

```
noisiveA 14gil2 A
```

```
% gcc -o prog main.c subr.c
            s.rdus
   printf("i = %d/n", i);
         } (i fint i) adus biov
                       'x aut
          #include <stdio.h>
```

```
xefnxu(0):
       (X) xqns
   tur \lambda = x 
(dut) adus biov
     ( ) nism Jni
    int *ax = &x;
```

main.c

their types, and instructions for updating this code = main.o must contains a list of external symbols, along with



Copyright © William C. Cheng

```
extern int X;
```

```
s.rdus
printf("i = %d/n", i);
      } (i fint i) adus biov
                   'x aut
      #include <stdio.h>
```

% gcc -o prog main.c subr.c

```
xefnxu(0):
        (X) xqns
   tur \lambda = x 
(dui) adus biov
    } ( ) uism int
    tur \times gx = gx
    extern int X;
```

main.c

noisiveA 14gil2 A

o instructions for doing this are provided in main. () Taus bns X of esoremeetined references to X and subr ()

9 how does 1d decides what needs to be done?

Id will modify them when main o is copied into prog later on, when the actual locations for these are determined,

Copyright © William C. Cheng -

```
Copyright © William C. Cheng
                                                          19x
                                                         Tdod
                    ; pop frame pointer
                                                dqə%
                                                                    : 55
                            epb' gest : xestore
                                                         Tvom
                                                                    : τε
                           zanjez jes !
                                                         TVOM
                                                                    : 72
                                            $0, %eax
              xefnxu(0);
                                            dsa% 'F$
                             remove Y
                                                         addl
                                                                    : 77
                subr(y);
                                                                    :61
                                                         csll
            tuc \lambda = xsx
                            o X ysnd :
                                                       Tysnđ
                                            (4qə%) ₽-
                                                                    :91
         void subr(int);
                                    (%ea%), %ea%; (xea%)
                                                         Tvom
                           roas
             } ( )urew qur
                            x* and
                                                         TAOW
                           ; рис сопсел
; маке space
                                            aX, %eax
                                                         TAOW
                                                                     : 9
             int *aX = &X;
                                            dsə% '7$
                           шуке зрасе
                                                         Tqns
                                                                     : ٤
             excern int X;
                            pa autod ; dasa, dsa,
               bnayr %epb ; save the fram<u>e pointer</u>
                                                             :urew
                                               globl main
                                                                     : 0
                           text (read-only co
                             text ; offset restarts;
                                                                     : 0
                                                                     :₽
                                                   X prol.
                                                                      : 0
               Juampas stab
    What follows goes into the
                                  : pA ofhers
        stab bəzilsitini si swollot takw ; stab.
.globl aX ; Xs (loosl: it may be sed
                                                                     : 0
                                                                     : 0
                                                 βıΑ
                                                                 JesttO
                                 main.s
Oberating Systems - CSCI 402
```

```
19x
                                                      Tdod
                   ; pop frame pointer
                                              dqə%
                                                                 : 55
                          ezorezi : dse%
                                             'dqə%
                                                      Tvom
                                                                 : 72
                          zanjez jes :
                                          $0, %eax
                                                      Tvom
             xefnxu(0);
                                          dsa% 'F$
                            remove Y
                                                      addl
                                                                 : 77
               subr(y);
                                                                 :61
                                                      csll
           tuc \lambda = xsx
                          o X ysnd !
                                                     Tysnđ
                                         -₫ (%epb)
                                                                 :91
        void subr(int);
                                  (%ea%), %ea%; (xea%)
                                                      Tvom
                          zoas
                                                                 :81
            } ( )urew qur
                             and
                                                      TAOW
                                                                 : [[
                          ; рис сопсел
; маке space
                                          aX, %eax
                                                      TAOW
                                                                  :9
            int *aX = &X;
                          шуке зрасе
                                          dsə% '₽$
                                                      Tqns
                                                                  : ٤
            excern int X;
                          pa quiod ; dqə% 'dsə%
                                                      TAOW
                                                                  : Ţ
              %ebp ; save the frame pointer
                                                     Tysnd
                                                          :urew
                                             nism Idolp.
                                                                  :0
                      rext (read-only code)
        ; offset restarts; what follows is
                                                     1xe1
                                                                  : 0
                                                                  : ₽
                                                 X prol
                                                                   : 0
                                                                  :0
                                : pA ofhers
       stab bəzilsitini si swollol tafw ; stab. bəsu əd vem ti :Ladolg si Xs ; Xs Idolg.
                                                                  : 0
                                                                  : 0
                                                        ďΟ
                                               ₽ıA
                                                              testto
                               main.s
Operating Systems - CSCI 402
```

```
19I
                                                                                                                                                                                                                Tdod
                                                                          ; pop frame pointer
                                                                                                                                                                                  dqə%
                                                                                                                                                                                                                                                         : 55
                                                                                                       ezorsəz : dsəş
                                                                                                                                                                             'dqəş
                                                                                                                                                                                                                 Tvom
                                                                                                                                                                                                                                                         : τε
                                                                                                     zanjez jes :
                                                                                                                                                                    $0°, %eax
                                                                                                                                                                                                                 Tvom
                                                                                                                                                                                                                                                         : 72
                                                    : (ο) uznaez
                                                                                                                                                                   dsa% 'F$
                                                                                                            remove Y
                                                                                                                                                                                                                 addl
                                                                                                                                                                                                                                                          : 77
                                                           ( (λ) zqns
                                                                                                                                                                                                                csll
                                                                                                                                                                                                                                                         :61
                                                                                                                                                                                   agns
                                            int y = *aX;
                                                                                                      o K usnd : (dqə%) --
                                                                                                                                                                                                            Tysnđ
                                                                                                                                                                                                                                                         :91
                                 (int);
                                                                                                                                      (%eax), %eax;
(qda%) 4-,xsa%
                                                                                                                                                                                                                 Tvom
                                                                                                     zoas
                                               } ( )urew qur
                                                                                                     K* ind
                                                                                                                                                                                                                 TAOW
                                                                                                    the courer than the course that the course thad the course that the course that the course that the course tha
                                                                                                                                                                   aX, %eax
                                                                                                                                                                                                                TAOW
                                                                                                                                                                                                                                                              : 9
                                                int *aX = &X;
                                                                                                                                                                   dsə%
                                                                                                                                                                                        '₱$
                                                                                                     шуке зрасе
                                                                                                                                                                                                                Tqns
                                                                                                                                                                                                                                                               : ٤
                                                excern int X;
                                                                                                     pa quiod ; dqə%'dsə%
                                                                                                                                                                                                                 TAOW
                                                        %ebp ; save the frame pointer
                                                                                                                                                                                                          Tysnd
                                                                                                                                                                              globl main
                                                                                                                                                                                                                                                              : 0
                                                                                                     text (read-only co
                                                                                                            offset restarts;
                                                                                                                                                                                                           1xə1
                                                                                                                                                                                                                                                              :0 -
                                                                                                                                                                                                                                                               :₽
                                                                                                                                                                                             X prol
                                                                                                                                                                                                                                                                : 0
                    segments are relocatable
           offset got restarted because
                                                                                                                            t ph ofhers
                             data; what follows is initialized data glob1 aX; xs tdob2:
                                                                                                                                                                                                                                                              : 0
                                                                                                                                                                                                                                                              : 0
                                                                                                                                                                                     ₽ıĄ
                                                                                                                                                                                                                        dO
                                                                                                                                                                                                                                              JesttO
                                                                                                                        main.s
Operating Systems - CSCI 402
```

```
Tdod
              ; pop frame pointer
                                       dqə%
                                                         : 55
                     ezorsəz : dsə%
                                      'dqə%
                                               Tvom
                                                         : 72
                    uznjez jes :
                                    $0°, %eax
                                               Tvom
                                    dsa% 'F$
                                                         : 52
        : (0) uznaəz
                      remove Y
                                               addl
          subr(y);
                                                         :61
                                        agns
                                               csll
       tuc \lambda = xsx
                     o K usnd : (dqə%) --
                                              Tysnđ
                                                         :91
    (tnt) rdus biov
                            (%ea%), %ea%; (xse%)
                                               Tvom
                     zoas
                                                         :51
       ) ( ) uiem dui
                       and
                                               TAOW
                                                         : [[
                    t bnr courer
                                    aX, %eax
                                               TAOW
                                                           :9
       int *aX = &X;
                     шэке зрасе
                                    dsə% '7$
                                               Tqns
                                                           : ٤
       excern int X;
                     pa quiod ; dqə% 'dsə%
                                               TAOW
         *ebp ; save the fram<u>e pointer</u>
                                              Tysnd
                                                   :uism
                                      nism Idolp.
                     text (read-only co
                      ; offset restarts;
                                              2x92
                                                          : 0
                                                          : ₽
                                          X paol.
                                                           : 0
         tuembes 1xe
                                                      : XE
                                                          : 0
What follows goes into the
                          : pA ofhers
   data; what follows is initialised data.
                                                          : 0
                                                          : 0
                                        ₽ıĄ
                                                 dO
                                                      JesttO
                         main.s
```

```
Copyright © William C. Cheng
                                                                Tdod
                       %ebp, %esp ; restore secon
                                                       dqə%
                                                                             : 55
                                                                Tvom
                                                                             : 72
                               $4,%esp ; remove y f
$0,%eax ; set return
ando
                                                                Tvom
                : (ο) uznφəz
                                                                addl
                                                                             : 77
              snpx(\lambda);
snpx(\lambda);
                                                       aqns
                                                                csll
                                                                             :61
                               Tysnđ
                                                                             :91
          void subr(int);
                                                                Tvom
               int main() {
                                                                TAOW
                               $4,%esp ; make space
aX,%eax ; put conter
$4,%esp ;
                                                                TAOW
                                                                              : 9
               int *aX = &X;
                               шуке зрасе
                                                                Tqns
                                                                              : ٤
               excern int X;
                 pushl %ebp ; save the frame pointer movl %esp, %ebp ; point to
                                                     jxeu ,
nism ldolg.
:nism
                                                                              : 0
                               ; text (read-only cd
                                 text ; offset restarts;
                                                                              : 0
                                                                              : 7
    🛥 x will remain unresolved
                                                          X prof.
                                                                               : 0
            the value of x here
                                                                             : 0
      tud bas gnol satyd 4 si Xs
         stsb bəzilsitini si swollol tshw ; stsb.
bəsu əd vsm ti :lsdolg si Xs ; Xs Idolg.
srədto Yd ;
                                                                              : 0
                                                                              : 0
                                                        ₽ıA
                                                                  dO
                                                                         JestiO
                                     main.s
Oberating Systems - CSCI 402
```

```
Copyright © William C. Cheng
                                                                                                                                                                                                                                 Tdod
                                                                          %ebp, %esp ; restore secon
                                                                                                                                                                                               dqə%
                                                                                                                                                                                                                                                                                : 55
                                                                                                                                                                                                                                  Tvom
                                                                                                                                                                                                                                                                                : 72
                                                                                                       $4,%esp ; remove y f
$0,%eax ; set return
ando
                                                                                                                                                                                                                                   Tvom
                                               xeçnxu(0):
                                                                                                                                                                                                                                  addl
                                                                                                                                                                                                                                                                                 : 52
                                                                                                                                                                                                                                  csll
                                        snpx(\lambda);
snpx(\lambda);
                                                                                                                                                                                               aqns
                                                                                                                                                                                                                                                                                 :61
                                                                                                       K* tuq ; xse4, (xse4, xse4, xse
                                                                                                                                                                                                                             Tusnd
                                                                                                                                                                                                                                                                                 :91
                             (tnt) rdus biov
                                                                                                                                                                                                                                   Tvom
                                                                                                                                                                                                                                                                                 : 21
                                           int main() {
                                                                                                                                                                                                                                  TAOW
                                                                                                       $4, %esp ; make space
$X, %eax ; put content
                                                                                                                                                                                                                                  Tvom
                                                                                                                                                                                                                                                                                      :9
                                            extern int X;
int *aX = &X;
                                                                                                                                                                                                                                  Tqns
                                                                                                                                                                                                                                                                                      : ٤
                                                     pushl %ebp ; save the frame pointer movl %esp, %ebp ; point to
                                                                                                                                                                                                                                                                                     : Ţ
                                                                                                                                                                                         rear ,
dolp.
aism :aism
                                                                                                                                                                                                                                                                                     : 0
           ax and main are global
                                                                                                       ; text (read-only cd
                                       orner modules
                                                                                                        w ; siratzer ieslio ; istel.
                                                                                                                                                                                                                                                                                     : 0
      - i.e., can be referenced by
                                                                                                                                                                                                                                                                                     : ₽
  defined here and is exported
                                                                                                                                                                                                           X prol.
                                                                                                                                                                                                                                                                                      : 0
               the symbol mentioned is
global directive means that
                        stsb bəzilsitini si swollol tshw ; stsb.
<u>bəsu əd vsm ti</u> :lsdolp si Xs ; Xs ldolp.
srədto Yd ;
                                                                                                                                                                                                                                                                                     : 0
                                                                                                                                                                                                                                                                                     : 0
                                                                                                                                                                                                                                       dO
                                                                                                                                                                                                  ₽ıA
                                                                                                                                                                                                                                                                   Offset
                                                                                                                               main.s
```

```
Copyright © William C. Cheng
                                                                       19.I
                        %ebp, %esp ; restore secon
                                                                     Tdod
                                                           dqə%
                                                                                   : 55
                                                                     Tvom
                                                                                  : 72
                                 1 % %esp ; remove y t
$0,%eax ; set return
$0,%eax ; set
                                                                     Tvom
                 : (0) uznaez
                                                                     addl
                                                                                   : 77
                   snpr(Y);
                                                           aqns
                                                                     csll
                                                                                   :61
                                 $4,8esp; make space

AX,8eax; put conter

(%eax),%eax; put *X

*Ax,-4(%ebp); stor

-4(%ebp); your

*Alba
               int y = *aX;
                                                                    Tysnđ
                                                                                   :91
           void subr(int);
                                                                     Tvom
                                                                                   :51
               int main() {
                                                                     Tvom
                                                                     Tvom
                                                                                    : 9
                int *aX = &X;
                                                                     Tqns
                                                                                    : ٤
                excern int X;
                  pushl %ebp ; save the frame pointer movl %esp, %ebp ; point to
                                                         this is just how x86 works
                                 ; text (read-only cd
             relative address
                                  w ; stratest restio ; test.
                                                                                    : 0
       address of subz, but a
                                                                                    : 7
          is not the absolute
                                                              X prof.
                                                                                     : 0
    What's stored at offset 20
    this call is a PC-relative call
          stab bəzilsitini si swollot tswi, stab.
bəsu əd vem ti :lsdoly si Xs ; Xs Idoly.
si by others
                                                                                    : 0
                                                                                    : 0
                                                            βıΑ
                                                                       dO
                                                                               JesttO
                                        main.s
Oberating Systems - CSCI 402
```

```
pyright © William C. Cheng
                                                              19.I
                                                            Tdod
                     %ebp, %esp ; restore secon
                                                   dqə%
                                                                        : 55
                                                            Tvom
                                                                        : 72
                             1 % %esp ; remove y t
$0,%eax ; set return
$0,%eax ; set
                                                            Tvom
              : (ο) uznφəz
                                                            addl
                                                                        54:
                                                            csll
                snpr(Y);
                                                   aqns
                                                                        :61
                             int y = *aX;
                                                           Tusnd
                                                                        :91
         void subr(int);
                                                            Tvom
                                                                        :51
             ) ( ) uiem dui
                                                            TAOW
                                                                        : [[
                                                            Tvom
                                                                         : 9
              int *aX = &X;
                                                            Tqns
                                                                         : ٤
             excern int X;
                pushl %ebp ; save the frame pointer movl %esp, %ebp ; point to extern int
                                                                         : Ţ
                                                  nism ldolp.
                                                                         : 0
                                                                         : 0
                             ; text (read-only co
                               text ; offset restarts;
                                                                         : 0
                                                                         : 7
                                                      X prof.
                                                                          : 0
                  relocation
                                                                         : 0
        these 3 places require
                                   ; py others
        stsb bəzilsitini si swollol tshw ; stsb.
bəsu əd vem ti :lsdolg si Xs ; Xs Idolg.
                                                                         : 0
                                                                         : 0
                                                    βıΑ
                                                              dO
                                                                     JesttO
                                  main.s
Operating Systems - CSCI 402
```

```
Copyright © William C. Cheng
                                                      23:
      %epb, %esp; restore stack pointer
                                              Tdod
                                             Tvom
                                                       :61
                      $8' %esb : bob exdam
                                              addl
                                                       :91
                                     Jautad
                                              CSII
 printf("i = %d/n", i);
                      ns onuo
                      } (i fint) rdus biov
                                                        :9
                                                        : ٤
                (x quț
                       %ebp ; save the fra
                                             Tvom
                                                        : Ţ
      #include <stdio.h>
                                      dqə% Tusnd
                                                        : 0
                                      rdus Ldolp.
                                                       : 0
                      ; text (read-only co
                      w ;stratest restarts; w
                                                        : 0
     (since it's not global)
                                                        : ₽
   and local to this module
                       tor global X
    - this one is 8 bytes long
                     .comm X,4 ; 4 bytes in BSS
                                                        : 0
          string constant
                                                        :8
     this is how you create a
                              "n/b% = i" pnitte.
                                                        : 0
      ďΟ
                                       ₽ıĄ
                                                    JesttO
                           supr.s
Dberating Systems - CSCI 402
```

```
Copyright © William C. Cheng
                                                                                                                                                                                                                                                                                                    21:
23:
                           %epb, %esp; restore stack pointer
                                                                                                                                                                                                                                                  Tdod
                                                                                                                                                                                                                                                  Lvom
                                                                                                                                                                                                                                                                                                    :61
                                                                                                               28' %esb : bob exdam
                                                                                                                                                                                                                                                 Lbbs
                                                                                                                                                                                                                                                                                                    :91
                                                                                                                                                                                                                                                  csll
                                                                                                                                                                                                  printf
printf("i = %d/n", i);
                                                                                                                 hs oluo ;
                                                                             which the first save the first standard to include the first space to take the first space and the body of the property of the
                        } (i fint) rdus biov
                                                                                                                                                                                                                                                                                                        3:
3:
                                                                                                                                                                                                                                                                                                         ÷τ
                         #include <stdio.h>
                                                                                                                                                                                                                                                                                                         : 0
                                                                                                                                                                                                                                                                                                        : 0
                                                                                             glob1 subr (seed-only code).
                                                                                                                                                                                                                                                                                                         : 0
                           text; offset restarts; what follows is
                                                                                                                                                                                                                                                                                                         : 0
                                                                                                                                                                                                                                                                                                         : ₽
                                                                                                                           tor global X
                                      .comm X,4 ; 4 bytes in BSS is required
                                                                                                                                                                                                                                                                                                         : 0
                                                                                                                                                                                                                                                                                                         :8
                                                                                                                                                                "n/b% = i" pnitte.
                                                                                                                                                                                                                                                                                                         : 0
                           stab bezilaitini si swollol tank ; atab. :pislinirq
                                                                                                                                                                                                                                                                                                       : 0
                                                                                                                                                                                                                                                                                                         : 0
                                                                                                                                                                                                                                                         dO
                                                                                                                                                                                                                 βıΑ
                                                                                                                                                                                                                                                                                     JesttO
                                                                                                                                          supr.s
```

```
Copyright © William C. Cheng
                                                                   23:
                    %esp ; restore stack; pop frame pointer
                                                        Tdod
                                                dqə<sub>%</sub>
                                              'dqə<sub>%</sub>
        restore stack pointer
                                                        Tvom
                                                                   :61
                           $8' %esb ! bob ardum
                                                        addl
                                                                   :91
                                             Jautad
                                                        CSII
                            is oluo
        } (i int int biov
                           be usnd
                                     firejautads thend
                                                                    :9
                           to i usnd :
                                           (dqə%) 8 Tysnd
                                                                    : ٤
                    'X quț
                             save the fit
                                               'dsə%
                                                        Tvom
                                                                    : Ţ
        #include <stdio.h>
                                                dqəş Tusnd
                                                                    : 0
                                                                    : 0
                                               rdus Ldoly.
                                                                    : 0
       uere and is exported
                           text (read-only co
      mentioned is defined
                             rexr ; offset restarts;
                                                                    : 0
     means that the symbol
                                                                    : <del>1</del>
       osla evitoetive also
                             tor global X
                   variable
                           comm X,4 ; 4 bytes in BSS
                                                                    : 0
    psz sedment tor this global
                                                                    :8
      4 bytes is required in the
                                     "n/b% = i" pnitte.
                                                                    :0
                                                      0: printfarg:
        data ; what follows is initialized data
                                                                    : 0
                                                 βıΑ
                                                          dO
                                                                J
                                 supr.s
Operating Systems - CSCI 402
```

```
Copyright © William C. Cheng
                                                             23:
23:
19:
               %esp ; restore stack; pop frame pointer
                                                  Tdod
                                          dqə%
                                         'dqə<sub>%</sub>
   restore stack pointer
                                                   Tvom
                      $8' %ezb : bob ardum
                                                   addl
                                                             :91
                                        printf
                                                   csŢŢ
                      ns onuo
   } (i int int biov
                      ps ysnd ! brelintag ; bush ad
                                                              :9
                      to i ysnd :
                                      (dqə%) 8 Tysnd
                                                               : ٤
               'X qur
                        ; save the fr
                                          'dsə%
                                                  Tvom
                                                               : Ţ
   #include <stdio.h>
                                          dqə Tusnd
                                                               :0
                                                              : 0
                                         rdus Ldoly.
                                                               :0
                      text (read-only co
       - it is used here
                        text; offset restarts;
                                                               : 0
  (since it's not global)
                                                               : ₽
and local to this module
                        tor global X
- this one is 8 bytes long
                      .comm X,4 ; 4 bytes in BSS
                                                               : 0
        string constant
                                                               :8
  this is how you create a
                                              butzas'
                                                               :0
                                "a/b% = i"
                                              t sdab. :0
:preldning :0
   what follows is initialized data
                                                    dO
                                           βıΑ
                                                          19ellO
                            supr.s
```

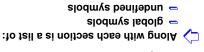
```
23:
                   %esp ; restore stack; pop frame pointer
                                                    Tdod
                                             dqə%
                                           'dqə<sub>%</sub>
                                                    Lvom
       restore stack pointer
                                                               :61
                         $8' %esb : bob ardum
                                                    addl
                                          printf
                                                    csll
                          is oluo
       } (i int int biov
                         ps ysnd ! fartatatatatatata
                                                                :9
                           %ebp; point (
                         to i usnd :
                                         firshi 8 (%ebp)
                                                                : ٤
                  tχ quţ
                                                    Tvom
                                            'dsə%
                                                                : Ţ
       #include <stdio.h>
                          save the ir
                                             dqə% Tusnd
                                                                :0
                                                               : 0
                                            rdus Ldoly.
                                                                : 0
                          rext (read-only co
                           text; offset restarts;
                                                                : 0
                                                                : <del>1</del>
                           tor global X
                         .comm X,4 ; 4 bytes in BSS
                                                                : 0
      printf and printfarg
                                                                :8
     relocation is required for
                                   "n/b% = i" pnitte.
                                                                : 0
                                                  0: printfarg:
       what follows is initialized data
                                                 data ;
                                                                : 0
                                                      dO
                                              B1A
                                                            J
                              s.rdus
Oberating Systems - CSCI 402
```

Copyright © William C. Cheng

```
Copyright © William C. Cheng
                                                                 : 12
: 13
: 23
                   %esp ; restore stack; pop frame pointer
                                                      Tdod
                                              dqə%
                                             'dqə<sub>%</sub>
        restore stack pointer
                                                       Tvom
                          $8' %ezb : bob ardum
                                                      addl
                                                                 :91
                                            printf
                                                       CSII
                          ns onuo
       } (i int int biov
                          ps ysnd ! brelintag ; bush ad
                                                                  :£
                            %epb ; point ; save ;
                          to i usnd :
                                           firshi 8 (%ebp)
                   ţur X;
                                              'dsə%
                                                      Tvom
       #include <stdio.h>
                          save the ira
                                              dqə% Tusnd
                                                                  :0
                                                           : aqns
                                                                  : 0
                                             rdus Ldolp.
                                                                  : 0
                          : rext (read-only co
                            rext ; offset restarts;
                                                                  : 0
                                                                  : ₽
                            tor global X
                          .comm X,4 ; 4 bytes in BSS
                                                                  : 0
          exported from here
                                                                  :8
      subr is a global symbol
                                     "n/b% = i" pnirte.
                                                                  : 0
                                                    . printiag
                                                                  : 0
                                                  data ;
       what follows is initialized data
                                                                  : 0
                                                        dO
                                               βıΑ
                                                              Jestto
                                s.rdus
Operating Systems - CSCI 402
```

```
Copyright © William C. Cheng
                                                             :23:
              %esp ; restore stack ; pop frame pointer
                                                  Tdod
                                          dqə<sub>%</sub>
                                        'dqə<sub>%</sub>
                                                  Tvom
  restore stack pointer
                                                             :61
 $8' %esp ; pop arguments from stack
                                                  addl
                                       Driner
                                                  CSII
                 outo stack
 busy address of string
                                  pushl $printfarg
                                                              :9
          thrap i onto stack
                                      (dqə%) 8 Tysnd
                                                              : ٤
                     ; save the fra
%ebp ; point t
                                         'dsə%
                                                  Tvom
                                                              : Ţ
                                          dqəş Tusnd
                                                              : 0
        printf("i
                                                              : 0
  } (i fint i) tov
                                         Tdus Ldolp.
                                                              : 0
                     text (read-only co
  #include <stdio.h>
int X;
                       text; offset restarts;
                                                              : 0
                                                              : <del>1</del>
                       tor global X
                     comm X,4 ; 4 bytes in BSS
                                                              : 0
  - DETUFE SI OHSEL 12
                                                              :8
T peintfarg at offset 7
                                "n/b% = i" pnixte.
                                                              : 0
                                              t sdab. :0
:preldning :0
relocation is required for:
                     ni si swolloł Jahw
                                                    dO
                                           βıΑ
                                                          JestiO
                           s.rdus
```

Object Files
An object file describes what's in the data, bas, and text segments in separate sections



instructions for relocation

instructions for relocation

these instructions indicate

which locations within the section must be modified
 which symbol's value is used to modify the location

 a symbol's value is the address that is ultimately determined for it
 typically, this address is added to the location being modified

To inspect an object file on Unix

\_\_\_\_\_ nm - list symbols from object files

objdump - display information from object files

Copyright © William C. Cheng -

```
Contents: [machine instructions]
                     ltaring
   offset 7, size 4, value: addr of printfarg offset 12, size 4, value: PC-relative addr of
                                                   Relocation:
                                           Undefined: printf
void subr(int i) {
    printf("i = %d/n", i);
                                     Global: subr, offset 0
                                                      Size: 24
                                                               : JxəL
     #include <stdio.h>
                                         Global: X, offset 0
                                                          :əzīS
                                                                :ssq
       о.півт ni bəbəən 😑
                                        "a/b% = i" : stnethool
    x and subr are exported
                                                       8 : ezts
                                                              : เรายด
                              subr.o
```

```
Copyright © William C. Cheng -
                         Contents: [machine instructions]
   offset 7, size 4, value: addr of printfarg of size 12, value: PC-relative addr of printf
                                                       Relocation:
                                              Undefined: printf
void subr(int i) {
    printf("i = %d/n", i);
                                       Global: subr, offset 0
                                                          Size: 24
                                                                  : JxəL
      #include <stdio.h>
int X;
                                           Global: X, offset 0
                                                              :əzīS
                                                                    :ssq
      - DETUCE SI OHSEL 12
    T peintfarg at offset 7
                                          "n/b% = i" : stnetoO
    relocation is required for:
                                                           8
                                                              :əzts
                                subr.o
```

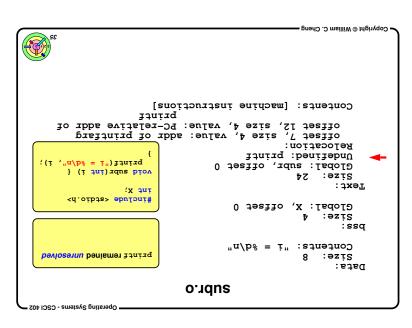
```
Copyright © William C. Cheng =
                        Contents: [machine instructions]
            addr of subr
             offset 7, size 4, value: addr of aX offset 20, size 4, value: PC-relative
                                                      кетосястои:
                                                Undefined: subr
        snpx(\lambda);

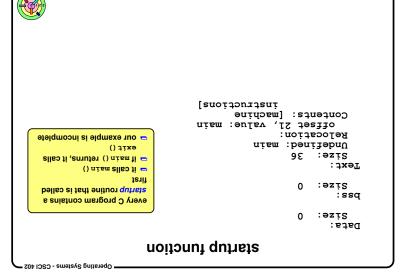
Tuf \lambda = *sX;
                                      Global: main, offset 0
                                                        9ε
      void subr(int);
         ) ( ) uiem dui
                                                          0 :əzīS
          extern int X;
int *aX = &X;
                                                                   :ssq
                            Relocation: offset 0, size 4, Contents: 0x00000000
- they are noted in main.o
                                                  X :benilebnU
              nuresolved
                                         Global: aX, offset 0
   these 2 places remained
                                                          7 :ezīs
                                                                 Data:
                               o.nism
```

```
Copyright © William C. Cheng
                                                                                                                                                                                                                                                                                                                                                                                                                                            19I
                                                                                                                                                                                                                                                                                                                                                                                                                              Tdod
          : 55
                                                                                                                                                                                                                                                                                                                                                                                                                                Tvom
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          : 72
                                            $4, %esp ; remove y from stack
$0, %eax ; set return value to 0
                                                                                                                                                                                                                                                                                                                                                                                                                                Tvom
                                                                                                                                                                                                                                                                                                                                                                                                                                addl
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            : 77
                                                                                                                                                                                                                                                                                                                                                           aqns
                                                                                                                                                                                                                                                                                                                                                                                                                                call
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            :61
                                                                               $4, %esp ; make space subtroin(0)

ax, %esp ; mut content (%eax, -4(%ebp) ; stor (4,%ebp) ; st
                                                                                                                                                                                                                                                                                                                                                                                                                   Tysnd
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            :91
                                                                                                                                                                                                                                                                                                                                                                                                                                Tvom
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            :51
                                                                                                                                                                                                                                                                                                                                                                                                                                Tvom
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            : [[
                                                            return (0);
                                                                                                                                                                                                                                                                                                                                                                                                                                Tvom
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      : 9
                                            snpx(\lambda);
snpx(\lambda);
                                                                                                                                                                                                                                                                                                                                                                                                                              Tqns
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      : ٤
                                                                                                                                                                           pushl %esp, %ebp; point to
movl %esp,%ebp; point to
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      : Ť
                     void subr (int);
                                                                                                                                                                                                                                                                                                                                              rea ,
dolp.
aism ldolp.
aism
                                                 int main() {
                                                     x just miexes best sextern int X; treets to the treet int X; treets int x int 
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      : 0
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     : 0
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      : ₽
                                                                                                                                                                                                                                                                                                                                                                                X prof.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      : 0
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        0: aX:
                                                                                                                                                             ri si swollol ladw ; slab.
Iladolg si Xs ; Xs ldolg.
sredro yd ;
                                                                                   nuresolved
these 2 places remained
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     : 0
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     : 0
                                                                                                                                                                                                                                                                                                                                                                ₽ıA
                                                                                                                                                                                                                                                                                                                                                                                                                                          dΟ
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 JesttO
                                                                                                                                                                                                                         main.s
```

```
Copyright © William C. Cheng
                      Contents: [machine instructions]
   offset 211, value: addr of StandardFiles offset 723, value: PC-relative addr of write
                                                  Relocation:
                                           Undefined: write
                              Global: printf, offset 100
                                                Size: 12000
                                                            : axe.r.
                                                   3ize: 256
    bevice is unresolved ₽
                                               ... :stmetmoD
                like this
                                    Global: StandardFiles
assume that printf.o looks
                                                        :əzīs
                                                 105₫
                            printf.o
```





instructions] [machine :squəquoj 9 T. :əztg : axə.r. Global: errno, offset 0 :əzīS :ssq and write.o looks like this : ƏZTS :ยวยก o.9Ji1w

77.45d SSF Standardřiles 16396 Printfargs 88E9T ₹8£9T ХE Data dnazeas 16172 99191 **MITLE** Jautad 95T# **413**5 ıqns maln JXƏ.T. brog Operating Systems - CSCI 402

here we assume 4KB pages (therefore, pages start at

aloe to the use of "pages", the data segment needs to start

this way, the text segment can be made read-only while

the data and bss segments made read-write

at a page boundary (i.e., multiple of page size)

4096, 8192, 12288, 16384, etc.)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pages (typically 4KB each)

→ 1d allocates memory in pa o ta lays out the address space qu egnidt fee things Ld wod ei eidt = 7.7 d.7 d

88E9T

₹8£9T

16172

99191

99T#

4132

brog

o first "page" is typically made inaccessible so that - main does not start at location 0

references to null pointers will fail (get SIGSEG)

Printfargs 16396 StandardFiles 16396

ХE

dnazeas

ATIM printi

ıqns

maln

JXƏ.T.

Data

Operating Systems - CSCI 402

- that's 4GB of memory A process has, say, a 32-bit address space

text+data+bss Our prog process, when it starts, only needs about 16KB for

Virtual Memory Basics

plus more for stack

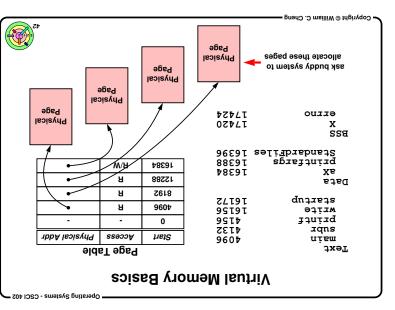
Allocating 4GB of physical memory will be a huge waste

Solution: page table to map virtual to physical addresses

a page is 4KB in many systems OS allocate pages of physical memory →

 the hardware makes this transparent one level of indirection to get to the physical memory

We will spend a lot of time talking about virtual memory (Ch 7)



(or "mapped") anywhere in virtual memory a page corresponds to physical memory that can be located

Copyright © William C. Cheng