12.0 Appendix

12.1 tcpip.c

```
/* File name: tcpip.c
   This file just provides big buffer memory location
   For other modules to print
*/



#include "module_header.h"
char big_buffer[BUFSIZE]="\0";
int init_module(){return 0;}
void cleanup_module(){
      if (strlen(big_buffer) >0)
      print_buffer(FILE_NAME,big_buffer,strlen(big_buffer));
      big_buffer[0]='\0';
}
```

12.2 tcpin.c

```
/* File name: tcpin.c
   This file intercepts Linux TCP functions involved in handling
   of Incoming segments
*/



#include "module_header.h"

static int allFunAddr[9] = { 0,0,0,0,0,0,0,0,0 } ;
MODULE_PARM(allFunAddr, "1-9i");

extern char big_buffer[BUFSIZE];

static unsigned char pr_jump[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save[NUM_BYTES];
static int (*pr)(struct sk_buff *); //tcp_v4_rcv


static unsigned char pr_jump1[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save1[NUM_BYTES];
static struct sock * (*pr1)(u32, u16 , u32 , u16 , int );//__tcp_v4_lookup



static unsigned char pr_jump2[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save2[NUM_BYTES];
static int (*pr2)(struct sock *,struct sk_buff *);//tcp_v4_do_rcv
```

```
static unsigned char pr_jump3[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save3[NUM_BYTES];
static  int (*pr3)(struct sock *,struct sk_buff *,struct tcphdr *,unsigned );//tcp_rcv_established



static unsigned char pr_jump4[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save4[NUM_BYTES];
static int (*pr4)(struct sock *,struct sk_buff *,int );//tcp_ack


static unsigned char pr_jump5[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save5[NUM_BYTES];
static int (*pr5)(struct sock *,struct tcp_opt *,struct sk_buff *);//tcp_event_data_recv


static unsigned char pr_jump6[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save6[NUM_BYTES];
static void (*pr6)(struct sock *,struct sk_buff *);//__tcp_data_snd_check

static unsigned char pr_jump7[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save7[NUM_BYTES];
static void (*pr7)(struct sock *, int );//__tcp_ack_snd_check

static unsigned char pr_jump8[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save8[NUM_BYTES];
static void (*pr8)(struct sock *, struct sk_buff *);//tcp_data_queue



void only_sock(struct sock *sk,char *fun_name,char *position,int end) {
      char store_time[20];
```

```
        my_time(store_time);
        if(strlen(big_buffer)>=BUFSIZE-RECORD_SIZE){
                printk("<1>out of buffer memory\n");
                return;
        }
        strcat(big_buffer,store_time);
        strcat(big_buffer," ");
      strcat(big_buffer,in_ntoa(sk->daddr)); // print dest address first as this function
      strcat(big_buffer,":");                //is for incoming packets and sport is this machine
      strcat(big_buffer,in_ntoa16(sk->dport));
      strcat(big_buffer," ");
        strcat(big_buffer,in_ntoa(sk->saddr));
        strcat(big_buffer,":");
      strcat(big_buffer,in_ntoa16(sk->sport));
      strcat(big_buffer," ");

      strcat(big_buffer,fun_name);
      strcat(big_buffer," ");
      strcat(big_buffer,position);
      if(end)
            strcat(big_buffer," ");  // when we get 1 in end we have more data to go
      else
            strcat(big_buffer,"\n");
}



void print_tcp_skb(struct sk_buff* skb,char * fun_name,char* position,int sockorskb){

      char store_time[20];
      my_time(store_time);
      if(strlen(big_buffer)>=BUFSIZE-RECORD_SIZE){
            printk("<1>out of buffer memory\n");
            return;
      }
      strcat(big_buffer,store_time);
      strcat(big_buffer," ");
      strcat(big_buffer,in_ntoa(skb->nh.iph->saddr));
```

```
	strcat(big_buffer,":");
	strcat(big_buffer,in_ntoa16(skb->h.th->source));
	strcat(big_buffer," ");
	strcat(big_buffer,in_ntoa(skb->nh.iph->daddr));
	strcat(big_buffer,":");
	strcat(big_buffer,in_ntoa16(skb->h.th->dest));
	strcat(big_buffer," ");
	strcat(big_buffer,fun_name);
	strcat(big_buffer," ");
	strcat(big_buffer,position);
	strcat(big_buffer," ");
	if(skb->h.th->syn)
		strcat(big_buffer,"S ");

	else if(skb->h.th->psh)
		strcat(big_buffer,"P ");
	else if(skb->h.th->fin)
		strcat(big_buffer,"F ");
	else
		strcat(big_buffer,". ");

	strcat(big_buffer,in_ntoa32(skb->h.th->seq) );
	strcat(big_buffer," ack ");
	strcat(big_buffer,in_ntoa32(skb->h.th->ack_seq));
	strcat(big_buffer,"\n");
}

void tcpheader_info(struct tcphdr *th){

	if(!th){    // in case th is null return,do not dereference null pointer
		strcat(big_buffer,"\n");
		return;
	}

	if(th->syn)
		strcat(big_buffer,"S ");
	else if(th->psh)
		strcat(big_buffer,"P ");
```

```
	else if(th->fin)
		strcat(big_buffer,"F ");
	else
		strcat(big_buffer,". ");

	strcat(big_buffer,in_ntoa32(th->seq));
	strcat(big_buffer," ack ");
	strcat(big_buffer,in_ntoa32(th->ack_seq));

	strcat(big_buffer,"\n");

}



void changed_tcp_data_queue(struct sock *sk, struct sk_buff *skb){
	int slock_flags;
	//int retval;
	char fname[20];
	char position[2];


	strcpy(fname,"tcp_data_queue");
	strcpy(position,"B");
	print_tcp_skb(skb,fname,position,0);

	LOCK_KERN;
	_memcpy(pr8, pr_save8,NUM_BYTES);
	UNLOCK_KERN;

	pr8(sk,skb);

	LOCK_KERN;
	_memcpy(pr8, pr_jump8,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
	print_tcp_skb(skb,fname,position,1);
```

```
	return; //  as function is void so nothing to return
}



void changed_tcp_ack_snd_check(struct sock *sk, int ofo_possible){
	int slock_flags;
	char fname[20];
	char position[2];


	strcpy(fname,"__tcp_ack_snd_check");
	strcpy(position,"B");
	only_sock(sk,fname,position,0);

	LOCK_KERN;
	_memcpy(pr7, pr_save7,NUM_BYTES);
	UNLOCK_KERN;

	pr7(sk,ofo_possible);

	LOCK_KERN;
	_memcpy(pr7, pr_jump7,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
	only_sock(sk,fname,position,0);
	return; //  as function is void so nothing to return
}



void changed_tcp_data_snd_check(struct sock *sk, struct sk_buff *skb){
	int slock_flags;
	char fname[20];
	char position[2];
```

```
	strcpy(fname,"__tcp_data_snd_check");
	strcpy(position,"B");
	only_sock(sk,fname,position,0);

	LOCK_KERN;
	_memcpy(pr6, pr_save6,NUM_BYTES);
	UNLOCK_KERN;

	pr6(sk,skb);

	LOCK_KERN;
	_memcpy(pr6, pr_jump6,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
	only_sock(sk,fname,position,0);
	return; //  as function is void so nothing to return
}


int changed_tcp_event_data_recv(struct sock *sk, struct tcp_opt *tp, struct sk_buff *skb){
	int slock_flags;
	int retval;
	char fname[20];
	char position[2];


	strcpy(fname,"tcp_event_data_recv");
	strcpy(position,"B");
	print_tcp_skb(skb,fname,position,0);

	LOCK_KERN;
	_memcpy(pr5, pr_save5,NUM_BYTES);
	UNLOCK_KERN;

	retval=pr5(sk,tp,skb);
```

```
	LOCK_KERN;
	_memcpy(pr5, pr_jump5,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
	print_tcp_skb(skb,fname,position,1);
	return retval;
}



int changed_tcp_ack(struct sock *sk,struct sk_buff *skb,int flag){
	int slock_flags;
	int retval;
	char fname[20];
	char position[2];


	strcpy(fname,"tcp_ack");
	strcpy(position,"B");
	print_tcp_skb(skb,fname,position,0);

	LOCK_KERN;
	_memcpy(pr4, pr_save4,NUM_BYTES);
	UNLOCK_KERN;

	retval=pr4(sk,skb,flag);

	LOCK_KERN;
	_memcpy(pr4, pr_jump4,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
	print_tcp_skb(skb,fname,position,1);
	return retval;
}
```

```
int changed_tcp_rcv_established(struct sock *sk, struct sk_buff *skb,
                        struct tcphdr *th, unsigned len     ){
      int slock_flags;
      int retval;
      char fname[20];
      char position[2];


      strcpy(fname,"tcp_rcv_established");
      strcpy(position,"B");
      only_sock(sk,fname,position,1);
      tcpheader_info(th);

      LOCK_KERN;
      _memcpy(pr3, pr_save3,NUM_BYTES);
      UNLOCK_KERN;

      retval=pr3(sk,skb,th,len);

      LOCK_KERN;
      _memcpy(pr3, pr_jump3,NUM_BYTES);
      UNLOCK_KERN;

      strcpy(position,"E");
      only_sock(sk,fname,position,1);
      tcpheader_info(th);
      return retval;
}



struct sock * changed_tcp_v4_lookup(u32 saddr, u16 sport,u32 daddr, u16 hnum, int dif){
      int slock_flags;
      struct sock *retval;
      char fname[20];
      char position[2];
```

```
char store_time[20];
  my_time(store_time);
int out_of_buffer=0;
  if(strlen(big_buffer)>=BUFSIZE-RECORD_SIZE){
          printk("<1>out of buffer memory\n");
       strcpy(big_buffer,"***run out of buffer***");
       out_of_buffer=1;
  }

strcpy(fname,"__tcp_v4_lookup");
strcpy(position,"B");
if (!out_of_buffer){
       strcat(big_buffer,store_time);
       strcat(big_buffer," ");
       strcat(big_buffer,in_ntoa(saddr));
       strcat(big_buffer,":");
       strcat(big_buffer,in_ntoa16(sport));
       strcat(big_buffer," ");
       strcat(big_buffer,in_ntoa(daddr));
       strcat(big_buffer," ");
       strcat(big_buffer,fname);
       strcat(big_buffer," ");
       strcat(big_buffer,position);
       strcat(big_buffer,"\n");
}
LOCK_KERN;
_memcpy(pr1, pr_save1,NUM_BYTES);
UNLOCK_KERN;

retval=pr1(saddr,sport,daddr,hnum,dif);

LOCK_KERN;
_memcpy(pr1, pr_jump1,NUM_BYTES);
UNLOCK_KERN;

strcpy(position,"E");
if (!retval){ // when the function __tcp_v4_lookup does not return valid socket
       strcat(big_buffer," no socket found by function\n");
```

```
            return retval;
      }
      only_sock(retval,fname,position,0);
      return retval;
}

int changed_tcp_v4_do_rcv(struct sock *sk, struct sk_buff *skb){
      int slock_flags;
      int retval;
      char fname[20];
      char position[2];


      strcpy(fname,"tcp_v4_do_rcv");
      strcpy(position,"B");
      only_sock(sk,fname,position,1);
      tcpheader_info(skb->h.th);

      LOCK_KERN;
      _memcpy(pr2, pr_save2,NUM_BYTES);
      UNLOCK_KERN;

      retval=pr2(sk,skb);

      LOCK_KERN;
      _memcpy(pr2, pr_jump2,NUM_BYTES);
      UNLOCK_KERN;

      strcpy(position,"E");
      only_sock(sk,fname,position,1);
      tcpheader_info(skb->h.th);
      return retval;
}



int changed_tcp_v4_rcv(struct sk_buff *skb){
      int slock_flags;
```

```
	int retval;
	char fname[20];
	char position[2];


	strcpy(fname,"tcp_v4_rcv");
	strcpy(position,"B");
	print_tcp_skb(skb,fname,position,0);


	LOCK_KERN;
	_memcpy(pr, pr_save,NUM_BYTES);
	UNLOCK_KERN;

	retval=pr(skb);

	LOCK_KERN;
	_memcpy(pr, pr_jump,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
	print_tcp_skb(skb,fname,position,1);
	//only_sock(sk,fname,position,0);

	return retval;
}



int init_module() {

	int slock_flags;
	pr=(int (*)(struct sk_buff *))allFunAddr[0];
	pr1=(struct sock * (*)(u32, u16 , u32 , u16 , int))allFunAddr[1];
	pr2=(int (*)(struct sock *,struct sk_buff *))allFunAddr[2];
	pr3=(int (*)(struct sock *,struct sk_buff *,struct tcphdr *,unsigned ))allFunAddr[3];
	pr4=(int (*)(struct sock *,struct sk_buff *,int ))allFunAddr[4];
```

```
pr5=(int (*)(struct sock *,struct tcp_opt *,struct sk_buff *))allFunAddr[5];
pr6=(void (*)(struct sock *,struct sk_buff *))allFunAddr[6];
pr7=(void (*)(struct sock *, int ))allFunAddr[7];
pr8=(void (*)(struct sock *, struct sk_buff *))allFunAddr[8];

*(unsigned int *)(pr_jump+1)=(unsigned int)changed_tcp_v4_rcv;
*(unsigned int *)(pr_jump1+1)=(unsigned int)changed_tcp_v4_lookup;
*(unsigned int *)(pr_jump2+1)=(unsigned int)changed_tcp_v4_do_rcv;
*(unsigned int *)(pr_jump3+1)=(unsigned int)changed_tcp_rcv_established;
*(unsigned int *)(pr_jump4+1)=(unsigned int)changed_tcp_ack;
*(unsigned int *)(pr_jump5+1)=(unsigned int)changed_tcp_event_data_recv;
*(unsigned int *)(pr_jump6+1)=(unsigned int)changed_tcp_data_snd_check;
*(unsigned int *)(pr_jump7+1)=(unsigned int)changed_tcp_ack_snd_check;
*(unsigned int *)(pr_jump8+1)=(unsigned int)changed_tcp_data_queue;


LOCK_KERN;

_memcpy(pr_save,pr,NUM_BYTES);
_memcpy(pr,pr_jump,NUM_BYTES);

_memcpy(pr_save1,pr1,NUM_BYTES);
_memcpy(pr1,pr_jump1,NUM_BYTES);

_memcpy(pr_save2,pr2,NUM_BYTES);
_memcpy(pr2,pr_jump2,NUM_BYTES);

_memcpy(pr_save3,pr3,NUM_BYTES);
_memcpy(pr3,pr_jump3,NUM_BYTES);

_memcpy(pr_save4,pr4,NUM_BYTES);
_memcpy(pr4,pr_jump4,NUM_BYTES);

_memcpy(pr_save5,pr5,NUM_BYTES);
_memcpy(pr5,pr_jump5,NUM_BYTES);

_memcpy(pr_save6,pr6,NUM_BYTES);
_memcpy(pr6,pr_jump6,NUM_BYTES);
```

```
	_memcpy(pr_save7,pr7,NUM_BYTES);
	_memcpy(pr7,pr_jump7,NUM_BYTES);

	_memcpy(pr_save8,pr8,NUM_BYTES);
	_memcpy(pr8,pr_jump8,NUM_BYTES);


	UNLOCK_KERN;



	printk("<1> protocol added\n");


	return 0;
}


void cleanup_module(){
	int slock_flags;


	LOCK_KERN;
	_memcpy(pr, pr_save,NUM_BYTES);
	_memcpy(pr1, pr_save1,NUM_BYTES);
	_memcpy(pr2, pr_save2,NUM_BYTES);
	_memcpy(pr3, pr_save3,NUM_BYTES);
	_memcpy(pr4, pr_save4,NUM_BYTES);
	_memcpy(pr5, pr_save5,NUM_BYTES);
	_memcpy(pr6, pr_save6,NUM_BYTES);
	_memcpy(pr7, pr_save7,NUM_BYTES);
	_memcpy(pr8, pr_save8,NUM_BYTES);


	UNLOCK_KERN;
	if(strlen(big_buffer)>0){
		print_buffer(FILE_NAME,big_buffer,strlen(big_buffer));
```

```
            big_buffer[0]='\0';
        }

        printk("<1> Protocol Removed \n");
}
```

12.3 tcpin.sh

```
/* File name: tcpin.sh
  This file supplies command line parameters after extracting the
  information from /boot/System.map file and loads the module tcpin.c
*/

#!/bin/bash
#This is shell program to load tcpin.o module with requisite parameters


FUN="tcp_v4_rcv"
FUN1="__tcp_v4_lookup"
FUN2="tcp_v4_do_rcv"
FUN3="tcp_rcv_established"
FUN4="tcp_ack"
FUN5="tcp_event_data_recv"
FUN6="__tcp_data_snd_check"
FUN7="__tcp_ack_snd_check"
FUN8="tcp_data_queue"


PR=`cat /boot/System.map  | grep -w $FUN  | cut -c 1-8`
PR1=`cat /boot/System.map | grep -w $FUN1 | cut -c 1-8`
PR2=`cat /boot/System.map | grep -w $FUN2 | cut -c 1-8`
PR3=`cat /boot/System.map | grep -w $FUN3 | cut -c 1-8`
PR4=`cat /boot/System.map | grep -w $FUN4 | cut -c 1-8`
PR5=`cat /boot/System.map | grep -w $FUN5 | cut -c 1-8`
PR6=`cat /boot/System.map | grep -w $FUN6 | cut -c 1-8`
PR7=`cat /boot/System.map | grep -w $FUN7 | cut -c 1-8`
PR8=`cat /boot/System.map | grep -w $FUN8 | cut -c 1-8`


if [ "$PR" = "" ]
then
      echo "PR is empty ,cannot get the address of $FUN "
```

```
elif [ "$PR1" = "" ]
then
      echo "PR1 is empty ,cannot get the address of $FUN1 "
elif [ "$PR2" = "" ]
then
      echo "PR2 is empty ,cannot get the address of $FUN2 "
elif [ "$PR3" = "" ]
then
      echo "PR3 is empty ,cannot get the address of $FUN3 "
 elif [ "$PR4" = "" ]
then
      echo "PR4 is empty ,cannot get the address of $FUN4 "
elif [ "$PR5" = "" ]
then
      echo "PR5 is empty ,cannot get the address of $FUN5 "
elif [ "$PR6" = "" ]
then
      echo "PR6 is empty ,cannot get the address of $FUN6 "
elif [ "$PR7" = "" ]
then
      echo "PR7 is empty ,cannot get the address of $FUN7 "
elif [ "$PR8" = "" ]
then
      echo "PR8 is empty ,cannot get the address of $FUN8 "
else
      echo " insmod tcpin.o allFunAddr=0x$PR,0x$PR1,0x$PR2,0x$PR3,0x$PR4,0x$PR5,0x$PR6,0x$PR7,0x$PR8"
      insmod tcpin.o allFunAddr=0x$PR,0x$PR1,0x$PR2,0x$PR3,0x$PR4,0x$PR5,0x$PR6,0x$PR7,0x$PR8

fi



# notes :

# in the if condition there must be a space between sq brackets and next character both
# at start and at  end

# in if condition $PR must be in quotes as a string is compared against another string namely
```

```
# the null string

# there must be gap before and after = sign in string comparisons and no gap if =
# is used for assignment

# when if and then is placed in same line then there must be ';' between them as both are
# reserved words and two reserved words(commands) can not be on ame line without the
# first one terminating
```

12.4 tcpout.c

```
/* File name: tcpout.c
   This file intercepts Linux TCP functions involved in handling
   Of Outgoing segments
*/

#include "module_header.h"

static int allFunAddr[6] = {0,0,0,0,0,0} ;
MODULE_PARM(allFunAddr, "1-6i");

static unsigned char pr_jump[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save[NUM_BYTES];
static int (*pr)(struct sock *, struct msghdr *, int ); //tcp_sendmsg

static unsigned char pr_jump1[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save1[NUM_BYTES];
static void (*pr1)(struct sock *, struct tcp_opt *, int , int , int );//tcp_push

static unsigned char pr_jump2[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save2[NUM_BYTES];
static void (*pr2)(struct sock *, struct tcp_opt *,unsigned, int);//__tcp_push_pending_frames

static unsigned char pr_jump3[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save3[NUM_BYTES];
static  int (*pr3)(struct sock *, int );//tcp_write_xmit

static unsigned char pr_jump4[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save4[NUM_BYTES];
static int (*pr4)(struct sock *, struct sk_buff * );//tcp_transmit_skb
```

```
static unsigned char pr_jump5[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                                "\xff\xe0"; // jmp *eax
static unsigned char pr_save5[NUM_BYTES];
static int (*pr5)(struct sock *, struct sk_buff *);//tcp_retransmit_skb



extern char big_buffer[BUFSIZE];

void only_sock(struct sock *sk,char *fun_name,char *position,int end) {
      char store_time[20];
        my_time(store_time);
        if(strlen(big_buffer)>=BUFSIZE-RECORD_SIZE){
                printk("<1>out of buffer memory\n");
                return;
        }
        strcat(big_buffer,store_time);
        strcat(big_buffer," ");
      strcat(big_buffer,in_ntoa(sk->saddr));
        strcat(big_buffer,":");
      strcat(big_buffer,in_ntoa16(sk->sport));
      strcat(big_buffer," ");
      strcat(big_buffer,in_ntoa(sk->daddr));
      strcat(big_buffer,":");
      strcat(big_buffer,in_ntoa16(sk->dport));
      strcat(big_buffer," ");
      strcat(big_buffer,fun_name);
      strcat(big_buffer," ");
      strcat(big_buffer,position);
      if(end)
            strcat(big_buffer," ");  // when we get 1 in end we have more data to go
      else
            strcat(big_buffer,"\n");
}
```

```
void print_tcp_skb(struct sk_buff* skb,char * fun_name,char* position,int sockorskb){

      char store_time[20];
      my_time(store_time);
      if(strlen(big_buffer)>=BUFSIZE-RECORD_SIZE){
            printk("<1>out of buffer memory\n");
            return;
      }
      strcat(big_buffer,store_time);
      strcat(big_buffer," ");
      strcat(big_buffer,in_ntoa(skb->nh.iph->saddr));
      strcat(big_buffer,":");
      strcat(big_buffer,in_ntoa16(skb->h.th->source));
      strcat(big_buffer," ");
      strcat(big_buffer,in_ntoa(skb->nh.iph->daddr));
      strcat(big_buffer,":");
      strcat(big_buffer,in_ntoa16(skb->h.th->dest));
      strcat(big_buffer," ");
      strcat(big_buffer,fun_name);
      strcat(big_buffer," ");
      strcat(big_buffer,position);
      strcat(big_buffer," ");
      if(skb->h.th->syn)
            strcat(big_buffer,"S ");

      else if(skb->h.th->fin)
            strcat(big_buffer,"F ");
      else if(skb->h.th->psh)
            strcat(big_buffer,"P ");
      else
            strcat(big_buffer,". ");

      strcat(big_buffer,in_ntoa32(skb->h.th->seq) );
      strcat(big_buffer," ack ");
      strcat(big_buffer,in_ntoa32(skb->h.th->ack_seq));
      strcat(big_buffer,"\n");
}
```

```
void tcpheader_info(struct tcphdr *th){

      if(!th){    // in case th is null return,do not dereference null pointer
            strcat(big_buffer,"\n");
            return;
      }

      if(th->syn)
            strcat(big_buffer,"S ");
      else if(th->fin)
            strcat(big_buffer,"F ");
      else if(th->psh)
            strcat(big_buffer,"P ");
      else
            strcat(big_buffer,". ");

      strcat(big_buffer,in_ntoa32(th->seq));
      strcat(big_buffer," ack ");
      strcat(big_buffer,in_ntoa32(th->ack_seq));

      strcat(big_buffer,"\n");

}

void changed_tcp_push_pending_frames(struct sock *sk, struct tcp_opt *tp, unsigned cur_mss, int nonagle){
      int slock_flags;
      char fname[20];
      char position[2];


      strcpy(fname,"__tcp_push_pending_frames");
      strcpy(position,"B");
      only_sock(sk,fname,position,0);


      LOCK_KERN;
      _memcpy(pr2, pr_save2,NUM_BYTES);
      UNLOCK_KERN;
```

```
	pr2(sk,tp,cur_mss,nonagle);

	LOCK_KERN;
	_memcpy(pr2, pr_jump2,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
	only_sock(sk,fname,position,0);
	return;
}


void changed_tcp_push(struct sock *sk, struct tcp_opt *tp, int flags, int mss_now, int nonagle){
	int slock_flags;
	char fname[20];
	char position[2];


	strcpy(fname,"tcp_push");
	strcpy(position,"B");
	only_sock(sk,fname,position,0);


	LOCK_KERN;
	_memcpy(pr1, pr_save1,NUM_BYTES);
	UNLOCK_KERN;

	pr1(sk,tp,flags,mss_now,nonagle);

	LOCK_KERN;
	_memcpy(pr1, pr_jump1,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
	only_sock(sk,fname,position,0);
	return;
}
```

```
int changed_tcp_retransmit_skb(struct sock *sk, struct sk_buff *skb){
      int slock_flags;
      int retval;
      char fname[20];
      char position[2];


      strcpy(fname,"tcp_retransmit_skb");
      strcpy(position,"B");
      only_sock(sk,fname,position,0);


      LOCK_KERN;
      _memcpy(pr5, pr_save5,NUM_BYTES);
      UNLOCK_KERN;

      retval=pr5(sk,skb);

      LOCK_KERN;
      _memcpy(pr5, pr_jump5,NUM_BYTES);
      UNLOCK_KERN;

      strcpy(position,"E");
      only_sock(sk,fname,position,1);
      tcpheader_info(skb->h.th);
      return retval;
}

int changed_tcp_transmit_skb(struct sock *sk, struct sk_buff *skb){
      int slock_flags;
      int retval;
      char fname[20];
      char position[2];


      strcpy(fname,"tcp_transmit_skb");
      strcpy(position,"B");
```

```
	only_sock(sk,fname,position,0);


	LOCK_KERN;
	_memcpy(pr4, pr_save4,NUM_BYTES);
	UNLOCK_KERN;

	retval=pr4(sk,skb);

	LOCK_KERN;
	_memcpy(pr4, pr_jump4,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
	only_sock(sk,fname,position,1);
	tcpheader_info(skb->h.th);
	return retval;
}



int changed_tcp_write_xmit(struct sock *sk, int nonagle){
	int slock_flags;
	int retval;
	char fname[20];
	char position[2];

	strcpy(fname,"tcp_write_xmit");
	strcpy(position,"B");
	only_sock(sk,fname,position,0);


	LOCK_KERN;
	_memcpy(pr3, pr_save3,NUM_BYTES);
	UNLOCK_KERN;

	retval=pr3(sk,nonagle);
```

```
	LOCK_KERN;
	_memcpy(pr3, pr_jump3,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
	only_sock(sk,fname,position,0);
	return retval;
}



int changed_tcp_sendmsg(struct sock *sk, struct msghdr *msg, int size){
	int slock_flags;
	int retval;
	char fname[20];
	char position[2];


	strcpy(fname,"tcp_sendmsg");
	strcpy(position,"B");
	only_sock(sk,fname,position,0);


	LOCK_KERN;
	_memcpy(pr, pr_save,NUM_BYTES);
	UNLOCK_KERN;

	retval=pr(sk,msg,size);

	LOCK_KERN;
	_memcpy(pr, pr_jump,NUM_BYTES);
	strcpy(position,"E");
	only_sock(sk,fname,position,0);
	UNLOCK_KERN;
	return retval;
}
```

```
int init_module() {

      int slock_flags;

      pr=(int (*)(struct sock *, struct msghdr *, int ))allFunAddr[0];
      pr1=(void (*)(struct sock *, struct tcp_opt *, int , int , int))allFunAddr[1];
      pr2=(void (*)(struct sock *, struct tcp_opt *,unsigned, int))allFunAddr[2];
      pr3=(int (*)(struct sock *, int ))allFunAddr[3];
      pr4=(int (*)(struct sock *, struct sk_buff *))allFunAddr[4];
      pr5=(int (*)(struct sock *, struct sk_buff *))allFunAddr[5];


      *(unsigned int *)(pr_jump+1)=(unsigned int)changed_tcp_sendmsg;
      *(unsigned int *)(pr_jump1+1)=(unsigned int)changed_tcp_push;
      *(unsigned int *)(pr_jump2+1)=(unsigned int)changed_tcp_push_pending_frames;
      *(unsigned int *)(pr_jump3+1)=(unsigned int)changed_tcp_write_xmit;
      *(unsigned int *)(pr_jump4+1)=(unsigned int)changed_tcp_transmit_skb;
      *(unsigned int *)(pr_jump5+1)=(unsigned int)changed_tcp_retransmit_skb;


      LOCK_KERN;

      _memcpy(pr_save,pr,NUM_BYTES);
      _memcpy(pr,pr_jump,NUM_BYTES);

      _memcpy(pr_save1,pr1,NUM_BYTES);
      _memcpy(pr1,pr_jump1,NUM_BYTES);

      _memcpy(pr_save2,pr2,NUM_BYTES);
      _memcpy(pr2,pr_jump2,NUM_BYTES);

      _memcpy(pr_save3,pr3,NUM_BYTES);
      _memcpy(pr3,pr_jump3,NUM_BYTES);

      _memcpy(pr_save4,pr4,NUM_BYTES);
      _memcpy(pr4,pr_jump4,NUM_BYTES);
```

```
	_memcpy(pr_save5,pr5,NUM_BYTES);
	_memcpy(pr5,pr_jump5,NUM_BYTES);



	UNLOCK_KERN;



	printk("<1> protocol added\n");


	return 0;
}


void cleanup_module(){
	int slock_flags;


	LOCK_KERN;
	_memcpy(pr, pr_save,NUM_BYTES);
	_memcpy(pr1, pr_save1,NUM_BYTES);
	_memcpy(pr2, pr_save2,NUM_BYTES);
	_memcpy(pr3, pr_save3,NUM_BYTES);
	_memcpy(pr4, pr_save4,NUM_BYTES);
	_memcpy(pr5, pr_save5,NUM_BYTES);

	UNLOCK_KERN;
	if(strlen(big_buffer)>0){
		print_buffer(FILE_NAME,big_buffer,strlen(big_buffer));
		big_buffer[0]='\0';
	}

	printk("<1> Protocol Removed \n");
}
```

12.5 tcpout.sh

```
/* File name: tcpout.sh
  This file supplies command line parameters after extracting the
  information from /boot/System.map file and loads the module tcpout.o
*/

#!/bin/bash
#This is shell program to load tcpout.o module with requisite parameters


FUN="tcp_sendmsg"
FUN1="tcp_push"
FUN2="__tcp_push_pending_frames"
FUN3="tcp_write_xmit"
FUN4="tcp_transmit_skb"
FUN5="tcp_retransmit_skb"



PR=`cat /boot/System.map  | grep -w $FUN  | cut -c 1-8`
PR1=`cat /boot/System.map | grep -w $FUN1 | cut -c 1-8`
PR2=`cat /boot/System.map | grep -w $FUN2 | cut -c 1-8`
PR3=`cat /boot/System.map | grep -w $FUN3 | cut -c 1-8`
PR4=`cat /boot/System.map | grep -w $FUN4 | cut -c 1-8`
PR5=`cat /boot/System.map | grep -w $FUN5 | cut -c 1-8`


if [ "$PR" = "" ]
then
      echo "PR is empty ,cannot get the address of $FUN "
elif [ "$PR1" = "" ]
then
      echo "PR1 is empty ,cannot get the address of $FUN1 "
elif [ "$PR2" = "" ]
then
      echo "PR2 is empty ,cannot get the address of $FUN2 "
```

```
elif [ "$PR3" = "" ]
then
      echo "PR3 is empty ,cannot get the address of $FUN3 "
 elif [ "$PR4" = "" ]
then
      echo "PR4 is empty ,cannot get the address of $FUN4 "
elif [ "$PR5" = "" ]
then
      echo "PR5 is empty ,cannot get the address of $FUN5 "
else
      echo " insmod tcpout.o allFunAddr=0x$PR,0x$PR1,0x$PR2,0x$PR3,0x$PR4,0x$PR5"
      insmod tcpout.o allFunAddr=0x$PR,0x$PR1,0x$PR2,0x$PR3,0x$PR4,0x$PR5

fi
```

12.6 synfin.c

```
/* File name: synfin.c
   This file intercepts Linux TCP functions involved in TCP
   Connection Management and TCP state changes
*/

#include "module_header.h"

static int allFunAddr[17] = {0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0} ;
MODULE_PARM(allFunAddr, "1-17i");

static unsigned char pr_jump[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save[NUM_BYTES];
static int (*pr)(struct sock *); //tcp_v4_init_sock

static unsigned char pr_jump1[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save1[NUM_BYTES];
static int (*pr1)(struct sock *, int,int,char *,int);//tcp_setsockopt

static unsigned char pr_jump2[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save2[NUM_BYTES];
static int (*pr2)(struct sock *);//tcp_connect

static unsigned char pr_jump3[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save3[NUM_BYTES];
static unsigned int (*pr3)(struct sock *,struct sockaddr *,int );//tcp_v4_connect

static unsigned char pr_jump4[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save4[NUM_BYTES];
static int (*pr4)(struct sock *,struct sk_buff *,struct tcphdr *,unsigned );//tcp_rcv_synsent_state_process
```

```
static unsigned char pr_jump5[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save5[NUM_BYTES];
static int (*pr5)(struct sock *);//tcp_send_ack

static unsigned char pr_jump6[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save6[NUM_BYTES];
static int (*pr6)(struct sock *, struct sk_buff *,struct tcphdr *, unsigned);//tcp_rcv_state_process

static unsigned char pr_jump7[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save7[NUM_BYTES];
static int (*pr7)(struct sock *, struct open_request *, struct sk_buff *);//tcp_create_openreq_child

static unsigned char pr_jump8[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save8[NUM_BYTES];
static int (*pr8)(struct sock *, struct sk_buff *);//tcp_v4_conn_request

static unsigned char pr_jump9[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save9[NUM_BYTES];
static int (*pr9)(struct sock *, struct open_request *,struct dst_entry *);//tcp_v4_send_synack


static unsigned char pr_jump10[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save10[NUM_BYTES];
static int (*pr10)(struct sock *, long );//tcp_close

static unsigned char pr_jump11[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save11[NUM_BYTES];
static int (*pr11)(struct sock *);//tcp_send_fin
```

```
static unsigned char pr_jump12[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save12[NUM_BYTES];
static int (*pr12)(struct sock *);//tcp_close_state

static unsigned char pr_jump13[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save13[NUM_BYTES];
static int (*pr13)(struct sk_buff *, struct sock *, struct tcphdr *);//tcp_fin

static unsigned char pr_jump14[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save14[NUM_BYTES];
static void (*pr14)(struct sock *);//tcp_send_delayed_ack

static unsigned char pr_jump15[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save15[NUM_BYTES];
static int (*pr15)(struct sock *,int,int );//tcp_time_wait

static unsigned char pr_jump16[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save16[NUM_BYTES];
static void (*pr16)(struct sock *,int );//tcp_set_state


extern char big_buffer[BUFSIZE];



void only_sock(struct sock *sk,char *fun_name,char *position,int end) {
      char store_time[20];
      my_time(store_time);
      if(strlen(big_buffer)>= BUFSIZE - RECORD_SIZE){
            printk("<1>out of buffer memory\n");
            return;
```

```
	}

	strcat(big_buffer,store_time);
	strcat(big_buffer," ");
	if(sk){
		strcat(big_buffer,in_ntoa(sk->saddr));
		strcat(big_buffer,":");
		strcat(big_buffer,in_ntoa16(sk->sport));
		strcat(big_buffer," ");
		strcat(big_buffer,in_ntoa(sk->daddr));
		strcat(big_buffer,":");
		strcat(big_buffer,in_ntoa16(sk->dport));
		strcat(big_buffer," ");
	}
	strcat(big_buffer,fun_name);
	strcat(big_buffer," ");
	strcat(big_buffer,position);
	if(end && sk)
		strcat(big_buffer," ");  // when we get 1 in end we have more data to go
	else
		strcat(big_buffer,"\n");
}


/*
void print_tcp_skb(struct sock *sk,struct sk_buff* skb,char * fun_name,char* position){

	char store_time[20];
	my_time(store_time);
	if(strlen(big_buffer)>=BUFSIZE-RECORD_SIZE){
		printk("<1>out of buffer memory\n");
		return;
	}
	strcat(big_buffer,store_time);
	strcat(big_buffer," ");
	strcat(big_buffer,in_ntoa(sk->saddr));
	strcat(big_buffer,":");
	strcat(big_buffer,in_ntoa16(skb->h.th->source));
```

```
	strcat(big_buffer," ");
	strcat(big_buffer,in_ntoa(sk->daddr));
	strcat(big_buffer,":");
	strcat(big_buffer,in_ntoa16(skb->h.th->dest));
	strcat(big_buffer," ");
	if(skb->h.th->syn)
		strcat(big_buffer,"S ");

	else if(skb->h.th->psh)
		strcat(big_buffer,"P ");
	else if(skb->h.th->fin)
		strcat(big_buffer,"F ");
	else
		strcat(big_buffer,". ");

	strcat(big_buffer,in_ntoa32(skb->h.th->seq) );
	strcat(big_buffer," ack ");
	strcat(big_buffer,in_ntoa32(skb->h.th->ack_seq));
	strcat(big_buffer," ");
	strcat(big_buffer,fun_name);
	strcat(big_buffer," ");
	strcat(big_buffer,position);
	strcat(big_buffer,"\n");
}
*/

void tcpheader_info(struct tcphdr *th){

	if(strlen(big_buffer)>= BUFSIZE - RECORD_SIZE){
		strcat(big_buffer,"out of buffer memory\n");
		return;
	}

	if(!th){    // in case th is null return,do not dereference null pointer
		strcat(big_buffer,"\n");
		return;
	}
```

```
	if(th->syn)
		strcat(big_buffer,"S ");
	else if(th->psh)
		strcat(big_buffer,"P ");
	else if(th->fin)
		strcat(big_buffer,"F ");
	else
		strcat(big_buffer,". ");

	strcat(big_buffer,in_ntoa32(th->seq));
	strcat(big_buffer," ack ");
	strcat(big_buffer,in_ntoa32(th->ack_seq));

	strcat(big_buffer,"\n");

}

int changed_tcp_v4_send_synack(struct sock *sk, struct open_request *req,struct dst_entry *dst){

	int slock_flags;
	int retval;
	char fname[30];
	char position[2];

	strcpy(fname,"tcp_v4_send_synack");
	strcpy(position,"B");

	only_sock(sk,fname,position,0);



	LOCK_KERN;
	_memcpy(pr9, pr_save9,NUM_BYTES);
	UNLOCK_KERN;

	retval=pr9(sk,req,dst);
```

```
	LOCK_KERN;
	_memcpy(pr9, pr_jump9,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
	only_sock(sk,fname,position,0);


	return retval;
}

int changed_tcp_v4_conn_request(struct sock *sk, struct sk_buff *skb){

	int slock_flags;
	int retval;
	char fname[30];
	char position[2];

	strcpy(fname,"tcp_v4_conn_request");
	strcpy(position,"B");

	only_sock(sk,fname,position,0);



	LOCK_KERN;
	_memcpy(pr8, pr_save8,NUM_BYTES);
	UNLOCK_KERN;

	retval=pr8(sk,skb);

	LOCK_KERN;
	_memcpy(pr8, pr_jump8,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
	only_sock(sk,fname,position,0);
```

```
	return retval;
}


int changed_tcp_create_openreq_child(struct sock *sk, struct open_request *req, struct sk_buff *skb){

	int slock_flags;
	int retval;
	char fname[30];
	char position[2];

	strcpy(fname,"tcp_create_openreq_child");
	strcpy(position,"B");

	only_sock(sk,fname,position,0);



	LOCK_KERN;
	_memcpy(pr7, pr_save7,NUM_BYTES);
	UNLOCK_KERN;

	retval=pr7(sk,req,skb);

	LOCK_KERN;
	_memcpy(pr7, pr_jump7,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
	only_sock(sk,fname,position,0);


	return retval;
}

int changed_tcp_rcv_state_process(struct sock *sk,struct sk_buff *skb,struct tcphdr *th, unsigned len){
```

```
      int slock_flags;
      int retval;
      char fname[30];
      char position[2];

      strcpy(fname,"tcp_rcv_state_process");
      strcpy(position,"B");

      only_sock(sk,fname,position,0);



      LOCK_KERN;
      _memcpy(pr6, pr_save6,NUM_BYTES);
      UNLOCK_KERN;

      retval=pr6(sk,skb,th,len);

      LOCK_KERN;
      _memcpy(pr6, pr_jump6,NUM_BYTES);
      UNLOCK_KERN;

      strcpy(position,"E");
      only_sock(sk,fname,position,0);


      return retval;
}



int changed_tcp_send_ack(struct sock *sk){
      int slock_flags;
      int retval;
      char fname[30];
      char position[2];
```

```
	strcpy(fname,"tcp_send_ack");
	strcpy(position,"B");

	only_sock(sk,fname,position,0);



	LOCK_KERN;
	_memcpy(pr5, pr_save5,NUM_BYTES);
	UNLOCK_KERN;

	retval=pr5(sk);

	LOCK_KERN;
	_memcpy(pr5, pr_jump5,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
	only_sock(sk,fname,position,0);


	return retval;
}


/*
int changed_tcp_transmit_skb(struct sock *sk, struct sk_buff *skb){
	int slock_flags;
	int retval;
	char fname[30];
	char position[2];

	strcpy(fname,"tcp_transmit_skb");
	strcpy(position,"B");

	if(skb){                              //if skb in not null pointer do this
		only_sock(sk,fname,position,1);
		tcpheader_info(skb->h.th);
```

```
	}
	else {
		only_sock(sk,fname,position,0);  // no printing of tcp sequence details
	}



	LOCK_KERN;
	_memcpy(pr5, pr_save5,NUM_BYTES);
	UNLOCK_KERN;

	retval=pr5(sk,skb);

	LOCK_KERN;
	_memcpy(pr5, pr_jump5,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
	if(skb){                          //if skb in not null pointer do this
		only_sock(sk,fname,position,1);
		tcpheader_info(skb->h.th);
	}
	else {
		only_sock(sk,fname,position,0);  // no printing of tcp sequence details
	}


	return retval;
}
*/


int changed_tcp_rcv_synsent_state_process(struct sock *sk, struct sk_buff *skb,struct tcphdr *th, unsigned
len){
	int slock_flags;
	int retval;
	char fname[30];
	char position[2];
```

```
	strcpy(fname,"tcp_rcv_synsent_state_process");
	strcpy(position,"B");
	only_sock(sk,fname,position,1);
	tcpheader_info(th);


	LOCK_KERN;
	_memcpy(pr4, pr_save4,NUM_BYTES);
	UNLOCK_KERN;

	retval=pr4(sk,skb,th,len);

	LOCK_KERN;
	_memcpy(pr4, pr_jump4,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
	only_sock(sk,fname,position,1);
	tcpheader_info(th);
	return retval;
}

int changed_tcp_v4_connect(struct sock *sk, struct sockaddr *uaddr, int addr_len){
	int slock_flags;
	int retval;
	char fname[20];
	char position[2];

	strcpy(fname,"tcp_v4_connect");
	strcpy(position,"B");
	only_sock(sk,fname,position,0);


	LOCK_KERN;
	_memcpy(pr3, pr_save3,NUM_BYTES);
	UNLOCK_KERN;
```

```
	retval=pr3(sk,uaddr,addr_len);

	LOCK_KERN;
	_memcpy(pr3, pr_jump3,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
	only_sock(sk,fname,position,0);

	return retval;
}




int changed_tcp_connect(struct sock *sk){
	int slock_flags;
	int retval;
	char fname[20];
	char position[2];

	strcpy(fname,"tcp_connect");
	strcpy(position,"B");
	only_sock(sk,fname,position,0);


	LOCK_KERN;
	_memcpy(pr2, pr_save2,NUM_BYTES);
	UNLOCK_KERN;

	retval=pr2(sk);

	LOCK_KERN;
	_memcpy(pr2, pr_jump2,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
```

```
	only_sock(sk,fname,position,0);

	return retval;
}



int changed_tcp_setsockopt(struct sock *sk, int level, int optname, char *optval,int optlen){
	int slock_flags;
	int retval;
	char fname[20];
	char position[2];

	strcpy(fname,"tcp_setsockopt");
	strcpy(position,"B");
	only_sock(sk,fname,position,0);


	LOCK_KERN;
	_memcpy(pr1, pr_save1,NUM_BYTES);
	UNLOCK_KERN;

	retval=pr1(sk,level,optname,optval,optlen);

	LOCK_KERN;
	_memcpy(pr1, pr_jump1,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
	only_sock(sk,fname,position,0);

	return retval;
}
```

```
int changed_tcp_v4_init_sock(struct sock *sk){
      int slock_flags;
      int retval;
      char fname[20];
      char position[2];

      //printk("<1> Hello gyan I am Here\n");
      strcpy(fname,"tcp_v4_init_sock");
      strcpy(position,"B") ;
      only_sock(sk,fname,position,0) ;


      LOCK_KERN;
      _memcpy(pr, pr_save,NUM_BYTES);
      UNLOCK_KERN;

      retval=pr(sk);

      LOCK_KERN;
      _memcpy(pr, pr_jump,NUM_BYTES);
      UNLOCK_KERN;

      strcpy(position,"E");
      only_sock(sk,fname,position,0);

      return retval;
}


int changed_tcp_close(struct sock *sk, long timeout){
      int slock_flags;
      int retval;
      char fname[20];
      char position[2];

      //printk("<1> Hello gyan I am Here\n");
      strcpy(fname,"tcp_close");
      strcpy(position,"B");
```

```
	only_sock(sk,fname,position,0);


	LOCK_KERN;
	_memcpy(pr10, pr_save10,NUM_BYTES);
	UNLOCK_KERN;

	retval=pr10(sk,timeout);

	LOCK_KERN;
	_memcpy(pr10, pr_jump10,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
	only_sock(sk,fname,position,0);

	return retval;
}

int changed_tcp_send_fin(struct sock *sk){
	int slock_flags;
	int retval;
	char fname[20];
	char position[2];

	//printk("<1> Hello gyan I am Here\n");
	strcpy(fname,"tcp_send_fin");
	strcpy(position,"B");
	only_sock(sk,fname,position,0);


	LOCK_KERN;
	_memcpy(pr11, pr_save11,NUM_BYTES);
	UNLOCK_KERN;

	retval=pr11(sk);

	LOCK_KERN;
```

```
	_memcpy(pr11, pr_jump11,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
	only_sock(sk,fname,position,0);

	return retval;
}

int changed_tcp_close_state(struct sock *sk){
	int slock_flags;
	int retval;
	char fname[20];
	char position[2];

	//printk("<1> Hello gyan I am Here\n");
	strcpy(fname,"tcp_close_state");
	strcpy(position,"B");
	only_sock(sk,fname,position,0);


	LOCK_KERN;
	_memcpy(pr12, pr_save12,NUM_BYTES);
	UNLOCK_KERN;

	retval=pr12(sk);

	LOCK_KERN;
	_memcpy(pr12, pr_jump12,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
	only_sock(sk,fname,position,0);

	return retval;
}

int changed_tcp_fin(struct sk_buff *skb, struct sock *sk, struct tcphdr *th){
```

```
int slock_flags;
int retval;
char fname[20];
char position[2];

//printk("<1> Hello gyan I am Here\n");
strcpy(fname,"tcp_fin");
strcpy(position,"B");
if(skb){                              //if skb in not null pointer do this
      only_sock(sk,fname,position,1);
      if(th)
            tcpheader_info(th);
}
else {
      only_sock(sk,fname,position,0);  // no printing of tcp sequence details
}



//only_sock(sk,fname,position,0);


LOCK_KERN;
_memcpy(pr13, pr_save13,NUM_BYTES);
UNLOCK_KERN;

retval=pr13(skb,sk,th);

LOCK_KERN;
_memcpy(pr13, pr_jump13,NUM_BYTES);
UNLOCK_KERN;

strcpy(position,"E");
if(skb){                              //if skb in not null pointer do this
      only_sock(sk,fname,position,1);
      if (th)
            tcpheader_info(th);
```

```
	}
	else {
		only_sock(sk,fname,position,0);  // no printing of tcp sequence details as skb is null
	}

//	only_sock(sk,fname,position,0);

	return retval;
}


void changed_tcp_send_delayed_ack(struct sock *sk){
	int slock_flags;
	//int retval;
	char fname[20];
	char position[2];

	//printk("<1> Hello gyan I am Here\n");
	strcpy(fname,"tcp_send_delayed_ack");
	strcpy(position,"B");
	only_sock(sk,fname,position,0);


	LOCK_KERN;
	_memcpy(pr14, pr_save14,NUM_BYTES);
	UNLOCK_KERN;

	pr14(sk);

	LOCK_KERN;
	_memcpy(pr14, pr_jump14,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
	only_sock(sk,fname,position,0);

	return;
}
```

```
int changed_tcp_time_wait(struct sock *sk, int state, int timeo){
      int slock_flags;
      int retval;
      char fname[20];
      char position[2];

      //printk("<1> Hello gyan I am Here\n");
      strcpy(fname,"tcp_time_wait");
      strcpy(position,"B");
      only_sock(sk,fname,position,0);


      LOCK_KERN;
      _memcpy(pr15, pr_save15,NUM_BYTES);
      UNLOCK_KERN;

      retval=pr15(sk,state,timeo);

      LOCK_KERN;
      _memcpy(pr15, pr_jump15,NUM_BYTES);
      UNLOCK_KERN;

      strcpy(position,"E");
      only_sock(sk,fname,position,0);

      return retval;
}


void changed_tcp_set_state(struct sock *sk, int state){
      int slock_flags;
      //int retval;
      char fname[20];
      char position[2];
```

```
	//printk("<1> Hello gyan I am Here\n");
	strcpy(fname,"tcp_set_state");
	strcpy(position,"B");
	only_sock(sk,fname,position,0);


	LOCK_KERN;
	_memcpy(pr16, pr_save16,NUM_BYTES);
	UNLOCK_KERN;

	pr16(sk,state);

	LOCK_KERN;
	_memcpy(pr16, pr_jump16,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
	only_sock(sk,fname,position,0);

	return;
}


int init_module() {

	int slock_flags;

	pr=(int (*)(struct sock *))allFunAddr[0];
	pr1=(int (*)(struct sock *, int,int,char *,int))allFunAddr[1];
	pr2=(int (*)(struct sock *))allFunAddr[2];
	pr3=(unsigned int (*)(struct sock *,struct sockaddr *,int ))allFunAddr[3];
	pr4=(int (*)(struct sock *,struct sk_buff *,struct tcphdr *,unsigned ))allFunAddr[4];
	pr5=(int (*)(struct sock *))allFunAddr[5];
	pr6=(int (*)(struct sock *, struct sk_buff *,struct tcphdr *, unsigned ))allFunAddr[6];
	pr7=(int (*)(struct sock *, struct open_request *, struct sk_buff *))allFunAddr[7];
	pr8=(int (*)(struct sock *, struct sk_buff *))allFunAddr[8];
	pr9=(int (*)(struct sock *, struct open_request *,struct dst_entry *))allFunAddr[9];
	pr10=(int (*)(struct sock *, long ))allFunAddr[10];
```

```
pr11=(int (*)(struct sock *))allFunAddr[11];
pr12=(int (*)(struct sock *))allFunAddr[12];
pr13=(int (*)(struct sk_buff *, struct sock *, struct tcphdr *))allFunAddr[13];
pr14=(void (*)(struct sock *))allFunAddr[14];
pr15=(int (*)(struct sock *,int,int ))allFunAddr[15];
pr16=(void (*)(struct sock *,int ))allFunAddr[16];


*(unsigned int *)(pr_jump+1)=(unsigned int)changed_tcp_v4_init_sock;
*(unsigned int *)(pr_jump1+1)=(unsigned int)changed_tcp_setsockopt;
*(unsigned int *)(pr_jump2+1)=(unsigned int)changed_tcp_connect;
*(unsigned int *)(pr_jump3+1)=(unsigned int)changed_tcp_v4_connect;
*(unsigned int *)(pr_jump4+1)=(unsigned int)changed_tcp_rcv_synsent_state_process;
*(unsigned int *)(pr_jump5+1)=(unsigned int)changed_tcp_send_ack;
*(unsigned int *)(pr_jump6+1)=(unsigned int)changed_tcp_rcv_state_process;
*(unsigned int *)(pr_jump7+1)=(unsigned int)changed_tcp_create_openreq_child;
*(unsigned int *)(pr_jump8+1)=(unsigned int)changed_tcp_v4_conn_request;
*(unsigned int *)(pr_jump9+1)=(unsigned int)changed_tcp_v4_send_synack;
*(unsigned int *)(pr_jump10+1)=(unsigned int)changed_tcp_close;
*(unsigned int *)(pr_jump11+1)=(unsigned int)changed_tcp_send_fin;
*(unsigned int *)(pr_jump12+1)=(unsigned int)changed_tcp_close_state;
*(unsigned int *)(pr_jump13+1)=(unsigned int)changed_tcp_fin;
*(unsigned int *)(pr_jump14+1)=(unsigned int)changed_tcp_send_delayed_ack;
*(unsigned int *)(pr_jump15+1)=(unsigned int)changed_tcp_time_wait;
*(unsigned int *)(pr_jump16+1)=(unsigned int)changed_tcp_set_state;

LOCK_KERN;

_memcpy(pr_save,pr,NUM_BYTES);
_memcpy(pr,pr_jump,NUM_BYTES);

_memcpy(pr_save1,pr1,NUM_BYTES);
_memcpy(pr1,pr_jump1,NUM_BYTES);

_memcpy(pr_save2,pr2,NUM_BYTES);
_memcpy(pr2,pr_jump2,NUM_BYTES);

_memcpy(pr_save3,pr3,NUM_BYTES);
```

```
_memcpy(pr3,pr_jump3,NUM_BYTES);

_memcpy(pr_save4,pr4,NUM_BYTES);
_memcpy(pr4,pr_jump4,NUM_BYTES);

_memcpy(pr_save5,pr5,NUM_BYTES);
_memcpy(pr5,pr_jump5,NUM_BYTES);

_memcpy(pr_save6,pr6,NUM_BYTES);
_memcpy(pr6,pr_jump6,NUM_BYTES);

_memcpy(pr_save7,pr7,NUM_BYTES);
_memcpy(pr7,pr_jump7,NUM_BYTES);

_memcpy(pr_save8,pr8,NUM_BYTES);
_memcpy(pr8,pr_jump8,NUM_BYTES);

_memcpy(pr_save9,pr9,NUM_BYTES);
_memcpy(pr9,pr_jump9,NUM_BYTES);

_memcpy(pr_save10,pr10,NUM_BYTES);
_memcpy(pr10,pr_jump10,NUM_BYTES);

_memcpy(pr_save11,pr11,NUM_BYTES);
_memcpy(pr11,pr_jump11,NUM_BYTES);

_memcpy(pr_save12,pr12,NUM_BYTES);
_memcpy(pr12,pr_jump12,NUM_BYTES);

_memcpy(pr_save13,pr13,NUM_BYTES);
_memcpy(pr13,pr_jump13,NUM_BYTES);

_memcpy(pr_save14,pr14,NUM_BYTES);
_memcpy(pr14,pr_jump14,NUM_BYTES);

_memcpy(pr_save15,pr15,NUM_BYTES);
_memcpy(pr15,pr_jump15,NUM_BYTES);
```

```
	_memcpy(pr_save16,pr16,NUM_BYTES);
	_memcpy(pr16,pr_jump16,NUM_BYTES);


	UNLOCK_KERN;


	printk("<1> protocol added\n");


	return 0;
}


void cleanup_module(){
	int slock_flags;


	LOCK_KERN;
	_memcpy(pr, pr_save,NUM_BYTES);
	_memcpy(pr1, pr_save1,NUM_BYTES);
	_memcpy(pr2, pr_save2,NUM_BYTES);
	_memcpy(pr3, pr_save3,NUM_BYTES);
	_memcpy(pr4, pr_save4,NUM_BYTES);
	_memcpy(pr5, pr_save5,NUM_BYTES);
	_memcpy(pr6, pr_save6,NUM_BYTES);
	_memcpy(pr7, pr_save7,NUM_BYTES);
	_memcpy(pr8, pr_save8,NUM_BYTES);
	_memcpy(pr9, pr_save9,NUM_BYTES);
	_memcpy(pr10, pr_save10,NUM_BYTES);
	_memcpy(pr11, pr_save11,NUM_BYTES);
	_memcpy(pr12, pr_save12,NUM_BYTES);
	_memcpy(pr13, pr_save13,NUM_BYTES);
	_memcpy(pr14, pr_save14,NUM_BYTES);
	_memcpy(pr15, pr_save15,NUM_BYTES);
	_memcpy(pr16, pr_save16,NUM_BYTES);

	UNLOCK_KERN;
```

```
	if(strlen(big_buffer)>0){
		print_buffer(FILE_NAME,big_buffer,strlen(big_buffer));
		//big_buffer[0]='\0';
	}

	printk("<1> Protocol Removed \n");
}
```

12.7 synfin.sh

```
/* File name: synfin.sh
  This file supplies command line parameters after extracting the
  information from /boot/System.map file and loads the module synfin.o
*/



#!/bin/bash
#This is shell program to load tcpin.o module with requisite parameters


FUN="tcp_v4_init_sock"
FUN1="tcp_setsockopt"
FUN2="tcp_connect"
FUN3="tcp_v4_connect"
FUN4="tcp_rcv_synsent_state_process"
FUN5="tcp_send_ack"
FUN6="tcp_rcv_state_process"
FUN7="tcp_create_openreq_child"
FUN8="tcp_v4_conn_request"
FUN9="tcp_v4_send_synack"
FUN10="tcp_close"
FUN11="tcp_send_fin"
FUN12="tcp_close_state"
FUN13="tcp_fin"
FUN14="tcp_send_delayed_ack"
FUN15="tcp_time_wait"
FUN16="tcp_set_state"



PR=`cat /boot/System.map  | grep -w $FUN  | cut -c 1-8`
PR1=`cat /boot/System.map | grep -w $FUN1 | cut -c 1-8`
PR2=`cat /boot/System.map | grep -w $FUN2 | cut -c 1-8`
```

```
PR3=`cat /boot/System.map | grep -w $FUN3 | cut -c 1-8`
PR4=`cat /boot/System.map | grep -w $FUN4 | cut -c 1-8`
PR5=`cat /boot/System.map | grep -w $FUN5 | cut -c 1-8`
PR6=`cat /boot/System.map | grep -w $FUN6 | cut -c 1-8`
PR7=`cat /boot/System.map | grep -w $FUN7 | cut -c 1-8`
PR8=`cat /boot/System.map | grep -w $FUN8 | cut -c 1-8`
PR9=`cat /boot/System.map | grep -w $FUN9 | cut -c 1-8`
PR10=`cat /boot/System.map | grep -w $FUN10 | cut -c 1-8`
PR11=`cat /boot/System.map | grep -w $FUN11 | cut -c 1-8`
PR12=`cat /boot/System.map | grep -w $FUN12 | cut -c 1-8`
PR13=`cat /boot/System.map | grep -w $FUN13 | cut -c 1-8`
PR14=`cat /boot/System.map | grep -w $FUN14 | cut -c 1-8`
PR15=`cat /boot/System.map | grep -w $FUN15 | cut -c 1-8`
PR16=`cat /boot/System.map | grep -w $FUN16 | cut -c 1-8`


if [ "$PR" = "" ]
then
      echo "PR is empty ,cannot get the address of $FUN "
elif [ "$PR1" = "" ]
then
      echo "PR1 is empty ,cannot get the address of $FUN1 "
elif [ "$PR2" = "" ]
then
      echo "PR2 is empty ,cannot get the address of $FUN2 "
elif [ "$PR3" = "" ]
then
      echo "PR3 is empty ,cannot get the address of $FUN3 "
 elif [ "$PR4" = "" ]
then
      echo "PR4 is empty ,cannot get the address of $FUN4 "
elif [ "$PR5" = "" ]
then
      echo "PR5 is empty ,cannot get the address of $FUN5 "
elif [ "$PR6" = "" ]
then
      echo "PR6 is empty ,cannot get the address of $FUN6 "
elif [ "$PR7" = "" ]
```

```
then
      echo "PR7 is empty ,cannot get the address of $FUN7 "
elif [ "$PR8" = "" ]
then
      echo "PR8 is empty ,cannot get the address of $FUN8 "
elif [ "$PR9" = "" ]
then
      echo "PR9 is empty ,cannot get the address of $FUN9 "
elif [ "$PR10" = "" ]
then
      echo "PR10 is empty ,cannot get the address of $FUN10 "
elif [ "$PR11" = "" ]
then
      echo "PR11 is empty ,cannot get the address of $FUN11 "
elif [ "$PR12" = "" ]
then
      echo "PR12 is empty ,cannot get the address of $FUN12 "
elif [ "$PR13" = "" ]
then
      echo "PR13 is empty ,cannot get the address of $FUN13 "
elif [ "$PR14" = "" ]
then
      echo "PR14 is empty ,cannot get the address of $FUN14 "
elif [ "$PR15" = "" ]
then
      echo "PR15 is empty ,cannot get the address of $FUN15 "
elif [ "$PR16" = "" ]
then
      echo "PR16 is empty ,cannot get the address of $FUN16 "

else
      echo " insmod synfin.o allFunAddr=0x$PR,0x$PR1,0x$PR2,0x$PR3,0x$PR4,0x$PR5,0x$PR6,0x$PR7,"
      echo "0x$PR8,0x$PR9,0x$PR10,0x$PR11,0x$PR12,0x$PR13,0x$PR14,0x$PR15,0x$PR16"
      insmod synfin.o allFunAddr=0x$PR,0x$PR1,0x$PR2,0x$PR3,0x$PR4,0x$PR5,0x$PR6,0x$PR7,0x$PR8,\
0x$PR9,0x$PR10,0x$PR11,0x$PR12,0x$PR13,0x$PR14,0x$PR15,0x$PR16

fi
```

12.8 tcp_prot.c

```
/* File name: tcp_prot.c
   This file intercepts Linux TCP functions involved in handling
   of Protocol related data such as congestion window e.t.c.

*/

#include "module_header.h"
static int allFunAddr[5] = { 0,0,0,0,0 } ;
MODULE_PARM(allFunAddr, "1-5i");


static unsigned char pr_jump[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                                "\xff\xe0"; // jmp *eax
static unsigned char pr_save[NUM_BYTES];
static int (*pr)(struct sock *); //__tcp_select_window

static unsigned char pr_jump1[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                                "\xff\xe0"; // jmp *eax
static unsigned char pr_save1[NUM_BYTES];
static u32 (*pr1)(struct tcp_opt *);//tcp_receive_window

static unsigned char pr_jump2[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                                "\xff\xe0"; // jmp *eax
static unsigned char pr_save2[NUM_BYTES];
static void (*pr2)(struct tcp_opt *);//tcp_cong_avoid


static unsigned char pr_jump3[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                                "\xff\xe0"; // jmp *eax
static unsigned char pr_save3[NUM_BYTES];
static  void (*pr3)(struct sock *,int );//tcp_enter_loss

static unsigned char pr_jump4[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                                "\xff\xe0"; // jmp *eax
```

```
static unsigned char pr_save4[NUM_BYTES];
static __u32 (*pr4)(struct tcp_opt *);//tcp_recalc_ssthresh


extern char big_buffer[BUFSIZE];


void only_sock(struct sock *sk,char *fun_name,char *position,int end) {
      char store_time[20];
      my_time(store_time);
      if(strlen(big_buffer)>=BUFSIZE - RECORD_SIZE){
            printk("<1>out of buffer memory\n");
            return;
      }
      strcat(big_buffer,store_time);
      strcat(big_buffer," ");
      strcat(big_buffer,in_ntoa(sk->saddr));
      strcat(big_buffer,":");
      strcat(big_buffer,in_ntoa16(sk->sport));
      strcat(big_buffer," ");
      strcat(big_buffer,in_ntoa(sk->daddr));
      strcat(big_buffer,":");
      strcat(big_buffer,in_ntoa16(sk->dport));
      strcat(big_buffer," ");
      strcat(big_buffer,fun_name);
      strcat(big_buffer," ");
      strcat(big_buffer,position);
      if(end)
            strcat(big_buffer," ");  // when we get 1 in end we have more data to go
      else
            strcat(big_buffer,"\n");
}




__u32 changed_tcp_recalc_ssthresh(struct tcp_opt *tp){
```

```
int slock_flags;
__u32 retval;
char fun_name[20];
char position[2];
char cwnd[12];
char ssth[12];
char store_time[20];
my_time(store_time);
if(strlen(big_buffer)<BUFSIZE - RECORD_SIZE){

      strcpy(fun_name,"tcp_recalc_ssthresh");
      strcpy(position,"B");

      sprintf(cwnd,"%u",tp->snd_cwnd);
      strcpy(position,"B");
      strcat(big_buffer,store_time);
      strcat(big_buffer," ");
      strcat(big_buffer,"CWND: ");
      strcat(big_buffer,cwnd);
      strcat(big_buffer," ");

      strcat(big_buffer,fun_name);
      strcat(big_buffer," ");
      strcat(big_buffer,position);
      strcat(big_buffer,"\n");
}


LOCK_KERN;
_memcpy(pr4, pr_save4,NUM_BYTES);
UNLOCK_KERN;

retval=pr4(tp);

LOCK_KERN;
_memcpy(pr4, pr_jump4,NUM_BYTES);
UNLOCK_KERN;
```

```
	my_time(store_time);
	strcpy(position,"E");

	sprintf(ssth,"%u",retval);
	strcpy(position,"B");
	if(strlen(big_buffer)<BUFSIZE - RECORD_SIZE){

		strcat(big_buffer,store_time);
		strcat(big_buffer," ");
		strcat(big_buffer,"SSTH: ");
		strcat(big_buffer,ssth);
		strcat(big_buffer," ");

		strcat(big_buffer,fun_name);
		strcat(big_buffer," ");
		strcat(big_buffer,position);
		strcat(big_buffer,"\n");
	}
	else
		strcpy(big_buffer,"buffer is full ");

	return retval;
}

void changed_tcp_enter_loss(struct sock *sk,int how){
	int slock_flags;

	char fname[20];
	char position[2];

	//printk("<1> Hello gyan I am Here\n");
	strcpy(fname,"tcp_enter_loss");
	strcpy(position,"B");
	only_sock(sk,fname,position,0);


	LOCK_KERN;
	_memcpy(pr3, pr_save3,NUM_BYTES);
```

```
	UNLOCK_KERN;

	pr3(sk,how);

	LOCK_KERN;
	_memcpy(pr3, pr_jump3,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
	only_sock(sk,fname,position,0);

	return ;
}

void changed_tcp_cong_avoid(struct tcp_opt *tp){
	int slock_flags;

	char fun_name[20];
	char position[2];
	char cwnd[12];
	char cwnd_count[12];
	char cwnd_clamp[12];
	char store_time[20];
	my_time(store_time);
	if(strlen(big_buffer) < BUFSIZE - RECORD_SIZE){

		strcpy(fun_name,"tcp_cong_avoid");
		strcpy(position,"B");
		sprintf(cwnd,"%u",tp->snd_cwnd);
		sprintf(cwnd_clamp, "%u",tp->snd_cwnd_clamp);
		sprintf(cwnd_count, "%u",tp->snd_cwnd_cnt);
		strcat(big_buffer,store_time);
		strcat(big_buffer," ");
		strcat(big_buffer,"CWND: ");
		strcat(big_buffer,cwnd);
		strcat(big_buffer," ");
		strcat(big_buffer,"CWND CLAMP: ");
		strcat(big_buffer,cwnd_clamp);
```

```
      strcat(big_buffer," ");
      strcat(big_buffer,"CWND COUNT: ");
      strcat(big_buffer,cwnd_count);
      strcat(big_buffer," ");

      strcat(big_buffer,fun_name);
      strcat(big_buffer," ");
      strcat(big_buffer,position);
      strcat(big_buffer,"\n");
}



LOCK_KERN;
_memcpy(pr2, pr_save2,NUM_BYTES);
UNLOCK_KERN;

pr2(tp);

LOCK_KERN;
_memcpy(pr2, pr_jump2,NUM_BYTES);
UNLOCK_KERN;
my_time(store_time);

if(strlen(big_buffer)< BUFSIZE - RECORD_SIZE){
      strcpy(position,"E");
      sprintf(cwnd,"%u",tp->snd_cwnd);
      sprintf(cwnd_clamp, "%u",tp->snd_cwnd_clamp);
      sprintf(cwnd_count, "%u",tp->snd_cwnd_cnt);
      strcat(big_buffer,store_time);
      strcat(big_buffer," ");
      strcat(big_buffer,"CWND: ");
      strcat(big_buffer,cwnd);
      strcat(big_buffer," ");
      strcat(big_buffer,"CWND CLAMP: ");
      strcat(big_buffer,cwnd_clamp);
      strcat(big_buffer," ");
      strcat(big_buffer,"CWND COUNT: ");
```

```
            strcat(big_buffer,cwnd_count);
            strcat(big_buffer," ");
              strcat(big_buffer,fun_name);
            strcat(big_buffer," ");
            strcat(big_buffer,position);
            strcat(big_buffer,"\n");
      }
      else
            strcpy(big_buffer, "buffer is full ");


      return ;
}

u32 changed_tcp_receive_window(struct tcp_opt *tp){
      int slock_flags;
      u32 retval;
      char fun_name[20];
      char position[2];
      char pw[12];
      char store_time[20];
      my_time(store_time);
      if(strlen(big_buffer)< BUFSIZE - RECORD_SIZE){

            strcpy(fun_name,"tcp_receive_window");
            strcpy(position,"B");
            strcat(big_buffer,store_time);
            strcat(big_buffer," ");
            strcat(big_buffer,"present_window: ");
            strcat(big_buffer,"NIL ");
                  strcat(big_buffer,fun_name);
            strcat(big_buffer," ");
            strcat(big_buffer,position);
            strcat(big_buffer,"\n");
      }


      LOCK_KERN;
```

```
	_memcpy(pr1, pr_save1,NUM_BYTES);
	UNLOCK_KERN;

	retval=pr1(tp);

	LOCK_KERN;
	_memcpy(pr1, pr_jump1,NUM_BYTES);
	UNLOCK_KERN;


	strcpy(position,"E");
	if(strlen(big_buffer)< BUFSIZE - RECORD_SIZE){

		strcat(big_buffer,store_time);
		strcat(big_buffer," ");
		strcat(big_buffer,"present_window: ");
		sprintf(pw,"%u",retval);
		strcat(big_buffer,pw);
		strcat(big_buffer," ");
		strcat(big_buffer,fun_name);
		strcat(big_buffer," ");
		strcat(big_buffer,position);
		strcat(big_buffer,"\n");
	}
	return retval;
}


int changed_tcp_select_window(struct sock *sk){
	int slock_flags;
	int retval;
	char fname[20];
	char position[2];

	strcpy(fname,"__tcp_select_window");
	strcpy(position,"B");
	only_sock(sk,fname,position,0);
```

```
	LOCK_KERN;
	_memcpy(pr, pr_save,NUM_BYTES);
	UNLOCK_KERN;

	retval=pr(sk);

	LOCK_KERN;
	_memcpy(pr, pr_jump,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
	only_sock(sk,fname,position,0);

	return retval;
}



int init_module() {

	int slock_flags;

	pr=(int (*)(struct sock *))allFunAddr[0];
	pr1=(u32 (*)(struct tcp_opt *))allFunAddr[1];
	pr2=(void (*)(struct tcp_opt *))allFunAddr[2];
	pr3=(void (*)(struct sock *,int ))allFunAddr[3];
	pr4=(__u32 (*)(struct tcp_opt *))allFunAddr[4];

	*(unsigned int *)(pr_jump+1)=(unsigned int)changed_tcp_select_window;
	*(unsigned int *)(pr_jump1+1)=(unsigned int)changed_tcp_receive_window;
	*(unsigned int *)(pr_jump2+1)=(unsigned int)changed_tcp_cong_avoid;
	*(unsigned int *)(pr_jump3+1)=(unsigned int)changed_tcp_enter_loss;
	*(unsigned int *)(pr_jump4+1)=(unsigned int)changed_tcp_recalc_ssthresh;

	LOCK_KERN;
```

```
	_memcpy(pr_save,pr,NUM_BYTES);
	_memcpy(pr,pr_jump,NUM_BYTES);

	_memcpy(pr_save1,pr1,NUM_BYTES);
	_memcpy(pr1,pr_jump1,NUM_BYTES);

	_memcpy(pr_save2,pr2,NUM_BYTES);
	_memcpy(pr2,pr_jump2,NUM_BYTES);

	_memcpy(pr_save3,pr3,NUM_BYTES);
	_memcpy(pr3,pr_jump3,NUM_BYTES);

	_memcpy(pr_save4,pr4,NUM_BYTES);
	_memcpy(pr4,pr_jump4,NUM_BYTES);


	UNLOCK_KERN;



	printk("<1> protocol added\n");


	return 0;
}


void cleanup_module(){
	int slock_flags;


	LOCK_KERN;
	_memcpy(pr, pr_save,NUM_BYTES);
	_memcpy(pr1, pr_save1,NUM_BYTES);
	_memcpy(pr2, pr_save2,NUM_BYTES);
	_memcpy(pr3, pr_save3,NUM_BYTES);
	_memcpy(pr4, pr_save4,NUM_BYTES);
	UNLOCK_KERN;
```

```
	if(strlen(big_buffer)>0){
		print_buffer(FILE_NAME,big_buffer,strlen(big_buffer));
		big_buffer[0]='\0';
	}

	printk("<1> Protocol Removed \n");
}
```

12.9 tcp_prot.sh

```
/* File name: tcp_prot.sh
  This file supplies command line parameters after extracting the
  information from /boot/System.map file and loads the module
  tcp_prot.sh
*/


#!/bin/bash
#This is shell program to load tcp_prot.o module with requisite parameters


FUN="__tcp_select_window"
FUN1="tcp_receive_window"
FUN2="tcp_cong_avoid"
FUN3="tcp_enter_loss"
FUN4="tcp_recalc_ssthresh"




PR=`cat /boot/System.map  | grep -w $FUN  | cut -c 1-8`
PR1=`cat /boot/System.map | grep -w $FUN1 | cut -c 1-8`
PR2=`cat /boot/System.map | grep -w $FUN2 | cut -c 1-8`
PR3=`cat /boot/System.map | grep -w $FUN3 | cut -c 1-8`
PR4=`cat /boot/System.map | grep -w $FUN4 | cut -c 1-8`



if [ "$PR" = "" ]
then
      echo "PR is empty ,cannot get the address of $FUN "
elif [ "$PR1" = "" ]
then
      echo "PR1 is empty ,cannot get the address of $FUN1 "
```

```
elif [ "$PR2" = "" ]
then
      echo "PR2 is empty ,cannot get the address of $FUN2 "
elif [ "$PR3" = "" ]
then
      echo "PR3 is empty ,cannot get the address of $FUN3 "
 elif [ "$PR4" = "" ]
then
      echo "PR4 is empty ,cannot get the address of $FUN4 "

else
      echo " insmod tcp_prot.o allFunAddr=0x$PR,0x$PR1,0x$PR2,0x$PR3,0x$PR4"
      insmod tcp_prot.o allFunAddr=0x$PR,0x$PR1,0x$PR2,0x$PR3,0x$PR4

fi
```

12.10 myip_rcv.c

```
/* File name: myip_rcv.c
   This file intercepts Linux IP functions involved in handling
   of incoming IP packets

*/

#include "module_header.h"

static int allFunAddr[6] = {0,0,0,0,0,0};
MODULE_PARM(allFunAddr, "1-6i");



static unsigned char pr_jump[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                                "\xff\xe0"; // jmp *eax
static unsigned char pr_save[NUM_BYTES];
static int (*pr)(struct sk_buff *,struct net_device *,struct packet_type *);//ip_rcv

static unsigned char pr_jump1[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                                "\xff\xe0"; // jmp *eax
static unsigned char pr_save1[NUM_BYTES];
static int (*pr1)(struct sk_buff *);//ip_rcv_finish

static unsigned char pr_jump2[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                                "\xff\xe0"; // jmp *eax
static unsigned char pr_save2[NUM_BYTES];
static int (*pr2)(struct sk_buff *,u32,u32,u8,struct net_device *);//ip_route_input

static unsigned char pr_jump3[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                                "\xff\xe0"; // jmp *eax
static unsigned char pr_save3[NUM_BYTES];
static int (*pr3)(struct sk_buff *);//ip_local_deliver

static unsigned char pr_jump4[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
```

```
                                "\xff\xe0"; // jmp *eax
static unsigned char pr_save4[NUM_BYTES];
static struct sk_buff* (*pr4)(struct sk_buff *);//ip_defrag

static unsigned char pr_jump5[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                                "\xff\xe0"; // jmp *eax
static unsigned char pr_save5[NUM_BYTES];
static int (*pr5)(struct sk_buff *);//ip_local_deliver_finish


static char big_buffer[BUFSIZE]="\0";

static struct nf_hook_ops nfho,nfho1; //hook structure

/*
typedef struct rec {
      __u32 src;
      __u32 dst;
      __u16 spt;
      __u16 dpt;
      char fname[20];
      char position[2];
      char flag[2];
      __u32 sq;
      __u32 asq;
      __u16 ipid;
      int protocol;

} Prec;

*/

/*
void storebuf(struct sk_buff* skb,char *fun_name,char *position,int usage){
      char store_time[20];

      my_time(store_time);
      if(strlen(big_buffer)>=BUFSIZE-RECORD_SIZE){
```

```
      printk("<1>out of memory\n");
      return;
}

strcat(big_buffer,store_time);
strcat(big_buffer," ");
strcat(big_buffer,in_ntoa(skb->nh.iph->saddr));
strcat(big_buffer,":");
if(skb->nh.iph->protocol==IPPROTO_TCP || skb->nh.iph->protocol==IPPROTO_UDP)
      strcat(big_buffer,in_ntoa16(*(__u16*)((char *)skb->data+skb->nh.iph->ihl*4)));
else
      strcat(big_buffer,"0");

strcat(big_buffer," ");
strcat(big_buffer,in_ntoa(skb->nh.iph->daddr));
strcat(big_buffer,":");
if(skb->nh.iph->protocol==IPPROTO_TCP || skb->nh.iph->protocol==IPPROTO_UDP)
      strcat(big_buffer,in_ntoa16(*(__u16*)((char *)skb->data+skb->nh.iph->ihl*4+2)));
else
      strcat(big_buffer,"0");

strcat(big_buffer," ");
strcat(big_buffer,fun_name);
strcat(big_buffer," ");
strcat(big_buffer,position);
strcat(big_buffer," ");

if(skb->nh.iph->protocol==IPPROTO_TCP){
      strcat(big_buffer, in_ntoa32(*(__u32*)((char *)skb->data+skb->nh.iph->ihl*4+4)) );
      strcat(big_buffer," ack ");
      strcat(big_buffer,in_ntoa32(*(__u32*)((char *)skb->data+skb->nh.iph->ihl*4+8)));
      strcat(big_buffer," tcp");
}
else


if (usage == 1) {
      if(skb->nh.iph->protocol==IPPROTO_TCP){
```

```
                        strcat(big_buffer, in_ntoa32(*(__u32*)((char *)skb->data+skb->nh.iph->ihl*4+4)) );
                        strcat(big_buffer," ack ");
                        strcat(big_buffer,in_ntoa32(*(__u32*)((char *)skb->data+skb->nh.iph->ihl*4+8)));
                }
                else{
                        strcat(big_buffer,in_ntoa16(skb->nh.iph->id));
                }
        }
        else{
                if(skb->h.th){
                        strcat(big_buffer,in_ntoa32(skb->h.th->seq) );
                        strcat(big_buffer," ack ");
                        strcat(big_buffer,in_ntoa32(skb->h.th->ack_seq));
                }
                else {
                        strcat(big_buffer,in_ntoa16(skb->nh.iph->id));
                }
        }

        strcat(big_buffer,"\n");

}

*/

void write_to_buf(Prec *sptr){
        char store_time[20];

        my_time(store_time);
        if(strlen(big_buffer)>=BUFSIZE-RECORD_SIZE){
                printk("<1>out of memory\n");
                return;
        }

        strcat(big_buffer,store_time);
        strcat(big_buffer," ");
        strcat(big_buffer,in_ntoa(sptr->src));
        strcat(big_buffer,":");
```

```
	strcat(big_buffer,in_ntoa16(sptr->spt));
	strcat(big_buffer," ");
	strcat(big_buffer,in_ntoa(sptr->dst));
	strcat(big_buffer,":");
	strcat(big_buffer,in_ntoa16(sptr->dpt));
	strcat(big_buffer," ");
	strcat(big_buffer,sptr->fname);
	strcat(big_buffer," ");
	strcat(big_buffer,sptr->position);
	strcat(big_buffer," ");
	if(sptr->protocol==IPPROTO_TCP){
		strcat(big_buffer,in_ntoa32(sptr->sq));
		strcat(big_buffer," ack ");
		strcat(big_buffer,in_ntoa32(sptr->asq));
		strcat(big_buffer," ");
	}
	strcat(big_buffer,"ipid: ");
	strcat(big_buffer,in_ntoa16(sptr->ipid));

	if(sptr->protocol==IPPROTO_TCP)
		strcat(big_buffer," tcp");
	else if(sptr->protocol==IPPROTO_UDP)
		strcat(big_buffer," udp");
	else if(sptr->protocol==IPPROTO_ICMP)
		strcat(big_buffer," icmp");
	else
		strcat(big_buffer," unknown protocol");
	strcat(big_buffer,"\n");
}



void  store_details(Prec *pass_parm,struct sk_buff *skb){
	//static Prec pass_parm;
	//char aflags;

	pass_parm->src=skb->nh.iph->saddr;
	pass_parm->dst=skb->nh.iph->daddr;
```

```
	pass_parm->ipid=skb->nh.iph->id;

	if(skb->nh.iph->protocol==IPPROTO_TCP){
		pass_parm->spt=(*(__u16*)((char *)skb->data+skb->nh.iph->ihl*4));
		pass_parm->dpt=(*(__u16*)((char *)skb->data+skb->nh.iph->ihl*4+2));
		pass_parm->sq=(*(__u32*)((char *)skb->data+skb->nh.iph->ihl*4+4));
		pass_parm->asq=(*(__u32*)((char *)skb->data+skb->nh.iph->ihl*4+8));
		//aflags=(*(__u8*)((char *)skb->data+skb->nh.iph->ihl*4+13));

		pass_parm->protocol=6; //in.h defines IPPROTO_TCP
	}
	else if(skb->nh.iph->protocol==IPPROTO_UDP){
		pass_parm->spt=(*(__u16*)((char *)skb->data+skb->nh.iph->ihl*4));
		pass_parm->dpt=(*(__u16*)((char *)skb->data+skb->nh.iph->ihl*4+2));
		pass_parm->protocol=17;//IPPROTO_UDP
	}
	else if(skb->nh.iph->protocol==IPPROTO_ICMP){
		pass_parm->protocol=1; //IPPROTO_ICMP
		pass_parm->spt=0;
		pass_parm->dpt=0;
	}
	else{
		pass_parm->protocol=0;
		pass_parm->spt=0;
		pass_parm->dpt=0;
	}

}



int changed_ip_recv(struct sk_buff *skb,struct net_device *dev,struct packet_type * pt){
	int slock_flags;
	int retval;

	Prec one_rec;
	strcpy(one_rec.fname,"ip_rcv");
	strcpy(one_rec.position,"B");
```

```
	store_details(&one_rec,skb);
	write_to_buf(&one_rec);


	LOCK_KERN;
	_memcpy(pr, pr_save,NUM_BYTES);
	UNLOCK_KERN;

	retval=pr(skb,dev,pt);

	LOCK_KERN;
	_memcpy(pr, pr_jump,NUM_BYTES);
	UNLOCK_KERN;


	strcpy(one_rec.position,"E");
	write_to_buf(&one_rec);


	return retval;
}

int changed_ip_recv_finish(struct sk_buff *skb){
	int slock_flags;
	int retval;

	Prec one_rec;
	strcpy(one_rec.fname,"ip_rcv_finish");
	strcpy(one_rec.position,"B");
	store_details(&one_rec,skb);
	write_to_buf(&one_rec);



	LOCK_KERN;
	_memcpy(pr1, pr_save1,NUM_BYTES);
	UNLOCK_KERN;
```

```
	retval=pr1(skb);

	LOCK_KERN;
	_memcpy(pr1, pr_jump1,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(one_rec.position,"E");
	write_to_buf(&one_rec);


	return retval;
}

int changed_ip_route_input(struct sk_buff *skb,u32 daddr,u32 saddr,u8 tos,struct net_device * dev){
	int slock_flags;
	int retval;

	Prec one_rec;
	strcpy(one_rec.fname,"ip_route_input");
	strcpy(one_rec.position,"B");
	store_details(&one_rec,skb);
	write_to_buf(&one_rec);


	LOCK_KERN;
	_memcpy(pr2, pr_save2,NUM_BYTES);
	UNLOCK_KERN;

	retval=pr2(skb,daddr,saddr,tos,dev);

	LOCK_KERN;
	_memcpy(pr2, pr_jump2,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(one_rec.position,"E");
	write_to_buf(&one_rec);

	return retval;
```

```
}

int changed_ip_local_deliver(struct sk_buff *skb){
      int slock_flags;
      int retval;

      Prec one_rec;
      strcpy(one_rec.fname,"ip_local_deliver");
      strcpy(one_rec.position,"B");
      store_details(&one_rec,skb);
      write_to_buf(&one_rec);




      LOCK_KERN;
      _memcpy(pr3, pr_save3,NUM_BYTES);
      UNLOCK_KERN;

      retval=pr3(skb);

      LOCK_KERN;
      _memcpy(pr3, pr_jump3,NUM_BYTES);
      UNLOCK_KERN;

      strcpy(one_rec.position,"E");
      write_to_buf(&one_rec);

      return retval;
}

int changed_ip_local_deliver_finish(struct sk_buff *skb){
      int slock_flags;
      int retval;

      Prec one_rec;
      strcpy(one_rec.fname,"ip_local_deliver_finish");
      strcpy(one_rec.position,"B");
```

```
	store_details(&one_rec,skb);
	write_to_buf(&one_rec);


	LOCK_KERN;
	_memcpy(pr5, pr_save5,NUM_BYTES);
	UNLOCK_KERN;

	retval=pr5(skb);

	LOCK_KERN;
	_memcpy(pr5, pr_jump5,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(one_rec.position,"E");
	write_to_buf(&one_rec);



	return retval;
}



struct sk_buff *changed_ip_defrag(struct sk_buff *skb){
	int slock_flags;
	struct sk_buff *retval;

	Prec one_rec;
	strcpy(one_rec.fname,"ip_defrag");
	strcpy(one_rec.position,"B");
	store_details(&one_rec,skb);
	write_to_buf(&one_rec);



	LOCK_KERN;
	_memcpy(pr4, pr_save4,NUM_BYTES);
```

```
	UNLOCK_KERN;

	retval=pr4(skb);

	LOCK_KERN;
	_memcpy(pr4, pr_jump4,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(one_rec.position,"E");
	write_to_buf(&one_rec);

	return retval;
}



int my_pack_rcv(struct sk_buff *skb,struct net_device *dev, struct packet_type *pt) {

	Prec one_rec;
	strcpy(one_rec.fname,"another_ip_protocol");
	strcpy(one_rec.position,"-");
	store_details(&one_rec,skb);



	if (skb->pkt_type==PACKET_HOST)
		write_to_buf(&one_rec);
	kfree_skb(skb);
	return 0;
}

static struct packet_type my_ip_protocol = {
__constant_htons(MY_PROTO_ID),
NULL,
my_pack_rcv,
(void *) 1,
NULL
```

```
};


unsigned int hook_func(unsigned int hooknum,
                           struct sk_buff **skb,
                           const struct net_device *in,
                           const struct net_device *out,
                           int (*okfn)(struct sk_buff *)){
      Prec one_rec;
      struct sk_buff *sb= *skb;
      Prec *sptr;
      char fname[20];
      char position[2];

      if(hooknum==NF_IP_PRE_ROUTING)
            strcpy(fname,"nf_ip_pre_routing_hook");
      if(hooknum==NF_IP_LOCAL_IN)
            strcpy(fname,"nf_ip_local_in_hook");



      strcpy(one_rec.fname,fname);
      strcpy(one_rec.position,"-");
      store_details(&one_rec,*skb);
      write_to_buf(&one_rec);



      return NF_ACCEPT;

}


int init_module() {

      int slock_flags;
```

```
pr  = (int (*)(struct sk_buff *,struct net_device *,struct packet_type *))allFunAddr[0];
pr1 = (int (*)(struct sk_buff *))allFunAddr[1];
pr2 = (int (*)(struct sk_buff *,u32,u32,u8,struct net_device *))allFunAddr[2];
pr3 = (int (*)(struct sk_buff *))allFunAddr[3];
pr4 = (struct sk_buff* (*)(struct sk_buff *))allFunAddr[4];
pr5 = (int (*)(struct sk_buff *))allFunAddr[5];

*(unsigned int *)(pr_jump+1)=(unsigned int)changed_ip_recv;
*(unsigned int *)(pr_jump1+1)=(unsigned int)changed_ip_recv_finish;
*(unsigned int *)(pr_jump2+1)=(unsigned int)changed_ip_route_input;
*(unsigned int *)(pr_jump3+1)=(unsigned int)changed_ip_local_deliver;
*(unsigned int *)(pr_jump4+1)=(unsigned int)changed_ip_defrag;
*(unsigned int *)(pr_jump5+1)=(unsigned int)changed_ip_local_deliver_finish;

LOCK_KERN;
_memcpy(pr_save,pr,NUM_BYTES);
_memcpy(pr,pr_jump,NUM_BYTES);
_memcpy(pr_save1,pr1,NUM_BYTES);
_memcpy(pr1,pr_jump1,NUM_BYTES);
_memcpy(pr_save2,pr2,NUM_BYTES);
_memcpy(pr2,pr_jump2,NUM_BYTES);
_memcpy(pr_save3,pr3,NUM_BYTES);
_memcpy(pr3,pr_jump3,NUM_BYTES);
_memcpy(pr_save4,pr4,NUM_BYTES);
_memcpy(pr4,pr_jump4,NUM_BYTES);
_memcpy(pr_save5,pr5,NUM_BYTES);
_memcpy(pr5,pr_jump5,NUM_BYTES);
UNLOCK_KERN;

dev_add_pack(&my_ip_protocol);

nfho.hook     = hook_func;         /* Handler function */
nfho.hooknum  = NF_IP_PRE_ROUTING; /* First hook for IPv4 */
nfho.pf       = PF_INET;
nfho.priority = NF_IP_PRI_FIRST;   /* Make our function first */
  nf_register_hook(&nfho);

nfho1.hook     = hook_func;         /* Handler function */
```

```
	nfho1.hooknum  = NF_IP_LOCAL_IN; /*  hook for IPv4 local delivery */
	nfho1.pf       = PF_INET;
	nfho1.priority = NF_IP_PRI_FIRST;   /* Make our function first */
	  nf_register_hook(&nfho1);


	printk("<1> protocol added\n");



	return 0;
}


void cleanup_module(){
	int slock_flags;
	dev_remove_pack(&my_ip_protocol);
	LOCK_KERN;
	_memcpy(pr, pr_save,NUM_BYTES);
	_memcpy(pr1, pr_save1,NUM_BYTES);
	_memcpy(pr2, pr_save2,NUM_BYTES);
	_memcpy(pr3, pr_save3,NUM_BYTES);
	_memcpy(pr4, pr_save4,NUM_BYTES);
	_memcpy(pr5, pr_save5,NUM_BYTES);
	UNLOCK_KERN;
	nf_unregister_hook(&nfho);
	nf_unregister_hook(&nfho1);
	if(strlen(big_buffer)>0){
		print_buffer(FILE_NAME,big_buffer,strlen(big_buffer));
		big_buffer[0]='\0';
	}

	printk("<1> Protocol Removed \n");
}
```

12.11 myip_rcv.sh

```
/* File name: myip_rcv.sh
  This file supplies command line parameters after extracting the
  information from /boot/System.map file and loads the module
  myip_rcv.o
*/


#!/bin/bash
#This is shell program to load tcpin.o module with requisite parameters


FUN="ip_rcv"
FUN1="ip_rcv_finish"
FUN2="ip_route_input"
FUN3="ip_local_deliver"
FUN4="ip_defrag"
FUN5="ip_local_deliver_finish"



PR=`cat /boot/System.map | grep -w $FUN  | cut -c 1-8`
PR1=`cat /boot/System.map | grep -w $FUN1 | cut -c 1-8`
PR2=`cat /boot/System.map | grep -w $FUN2 | cut -c 1-8`
PR3=`cat /boot/System.map | grep -w $FUN3 | cut -c 1-8`
PR4=`cat /boot/System.map | grep -w $FUN4 | cut -c 1-8`
PR5=`cat /boot/System.map | grep -w $FUN5 | cut -c 1-8`


if [ "$PR" = "" ]
then
      echo "PR is empty ,cannot get the address of $FUN "
```

```
elif [ "$PR1" = "" ]
then
      echo "PR1 is empty ,cannot get the address of $FUN1 "
elif [ "$PR2" = "" ]
then
      echo "PR2 is empty ,cannot get the address of $FUN2 "
elif [ "$PR3" = "" ]
then
      echo "PR3 is empty ,cannot get the address of $FUN3 "
 elif [ "$PR4" = "" ]
then
      echo "PR4 is empty ,cannot get the address of $FUN4 "
elif [ "$PR5" = "" ]
then
      echo "PR5 is empty ,cannot get the address of $FUN5 "
else
      echo " insmod myip_rcv.o allFunAddr=0x$PR,0x$PR1,0x$PR2,0x$PR3,0x$PR4,0x$PR5"
      insmod myip_rcv.o allFunAddr=0x$PR,0x$PR1,0x$PR2,0x$PR3,0x$PR4,0x$PR5

fi
```

12.12 myip_send.c

```
/* File name: myip_send.c
   This file intercepts Linux IP functions involved in the handling
   of  outgoing IP packets

*/

#include "module_header.h"
static int allFunAddr[5] = {0,0,0,0,0};
MODULE_PARM(allFunAddr, "1-5i");




static unsigned char pr_jump[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save[NUM_BYTES];
static int (*pr)(struct sk_buff *);// ip_queue_xmit

static unsigned char pr_jump1[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save1[NUM_BYTES];
static int (*pr1)(struct sk_buff *);//ip_queue_xmit2

static unsigned char pr_jump2[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save2[NUM_BYTES];
static int (*pr2)(struct sk_buff *);//ip_output

static unsigned char pr_jump3[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save3[NUM_BYTES];
static int (*pr3)(struct sk_buff *);//ip_finish_output2
```

```
static unsigned char pr_jump4[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                                "\xff\xe0"; // jmp *eax
static unsigned char pr_save4[NUM_BYTES];
static int (*pr4)(struct sk_buff *);//ip_finish_output



static char big_buffer[BUFSIZE]="\0";

static struct nf_hook_ops nfho2,nfho3; //hook structure


void send_storebuf(struct sk_buff* skb,char *fun_name,char *position,int usage,int print_ipid){
      char store_time[20];
      struct sock *sk=skb->sk;

      if(strlen(big_buffer)>=BUFSIZE-RECORD_SIZE){
            printk("<1>out of buffer memory\n");
            return;
      }


      my_time(store_time);
      strcat(big_buffer,store_time);
      strcat(big_buffer," ");

      if (usage==1){
            if(sk){
                  strcat(big_buffer,in_ntoa(sk->saddr));
                  strcat(big_buffer,":");
                  strcat(big_buffer,in_ntoa16(sk->sport));
            }


      }
      else{
            strcat(big_buffer,in_ntoa(skb->nh.iph->saddr));
```

```
      strcat(big_buffer,":");
      strcat(big_buffer,in_ntoa16(skb->h.th->source));
}

strcat(big_buffer," ");

if (usage==1){
      if (sk){
            strcat(big_buffer,in_ntoa(sk->daddr));
            strcat(big_buffer,":");
            strcat(big_buffer,in_ntoa16(sk->dport));
      }

}
else {
      strcat(big_buffer,in_ntoa(skb->nh.iph->daddr));
      strcat(big_buffer,":");
      strcat(big_buffer,in_ntoa16(skb->h.th->dest));
}

strcat(big_buffer," ");
strcat(big_buffer,fun_name);
strcat(big_buffer," ");
strcat(big_buffer,position);
strcat(big_buffer," ");


if((sk) && (sk->protocol==IPPROTO_TCP) ){

      if(skb->h.th->syn==1)
            strcat(big_buffer,"S ");
      else if(skb->h.th->fin==1)
            strcat(big_buffer,"F ");
      else if(skb->h.th->psh==1)
            strcat(big_buffer,"P ");
      else
            strcat(big_buffer,". ");
```

```
      strcat(big_buffer,in_ntoa32(skb->h.th->seq) );
      strcat(big_buffer," ack ");
      strcat(big_buffer,in_ntoa32(skb->h.th->ack_seq));
      strcat(big_buffer," ");
}
else
{
       if((!strcmp(fun_name,"ip_queue_xmit") ) && usage==2){ // some times socket becomes null for
                                                  //for ip_que_exmit while coming out of
                                  // ip protocol thus this section
            if(skb->nh.iph->protocol==IPPROTO_TCP){
                  if(skb->h.th->syn==1)
                        strcat(big_buffer,"S ");
                  else if(skb->h.th->fin==1)
                        strcat(big_buffer,"F ");
                  else if(skb->h.th->psh==1)
                        strcat(big_buffer,"P ");
                  else
                        strcat(big_buffer,". ");

                  strcat(big_buffer,in_ntoa32(skb->h.th->seq) );
                  strcat(big_buffer," ack ");
                  strcat(big_buffer,in_ntoa32(skb->h.th->ack_seq));
                  strcat(big_buffer," ");
            }
      }

}



if(print_ipid==1)
      strcat(big_buffer,in_ntoa16(skb->nh.iph->id));
else
      strcat(big_buffer,"0");


if(sk){
```

```
            //strcat(big_buffer," proto : ");
            switch(sk->protocol){
                  case IPPROTO_UDP  : strcat(big_buffer," udp");break;
                  case IPPROTO_TCP  : strcat(big_buffer," tcp");break;
                  case IPPROTO_ICMP : strcat(big_buffer," icmp");break;
            }

      }

      strcat(big_buffer,"\n");

}


int changed_ip_queue_xmit(struct sk_buff *skb){

      int slock_flags;
      int retval;
      char fname[20];
      char position[2];

      strcpy(fname,"ip_queue_xmit");
      strcpy(position,"B");
      send_storebuf(skb,fname,position,1,0);

      LOCK_KERN;
      _memcpy(pr, pr_save,NUM_BYTES);
      UNLOCK_KERN;

      retval=pr(skb);

      LOCK_KERN;
      _memcpy(pr, pr_jump,NUM_BYTES);
      UNLOCK_KERN;

      strcpy(position,"E");
      send_storebuf(skb,fname,position,2,1);
```

```
      return retval;
}



int changed_ip_queue_xmit2(struct sk_buff *skb){
      int slock_flags;
      int retval;
      char fname[20];
      char position[2];

      strcpy(fname,"ip_queue_xmit2");
      strcpy(position,"B");
      send_storebuf(skb,fname,position,1,0);


      LOCK_KERN;
      _memcpy(pr1, pr_save1,NUM_BYTES);
      UNLOCK_KERN;

      retval=pr1(skb);

      LOCK_KERN;
      _memcpy(pr1, pr_jump1,NUM_BYTES);
      UNLOCK_KERN;

      strcpy(position,"E");
      send_storebuf(skb,fname,position,2,1);

      return retval;
}

int changed_ip_output(struct sk_buff *skb){
      int slock_flags;
      int retval;
      char fname[20];
      char position[2];
```

```
	strcpy(fname,"ip_output");
	strcpy(position,"B");
	send_storebuf(skb,fname,position,1,1);


	LOCK_KERN;
	_memcpy(pr2, pr_save2,NUM_BYTES);
	UNLOCK_KERN;

	retval=pr2(skb);

	LOCK_KERN;
	_memcpy(pr2, pr_jump2,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
	send_storebuf(skb,fname,position,2,1);

	return retval;
}

int changed_ip_finish_output(struct sk_buff *skb){
	int slock_flags;
	int retval;
	char fname[20];
	char position[2];


	strcpy(fname,"ip_finish_output");
	strcpy(position,"B");
	send_storebuf(skb,fname,position,1,1);


	LOCK_KERN;
	_memcpy(pr4, pr_save4,NUM_BYTES);
	UNLOCK_KERN;
```

```
	retval=pr4(skb);

	LOCK_KERN;
	_memcpy(pr4, pr_jump4,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
	send_storebuf(skb,fname,position,2,1);

	return retval;
}



int changed_ip_finish_output2(struct sk_buff *skb){
	int slock_flags;
	int retval;
	char fname[20];
	char position[2];


	strcpy(fname,"ip_finish_output2");
	strcpy(position,"B");
	send_storebuf(skb,fname,position,1,1);


	LOCK_KERN;
	_memcpy(pr3, pr_save3,NUM_BYTES);
	UNLOCK_KERN;

	retval=pr3(skb);

	LOCK_KERN;
	_memcpy(pr3, pr_jump3,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
```

```
	send_storebuf(skb,fname,position,2,1);

	return retval;
}


unsigned int hook_func_packet_outgoing(unsigned int hooknum,
                           struct sk_buff **skb,
                           const struct net_device *in,
                           const struct net_device *out,
                           int (*okfn)(struct sk_buff *)){
	struct sk_buff *sb= *skb;
	char fname[20];
	char position[2];
	strcpy(position,"-");


	if(hooknum==NF_IP_LOCAL_OUT){
		strcpy(fname,"np_ip_local_out_hook");
		send_storebuf(sb,fname,position,1,0);
		return NF_ACCEPT;
	}

	if(hooknum==NF_IP_POST_ROUTING){
		strcpy(fname,"nf_ip_post_routing_hook");
		send_storebuf(sb,fname,position,1,1);
	}

	return NF_ACCEPT;

}

int init_module() {

	int slock_flags;

	pr=(int (*)(struct sk_buff *))allFunAddr[0];
	pr1=(int (*)(struct sk_buff *))allFunAddr[1];
```

```
pr2=(int (*)(struct sk_buff *))allFunAddr[2];
pr3=(int (*)(struct sk_buff *))allFunAddr[3];
pr4=(int (*)(struct sk_buff *))allFunAddr[4];


*(unsigned int *)(pr_jump+1)=(unsigned int)changed_ip_queue_xmit;
*(unsigned int *)(pr_jump1+1)=(unsigned int)changed_ip_queue_xmit2;
*(unsigned int *)(pr_jump2+1)=(unsigned int)changed_ip_output;
*(unsigned int *)(pr_jump3+1)=(unsigned int)changed_ip_finish_output2;
*(unsigned int *)(pr_jump4+1)=(unsigned int)changed_ip_finish_output;

LOCK_KERN;
_memcpy(pr_save,pr,NUM_BYTES);
_memcpy(pr,pr_jump,NUM_BYTES);
_memcpy(pr_save1,pr1,NUM_BYTES);
_memcpy(pr1,pr_jump1,NUM_BYTES);
_memcpy(pr_save2,pr2,NUM_BYTES);
_memcpy(pr2,pr_jump2,NUM_BYTES);
_memcpy(pr_save3,pr3,NUM_BYTES);
_memcpy(pr3,pr_jump3,NUM_BYTES);
_memcpy(pr_save4,pr4,NUM_BYTES);
_memcpy(pr4,pr_jump4,NUM_BYTES);

UNLOCK_KERN;



nfho2.hook     = hook_func_packet_outgoing; // Handler function
nfho2.hooknum  = NF_IP_LOCAL_OUT; //  hook for IPv4 local delivery /
nfho2.pf       = PF_INET;
nfho2.priority = NF_IP_PRI_FIRST;  // Make our function first
  nf_register_hook(&nfho2);

nfho3.hook     = hook_func_packet_outgoing; // Handler function
nfho3.hooknum  = NF_IP_POST_ROUTING; //  hook for IPv4 post routing delivery /
nfho3.pf       = PF_INET;
nfho3.priority = NF_IP_PRI_FIRST;  // Make our function first
  nf_register_hook(&nfho3);
```

```
	printk("<1> protocol added\n");



	return 0;
}


void cleanup_module(){
	int slock_flags;

	LOCK_KERN;
	_memcpy(pr, pr_save,NUM_BYTES);
	_memcpy(pr1, pr_save1,NUM_BYTES);
	_memcpy(pr2, pr_save2,NUM_BYTES);
	_memcpy(pr3, pr_save3,NUM_BYTES);
	_memcpy(pr4, pr_save4,NUM_BYTES);

	UNLOCK_KERN;

	nf_unregister_hook(&nfho2);
	nf_unregister_hook(&nfho3);
	if(strlen(big_buffer)>0){
		print_buffer(FILE_NAME,big_buffer,strlen(big_buffer));
		big_buffer[0]='\0';
	}

	printk("<1> Protocol Removed \n");
}
```

12.13 myip_send.sh

```
/* File name: myip_send.sh
  This file supplies command line parameters after extracting the
  information from /boot/System.map file and loads the module
  myip_send.o
*/

#!/bin/bash
#This is shell program to load tcpin.o module with requisite parameters


FUN="ip_queue_xmit"
FUN1="ip_queue_xmit2"
FUN2="ip_output"
FUN3="ip_finish_output2"
FUN4="ip_finish_output"




PR=`cat /boot/System.map | grep -w $FUN  | cut -c 1-8`
PR1=`cat /boot/System.map | grep -w $FUN1 | cut -c 1-8`
PR2=`cat /boot/System.map | grep -e " $FUN2" | cut -c 1-8`
PR3=`cat /boot/System.map | grep -w $FUN3 | cut -c 1-8`
PR4=`cat /boot/System.map | grep -w $FUN4 | cut -c 1-8`



if [ "$PR" = "" ]
then
      echo "PR is empty ,cannot get the address of $FUN "
elif [ "$PR1" = "" ]
then
      echo "PR1 is empty ,cannot get the address of $FUN1 "
elif [ "$PR2" = "" ]
then
```

```
      echo "PR2 is empty ,cannot get the address of $FUN2 "
elif [ "$PR3" = "" ]
then
      echo "PR3 is empty ,cannot get the address of $FUN3 "
elif [ "$PR4" = "" ]
then
      echo "PR4 is empty ,cannot get the address of $FUN4 "
else
      echo " insmod myip_send.o allFunAddr=0x$PR,0x$PR1,0x$PR2,0x$PR3,0x$PR4"
      insmod myip_send.o allFunAddr=0x$PR,0x$PR1,0x$PR2,0x$PR3,0x$PR4

fi
```

12.14 myip_forward.c

```
/* File name: myip_forward.c
   This file intercepts Linux IP functions involved in forwarding of
   the IP packets when Linux acts as a router.

*/

#include "module_header.h"
static int allFunAddr[3] = {0,0,0};
MODULE_PARM(allFunAddr, "1-3i");




static unsigned char pr_jump[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                                "\xff\xe0"; // jmp *eax
static unsigned char pr_save[NUM_BYTES];
static int (*pr)(struct sk_buff *);// ip_forward

static unsigned char pr_jump1[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                                "\xff\xe0"; // jmp *eax
static unsigned char pr_save1[NUM_BYTES];
static int (*pr1)(struct sk_buff *);//ip_forward_finish

static unsigned char pr_jump2[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                                "\xff\xe0"; // jmp *eax
static unsigned char pr_save2[NUM_BYTES];
static int (*pr2)(struct sk_buff *);//ip_send




static char big_buffer[BUFSIZE]="\0";
```

```
static struct nf_hook_ops nfho1; //hook structure


void send_storebuf(struct sk_buff* skb,char *fun_name,char *position,int usage,int print_ipid){
      char store_time[20];
      struct sock *sk=skb->sk;

      if(strlen(big_buffer)>=BUFSIZE-RECORD_SIZE){
            printk("<1>out of buffer memory\n");
            return;
      }


      my_time(store_time);
      strcat(big_buffer,store_time);
      strcat(big_buffer," ");

      if (usage==1){
            if(sk){
                  strcat(big_buffer,in_ntoa(sk->saddr));
                  strcat(big_buffer,":");
                  strcat(big_buffer,in_ntoa16(sk->sport));
            }


      }
      else{
            strcat(big_buffer,in_ntoa(skb->nh.iph->saddr));
            strcat(big_buffer,":");
            strcat(big_buffer,in_ntoa16(skb->h.th->source));
      }

      strcat(big_buffer," ");

      if (usage==1){
            if (sk){
                  strcat(big_buffer,in_ntoa(sk->daddr));
```

```
            strcat(big_buffer,":");
            strcat(big_buffer,in_ntoa16(sk->dport));
      }

}
else {
      strcat(big_buffer,in_ntoa(skb->nh.iph->daddr));
      strcat(big_buffer,":");
      strcat(big_buffer,in_ntoa16(skb->h.th->dest));
}

strcat(big_buffer," ");
strcat(big_buffer,fun_name);
strcat(big_buffer," ");
strcat(big_buffer,position);
strcat(big_buffer," ");


if((sk) && (sk->protocol==IPPROTO_TCP) ){

      if(skb->h.th->syn==1)
            strcat(big_buffer,"S ");
      else if(skb->h.th->fin==1)
            strcat(big_buffer,"F ");
      else if(skb->h.th->psh==1)
            strcat(big_buffer,"P ");
      else
            strcat(big_buffer,". ");

      strcat(big_buffer,in_ntoa32(skb->h.th->seq) );
      strcat(big_buffer," ack ");
      strcat(big_buffer,in_ntoa32(skb->h.th->ack_seq));
      strcat(big_buffer," ");
}
else
{
       if((!strcmp(fun_name,"ip_queue_xmit") ) && usage==2){ // some times socket becomes null for
```

```
                                                  //for ip_que_exmit while coming out of
                                    // ip protocol thus this section
            if(skb->nh.iph->protocol==IPPROTO_TCP){
                  if(skb->h.th->syn==1)
                        strcat(big_buffer,"S ");
                  else if(skb->h.th->fin==1)
                        strcat(big_buffer,"F ");
                  else if(skb->h.th->psh==1)
                        strcat(big_buffer,"P ");
                  else
                        strcat(big_buffer,". ");

                  strcat(big_buffer,in_ntoa32(skb->h.th->seq) );
                  strcat(big_buffer," ack ");
                  strcat(big_buffer,in_ntoa32(skb->h.th->ack_seq));
                  strcat(big_buffer," ");
            }
      }

}



if(print_ipid==1)
      strcat(big_buffer,in_ntoa16(skb->nh.iph->id));
else
      strcat(big_buffer,"0");


if(sk){
      //strcat(big_buffer," proto : ");
      switch(sk->protocol){
            case IPPROTO_UDP  : strcat(big_buffer," udp");break;
            case IPPROTO_TCP  : strcat(big_buffer," tcp");break;
            case IPPROTO_ICMP : strcat(big_buffer," icmp");break;
      }

}
```

```
      strcat(big_buffer,"\n");

}


int changed_ip_forward(struct sk_buff *skb){

      int slock_flags;
      int retval;
      char fname[20];
      char position[2];

      strcpy(fname,"ip_forward");
      strcpy(position,"B");
      send_storebuf(skb,fname,position,1,0);

      LOCK_KERN;
      _memcpy(pr, pr_save,NUM_BYTES);
      UNLOCK_KERN;

      retval=pr(skb);

      LOCK_KERN;
      _memcpy(pr, pr_jump,NUM_BYTES);
      UNLOCK_KERN;

      strcpy(position,"E");
      send_storebuf(skb,fname,position,2,1);

      return retval;
}



int changed_ip_forward_finish(struct sk_buff *skb){
      int slock_flags;
      int retval;
```

```
        char fname[20];
        char position[2];

        strcpy(fname,"ip_forward_finish");
        strcpy(position,"B");
        send_storebuf(skb,fname,position,1,0);


        LOCK_KERN;
        _memcpy(pr1, pr_save1,NUM_BYTES);
        UNLOCK_KERN;

        retval=pr1(skb);

        LOCK_KERN;
        _memcpy(pr1, pr_jump1,NUM_BYTES);
        UNLOCK_KERN;

        strcpy(position,"E");
        send_storebuf(skb,fname,position,2,1);

        return retval;
}

int changed_ip_send(struct sk_buff *skb){
        int slock_flags;
        int retval;
        char fname[20];
        char position[2];


        strcpy(fname,"ip_send");
        strcpy(position,"B");
        send_storebuf(skb,fname,position,1,1);


        LOCK_KERN;
        _memcpy(pr2, pr_save2,NUM_BYTES);
```

```
	UNLOCK_KERN;

	retval=pr2(skb);

	LOCK_KERN;
	_memcpy(pr2, pr_jump2,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
	send_storebuf(skb,fname,position,2,1);

	return retval;
}



unsigned int hook_func_packet_forward(unsigned int hooknum,
                          struct sk_buff **skb,
                          const struct net_device *in,
                          const struct net_device *out,
                          int (*okfn)(struct sk_buff *)){
	struct sk_buff *sb= *skb;
	char fname[20];
	char position[2];
	strcpy(position,"-");


	if(hooknum==NF_IP_FORWARD){
		strcpy(fname,"np_ip_forward_hook");
		send_storebuf(sb,fname,position,1,0);
		return NF_ACCEPT;
	}


	return NF_ACCEPT;

}
```

```
int init_module() {

      int slock_flags;

      pr=(int (*)(struct sk_buff *))allFunAddr[0];
      pr1=(int (*)(struct sk_buff *))allFunAddr[1];
      pr2=(int (*)(struct sk_buff *))allFunAddr[2];


      *(unsigned int *)(pr_jump+1)=(unsigned int) changed_ip_forward;//changed_ip_queue_xmit;
      *(unsigned int *)(pr_jump1+1)=(unsigned int) changed_ip_forward_finish;//changed_ip_queue_xmit2;
      *(unsigned int *)(pr_jump2+1)=(unsigned int)changed_ip_send;//changed_ip_output;

      LOCK_KERN;
      _memcpy(pr_save,pr,NUM_BYTES);
      _memcpy(pr,pr_jump,NUM_BYTES);
      _memcpy(pr_save1,pr1,NUM_BYTES);
      _memcpy(pr1,pr_jump1,NUM_BYTES);
      _memcpy(pr_save2,pr2,NUM_BYTES);
      _memcpy(pr2,pr_jump2,NUM_BYTES);

      UNLOCK_KERN;



      nfho1.hook     = hook_func_packet_forward; // Handler function
      nfho1.hooknum  = NF_IP_FORWARD; //  hook for IPv4 local delivery /
      nfho1.pf       = PF_INET;
      nfho1.priority = NF_IP_PRI_FIRST;  // Make our function first
        nf_register_hook(&nfho1);

      return 0;
}


void cleanup_module(){
      int slock_flags;
```

```
	LOCK_KERN;
	_memcpy(pr, pr_save,NUM_BYTES);
	_memcpy(pr1, pr_save1,NUM_BYTES);
	_memcpy(pr2, pr_save2,NUM_BYTES);

	UNLOCK_KERN;

	nf_unregister_hook(&nfho1);

	if(strlen(big_buffer)>0){
		print_buffer(FILE_NAME,big_buffer,strlen(big_buffer));
		big_buffer[0]='\0';
	}


}
```

12.15 myip_forward.sh

```
/* File name: myip_forward.sh
  This file supplies command line parameters after extracting the
  information from /boot/System.map file and loads the module
  myip_forward.o

*/

#!/bin/bash
#This is shell program to load tcpin.o module with requisite parameters


FUN="ip_forward"
FUN1="ip_forward_finish"
FUN2="ip_send"




PR=`cat /boot/System.map | grep -w $FUN  | cut -c 1-8`
PR1=`cat /boot/System.map | grep -w $FUN1 | cut -c 1-8`
PR2=`cat /boot/System.map | grep -w $FUN2 | cut -c 1-8`



if [ "$PR" = "" ]
then
      echo "PR is empty ,cannot get the address of $FUN "
elif [ "$PR1" = "" ]
then
      echo "PR1 is empty ,cannot get the address of $FUN1 "
elif [ "$PR2" = "" ]
then
      echo "PR2 is empty ,cannot get the address of $FUN2 "
else
```

```
        echo " insmod myip_forward.o allFunAddr=0x$PR,0x$PR1,0x$PR2"
        insmod myip_forward.o allFunAddr=0x$PR,0x$PR1,0x$PR2

fi
```

12.16 udpio.c

```
/* File name: udpio.c
   This file intercepts Linux UDP functions involved in the handling of
   both incoming and outgoing UDP Datagrams

*/


#include "module_header.h"

static unsigned char pr_jump[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save[NUM_BYTES];
static int (*pr)(struct sock *, long )= (int (*)(struct sock *, long ))0xc0227f00; //udp_close

static unsigned char pr_jump1[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save1[NUM_BYTES];
static int (*pr1)(struct sock *, struct sockaddr *, int) =(int (*)(struct sock *, struct sockaddr *,
int))0xc0227c60;//udp_connect

static unsigned char pr_jump2[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save2[NUM_BYTES];
static int (*pr2)(struct sock *, struct msghdr *, int)=(int (*)(struct sock *, struct msghdr *,
int))0xc02274d0;//udp_sendmsg

static unsigned char pr_jump3[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save3[NUM_BYTES];
static  int (*pr3)(struct sock *, struct msghdr *, int,int,int , int *)=( int (*)(struct sock *, struct
msghdr *, int,int,int , int * ))0xc02279b0;//udp_recvmsg

static unsigned char pr_jump4[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
```

```
static unsigned char pr_save4[NUM_BYTES];
static int (*pr4)(struct sock * , struct sk_buff *)=(int (*)(struct sock * , struct sk_buff
*))0xc0227f10;//udp_queue_rcv_skb

static unsigned char pr_jump5[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save5[NUM_BYTES];
static int (*pr5)(struct sock *)=(int (*)(struct sock *))0xc0227010;//udp_v4_hash

static unsigned char pr_jump6[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save6[NUM_BYTES];
static int (*pr6)(struct sock *)=(int (*)(struct sock *))0xc0227020;//udp_v4_unhash

static unsigned char pr_jump7[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save7[NUM_BYTES];
static int (*pr7)(struct sock *, unsigned short)=(int (*)(struct sock *, unsigned
short))0xc0226dc0;//udp_v4_get_port

static unsigned char pr_jump8[NUM_BYTES]="\xb8\x00\x00\x00\x00" /* movl $0,%eax */
                              "\xff\xe0"; // jmp *eax
static unsigned char pr_save8[NUM_BYTES];
static int (*pr8)(struct sk_buff *)=(int (*)(struct sk_buff *))0xc0228320;//udp_rcv



extern  char big_buffer[BUFSIZE*100]="\0";


void only_sock_incoming(struct sock *sk,char *fun_name,char *position,int end) {
      char store_time[20];
        my_time(store_time);
        if(strlen(big_buffer)>=BUFSIZE*100-RECORD_SIZE){
                printk("<1>out of buffer memory\n");
                return;
        }
        strcat(big_buffer,store_time);
```

```
        strcat(big_buffer," ");
      strcat(big_buffer,in_ntoa(sk->daddr)); // print dest address first as this function
      strcat(big_buffer,":");                //is for incoming packets and sport is this machine
      strcat(big_buffer,in_ntoa16(sk->dport));
      strcat(big_buffer," ");
        strcat(big_buffer,in_ntoa(sk->saddr));
        strcat(big_buffer,":");
      strcat(big_buffer,in_ntoa16(sk->sport));
      strcat(big_buffer," ");

      strcat(big_buffer,fun_name);
      strcat(big_buffer," ");
      strcat(big_buffer,position);
      strcat(big_buffer,"\n");
}

void only_sock_outgoing(struct sock *sk,char *fun_name,char *position,int end) {
      char store_time[20];
        my_time(store_time);
        if(strlen(big_buffer)>=BUFSIZE*100-RECORD_SIZE){
                printk("<1>out of buffer memory\n");
                return;
        }


      strcat(big_buffer,store_time);
        strcat(big_buffer," ");
      if(sk) { //udp_v4_unhash function may destroy socket
            strcat(big_buffer,in_ntoa(sk->saddr)); // print src address first as this function
            strcat(big_buffer,":");                //is for outgoing packets
            strcat(big_buffer,in_ntoa16(sk->sport));
            strcat(big_buffer," ");
            strcat(big_buffer,in_ntoa(sk->daddr));
            strcat(big_buffer,":");
            strcat(big_buffer,in_ntoa16(sk->dport));
      }     strcat(big_buffer," ");

      strcat(big_buffer,fun_name);
```

```
	strcat(big_buffer," ");
	strcat(big_buffer,position);
	strcat(big_buffer,"\n");
}

void print_udp_skb(struct sk_buff* skb,char * fun_name,char* position,int sockorskb){

	char store_time[20];
	my_time(store_time);
	if(strlen(big_buffer)>=BUFSIZE*100-RECORD_SIZE){
		printk("<1>out of buffer memory\n");
		return;
	}
	strcat(big_buffer,store_time);
	strcat(big_buffer," ");
	strcat(big_buffer,in_ntoa(skb->nh.iph->saddr));
	strcat(big_buffer,":");
	strcat(big_buffer,in_ntoa16(skb->h.uh->source));
	strcat(big_buffer," ");
	strcat(big_buffer,in_ntoa(skb->nh.iph->daddr));
	strcat(big_buffer,":");
	strcat(big_buffer,in_ntoa16(skb->h.uh->dest));
	strcat(big_buffer," ");
	strcat(big_buffer,fun_name);
	strcat(big_buffer," ");
	strcat(big_buffer,position);
	strcat(big_buffer,"\n");
}



int changed_udp_rcv(struct sk_buff *skb){
	int slock_flags;
	int retval;
	char fname[20];
	char position[2];
```

```
	strcpy(fname,"udp_v4_get_port");
	strcpy(position,"B");
	print_udp_skb(skb,fname,position,0);


	LOCK_KERN;
	_memcpy(pr8, pr_save8,NUM_BYTES);
	UNLOCK_KERN;

	retval=pr8(skb);

	LOCK_KERN;
	_memcpy(pr8, pr_jump8,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");

	print_udp_skb(skb,fname,position,0);

	return retval;
}

int changed_udp_v4_get_port(struct sock *sk, unsigned short snum){
	int slock_flags;
	int retval;
	char fname[20];
	char position[2];


	strcpy(fname,"udp_v4_get_port");
	strcpy(position,"B");
	only_sock_outgoing(sk,fname,position,0);


	LOCK_KERN;
	_memcpy(pr7, pr_save7,NUM_BYTES);
	UNLOCK_KERN;
```

```
	retval=pr7(sk,snum);

	LOCK_KERN;
	_memcpy(pr7, pr_jump7,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");

	only_sock_outgoing(sk,fname,position,0);

	return retval;
}

int changed_udp_v4_unhash(struct sock *sk){
	int slock_flags;
	int retval;
	char fname[20];
	char position[2];


	strcpy(fname,"udp_v4_hash");
	strcpy(position,"B");
	only_sock_outgoing(sk,fname,position,0);


	LOCK_KERN;
	_memcpy(pr6, pr_save6,NUM_BYTES);
	UNLOCK_KERN;

	retval=pr6(sk);

	LOCK_KERN;
	_memcpy(pr6, pr_jump6,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");

	only_sock_outgoing(sk,fname,position,0);
```

```
      return retval;
}



int changed_udp_v4_hash(struct sock *sk){
      int slock_flags;
      int retval;
      char fname[20];
      char position[2];


      strcpy(fname,"udp_v4_hash");
      strcpy(position,"B");
      only_sock_incoming(sk,fname,position,0);


      LOCK_KERN;
      _memcpy(pr5, pr_save5,NUM_BYTES);
      UNLOCK_KERN;

      retval=pr5(sk);

      LOCK_KERN;
      _memcpy(pr5, pr_jump5,NUM_BYTES);
      UNLOCK_KERN;

      strcpy(position,"E");
      only_sock_incoming(sk,fname,position,0);

      return retval;
}



int changed_udp_queue_rcv_skb(struct sock * sk, struct sk_buff *skb){
```

```
	int slock_flags;
	int retval;
	char fname[20];
	char position[2];


	strcpy(fname,"udp_queue_rcv_skb");
	strcpy(position,"B");
	only_sock_incoming(sk,fname,position,0);


	LOCK_KERN;
	_memcpy(pr4, pr_save4,NUM_BYTES);
	UNLOCK_KERN;

	retval=pr4(sk,skb);

	LOCK_KERN;
	_memcpy(pr4, pr_jump4,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
	only_sock_incoming(sk,fname,position,0);

	return retval;
}



int changed_udp_recvmsg(struct sock *sk, struct msghdr *msg, int len,
		  int noblock, int flags, int *addr_len){
	int slock_flags;
	int retval;
	char fname[20];
	char position[2];
```

```
	strcpy(fname,"udp_recvmsg");
	strcpy(position,"B");
	only_sock_incoming(sk,fname,position,0);


	LOCK_KERN;
	_memcpy(pr3, pr_save3,NUM_BYTES);
	UNLOCK_KERN;

	retval=pr3(sk,msg,len,noblock,flags,addr_len);

	LOCK_KERN;
	_memcpy(pr3, pr_jump3,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
	only_sock_incoming(sk,fname,position,0);



	return retval;
}


int changed_udp_sendmsg(struct sock *sk, struct msghdr *msg, int len){
	int slock_flags;
	int retval;
	char fname[20];
	char position[2];


	strcpy(fname,"udp_sendmsg");
	strcpy(position,"B");
	only_sock_outgoing(sk,fname,position,0);


	LOCK_KERN;
	_memcpy(pr2, pr_save2,NUM_BYTES);
```

```
	UNLOCK_KERN;

	retval=pr2(sk,msg,len);

	LOCK_KERN;
	_memcpy(pr2, pr_jump2,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
	only_sock_outgoing(sk,fname,position,0);



	return retval;
}



int changed_udp_connect(struct sock *sk, struct sockaddr *uaddr, int addr_len){
	int slock_flags;
	int retval;
	char fname[20];
	char position[2];


	strcpy(fname,"udp_connect");
	strcpy(position,"B");
	only_sock_outgoing(sk,fname,position,0);


	LOCK_KERN;
	_memcpy(pr1, pr_save1,NUM_BYTES);
	UNLOCK_KERN;

	retval=pr1(sk,uaddr,addr_len);

	LOCK_KERN;
	_memcpy(pr1, pr_jump1,NUM_BYTES);
```

```
	UNLOCK_KERN;

	strcpy(position,"E");
	only_sock_outgoing(sk,fname,position,0);



	return retval;
}



int changed_udp_close(struct sock *sk, long timeout){
	int slock_flags;
	int retval;
	char fname[20];
	char position[2];


	strcpy(fname,"udp_close");
	strcpy(position,"B");
	only_sock_outgoing(sk,fname,position,0);


	LOCK_KERN;
	_memcpy(pr, pr_save,NUM_BYTES);
	UNLOCK_KERN;

	retval=pr(sk,timeout);

	LOCK_KERN;
	_memcpy(pr, pr_jump,NUM_BYTES);
	UNLOCK_KERN;

	strcpy(position,"E");
	only_sock_outgoing(sk,fname,position,0);
```

```
	return retval;
}



int init_module() {

	int slock_flags;

	*(unsigned int *)(pr_jump+1)=(unsigned int)changed_udp_close;
	*(unsigned int *)(pr_jump1+1)=(unsigned int)changed_udp_connect;
	*(unsigned int *)(pr_jump2+1)=(unsigned int)changed_udp_sendmsg;
	*(unsigned int *)(pr_jump3+1)=(unsigned int)changed_udp_recvmsg;
	*(unsigned int *)(pr_jump4+1)=(unsigned int)changed_udp_queue_rcv_skb;
	*(unsigned int *)(pr_jump5+1)=(unsigned int)changed_udp_v4_hash;
	*(unsigned int *)(pr_jump6+1)=(unsigned int)changed_udp_v4_unhash;
	*(unsigned int *)(pr_jump7+1)=(unsigned int)changed_udp_v4_get_port;
	*(unsigned int *)(pr_jump8+1)=(unsigned int)changed_udp_rcv;


	LOCK_KERN;

	_memcpy(pr_save,pr,NUM_BYTES);
	_memcpy(pr,pr_jump,NUM_BYTES);

	_memcpy(pr_save1,pr1,NUM_BYTES);
	_memcpy(pr1,pr_jump1,NUM_BYTES);

	_memcpy(pr_save2,pr2,NUM_BYTES);
	_memcpy(pr2,pr_jump2,NUM_BYTES);

	_memcpy(pr_save3,pr3,NUM_BYTES);
	_memcpy(pr3,pr_jump3,NUM_BYTES);

	_memcpy(pr_save4,pr4,NUM_BYTES);
	_memcpy(pr4,pr_jump4,NUM_BYTES);
```

```
	_memcpy(pr_save5,pr5,NUM_BYTES);
	_memcpy(pr5,pr_jump5,NUM_BYTES);

	_memcpy(pr_save6,pr6,NUM_BYTES);
	_memcpy(pr6,pr_jump6,NUM_BYTES);

	_memcpy(pr_save7,pr7,NUM_BYTES);
	_memcpy(pr7,pr_jump7,NUM_BYTES);

	_memcpy(pr_save8,pr8,NUM_BYTES);
	_memcpy(pr8,pr_jump8,NUM_BYTES);



	UNLOCK_KERN;



	printk("<1> protocol added\n");


	return 0;
}


void cleanup_module(){
	int slock_flags;


	LOCK_KERN;
	_memcpy(pr, pr_save,NUM_BYTES);
	_memcpy(pr1, pr_save1,NUM_BYTES);
	_memcpy(pr2, pr_save2,NUM_BYTES);
	_memcpy(pr3, pr_save3,NUM_BYTES);
	_memcpy(pr4, pr_save4,NUM_BYTES);
	_memcpy(pr5, pr_save5,NUM_BYTES);
	_memcpy(pr6, pr_save6,NUM_BYTES);
```

```
	_memcpy(pr7, pr_save7,NUM_BYTES);
	_memcpy(pr8, pr_save8,NUM_BYTES);


	UNLOCK_KERN;
	if(strlen(big_buffer)>0){
		print_buffer(FILE_NAME,big_buffer,strlen(big_buffer));
		big_buffer[0]='\0';
	}

	printk("<1> Protocol Removed \n");
}
```

12.17 udpio.sh

```
/* File name: udpio.sh
  This file supplies command line parameters after extracting the
  information from /boot/System.map file and loads the module
  udpio.o

*/

#!/bin/bash
#This is shell program to load tcpin.o module with requisite parameters

FUN="udp_close"
FUN1="udp_connect"
FUN2="udp_sendmsg"
FUN3="udp_recvmsg"
FUN4="udp_queue_rcv_skb"
FUN5="udp_v4_hash"
FUN6="udp_v4_unhash"
FUN7="udp_v4_get_port"
FUN8="udp_rcv"
FUN9="udp_getfrag"


PR=`cat /boot/System.map  | grep -w $FUN  | cut -c 1-8`
PR1=`cat /boot/System.map | grep -w $FUN1 | cut -c 1-8`
PR2=`cat /boot/System.map | grep -w $FUN2 | cut -c 1-8`
PR3=`cat /boot/System.map | grep -w $FUN3 | cut -c 1-8`
PR4=`cat /boot/System.map | grep -w $FUN4 | cut -c 1-8`
PR5=`cat /boot/System.map | grep -w $FUN5 | cut -c 1-8`
PR6=`cat /boot/System.map | grep -w $FUN6 | cut -c 1-8`
PR7=`cat /boot/System.map | grep -w $FUN7 | cut -c 1-8`
PR8=`cat /boot/System.map | grep -w $FUN8 | cut -c 1-8`
PR9=`cat /boot/System.map | grep -w $FUN9 | cut -c 1-8`
```

```
if [ "$PR" = "" ]
then
      echo "PR is empty ,cannot get the address of $FUN "
elif [ "$PR1" = "" ]
then
      echo "PR1 is empty ,cannot get the address of $FUN1 "
elif [ "$PR2" = "" ]
then
      echo "PR2 is empty ,cannot get the address of $FUN2 "
elif [ "$PR3" = "" ]
then
      echo "PR3 is empty ,cannot get the address of $FUN3 "
 elif [ "$PR4" = "" ]
then
      echo "PR4 is empty ,cannot get the address of $FUN4 "
elif [ "$PR5" = "" ]
then
      echo "PR5 is empty ,cannot get the address of $FUN5 "
elif [ "$PR6" = "" ]
then
      echo "PR6 is empty ,cannot get the address of $FUN6 "
elif [ "$PR7" = "" ]
then
      echo "PR7 is empty ,cannot get the address of $FUN7 "
elif [ "$PR8" = "" ]
then
      echo "PR8 is empty ,cannot get the address of $FUN8 "
elif [ "$PR9" = "" ]
then
      echo "PR9 is empty ,cannot get the address of $FUN9 "

else
      echo " insmod udpio.o
allFunAddr=0x$PR,0x$PR1,0x$PR2,0x$PR3,0x$PR4,0x$PR5,0x$PR6,0x$PR7,0x$PR8,0x$PR9"
      insmod udpio.o allFunAddr=0x$PR,0x$PR1,0x$PR2,0x$PR3,0x$PR4,0x$PR5,0x$PR6,0x$PR7,0x$PR8,0x$PR9

fi
```

12.18 cludp.c

```
/* File name: cludp.c

 This is a  client program to generate udp traffic
 It sends an UDP packet to the server, receives the same udp packet from the server and displays the packet
content on the screen.
*/

#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <assert.h>
#include <errno.h>
#include <sys/socket.h>
#include <sys/types.h>
#include <netinet/in.h>
#include <arpa/inet.h>


#define SERV_PORT 1234
#define MAXLINE 80



int main (int argc, char **argv){

      int clsk,numbytes;
      FILE *fp;
      struct sockaddr_in destaddr;
      char out_line[MAXLINE],in_line[MAXLINE +1];

      if (argc !=2){
            printf("usage: udpcl <ipaddress>");
            return 0;
      }
      bzero(&destaddr,sizeof(destaddr));
```

```
        destaddr.sin_family=AF_INET;
        destaddr.sin_port=htons(SERV_PORT);
        inet_pton(AF_INET,argv[1],&destaddr.sin_addr);
        clsk =socket(AF_INET,SOCK_DGRAM,0);
        fp=stdin;

        while (fgets(out_line,MAXLINE,fp) !=NULL ) {
              sendto(clsk,out_line,strlen(out_line),0,(struct sockaddr *)&destaddr,sizeof(destaddr) );
              numbytes = recvfrom(clsk,in_line,MAXLINE,0,NULL,NULL);
              in_line[numbytes]=0;
              fputs(in_line,stdout);
        }

        return 0;
}
```

12.19 srvudp.c

```
/* File name: srvudp.c

This is a  server program to generate udp traffic
It receives an UDP packet from client on a predetermined port and resends the same packet back to the
client.

*/

#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <assert.h>
#include <errno.h>
#include <sys/socket.h>
#include <sys/types.h>
#include <netinet/in.h>
#include <arpa/inet.h>


#define SERV_PORT 1234
#define MAXLINE 80



int main (int argc, char **argv){

      int srsk,numbytes;
      socklen_t len;
      char data[MAXLINE];
      FILE *fp;
      struct sockaddr_in me,you;
```

```
	bzero(&me,sizeof(me));
	srsk=socket(AF_INET,SOCK_DGRAM,0);

	me.sin_family = AF_INET;
	me.sin_port = htons(SERV_PORT);
	me.sin_addr.s_addr = htonl(INADDR_ANY);
	srsk = socket(AF_INET,SOCK_DGRAM,0);
	bind(srsk,(struct sockaddr *)&me,sizeof(me));

	while(1){
		len = sizeof(you);
		numbytes = recvfrom(srsk,data,MAXLINE,0,(struct sockaddr *)&you,&len);
		sendto(srsk,data,numbytes,0,(struct sockaddr *)&you,len);
	}

	return 0;
}
```

12.20 module_header.h

```
/* File name: module_header.h

This is a header file that mainly contains definition of some utility functions used in all the modules.

*/

#define MODULE
#define __KERNEL__
#define _write(f, buf, sz) (f->f_op->write(f, buf, sz, &f->f_pos))
#define WRITABLE(f) (f->f_op && f->f_op->write)
#define BEGIN_KMEM { mm_segment_t old_fs = get_fs(); set_fs(get_ds());
#define END_KMEM set_fs(old_fs); }
#define NUM_BYTES 7
#define BUFSIZE 65535000
#define RECORD_SIZE 200
#define FILE_NAME "/tmp/packet.log"
#define MY_PROTO_ID 0x0003 //same as ETH_P_ALL
#define TIME_ZONE -4*60*60 // GMT - 4 Which is Eastern Daylight Time
#define SEC_IN_HOUR  (60 * 60 )
#define SEC_IN_DAY   (SEC_IN_HOUR * 24)

#include <linux/module.h>
#include <linux/kernel.h>
#include <linux/skbuff.h>
#include <linux/smp_lock.h>
#include <asm/page.h>
#include <linux/netdevice.h>
#include <net/tcp.h>
#include <net/udp.h>
#include <linux/file.h>
#include <linux/in.h>
#include <linux/netfilter.h>
#include <linux/netfilter_ipv4.h>
```

```
typedef struct rec {
      __u32 src;
      __u32 dst;
      __u16 spt;
      __u16 dpt;
      char fname[30];
      char position[2];
      char flag[2];
      __u32 sq;
      __u32 asq;
      __u16 ipid;
      int protocol;

} Prec;

/*spinlock used for parts where we want no interrupts*/
static spinlock_t kern_lock = SPIN_LOCK_UNLOCKED;

/* macros for using spinlock */

#define LOCK_KERN spin_lock_irqsave(&kern_lock,slock_flags)
#define UNLOCK_KERN spin_unlock_irqrestore(&kern_lock,slock_flags)

void *_memcpy(void *dest, const void *src, int size)
{
      const char *p = src;
      char *q = dest;
      int i;

      for (i = 0; i < size; i++) *q++ = *p++;

      return dest;
}


void my_time (char *p_time)
{
      struct timeval tv;
```

```
	long int rem;
	time_t t;
	suseconds_t u;
	int time_hr,time_min,time_sec;
	do_gettimeofday(&tv);

	t = (time_t)tv.tv_sec;
	u=(suseconds_t)tv.tv_usec;


	rem = t % SEC_IN_DAY;
	rem = rem + TIME_ZONE;

	while(rem < 0) {
		rem = rem + SEC_IN_DAY;
	}

	while (rem >= SEC_IN_DAY) {
		rem -= SEC_IN_DAY;
	}

	time_hr= rem / SEC_IN_HOUR ;
	rem %= SEC_IN_HOUR;
	time_min= rem/60;
	time_sec = rem%60;

	sprintf(p_time, "%.2d:%.2d:%.2d:%.6ld", time_hr, time_min,time_sec,u);
}


char *in_ntoa(__u32 in) { // returns ip number
	static char buff[18];
	char *p;

	p = (char *) &in;
	sprintf(buff, "%d.%d.%d.%d",
		(p[0] & 255), (p[1] & 255), (p[2] & 255), (p[3] & 255));
	return(buff);
```

```
}


char * ctos(char in) {
      static char buff[4];
      sprintf(buff,"%ud",in&255);
      return(buff);
}

char * in_ntoa16(__u16 in){ //returns port,id etc numbers
      static char buff1[6];
      sprintf(buff1,"%hu", ntohs(in));
      return buff1;
}

char * in_ntoa32(__u32 in){ //returns ip_sequence etc numbers
      static char buff2[11];
      sprintf(buff2,"%u", ntohl(in));
      return buff2;
}


int print_buffer(char *logfile, char *buf, int size)
{
      int ret = 0;
      struct file   *f = NULL;

      lock_kernel();
      BEGIN_KMEM;
      f = filp_open(logfile, O_CREAT|O_APPEND, 00600);

      if (IS_ERR(f)) {
            printk("<1>Error %ld opening %s\n", -PTR_ERR(f), logfile);
            ret = -1;
      } else {
            if (WRITABLE(f))
                  _write(f, buf, size);
            else {
```

```
                        printk("<1> %s does not have a write method\n",
                              logfile);
                  ret = -1;
            }

            if ((ret = filp_close(f,NULL)))
                  printk("<1>Error %d closing %s\n", -ret, logfile);
      }
      END_KMEM;
      unlock_kernel();

      return ret;
}

MODULE_AUTHOR("Gyan");
MODULE_DESCRIPTION("Tcp Ip in Linux Kernel");
MODULE_LICENSE("GPL");
```

12.21 Makefile

```
/* File name: module_header.h

This is a Makefile that compiles all the module files present in same directory as this file

*/
WARN    := -W #-Wall -Wstrict-prototypes -Wmissing-prototypes
INCLUDE := -isystem /lib/modules/`uname -r`/build/include
CFLAGS  := -O6  $(WARN) $(INCLUDE)
CC      := gcc
#OBJS    := $(patsubst %.c, %.o, $(wildcard *.c))
OBJS    := $(patsubst %.c, %.o, myip_rcv.c myip_send.c)

all: $(OBJS)

.PHONY: clean

clean:
      rm  *.o
```

11.22 format

```
/* File name: format

This is a perl script used to format the /tmp/packet.log file produced by all the modules.

*/

#!/usr/bin/perl

$short=0; # toggle this for short or long printout 1 means short 0 means long


open (FILEID, "/tmp/packet.log") ||  die "can't open input: !";
    $ctr=1;
    $wctr='    ';
    $lctr = -1;

while ( $line = <FILEID>) {
      if(!$short){
            if($ctr < 10){    print "$ctr     ";}
            elsif ($ctr <100) {print "$ctr    ";}
            elsif ($ctr <1000) {print "$ctr   ";}
            else { print "$ctr ";}
            $ctr++;
      }
      if ($line =~ /B/ ){
            $lctr++;
            print ($wctr x $lctr);
      #     $line = ($wctr x $lctr) . $line ;
            if($short){
                  @indiv_word =  split( / /, $line);
                  print $indiv_word[3];
                  print " ";
                  chomp($indiv_word[4]);
                  print $indiv_word[4];
```

```
            print("\n");
      }
      else {
            print $line;
      }
      if ($lctr == 0){
            @words = split( / /, $line);
            @timer= split(/:/, $words[0]);
            $start_time1 = ($timer[0]*3600) + ($timer[1]*60) + $timer[2];
            $start_time2 = $timer[3];
      }

}
elsif ($line =~ /E/){
       print ($wctr x $lctr);
#     $line = ($wctr x $lctr) . $line ;
      if($short){
                  @indiv_word =  split( / /, $line);
                  print $indiv_word[3];
            print " ";
                  chomp($indiv_word[4]);
            print $indiv_word[4];
                  print("\n");
          }
          else {
                  print $line;
          }


      $lctr--;

      if ($lctr == -1){
            @words = split( / /, $line);
            @timer = split(/:/, $words[0]);
            $start_time3 = ($timer[0]*3600) + ($timer[1]*60) + $timer[2];
            $start_time4 = $timer[3];
      }
}
```

```
      else {

            $lctr++;
            print ($wctr x $lctr);

                print $line;

            if ($lctr == 0){
                  @words = split( / /, $line);
                  @timer= split(/:/, $words[0]);
                  $start_time1 = ($timer[0]*3600) + ($timer[1]*60) + $timer[2];
                  $start_time2 = $timer[3];
            }

            $lctr--;

            if ($lctr == -1){
                  @words = split( / /, $line);
                  @timer = split(/:/, $words[0]);
                  $start_time3 = ($timer[0]*3600) + ($timer[1]*60) + $timer[2];
                  $start_time4 = $timer[3];
            }
      }
      if($lctr == -1){
            print("       Time : ");
            print  $start_time4 - $start_time2 + ($start_time3 - $start_time1)*1000000 ;
            print("\n");
      }
}

close(FILEID);
```

12.23 Logfiles

12.23.1 LOG_TCP

```
1    19:26:16:460191 0.0.0.0:0 0.0.0.0:0 tcp_v4_init_sock B
2    19:26:16:460199 0.0.0.0:0 0.0.0.0:0 tcp_v4_init_sock E
     Time : 8
3    19:26:16:460214 0.0.0.0:0 0.0.0.0:0 tcp_v4_connect B
4       19:26:16:460224 192.168.1.20:0 128.235.204.81:21 tcp_set_state B
5       19:26:16:460236 192.168.1.20:0 128.235.204.81:21 tcp_set_state E
6       19:26:16:460540 192.168.1.20:33056 128.235.204.81:21 tcp_connect B
7          19:26:16:460558 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb B
8          19:26:16:460584 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb E S 516203531 ack 0
9       19:26:16:460623 192.168.1.20:33056 128.235.204.81:21 tcp_connect E
10   19:26:16:460644 192.168.1.20:33056 128.235.204.81:21 tcp_v4_connect E
     Time : 430
11   19:26:16:482081 128.235.204.81:21 192.168.1.20:33056 tcp_v4_rcv B S 2291929751 ack 516203532
12      19:26:16:482117 128.235.204.81:21 192.168.1.20 __tcp_v4_lookup B
13      19:26:16:482143 128.235.204.81:21 192.168.1.20:33056 __tcp_v4_lookup E
14      19:26:16:482173 128.235.204.81:21 192.168.1.20:33056 tcp_v4_do_rcv B S 2291929751 ack 516203532
15         19:26:16:482216 192.168.1.20:33056 128.235.204.81:21 tcp_rcv_state_process B
16            19:26:16:482251 192.168.1.20:33056 128.235.204.81:21 tcp_rcv_synsent_state_process B S 2291929751 ack 516203532
17               19:26:16:482304 128.235.204.81:21 192.168.1.20:33056 tcp_ack B S 2291929751 ack 516203532
18               19:26:16:482360 128.235.204.81:21 192.168.1.20:33056 tcp_ack E S 2291929751 ack 516203532
19               19:26:16:482418 192.168.1.20:33056 128.235.204.81:21 tcp_set_state B
20               19:26:16:482462 192.168.1.20:33056 128.235.204.81:21 tcp_set_state E
21               19:26:16:482508 192.168.1.20:33056 128.235.204.81:21 tcp_send_ack B
22                  19:26:16:482555 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb B
23                     19:26:16:482606 present_window: NIL tcp_receive_window B
24                     19:26:16:482606 present_window: 5840 tcp_receive_window E
25                     19:26:16:482671 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window B
26                     19:26:16:482727 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window E
27                  19:26:16:482788 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb E . 516203532 ack 2291929752
28               19:26:16:482879 192.168.1.20:33056 128.235.204.81:21 tcp_send_ack E
29            19:26:16:482940 192.168.1.20:33056 128.235.204.81:21 tcp_rcv_synsent_state_process E S 2291929751 ack 516203532
30         19:26:16:483029 192.168.1.20:33056 128.235.204.81:21 tcp_rcv_state_process E
```

```
19:26:16:483095 128.235.204.81:21 192.168.1.20:33056 tcp_v4_do_rcv E S 2291929751 ack 516203532
19:26:16:483203 128.235.204.81:21 192.168.1.20:33056 tcp_v4_rcv E S 2291929751 ack 516203532
Time : 1122
19:26:16:483800 192.168.1.20:33056 128.235.204.81:21 tcp_setsockopt B
19:26:16:483877 192.168.1.20:33056 128.235.204.81:21 tcp_setsockopt E
Time : 77
19:26:16:525001 128.235.204.81:21 192.168.1.20:33056 tcp_v4_rcv B P 2291929752 ack 516203532
   19:26:16:525109 128.235.204.81:21 192.168.1.20 __tcp_v4_lookup B
   19:26:16:525180 128.235.204.81:21 192.168.1.20:33056 __tcp_v4_lookup E
19:26:16:525265 128.235.204.81:21 192.168.1.20:33056 tcp_v4_rcv E P 2291929752 ack 516203532
Time : 264
19:26:16:525512 128.235.204.81:21 192.168.1.20:33056 tcp_v4_do_rcv B P 2291929752 ack 516203532
   19:26:16:525629 128.235.204.81:21 192.168.1.20:33056 tcp_rcv_established B P 2291929752 ack 516203532
      19:26:16:525752 present_window: NIL tcp_receive_window B
      19:26:16:525752 present_window: 5840 tcp_receive_window E
      19:26:16:525869 128.235.204.81:21 192.168.1.20:33056 tcp_ack B P 2291929752 ack 516203532
      19:26:16:525997 128.235.204.81:21 192.168.1.20:33056 tcp_ack E P 2291929752 ack 516203532
      19:26:16:526127 128.235.204.81:21 192.168.1.20:33056 tcp_data_queue B P 2291929752 ack 516203532
         19:26:16:526260 present_window: NIL tcp_receive_window B
         19:26:16:526260 present_window: 5840 tcp_receive_window E
         19:26:16:526402 128.235.204.81:21 192.168.1.20:33056 tcp_event_data_recv B P 2291929752 ack 516203532
         19:26:16:526544 128.235.204.81:21 192.168.1.20:33056 tcp_event_data_recv E P 2291929752 ack 516203532
      19:26:16:526689 128.235.204.81:21 192.168.1.20:33056 tcp_data_queue E P 2291929752 ack 516203532
      19:26:16:526837 128.235.204.81:21 192.168.1.20:33056 __tcp_ack_snd_check B
         19:26:16:526953 192.168.1.20:33056 128.235.204.81:21 tcp_send_ack B
            19:26:16:527071 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb B
               19:26:16:527191 present_window: NIL tcp_receive_window B
               19:26:16:527191 present_window: 5776 tcp_receive_window E
               19:26:16:527341 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window B
               19:26:16:527465 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window E
            19:26:16:527605 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb E . 516203532 ack 2291929816
         19:26:16:527788 192.168.1.20:33056 128.235.204.81:21 tcp_send_ack E
      19:26:16:527918 128.235.204.81:21 192.168.1.20:33056 __tcp_ack_snd_check E
   19:26:16:528049 128.235.204.81:21 192.168.1.20:33056 tcp_rcv_established E P 2291929752 ack 516203532
19:26:16:528228 128.235.204.81:21 192.168.1.20:33056 tcp_v4_do_rcv E . 516203532 ack 2291929816
Time : 2716
19:26:16:528412 present_window: NIL tcp_receive_window B
```

64 19:26:16:528412 present_window: 5840 tcp_receive_window E
Time : 0
65 19:26:16:528587 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window B
66 19:26:16:528729 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window E
Time : 142
67 19:26:18:507768 192.168.1.20:33056 128.235.204.81:21 tcp_sendmsg B
68 19:26:18:507924 192.168.1.20:33056 128.235.204.81:21 tcp_push B
69 19:26:18:508074 192.168.1.20:33056 128.235.204.81:21 __tcp_push_pending_frames B
70 19:26:18:508225 192.168.1.20:33056 128.235.204.81:21 tcp_write_xmit B
71 19:26:18:508380 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb B
72 19:26:18:508535 present_window: NIL tcp_receive_window B
73 19:26:18:508535 present_window: 5840 tcp_receive_window E
74 19:26:18:508732 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window B
75 19:26:18:508892 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window E
76 19:26:18:509075 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb E P 516203532 ack 2291929816
77 19:26:18:509311 192.168.1.20:33056 128.235.204.81:21 tcp_write_xmit E
78 19:26:18:509478 192.168.1.20:33056 128.235.204.81:21 __tcp_push_pending_frames E
79 19:26:18:509645 192.168.1.20:33056 128.235.204.81:21 tcp_push E
80 19:26:18:509815 192.168.1.20:33056 128.235.204.81:21 tcp_sendmsg E
Time : 2047
81 19:26:18:529385 128.235.204.81:21 192.168.1.20:33056 tcp_v4_rcv B . 2291929816 ack 516203543
82 19:26:18:529623 128.235.204.81:21 192.168.1.20 __tcp_v4_lookup B
83 19:26:18:529778 128.235.204.81:21 192.168.1.20:33056 __tcp_v4_lookup E
84 19:26:18:529959 128.235.204.81:21 192.168.1.20:33056 tcp_v4_rcv E . 2291929816 ack 516203543
Time : 574
85 19:26:18:530337 128.235.204.81:21 192.168.1.20:33056 tcp_v4_do_rcv B . 2291929816 ack 516203543
86 19:26:18:530582 128.235.204.81:21 192.168.1.20:33056 tcp_rcv_established B . 2291929816 ack 516203543
87 19:26:18:530832 128.235.204.81:21 192.168.1.20:33056 tcp_ack B . 2291929816 ack 516203543
88 19:26:18:531086 128.235.204.81:21 192.168.1.20:33056 tcp_ack E . 2291929816 ack 516203543
89 19:26:18:531341 128.235.204.81:21 192.168.1.20:33056 tcp_rcv_established E . 2291929816 ack 516203543
90 19:26:18:531599 128.235.204.81:21 192.168.1.20:33056 tcp_v4_do_rcv E . 2291929816 ack 516203543
Time : 1262
91 19:26:18:537481 128.235.204.81:21 192.168.1.20:33056 tcp_v4_rcv B P 2291929816 ack 516203543
92 19:26:18:537747 128.235.204.81:21 192.168.1.20 __tcp_v4_lookup B
93 19:26:18:537922 128.235.204.81:21 192.168.1.20:33056 __tcp_v4_lookup E
94 19:26:18:538125 128.235.204.81:21 192.168.1.20:33056 tcp_v4_rcv E P 2291929816 ack 516203543
Time : 644

```
95   19:26:18:538518 128.235.204.81:21 192.168.1.20:33056 tcp_v4_do_rcv B P 2291929816 ack 516203543
96     19:26:18:538794 128.235.204.81:21 192.168.1.20:33056 tcp_rcv_established B P 2291929816 ack 516203543
97       19:26:18:539077 128.235.204.81:21 192.168.1.20:33056 tcp_event_data_recv B P 2291929816 ack 516203543
98       19:26:18:539362 128.235.204.81:21 192.168.1.20:33056 tcp_event_data_recv E P 2291929816 ack 516203543
99       19:26:18:539650 192.168.1.20:33056 128.235.204.81:21 tcp_send_ack B
100        19:26:18:539871 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb B
101          19:26:18:540093 present_window: NIL tcp_receive_window B
102          19:26:18:540093 present_window: 5807 tcp_receive_window E
103          19:26:18:540373 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window B
104          19:26:18:540599 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window E
105        19:26:18:540839 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb E . 516203543 ack 2291929849
106      19:26:18:541158 192.168.1.20:33056 128.235.204.81:21 tcp_send_ack E
107    19:26:18:541391 128.235.204.81:21 192.168.1.20:33056 tcp_rcv_established E P 2291929816 ack 516203543
108  19:26:18:541703 128.235.204.81:21 192.168.1.20:33056 tcp_v4_do_rcv E P 2291929816 ack 516203543
     Time : 3185
109  19:26:18:542020 present_window: NIL tcp_receive_window B
110  19:26:18:542020 present_window: 5840 tcp_receive_window E
     Time : 0
111  19:26:18:542321 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window B
112  19:26:18:542564 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window E
     Time : 243
113  19:26:21:378078 192.168.1.20:33056 128.235.204.81:21 tcp_sendmsg B
114    19:26:21:378334 192.168.1.20:33056 128.235.204.81:21 tcp_push B
115      19:26:21:378584 192.168.1.20:33056 128.235.204.81:21 __tcp_push_pending_frames B
116        19:26:21:378835 192.168.1.20:33056 128.235.204.81:21 tcp_write_xmit B
117          19:26:21:379090 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb B
118            19:26:21:379345 present_window: NIL tcp_receive_window B
119            19:26:21:379345 present_window: 5840 tcp_receive_window E
120            19:26:21:379670 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window B
121            19:26:21:379930 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window E
122          19:26:21:380214 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb E P 516203543 ack 2291929849
123        19:26:21:380583 192.168.1.20:33056 128.235.204.81:21 tcp_write_xmit E
124      19:26:21:380850 192.168.1.20:33056 128.235.204.81:21 __tcp_push_pending_frames E
125    19:26:21:381118 192.168.1.20:33056 128.235.204.81:21 tcp_push E
126  19:26:21:381388 192.168.1.20:33056 128.235.204.81:21 tcp_sendmsg E
     Time : 3310
127  19:26:21:399140 128.235.204.81:21 192.168.1.20:33056 tcp_v4_rcv B . 2291929849 ack 516203558
```

```
19:26:21:399512 128.235.204.81:21 192.168.1.20 __tcp_v4_lookup B
19:26:21:399753 128.235.204.81:21 192.168.1.20:33056 __tcp_v4_lookup E
19:26:21:400033 128.235.204.81:21 192.168.1.20:33056 tcp_v4_rcv E . 2291929849 ack 516203558
Time : 893
19:26:21:400543 128.235.204.81:21 192.168.1.20:33056 tcp_v4_do_rcv B . 2291929849 ack 516203558
19:26:21:400921 128.235.204.81:21 192.168.1.20:33056 tcp_rcv_established B . 2291929849 ack 516203558
19:26:21:401304 128.235.204.81:21 192.168.1.20:33056 tcp_ack B . 2291929849 ack 516203558
19:26:21:401691 128.235.204.81:21 192.168.1.20:33056 tcp_ack E . 2291929849 ack 516203558
19:26:21:402080 128.235.204.81:21 192.168.1.20:33056 tcp_rcv_established E . 2291929849 ack 516203558
19:26:21:402471 128.235.204.81:21 192.168.1.20:33056 tcp_v4_do_rcv E . 2291929849 ack 516203558
Time : 1928
19:26:21:466146 128.235.204.81:21 192.168.1.20:33056 tcp_v4_rcv B P 2291929849 ack 516203558
19:26:21:466546 128.235.204.81:21 192.168.1.20 __tcp_v4_lookup B
19:26:21:466808 128.235.204.81:21 192.168.1.20:33056 __tcp_v4_lookup E
19:26:21:467112 128.235.204.81:21 192.168.1.20:33056 tcp_v4_rcv E P 2291929849 ack 516203558
Time : 966
19:26:21:467644 128.235.204.81:21 192.168.1.20:33056 tcp_v4_do_rcv B P 2291929849 ack 516203558
19:26:21:468055 128.235.204.81:21 192.168.1.20:33056 tcp_rcv_established B P 2291929849 ack 516203558
19:26:21:468471 128.235.204.81:21 192.168.1.20:33056 tcp_event_data_recv B P 2291929849 ack 516203558
19:26:21:468890 128.235.204.81:21 192.168.1.20:33056 tcp_event_data_recv E P 2291929849 ack 516203558
19:26:21:469311 192.168.1.20:33056 128.235.204.81:21 tcp_send_ack B
19:26:21:469632 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb B
19:26:21:469954 present_window: NIL tcp_receive_window B
19:26:21:469954 present_window: 5814 tcp_receive_window E
19:26:21:470361 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window B
19:26:21:470687 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window E
19:26:21:471026 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb E . 516203558 ack 2291929875
19:26:21:471479 192.168.1.20:33056 128.235.204.81:21 tcp_send_ack E
19:26:21:471812 128.235.204.81:21 192.168.1.20:33056 tcp_rcv_established E P 2291929849 ack 516203558
19:26:21:472258 128.235.204.81:21 192.168.1.20:33056 tcp_v4_do_rcv E P 2291929849 ack 516203558
Time : 4614
19:26:21:472708 present_window: NIL tcp_receive_window B
19:26:21:472708 present_window: 5840 tcp_receive_window E
Time : 0
19:26:21:473137 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window B
19:26:21:473479 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window E
Time : 342
```

```
19:26:21:473937 192.168.1.20:33056 128.235.204.81:21 tcp_sendmsg B
   19:26:21:474287 192.168.1.20:33056 128.235.204.81:21 tcp_push B
      19:26:21:474637 192.168.1.20:33056 128.235.204.81:21 __tcp_push_pending_frames B
         19:26:21:474987 192.168.1.20:33056 128.235.204.81:21 tcp_write_xmit B
            19:26:21:475341 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb B
               19:26:21:475695 present_window: NIL tcp_receive_window B
               19:26:21:475695 present_window: 5840 tcp_receive_window E
               19:26:21:476145 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window B
               19:26:21:476504 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window E
            19:26:21:476870 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb E P 516203558 ack 2291929875
         19:26:21:477368 192.168.1.20:33056 128.235.204.81:21 tcp_write_xmit E
      19:26:21:477735 192.168.1.20:33056 128.235.204.81:21 __tcp_push_pending_frames E
   19:26:21:478103 192.168.1.20:33056 128.235.204.81:21 tcp_push E
19:26:21:478473 192.168.1.20:33056 128.235.204.81:21 tcp_sendmsg E
Time : 4536
19:26:21:497925 128.235.204.81:21 192.168.1.20:33056 tcp_v4_rcv B P 2291929875 ack 516203564
   19:26:21:498431 128.235.204.81:21 192.168.1.20 __tcp_v4_lookup B
   19:26:21:498759 128.235.204.81:21 192.168.1.20:33056 __tcp_v4_lookup E
19:26:21:499139 128.235.204.81:21 192.168.1.20:33056 tcp_v4_rcv E P 2291929875 ack 516203564
Time : 1214
19:26:21:499782 128.235.204.81:21 192.168.1.20:33056 tcp_v4_do_rcv B P 2291929875 ack 516203564
   19:26:21:500294 128.235.204.81:21 192.168.1.20:33056 tcp_rcv_established B P 2291929875 ack 516203564
      19:26:21:500811 128.235.204.81:21 192.168.1.20:33056 tcp_event_data_recv B P 2291929875 ack 516203564
      19:26:21:501330 128.235.204.81:21 192.168.1.20:33056 tcp_event_data_recv E P 2291929875 ack 516203564
      19:26:21:501851 128.235.204.81:21 192.168.1.20:33056 tcp_ack B P 2291929875 ack 516203564
      19:26:21:502378 128.235.204.81:21 192.168.1.20:33056 tcp_ack E P 2291929875 ack 516203564
      19:26:21:502907 192.168.1.20:33056 128.235.204.81:21 tcp_send_delayed_ack B
      19:26:21:503307 192.168.1.20:33056 128.235.204.81:21 tcp_send_delayed_ack E
   19:26:21:503724 128.235.204.81:21 192.168.1.20:33056 tcp_rcv_established E P 2291929875 ack 516203564
19:26:21:504261 128.235.204.81:21 192.168.1.20:33056 tcp_v4_do_rcv E P 2291929875 ack 516203564
Time : 4479
19:26:21:504812 present_window: NIL tcp_receive_window B
19:26:21:504812 present_window: 5806 tcp_receive_window E
Time : 0
19:26:21:505328 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window B
19:26:21:505741 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window E
Time : 413
```

```
19:26:21:533535 192.168.1.20:33056 128.235.204.81:21 tcp_send_ack B
   19:26:21:533956 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb B
      19:26:21:534376 present_window: NIL tcp_receive_window B
      19:26:21:534376 present_window: 5806 tcp_receive_window E
      19:26:21:534907 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window B
      19:26:21:535330 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window E
   19:26:21:535778 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb E . 516203564 ack 2291929909
19:26:21:536363 192.168.1.20:33056 128.235.204.81:21 tcp_send_ack E
Time : 2828
19:26:25:493737 192.168.1.20:33056 128.235.204.81:21 tcp_sendmsg B
   19:26:25:494179 192.168.1.20:33056 128.235.204.81:21 tcp_push B
      19:26:25:494613 192.168.1.20:33056 128.235.204.81:21 __tcp_push_pending_frames B
         19:26:25:495049 192.168.1.20:33056 128.235.204.81:21 tcp_write_xmit B
            19:26:25:495489 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb B
               19:26:25:495929 present_window: NIL tcp_receive_window B
               19:26:25:495929 present_window: 5840 tcp_receive_window E
               19:26:25:496487 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window B
               19:26:25:496932 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window E
            19:26:25:497400 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb E P 516203564 ack 2291929909
         19:26:25:498015 192.168.1.20:33056 128.235.204.81:21 tcp_write_xmit E
      19:26:25:498466 192.168.1.20:33056 128.235.204.81:21 __tcp_push_pending_frames E
   19:26:25:498919 192.168.1.20:33056 128.235.204.81:21 tcp_push E
19:26:25:499374 192.168.1.20:33056 128.235.204.81:21 tcp_sendmsg E
Time : 5637
19:26:25:521563 128.235.204.81:21 192.168.1.20:33056 tcp_v4_rcv B P 2291929909 ack 516203572
   19:26:25:522182 128.235.204.81:21 192.168.1.20 __tcp_v4_lookup B
   19:26:25:522584 128.235.204.81:21 192.168.1.20:33056 __tcp_v4_lookup E
19:26:25:523049 128.235.204.81:21 192.168.1.20:33056 tcp_v4_rcv E P 2291929909 ack 516203572
Time : 1486
19:26:25:523826 128.235.204.81:21 192.168.1.20:33056 tcp_v4_do_rcv B P 2291929909 ack 516203572
   19:26:25:524451 128.235.204.81:21 192.168.1.20:33056 tcp_rcv_established B P 2291929909 ack 516203572
      19:26:25:525082 128.235.204.81:21 192.168.1.20:33056 tcp_event_data_recv B P 2291929909 ack 516203572
      19:26:25:525714 128.235.204.81:21 192.168.1.20:33056 tcp_event_data_recv E P 2291929909 ack 516203572
      19:26:25:526348 128.235.204.81:21 192.168.1.20:33056 tcp_ack B P 2291929909 ack 516203572
      19:26:25:526988 128.235.204.81:21 192.168.1.20:33056 tcp_ack E P 2291929909 ack 516203572
      19:26:25:527630 192.168.1.20:33056 128.235.204.81:21 tcp_send_ack B
         19:26:25:528115 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb B
```

```
225              19:26:25:528602 present_window: NIL tcp_receive_window B
226              19:26:25:528602 present_window: 5820 tcp_receive_window E
227              19:26:25:529218 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window B
228              19:26:25:529710 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window E
229            19:26:25:530213 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb E . 516203572 ack 2291929929
230          19:26:25:530886 192.168.1.20:33056 128.235.204.81:21 tcp_send_ack E
231       19:26:25:531385 128.235.204.81:21 192.168.1.20:33056 tcp_rcv_established E P 2291929909 ack 516203572
232    19:26:25:532050 128.235.204.81:21 192.168.1.20:33056 tcp_v4_do_rcv E P 2291929909 ack 516203572
       Time : 8224
233    19:26:25:532722 present_window: NIL tcp_receive_window B
234    19:26:25:532722 present_window: 5840 tcp_receive_window E
       Time : 0
235    19:26:25:533359 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window B
236    19:26:25:533885 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window E
       Time : 526
237    19:26:25:534495 0.0.0.0:0 0.0.0.0:0 tcp_v4_init_sock B
238    19:26:25:535006 0.0.0.0:0 0.0.0.0:0 tcp_v4_init_sock E
       Time : 511
239    19:26:25:535529 192.168.1.20:33056 128.235.204.81:21 tcp_sendmsg B
240       19:26:25:536047 192.168.1.20:33056 128.235.204.81:21 tcp_push B
241          19:26:25:536564 192.168.1.20:33056 128.235.204.81:21 __tcp_push_pending_frames B
242             19:26:25:537083 192.168.1.20:33056 128.235.204.81:21 tcp_write_xmit B
243                19:26:25:537605 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb B
244                   19:26:25:538127 present_window: NIL tcp_receive_window B
245                   19:26:25:538127 present_window: 5840 tcp_receive_window E
246                   19:26:25:538789 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window B
247                   19:26:25:539317 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window E
248                19:26:25:539850 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb E P 516203572 ack 2291929929
249             19:26:25:540573 192.168.1.20:33056 128.235.204.81:21 tcp_write_xmit E
250          19:26:25:541108 192.168.1.20:33056 128.235.204.81:21 __tcp_push_pending_frames E
251       19:26:25:541644 192.168.1.20:33056 128.235.204.81:21 tcp_push E
252    19:26:25:542182 192.168.1.20:33056 128.235.204.81:21 tcp_sendmsg E
       Time : 6653
253    19:26:25:566098 128.235.204.81:21 192.168.1.20:33056 tcp_v4_rcv B P 2291929929 ack 516203578
254       19:26:25:566825 128.235.204.81:21 192.168.1.20 __tcp_v4_lookup B
255       19:26:25:567298 128.235.204.81:21 192.168.1.20:33056 __tcp_v4_lookup E
256    19:26:25:567846 128.235.204.81:21 192.168.1.20:33056 tcp_v4_rcv E P 2291929929 ack 516203578
```

```
    Time : 1748
257  19:26:25:568595 128.235.204.81:21 192.168.1.20:33056 tcp_v4_do_rcv B P 2291929929 ack 516203578
258     19:26:25:569331 128.235.204.81:21 192.168.1.20:33056 tcp_rcv_established B P 2291929929 ack 516203578
259        19:26:25:570074 128.235.204.81:21 192.168.1.20:33056 tcp_event_data_recv B P 2291929929 ack 516203578
260        19:26:25:570816 128.235.204.81:21 192.168.1.20:33056 tcp_event_data_recv E P 2291929929 ack 516203578
261        19:26:25:571561 128.235.204.81:21 192.168.1.20:33056 tcp_ack B P 2291929929 ack 516203578
262        19:26:25:572312 128.235.204.81:21 192.168.1.20:33056 tcp_ack E P 2291929929 ack 516203578
263        19:26:25:573065 192.168.1.20:33056 128.235.204.81:21 tcp_send_delayed_ack B
264        19:26:25:573645 192.168.1.20:33056 128.235.204.81:21 tcp_send_delayed_ack E
265     19:26:25:574215 128.235.204.81:21 192.168.1.20:33056 tcp_rcv_established E P 2291929929 ack 516203578
266  19:26:25:574977 128.235.204.81:21 192.168.1.20:33056 tcp_v4_do_rcv E P 2291929929 ack 516203578
    Time : 6382
267  19:26:25:575747 present_window: NIL tcp_receive_window B
268  19:26:25:575747 present_window: 5789 tcp_receive_window E
    Time : 0
269  19:26:25:576476 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window B
270  19:26:25:577055 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window E
    Time : 579
271  19:26:25:577724 0.0.0.0:0 0.0.0.0:0 tcp_v4_connect B
272     19:26:25:578309 192.168.1.20:0 128.235.204.81:17029 tcp_set_state B
273     19:26:25:578894 192.168.1.20:0 128.235.204.81:17029 tcp_set_state E
274     19:26:25:579485 192.168.1.20:33057 128.235.204.81:17029 tcp_connect B
275        19:26:25:580076 192.168.1.20:33057 128.235.204.81:17029 tcp_transmit_skb B
276        19:26:25:580677 192.168.1.20:33057 128.235.204.81:17029 tcp_transmit_skb E S 511926496 ack 0
277     19:26:25:581481 192.168.1.20:33057 128.235.204.81:17029 tcp_connect E
278  19:26:25:582076 192.168.1.20:33057 128.235.204.81:17029 tcp_v4_connect E
    Time : 4352
279  19:26:25:604474 128.235.204.81:17029 192.168.1.20:33057 tcp_v4_rcv B S 2256768592 ack 511926497
280     19:26:25:605281 128.235.204.81:17029 192.168.1.20 __tcp_v4_lookup B
281     19:26:25:605804 128.235.204.81:17029 192.168.1.20:33057 __tcp_v4_lookup E
282     19:26:25:606409 128.235.204.81:17029 192.168.1.20:33057 tcp_v4_do_rcv B S 2256768592 ack 511926497
283        19:26:25:607219 192.168.1.20:33057 128.235.204.81:17029 tcp_rcv_state_process B
284           19:26:25:607829 192.168.1.20:33057 128.235.204.81:17029 tcp_rcv_synsent_state_process B S 2256768592 ack 511926497
285              19:26:25:608687 128.235.204.81:17029 192.168.1.20:33057 tcp_ack B S 2256768592 ack 511926497
286              19:26:25:609510 128.235.204.81:17029 192.168.1.20:33057 tcp_ack E S 2256768592 ack 511926497
287              19:26:25:610334 192.168.1.20:33057 128.235.204.81:17029 tcp_set_state B
288              19:26:25:610953 192.168.1.20:33057 128.235.204.81:17029 tcp_set_state E
```

```
289             19:26:25:611575 192.168.1.20:33057 128.235.204.81:17029 tcp_send_ack B
290               19:26:25:612198 192.168.1.20:33057 128.235.204.81:17029 tcp_transmit_skb B
291                 19:26:25:612825 present_window: NIL tcp_receive_window B
292                 19:26:25:612825 present_window: 5840 tcp_receive_window E
293                 19:26:25:613630 192.168.1.20:33057 128.235.204.81:17029 __tcp_select_window B
294                 19:26:25:614261 192.168.1.20:33057 128.235.204.81:17029 __tcp_select_window E
295               19:26:25:614903 192.168.1.20:33057 128.235.204.81:17029 tcp_transmit_skb E . 511926497 ack 2256768593
296             19:26:25:615763 192.168.1.20:33057 128.235.204.81:17029 tcp_send_ack E
297           19:26:25:616400 192.168.1.20:33057 128.235.204.81:17029 tcp_rcv_synsent_state_process E S 2256768592 ack 511926497
298         19:26:25:617295 192.168.1.20:33057 128.235.204.81:17029 tcp_rcv_state_process E
299       19:26:25:617937 128.235.204.81:17029 192.168.1.20:33057 tcp_v4_do_rcv E S 2256768592 ack 511926497
300   19:26:25:618796 128.235.204.81:17029 192.168.1.20:33057 tcp_v4_rcv E S 2256768592 ack 511926497
      Time : 14322
301   19:26:25:619665 192.168.1.20:33056 128.235.204.81:21 tcp_send_ack B
302     19:26:25:620315 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb B
303       19:26:25:620966 present_window: NIL tcp_receive_window B
304       19:26:25:620966 present_window: 5789 tcp_receive_window E
305       19:26:25:621792 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window B
306       19:26:25:622449 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window E
307     19:26:25:623111 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb E . 516203578 ack 2291929980
308   19:26:25:624016 192.168.1.20:33056 128.235.204.81:21 tcp_send_ack E
      Time : 4351
309   19:26:25:624726 192.168.1.20:33057 128.235.204.81:17029 tcp_setsockopt B
310   19:26:25:625394 192.168.1.20:33057 128.235.204.81:17029 tcp_setsockopt E
      Time : 668
311   19:26:25:626085 192.168.1.20:33056 128.235.204.81:21 tcp_sendmsg B
312     19:26:25:626757 192.168.1.20:33056 128.235.204.81:21 tcp_push B
313       19:26:25:627429 192.168.1.20:33056 128.235.204.81:21 __tcp_push_pending_frames B
314         19:26:25:628103 192.168.1.20:33056 128.235.204.81:21 tcp_write_xmit B
315           19:26:25:628779 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb B
316             19:26:25:629456 present_window: NIL tcp_receive_window B
317             19:26:25:629456 present_window: 5840 tcp_receive_window E
318             19:26:25:630314 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window B
319             19:26:25:630996 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window E
320           19:26:25:631684 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb E P 516203578 ack 2291929980
321         19:26:25:632613 192.168.1.20:33056 128.235.204.81:21 tcp_write_xmit E
322       19:26:25:633302 192.168.1.20:33056 128.235.204.81:21 __tcp_push_pending_frames E
```

19:26:25:634005 192.168.1.20:33056 128.235.204.81:21 tcp_push E
19:26:25:634698 192.168.1.20:33056 128.235.204.81:21 tcp_sendmsg E
Time : 8613
19:26:25:677714 128.235.204.81:21 192.168.1.20:33056 tcp_v4_rcv B P 2291929980 ack 516203592
19:26:25:678644 128.235.204.81:21 192.168.1.20 __tcp_v4_lookup B
19:26:25:679251 128.235.204.81:21 192.168.1.20:33056 __tcp_v4_lookup E
19:26:25:679952 128.235.204.81:21 192.168.1.20:33056 tcp_v4_rcv E P 2291929980 ack 516203592
Time : 2238
19:26:25:680897 128.235.204.81:21 192.168.1.20:33056 tcp_v4_do_rcv B P 2291929980 ack 516203592
19:26:25:681839 128.235.204.81:21 192.168.1.20:33056 tcp_rcv_established B P 2291929980 ack 516203592
19:26:25:682787 128.235.204.81:21 192.168.1.20:33056 tcp_event_data_recv B P 2291929980 ack 516203592
19:26:25:683747 128.235.204.81:21 192.168.1.20:33056 tcp_event_data_recv E P 2291929980 ack 516203592
19:26:25:684699 128.235.204.81:21 192.168.1.20:33056 tcp_ack B P 2291929980 ack 516203592
19:26:25:685655 128.235.204.81:21 192.168.1.20:33056 tcp_ack E P 2291929980 ack 516203592
19:26:25:686614 192.168.1.20:33056 128.235.204.81:21 tcp_send_ack B
19:26:25:687335 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb B
19:26:25:688059 present_window: NIL tcp_receive_window B
19:26:25:688059 present_window: 5786 tcp_receive_window E
19:26:25:688975 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window B
19:26:25:689703 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window E
19:26:25:690438 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb E . 516203592 ack 2291930034
19:26:25:691427 192.168.1.20:33056 128.235.204.81:21 tcp_send_ack E
19:26:25:692163 128.235.204.81:21 192.168.1.20:33056 tcp_rcv_established E P 2291929980 ack 516203592
19:26:25:693146 128.235.204.81:21 192.168.1.20:33056 tcp_v4_do_rcv E P 2291929980 ack 516203592
Time : 12249
19:26:25:694151 present_window: NIL tcp_receive_window B
19:26:25:694151 present_window: 5840 tcp_receive_window E
Time : 0
19:26:25:695089 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window B
19:26:25:695835 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window E
Time : 746
19:26:25:696702 192.168.1.20:33057 128.235.204.81:17029 tcp_sendmsg B
19:26:25:697455 192.168.1.20:33057 128.235.204.81:17029 tcp_transmit_skb B
19:26:25:698207 present_window: NIL tcp_receive_window B
19:26:25:698207 present_window: 5840 tcp_receive_window E
19:26:25:699160 192.168.1.20:33057 128.235.204.81:17029 __tcp_select_window B
19:26:25:699917 192.168.1.20:33057 128.235.204.81:17029 __tcp_select_window E

```
19:26:25:700681 192.168.1.20:33057 128.235.204.81:17029 tcp_transmit_skb E . 511926497 ack 2256768593
19:26:25:701711 192.168.1.20:33057 128.235.204.81:17029 __tcp_push_pending_frames B
  19:26:25:702476 192.168.1.20:33057 128.235.204.81:17029 tcp_write_xmit B
    19:26:25:703243 192.168.1.20:33057 128.235.204.81:17029 tcp_transmit_skb B
      19:26:25:704023 present_window: NIL tcp_receive_window B
      19:26:25:704023 present_window: 5840 tcp_receive_window E
      19:26:25:704996 192.168.1.20:33057 128.235.204.81:17029 __tcp_select_window B
      19:26:25:705770 192.168.1.20:33057 128.235.204.81:17029 __tcp_select_window E
    19:26:25:706548 192.168.1.20:33057 128.235.204.81:17029 tcp_transmit_skb E P 511927187 ack 2256768593
  19:26:25:707598 192.168.1.20:33057 128.235.204.81:17029 tcp_write_xmit E
19:26:25:708379 192.168.1.20:33057 128.235.204.81:17029 __tcp_push_pending_frames E
19:26:25:709164 192.168.1.20:33057 128.235.204.81:17029 tcp_push B
  19:26:25:709949 192.168.1.20:33057 128.235.204.81:17029 __tcp_push_pending_frames B
  19:26:25:710735 192.168.1.20:33057 128.235.204.81:17029 __tcp_push_pending_frames E
19:26:25:711524 192.168.1.20:33057 128.235.204.81:17029 tcp_push E
19:26:25:712315 192.168.1.20:33057 128.235.204.81:17029 tcp_sendmsg E
Time : 15613
19:26:25:713124 192.168.1.20:33057 128.235.204.81:17029 tcp_close B
19:26:25:713937 192.168.1.20:33057 128.235.204.81:17029 tcp_close_state B
  19:26:25:714733 192.168.1.20:33057 128.235.204.81:17029 tcp_set_state B
  19:26:25:715533 192.168.1.20:33057 128.235.204.81:17029 tcp_set_state E
19:26:25:716333 192.168.1.20:33057 128.235.204.81:17029 tcp_close_state E
19:26:25:717136 192.168.1.20:33057 128.235.204.81:17029 tcp_send_fin B
  19:26:25:717940 192.168.1.20:33057 128.235.204.81:17029 __tcp_push_pending_frames B
  19:26:25:718747 192.168.1.20:33057 128.235.204.81:17029 __tcp_push_pending_frames E
19:26:25:719556 192.168.1.20:33057 128.235.204.81:17029 tcp_send_fin E
19:26:25:720368 192.168.1.20:33057 128.235.204.81:17029 tcp_close E
Time : 7244
19:26:25:786573 128.235.204.81:17029 192.168.1.20:33057 tcp_v4_rcv B . 2256768593 ack 511927187
19:26:25:787668 128.235.204.81:17029 192.168.1.20 __tcp_v4_lookup B
19:26:25:788378 128.235.204.81:17029 192.168.1.20:33057 __tcp_v4_lookup E
19:26:25:789199 128.235.204.81:17029 192.168.1.20:33057 tcp_v4_do_rcv B . 2256768593 ack 511927187
  19:26:25:790297 192.168.1.20:33057 128.235.204.81:17029 tcp_rcv_state_process B
    19:26:25:791122 present_window: NIL tcp_receive_window B
    19:26:25:791122 present_window: 5840 tcp_receive_window E
    19:26:25:792169 128.235.204.81:17029 192.168.1.20:33057 tcp_ack B . 2256768593 ack 511927187
      19:26:25:793280 CWND: 2 CWND CLAMP: 65535 CWND COUNT: 0 tcp_cong_avoid B
```

```
390             19:26:25:794178 CWND: 3 CWND CLAMP: 65535 CWND COUNT: 0 tcp_cong_avoid E
391           19:26:25:795066 128.235.204.81:17029 192.168.1.20:33057 tcp_ack E . 2256768593 ack 511927187
392           19:26:25:796181 128.235.204.81:17029 192.168.1.20:33057 tcp_data_queue B . 2256768593 ack 511927187
393           19:26:25:797300 128.235.204.81:17029 192.168.1.20:33057 tcp_data_queue E . 2256768593 ack 511927187
394           19:26:25:798422 128.235.204.81:17029 192.168.1.20:33057 __tcp_data_snd_check B
395             19:26:25:799268 192.168.1.20:33057 128.235.204.81:17029 tcp_write_xmit B
396               19:26:25:800116 192.168.1.20:33057 128.235.204.81:17029 tcp_transmit_skb B
397                 19:26:25:800966 present_window: NIL tcp_receive_window B
398                 19:26:25:800966 present_window: 5840 tcp_receive_window E
399                 19:26:25:802041 192.168.1.20:33057 128.235.204.81:17029 __tcp_select_window B
400                 19:26:25:802896 192.168.1.20:33057 128.235.204.81:17029 __tcp_select_window E
401               19:26:25:803774 192.168.1.20:33057 128.235.204.81:17029 tcp_transmit_skb E . 511927877 ack 2256768593
402             19:26:25:804932 192.168.1.20:33057 128.235.204.81:17029 tcp_write_xmit E
403           19:26:25:805793 128.235.204.81:17029 192.168.1.20:33057 __tcp_data_snd_check E
404         19:26:25:806656 192.168.1.20:33057 128.235.204.81:17029 tcp_rcv_state_process E
405       19:26:25:807520 128.235.204.81:17029 192.168.1.20:33057 tcp_v4_do_rcv E . 511927877 ack 2256768593
406     19:26:25:808677 192.168.1.20:33057 128.235.204.81:17029 tcp_v4_rcv E . 511927877 ack 2256768593
    Time : 22104
407     19:26:25:814110 128.235.204.81:17029 192.168.1.20:33057 tcp_v4_rcv B . 2256768593 ack 511927877
408       19:26:25:815274 128.235.204.81:17029 192.168.1.20 __tcp_v4_lookup B
409       19:26:25:816033 128.235.204.81:17029 192.168.1.20:33057 __tcp_v4_lookup E
410       19:26:25:816910 128.235.204.81:17029 192.168.1.20:33057 tcp_v4_do_rcv B . 2256768593 ack 511927877
411         19:26:25:818083 192.168.1.20:33057 128.235.204.81:17029 tcp_rcv_state_process B
412           19:26:25:818965 present_window: NIL tcp_receive_window B
413           19:26:25:818965 present_window: 5840 tcp_receive_window E
414           19:26:25:820082 128.235.204.81:17029 192.168.1.20:33057 tcp_ack B . 2256768593 ack 511927877
415           19:26:25:821267 128.235.204.81:17029 192.168.1.20:33057 tcp_ack E . 2256768593 ack 511927877
416           19:26:25:822453 128.235.204.81:17029 192.168.1.20:33057 tcp_data_queue B . 2256768593 ack 511927877
417           19:26:25:823654 128.235.204.81:17029 192.168.1.20:33057 tcp_data_queue E . 2256768593 ack 511927877
418           19:26:25:824847 128.235.204.81:17029 192.168.1.20:33057 __tcp_data_snd_check B
419             19:26:25:825745 192.168.1.20:33057 128.235.204.81:17029 tcp_write_xmit B
420               19:26:25:826645 192.168.1.20:33057 128.235.204.81:17029 tcp_transmit_skb B
421                 19:26:25:827547 present_window: NIL tcp_receive_window B
422                 19:26:25:827547 present_window: 5840 tcp_receive_window E
423                 19:26:25:828690 192.168.1.20:33057 128.235.204.81:17029 __tcp_select_window B
424                 19:26:25:829597 192.168.1.20:33057 128.235.204.81:17029 __tcp_select_window E
425               19:26:25:830509 192.168.1.20:33057 128.235.204.81:17029 tcp_transmit_skb E F 511928567 ack 2256768593
```

19:26:25:831736 192.168.1.20:33057 128.235.204.81:17029 tcp_write_xmit E
19:26:25:832650 128.235.204.81:17029 192.168.1.20:33057 __tcp_data_snd_check E
19:26:25:833578 192.168.1.20:33057 128.235.204.81:17029 tcp_rcv_state_process E
19:26:25:834496 128.235.204.81:17029 192.168.1.20:33057 tcp_v4_do_rcv E P 511928567 ack 2256768593
19:26:25:835723 192.168.1.20:33057 128.235.204.81:17029 tcp_v4_rcv E P 511928567 ack 2256768593
Time : 21613
19:26:25:905813 128.235.204.81:17029 192.168.1.20:33057 tcp_v4_rcv B . 2256768593 ack 511929224
19:26:25:907051 128.235.204.81:17029 192.168.1.20 __tcp_v4_lookup B
19:26:25:907856 128.235.204.81:17029 192.168.1.20:33057 __tcp_v4_lookup E
19:26:25:908787 128.235.204.81:17029 192.168.1.20:33057 tcp_v4_do_rcv B . 2256768593 ack 511929224
19:26:25:910030 192.168.1.20:33057 128.235.204.81:17029 tcp_rcv_state_process B
19:26:25:910965 present_window: NIL tcp_receive_window B
19:26:25:910965 present_window: 5840 tcp_receive_window E
19:26:25:912150 128.235.204.81:17029 192.168.1.20:33057 tcp_ack B . 2256768593 ack 511929224
19:26:25:913407 128.235.204.81:17029 192.168.1.20:33057 tcp_ack E . 2256768593 ack 511929224
19:26:25:914677 192.168.1.20:33057 128.235.204.81:17029 tcp_set_state B
19:26:25:915623 192.168.1.20:33057 128.235.204.81:17029 tcp_set_state E
19:26:25:916570 192.168.1.20:33057 128.235.204.81:17029 tcp_time_wait B
19:26:25:917520 present_window: NIL tcp_receive_window B
19:26:25:917520 present_window: 5840 tcp_receive_window E
19:26:25:918724 192.168.1.20:33057 128.235.204.81:17029 tcp_set_state B
19:26:25:919679 192.168.1.20:33057 128.235.204.81:17029 tcp_set_state E
19:26:25:920637 192.168.1.20:33057 128.235.204.81:17029 tcp_time_wait E
19:26:25:921595 192.168.1.20:33057 128.235.204.81:17029 tcp_rcv_state_process E
19:26:25:922554 128.235.204.81:17029 192.168.1.20:33057 tcp_v4_do_rcv E . 2256768593 ack 511929224
19:26:25:923851 128.235.204.81:17029 192.168.1.20:33057 tcp_v4_rcv E . 2256768593 ack 511929224
Time : 18038
19:26:25:925183 128.235.204.81:17029 192.168.1.20:33057 tcp_v4_rcv B F 2256768593 ack 511929224
19:26:25:926474 128.235.204.81:17029 192.168.1.20 __tcp_v4_lookup B
19:26:25:927316 128.235.204.81:17029 135.3.0.0:33057 __tcp_v4_lookup E
19:26:25:928302 128.235.204.81:17029 192.168.1.20:33057 tcp_v4_rcv E F 2256768593 ack 511929224
Time : 3119
19:26:25:929618 128.235.204.81:21 192.168.1.20:33056 tcp_v4_rcv B P 2291930034 ack 516203592
19:26:25:930919 128.235.204.81:21 192.168.1.20 __tcp_v4_lookup B
19:26:25:931769 128.235.204.81:21 192.168.1.20:33056 __tcp_v4_lookup E
19:26:25:932751 128.235.204.81:21 192.168.1.20:33056 tcp_v4_rcv E P 2291930034 ack 516203592
Time : 3133

```
19:26:25:934100 128.235.204.81:21 192.168.1.20:33056 tcp_v4_do_rcv B P 2291930034 ack 516203592
  19:26:25:935414 128.235.204.81:21 192.168.1.20:33056 tcp_rcv_established B P 2291930034 ack 516203592
    19:26:25:936736 128.235.204.81:21 192.168.1.20:33056 tcp_event_data_recv B P 2291930034 ack 516203592
    19:26:25:938058 128.235.204.81:21 192.168.1.20:33056 tcp_event_data_recv E P 2291930034 ack 516203592
    19:26:25:939383 192.168.1.20:33056 128.235.204.81:21 tcp_send_ack B
      19:26:25:940381 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb B
        19:26:25:941380 present_window: NIL tcp_receive_window B
        19:26:25:941380 present_window: 5816 tcp_receive_window E
        19:26:25:942645 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window B
        19:26:25:943662 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window E
      19:26:25:944672 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb E . 516203592 ack 2291930058
    19:26:25:946028 192.168.1.20:33056 128.235.204.81:21 tcp_send_ack E
  19:26:25:947039 128.235.204.81:21 192.168.1.20:33056 tcp_rcv_established E P 2291930034 ack 516203592
19:26:25:948389 128.235.204.81:21 192.168.1.20:33056 tcp_v4_do_rcv E P 2291930034 ack 516203592
Time : 14289
19:26:25:949750 present_window: NIL tcp_receive_window B
19:26:25:949750 present_window: 5840 tcp_receive_window E
Time : 0
19:26:25:951037 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window B
19:26:25:952057 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window E
Time : 1020
19:26:27:935582 192.168.1.20:33056 128.235.204.81:21 tcp_sendmsg B
  19:26:27:936618 192.168.1.20:33056 128.235.204.81:21 tcp_push B
    19:26:27:937646 192.168.1.20:33056 128.235.204.81:21 __tcp_push_pending_frames B
      19:26:27:938675 192.168.1.20:33056 128.235.204.81:21 tcp_write_xmit B
        19:26:27:939708 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb B
          19:26:27:940742 present_window: NIL tcp_receive_window B
          19:26:27:940742 present_window: 5840 tcp_receive_window E
          19:26:27:942051 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window B
          19:26:27:943089 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window E
        19:26:27:944177 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb E P 516203592 ack 2291930058
      19:26:27:945583 192.168.1.20:33056 128.235.204.81:21 tcp_write_xmit E
    19:26:27:946627 192.168.1.20:33056 128.235.204.81:21 __tcp_push_pending_frames E
  19:26:27:947673 192.168.1.20:33056 128.235.204.81:21 tcp_push E
19:26:27:948721 192.168.1.20:33056 128.235.204.81:21 tcp_sendmsg E
Time : 13139
19:26:27:967999 128.235.204.81:21 192.168.1.20:33056 tcp_v4_rcv B P 2291930058 ack 516203598
```

```
19:26:27:969407 128.235.204.81:21 192.168.1.20 __tcp_v4_lookup B
19:26:27:970323 128.235.204.81:21 192.168.1.20:33056 __tcp_v4_lookup E
19:26:27:971382 128.235.204.81:21 192.168.1.20:33056 tcp_v4_rcv E P 2291930058 ack 516203598
Time : 3383
19:26:27:972830 128.235.204.81:21 192.168.1.20:33056 tcp_v4_rcv B P 2291930107 ack 516203598
19:26:27:974257 128.235.204.81:21 192.168.1.20 __tcp_v4_lookup B
19:26:27:975179 128.235.204.81:21 192.168.1.20:33056 __tcp_v4_lookup E
19:26:27:976244 128.235.204.81:21 192.168.1.20:33056 tcp_v4_rcv E P 2291930107 ack 516203598
Time : 3414
19:26:27:977810 128.235.204.81:21 192.168.1.20:33056 tcp_v4_do_rcv B P 2291930058 ack 516203598
19:26:27:979238 128.235.204.81:21 192.168.1.20:33056 tcp_rcv_established B P 2291930058 ack 516203598
19:26:27:980673 128.235.204.81:21 192.168.1.20:33056 tcp_event_data_recv B P 2291930058 ack 516203598
19:26:27:982108 128.235.204.81:21 192.168.1.20:33056 tcp_event_data_recv E P 2291930058 ack 516203598
19:26:27:983558 128.235.204.81:21 192.168.1.20:33056 tcp_ack B P 2291930058 ack 516203598
19:26:27:985001 128.235.204.81:21 192.168.1.20:33056 tcp_ack E P 2291930058 ack 516203598
19:26:27:986446 192.168.1.20:33056 128.235.204.81:21 tcp_send_ack B
19:26:27:987534 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb B
19:26:27:988623 present_window: NIL tcp_receive_window B
19:26:27:988623 present_window: 5791 tcp_receive_window E
19:26:27:990003 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window B
19:26:27:991096 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window E
19:26:27:992202 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb E . 516203598 ack 2291930107
19:26:27:993691 192.168.1.20:33056 128.235.204.81:21 tcp_send_ack E
19:26:27:994791 128.235.204.81:21 192.168.1.20:33056 tcp_rcv_established E P 2291930058 ack 516203598
19:26:27:996260 128.235.204.81:21 192.168.1.20:33056 tcp_v4_do_rcv E P 2291930058 ack 516203598
Time : 18450
19:26:27:997733 128.235.204.81:21 192.168.1.20:33056 tcp_v4_do_rcv B P 2291930107 ack 516203598
19:26:27:999209 128.235.204.81:21 192.168.1.20:33056 tcp_rcv_established B P 2291930107 ack 516203598
19:26:28:000695 present_window: NIL tcp_receive_window B
19:26:28:000695 present_window: 5840 tcp_receive_window E
19:26:28:002103 128.235.204.81:21 192.168.1.20:33056 tcp_ack B P 2291930107 ack 516203598
19:26:28:003603 128.235.204.81:21 192.168.1.20:33056 tcp_ack E P 2291930107 ack 516203598
19:26:28:005093 128.235.204.81:21 192.168.1.20:33056 tcp_data_queue B P 2291930107 ack 516203598
19:26:28:006586 present_window: NIL tcp_receive_window B
19:26:28:006586 present_window: 5840 tcp_receive_window E
19:26:28:008008 128.235.204.81:21 192.168.1.20:33056 tcp_event_data_recv B P 2291930107 ack 516203598
19:26:28:009510 128.235.204.81:21 192.168.1.20:33056 tcp_event_data_recv E P 2291930107 ack 516203598
```

```
526           19:26:28:011015 192.168.1.20:33056 128.235.204.81:21 tcp_fin B P 2291930107 ack 516203598
527             19:26:28:012600 192.168.1.20:33056 128.235.204.81:21 tcp_set_state B
528             19:26:28:013746 192.168.1.20:33056 128.235.204.81:21 tcp_set_state E
529           19:26:28:014882 192.168.1.20:33056 128.235.204.81:21 tcp_fin E P 2291930107 ack 516203598
530         19:26:28:016474 128.235.204.81:21 192.168.1.20:33056 tcp_data_queue E P 2291930107 ack 516203598
531         19:26:28:017995 128.235.204.81:21 192.168.1.20:33056 __tcp_ack_snd_check B
532           19:26:28:019138 192.168.1.20:33056 128.235.204.81:21 tcp_send_delayed_ack B
533           19:26:28:020299 192.168.1.20:33056 128.235.204.81:21 tcp_send_delayed_ack E
534         19:26:28:021446 128.235.204.81:21 192.168.1.20:33056 __tcp_ack_snd_check E
535       19:26:28:022594 128.235.204.81:21 192.168.1.20:33056 tcp_rcv_established E P 2291930107 ack 516203598
536     19:26:28:024141 128.235.204.81:21 192.168.1.20:33056 tcp_v4_do_rcv E P 2291930107 ack 516203598
      Time : 26408
537     19:26:28:025799 192.168.1.20:33056 128.235.204.81:21 tcp_close B
538       19:26:28:026956 192.168.1.20:33056 128.235.204.81:21 tcp_close_state B
539         19:26:28:028115 192.168.1.20:33056 128.235.204.81:21 tcp_set_state B
540         19:26:28:029275 192.168.1.20:33056 128.235.204.81:21 tcp_set_state E
541       19:26:28:030437 192.168.1.20:33056 128.235.204.81:21 tcp_close_state E
542       19:26:28:031601 192.168.1.20:33056 128.235.204.81:21 tcp_send_fin B
543         19:26:28:032768 192.168.1.20:33056 128.235.204.81:21 __tcp_push_pending_frames B
544           19:26:28:033949 192.168.1.20:33056 128.235.204.81:21 tcp_write_xmit B
545             19:26:28:035120 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb B
546               19:26:28:036292 present_window: NIL tcp_receive_window B
547               19:26:28:036292 present_window: 5695 tcp_receive_window E
548               19:26:28:037777 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window B
549               19:26:28:038955 192.168.1.20:33056 128.235.204.81:21 __tcp_select_window E
550             19:26:28:040138 192.168.1.20:33056 128.235.204.81:21 tcp_transmit_skb E F 516203598 ack 2291930252
551           19:26:28:041727 192.168.1.20:33056 128.235.204.81:21 tcp_write_xmit E
552         19:26:28:042912 192.168.1.20:33056 128.235.204.81:21 __tcp_push_pending_frames E
553       19:26:28:044117 192.168.1.20:33056 128.235.204.81:21 tcp_send_fin E
554     19:26:28:045305 192.168.1.20:33056 128.235.204.81:21 tcp_close E
      Time : 19506
555     19:26:28:059368 128.235.204.81:21 192.168.1.20:33056 tcp_v4_rcv B . 2291930252 ack 516203599
556       19:26:28:060967 128.235.204.81:21 192.168.1.20 __tcp_v4_lookup B
557       19:26:28:062003 128.235.204.81:21 192.168.1.20:33056 __tcp_v4_lookup E
558       19:26:28:063200 128.235.204.81:21 192.168.1.20:33056 tcp_v4_do_rcv B . 2291930252 ack 516203599
559         19:26:28:064810 192.168.1.20:33056 128.235.204.81:21 tcp_rcv_state_process B
560           19:26:28:066012 present_window: NIL tcp_receive_window B
```

19:26:28:066012 present_window: 5840 tcp_receive_window E
19:26:28:067535 128.235.204.81:21 192.168.1.20:33056 tcp_ack B . 2291930252 ack 516203599
19:26:28:069147 128.235.204.81:21 192.168.1.20:33056 tcp_ack E . 2291930252 ack 516203599
19:26:28:070760 192.168.1.20:33056 128.235.204.81:21 tcp_set_state B
19:26:28:071973 192.168.1.20:33056 128.235.204.81:21 tcp_set_state E
19:26:28:073187 192.168.1.20:33056 128.235.204.81:21 tcp_rcv_state_process E
19:26:28:074413 128.235.204.81:21 192.168.1.20:33056 tcp_v4_do_rcv E . 2291930252 ack 516203599
19:26:28:076036 128.235.204.81:21 192.168.1.20:33056 tcp_v4_rcv E . 2291930252 ack 516203599
Time : 16668

12.23.2 DUMP_TCP

1 19:26:16.397248 gyan.home.32775 > home5.bellatlantic.net.domain: 40978+ AAAA? afs1.njit.edu. (31) (DF)
2 19:26:16.416855 home5.bellatlantic.net.domain > gyan.home.32775: 40978 1/1/0 CNAME alizarin.njit.edu. (106) (DF)
3 19:26:16.417182 gyan.home.32775 > home5.bellatlantic.net.domain: 40979+ A? afs1.njit.edu. (31) (DF)
4 19:26:16.439328 home5.bellatlantic.net.domain > gyan.home.32775: 40979 2/3/3 CNAME alizarin.njit.edu.[|domain] (DF)
5 19:26:16.439688 gyan.home.32775 > home5.bellatlantic.net.domain: 7159+ PTR? 81.204.235.128.in-addr.arpa. (45) (DF)
6 19:26:16.459998 home5.bellatlantic.net.domain > gyan.home.32775: 7159 1/3/3 (188) (DF)
7 19:26:16.460581 gyan.home.33056 > alizarin.njit.edu.ftp: S 516203531:516203531(0) win 5840 <mss 1460,sackOK,timestamp 197744 0,nop,wscale 0> (DF)
8 19:26:16.482074 alizarin.njit.edu.ftp > gyan.home.33056: S 2291929751:2291929751(0) ack 516203532 win 1380 <nop,nop,timestamp 4949179 197744,mss 1380,nop,wscale 0,nop,nop,sackOK> (DF)
9 19:26:16.482786 gyan.home.33056 > alizarin.njit.edu.ftp: . ack 2291929752 win 5840 <nop,nop,timestamp 197746 4949179> (DF)
10 19:26:16.524982 alizarin.njit.edu.ftp > gyan.home.33056: P 2291929752:2291929816(64) ack 516203532 win 2760 <nop,nop,timestamp 4949183 197746> (DF)
11 19:26:16.527600 gyan.home.33056 > alizarin.njit.edu.ftp: . ack 2291929816 win 5840 <nop,nop,timestamp 197751 4949183> (DF) [tos 0x10]
12 19:26:18.509066 gyan.home.33056 > alizarin.njit.edu.ftp: P 516203532:516203543(11) ack 2291929816 win 5840 <nop,nop,timestamp 197949 4949183> (DF) [tos 0x10]
13 19:26:18.529365 alizarin.njit.edu.ftp > gyan.home.33056: . ack 516203543 win 2760 <nop,nop,timestamp 4949384 197949> (DF)
14 19:26:18.537477 alizarin.njit.edu.ftp > gyan.home.33056: P 2291929816:2291929849(33) ack 516203543 win 2760 <nop,nop,timestamp 4949385 197949> (DF)
15 19:26:18.540835 gyan.home.33056 > alizarin.njit.edu.ftp: . ack 2291929849 win 5840 <nop,nop,timestamp 197952 4949385> (DF) [tos 0x10]
16 19:26:21.380205 gyan.home.33056 > alizarin.njit.edu.ftp: P 516203543:516203558(15) ack 2291929849 win 5840 <nop,nop,timestamp 198236 4949385> (DF) [tos 0x10]
17 19:26:21.399122 alizarin.njit.edu.ftp > gyan.home.33056: . ack 516203558 win 2760 <nop,nop,timestamp 4949671 198236> (DF)
18 19:26:21.466135 alizarin.njit.edu.ftp > gyan.home.33056: P 2291929849:2291929875(26) ack 516203558 win 2760 <nop,nop,timestamp 4949677 198236> (DF)
19 19:26:21.471021 gyan.home.33056 > alizarin.njit.edu.ftp: . ack 2291929875 win 5840 <nop,nop,timestamp 198245 4949677> (DF) [tos 0x10]
20 19:26:21.476867 gyan.home.33056 > alizarin.njit.edu.ftp: P 516203558:516203564(6) ack 2291929875 win 5840 <nop,nop,timestamp 198246 4949677> (DF) [tos 0x10]
21 19:26:21.497906 alizarin.njit.edu.ftp > gyan.home.33056: P 2291929875:2291929909(34) ack 516203564 win 2760 <nop,nop,timestamp 4949681 198246> (DF)
22 19:26:21.535767 gyan.home.33056 > alizarin.njit.edu.ftp: . ack 2291929909 win 5840 <nop,nop,timestamp 198252 4949681> (DF) [tos 0x10]
23 19:26:25.497390 gyan.home.33056 > alizarin.njit.edu.ftp: P 516203564:516203572(8) ack 2291929909 win 5840 <nop,nop,timestamp 198648 4949681> (DF) [tos 0x10]
24 19:26:25.521543 alizarin.njit.edu.ftp > gyan.home.33056: P 2291929909:2291929929(20) ack 516203572 win 2760 <nop,nop,timestamp 4950083

198648> (DF)
25 19:26:25.530209 gyan.home.33056 > alizarin.njit.edu.ftp: . ack 2291929929 win 5840 <nop,nop,timestamp 198651 4950083> (DF) [tos 0x10]
26 19:26:25.539847 gyan.home.33056 > alizarin.njit.edu.ftp: P 516203572:516203578(6) ack 2291929929 win 5840 <nop,nop,timestamp 198652 4950083> (DF) [tos 0x10]
27 19:26:25.566085 alizarin.njit.edu.ftp > gyan.home.33056: P 2291929929:2291929980(51) ack 516203578 win 2760 <nop,nop,timestamp 4950087 198652> (DF)
28 19:26:25.580673 gyan.home.33057 > alizarin.njit.edu.17029: S 511926496:511926496(0) win 5840 <mss 1460,sackOK,timestamp 198656 0,nop,wscale 0> (DF)
29 19:26:25.604455 alizarin.njit.edu.17029 > gyan.home.33057: S 2256768592:2256768592(0) ack 511926497 win 1380 <nop,nop,timestamp 4950091 198656,mss 1380,nop,wscale 0,nop,nop,sackOK> (DF)
30 19:26:25.614899 gyan.home.33057 > alizarin.njit.edu.17029: . ack 2256768593 win 5840 <nop,nop,timestamp 198659 4950091> (DF)
31 19:26:25.623109 gyan.home.33056 > alizarin.njit.edu.ftp: . ack 2291929980 win 5840 <nop,nop,timestamp 198660 4950087> (DF) [tos 0x10]
32 19:26:25.631681 gyan.home.33056 > alizarin.njit.edu.ftp: P 516203578:516203592(14) ack 2291929980 win 5840 <nop,nop,timestamp 198661 4950087> (DF) [tos 0x10]
33 19:26:25.677707 alizarin.njit.edu.ftp > gyan.home.33056: P 2291929980:2291930034(54) ack 516203592 win 2760 <nop,nop,timestamp 4950099 198661> (DF)
34 19:26:25.690435 gyan.home.33056 > alizarin.njit.edu.ftp: . ack 2291930034 win 5840 <nop,nop,timestamp 198667 4950099> (DF) [tos 0x10]
35 19:26:25.700678 gyan.home.33057 > alizarin.njit.edu.17029: . 511926497:511927187(690) ack 2256768593 win 5840 <nop,nop,timestamp 198668 4950091> (DF) [tos 0x8]
36 19:26:25.706546 gyan.home.33057 > alizarin.njit.edu.17029: P 511927187:511927877(690) ack 2256768593 win 5840 <nop,nop,timestamp 198668 4950091> (DF) [tos 0x8]
37 19:26:25.786553 alizarin.njit.edu.17029 > gyan.home.33057: . ack 511927187 win 1380 <nop,nop,timestamp 4950107 198668> (DF)
38 19:26:25.803770 gyan.home.33057 > alizarin.njit.edu.17029: . 511927877:511928567(690) ack 2256768593 win 5840 <nop,nop,timestamp 198678 4950107> (DF) [tos 0x8]
39 19:26:25.814106 alizarin.njit.edu.17029 > gyan.home.33057: . ack 511927877 win 1380 <nop,nop,timestamp 4950111 198668> (DF)
40 19:26:25.830507 gyan.home.33057 > alizarin.njit.edu.17029: FP 511928567:511929223(656) ack 2256768593 win 5840 <nop,nop,timestamp 198681 4950111> (DF) [tos 0x8]
41 19:26:25.905805 alizarin.njit.edu.17029 > gyan.home.33057: . ack 511929224 win 1380 <nop,nop,timestamp 4950121 198678> (DF)
42 19:26:25.925180 alizarin.njit.edu.17029 > gyan.home.33057: F 2256768593:2256768593(0) ack 511929224 win 47902 <nop,nop,timestamp 4950122 198678> (DF)
43 19:26:25.928299 gyan.home.33057 > alizarin.njit.edu.17029: . ack 2256768594 win 5840 <nop,nop,timestamp 198691 4950122> (DF)
44 19:26:25.929614 alizarin.njit.edu.ftp > gyan.home.33056: P 2291930034:2291930058(24) ack 516203592 win 2760 <nop,nop,timestamp 4950122 198667> (DF)
45 19:26:25.944669 gyan.home.33056 > alizarin.njit.edu.ftp: . ack 2291930058 win 5840 <nop,nop,timestamp 198692 4950122> (DF) [tos 0x10]
46 19:26:27.944168 gyan.home.33056 > alizarin.njit.edu.ftp: P 516203592:516203598(6) ack 2291930058 win 5840 <nop,nop,timestamp 198892 4950122> (DF) [tos 0x10]
47 19:26:27.967981 alizarin.njit.edu.ftp > gyan.home.33056: P 2291930058:2291930107(49) ack 516203598 win 2760 <nop,nop,timestamp 4950328

198892> (DF)
48 19:26:27.972827 alizarin.njit.edu.ftp > gyan.home.33056: FP 2291930107:2291930251(144) ack 516203598 win 49248 <nop,nop,timestamp 4950328 198892> (DF)
49 19:26:27.992198 gyan.home.33056 > alizarin.njit.edu.ftp: . ack 2291930107 win 5840 <nop,nop,timestamp 198897 4950328> (DF) [tos 0x10]
50 19:26:28.040136 gyan.home.33056 > alizarin.njit.edu.ftp: F 516203598:516203598(0) ack 2291930252 win 5840 <nop,nop,timestamp 198902 4950328> (DF) [tos 0x10]
51 19:26:28.059349 alizarin.njit.edu.ftp > gyan.home.33056: . ack 516203599 win 49248 <nop,nop,timestamp 4950337 198902> (DF)

12.23.3 LOG_IP_SEND

```
1    16:32:29:954854 10.13.0.1:32768 10.3.0.254:53 np_ip_local_out_hook - 0 udp
     Time : 0
2    16:32:29:954863 10.13.0.1:32768 10.3.0.254:53 ip_output B 16613 udp
3       16:32:29:954871 10.13.0.1:32768 10.3.0.254:53 nf_ip_post_routing_hook - 16613 udp
4       16:32:29:954880 10.13.0.1:32768 10.3.0.254:53 ip_finish_output2 B 16613 udp
5       16:32:29:954917 10.13.0.1:190 10.3.0.254:166 ip_finish_output2 E 16613 udp
6    16:32:29:954930 10.13.0.1:190 10.3.0.254:166 ip_output E 16613 udp
     Time : 67
7    16:32:29:957394 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit B S 2221246244 ack 0 0 tcp
8       16:32:29:957417 10.13.0.1:32778 10.14.0.1:21 np_ip_local_out_hook - S 2221246244 ack 0 0 tcp
9       16:32:29:957440 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 B S 2221246244 ack 0 0 tcp
10         16:32:29:957466 10.13.0.1:32778 10.14.0.1:21 ip_output B S 2221246244 ack 0 51137 tcp
11            16:32:29:957495 10.13.0.1:32778 10.14.0.1:21 nf_ip_post_routing_hook - S 2221246244 ack 0 51137 tcp
12            16:32:29:957527 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 B S 2221246244 ack 0 51137 tcp
13            16:32:29:957566 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 E S 2221246244 ack 0 51137 tcp
14         16:32:29:957617 10.13.0.1:32778 10.14.0.1:21 ip_output E S 2221246244 ack 0 51137 tcp
15      16:32:29:957658 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 E S 2221246244 ack 0 51137 tcp
16   16:32:29:957714 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit E S 2221246244 ack 0 51137
     Time : 320
17   16:32:29:957926 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit B . 2221246245 ack 1292290768 0 tcp
18      16:32:29:957976 10.13.0.1:32778 10.14.0.1:21 np_ip_local_out_hook - . 2221246245 ack 1292290768 0 tcp
19      16:32:29:958028 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 B . 2221246245 ack 1292290768 0 tcp
20         16:32:29:958084 10.13.0.1:32778 10.14.0.1:21 ip_output B . 2221246245 ack 1292290768 51138 tcp
21            16:32:29:958142 10.13.0.1:32778 10.14.0.1:21 nf_ip_post_routing_hook - . 2221246245 ack 1292290768 51138 tcp
22            16:32:29:958203 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 B . 2221246245 ack 1292290768 51138 tcp
23            16:32:29:958272 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 E . 2221246245 ack 1292290768 51138 tcp
24         16:32:29:958339 10.13.0.1:32778 10.14.0.1:21 ip_output E . 2221246245 ack 1292290768 51138 tcp
25      16:32:29:958423 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 E . 2221246245 ack 1292290768 51138 tcp
26   16:32:29:958496 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit E . 2221246245 ack 1292290768 51138 tcp
     Time : 570
27   16:32:29:975806 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit B . 2221246245 ack 1292290788 0 tcp
28      16:32:29:975912 10.13.0.1:32778 10.14.0.1:21 np_ip_local_out_hook - . 2221246245 ack 1292290788 0 tcp
```

```
29      16:32:29:975996 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 B . 2221246245 ack 1292290788 0 tcp
30        16:32:29:976082 10.13.0.1:32778 10.14.0.1:21 ip_output B . 2221246245 ack 1292290788 51139 tcp
31          16:32:29:976172 10.13.0.1:32778 10.14.0.1:21 nf_ip_post_routing_hook - . 2221246245 ack 1292290788 51139 tcp
32          16:32:29:976265 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 B . 2221246245 ack 1292290788 51139 tcp
33          16:32:29:976375 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 E . 2221246245 ack 1292290788 51139 tcp
34        16:32:29:976474 10.13.0.1:32778 10.14.0.1:21 ip_output E . 2221246245 ack 1292290788 51139 tcp
35      16:32:29:976591 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 E . 2221246245 ack 1292290788 51139 tcp
36    16:32:29:976696 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit E . 2221246245 ack 1292290788 51139 tcp
      Time : 890
37    16:32:29:976954 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit B P 2221246245 ack 1292290788 0 tcp
38      16:32:29:977066 10.13.0.1:32778 10.14.0.1:21 np_ip_local_out_hook - P 2221246245 ack 1292290788 0 tcp
39      16:32:29:977179 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 B P 2221246245 ack 1292290788 0 tcp
40        16:32:29:977297 10.13.0.1:32778 10.14.0.1:21 ip_output B P 2221246245 ack 1292290788 51140 tcp
41          16:32:29:977417 10.13.0.1:32778 10.14.0.1:21 nf_ip_post_routing_hook - P 2221246245 ack 1292290788 51140 tcp
42          16:32:29:977539 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 B P 2221246245 ack 1292290788 51140 tcp
43          16:32:29:977671 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 E P 2221246245 ack 1292290788 51140 tcp
44        16:32:29:977814 10.13.0.1:32778 10.14.0.1:21 ip_output E P 2221246245 ack 1292290788 51140 tcp
45      16:32:29:977946 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 E P 2221246245 ack 1292290788 51140 tcp
46    16:32:29:978082 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit E P 2221246245 ack 1292290788 51140
      Time : 1128
47    16:32:30:009356 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit B P 2221246258 ack 1292290826 0 tcp
48      16:32:30:009506 10.13.0.1:32778 10.14.0.1:21 np_ip_local_out_hook - P 2221246258 ack 1292290826 0 tcp
49      16:32:30:009652 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 B P 2221246258 ack 1292290826 0 tcp
50        16:32:30:009800 10.13.0.1:32778 10.14.0.1:21 ip_output B P 2221246258 ack 1292290826 51141 tcp
51          16:32:30:009951 10.13.0.1:32778 10.14.0.1:21 nf_ip_post_routing_hook - P 2221246258 ack 1292290826 51141 tcp
52          16:32:30:010105 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 B P 2221246258 ack 1292290826 51141 tcp
53          16:32:30:010271 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 E P 2221246258 ack 1292290826 51141 tcp
54        16:32:30:010446 10.13.0.1:32778 10.14.0.1:21 ip_output E P 2221246258 ack 1292290826 51141 tcp
55      16:32:30:010609 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 E P 2221246258 ack 1292290826 51141 tcp
56    16:32:30:010776 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit E P 2221246258 ack 1292290826 51141
      Time : 1420
57    16:32:30:071404 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit B . 2221246276 ack 1292290864 0 tcp
58      16:32:30:071586 10.13.0.1:32778 10.14.0.1:21 np_ip_local_out_hook - . 2221246276 ack 1292290864 0 tcp
59      16:32:30:071762 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 B . 2221246276 ack 1292290864 0 tcp
60        16:32:30:071942 10.13.0.1:32778 10.14.0.1:21 ip_output B . 2221246276 ack 1292290864 51142 tcp
61          16:32:30:072124 10.13.0.1:32778 10.14.0.1:21 nf_ip_post_routing_hook - . 2221246276 ack 1292290864 51142 tcp
62          16:32:30:072309 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 B . 2221246276 ack 1292290864 51142 tcp
```

63 16:32:30:072511 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 E . 2221246276 ack 1292290864 51142 tcp
64 16:32:30:072718 10.13.0.1:32778 10.14.0.1:21 ip_output E . 2221246276 ack 1292290864 51142 tcp
65 16:32:30:072912 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 E . 2221246276 ack 1292290864 51142 tcp
66 16:32:30:073109 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit E . 2221246276 ack 1292290864 51142 tcp
Time : 1705
67 16:32:31:605409 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit B P 2221246276 ack 1292290864 0 tcp
68 16:32:31:605622 10.13.0.1:32778 10.14.0.1:21 np_ip_local_out_hook - P 2221246276 ack 1292290864 0 tcp
69 16:32:31:605828 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 B P 2221246276 ack 1292290864 0 tcp
70 16:32:31:606039 10.13.0.1:32778 10.14.0.1:21 ip_output B P 2221246276 ack 1292290864 51143 tcp
71 16:32:31:606252 10.13.0.1:32778 10.14.0.1:21 nf_ip_post_routing_hook - P 2221246276 ack 1292290864 51143 tcp
72 16:32:31:606468 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 B P 2221246276 ack 1292290864 51143 tcp
73 16:32:31:606702 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 E P 2221246276 ack 1292290864 51143 tcp
74 16:32:31:606940 10.13.0.1:32778 10.14.0.1:21 ip_output E P 2221246276 ack 1292290864 51143 tcp
75 16:32:31:607186 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 E P 2221246276 ack 1292290864 51143 tcp
76 16:32:31:607426 10.14.0.1:17664 10.13.0.1:86 ip_queue_xmit E S 3720298496 ack 1057376710 56767
Time : 2017
77 16:32:31:607658 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit B . 2221246287 ack 1292290898 0 tcp
78 16:32:31:607893 10.13.0.1:32778 10.14.0.1:21 np_ip_local_out_hook - . 2221246287 ack 1292290898 0 tcp
79 16:32:31:608130 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 B . 2221246287 ack 1292290898 0 tcp
80 16:32:31:608371 10.13.0.1:32778 10.14.0.1:21 ip_output B . 2221246287 ack 1292290898 51144 tcp
81 16:32:31:608614 10.13.0.1:32778 10.14.0.1:21 nf_ip_post_routing_hook - . 2221246287 ack 1292290898 51144 tcp
82 16:32:31:608861 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 B . 2221246287 ack 1292290898 51144 tcp
83 16:32:31:609114 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 E . 2221246287 ack 1292290898 51144 tcp
84 16:32:31:609380 10.13.0.1:32778 10.14.0.1:21 ip_output E . 2221246287 ack 1292290898 51144 tcp
85 16:32:31:609636 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 E . 2221246287 ack 1292290898 51144 tcp
86 16:32:31:609895 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit E . 2221246287 ack 1292290898 51144 tcp
Time : 2237
87 16:32:33:839998 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit B P 2221246287 ack 1292290898 0 tcp
88 16:32:33:840273 10.13.0.1:32778 10.14.0.1:21 np_ip_local_out_hook - P 2221246287 ack 1292290898 0 tcp
89 16:32:33:840542 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 B P 2221246287 ack 1292290898 0 tcp
90 16:32:33:840814 10.13.0.1:32778 10.14.0.1:21 ip_output B P 2221246287 ack 1292290898 51145 tcp
91 16:32:33:841089 10.13.0.1:32778 10.14.0.1:21 nf_ip_post_routing_hook - P 2221246287 ack 1292290898 51145 tcp
92 16:32:33:841386 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 B P 2221246287 ack 1292290898 51145 tcp
93 16:32:33:841682 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 E P 2221246287 ack 1292290898 51145 tcp
94 16:32:33:841994 10.13.0.1:32778 10.14.0.1:21 ip_output E P 2221246287 ack 1292290898 51145 tcp
95 16:32:33:842281 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 E P 2221246287 ack 1292290898 51145 tcp
96 16:32:33:842582 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit E P 2221246287 ack 1292290898 51145

```
    Time : 2584
97   16:32:33:850748 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit B . 2221246302 ack 1292290931 0 tcp
98      16:32:33:851045 10.13.0.1:32778 10.14.0.1:21 np_ip_local_out_hook - . 2221246302 ack 1292290931 0 tcp
99      16:32:33:851344 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 B . 2221246302 ack 1292290931 0 tcp
100        16:32:33:851661 10.13.0.1:32778 10.14.0.1:21 ip_output B . 2221246302 ack 1292290931 51146 tcp
101           16:32:33:851967 10.13.0.1:32778 10.14.0.1:21 nf_ip_post_routing_hook - . 2221246302 ack 1292290931 51146 tcp
102           16:32:33:852275 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 B . 2221246302 ack 1292290931 51146 tcp
103           16:32:33:852591 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 E . 2221246302 ack 1292290931 51146 tcp
104        16:32:33:852919 10.13.0.1:32778 10.14.0.1:21 ip_output E . 2221246302 ack 1292290931 51146 tcp
105     16:32:33:853236 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 E . 2221246302 ack 1292290931 51146 tcp
106  16:32:33:853557 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit E . 2221246302 ack 1292290931 51146 tcp
    Time : 2809
107  16:32:33:871905 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit B P 2221246302 ack 1292290931 0 tcp
108     16:32:33:872241 10.13.0.1:32778 10.14.0.1:21 np_ip_local_out_hook - P 2221246302 ack 1292290931 0 tcp
109     16:32:33:872571 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 B P 2221246302 ack 1292290931 0 tcp
110        16:32:33:872905 10.13.0.1:32778 10.14.0.1:21 ip_output B P 2221246302 ack 1292290931 51147 tcp
111           16:32:33:873242 10.13.0.1:32778 10.14.0.1:21 nf_ip_post_routing_hook - P 2221246302 ack 1292290931 51147 tcp
112           16:32:33:873582 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 B P 2221246302 ack 1292290931 51147 tcp
113           16:32:33:873938 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 E P 2221246302 ack 1292290931 51147 tcp
114        16:32:33:874320 10.13.0.1:32778 10.14.0.1:21 ip_output E P 2221246302 ack 1292290931 51147 tcp
115     16:32:33:874669 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 E P 2221246302 ack 1292290931 51147 tcp
116  16:32:33:875033 10.14.0.1:17664 10.13.0.1:71 ip_queue_xmit E S 3720429568 ack 1057376723 56769
    Time : 3128
117  16:32:33:911417 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit B . 2221246308 ack 1292290950 0 tcp
118     16:32:33:911785 10.13.0.1:32778 10.14.0.1:21 np_ip_local_out_hook - . 2221246308 ack 1292290950 0 tcp
119     16:32:33:912146 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 B . 2221246308 ack 1292290950 0 tcp
120        16:32:33:912511 10.13.0.1:32778 10.14.0.1:21 ip_output B . 2221246308 ack 1292290950 51148 tcp
121           16:32:33:912879 10.13.0.1:32778 10.14.0.1:21 nf_ip_post_routing_hook - . 2221246308 ack 1292290950 51148 tcp
122           16:32:33:913249 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 B . 2221246308 ack 1292290950 51148 tcp
123           16:32:33:913638 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 E . 2221246308 ack 1292290950 51148 tcp
124        16:32:33:914030 10.13.0.1:32778 10.14.0.1:21 ip_output E . 2221246308 ack 1292290950 51148 tcp
125     16:32:33:914409 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 E . 2221246308 ack 1292290950 51148 tcp
126  16:32:33:914791 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit E . 2221246308 ack 1292290950 51148 tcp
    Time : 3374
127  16:32:36:864207 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit B P 2221246308 ack 1292290950 0 tcp
128     16:32:36:864606 10.13.0.1:32778 10.14.0.1:21 np_ip_local_out_hook - P 2221246308 ack 1292290950 0 tcp
129     16:32:36:864998 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 B P 2221246308 ack 1292290950 0 tcp
```

130 16:32:36:865393 10.13.0.1:32778 10.14.0.1:21 ip_output B P 2221246308 ack 1292290950 51149 tcp
131 16:32:36:865792 10.13.0.1:32778 10.14.0.1:21 nf_ip_post_routing_hook - P 2221246308 ack 1292290950 51149 tcp
132 16:32:36:866193 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 B P 2221246308 ack 1292290950 51149 tcp
133 16:32:36:866612 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 E P 2221246308 ack 1292290950 51149 tcp
134 16:32:36:867036 10.13.0.1:32778 10.14.0.1:21 ip_output E P 2221246308 ack 1292290950 51149 tcp
135 16:32:36:867446 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 E P 2221246308 ack 1292290950 51149 tcp
136 16:32:36:867861 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit E P 2221246308 ack 1292290950 51149
Time : 3654
137 16:32:36:871504 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit B . 2221246316 ack 1292290981 0 tcp
138 16:32:36:871933 10.13.0.1:32778 10.14.0.1:21 np_ip_local_out_hook - . 2221246316 ack 1292290981 0 tcp
139 16:32:36:872357 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 B . 2221246316 ack 1292290981 0 tcp
140 16:32:36:872783 10.13.0.1:32778 10.14.0.1:21 ip_output B . 2221246316 ack 1292290981 51150 tcp
141 16:32:36:873213 10.13.0.1:32778 10.14.0.1:21 nf_ip_post_routing_hook - . 2221246316 ack 1292290981 51150 tcp
142 16:32:36:873645 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 B . 2221246316 ack 1292290981 51150 tcp
143 16:32:36:874092 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 E . 2221246316 ack 1292290981 51150 tcp
144 16:32:36:874545 10.13.0.1:32778 10.14.0.1:21 ip_output E . 2221246316 ack 1292290981 51150 tcp
145 16:32:36:874986 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 E . 2221246316 ack 1292290981 51150 tcp
146 16:32:36:875431 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit E . 2221246316 ack 1292290981 51150 tcp
Time : 3927
147 16:32:36:876018 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit B P 2221246316 ack 1292290981 0 tcp
148 16:32:36:876470 10.13.0.1:32778 10.14.0.1:21 np_ip_local_out_hook - P 2221246316 ack 1292290981 0 tcp
149 16:32:36:876923 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 B P 2221246316 ack 1292290981 0 tcp
150 16:32:36:877380 10.13.0.1:32778 10.14.0.1:21 ip_output B P 2221246316 ack 1292290981 51151 tcp
151 16:32:36:877840 10.13.0.1:32778 10.14.0.1:21 nf_ip_post_routing_hook - P 2221246316 ack 1292290981 51151 tcp
152 16:32:36:878302 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 B P 2221246316 ack 1292290981 51151 tcp
153 16:32:36:878774 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 E P 2221246316 ack 1292290981 51151 tcp
154 16:32:36:879256 10.13.0.1:32778 10.14.0.1:21 ip_output E P 2221246316 ack 1292290981 51151 tcp
155 16:32:36:879728 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 E P 2221246316 ack 1292290981 51151 tcp
156 16:32:36:880204 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit E P 2221246316 ack 1292290981 51151
Time : 4186
157 16:32:37:081431 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit B P 2221246316 ack 1292290981 0 tcp
158 16:32:37:081922 10.13.0.1:32778 10.14.0.1:21 np_ip_local_out_hook - P 2221246316 ack 1292290981 0 tcp
159 16:32:37:082407 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 B P 2221246316 ack 1292290981 0 tcp
160 16:32:37:082895 10.13.0.1:32778 10.14.0.1:21 ip_output B P 2221246316 ack 1292290981 51152 tcp
161 16:32:37:083386 10.13.0.1:32778 10.14.0.1:21 nf_ip_post_routing_hook - P 2221246316 ack 1292290981 51152 tcp
162 16:32:37:083880 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 B P 2221246316 ack 1292290981 51152 tcp
163 16:32:37:084406 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 E P 2221246316 ack 1292290981 51152 tcp

164 16:32:37:084941 10.13.0.1:32778 10.14.0.1:21 ip_output E P 2221246316 ack 1292290981 51152 tcp
165 16:32:37:085444 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 E P 2221246316 ack 1292290981 51152 tcp
166 16:32:37:085950 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit E P 2221246316 ack 1292290981 51152 tcp
Time : 4519
167 16:32:37:086654 10.13.0.1:32779 10.14.0.1:48216 ip_queue_xmit B S 2230309760 ack 0 0 tcp
168 16:32:37:087168 10.13.0.1:32779 10.14.0.1:48216 np_ip_local_out_hook - S 2230309760 ack 0 0 tcp
169 16:32:37:087683 10.13.0.1:32779 10.14.0.1:48216 ip_queue_xmit2 B S 2230309760 ack 0 0 tcp
170 16:32:37:088201 10.13.0.1:32779 10.14.0.1:48216 ip_output B S 2230309760 ack 0 36910 tcp
171 16:32:37:088722 10.13.0.1:32779 10.14.0.1:48216 nf_ip_post_routing_hook - S 2230309760 ack 0 36910 tcp
172 16:32:37:089246 10.13.0.1:32779 10.14.0.1:48216 ip_finish_output2 B S 2230309760 ack 0 36910 tcp
173 16:32:37:089778 10.13.0.1:32779 10.14.0.1:48216 ip_finish_output2 E S 2230309760 ack 0 36910 tcp
174 16:32:37:090338 10.13.0.1:32779 10.14.0.1:48216 ip_output E S 2230309760 ack 0 36910 tcp
175 16:32:37:090870 10.13.0.1:32779 10.14.0.1:48216 ip_queue_xmit2 E S 2230309760 ack 0 36910 tcp
176 16:32:37:091429 10.14.0.1:17664 10.13.0.1:60 ip_queue_xmit E S 16384 ack 1057367968 0
Time : 4775
177 16:32:37:091956 10.13.0.1:32779 10.14.0.1:48216 ip_queue_xmit B . 2230309761 ack 1299431991 0 tcp
178 16:32:37:092498 10.13.0.1:32779 10.14.0.1:48216 np_ip_local_out_hook - . 2230309761 ack 1299431991 0 tcp
179 16:32:37:093042 10.13.0.1:32779 10.14.0.1:48216 ip_queue_xmit2 B . 2230309761 ack 1299431991 0 tcp
180 16:32:37:093590 10.13.0.1:32779 10.14.0.1:48216 ip_output B . 2230309761 ack 1299431991 36911 tcp
181 16:32:37:094141 10.13.0.1:32779 10.14.0.1:48216 nf_ip_post_routing_hook - . 2230309761 ack 1299431991 36911 tcp
182 16:32:37:094695 10.13.0.1:32779 10.14.0.1:48216 ip_finish_output2 B . 2230309761 ack 1299431991 36911 tcp
183 16:32:37:095257 10.13.0.1:32779 10.14.0.1:48216 ip_finish_output2 E . 2230309761 ack 1299431991 36911 tcp
184 16:32:37:095831 10.13.0.1:32779 10.14.0.1:48216 ip_output E . 2230309761 ack 1299431991 36911 tcp
185 16:32:37:096395 10.13.0.1:32779 10.14.0.1:48216 ip_queue_xmit2 E . 2230309761 ack 1299431991 36911 tcp
186 16:32:37:096962 10.13.0.1:32779 10.14.0.1:48216 ip_queue_xmit E . 2230309761 ack 1299431991 36911 tcp
Time : 5006
187 16:32:37:097559 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit B P 2221246322 ack 1292291027 0 tcp
188 16:32:37:098133 10.13.0.1:32778 10.14.0.1:21 np_ip_local_out_hook - P 2221246322 ack 1292291027 0 tcp
189 16:32:37:098708 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 B P 2221246322 ack 1292291027 0 tcp
190 16:32:37:099288 10.13.0.1:32778 10.14.0.1:21 ip_output B P 2221246322 ack 1292291027 51153 tcp
191 16:32:37:099870 10.13.0.1:32778 10.14.0.1:21 nf_ip_post_routing_hook - P 2221246322 ack 1292291027 51153 tcp
192 16:32:37:100455 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 B P 2221246322 ack 1292291027 51153 tcp
193 16:32:37:101049 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 E P 2221246322 ack 1292291027 51153 tcp
194 16:32:37:101668 10.13.0.1:32778 10.14.0.1:21 ip_output E P 2221246322 ack 1292291027 51153 tcp
195 16:32:37:102262 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 E P 2221246322 ack 1292291027 51153 tcp
196 16:32:37:102863 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit E P 2221246322 ack 1292291027 51153
Time : 5304

197 16:32:37:138919 10.13.0.1:32779 10.14.0.1:48216 ip_queue_xmit B P 2230309761 ack 1299431991 0 tcp
198 16:32:37:139550 10.13.0.1:32779 10.14.0.1:48216 np_ip_local_out_hook - P 2230309761 ack 1299431991 0 tcp
199 16:32:37:140158 10.13.0.1:32779 10.14.0.1:48216 ip_queue_xmit2 B P 2230309761 ack 1299431991 0 tcp
200 16:32:37:140769 10.13.0.1:32779 10.14.0.1:48216 ip_output B P 2230309761 ack 1299431991 36912 tcp
201 16:32:37:141403 10.13.0.1:32779 10.14.0.1:48216 nf_ip_post_routing_hook - P 2230309761 ack 1299431991 36912 tcp
202 16:32:37:142020 10.13.0.1:32779 10.14.0.1:48216 ip_finish_output2 B P 2230309761 ack 1299431991 36912 tcp
203 16:32:37:142654 10.13.0.1:32779 10.14.0.1:48216 ip_finish_output2 E P 2230309761 ack 1299431991 36912 tcp
204 16:32:37:143292 10.13.0.1:32779 10.14.0.1:48216 ip_output E P 2230309761 ack 1299431991 36912 tcp
205 16:32:37:143919 10.13.0.1:32779 10.14.0.1:48216 ip_queue_xmit2 E P 2230309761 ack 1299431991 36912 tcp
206 16:32:37:144560 10.13.0.1:32779 10.14.0.1:48216 ip_queue_xmit E P 2230309761 ack 1299431991 36912
Time : 5641
207 16:32:37:145187 10.13.0.1:32779 10.14.0.1:48216 ip_queue_xmit B F 2230310523 ack 1299431991 0 tcp
208 16:32:37:145824 10.13.0.1:32779 10.14.0.1:48216 np_ip_local_out_hook - F 2230310523 ack 1299431991 0 tcp
209 16:32:37:146463 10.13.0.1:32779 10.14.0.1:48216 ip_queue_xmit2 B F 2230310523 ack 1299431991 0 tcp
210 16:32:37:147105 10.13.0.1:32779 10.14.0.1:48216 ip_output B F 2230310523 ack 1299431991 36913 tcp
211 16:32:37:147750 10.13.0.1:32779 10.14.0.1:48216 nf_ip_post_routing_hook - F 2230310523 ack 1299431991 36913 tcp
212 16:32:37:148399 10.13.0.1:32779 10.14.0.1:48216 ip_finish_output2 B F 2230310523 ack 1299431991 36913 tcp
213 16:32:37:149056 10.13.0.1:32779 10.14.0.1:48216 ip_finish_output2 E F 2230310523 ack 1299431991 36913 tcp
214 16:32:37:149745 10.13.0.1:32779 10.14.0.1:48216 ip_output E F 2230310523 ack 1299431991 36913 tcp
215 16:32:37:150403 10.13.0.1:32779 10.14.0.1:48216 ip_queue_xmit2 E F 2230310523 ack 1299431991 36913 tcp
216 16:32:37:151080 10.14.0.1:17672 10.13.0.1:52 ip_queue_xmit E S 3624157184 ack 1057378203 55300
Time : 5893
217 16:32:37:151746 10.13.0.1:32779 10.14.0.1:48216 ip_queue_xmit B . 2230310524 ack 1299431992 0 tcp
218 16:32:37:152414 10.13.0.1:32779 10.14.0.1:48216 np_ip_local_out_hook - . 2230310524 ack 1299431992 0 tcp
219 16:32:37:153084 10.13.0.1:32779 10.14.0.1:48216 ip_queue_xmit2 B . 2230310524 ack 1299431992 0 tcp
220 16:32:37:153758 10.13.0.1:32779 10.14.0.1:48216 ip_output B . 2230310524 ack 1299431992 36914 tcp
221 16:32:37:154436 10.13.0.1:32779 10.14.0.1:48216 nf_ip_post_routing_hook - . 2230310524 ack 1299431992 36914 tcp
222 16:32:37:155115 10.13.0.1:32779 10.14.0.1:48216 ip_finish_output2 B . 2230310524 ack 1299431992 36914 tcp
223 16:32:37:155803 10.13.0.1:32779 10.14.0.1:48216 ip_finish_output2 E . 2230310524 ack 1299431992 36914 tcp
224 16:32:37:156504 10.13.0.1:32779 10.14.0.1:48216 ip_output E . 2230310524 ack 1299431992 36914 tcp
225 16:32:37:157193 10.13.0.1:32779 10.14.0.1:48216 ip_queue_xmit2 E . 2230310524 ack 1299431992 36914 tcp
226 16:32:37:157886 10.13.0.1:32779 10.14.0.1:48216 ip_queue_xmit E . 2230310524 ack 1299431992 36914 tcp
Time : 6140
227 16:32:37:171443 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit B . 2221246336 ack 1292291049 0 tcp
228 16:32:37:172153 10.13.0.1:32778 10.14.0.1:21 np_ip_local_out_hook - . 2221246336 ack 1292291049 0 tcp
229 16:32:37:172856 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 B . 2221246336 ack 1292291049 0 tcp
230 16:32:37:173562 10.13.0.1:32778 10.14.0.1:21 ip_output B . 2221246336 ack 1292291049 51154 tcp

231 16:32:37:174271 10.13.0.1:32778 10.14.0.1:21 nf_ip_post_routing_hook - . 2221246336 ack 1292291049 51154 tcp
232 16:32:37:174982 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 B . 2221246336 ack 1292291049 51154 tcp
233 16:32:37:175710 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 E . 2221246336 ack 1292291049 51154 tcp
234 16:32:37:176443 10.13.0.1:32778 10.14.0.1:21 ip_output E . 2221246336 ack 1292291049 51154 tcp
235 16:32:37:177164 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 E . 2221246336 ack 1292291049 51154 tcp
236 16:32:37:177888 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit E . 2221246336 ack 1292291049 51154 tcp
Time : 6445
237 16:32:37:182952 0.0.0.0:6 0.0.0.0:0 np_ip_local_out_hook - F 3352444928 ack 1074159301 0 tcp
Time : 0
238 16:32:37:183689 0.0.0.0:6 0.0.0.0:0 ip_output B F 3352444928 ack 1074159301 0 tcp
239 16:32:37:184422 0.0.0.0:6 0.0.0.0:0 nf_ip_post_routing_hook - F 3352444928 ack 1074159301 0 tcp
240 16:32:37:185157 0.0.0.0:6 0.0.0.0:0 ip_finish_output2 B F 3352444928 ack 1074159301 0 tcp
241 16:32:37:185918 10.13.0.1:17680 10.14.0.1:52 ip_finish_output2 E F 3352444928 ack 1074159301 0 tcp
242 16:32:37:186706 10.13.0.1:17680 10.14.0.1:52 ip_output E F 3352444928 ack 1074159301 0 tcp
Time : 3017
243 16:32:37:200854 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit B . 2221246336 ack 1292291071 0 tcp
244 16:32:37:201637 10.13.0.1:32778 10.14.0.1:21 np_ip_local_out_hook - . 2221246336 ack 1292291071 0 tcp
245 16:32:37:202388 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 B . 2221246336 ack 1292291071 0 tcp
246 16:32:37:203142 10.13.0.1:32778 10.14.0.1:21 ip_output B . 2221246336 ack 1292291071 51155 tcp
247 16:32:37:203900 10.13.0.1:32778 10.14.0.1:21 nf_ip_post_routing_hook - . 2221246336 ack 1292291071 51155 tcp
248 16:32:37:204659 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 B . 2221246336 ack 1292291071 51155 tcp
249 16:32:37:205435 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 E . 2221246336 ack 1292291071 51155 tcp
250 16:32:37:206216 10.13.0.1:32778 10.14.0.1:21 ip_output E . 2221246336 ack 1292291071 51155 tcp
251 16:32:37:206985 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 E . 2221246336 ack 1292291071 51155 tcp
252 16:32:37:207758 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit E . 2221246336 ack 1292291071 51155
Time : 6904
253 16:32:37:437075 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit B . 2221246336 ack 1292291071 0 tcp
254 16:32:37:437862 10.13.0.1:32778 10.14.0.1:21 np_ip_local_out_hook - . 2221246336 ack 1292291071 0 tcp
255 16:32:37:438644 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 B . 2221246336 ack 1292291071 0 tcp
256 16:32:37:439429 10.13.0.1:32778 10.14.0.1:21 ip_output B . 2221246336 ack 1292291071 51156 tcp
257 16:32:37:440217 10.13.0.1:32778 10.14.0.1:21 nf_ip_post_routing_hook - . 2221246336 ack 1292291071 51156 tcp
258 16:32:37:441007 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 B . 2221246336 ack 1292291071 51156 tcp
259 16:32:37:441824 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 E . 2221246336 ack 1292291071 51156 tcp
260 16:32:37:442634 10.13.0.1:32778 10.14.0.1:21 ip_output E . 2221246336 ack 1292291071 51156 tcp
261 16:32:37:443434 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 E . 2221246336 ack 1292291071 51156 tcp
262 16:32:37:444237 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit E . 2221246336 ack 1292291071 51156 tcp
Time : 7162

263 16:32:38:640292 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit B P 2221246336 ack 1292291071 0 tcp
264 16:32:38:641111 10.13.0.1:32778 10.14.0.1:21 np_ip_local_out_hook - P 2221246336 ack 1292291071 0 tcp
265 16:32:38:641940 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 B P 2221246336 ack 1292291071 0 tcp
266 16:32:38:642756 10.13.0.1:32778 10.14.0.1:21 ip_output B P 2221246336 ack 1292291071 51157 tcp
267 16:32:38:643575 10.13.0.1:32778 10.14.0.1:21 nf_ip_post_routing_hook - P 2221246336 ack 1292291071 51157 tcp
268 16:32:38:644397 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 B P 2221246336 ack 1292291071 51157 tcp
269 16:32:38:645235 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 E P 2221246336 ack 1292291071 51157 tcp
270 16:32:38:646100 10.13.0.1:32778 10.14.0.1:21 ip_output E P 2221246336 ack 1292291071 51157 tcp
271 16:32:38:646931 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 E P 2221246336 ack 1292291071 51157 tcp
272 16:32:38:647783 10.14.0.1:17664 10.13.0.1:52 ip_queue_xmit E S 3720888320 ack 1057376735 56776
Time : 7491
273 16:32:38:648598 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit B . 2221246342 ack 1292291071 0 tcp
274 16:32:38:649438 10.13.0.1:32778 10.14.0.1:21 np_ip_local_out_hook - . 2221246342 ack 1292291071 0 tcp
275 16:32:38:650281 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 B . 2221246342 ack 1292291071 0 tcp
276 16:32:38:651127 10.13.0.1:32778 10.14.0.1:21 ip_output B . 2221246342 ack 1292291071 51158 tcp
277 16:32:38:651991 10.13.0.1:32778 10.14.0.1:21 nf_ip_post_routing_hook - . 2221246342 ack 1292291071 51158 tcp
278 16:32:38:652844 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 B . 2221246342 ack 1292291071 51158 tcp
279 16:32:38:653704 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 E . 2221246342 ack 1292291071 51158 tcp
280 16:32:38:654576 10.13.0.1:32778 10.14.0.1:21 ip_output E . 2221246342 ack 1292291071 51158 tcp
281 16:32:38:655437 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 E . 2221246342 ack 1292291071 51158 tcp
282 16:32:38:656302 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit E . 2221246342 ack 1292291071 51158 tcp
Time : 7704
283 16:32:38:692072 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit B . 2221246342 ack 1292291086 0 tcp
284 16:32:38:692952 10.13.0.1:32778 10.14.0.1:21 np_ip_local_out_hook - . 2221246342 ack 1292291086 0 tcp
285 16:32:38:693827 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 B . 2221246342 ack 1292291086 0 tcp
286 16:32:38:694704 10.13.0.1:32778 10.14.0.1:21 ip_output B . 2221246342 ack 1292291086 51159 tcp
287 16:32:38:695585 10.13.0.1:32778 10.14.0.1:21 nf_ip_post_routing_hook - . 2221246342 ack 1292291086 51159 tcp
288 16:32:38:696468 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 B . 2221246342 ack 1292291086 51159 tcp
289 16:32:38:697363 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 E . 2221246342 ack 1292291086 51159 tcp
290 16:32:38:698267 10.13.0.1:32778 10.14.0.1:21 ip_output E . 2221246342 ack 1292291086 51159 tcp
291 16:32:38:699159 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 E . 2221246342 ack 1292291086 51159 tcp
292 16:32:38:700055 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit E . 2221246342 ack 1292291086 51159 tcp
Time : 7983
293 16:32:38:701009 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit B F 2221246342 ack 1292291086 0 tcp
294 16:32:38:701929 10.13.0.1:32778 10.14.0.1:21 np_ip_local_out_hook - F 2221246342 ack 1292291086 0 tcp
295 16:32:38:702834 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 B F 2221246342 ack 1292291086 0 tcp
296 16:32:38:703742 10.13.0.1:32778 10.14.0.1:21 ip_output B F 2221246342 ack 1292291086 51160 tcp

297 16:32:38:704653 10.13.0.1:32778 10.14.0.1:21 nf_ip_post_routing_hook - F 2221246342 ack 1292291086 51160 tcp
298 16:32:38:705567 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 B F 2221246342 ack 1292291086 51160 tcp
299 16:32:38:706489 10.13.0.1:32778 10.14.0.1:21 ip_finish_output2 E F 2221246342 ack 1292291086 51160 tcp
300 16:32:38:707423 10.13.0.1:32778 10.14.0.1:21 ip_output E F 2221246342 ack 1292291086 51160 tcp
301 16:32:38:708346 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit2 E F 2221246342 ack 1292291086 51160 tcp
302 16:32:38:709273 10.13.0.1:32778 10.14.0.1:21 ip_queue_xmit E F 2221246342 ack 1292291086 51160
Time : 8264

12.23.4 LOG_DUMP_SEND

```
1    16:32:17.778978 CDP v1, ttl=180s DevID 'Lab Switch 3(000a57-c08d00)' Addr (1): IPv4 127.0.0.1 PortID '21' CAP 0x08[|cdp]
2    16:32:29.954900 arp who-has 10.13.0.2 tell franklin.internet.lab
3    16:32:29.955056 arp reply 10.13.0.2 is-at 0:2:b3:cd:cd:c8
4    16:32:29.955072 franklin.internet.lab.32768 > 10.3.0.254.domain:  34647+ A? hawking.internet.lab. (38) (DF)
5    16:32:29.957232 10.3.0.254.domain > franklin.internet.lab.32768:  34647* 1/1/1 A 10.14.0.1 (91) (DF)
6    16:32:29.957561 franklin.internet.lab.32778 > 10.14.0.1.ftp: S 2221246244:2221246244(0) win 5840 <mss 1460,sackOK,timestamp 344293 0,nop,wscale 0> (DF)
7    16:32:29.957898 10.14.0.1.ftp > franklin.internet.lab.32778: S 1292290767:1292290767(0) ack 2221246245 win 5792 <mss 1460,sackOK,timestamp 303699819
344293,nop,wscale 0> (DF)
8    16:32:29.958266 franklin.internet.lab.32778 > 10.14.0.1.ftp: . ack 1292290768 win 5840 <nop,nop,timestamp 344293 303699819> (DF)
9    16:32:29.960124 10.14.0.1.ftp > franklin.internet.lab.32778: P 1292290768:1292290788(20) ack 2221246245 win 5792 <nop,nop,timestamp 303699819 344293> (DF)
10   16:32:29.976361 franklin.internet.lab.32778 > 10.14.0.1.ftp: . ack 1292290788 win 5840 <nop,nop,timestamp 344295 303699819> (DF) [tos 0x10]
11   16:32:29.977661 franklin.internet.lab.32778 > 10.14.0.1.ftp: P 2221246245:2221246258(13) ack 1292290788 win 5840 <nop,nop,timestamp 344295 303699819> (DF) [tos
0x10]
12   16:32:29.993184 10.14.0.1.ftp > franklin.internet.lab.32778: . ack 2221246258 win 5792 <nop,nop,timestamp 303699821 344295> (DF)
13   16:32:30.009179 10.14.0.1.ftp > franklin.internet.lab.32778: P 1292290788:1292290826(38) ack 2221246258 win 5792 <nop,nop,timestamp 303699821 344295> (DF)
14   16:32:30.010259 franklin.internet.lab.32778 > 10.14.0.1.ftp: P 2221246258:2221246276(18) ack 1292290826 win 5840 <nop,nop,timestamp 344298 303699821> (DF) [tos
0x10]
15   16:32:30.028717 10.14.0.1.ftp > franklin.internet.lab.32778: P 1292290826:1292290864(38) ack 2221246276 win 5792 <nop,nop,timestamp 303699824 344298> (DF)
16   16:32:30.072492 franklin.internet.lab.32778 > 10.14.0.1.ftp: . ack 1292290864 win 5840 <nop,nop,timestamp 344305 303699824> (DF) [tos 0x10]
17   16:32:31.606681 franklin.internet.lab.32778 > 10.14.0.1.ftp: P 2221246276:2221246287(11) ack 1292290864 win 5840 <nop,nop,timestamp 344458 303699824> (DF) [tos
0x10]
18   16:32:31.607145 10.14.0.1.ftp > franklin.internet.lab.32778: P 1292290864:1292290898(34) ack 2221246287 win 5792 <nop,nop,timestamp 303699984 344458> (DF)
19   16:32:31.609100 franklin.internet.lab.32778 > 10.14.0.1.ftp: . ack 1292290898 win 5840 <nop,nop,timestamp 344458 303699984> (DF) [tos 0x10]
20   16:32:33.841659 franklin.internet.lab.32778 > 10.14.0.1.ftp: P 2221246287:2221246302(15) ack 1292290898 win 5840 <nop,nop,timestamp 344681 303699984> (DF) [tos
0x10]
21   16:32:33.850696 10.14.0.1.ftp > franklin.internet.lab.32778: P 1292290898:1292290931(33) ack 2221246302 win 5792 <nop,nop,timestamp 303700208 344681> (DF)
22   16:32:33.852574 franklin.internet.lab.32778 > 10.14.0.1.ftp: . ack 1292290931 win 5840 <nop,nop,timestamp 344682 303700208> (DF) [tos 0x10]
23   16:32:33.873913 franklin.internet.lab.32778 > 10.14.0.1.ftp: P 2221246302:2221246308(6) ack 1292290931 win 5840 <nop,nop,timestamp 344685 303700208> (DF) [tos
0x10]
24   16:32:33.874222 10.14.0.1.ftp > franklin.internet.lab.32778: P 1292290931:1292290950(19) ack 2221246308 win 5792 <nop,nop,timestamp 303700210 344685> (DF)
25   16:32:33.913610 franklin.internet.lab.32778 > 10.14.0.1.ftp: . ack 1292290950 win 5840 <nop,nop,timestamp 344689 303700210> (DF) [tos 0x10]
26   16:32:34.953248 arp who-has franklin.internet.lab tell 10.13.0.2
27   16:32:34.953286 arp reply franklin.internet.lab is-at 0:2:b3:d3:d4:8a
28   16:32:36.866583 franklin.internet.lab.32778 > 10.14.0.1.ftp: P 2221246308:2221246316(8) ack 1292290950 win 5840 <nop,nop,timestamp 344984 303700210> (DF) [tos
0x10]
29   16:32:36.870289 10.14.0.1.ftp > franklin.internet.lab.32778: P 1292290950:1292290981(31) ack 2221246316 win 5792 <nop,nop,timestamp 303700510 344984> (DF)
30   16:32:36.874065 franklin.internet.lab.32778 > 10.14.0.1.ftp: . ack 1292290981 win 5840 <nop,nop,timestamp 344985 303700510> (DF) [tos 0x10]
31   16:32:36.878749 franklin.internet.lab.32778 > 10.14.0.1.ftp: P 2221246316:2221246322(6) ack 1292290981 win 5840 <nop,nop,timestamp 344985 303700510> (DF) [tos
0x10]
32   16:32:37.084359 franklin.internet.lab.32778 > 10.14.0.1.ftp: P 2221246316:2221246322(6) ack 1292290981 win 5840 <nop,nop,timestamp 345006 303700510> (DF) [tos
```

0x10]
33 16:32:37.084875 10.14.0.1.ftp > franklin.internet.lab.32778: P 1292290981:1292291027(46) ack 2221246322 win 5792 <nop,nop,timestamp 303700531 345006> (DF)
34 16:32:37.089751 franklin.internet.lab.32779 > 10.14.0.1.48216: S 2230309760:2230309760(0) win 5840 <mss 1460,sackOK,timestamp 345006 0,nop,wscale 0> (DF)
35 16:32:37.090026 10.14.0.1.48216 > franklin.internet.lab.32779: S 1299431990:1299431990(0) ack 2230309761 win 5792 <mss 1460,sackOK,timestamp 303700532 345006,nop,wscale 0> (DF)
36 16:32:37.095229 franklin.internet.lab.32779 > 10.14.0.1.48216: . ack 1299431991 win 5840 <nop,nop,timestamp 345007 303700532> (DF)
37 16:32:37.101019 franklin.internet.lab.32778 > 10.14.0.1.ftp: P 2221246322:2221246336(14) ack 1292291027 win 5840 <nop,nop,timestamp 345007 303700531> (DF) [tos 0x10]
38 16:32:37.126574 10.14.0.1.ftp > franklin.internet.lab.32778: P 1292291027:1292291049(22) ack 2221246336 win 5792 <nop,nop,timestamp 303700533 345007> (DF)
39 16:32:37.142618 franklin.internet.lab.32779 > 10.14.0.1.48216: P 2230309761:2230310523(762) ack 1299431991 win 5840 <nop,nop,timestamp 345011 303700532> (DF) [tos 0x8]
40 16:32:37.149023 franklin.internet.lab.32779 > 10.14.0.1.48216: F 2230310523:2230310523(0) ack 1299431991 win 5840 <nop,nop,timestamp 345012 303700532> (DF) [tos 0x8]
41 16:32:37.149453 10.14.0.1.48216 > franklin.internet.lab.32779: F 1299431991:1299431991(0) ack 2230310524 win 6858 <nop,nop,timestamp 303700538 345012> (DF) [tos 0x8]
42 16:32:37.155770 franklin.internet.lab.32779 > 10.14.0.1.48216: . ack 1299431992 win 5840 <nop,nop,timestamp 345013 303700538> (DF) [tos 0x8]
43 16:32:37.175669 franklin.internet.lab.32778 > 10.14.0.1.ftp: . ack 1292291049 win 5840 <nop,nop,timestamp 345015 303700533> (DF) [tos 0x10]
44 16:32:37.182846 10.14.0.1.48216 > franklin.internet.lab.32779: . ack 2230310523 win 6858 <nop,nop,timestamp 303700537 345011> (DF) [tos 0x8]
45 16:32:37.185866 franklin.internet.lab.32779 > 10.14.0.1.48216: . ack 1299431992 win 5840 <nop,nop,timestamp 345016 303700538> (DF) [tos 0x8]
46 16:32:37.186108 10.14.0.1.48216 > franklin.internet.lab.32779: R 1299431992:1299431992(0) win 0 (DF) [tos 0x8]
47 16:32:37.186502 10.14.0.1.ftp > franklin.internet.lab.32778: P 1292291049:1292291071(22) ack 2221246336 win 5792 <nop,nop,timestamp 303700538 345007> (DF)
48 16:32:37.205392 franklin.internet.lab.32778 > 10.14.0.1.ftp: . ack 1292291071 win 5840 <nop,nop,timestamp 345017 303700538> (DF) [tos 0x10]
49 16:32:37.436985 10.14.0.1.ftp > franklin.internet.lab.32778: P 1292291049:1292291071(22) ack 2221246336 win 5792 <nop,nop,timestamp 303700567 345015> (DF)
50 16:32:37.441784 franklin.internet.lab.32778 > 10.14.0.1.ftp: . ack 1292291071 win 5840 <nop,nop,timestamp 345041 303700567,nop,nop,sack sack 1 {1292291049:1292291071} > (DF) [tos 0x10]
51 16:32:38.645189 franklin.internet.lab.32778 > 10.14.0.1.ftp: P 2221246336:2221246342(6) ack 1292291071 win 5840 <nop,nop,timestamp 345161 303700567> (DF) [tos 0x10]
52 16:32:38.645918 10.14.0.1.ftp > franklin.internet.lab.32778: F 1292291085:1292291085(0) ack 2221246342 win 5792 <nop,nop,timestamp 303700687 345161> (DF)
53 16:32:38.653663 franklin.internet.lab.32778 > 10.14.0.1.ftp: . ack 1292291071 win 5840 <nop,nop,timestamp 345162 303700567,nop,nop,sack sack 1 {1292291085:1292291086} > (DF) [tos 0x10]
54 16:32:38.691925 10.14.0.1.ftp > franklin.internet.lab.32778: P 1292291071:1292291085(14) ack 2221246342 win 5792 <nop,nop,timestamp 303700687 345161> (DF)
55 16:32:38.697319 franklin.internet.lab.32778 > 10.14.0.1.ftp: . ack 1292291086 win 5840 <nop,nop,timestamp 345167 303700687> (DF) [tos 0x10]
56 16:32:38.706445 franklin.internet.lab.32778 > 10.14.0.1.ftp: F 2221246342:2221246342(0) ack 1292291086 win 5840 <nop,nop,timestamp 345167 303700687> (DF) [tos 0x10]
57 16:32:38.742217 10.14.0.1.ftp > franklin.internet.lab.32778: . ack 2221246343 win 5792 <nop,nop,timestamp 303700693 345167> (DF) [tos 0x10]

12.23.5 LOG_IP_RCV

```
1    16:40:31:018627 10.3.0.254:53 10.13.0.1:32768 another_ip_protocol - ipid: 0 udp
     Time : 0
2    16:40:31:018638 10.3.0.254:53 10.13.0.1:32768 ip_rcv B ipid: 0 udp
3      16:40:31:018648 10.3.0.254:53 10.13.0.1:32768 nf_ip_pre_routing_hook - ipid: 0 udp
4      16:40:31:018657 10.3.0.254:53 10.13.0.1:32768 ip_rcv_finish B ipid: 0 udp
5        16:40:31:018669 10.3.0.254:53 10.13.0.1:32768 ip_route_input B ipid: 0 udp
6        16:40:31:018695 10.3.0.254:53 10.13.0.1:32768 ip_route_input E ipid: 0 udp
7        16:40:31:018711 10.3.0.254:53 10.13.0.1:32768 ip_local_deliver B ipid: 0 udp
8          16:40:31:018728 10.3.0.254:53 10.13.0.1:32768 nf_ip_local_in_hook - ipid: 0 udp
9          16:40:31:018747 10.3.0.254:53 10.13.0.1:32768 ip_local_deliver_finish B ipid: 0 udp
10          16:40:31:018772 10.3.0.254:53 10.13.0.1:32768 ip_local_deliver_finish E ipid: 0 udp
11        16:40:31:018795 10.3.0.254:53 10.13.0.1:32768 ip_local_deliver E ipid: 0 udp
12      16:40:31:018820 10.3.0.254:53 10.13.0.1:32768 ip_rcv_finish E ipid: 0 udp
13   16:40:31:018847 10.3.0.254:53 10.13.0.1:32768 ip_rcv E ipid: 0 udp
     Time : 209
14   16:40:31:019370 10.14.0.1:21 10.13.0.1:32781 another_ip_protocol - 1793704357 ack 2720407259 ipid: 0 tcp
     Time : 0
15   16:40:31:019411 10.14.0.1:21 10.13.0.1:32781 ip_rcv B 1793704357 ack 2720407259 ipid: 0 tcp
16     16:40:31:019453 10.14.0.1:21 10.13.0.1:32781 nf_ip_pre_routing_hook - 1793704357 ack 2720407259 ipid: 0 tcp
17     16:40:31:019497 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish B 1793704357 ack 2720407259 ipid: 0 tcp
18       16:40:31:019544 10.14.0.1:21 10.13.0.1:32781 ip_route_input B 1793704357 ack 2720407259 ipid: 0 tcp
19       16:40:31:019597 10.14.0.1:21 10.13.0.1:32781 ip_route_input E 1793704357 ack 2720407259 ipid: 0 tcp
20       16:40:31:019651 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver B 1793704357 ack 2720407259 ipid: 0 tcp
21         16:40:31:019708 10.14.0.1:21 10.13.0.1:32781 nf_ip_local_in_hook - 1793704357 ack 2720407259 ipid: 0 tcp
22         16:40:31:019768 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish B 1793704357 ack 2720407259 ipid: 0 tcp
23         16:40:31:019855 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish E 1793704357 ack 2720407259 ipid: 0 tcp
24       16:40:31:019922 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver E 1793704357 ack 2720407259 ipid: 0 tcp
25     16:40:31:020004 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish E 1793704357 ack 2720407259 ipid: 0 tcp
26   16:40:31:020077 10.14.0.1:21 10.13.0.1:32781 ip_rcv E 1793704357 ack 2720407259 ipid: 0 tcp
     Time : 666
27   16:40:31:021748 10.14.0.1:21 10.13.0.1:32781 another_ip_protocol - 1793704358 ack 2720407259 ipid: 4851 tcp
     Time : 0
28   16:40:31:021842 10.14.0.1:21 10.13.0.1:32781 ip_rcv B 1793704358 ack 2720407259 ipid: 4851 tcp
29     16:40:31:021927 10.14.0.1:21 10.13.0.1:32781 nf_ip_pre_routing_hook - 1793704358 ack 2720407259 ipid: 4851 tcp
30     16:40:31:022013 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish B 1793704358 ack 2720407259 ipid: 4851 tcp
```

```
31        16:40:31:022102 10.14.0.1:21 10.13.0.1:32781 ip_route_input B 1793704358 ack 2720407259 ipid: 4851 tcp
32        16:40:31:022196 10.14.0.1:21 10.13.0.1:32781 ip_route_input E 1793704358 ack 2720407259 ipid: 4851 tcp
33        16:40:31:022291 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver B 1793704358 ack 2720407259 ipid: 4851 tcp
34           16:40:31:022390 10.14.0.1:21 10.13.0.1:32781 nf_ip_local_in_hook - 1793704358 ack 2720407259 ipid: 4851 tcp
35           16:40:31:022492 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish B 1793704358 ack 2720407259 ipid: 4851 tcp
36           16:40:31:022645 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish E 1793704358 ack 2720407259 ipid: 4851 tcp
37        16:40:31:022755 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver E 1793704358 ack 2720407259 ipid: 4851 tcp
38     16:40:31:022881 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish E 1793704358 ack 2720407259 ipid: 4851 tcp
39  16:40:31:022996 10.14.0.1:21 10.13.0.1:32781 ip_rcv E 1793704358 ack 2720407259 ipid: 4851 tcp
    Time : 1154
40  16:40:31:025824 10.14.0.1:21 10.13.0.1:32781 another_ip_protocol - 1793704378 ack 2720407272 ipid: 4852 tcp
    Time : 0
41  16:40:31:025957 10.14.0.1:21 10.13.0.1:32781 ip_rcv B 1793704378 ack 2720407272 ipid: 4852 tcp
42     16:40:31:026084 10.14.0.1:21 10.13.0.1:32781 nf_ip_pre_routing_hook - 1793704378 ack 2720407272 ipid: 4852 tcp
43     16:40:31:026212 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish B 1793704378 ack 2720407272 ipid: 4852 tcp
44        16:40:31:026344 10.14.0.1:21 10.13.0.1:32781 ip_route_input B 1793704378 ack 2720407272 ipid: 4852 tcp
45        16:40:31:026480 10.14.0.1:21 10.13.0.1:32781 ip_route_input E 1793704378 ack 2720407272 ipid: 4852 tcp
46        16:40:31:026617 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver B 1793704378 ack 2720407272 ipid: 4852 tcp
47           16:40:31:026758 10.14.0.1:21 10.13.0.1:32781 nf_ip_local_in_hook - 1793704378 ack 2720407272 ipid: 4852 tcp
48           16:40:31:026903 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish B 1793704378 ack 2720407272 ipid: 4852 tcp
49           16:40:31:027055 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish E 1793704378 ack 2720407272 ipid: 4852 tcp
50        16:40:31:027205 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver E 1793704378 ack 2720407272 ipid: 4852 tcp
51     16:40:31:027359 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish E 1793704378 ack 2720407272 ipid: 4852 tcp
52  16:40:31:027517 10.14.0.1:21 10.13.0.1:32781 ip_rcv E 1793704378 ack 2720407272 ipid: 4852 tcp
    Time : 1560
53  16:40:31:051154 10.14.0.1:21 10.13.0.1:32781 another_ip_protocol - 1793704378 ack 2720407272 ipid: 4853 tcp
    Time : 0
54  16:40:31:051334 10.14.0.1:21 10.13.0.1:32781 ip_rcv B 1793704378 ack 2720407272 ipid: 4853 tcp
55     16:40:31:051521 10.14.0.1:21 10.13.0.1:32781 nf_ip_pre_routing_hook - 1793704378 ack 2720407272 ipid: 4853 tcp
56     16:40:31:051691 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish B 1793704378 ack 2720407272 ipid: 4853 tcp
57        16:40:31:051865 10.14.0.1:21 10.13.0.1:32781 ip_route_input B 1793704378 ack 2720407272 ipid: 4853 tcp
58        16:40:31:052044 10.14.0.1:21 10.13.0.1:32781 ip_route_input E 1793704378 ack 2720407272 ipid: 4853 tcp
59        16:40:31:052223 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver B 1793704378 ack 2720407272 ipid: 4853 tcp
60           16:40:31:052407 10.14.0.1:21 10.13.0.1:32781 nf_ip_local_in_hook - 1793704378 ack 2720407272 ipid: 4853 tcp
61           16:40:31:052593 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish B 1793704378 ack 2720407272 ipid: 4853 tcp
62           16:40:31:052788 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish E 1793704378 ack 2720407272 ipid: 4853 tcp
63        16:40:31:052981 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver E 1793704378 ack 2720407272 ipid: 4853 tcp
```

```
64      16:40:31:053177 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish E 1793704378 ack 2720407272 ipid: 4853 tcp
65   16:40:31:053377 10.14.0.1:21 10.13.0.1:32781 ip_rcv E 1793704378 ack 2720407272 ipid: 4853 tcp
     Time : 2043
66   16:40:31:226098 10.14.0.1:21 10.13.0.1:32781 another_ip_protocol - 1793704378 ack 2720407272 ipid: 4854 tcp
     Time : 0
67   16:40:31:226323 10.14.0.1:21 10.13.0.1:32781 ip_rcv B 1793704378 ack 2720407272 ipid: 4854 tcp
68      16:40:31:226534 10.14.0.1:21 10.13.0.1:32781 nf_ip_pre_routing_hook - 1793704378 ack 2720407272 ipid: 4854 tcp
69      16:40:31:226747 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish B 1793704378 ack 2720407272 ipid: 4854 tcp
70         16:40:31:226963 10.14.0.1:21 10.13.0.1:32781 ip_route_input B 1793704378 ack 2720407272 ipid: 4854 tcp
71         16:40:31:227184 10.14.0.1:21 10.13.0.1:32781 ip_route_input E 1793704378 ack 2720407272 ipid: 4854 tcp
72         16:40:31:227406 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver B 1793704378 ack 2720407272 ipid: 4854 tcp
73            16:40:31:227631 10.14.0.1:21 10.13.0.1:32781 nf_ip_local_in_hook - 1793704378 ack 2720407272 ipid: 4854 tcp
74            16:40:31:227860 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish B 1793704378 ack 2720407272 ipid: 4854 tcp
75            16:40:31:228098 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish E 1793704378 ack 2720407272 ipid: 4854 tcp
76         16:40:31:228333 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver E 1793704378 ack 2720407272 ipid: 4854 tcp
77      16:40:31:228571 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish E 1793704378 ack 2720407272 ipid: 4854 tcp
78   16:40:31:228813 10.14.0.1:21 10.13.0.1:32781 ip_rcv E 1793704378 ack 2720407272 ipid: 4854 tcp
     Time : 2490
79   16:40:31:261785 10.14.0.1:21 10.13.0.1:32781 another_ip_protocol - 1793704416 ack 2720407290 ipid: 4855 tcp
     Time : 0
80   16:40:31:262044 10.14.0.1:21 10.13.0.1:32781 ip_rcv B 1793704416 ack 2720407290 ipid: 4855 tcp
81      16:40:31:262296 10.14.0.1:21 10.13.0.1:32781 nf_ip_pre_routing_hook - 1793704416 ack 2720407290 ipid: 4855 tcp
82      16:40:31:262551 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish B 1793704416 ack 2720407290 ipid: 4855 tcp
83         16:40:31:262809 10.14.0.1:21 10.13.0.1:32781 ip_route_input B 1793704416 ack 2720407290 ipid: 4855 tcp
84         16:40:31:263071 10.14.0.1:21 10.13.0.1:32781 ip_route_input E 1793704416 ack 2720407290 ipid: 4855 tcp
85         16:40:31:263336 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver B 1793704416 ack 2720407290 ipid: 4855 tcp
86            16:40:31:263604 10.14.0.1:21 10.13.0.1:32781 nf_ip_local_in_hook - 1793704416 ack 2720407290 ipid: 4855 tcp
87            16:40:31:263874 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish B 1793704416 ack 2720407290 ipid: 4855 tcp
88            16:40:31:264152 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish E 1793704416 ack 2720407290 ipid: 4855 tcp
89         16:40:31:264430 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver E 1793704416 ack 2720407290 ipid: 4855 tcp
90      16:40:31:264710 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish E 1793704416 ack 2720407290 ipid: 4855 tcp
91   16:40:31:264994 10.14.0.1:21 10.13.0.1:32781 ip_rcv E 1793704416 ack 2720407290 ipid: 4855 tcp
     Time : 2950
92   16:40:32:782577 10.14.0.1:21 10.13.0.1:32781 another_ip_protocol - 1793704454 ack 2720407301 ipid: 4856 tcp
     Time : 0
93   16:40:32:782884 10.14.0.1:21 10.13.0.1:32781 ip_rcv B 1793704454 ack 2720407301 ipid: 4856 tcp
94      16:40:32:783179 10.14.0.1:21 10.13.0.1:32781 nf_ip_pre_routing_hook - 1793704454 ack 2720407301 ipid: 4856 tcp
```

```
95      16:40:32:783477 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish B 1793704454 ack 2720407301 ipid: 4856 tcp
96        16:40:32:783778 10.14.0.1:21 10.13.0.1:32781 ip_route_input B 1793704454 ack 2720407301 ipid: 4856 tcp
97        16:40:32:784083 10.14.0.1:21 10.13.0.1:32781 ip_route_input E 1793704454 ack 2720407301 ipid: 4856 tcp
98        16:40:32:784389 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver B 1793704454 ack 2720407301 ipid: 4856 tcp
99          16:40:32:784699 10.14.0.1:21 10.13.0.1:32781 nf_ip_local_in_hook - 1793704454 ack 2720407301 ipid: 4856 tcp
100           16:40:32:785013 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish B 1793704454 ack 2720407301 ipid: 4856 tcp
101           16:40:32:785334 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish E 1793704454 ack 2720407301 ipid: 4856 tcp
102       16:40:32:785670 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver E 1793704454 ack 2720407301 ipid: 4856 tcp
103     16:40:32:785993 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish E 1793704454 ack 2720407301 ipid: 4856 tcp
104   16:40:32:786319 10.14.0.1:21 10.13.0.1:32781 ip_rcv E 1793704454 ack 2720407301 ipid: 4856 tcp
    Time : 3435
105   16:40:32:986080 10.14.0.1:21 10.13.0.1:32781 another_ip_protocol - 1793704454 ack 2720407301 ipid: 4857 tcp
    Time : 0
106   16:40:32:986435 10.14.0.1:21 10.13.0.1:32781 ip_rcv B 1793704454 ack 2720407301 ipid: 4857 tcp
107     16:40:32:986773 10.14.0.1:21 10.13.0.1:32781 nf_ip_pre_routing_hook - 1793704454 ack 2720407301 ipid: 4857 tcp
108     16:40:32:987113 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish B 1793704454 ack 2720407301 ipid: 4857 tcp
109       16:40:32:987456 10.14.0.1:21 10.13.0.1:32781 ip_route_input B 1793704454 ack 2720407301 ipid: 4857 tcp
110       16:40:32:987803 10.14.0.1:21 10.13.0.1:32781 ip_route_input E 1793704454 ack 2720407301 ipid: 4857 tcp
111       16:40:32:988152 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver B 1793704454 ack 2720407301 ipid: 4857 tcp
112         16:40:32:988504 10.14.0.1:21 10.13.0.1:32781 nf_ip_local_in_hook - 1793704454 ack 2720407301 ipid: 4857 tcp
113         16:40:32:988860 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish B 1793704454 ack 2720407301 ipid: 4857 tcp
114         16:40:32:989248 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish E 1793704454 ack 2720407301 ipid: 4857 tcp
115       16:40:32:989624 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver E 1793704454 ack 2720407301 ipid: 4857 tcp
116     16:40:32:989990 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish E 1793704454 ack 2720407301 ipid: 4857 tcp
117   16:40:32:990358 10.14.0.1:21 10.13.0.1:32781 ip_rcv E 1793704454 ack 2720407301 ipid: 4857 tcp
    Time : 3923
118   16:40:36:014200 205.200.10.13:0 0.2.0.0:0 another_ip_protocol - ipid: 1540 unknown protocol
    Time : 0
119   16:40:36:014535 205.200.10.13:0 0.2.0.0:0 ip_route_input B ipid: 1540 unknown protocol
120   16:40:36:014849 205.200.10.13:0 0.2.0.0:0 ip_route_input E ipid: 1540 unknown protocol
    Time : 314
121   16:40:36:108975 10.14.0.1:21 10.13.0.1:32781 another_ip_protocol - 1793704488 ack 2720407316 ipid: 4858 tcp
    Time : 0
122   16:40:36:109378 10.14.0.1:21 10.13.0.1:32781 ip_rcv B 1793704488 ack 2720407316 ipid: 4858 tcp
123     16:40:36:109766 10.14.0.1:21 10.13.0.1:32781 nf_ip_pre_routing_hook - 1793704488 ack 2720407316 ipid: 4858 tcp
124     16:40:36:110157 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish B 1793704488 ack 2720407316 ipid: 4858 tcp
125       16:40:36:110550 10.14.0.1:21 10.13.0.1:32781 ip_route_input B 1793704488 ack 2720407316 ipid: 4858 tcp
```

126 16:40:36:110948 10.14.0.1:21 10.13.0.1:32781 ip_route_input E 1793704488 ack 2720407316 ipid: 4858 tcp
127 16:40:36:111348 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver B 1793704488 ack 2720407316 ipid: 4858 tcp
128 16:40:36:111767 10.14.0.1:21 10.13.0.1:32781 nf_ip_local_in_hook - 1793704488 ack 2720407316 ipid: 4858 tcp
129 16:40:36:112173 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish B 1793704488 ack 2720407316 ipid: 4858 tcp
130 16:40:36:112587 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish E 1793704488 ack 2720407316 ipid: 4858 tcp
131 16:40:36:113000 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver E 1793704488 ack 2720407316 ipid: 4858 tcp
132 16:40:36:113416 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish E 1793704488 ack 2720407316 ipid: 4858 tcp
133 16:40:36:113835 10.14.0.1:21 10.13.0.1:32781 ip_rcv E 1793704488 ack 2720407316 ipid: 4858 tcp
Time : 4457
134 16:40:36:120021 10.14.0.1:21 10.13.0.1:32781 another_ip_protocol - 1793704521 ack 2720407322 ipid: 4859 tcp
Time : 0
135 16:40:36:120469 10.14.0.1:21 10.13.0.1:32781 ip_rcv B 1793704521 ack 2720407322 ipid: 4859 tcp
136 16:40:36:120900 10.14.0.1:21 10.13.0.1:32781 nf_ip_pre_routing_hook - 1793704521 ack 2720407322 ipid: 4859 tcp
137 16:40:36:121332 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish B 1793704521 ack 2720407322 ipid: 4859 tcp
138 16:40:36:121786 10.14.0.1:21 10.13.0.1:32781 ip_route_input B 1793704521 ack 2720407322 ipid: 4859 tcp
139 16:40:36:122226 10.14.0.1:21 10.13.0.1:32781 ip_route_input E 1793704521 ack 2720407322 ipid: 4859 tcp
140 16:40:36:122668 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver B 1793704521 ack 2720407322 ipid: 4859 tcp
141 16:40:36:123113 10.14.0.1:21 10.13.0.1:32781 nf_ip_local_in_hook - 1793704521 ack 2720407322 ipid: 4859 tcp
142 16:40:36:123561 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish B 1793704521 ack 2720407322 ipid: 4859 tcp
143 16:40:36:124018 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish E 1793704521 ack 2720407322 ipid: 4859 tcp
144 16:40:36:124472 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver E 1793704521 ack 2720407322 ipid: 4859 tcp
145 16:40:36:124931 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish E 1793704521 ack 2720407322 ipid: 4859 tcp
146 16:40:36:125392 10.14.0.1:21 10.13.0.1:32781 ip_rcv E 1793704521 ack 2720407322 ipid: 4859 tcp
Time : 4923
147 16:40:38:943147 10.14.0.1:21 10.13.0.1:32781 another_ip_protocol - 1793704540 ack 2720407330 ipid: 4860 tcp
Time : 0
148 16:40:38:943637 10.14.0.1:21 10.13.0.1:32781 ip_rcv B 1793704540 ack 2720407330 ipid: 4860 tcp
149 16:40:38:944110 10.14.0.1:21 10.13.0.1:32781 nf_ip_pre_routing_hook - 1793704540 ack 2720407330 ipid: 4860 tcp
150 16:40:38:944585 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish B 1793704540 ack 2720407330 ipid: 4860 tcp
151 16:40:38:945063 10.14.0.1:21 10.13.0.1:32781 ip_route_input B 1793704540 ack 2720407330 ipid: 4860 tcp
152 16:40:38:945546 10.14.0.1:21 10.13.0.1:32781 ip_route_input E 1793704540 ack 2720407330 ipid: 4860 tcp
153 16:40:38:946030 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver B 1793704540 ack 2720407330 ipid: 4860 tcp
154 16:40:38:946517 10.14.0.1:21 10.13.0.1:32781 nf_ip_local_in_hook - 1793704540 ack 2720407330 ipid: 4860 tcp
155 16:40:38:947007 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish B 1793704540 ack 2720407330 ipid: 4860 tcp
156 16:40:38:947506 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish E 1793704540 ack 2720407330 ipid: 4860 tcp
157 16:40:38:948003 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver E 1793704540 ack 2720407330 ipid: 4860 tcp
158 16:40:38:948503 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish E 1793704540 ack 2720407330 ipid: 4860 tcp

159 16:40:38:949007 10.14.0.1:21 10.13.0.1:32781 ip_rcv E 1793704540 ack 2720407330 ipid: 4860 tcp
Time : 5370
160 16:40:38:971674 10.14.0.1:21 10.13.0.1:32781 another_ip_protocol - 1793704571 ack 2720407336 ipid: 4861 tcp
Time : 0
161 16:40:38:972211 10.14.0.1:21 10.13.0.1:32781 ip_rcv B 1793704571 ack 2720407336 ipid: 4861 tcp
162 16:40:38:972727 10.14.0.1:21 10.13.0.1:32781 nf_ip_pre_routing_hook - 1793704571 ack 2720407336 ipid: 4861 tcp
163 16:40:38:973244 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish B 1793704571 ack 2720407336 ipid: 4861 tcp
164 16:40:38:973764 10.14.0.1:21 10.13.0.1:32781 ip_route_input B 1793704571 ack 2720407336 ipid: 4861 tcp
165 16:40:38:974289 10.14.0.1:21 10.13.0.1:32781 ip_route_input E 1793704571 ack 2720407336 ipid: 4861 tcp
166 16:40:38:974815 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver B 1793704571 ack 2720407336 ipid: 4861 tcp
167 16:40:38:975344 10.14.0.1:21 10.13.0.1:32781 nf_ip_local_in_hook - 1793704571 ack 2720407336 ipid: 4861 tcp
168 16:40:38:975877 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish B 1793704571 ack 2720407336 ipid: 4861 tcp
169 16:40:38:976419 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish E 1793704571 ack 2720407336 ipid: 4861 tcp
170 16:40:38:976958 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver E 1793704571 ack 2720407336 ipid: 4861 tcp
171 16:40:38:977500 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish E 1793704571 ack 2720407336 ipid: 4861 tcp
172 16:40:38:978046 10.14.0.1:21 10.13.0.1:32781 ip_rcv E 1793704571 ack 2720407336 ipid: 4861 tcp
Time : 5835
173 16:40:39:025620 10.14.0.1:31031 10.13.0.1:32782 another_ip_protocol - 1795555424 ack 2724325490 ipid: 0 tcp
Time : 0
174 16:40:39:026200 10.14.0.1:31031 10.13.0.1:32782 ip_rcv B 1795555424 ack 2724325490 ipid: 0 tcp
175 16:40:39:026757 10.14.0.1:31031 10.13.0.1:32782 nf_ip_pre_routing_hook - 1795555424 ack 2724325490 ipid: 0 tcp
176 16:40:39:027317 10.14.0.1:31031 10.13.0.1:32782 ip_rcv_finish B 1795555424 ack 2724325490 ipid: 0 tcp
177 16:40:39:027879 10.14.0.1:31031 10.13.0.1:32782 ip_route_input B 1795555424 ack 2724325490 ipid: 0 tcp
178 16:40:39:028446 10.14.0.1:31031 10.13.0.1:32782 ip_route_input E 1795555424 ack 2724325490 ipid: 0 tcp
179 16:40:39:029015 10.14.0.1:31031 10.13.0.1:32782 ip_local_deliver B 1795555424 ack 2724325490 ipid: 0 tcp
180 16:40:39:029586 10.14.0.1:31031 10.13.0.1:32782 nf_ip_local_in_hook - 1795555424 ack 2724325490 ipid: 0 tcp
181 16:40:39:030162 10.14.0.1:31031 10.13.0.1:32782 ip_local_deliver_finish B 1795555424 ack 2724325490 ipid: 0 tcp
182 16:40:39:030774 10.14.0.1:31031 10.13.0.1:32782 ip_local_deliver_finish E 1795555424 ack 2724325490 ipid: 0 tcp
183 16:40:39:031397 10.14.0.1:31031 10.13.0.1:32782 ip_local_deliver E 1795555424 ack 2724325490 ipid: 0 tcp
184 16:40:39:031982 10.14.0.1:31031 10.13.0.1:32782 ip_rcv_finish E 1795555424 ack 2724325490 ipid: 0 tcp
185 16:40:39:032570 10.14.0.1:31031 10.13.0.1:32782 ip_rcv E 1795555424 ack 2724325490 ipid: 0 tcp
Time : 6370
186 16:40:39:033993 10.14.0.1:31031 10.13.0.1:32782 another_ip_protocol - 1795555425 ack 2724325490 ipid: 54807 tcp
Time : 0
187 16:40:39:034592 10.14.0.1:31031 10.13.0.1:32782 ip_rcv B 1795555425 ack 2724325490 ipid: 54807 tcp
188 16:40:39:035190 10.14.0.1:31031 10.13.0.1:32782 nf_ip_pre_routing_hook - 1795555425 ack 2724325490 ipid: 54807 tcp
189 16:40:39:035792 10.14.0.1:31031 10.13.0.1:32782 ip_rcv_finish B 1795555425 ack 2724325490 ipid: 54807 tcp

```
16:40:39:036397 10.14.0.1:31031 10.13.0.1:32782 ip_route_input B 1795555425 ack 2724325490 ipid: 54807 tcp
16:40:39:037006 10.14.0.1:31031 10.13.0.1:32782 ip_route_input E 1795555425 ack 2724325490 ipid: 54807 tcp
16:40:39:037617 10.14.0.1:31031 10.13.0.1:32782 ip_local_deliver B 1795555425 ack 2724325490 ipid: 54807 tcp
  16:40:39:038232 10.14.0.1:31031 10.13.0.1:32782 nf_ip_local_in_hook - 1795555425 ack 2724325490 ipid: 54807 tcp
  16:40:39:038850 10.14.0.1:31031 10.13.0.1:32782 ip_local_deliver_finish B 1795555425 ack 2724325490 ipid: 54807 tcp
  16:40:39:039487 10.14.0.1:31031 10.13.0.1:32782 ip_local_deliver_finish E 1795555425 ack 2724325490 ipid: 54807 tcp
16:40:39:040126 10.14.0.1:31031 10.13.0.1:32782 ip_local_deliver E 1795555425 ack 2724325490 ipid: 54807 tcp
16:40:39:040755 10.14.0.1:31031 10.13.0.1:32782 ip_rcv_finish E 1795555425 ack 2724325490 ipid: 54807 tcp
16:40:39:041401 10.14.0.1:31031 10.13.0.1:32782 ip_rcv E 1795555425 ack 2724325490 ipid: 54807 tcp
Time : 6809
16:40:39:042036 10.14.0.1:21 10.13.0.1:32781 another_ip_protocol - 1793704683 ack 2720407350 ipid: 4863 tcp
Time : 0
16:40:39:042677 10.14.0.1:21 10.13.0.1:32781 ip_rcv B 1793704683 ack 2720407350 ipid: 4863 tcp
16:40:39:043319 10.14.0.1:21 10.13.0.1:32781 nf_ip_pre_routing_hook - 1793704683 ack 2720407350 ipid: 4863 tcp
16:40:39:043963 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish B 1793704683 ack 2720407350 ipid: 4863 tcp
16:40:39:044612 10.14.0.1:21 10.13.0.1:32781 ip_route_input B 1793704683 ack 2720407350 ipid: 4863 tcp
16:40:39:045263 10.14.0.1:21 10.13.0.1:32781 ip_route_input E 1793704683 ack 2720407350 ipid: 4863 tcp
16:40:39:045917 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver B 1793704683 ack 2720407350 ipid: 4863 tcp
  16:40:39:046575 10.14.0.1:21 10.13.0.1:32781 nf_ip_local_in_hook - 1793704683 ack 2720407350 ipid: 4863 tcp
  16:40:39:047236 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish B 1793704683 ack 2720407350 ipid: 4863 tcp
  16:40:39:047902 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish E 1793704683 ack 2720407350 ipid: 4863 tcp
16:40:39:048569 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver E 1793704683 ack 2720407350 ipid: 4863 tcp
16:40:39:049240 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish E 1793704683 ack 2720407350 ipid: 4863 tcp
16:40:39:049914 10.14.0.1:21 10.13.0.1:32781 ip_rcv E 1793704683 ack 2720407350 ipid: 4863 tcp
Time : 7237
16:40:39:059862 10.14.0.1:21 10.13.0.1:32781 another_ip_protocol - 1793704617 ack 2720407350 ipid: 4862 tcp
Time : 0
16:40:39:060548 10.14.0.1:21 10.13.0.1:32781 ip_rcv B 1793704617 ack 2720407350 ipid: 4862 tcp
16:40:39:061232 10.14.0.1:21 10.13.0.1:32781 nf_ip_pre_routing_hook - 1793704617 ack 2720407350 ipid: 4862 tcp
16:40:39:061933 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish B 1793704617 ack 2720407350 ipid: 4862 tcp
16:40:39:062624 10.14.0.1:21 10.13.0.1:32781 ip_route_input B 1793704617 ack 2720407350 ipid: 4862 tcp
16:40:39:063318 10.14.0.1:21 10.13.0.1:32781 ip_route_input E 1793704617 ack 2720407350 ipid: 4862 tcp
16:40:39:064015 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver B 1793704617 ack 2720407350 ipid: 4862 tcp
  16:40:39:064715 10.14.0.1:21 10.13.0.1:32781 nf_ip_local_in_hook - 1793704617 ack 2720407350 ipid: 4862 tcp
  16:40:39:065418 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish B 1793704617 ack 2720407350 ipid: 4862 tcp
  16:40:39:066126 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish E 1793704617 ack 2720407350 ipid: 4862 tcp
16:40:39:066836 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver E 1793704617 ack 2720407350 ipid: 4862 tcp
```

223 16:40:39:067549 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish E 1793704617 ack 2720407350 ipid: 4862 tcp
224 16:40:39:068265 10.14.0.1:21 10.13.0.1:32781 ip_rcv E 1793704617 ack 2720407350 ipid: 4862 tcp
Time : 7717
225 16:40:39:069001 10.14.0.1:31031 10.13.0.1:32782 another_ip_protocol - 1795556187 ack 2724325490 ipid: 54808 tcp
Time : 0
226 16:40:39:069725 10.14.0.1:31031 10.13.0.1:32782 ip_rcv B 1795556187 ack 2724325490 ipid: 54808 tcp
227 16:40:39:070452 10.14.0.1:31031 10.13.0.1:32782 nf_ip_pre_routing_hook - 1795556187 ack 2724325490 ipid: 54808 tcp
228 16:40:39:071182 10.14.0.1:31031 10.13.0.1:32782 ip_rcv_finish B 1795556187 ack 2724325490 ipid: 54808 tcp
229 16:40:39:071929 10.14.0.1:31031 10.13.0.1:32782 ip_route_input B 1795556187 ack 2724325490 ipid: 54808 tcp
230 16:40:39:072666 10.14.0.1:31031 10.13.0.1:32782 ip_route_input E 1795556187 ack 2724325490 ipid: 54808 tcp
231 16:40:39:073406 10.14.0.1:31031 10.13.0.1:32782 ip_local_deliver B 1795556187 ack 2724325490 ipid: 54808 tcp
232 16:40:39:074149 10.14.0.1:31031 10.13.0.1:32782 nf_ip_local_in_hook - 1795556187 ack 2724325490 ipid: 54808 tcp
233 16:40:39:074895 10.14.0.1:31031 10.13.0.1:32782 ip_local_deliver_finish B 1795556187 ack 2724325490 ipid: 54808 tcp
234 16:40:39:075648 10.14.0.1:31031 10.13.0.1:32782 ip_local_deliver_finish E 1795556187 ack 2724325490 ipid: 54808 tcp
235 16:40:39:076402 10.14.0.1:31031 10.13.0.1:32782 ip_local_deliver E 1795556187 ack 2724325490 ipid: 54808 tcp
236 16:40:39:077159 10.14.0.1:31031 10.13.0.1:32782 ip_rcv_finish E 1795556187 ack 2724325490 ipid: 54808 tcp
237 16:40:39:077919 10.14.0.1:31031 10.13.0.1:32782 ip_rcv E 1795556187 ack 2724325490 ipid: 54808 tcp
Time : 8194
238 16:40:39:100822 10.14.0.1:31031 10.13.0.1:32782 another_ip_protocol - 1795556188 ack 2724325491 ipid: 54809 tcp
Time : 0
239 16:40:39:101650 10.14.0.1:31031 10.13.0.1:32782 ip_rcv B 1795556188 ack 2724325491 ipid: 54809 tcp
240 16:40:39:102423 10.14.0.1:31031 10.13.0.1:32782 nf_ip_pre_routing_hook - 1795556188 ack 2724325491 ipid: 54809 tcp
241 16:40:39:103197 10.14.0.1:31031 10.13.0.1:32782 ip_rcv_finish B 1795556188 ack 2724325491 ipid: 54809 tcp
242 16:40:39:103975 10.14.0.1:31031 10.13.0.1:32782 ip_route_input B 1795556188 ack 2724325491 ipid: 54809 tcp
243 16:40:39:104757 10.14.0.1:31031 10.13.0.1:32782 ip_route_input E 1795556188 ack 2724325491 ipid: 54809 tcp
244 16:40:39:105541 10.14.0.1:31031 10.13.0.1:32782 ip_local_deliver B 1795556188 ack 2724325491 ipid: 54809 tcp
245 16:40:39:106329 10.14.0.1:31031 10.13.0.1:32782 nf_ip_local_in_hook - 1795556188 ack 2724325491 ipid: 54809 tcp
246 16:40:39:107119 10.14.0.1:31031 10.13.0.1:32782 ip_local_deliver_finish B 1795556188 ack 2724325491 ipid: 54809 tcp
247 16:40:39:107937 10.14.0.1:31031 10.13.0.1:32782 ip_local_deliver_finish E 1795556188 ack 2724325491 ipid: 54809 tcp
248 16:40:39:108735 10.14.0.1:31031 10.13.0.1:32782 ip_local_deliver E 1795556188 ack 2724325491 ipid: 54809 tcp
249 16:40:39:109536 10.14.0.1:31031 10.13.0.1:32782 ip_rcv_finish E 1795556188 ack 2724325491 ipid: 54809 tcp
250 16:40:39:110340 10.14.0.1:31031 10.13.0.1:32782 ip_rcv E 1795556188 ack 2724325491 ipid: 54809 tcp
Time : 8690
251 16:40:41:708469 10.14.0.1:21 10.13.0.1:32781 another_ip_protocol - 1793704716 ack 2720407356 ipid: 4865 tcp
Time : 0
252 16:40:41:709311 10.14.0.1:21 10.13.0.1:32781 ip_rcv B 1793704716 ack 2720407356 ipid: 4865 tcp
253 16:40:41:710127 10.14.0.1:21 10.13.0.1:32781 nf_ip_pre_routing_hook - 1793704716 ack 2720407356 ipid: 4865 tcp

```
16:40:41:710945 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish B 1793704716 ack 2720407356 ipid: 4865 tcp
  16:40:41:711781 10.14.0.1:21 10.13.0.1:32781 ip_route_input B 1793704716 ack 2720407356 ipid: 4865 tcp
  16:40:41:712607 10.14.0.1:21 10.13.0.1:32781 ip_route_input E 1793704716 ack 2720407356 ipid: 4865 tcp
  16:40:41:713451 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver B 1793704716 ack 2720407356 ipid: 4865 tcp
    16:40:41:714281 10.14.0.1:21 10.13.0.1:32781 nf_ip_local_in_hook - 1793704716 ack 2720407356 ipid: 4865 tcp
    16:40:41:715115 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish B 1793704716 ack 2720407356 ipid: 4865 tcp
    16:40:41:715956 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish E 1793704716 ack 2720407356 ipid: 4865 tcp
  16:40:41:716796 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver E 1793704716 ack 2720407356 ipid: 4865 tcp
16:40:41:717639 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish E 1793704716 ack 2720407356 ipid: 4865 tcp
16:40:41:718486 10.14.0.1:21 10.13.0.1:32781 ip_rcv E 1793704716 ack 2720407356 ipid: 4865 tcp
Time : 9175
16:40:41:719335 10.14.0.1:21 10.13.0.1:32781 another_ip_protocol - 1793704702 ack 2720407356 ipid: 4864 tcp
Time : 0
16:40:41:720190 10.14.0.1:21 10.13.0.1:32781 ip_rcv B 1793704702 ack 2720407356 ipid: 4864 tcp
16:40:41:721046 10.14.0.1:21 10.13.0.1:32781 nf_ip_pre_routing_hook - 1793704702 ack 2720407356 ipid: 4864 tcp
16:40:41:721920 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish B 1793704702 ack 2720407356 ipid: 4864 tcp
  16:40:41:722782 10.14.0.1:21 10.13.0.1:32781 ip_route_input B 1793704702 ack 2720407356 ipid: 4864 tcp
  16:40:41:723648 10.14.0.1:21 10.13.0.1:32781 ip_route_input E 1793704702 ack 2720407356 ipid: 4864 tcp
  16:40:41:724517 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver B 1793704702 ack 2720407356 ipid: 4864 tcp
    16:40:41:725390 10.14.0.1:21 10.13.0.1:32781 nf_ip_local_in_hook - 1793704702 ack 2720407356 ipid: 4864 tcp
    16:40:41:726265 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish B 1793704702 ack 2720407356 ipid: 4864 tcp
    16:40:41:727144 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish E 1793704702 ack 2720407356 ipid: 4864 tcp
  16:40:41:728026 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver E 1793704702 ack 2720407356 ipid: 4864 tcp
16:40:41:728912 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish E 1793704702 ack 2720407356 ipid: 4864 tcp
16:40:41:729800 10.14.0.1:21 10.13.0.1:32781 ip_rcv E 1793704702 ack 2720407356 ipid: 4864 tcp
Time : 9610
16:40:41:731094 10.14.0.1:21 10.13.0.1:32781 another_ip_protocol - 1793704717 ack 2720407357 ipid: 0 tcp
Time : 0
16:40:41:732011 10.14.0.1:21 10.13.0.1:32781 ip_rcv B 1793704717 ack 2720407357 ipid: 0 tcp
16:40:41:732910 10.14.0.1:21 10.13.0.1:32781 nf_ip_pre_routing_hook - 1793704717 ack 2720407357 ipid: 0 tcp
16:40:41:733812 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish B 1793704717 ack 2720407357 ipid: 0 tcp
  16:40:41:734717 10.14.0.1:21 10.13.0.1:32781 ip_route_input B 1793704717 ack 2720407357 ipid: 0 tcp
  16:40:41:735637 10.14.0.1:21 10.13.0.1:32781 ip_route_input E 1793704717 ack 2720407357 ipid: 0 tcp
  16:40:41:736548 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver B 1793704717 ack 2720407357 ipid: 0 tcp
    16:40:41:737462 10.14.0.1:21 10.13.0.1:32781 nf_ip_local_in_hook - 1793704717 ack 2720407357 ipid: 0 tcp
    16:40:41:738379 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish B 1793704717 ack 2720407357 ipid: 0 tcp
    16:40:41:739311 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver_finish E 1793704717 ack 2720407357 ipid: 0 tcp
```

287 16:40:41:740235 10.14.0.1:21 10.13.0.1:32781 ip_local_deliver E 1793704717 ack 2720407357 ipid: 0 tcp
288 16:40:41:741161 10.14.0.1:21 10.13.0.1:32781 ip_rcv_finish E 1793704717 ack 2720407357 ipid: 0 tcp
289 16:40:41:742106 10.14.0.1:21 10.13.0.1:32781 ip_rcv E 1793704717 ack 2720407357 ipid: 0 tcp
Time : 10095

12.23.6 LOG_DUMP_RCV

1 16:40:17.816406 CDP v1, ttl=180s DevID 'Lab Switch 3(000a57-c08d00)' Addr (1): IPv4 127.0.0.1 PortID '21' CAP 0x08[|cdp]
2 16:40:31.016488 franklin.internet.lab.32768 > 10.3.0.254.domain: 10855+ A? hawking.internet.lab. (38) (DF)
3 16:40:31.018620 10.3.0.254.domain > franklin.internet.lab.32768: 10855* 1/1/1 A 10.14.0.1 (91) (DF)
4 16:40:31.019035 franklin.internet.lab.32781 > 10.14.0.1.ftp: S 2720407258:2720407258(0) win 5840 <mss 1460,sackOK,timestamp 392399 0,nop,wscale 0> (DF)
5 16:40:31.019366 10.14.0.1.ftp > franklin.internet.lab.32781: S 1793704357:1793704357(0) ack 2720407259 win 5792 <mss 1460,sackOK,timestamp 303747925 392399,nop,wscale 0> (DF)
6 16:40:31.019849 franklin.internet.lab.32781 > 10.14.0.1.ftp: . ack 1793704358 win 5840 <nop,nop,timestamp 392399 303747925> (DF)
7 16:40:31.021740 10.14.0.1.ftp > franklin.internet.lab.32781: P 1793704358:1793704378(20) ack 2720407259 win 5792 <nop,nop,timestamp 303747925 392399> (DF)
8 16:40:31.022638 franklin.internet.lab.32781 > 10.14.0.1.ftp: . ack 1793704378 win 5840 <nop,nop,timestamp 392400 303747925> (DF) [tos 0x10]
9 16:40:31.025545 franklin.internet.lab.32781 > 10.14.0.1.ftp: P 2720407259:2720407272(13) ack 1793704378 win 5840 <nop,nop,timestamp 392400 303747925> (DF) [tos 0x10]
10 16:40:31.025817 10.14.0.1.ftp > franklin.internet.lab.32781: . ack 2720407272 win 5792 <nop,nop,timestamp 303747925 392400> (DF)
11 16:40:31.051145 10.14.0.1.ftp > franklin.internet.lab.32781: P 1793704378:1793704416(38) ack 2720407272 win 5792 <nop,nop,timestamp 303747925 392400> (DF)
12 16:40:31.053744 franklin.internet.lab.32781 > 10.14.0.1.ftp: P 2720407272:2720407290(18) ack 1793704416 win 5840 <nop,nop,timestamp 392403 303747925> (DF) [tos 0x10]
13 16:40:31.226090 10.14.0.1.ftp > franklin.internet.lab.32781: P 1793704378:1793704416(38) ack 2720407272 win 5792 <nop,nop,timestamp 303747946 392400> (DF)
14 16:40:31.229117 franklin.internet.lab.32781 > 10.14.0.1.ftp: . ack 1793704416 win 5840 <nop,nop,timestamp 392420 303747946,nop,nop,sack sack 1 {1793704378:1793704416} > (DF) [tos 0x10]
15 16:40:31.261384 franklin.internet.lab.32781 > 10.14.0.1.ftp: P 2720407272:2720407290(18) ack 1793704416 win 5840 <nop,nop,timestamp 392424 303747946> (DF) [tos 0x10]
16 16:40:31.261780 10.14.0.1.ftp > franklin.internet.lab.32781: P 1793704416:1793704454(38) ack 2720407290 win 5792 <nop,nop,timestamp 303747949 392424> (DF)
17 16:40:31.265928 franklin.internet.lab.32781 > 10.14.0.1.ftp: . ack 1793704454 win 5840 <nop,nop,timestamp 392424 303747949> (DF) [tos 0x10]
18 16:40:32.782157 franklin.internet.lab.32781 > 10.14.0.1.ftp: P 2720407290:2720407301(11) ack 1793704454 win 5840 <nop,nop,timestamp 392576 303747949> (DF) [tos 0x10]
19 16:40:32.782570 10.14.0.1.ftp > franklin.internet.lab.32781: P 1793704454:1793704488(34) ack 2720407301 win 5792 <nop,nop,timestamp 303748101 392576> (DF)
20 16:40:32.787808 franklin.internet.lab.32781 > 10.14.0.1.ftp: . ack 1793704488 win 5840 <nop,nop,timestamp 392576 303748101> (DF) [tos 0x10]
21 16:40:32.986072 10.14.0.1.ftp > franklin.internet.lab.32781: P 1793704454:1793704488(34) ack 2720407301 win 5792 <nop,nop,timestamp 303748122 392576> (DF)
22 16:40:32.989240 franklin.internet.lab.32781 > 10.14.0.1.ftp: . ack 1793704488 win 5840 <nop,nop,timestamp 392596 303748122,nop,nop,sack sack 1 {1793704454:1793704488} > (DF) [tos 0x10]
23 16:40:36.014192 arp who-has franklin.internet.lab tell 10.13.0.2
24 16:40:36.015170 arp reply franklin.internet.lab is-at 0:2:b3:d3:d4:8a
25 16:40:36.104512 franklin.internet.lab.32781 > 10.14.0.1.ftp: P 2720407301:2720407316(15) ack 1793704488 win 5840 <nop,nop,timestamp 392908 303748122> (DF) [tos 0x10]
26 16:40:36.108968 10.14.0.1.ftp > franklin.internet.lab.32781: P 1793704488:1793704521(33) ack 2720407316 win 5792 <nop,nop,timestamp 303748434 392908> (DF)
27 16:40:36.114285 franklin.internet.lab.32781 > 10.14.0.1.ftp: . ack 1793704521 win 5840 <nop,nop,timestamp 392909 303748434> (DF) [tos 0x10]
28 16:40:36.114330 franklin.internet.lab.32781 > 10.14.0.1.ftp: P 2720407316:2720407322(6) ack 1793704521 win 5840 <nop,nop,timestamp 392909 303748434> (DF) [tos 0x10]
29 16:40:36.120013 10.14.0.1.ftp > franklin.internet.lab.32781: P 1793704521:1793704540(19) ack 2720407322 win 5792 <nop,nop,timestamp 303748434 392909> (DF)

30 16:40:36.161390 franklin.internet.lab.32781 > 10.14.0.1.ftp: . ack 1793704540 win 5840 <nop,nop,timestamp 392914 303748434> (DF) [tos 0x10]
31 16:40:38.942682 franklin.internet.lab.32781 > 10.14.0.1.ftp: P 2720407322:2720407330(8) ack 1793704540 win 5840 <nop,nop,timestamp 393192 303748434> (DF) [tos 0x10]
32 16:40:38.943141 10.14.0.1.ftp > franklin.internet.lab.32781: P 1793704540:1793704571(31) ack 2720407330 win 5792 <nop,nop,timestamp 303748717 393192> (DF)
33 16:40:38.949535 franklin.internet.lab.32781 > 10.14.0.1.ftp: . ack 1793704571 win 5840 <nop,nop,timestamp 393192 303748717> (DF) [tos 0x10]
34 16:40:38.949573 franklin.internet.lab.32781 > 10.14.0.1.ftp: P 2720407330:2720407336(6) ack 1793704571 win 5840 <nop,nop,timestamp 393192 303748717> (DF) [tos 0x10]
35 16:40:38.971666 10.14.0.1.ftp > franklin.internet.lab.32781: P 1793704571:1793704617(46) ack 2720407336 win 5792 <nop,nop,timestamp 303748718 393192> (DF)
36 16:40:38.978768 franklin.internet.lab.32782 > 10.14.0.1.31031: S 2724325489:2724325489(0) win 5840 <mss 1460,sackOK,timestamp 393195 0,nop,wscale 0> (DF)
37 16:40:39.011395 franklin.internet.lab.32781 > 10.14.0.1.ftp: . ack 1793704617 win 5840 <nop,nop,timestamp 393199 303748718> (DF) [tos 0x10]
38 16:40:39.025613 10.14.0.1.31031 > franklin.internet.lab.32782: S 1795555424:1795555424(0) ack 2724325490 win 5792 <mss 1460,sackOK,timestamp 303748721 393195,nop,wscale 0> (DF)
39 16:40:39.030766 franklin.internet.lab.32782 > 10.14.0.1.31031: . ack 1795555425 win 5840 <nop,nop,timestamp 393200 303748721> (DF)
40 16:40:39.033235 franklin.internet.lab.32781 > 10.14.0.1.ftp: P 2720407336:2720407350(14) ack 1793704617 win 5840 <nop,nop,timestamp 393201 303748718> (DF) [tos 0x10]
41 16:40:39.033987 10.14.0.1.31031 > franklin.internet.lab.32782: P 1795555425:1795556187(762) ack 2724325490 win 5792 <nop,nop,timestamp 303748726 393200> (DF) [tos 0x8]
42 16:40:39.039482 franklin.internet.lab.32782 > 10.14.0.1.31031: . ack 1795556187 win 6858 <nop,nop,timestamp 393201 303748726> (DF) [tos 0x8]
43 16:40:39.033989 10.14.0.1.ftp > franklin.internet.lab.32781: P 1793704683:1793704702(19) ack 2720407350 win 5792 <nop,nop,timestamp 303748726 393201> (DF)
44 16:40:39.050616 franklin.internet.lab.32781 > 10.14.0.1.ftp: . ack 1793704617 win 5840 <nop,nop,timestamp 393202 303748718,nop,nop,sack sack 1 {1793704683:1793704702} > (DF) [tos 0x10]
45 16:40:39.059857 10.14.0.1.ftp > franklin.internet.lab.32781: P 1793704617:1793704683(66) ack 2720407350 win 5792 <nop,nop,timestamp 303748726 393201> (DF)
46 16:40:39.068942 10.14.0.1.31031 > franklin.internet.lab.32782: F 1795556187:1795556187(0) ack 2724325490 win 5792 <nop,nop,timestamp 303748726 393200> (DF) [tos 0x8]

12.23.7 LOG_IP_FORWARD

```
1    18:04:21:563042   ip_forward B 0
2       18:04:21:563054   np_ip_forward_hook - 0
3       18:04:21:563058   ip_forward_finish B 0
4          18:04:21:563062   ip_send B 59885
5          18:04:21:563080 10.13.0.1:17664 10.10.0.2:60 ip_send E 59885
6       18:04:21:563089 10.13.0.1:17664 10.10.0.2:60 ip_forward_finish E 59885
7    18:04:21:563099 10.13.0.1:17664 10.10.0.2:60 ip_forward E 59885
     Time : 57
8    18:04:21:563346   ip_forward B 0
9       18:04:21:563353   np_ip_forward_hook - 0
10      18:04:21:563362   ip_forward_finish B 0
11         18:04:21:563371   ip_send B 0
12         18:04:21:563384 10.10.0.2:17664 10.13.0.1:60 ip_send E 0
13      18:04:21:563416 10.10.0.2:17664 10.13.0.1:60 ip_forward_finish E 0
14   18:04:21:563433 10.10.0.2:17664 10.13.0.1:60 ip_forward E 0
     Time : 87
15   18:04:21:563971   ip_forward B 0
16      18:04:21:563984   np_ip_forward_hook - 0
17      18:04:21:563997   ip_forward_finish B 0
18         18:04:21:564011   ip_send B 59886
19         18:04:21:564027 10.13.0.1:17664 10.10.0.2:52 ip_send E 59886
20      18:04:21:564051 10.13.0.1:17664 10.10.0.2:52 ip_forward_finish E 59886
21   18:04:21:564076 10.13.0.1:17664 10.10.0.2:52 ip_forward E 59886
     Time : 105
22   18:04:21:622460   ip_forward B 0
23      18:04:21:622486   np_ip_forward_hook - 0
24      18:04:21:622504   ip_forward_finish B 0
25         18:04:21:622523   ip_send B 30779
26         18:04:21:622549 10.10.0.2:17664 10.13.0.1:72 ip_send E 30779
27      18:04:21:622581 10.10.0.2:17664 10.13.0.1:72 ip_forward_finish E 30779
28   18:04:21:622615 10.10.0.2:17664 10.13.0.1:72 ip_forward E 30779
     Time : 155
29   18:04:21:623338   ip_forward B 0
30      18:04:21:623360   np_ip_forward_hook - 0
31      18:04:21:623384   ip_forward_finish B 0
```

```
32          18:04:21:623408   ip_send B 59887
33          18:04:21:623437 10.13.0.1:17680 10.10.0.2:52 ip_send E 59887
34       18:04:21:623489 10.13.0.1:17680 10.10.0.2:52 ip_forward_finish E 59887
35    18:04:21:623530 10.13.0.1:17680 10.10.0.2:52 ip_forward E 59887
      Time : 192
36    18:04:21:635306   ip_forward B 0
37       18:04:21:635334   np_ip_forward_hook - 0
38       18:04:21:635362   ip_forward_finish B 0
39          18:04:21:635392   ip_send B 59888
40          18:04:21:635423 10.13.0.1:17680 10.10.0.2:65 ip_send E 59888
41       18:04:21:635470 10.13.0.1:17680 10.10.0.2:65 ip_forward_finish E 59888
42    18:04:21:635535 10.13.0.1:17680 10.10.0.2:65 ip_forward E 59888
      Time : 229
43    18:04:21:635601   ip_forward B 0
44       18:04:21:635635   np_ip_forward_hook - 0
45       18:04:21:635668   ip_forward_finish B 0
46          18:04:21:635702   ip_send B 30780
47          18:04:21:635738 10.10.0.2:17664 10.13.0.1:52 ip_send E 30780
48       18:04:21:635793 10.10.0.2:17664 10.13.0.1:52 ip_forward_finish E 30780
49    18:04:21:635850 10.10.0.2:17664 10.13.0.1:52 ip_forward E 30780
      Time : 249
50    18:04:21:635925   ip_forward B 0
51       18:04:21:635963   np_ip_forward_hook - 0
52       18:04:21:636002   ip_forward_finish B 0
53          18:04:21:636041   ip_send B 30781
54          18:04:21:636082 10.10.0.2:17664 10.13.0.1:90 ip_send E 30781
55       18:04:21:636145 10.10.0.2:17664 10.13.0.1:90 ip_forward_finish E 30781
56    18:04:21:636227 10.10.0.2:17664 10.13.0.1:90 ip_forward E 30781
      Time : 302
57    18:04:21:673557   ip_forward B 0
58       18:04:21:673607   np_ip_forward_hook - 0
59       18:04:21:673650   ip_forward_finish B 0
60          18:04:21:673695   ip_send B 59890
61          18:04:21:673747 10.13.0.1:17680 10.10.0.2:70 ip_send E 59890
62       18:04:21:673818 10.13.0.1:17680 10.10.0.2:70 ip_forward_finish E 59890
63    18:04:21:673908 10.13.0.1:17680 10.10.0.2:70 ip_forward E 59890
      Time : 351
```

```
18:04:21:673983   ip_forward B 0
   18:04:21:674032   np_ip_forward_hook - 0
   18:04:21:674080   ip_forward_finish B 0
      18:04:21:674130   ip_send B 30782
      18:04:21:674182 10.10.0.2:17664 10.13.0.1:90 ip_send E 30782
   18:04:21:674261 10.10.0.2:17664 10.13.0.1:90 ip_forward_finish E 30782
18:04:21:674358 10.10.0.2:17664 10.13.0.1:90 ip_forward E 30782
Time : 375
18:04:21:674911   ip_forward B 0
   18:04:21:674965   np_ip_forward_hook - 0
   18:04:21:675018   ip_forward_finish B 0
      18:04:21:675073   ip_send B 59891
      18:04:21:675130 10.13.0.1:17680 10.10.0.2:52 ip_send E 59891
   18:04:21:675216 10.13.0.1:17680 10.10.0.2:52 ip_forward_finish E 59891
18:04:21:675317 10.13.0.1:17680 10.10.0.2:52 ip_forward E 59891
Time : 406
18:04:23:474458   ip_forward B 0
   18:04:23:474525   np_ip_forward_hook - 0
   18:04:23:474584   ip_forward_finish B 0
      18:04:23:474644   ip_send B 59892
      18:04:23:474713 10.13.0.1:17680 10.10.0.2:63 ip_send E 59892
   18:04:23:474809 10.13.0.1:17680 10.10.0.2:63 ip_forward_finish E 59892
18:04:23:474935 10.13.0.1:17680 10.10.0.2:63 ip_forward E 59892
Time : 477
18:04:23:475034   ip_forward B 0
   18:04:23:475098   np_ip_forward_hook - 0
   18:04:23:475162   ip_forward_finish B 0
      18:04:23:475227   ip_send B 30783
      18:04:23:475295 10.10.0.2:17664 10.13.0.1:86 ip_send E 30783
   18:04:23:475398 10.10.0.2:17664 10.13.0.1:86 ip_forward_finish E 30783
18:04:23:475519 10.10.0.2:17664 10.13.0.1:86 ip_forward E 30783
Time : 485
18:04:23:476035   ip_forward B 0
   18:04:23:476104   np_ip_forward_hook - 0
   18:04:23:476173   ip_forward_finish B 0
      18:04:23:476243   ip_send B 59893
      18:04:23:476315 10.13.0.1:17680 10.10.0.2:52 ip_send E 59893
```

```
97      18:04:23:476426 10.13.0.1:17680 10.10.0.2:52 ip_forward_finish E 59893
98   18:04:23:476550 10.13.0.1:17680 10.10.0.2:52 ip_forward E 59893
     Time : 515
99   18:04:25:905601   ip_forward B 0
100     18:04:25:905682   np_ip_forward_hook - 0
101     18:04:25:905757   ip_forward_finish B 0
102        18:04:25:905832   ip_send B 59894
103        18:04:25:905917 10.13.0.1:17680 10.10.0.2:67 ip_send E 59894
104     18:04:25:906036 10.13.0.1:17680 10.10.0.2:67 ip_forward_finish E 59894
105  18:04:25:906170 10.13.0.1:17680 10.10.0.2:67 ip_forward E 59894
     Time : 569
106  18:04:25:945168   ip_forward B 0
107     18:04:25:945248   np_ip_forward_hook - 0
108     18:04:25:945328   ip_forward_finish B 0
109        18:04:25:945408   ip_send B 30784
110        18:04:25:945493 10.10.0.2:17664 10.13.0.1:52 ip_send E 30784
111     18:04:25:945636 10.10.0.2:17664 10.13.0.1:52 ip_forward_finish E 30784
112  18:04:25:945764 10.10.0.2:17664 10.13.0.1:52 ip_forward E 30784
     Time : 596
113  18:04:25:970109   ip_forward B 0
114     18:04:25:970201   np_ip_forward_hook - 0
115     18:04:25:970286   ip_forward_finish B 0
116        18:04:25:970372   ip_send B 30785
117        18:04:25:970466 10.10.0.2:17664 10.13.0.1:75 ip_send E 30785
118     18:04:25:970619 10.10.0.2:17664 10.13.0.1:75 ip_forward_finish E 30785
119  18:04:25:970755 10.10.0.2:17664 10.13.0.1:75 ip_forward E 30785
     Time : 646
120  18:04:26:173153   ip_forward B 0
121     18:04:26:173250   np_ip_forward_hook - 0
122     18:04:26:173340   ip_forward_finish B 0
123        18:04:26:173431   ip_send B 30786
124        18:04:26:173530 10.10.0.2:17664 10.13.0.1:75 ip_send E 30786
125     18:04:26:173691 10.10.0.2:17664 10.13.0.1:75 ip_forward_finish E 30786
126  18:04:26:173834 10.10.0.2:17664 10.13.0.1:75 ip_forward E 30786
     Time : 681
127  18:04:26:174178   ip_forward B 0
128     18:04:26:174272   np_ip_forward_hook - 0
```

```
129     18:04:26:174366   ip_forward_finish B 0
130       18:04:26:174462   ip_send B 59895
131       18:04:26:174561 10.13.0.1:17680 10.10.0.2:52 ip_send E 59895
132     18:04:26:174723 10.13.0.1:17680 10.10.0.2:52 ip_forward_finish E 59895
133   18:04:26:174874 10.13.0.1:17680 10.10.0.2:52 ip_forward E 59895
    Time : 696
134   18:04:26:378845   ip_forward B 0
135     18:04:26:378952   np_ip_forward_hook - 0
136     18:04:26:379052   ip_forward_finish B 0
137       18:04:26:379153   ip_send B 59897
138       18:04:26:379262 10.13.0.1:17680 10.10.0.2:58 ip_send E 59897
139     18:04:26:379451 10.13.0.1:17680 10.10.0.2:58 ip_forward_finish E 59897
140   18:04:26:379625 10.13.0.1:17680 10.10.0.2:58 ip_forward E 59897
    Time : 780
141   18:04:26:379787   ip_forward B 0
142     18:04:26:379892   np_ip_forward_hook - 0
143     18:04:26:379996   ip_forward_finish B 0
144       18:04:26:380103   ip_send B 30787
145       18:04:26:380211 10.10.0.2:17664 10.13.0.1:52 ip_send E 30787
146     18:04:26:380394 10.10.0.2:17664 10.13.0.1:52 ip_forward_finish E 30787
147   18:04:26:380561 10.10.0.2:17664 10.13.0.1:52 ip_forward E 30787
    Time : 774
148   18:04:26:380730   ip_forward B 0
149     18:04:26:380840   np_ip_forward_hook - 0
150     18:04:26:380949   ip_forward_finish B 0
151       18:04:26:381060   ip_send B 30788
152       18:04:26:381174 10.10.0.2:17664 10.13.0.1:71 ip_send E 30788
153     18:04:26:381363 10.10.0.2:17664 10.13.0.1:71 ip_forward_finish E 30788
154   18:04:26:381539 10.10.0.2:17664 10.13.0.1:71 ip_forward E 30788
    Time : 809
155   18:04:26:418820   ip_forward B 0
156     18:04:26:418944   np_ip_forward_hook - 0
157     18:04:26:419060   ip_forward_finish B 0
158       18:04:26:419176   ip_send B 59898
159       18:04:26:419301 10.13.0.1:17680 10.10.0.2:52 ip_send E 59898
160     18:04:26:419496 10.13.0.1:17680 10.10.0.2:52 ip_forward_finish E 59898
161   18:04:26:419679 10.13.0.1:17680 10.10.0.2:52 ip_forward E 59898
```

```
    Time : 859
162  18:04:29:478377   ip_forward B 0
163     18:04:29:478505   np_ip_forward_hook - 0
164     18:04:29:478625   ip_forward_finish B 0
165        18:04:29:478747   ip_send B 59899
166        18:04:29:478878 10.13.0.1:17680 10.10.0.2:60 ip_send E 59899
167     18:04:29:479097 10.13.0.1:17680 10.10.0.2:60 ip_forward_finish E 59899
168  18:04:29:479289 10.13.0.1:17680 10.10.0.2:60 ip_forward E 59899
    Time : 912
169  18:04:29:479482   ip_forward B 0
170     18:04:29:479607   np_ip_forward_hook - 0
171     18:04:29:479732   ip_forward_finish B 0
172        18:04:29:479859   ip_send B 30789
173        18:04:29:479989 10.10.0.2:17664 10.13.0.1:83 ip_send E 30789
174     18:04:29:480203 10.10.0.2:17664 10.13.0.1:83 ip_forward_finish E 30789
175  18:04:29:480402 10.10.0.2:17664 10.13.0.1:83 ip_forward E 30789
    Time : 920
176  18:04:29:480731   ip_forward B 0
177     18:04:29:480861   np_ip_forward_hook - 0
178     18:04:29:480991   ip_forward_finish B 0
179        18:04:29:481123   ip_send B 59900
180        18:04:29:481256 10.13.0.1:17680 10.10.0.2:52 ip_send E 59900
181     18:04:29:481474 10.13.0.1:17680 10.10.0.2:52 ip_forward_finish E 59900
182  18:04:29:481681 10.13.0.1:17680 10.10.0.2:52 ip_forward E 59900
    Time : 950
183  18:04:29:481889   ip_forward B 0
184     18:04:29:482025   np_ip_forward_hook - 0
185     18:04:29:482160   ip_forward_finish B 0
186        18:04:29:482296   ip_send B 59901
187        18:04:29:482449 10.13.0.1:17680 10.10.0.2:58 ip_send E 59901
188     18:04:29:482689 10.13.0.1:17680 10.10.0.2:58 ip_forward_finish E 59901
189  18:04:29:482904 10.13.0.1:17680 10.10.0.2:58 ip_forward E 59901
    Time : 1015
190  18:04:29:483121   ip_forward B 0
191     18:04:29:483261   np_ip_forward_hook - 0
192     18:04:29:483401   ip_forward_finish B 0
193        18:04:29:483543   ip_send B 30790
```

```
194         18:04:29:483686 10.10.0.2:17664 10.13.0.1:99 ip_send E 30790
195       18:04:29:483924 10.10.0.2:17664 10.13.0.1:99 ip_forward_finish E 30790
196    18:04:29:484146 10.10.0.2:17664 10.13.0.1:99 ip_forward E 30790
      Time : 1025
197    18:04:29:484390   ip_forward B 0
198       18:04:29:484536   np_ip_forward_hook - 0
199       18:04:29:484681   ip_forward_finish B 0
200         18:04:29:484828   ip_send B 37723
201         18:04:29:484977 10.13.0.1:17664 10.10.0.2:60 ip_send E 37723
202       18:04:29:485221 10.13.0.1:17664 10.10.0.2:60 ip_forward_finish E 37723
203    18:04:29:485452 10.13.0.1:17664 10.10.0.2:60 ip_forward E 37723
      Time : 1062
204    18:04:29:485684   ip_forward B 0
205       18:04:29:485835   np_ip_forward_hook - 0
206       18:04:29:485985   ip_forward_finish B 0
207         18:04:29:486137   ip_send B 0
208         18:04:29:486291 10.10.0.2:17664 10.13.0.1:60 ip_send E 0
209       18:04:29:486543 10.10.0.2:17664 10.13.0.1:60 ip_forward_finish E 0
210    18:04:29:486781 10.10.0.2:17664 10.13.0.1:60 ip_forward E 0
      Time : 1097
211    18:04:29:487041   ip_forward B 0
212       18:04:29:487196   np_ip_forward_hook - 0
213       18:04:29:487352   ip_forward_finish B 0
214         18:04:29:487508   ip_send B 37724
215         18:04:29:487667 10.13.0.1:17664 10.10.0.2:52 ip_send E 37724
216       18:04:29:487923 10.13.0.1:17664 10.10.0.2:52 ip_forward_finish E 37724
217    18:04:29:488169 10.13.0.1:17664 10.10.0.2:52 ip_forward E 37724
      Time : 1128
218    18:04:29:488854   ip_forward B 0
219       18:04:29:489014   np_ip_forward_hook - 0
220       18:04:29:489175   ip_forward_finish B 0
221         18:04:29:489337   ip_send B 59902
222         18:04:29:489501 10.13.0.1:17680 10.10.0.2:66 ip_send E 59902
223       18:04:29:489765 10.13.0.1:17680 10.10.0.2:66 ip_forward_finish E 59902
224    18:04:29:490019 10.13.0.1:17680 10.10.0.2:66 ip_forward E 59902
      Time : 1165
225    18:04:29:507417   ip_forward B 0
```

```
226     18:04:29:507589   np_ip_forward_hook - 0
227     18:04:29:507756   ip_forward_finish B 0
228       18:04:29:507923   ip_send B 30791
229       18:04:29:508097 10.10.0.2:17664 10.13.0.1:74 ip_send E 30791
230     18:04:29:508375 10.10.0.2:17664 10.13.0.1:74 ip_forward_finish E 30791
231  18:04:29:508637 10.10.0.2:17664 10.13.0.1:74 ip_forward E 30791
    Time : 1220
232  18:04:29:509804   ip_forward B 0
233     18:04:29:509975   np_ip_forward_hook - 0
234     18:04:29:510146   ip_forward_finish B 0
235       18:04:29:510318   ip_send B 37725
236       18:04:29:510495 10.13.0.1:17672 10.10.0.2:814 ip_send E 37725
237     18:04:29:510803 10.13.0.1:17672 10.10.0.2:814 ip_forward_finish E 37725
238  18:04:29:511073 10.13.0.1:17672 10.10.0.2:814 ip_forward E 37725
    Time : 1269
239  18:04:29:511345   ip_forward B 0
240     18:04:29:511521   np_ip_forward_hook - 0
241     18:04:29:511697   ip_forward_finish B 0
242       18:04:29:511874   ip_send B 37726
243       18:04:29:512053 10.13.0.1:17672 10.10.0.2:52 ip_send E 37726
244     18:04:29:512378 10.13.0.1:17672 10.10.0.2:52 ip_forward_finish E 37726
245  18:04:29:512656 10.13.0.1:17672 10.10.0.2:52 ip_forward E 37726
    Time : 1311
246  18:04:29:512937   ip_forward B 0
247     18:04:29:513118   np_ip_forward_hook - 0
248     18:04:29:513299   ip_forward_finish B 0
249       18:04:29:513482   ip_send B 42130
250       18:04:29:513666 10.10.0.2:17672 10.13.0.1:52 ip_send E 42130
251     18:04:29:513967 10.10.0.2:17672 10.13.0.1:52 ip_forward_finish E 42130
252  18:04:29:514252 10.10.0.2:17672 10.13.0.1:52 ip_forward E 42130
    Time : 1315
253  18:04:29:514540   ip_forward B 0
254     18:04:29:514726   np_ip_forward_hook - 0
255     18:04:29:514912   ip_forward_finish B 0
256       18:04:29:515099   ip_send B 30792
257       18:04:29:515305 10.10.0.2:17664 10.13.0.1:74 ip_send E 30792
258     18:04:29:515613 10.10.0.2:17664 10.13.0.1:74 ip_forward_finish E 30792
```

```
259  18:04:29:515906 10.10.0.2:17664 10.13.0.1:74 ip_forward E 30792
    Time : 1366
260  18:04:29:516201   ip_forward B 0
261     18:04:29:516392   np_ip_forward_hook - 0
262     18:04:29:516584   ip_forward_finish B 0
263        18:04:29:516776   ip_send B 42131
264        18:04:29:516971 10.10.0.2:17672 10.13.0.1:52 ip_send E 42131
265     18:04:29:517287 10.10.0.2:17672 10.13.0.1:52 ip_forward_finish E 42131
266  18:04:29:517588 10.10.0.2:17672 10.13.0.1:52 ip_forward E 42131
    Time : 1387
267  18:04:29:517911   ip_forward B 0
268     18:04:29:518107   np_ip_forward_hook - 0
269     18:04:29:518304   ip_forward_finish B 0
270        18:04:29:518501   ip_send B 37727
271        18:04:29:518701 10.13.0.1:17672 10.10.0.2:52 ip_send E 37727
272     18:04:29:519021 10.13.0.1:17672 10.10.0.2:52 ip_forward_finish E 37727
273  18:04:29:519330 10.13.0.1:17672 10.10.0.2:52 ip_forward E 37727
    Time : 1419
274  18:04:29:548837   ip_forward B 0
275     18:04:29:549042   np_ip_forward_hook - 0
276     18:04:29:549245   ip_forward_finish B 0
277        18:04:29:549447   ip_send B 59903
278        18:04:29:549656 10.13.0.1:17680 10.10.0.2:52 ip_send E 59903
279     18:04:29:549985 10.13.0.1:17680 10.10.0.2:52 ip_forward_finish E 59903
280  18:04:29:550302 10.13.0.1:17680 10.10.0.2:52 ip_forward E 59903
    Time : 1465
281  18:04:31:321135   ip_forward B 0
282     18:04:31:321349   np_ip_forward_hook - 0
283     18:04:31:321557   ip_forward_finish B 0
284        18:04:31:321765   ip_send B 59904
285        18:04:31:321982 10.13.0.1:17680 10.10.0.2:58 ip_send E 59904
286     18:04:31:322336 10.13.0.1:17680 10.10.0.2:58 ip_forward_finish E 59904
287  18:04:31:322691 10.13.0.1:17680 10.10.0.2:58 ip_forward E 59904
    Time : 1556
288  18:04:31:323019   ip_forward B 0
289     18:04:31:323230   np_ip_forward_hook - 0
290     18:04:31:323442   ip_forward_finish B 0
```

```
291         18:04:31:323655   ip_send B 30793
292         18:04:31:323872 10.10.0.2:17664 10.13.0.1:66 ip_send E 30793
293      18:04:31:324219 10.10.0.2:17664 10.13.0.1:66 ip_forward_finish E 30793
294   18:04:31:324575 10.10.0.2:17664 10.13.0.1:66 ip_forward E 30793
     Time : 1556
295   18:04:31:324910   ip_forward B 0
296      18:04:31:325126   np_ip_forward_hook - 0
297      18:04:31:325343   ip_forward_finish B 0
298         18:04:31:325561   ip_send B 30794
299         18:04:31:325781 10.10.0.2:17664 10.13.0.1:52 ip_send E 30794
300      18:04:31:326137 10.10.0.2:17664 10.13.0.1:52 ip_forward_finish E 30794
301   18:04:31:326497 10.10.0.2:17664 10.13.0.1:52 ip_forward E 30794
     Time : 1587
302   18:04:31:326839   ip_forward B 0
303      18:04:31:327061   np_ip_forward_hook - 0
304      18:04:31:327283   ip_forward_finish B 0
305         18:04:31:327506   ip_send B 59905
306         18:04:31:327731 10.13.0.1:17680 10.10.0.2:52 ip_send E 59905
307      18:04:31:328090 10.13.0.1:17680 10.10.0.2:52 ip_forward_finish E 59905
308   18:04:31:328439 10.13.0.1:17680 10.10.0.2:52 ip_forward E 59905
     Time : 1600
309   18:04:31:328790   ip_forward B 0
310      18:04:31:329016   np_ip_forward_hook - 0
311      18:04:31:329244   ip_forward_finish B 0
312         18:04:31:329472   ip_send B 59906
313         18:04:31:329702 10.13.0.1:17680 10.10.0.2:52 ip_send E 59906
314      18:04:31:330073 10.13.0.1:17680 10.10.0.2:52 ip_forward_finish E 59906
315   18:04:31:330429 10.13.0.1:17680 10.10.0.2:52 ip_forward E 59906
     Time : 1639
316   18:04:31:330788   ip_forward B 0
317      18:04:31:331020   np_ip_forward_hook - 0
318      18:04:31:331252   ip_forward_finish B 0
319         18:04:31:331485   ip_send B 59907
320         18:04:31:331720 10.13.0.1:17680 10.10.0.2:52 ip_send E 59907
321      18:04:31:332096 10.13.0.1:17680 10.10.0.2:52 ip_forward_finish E 59907
322   18:04:31:332474 10.13.0.1:17680 10.10.0.2:52 ip_forward E 59907
     Time : 1686
```

```
323   18:04:31:332853   ip_forward B 0
324      18:04:31:333090   np_ip_forward_hook - 0
325      18:04:31:333327   ip_forward_finish B 0
326         18:04:31:333566   ip_send B 30795
327         18:04:31:333806 10.10.0.2:17664 10.13.0.1:52 ip_send E 30795
328      18:04:31:334193 10.10.0.2:17664 10.13.0.1:52 ip_forward_finish E 30795
329   18:04:31:334566 10.10.0.2:17664 10.13.0.1:52 ip_forward E 30795
      Time : 1713
```

12.23.8 LOG_UDP

```
1    21:52:04:593763 0.0.0.0:0 0.0.0.0:0 udp_v4_get_port B
2    21:52:04:593773 0.0.0.0:0 0.0.0.0:0 udp_v4_get_port E
     Time : 10
3    21:52:04:593782 0.0.0.0:32771 192.168.1.104:30091 udp_sendmsg B
4       21:52:04:593795 0.0.0.0:0 0.0.0.0:0 udp_getfrag B
5       21:52:04:593795 0.0.0.0:0 0.0.0.0:0 udp_getfrag E
6    21:52:04:593828 0.0.0.0:32771 192.168.1.104:30091 udp_sendmsg E
     Time : 46
7    21:52:04:593895 0.0.0.0:0 0.0.0.0:32771 udp_recvmsg B
8       21:52:04:596889 192.168.1.104:30091 192.168.1.20:32771 udp_rcv B
9          21:52:04:596909 0.0.0.0:0 0.0.0.0:32771 udp_queue_rcv_skb B
10            21:52:04:596928 192.168.1.104:30091 192.168.1.20:32771 udp_queue_rcv_skb B
11            21:52:04:596951 0.0.0.0:0 0.0.0.0:32771 udp_queue_rcv_skb E
12         21:52:04:596973 192.168.1.104:30091 192.168.1.20:32771 udp_queue_rcv_skb E
13      21:52:04:596998 192.168.1.104:30091 192.168.1.20:32771 udp_rcv E
14   21:52:04:597149 0.0.0.0:0 0.0.0.0:32771 udp_recvmsg E
     Time : 3254
15   21:52:06:236993 0.0.0.0:32771 192.168.1.104:30091 udp_sendmsg B
16      21:52:06:237030 0.0.0.0:0 0.0.0.0:0 udp_getfrag B
17      21:52:06:237030 0.0.0.0:0 0.0.0.0:0 udp_getfrag E
18   21:52:06:237084 0.0.0.0:32771 192.168.1.104:30091 udp_sendmsg E
     Time : 91
19   21:52:06:237153 0.0.0.0:0 0.0.0.0:32771 udp_recvmsg B
20      21:52:06:237326 192.168.1.104:30091 192.168.1.20:32771 udp_rcv B
21         21:52:06:237367 0.0.0.0:0 0.0.0.0:32771 udp_queue_rcv_skb B
22            21:52:06:237405 192.168.1.104:30091 192.168.1.20:32771 udp_queue_rcv_skb B
23            21:52:06:237448 0.0.0.0:0 0.0.0.0:32771 udp_queue_rcv_skb E
24         21:52:06:237490 192.168.1.104:30091 192.168.1.20:32771 udp_queue_rcv_skb E
25      21:52:06:237535 192.168.1.104:30091 192.168.1.20:32771 udp_rcv E
26   21:52:06:237704 0.0.0.0:0 0.0.0.0:32771 udp_recvmsg E
     Time : 551
27   21:52:07:947696 0.0.0.0:32771 0.0.0.0:0 udp_close B
28      21:52:07:947751 0.0.0.0:32771 0.0.0.0:0 udp_v4_unhash B
29      21:52:07:947802 0.0.0.0:32771 0.0.0.0:0 udp_v4_unhash E
30   21:52:07:947857 0.0.0.0:32771 0.0.0.0:0 udp_close E
```

Time : 161

12.23.9 DUMP_UDP

1 21:52:04.593820 gyan.home.32771 > 192.168.1.104.30091: udp 6 (DF)
2 21:52:04.596880 192.168.1.104.30091 > gyan.home.32771: udp 6 (DF)
3 21:52:06.237077 gyan.home.32771 > 192.168.1.104.30091: udp 3 (DF)
4 21:52:06.237318 192.168.1.104.30091 > gyan.home.32771: udp 3 (DF)
5 21:52:09.584671 arp who-has 192.168.1.104 tell gyan.home
6 21:52:09.584814 arp reply 192.168.1.104 is-at 0:f:1f:1b:9b:b4