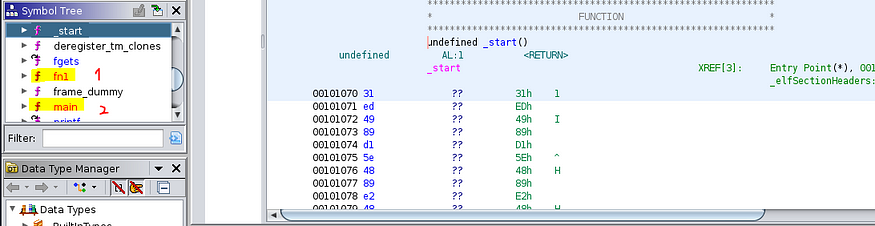
Örneğin ana blokta ne işlem yapılıyor asıl işlem ne bunu görmek için :

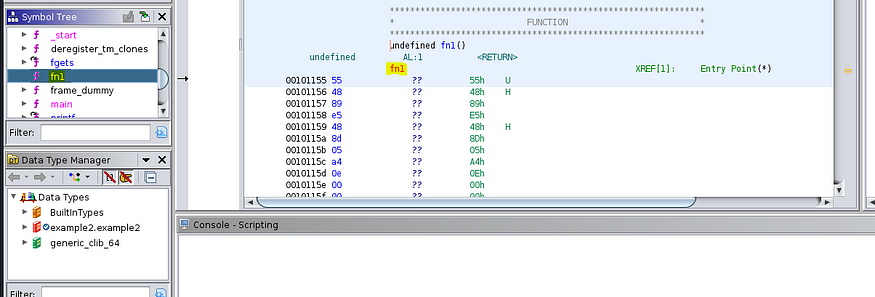


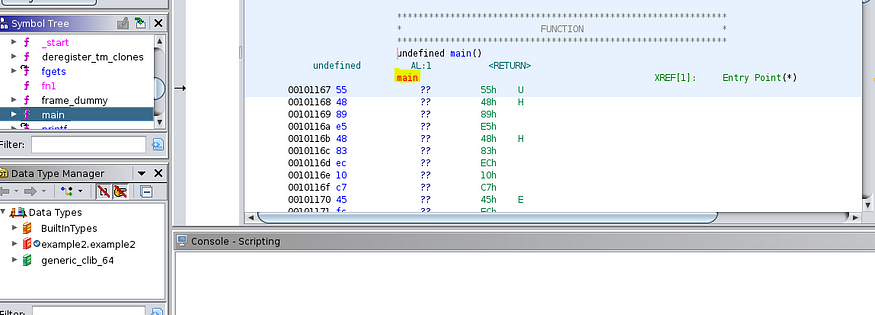
Basic gösterim açısından ilk örneği inceledik.Şimdi ikinci örneği açalım :



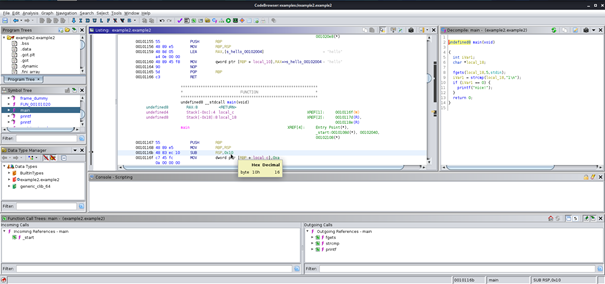
Bu örnekte kaç user ın main blogu oluşturdugunu bulalım : (symbol tree içinde functions a gidiyorum )





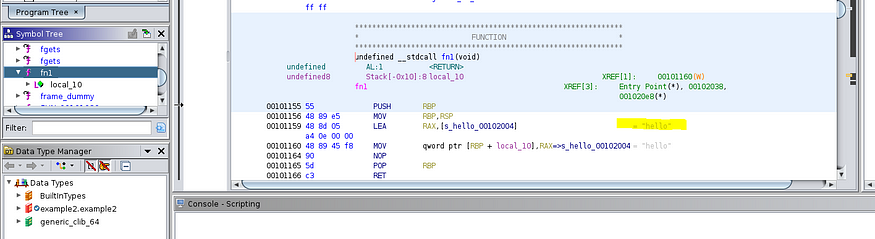


şimdi main fonksiyonunda ayarlanan ilk değişkeni bulalım :



Ayarlanan ilk değişken = 10

“Fn1” fonksiyonundaki ilk değişken neye ayarlanmıştır onu bulalım :

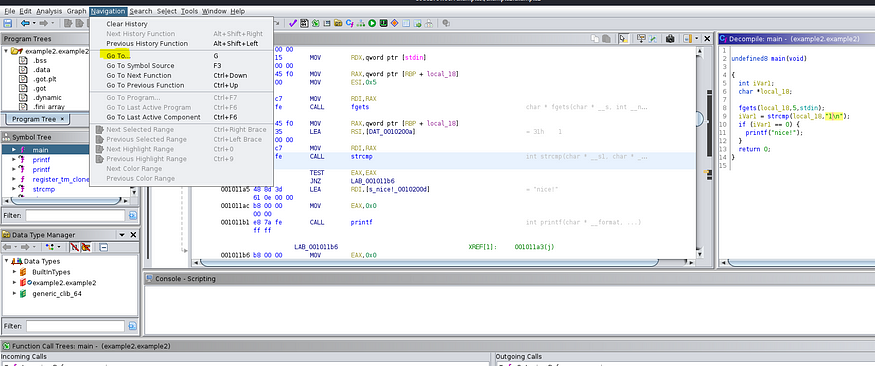


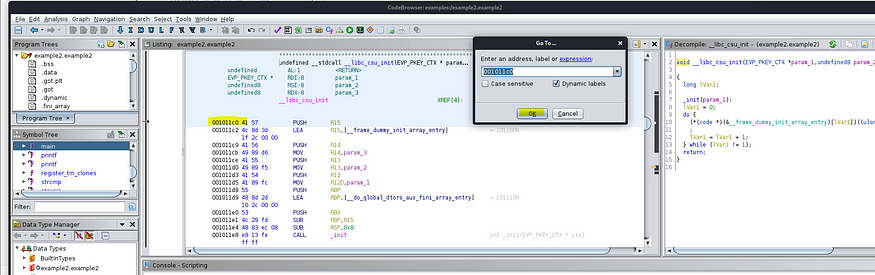
fn1 de “hello”

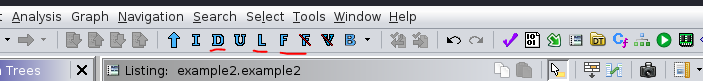
fonksiyonda girişi 1 olarak değiştirirsek :



search işlemi için aramak istediğin adresi gir :







L : Add Label , edit label işlemleri için kullanılır.

D :Disassemble

F:Float type belirleme

(ctrl ile kullanıldıgında işlev değişebilmektedir)