Project: DMZS-Biatchux(F.I.R.E.)
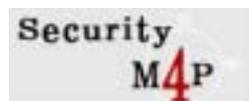
Bootable CD fire-0.4a

2003. 5. 20

jjshim AT Hanaro.com

Biatchux(F.I.R.E.)

.

,   . Biatchux

            .   ,   ,

CD- ROM   .   OS

            ,   ,   .   OS

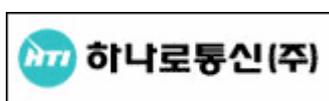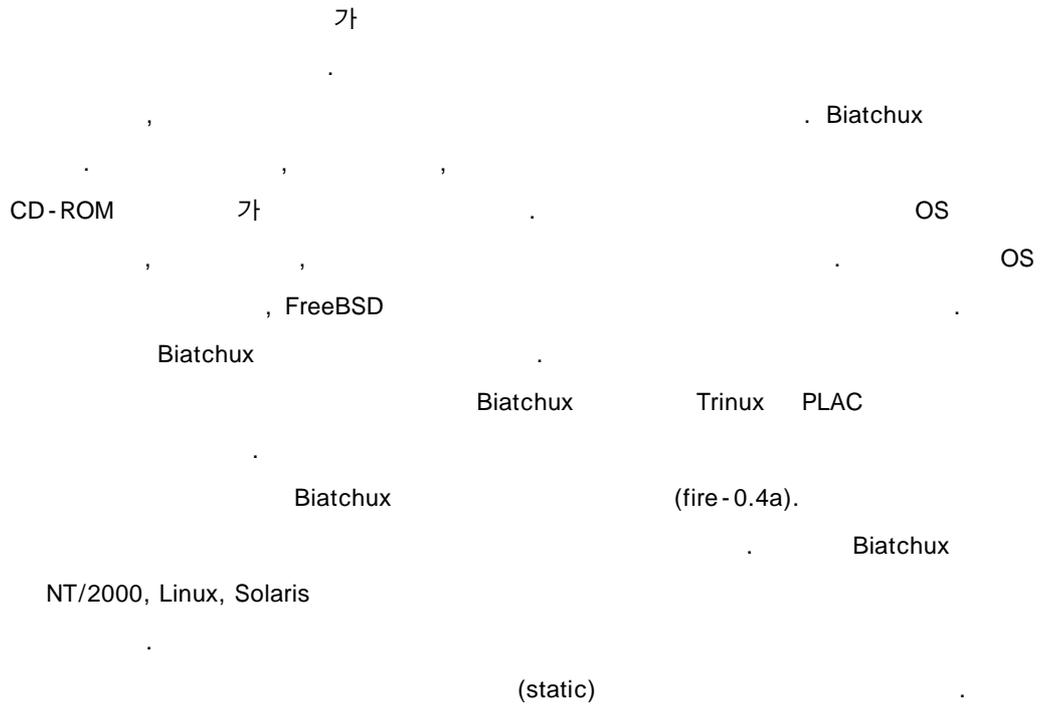   , FreeBSD   .

            Biatchux   .

                                                Biatchux   Trinux   PLAC

            .

                        Biatchux   (fire- 0.4a).

                                                                          .   Biatchux

        NT/2000, Linux, Solaris

            .

                                                (static)   .

Biatchux:

Biatchux　　　　　　　　　　　　.　　　　　　　　　　　　　　　　　　　Biatchux
　　　CD-ROM　　　　　　　　　　　　　　　　　　　.
　　　　　　　　　.

Biatchux

Biatchux　　　　　　　　CD-ROM　　　　　　　　　　　　.　　　　(Salusky　Zendzian)
　　　　　　　,　　　　,　　　　,　　　　　,
　　.　　　　　fire-0.4a　　,　　578MB　　　　　ISO　　　　　　　.　　ISO
　　　　　　　　CD　　　　　　(loopback)
　　　　　:

```
# mkdir FIRE_image
# mkdir /mnt/image
# cd FIRE_image
# wget http://aleron.dl.sourceforge.net/sourceforge/biatchux/fire-0.4a.iso
# mount –o ro,loop fire-0.4a.iso /mnt/image
```

```
[root@F_I_R_E root]# cd /opt/
[root@F_I_R_E opt]# mkdir FIRE_image
[root@F_I_R_E opt]# cd FIRE_image/
[root@F_I_R_E FIRE_image]# wget http://aleron.dl.sourceforge.net/sourceforge/bia
tchux/fire-0.4a.iso
--14:16:00--  http://aleron.dl.sourceforge.net/sourceforge/biatchux/fire-0.4a.is
o
           => `fire-0.4a.iso'
Resolving aleron.dl.sourceforge.net... done.
Connecting to aleron.dl.sourceforge.net[204.157.3.229]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 606,765,056 [text/plain]

 2% [                                    ] 13,213,320   217.20K/s    ETA 44:28
```

　　　　　　　　　　.

```
[root@F_I_R_E FIRE_image]# mount -o ro,loop fire-0.4a.iso /mnt/image/
[root@F_I_R_E FIRE_image]# ls -l /mnt/image/
total 17
-r-xr-xr-x    1 root      root          53 Nov 20  2002 autorun.inf
dr-xr-xr-x    3 root      root        2048 May  6 07:14 docs
-r--r--r--    1 root      root           5 May 15 02:16 FIRE-v0.4a.ver
dr-xr-xr-x    2 root      root        2048 May 14 14:22 fs
dr-xr-xr-x    2 root      root        2048 May 14 14:21 pkgs
dr-xr-xr-x    6 root      root        2048 Feb 16 13:35 statbins
dr-xr-xr-x   22 root      root        8192 May 11 11:16 win32
[root@F_I_R_E FIRE_image]#
```

. statbins   2.4.20 x86   2.7

static   (www.incident-response.org   )   NT/2000

(Cygwin   )   .   , win32   NT/2000

. Biatchux 0.4a   Red Hat   7.3   gcc 2.96, kernel version 2.4.20   .

Biatchux

CD-R   CD-ROM   Biatchux CD   .

BIOS   CD-ROM   .

CD-ROM   5   :

1. Fire

2. Fire-serial

3. Fire-X(800   600)

4. Fire-X(1024   768)

5. Memtest

Biatchux-serial   ,   . Memtest   x86 PC

.

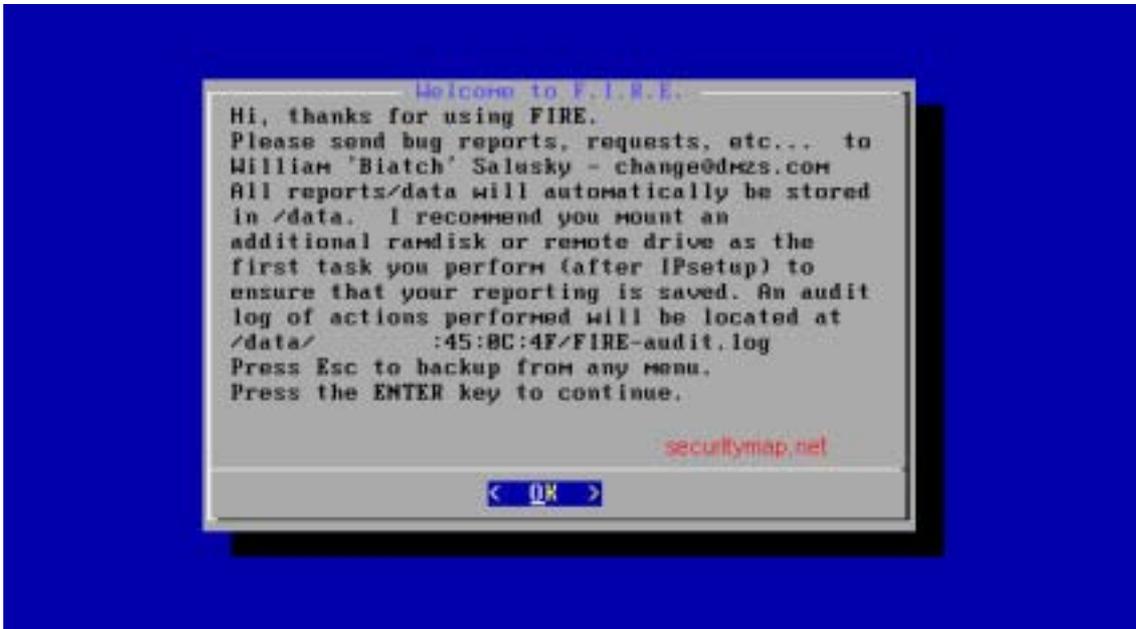Biatchux   /lib   /usr   CD-ROM   cramfs

, CD-ROM   ramdisk   .   CD-

ROM   .tgz   RAM   , CD-ROM

.

"Welcom to F.I.R.E."   (1). Biatchux

.

1. F.I.R.E.

1   Enter   4   .

Start-Here   Basic Config, Networking – etc...

Forensics   Forensics

Virus-Scan   Virus scanning for partition contents

PenTesting   Penetration Assessment tools

2. Biatchux

Start-Here   ,   (3).

IP   , DHCP   IP   .

VNC   .   CD-ROM   IP   VNC

.

3. Start-Here

MountDataDrv   (4)   .   ramdisk

NFS   SMB

.   USB-Drive   Firewire-Drv   USB   USB

.

.

(   )

netcat   ncftp   scp   ramdisk
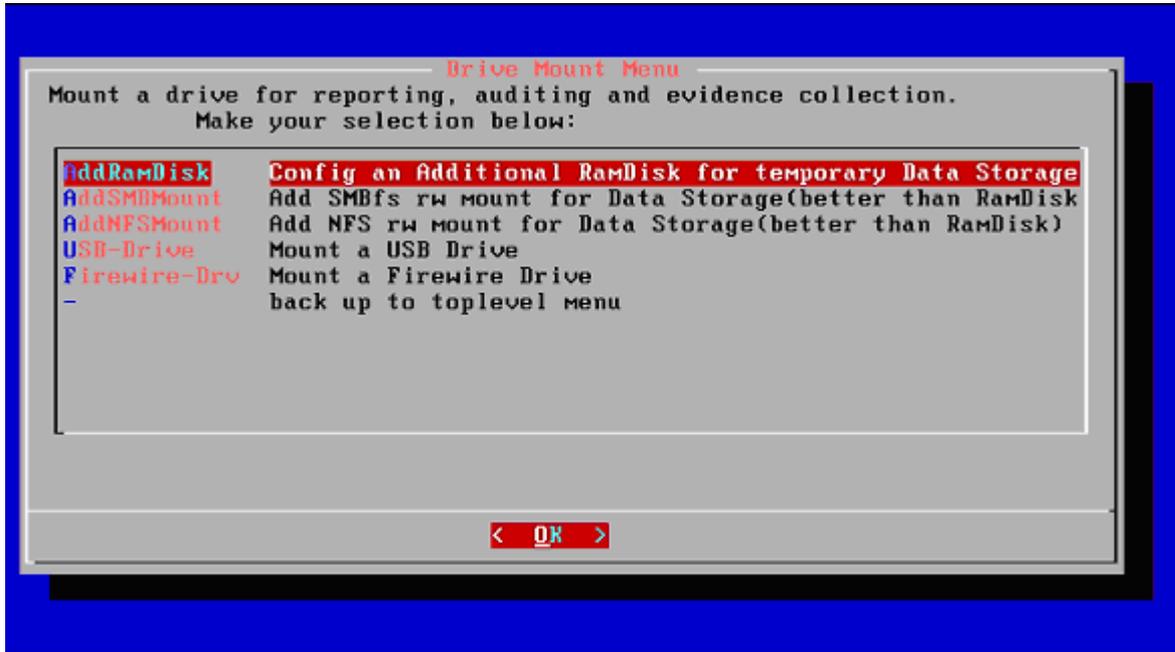
. Biatchux 0.4a   tfp   Apache

. netcat   /data   ,

(ex IP: 192.168.10.100)   :

$ nc –l   -p   3147 > forensic_data.tar

Biatchux   data   :

cd /data

tar cf - . | nc   -nv   192.168.10.100 3147

/data   RAM
.

4. Drive Mount

Start- Here   .
.

/data   ALT
(F1~F7)   (ALT+F1)   .

Biatchux

mac- robber
/data   Biatchux   .   Win32
.
, autopsy   .
.

Virus- Scan   F- Port
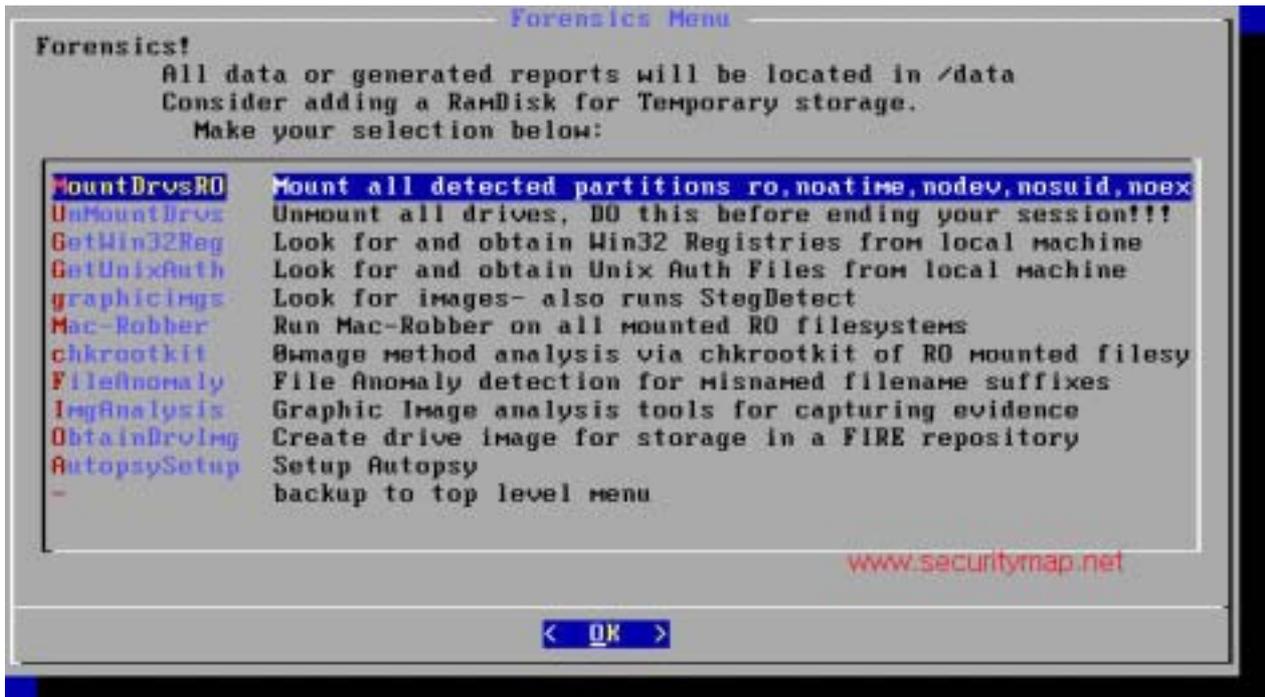. F- Port   DOS, Windows, Linux   . Biatchux
signature   .
Biatchux   CD- R   cramfs
signature
.   signature
.

5. Forensics

6. Virus Scanning

Biatchux   .
                                    .

                                    .

. Biatchux   static   CD-ROM
.   Biatchux   .

lsof, netstat, ls   mac-robber(   )
. Biatchux   .   LKM
'   '   '   '
'   '   '   '   .
md5
netcat   dd   . md5   .
md5   Fingerprint   . Biatchux
incident-response.org   , lsof, netcat   .
.

NT/2000   .
.   OS
Cygwin   Biatchux   CD-ROM
.   CD-ROM   Biatchux CD-ROM   biatchux.exe
.   5   CD-ROM   biatchux.exe
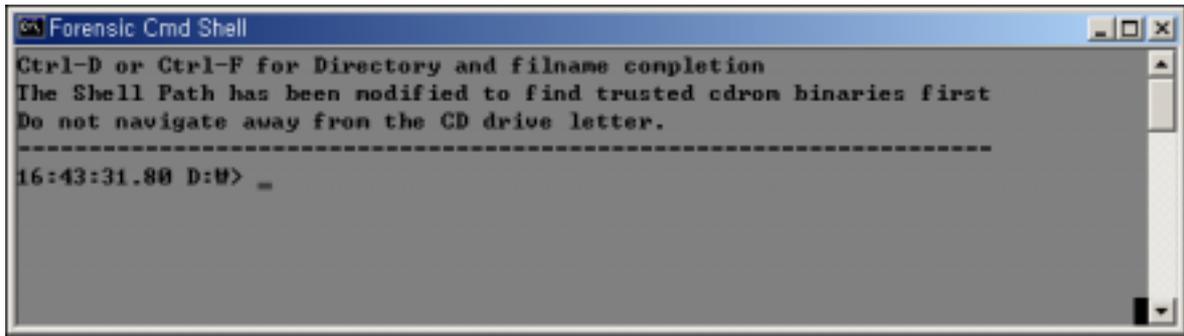.   cmdenv.bat   .
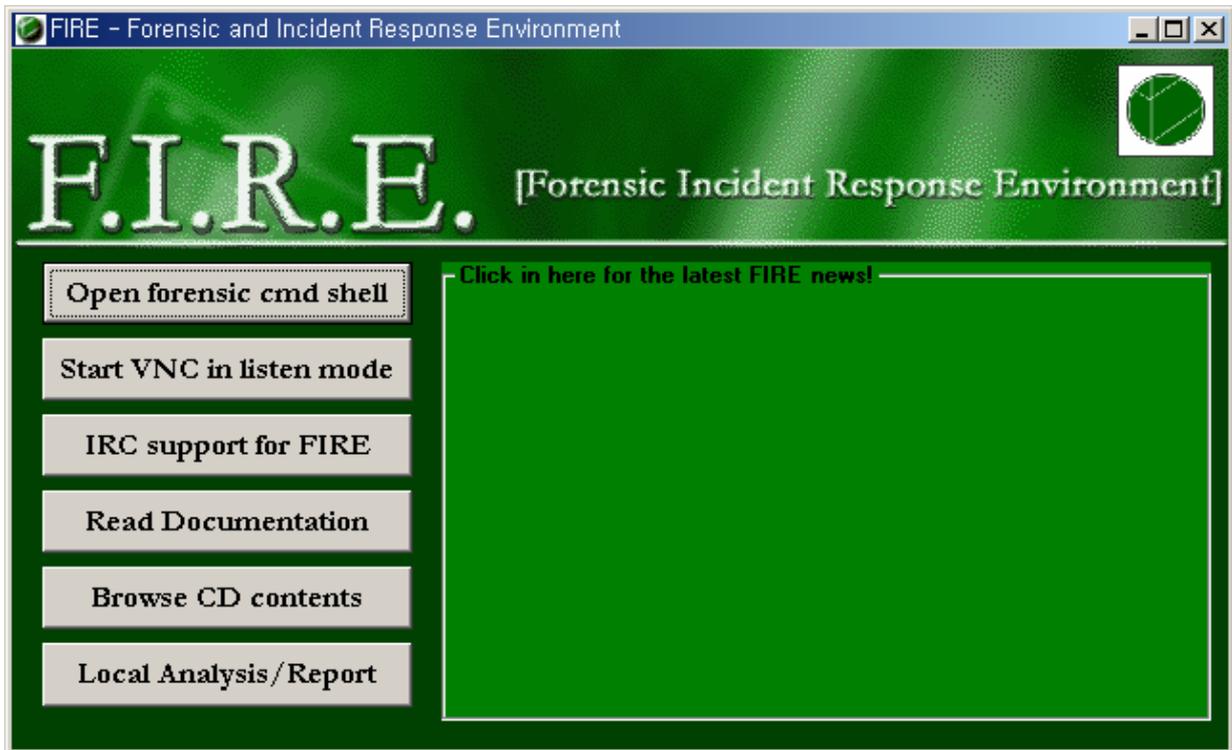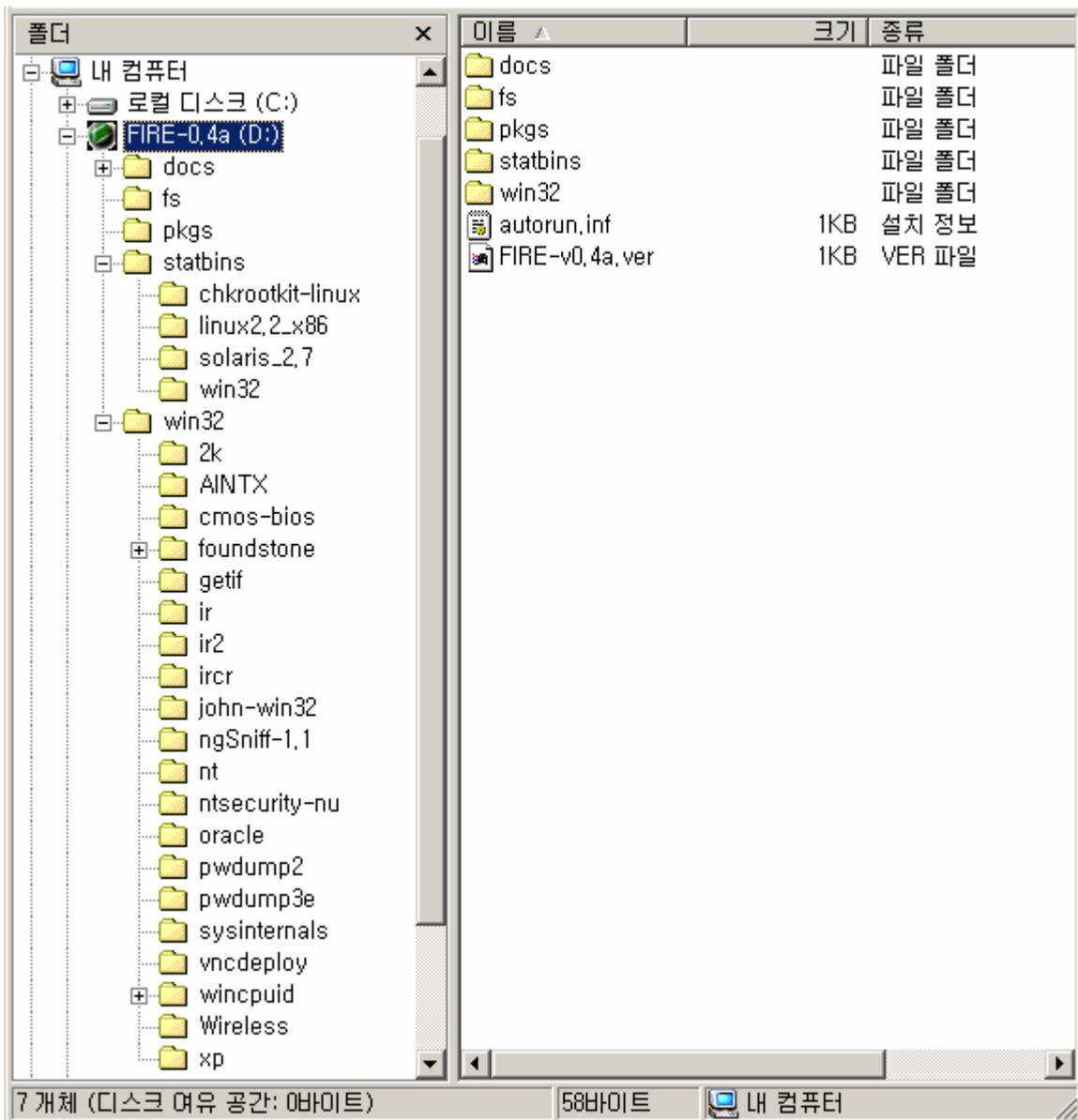

7. F.I.R.E. CD-ROM

(cmdenv.bat)   .   CD-ROM   cmd.exe
PATH   CD-ROM   .   8   .

```
Forensic Cmd Shell                                          _ □ ×
Ctrl-D or Ctrl-F for Directory and filname completion
The Shell Path has been modified to find trusted cdrom binaries first
Do not navigate away from the CD drive letter.
--------------------------------------------------------------
16:43:31.80 D:\> _
```

8. Forensics cmd shell

dmzs.com   IRC   IRC   .
                                    VNC   .
Biatchux   .   9
Biatchux CD- ROM   .

9. F.I.R.E.   CD- ROM

Cygwin   (Win32   ):

ansi2knr.exe	basename.exe	bison.exe	bzip2.exe	bunzip2.exe
bzip2recover.exe	cat.exe	chgrp.exe	chmod.exe	chown.exe
cksum.exe	cmp.exe	comm.exe	compress.exe	cp.exe
csplit.exe	cut.exe	date.exe	dd.exe	df.exe
diff.exe	diff3.exe	dirname.exe	du.exe	echo.exe
egrep.exe	env.exe	expand.exe	expr.exe	factor.exe
fgrep.exe	find.exe	flex.exe	fmt.exe	fold.exe
gawk.exe	make.exe	grep.exe	gsar.exe	gunzip.exe
gzip.exe	head.exe	id.exe	install.exe	join.exe
less.exe	ln.exe	logname.exe	ls.exe	m4.exe
md5sum.exe	mkdir.exe	mkfifo.exe	mknod.exe	mv.exe
mvdir.exe	nl.exe	od.exe	paste.exe	patch.exe
pathchk.exe	pr.exe	printenv.exe	printf.exe	ptx.exe
recode.exe	rm.exe	rman.exe	rmdir.exe	sdiff.exe
sed.exe	seq.exe	sleep.exe	sort.exe	sh.exe
shar.exe	split.exe	stego.exe	su.exe	sum.exe
sync.exe	tac.exe	tail.exe	tar.exe	tee.exe
test.exe	touch.exe	tr.exe	uname.exe	unexpand.exe
uniq.exe	unshar.exe	uudecode.exe	uuencode.exe	wc.exe
wget.exe	which.exe	whoami.exe	xargs.exe	yes.exe
zcat.exe				

Linux static   (Kernel 2.2 X86)

chgrp	chmod	chown	chroot	cksum
cp	cryptcat	cut	date	dd
df	du	echo	env	file
fold	head	hostname	icat	id
ifconfig	ils	ln	ls	lsof
mac- robber	md5	md5sum	mv	nc
netstat	od	pcat	printenv	pwd
rarp	read_data	rm	rmdir	route
search_data	sort	sync	tac	tail
touch	uniq	unrm	uptime	wc
who	whoami	arp	cat	

Solaris static   (solaris_2.7)

chmod	chown	chroot	cksum	cp
cut	date	dd	df	dirname
du	echo	env	factor	file
gunzip	gzip	head	hostid	hostname
icat	id	ils	join	lastcomm
ln	logname	ls	lsof	md5
md5sum	mkdir	mknod	mv	nc
od	pcat	printenv	pwd	rm
rmdir	rmt	sort	split	su
sum	sync	tail	tar	touch
uname	uniq	unrm	uptime	users
wc	who	whoami	cat	chgrp
zcat				

Win32

ntsecurity- nu	listmodules.exe	Use: . Syntax: listmodules PID Examples: listmodules 660
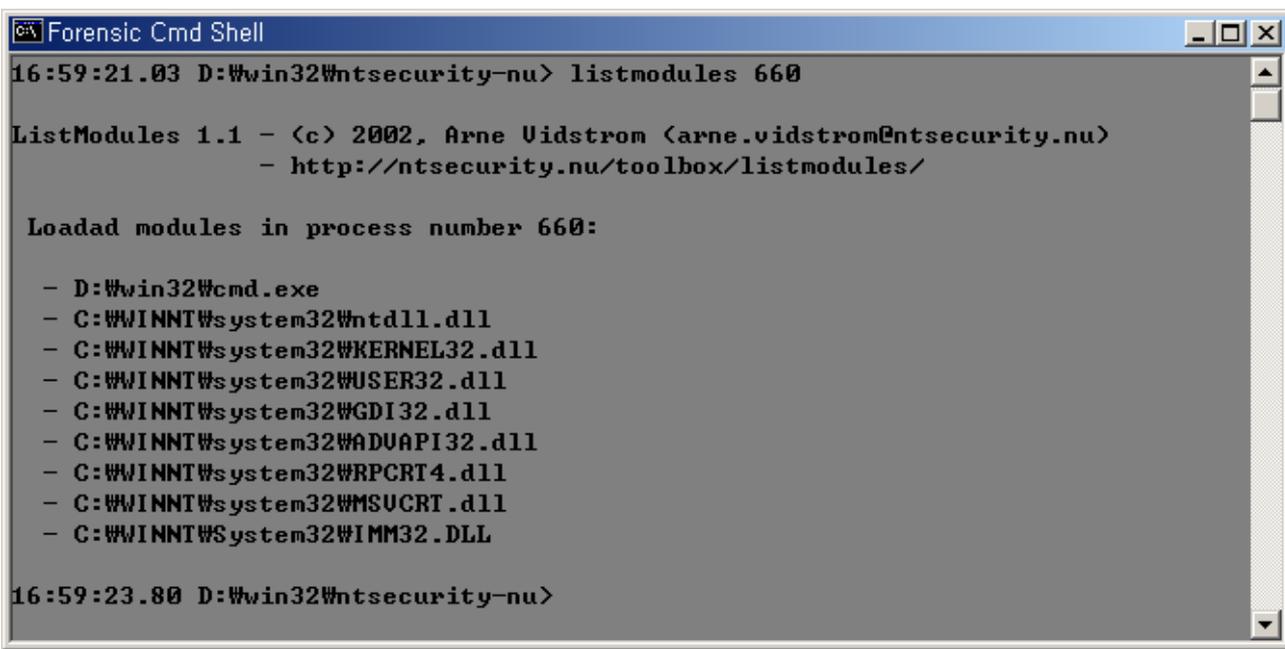
```
Forensic Cmd Shell                                    _ □ ×
16:59:21.03 D:\win32\ntsecurity-nu> listmodules 660

ListModules 1.1 - (c) 2002, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
             - http://ntsecurity.nu/toolbox/listmodules/

 Loadad modules in process number 660:

  - D:\win32\cmd.exe
  - C:\WINNT\system32\ntdll.dll
  - C:\WINNT\system32\KERNEL32.dll
  - C:\WINNT\system32\USER32.dll
  - C:\WINNT\system32\GDI32.dll
  - C:\WINNT\system32\ADVAPI32.dll
  - C:\WINNT\system32\RPCRT4.dll
  - C:\WINNT\system32\MSVCRT.dll
  - C:\WINNT\System32\IMM32.DLL

16:59:23.80 D:\win32\ntsecurity-nu>
```

ntsecurity- nu	dumpusers.exe	Use: . Syntax: DumpUsers - target <computername / IP> - type <notdc/dc> - start <start RID> - stop <stop RID> - mode <verbose/quiet>

ntsecurity- nu	browselist.exe	Use: Subnet .
		Syntax: browselist [Enter]
		Examples: > browselist [Enter]
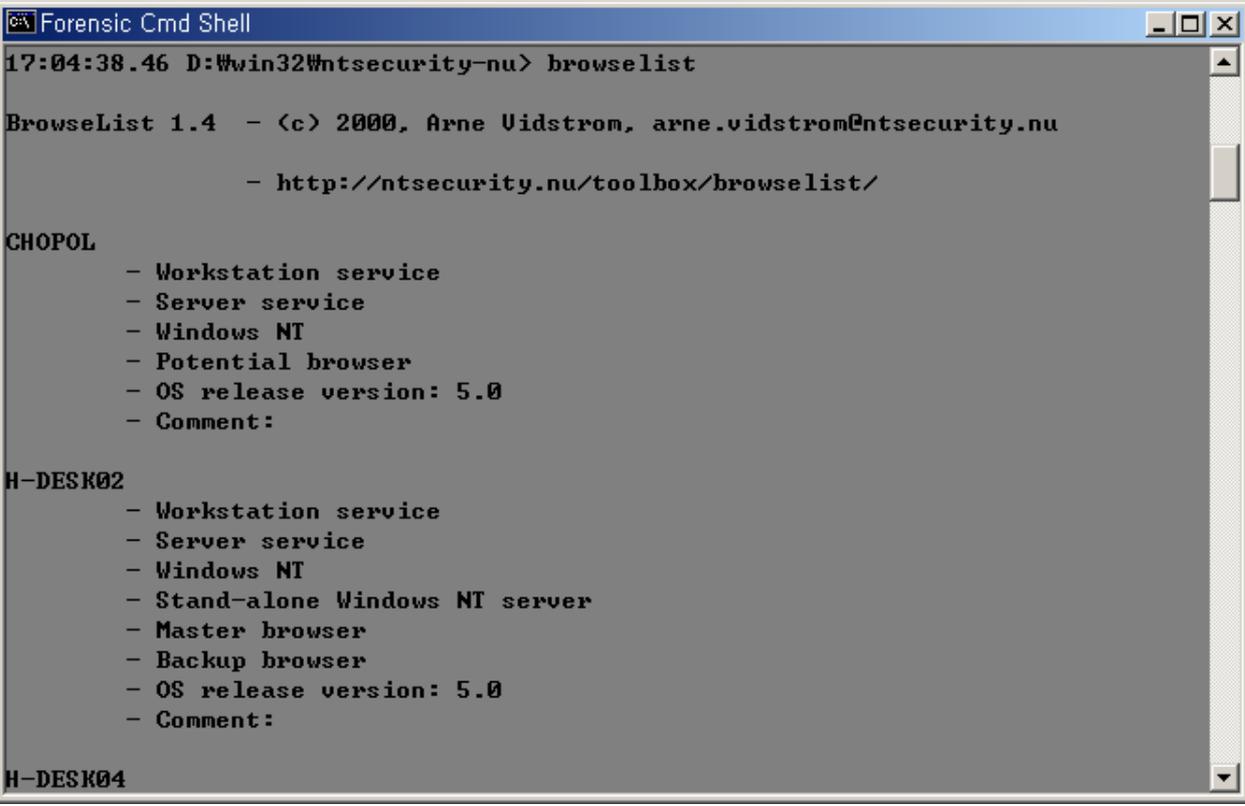
```
Forensic Cmd Shell                                              _ □ ×
17:04:38.46 D:\win32\ntsecurity-nu> browselist

BrowseList 1.4  - (c) 2000, Arne Vidstrom, arne.vidstrom@ntsecurity.nu

              - http://ntsecurity.nu/toolbox/browselist/

CHOPOL
        - Workstation service
        - Server service
        - Windows NT
        - Potential browser
        - OS release version: 5.0
        - Comment:

H-DESK02
        - Workstation service
        - Server service
        - Windows NT
        - Stand-alone Windows NT server
        - Master browser
        - Backup browser
        - OS release version: 5.0
        - Comment:

H-DESK04
```

ntsecurity- nu	winfo.exe	Use: null session .
		(, ,)
		Syntax: winfo IP –n
		Example: > winfo 192.168.10.100 - n
ntsecurity- nu	gsd.exe	Use: GSD(Get Service Dacl)
		. .
		Syntax: gsd <service name>
		Examples: > gsd server
ntsecurity- nu	macmatch.exe	Use: , , .
		Syntax: macmatch <drive/directory> <type> <start date/time> <stop date/time>
		Examples: macmatch c:\ temp - m 2003- 04- 10:12.01 2003- 05- 10:12.01
ntsecurity- nu	pmdump.exe	Use:
		.
		Syntax: pmdump <pid> <filename>
		Examples: > pmdump 600 c:\ forensics_data\ pmdump_600.dmp
ntsecurity- nu	periscope.exe	Use: PE .
		, .
		Syntax: PEriscope <filename> [- q]
		Examples: > PEriscope Cracking_tools.exe - q

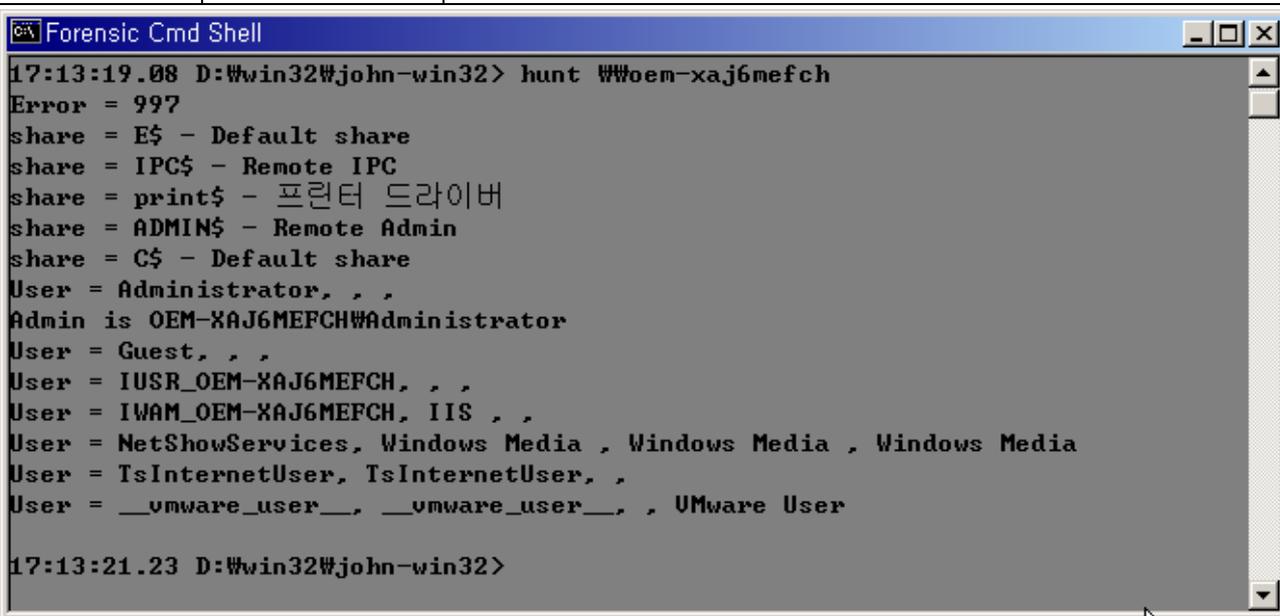| ntsecurity- nu | promiscdetect.exe | Use: NIC   promiscuous   . |
		Note: .
		Syntax: promiscdetect
		Example: > promiscdetect
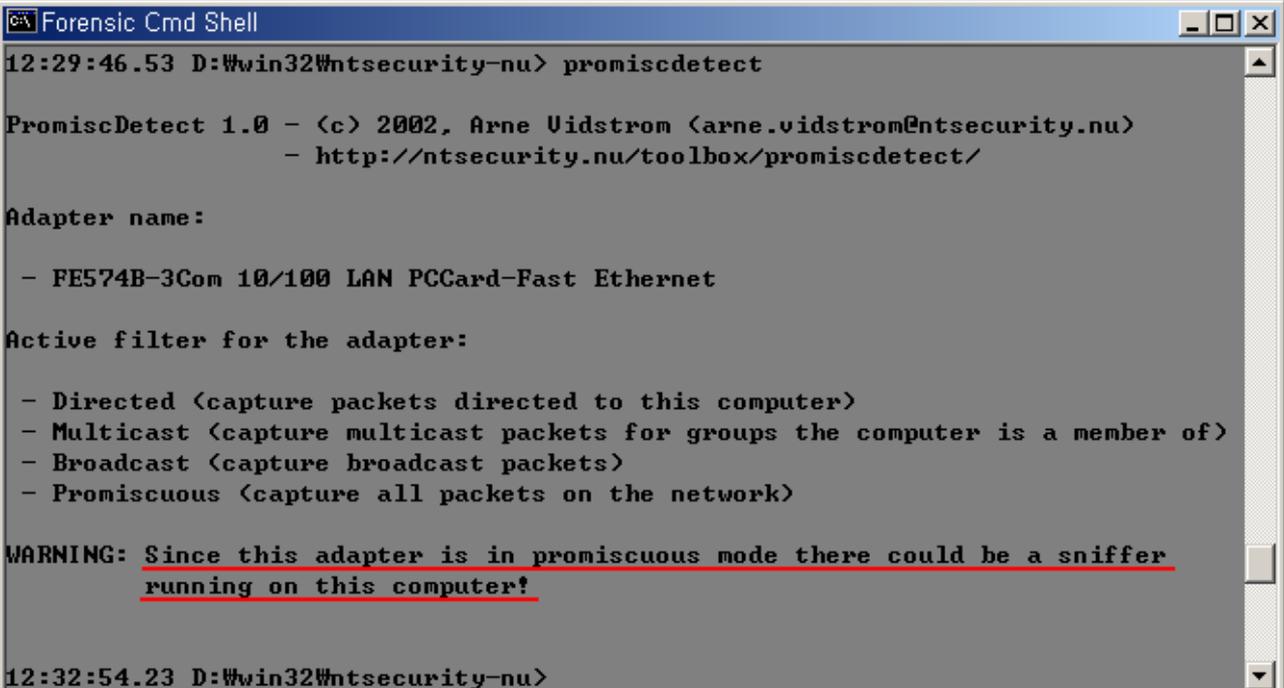

```
Forensic Cmd Shell                                    _ □ ×

12:29:46.53 D:\win32\ntsecurity-nu> promiscdetect

PromiscDetect 1.0 - (c) 2002, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
            - http://ntsecurity.nu/toolbox/promiscdetect/

Adapter name:

 - FE574B-3Com 10/100 LAN PCCard-Fast Ethernet

Active filter for the adapter:

 - Directed (capture packets directed to this computer)
 - Multicast (capture multicast packets for groups the computer is a member of)
 - Broadcast (capture broadcast packets)
 - Promiscuous (capture all packets on the network)

WARNING: Since this adapter is in promiscuous mode there could be a sniffer
         running on this computer!

12:32:54.23 D:\win32\ntsecurity-nu>
```

AINTX	abort.exe	Use: shutdown .
		Note: shutdown
		.
		Syntax: abort [- h hostname]
		Examples: 1)
		> abort
		2)
		> abort –h \ \ myserver
AINTX	addprpmem	Use: .
		Syntax: addgrpmem [- h hostname] - g group { - u user | - w glbl_grp}
		Examples: administrators jjshim
		➤ addgrpmem –g administrators –u jjshim
		➤ addprpmem –g users –w "domain users"
AINTX	bootmv.exe	Use: .
		Syntax: bootmv - s source_file [- d dest_file]
		Note:
		. ,
		.
		Examples: 1)
		➤ bootmv - s c:\ temp\ myfile - d c:\ temp\ rename_file

		2) > bootmv - s c:\ winnt\ system32\ cracking.dll
AINTX	buevt.exe	Use: . Syntax: buevt [- h hostname] - e event_log - f file_name Examples: > buevt - e Application - f evt_log_bu.evt

AINTX	chsvc.exe	Use: NT4/2000 .
		
		Syntax: chsvc [- h hostname] - s service_name options
		
		Examples: 1) wins " "
		
		        ➤ chsvc –s wins –d
		
		        2) wins " "
		
		        > chsvc –s wins - m

AINTX	clevt.exe	Use: .
		
		Syntax: clevt [- h hostname] - e event_log [- f backup_file]
		
		Note: .
		
		Examples: 1)
		
		        ➤ clevt - e Application
		
		        2)
		
		        > clevt - e Application - f App_evtlog.evt

AINTX	cpuser.exe	Use: . Syntax: cpuser [- h hostname] - u username options Examples: administrator > cpuser –u administrator –n jjshim –f "shim joung jae"
AINTX	df.exe	Use: . Syntax: df [drive1 drive2 ...] Examples: df c: d:
AINTX	du.exe	Use: (KB) . Syntax: du [- b - d - o - s - t] file1 ... Examples: du –t –s c:\ temp
AINTX	getprocinfo	Use: . Syntax: getprocinfo [- v] PID Examples: getprocinfo - v 600

AINTX	lsexe.exe	Use: .
		
		Syntax: lsexe [- s - v] - f file
		
		Examples: 1) cracking.dll
		
		        ➤ lsexe –f cracking.dll
		
		        ➤ lsexe –f winword.exe | find "Image Version"

AINTX	lssess.exe	Use: . Syntax: lssess [- h hostname] [- f] [- c client | - u userid] Examples: lssess - c hacker_pc

AINTX	lsshare.exe	Use: .
		Syntax: lsshare [- h hostname] [- acdfp] [- s sharename]
		Examples: 1)
		           ➢ lsshare or lsshare –a
		           2)
		           > lsshare - c

AINTX	lssvc.exe	Use: . Syntax: lssvc [- h hostname] [- adnsy | - s service_name] Examples: lssvc - yv
AINTX	lstcp.exe	Use: TCP/IP . Syntax: lstcp [- h hostname] Examples: lstcp
AINTX	lsuser.exe	Use: (, ,) . Syntax: lsuser [- h hostname] { - u userid | - acnt} Examples: lsuser - a
AINTX	memcheck.exe	Use: . Syntax: memcheck Examples: memcheck
AINTX	mksvc.exe	Use: . Syntax: mksvc [- h hostname] - s service_name options… Examples: remotecmd > mksvc - s Remotemcd - p c:\ hacking\ rcmdsvc.exe - e "Remote Command Service"
AINTX	nbtlookup.exe	Use: Netbios IP . Syntax: nbtlookup computer_name Examples: nbtlookup Hacker_PC
AINTX	portprobe.exe	Use: TCP/UDP OPEN . Syntax: portprobe host [- a] begin_port [end_port] Examples: portprobe 192.168.10.100 25- 40
AINTX	ps.exe	Use: . Syntax: ps [- h hostname] [- ft] [- p procid] Examples: ps –h \ \ Hacking_server or ps –p 23
AINTX	rmshare.exe	Use: . Syntax: rmshare [- h hostname] - s sharename Examples: rmshare –s foo_drive
AINTX	rmsvc.exe	Use: Syntax: rmsvc [- h hostname] - s service_name Examples: rmsvc –s Remotecmd

| AINTX	rmuser.exe	Use: Syntax: rmuser [- h hostname] - u username Examples: rmuser –h \ \ seriousPC –u cracker
AINTX	shutdown.exe	Use: shutdown Syntax: shutdown [- h hostname] [- fr - m message - w wait] Examples: shutdown - h \ \ myserver - w 60 –m "goodbye"
AINTX	startsvc.exe	Use: Syntax: startsvc [- h hostname] - s service Examples: startsvc –s "IIS Admin Service"
AINTX	stopsvc.exe	Use: Syntax: stopsvc [- h hostname] - s service [- p] Examples: stopsvc –s "IIS Admin Service"
AINTX	strings.exe	Use: Syntax: strings [- n min_str_len] [- ao] - f file Examples: strings –f hacking.obj
Foundstone	Attacker.exe	TCP/UDP . IP .
Foundstone	Bintext.exe	(Ascii) .
Foundstone	boping.exe	Back Oriffice Pinger . .
Foundstone	ddosping.exe	.
Foundstone	filewatch.exe	.
Foundstone	fpipe	Use: (redirector) . TCP/UDP . Syntax: FPipe [- hvu?] [- lrs <port>] [- i IP] IP Examples: fpipe - l 53 - s 53 - r 80 192.168.1.101

Foundstone	fport.exe	Use: (opened) TCP/IP
		
		                          .
		
		Syntax: fport /p /a /l /ap
		
		Examples: 1)
		
		       ➢ fport /p
		
		      2)
		
		      > fport /a

Foundstone	fscan.exe	Use: (sl.exe) Syntax: FScan [- abefhqnv?] [- cditz <n>] [- flo <file>] [- pu <n>[,<n>-<n>]] IP[,IP- IP] Examples: FScan - p 80 192.168.10.3,10.1.2.4,10.1.2.5- 10.1.2.20
Foundstone	ntlast.exe	/ / .
Foundstone	afind.exe	.

Foundstone	sfind.exe	NTFS
Foundstone	hunt.exe	Use: .
		Syntax: hunt \ \ servername
		Exampes: hunt \ \ Serious_PC

```
Forensic Cmd Shell                                              _ □ X
17:13:19.08 D:\win32\john-win32> hunt \\oem-xaj6mefch
Error = 997
share = E$ - Default share
share = IPC$ - Remote IPC
share = print$ - 프린터 드라이버
share = ADMIN$ - Remote Admin
share = C$ - Default share
User = Administrator, , ,
Admin is OEM-XAJ6MEFCH\Administrator
User = Guest, , ,
User = IUSR_OEM-XAJ6MEFCH, , ,
User = IWAM_OEM-XAJ6MEFCH, IIS , ,
User = NetShowServices, Windows Media , Windows Media , Windows Media
User = TsInternetUser, TsInternetUser, ,
User = __vmware_user__, __vmware_user__, , UMware User

17:13:21.23 D:\win32\john-win32>
```

getif	getif.2.2.exe	snmp (get, set, getnext, walk, trap)
john-win32	john.exe	Use: ( )
		Syntax: john [OPTIONS] [PASSWORD-FILES]
oracle	getsids.exe	Use: TNS listener Sid
		.
		Syntax: getsids <ip> <port>
		Examples: getsids 192.168.10.100 1521
pwdump2	pwdump2.exe	Use: NT/2000/XP SAM
		.
		Note: , SAM
		LC3(www.atstake.com/lc3) .
		Syntax: pwdump2 > passdump.txt
		Examples: pwdump2
pwdump3e	pwdump3e.exe	Use: NT/2000/XP SAM
		.
		Note: SAM .
		"Remote Registry Service" ADMIN$
		.
		Syntax: PWDUMP3E machineName [outputFile] [userName]
		Examples: pwdump3e \ \ 192.168.10.100
sysinternals	handle.exe	NT/2000/XP handle (Process PID,
		handle Value, Type, Access Mask, Name)

sysinternals	listdlls.exe	Use: NT/2000/XP dll (Process PID, Base Address, Mapped Size, Description, Version, Time Stamp, Memory Mapped, Path, Company Name, Image Base Address) Note: - Syntax: listdlls [-r] [processname|pid] listdlls [-r] [-d dllname] Examples: listdlls –r foo.exe

sysinternals	psexec.exe	Use: Symantec's PcAnywhere
		                                                    telnet .
		 Note:
		                                              telnet .
		 Syntax: psexec \\ computer [-u user [-p psswd]][-s][-i][-c [-f]][-d] cmd [arguments]
		 Examples: > psexec \\ serious_system cmd.exe
		       ➢ psexec \\ serious_system ipconfig /all
		       ➢ psexec \\ serious_system –c cracking_tools.exe
		       ➢ psexec \\ serious_system c:\ bin\ test.exe

sysinternals	psinfo.exe	Use: NT/2000/XP . Note: , , Hot-Fix Syntax: psinfo [-h] [-s] [\\ RemoteComputer] Examples: > psinfo \\ develop –h
sysinternals	pskill.exe	Use: . Syntax: pskill [\\ RemoteComputer [-u Username]] <process Id or name> Examples: > pskill \\ serious_com –u guest –p 1234 rcmd
sysinternals	pslist.exe	Use: . Note: NT/2000 , pslist . Syntax: pslist [-d][-m][-x][-t][-s [n] [-r n] [\\ computer [-u username][-p password] [name|pid] Examples: > pslist 503
sysinternals	psloggedon.exe	Use: "net" . Note: "Remote Registry Service" , . Syntax: psloggedon [-l] [-x] [\\ computername] Examples: > psloggedon -l
sysinternals	psloglist.exe	Use: . Syntax: psloglist [\\ RemoteComputer [-u Username [-p Password]]] [-s [-t delimiter]] [-n #	-d #][-c][-x][-r][-a mm/dd/yy][-b

		mm/dd/yy] [-f filter] [-l event log file] <event log>
		Examples: > psloglist security
sysinternals	psservice.exe	Use: NT/2000/XP .
		Syntax: psservice [\\Computer [-u Username [-p Password]]] <cmd> <optns>
		Examples: > psservice \\serious –u administrator –p 1234
ngSniff-1.1	ngsniff.exe	Use:
		W2K OS .
		Syntax: ngSniff --interface <num> [--help | --list-interfaces | --ignore-addr <host> | -only-addr <host>]
		Examples: > ngsniff --interface O --file c:\forensics_data\ngsniff.log
wincpuid	wcpuid.exe	Use: Win32 / Linux / FreeBSD OS
		.
		Syntax: wcpuid.exe
		Examples: > wcpuid.exe
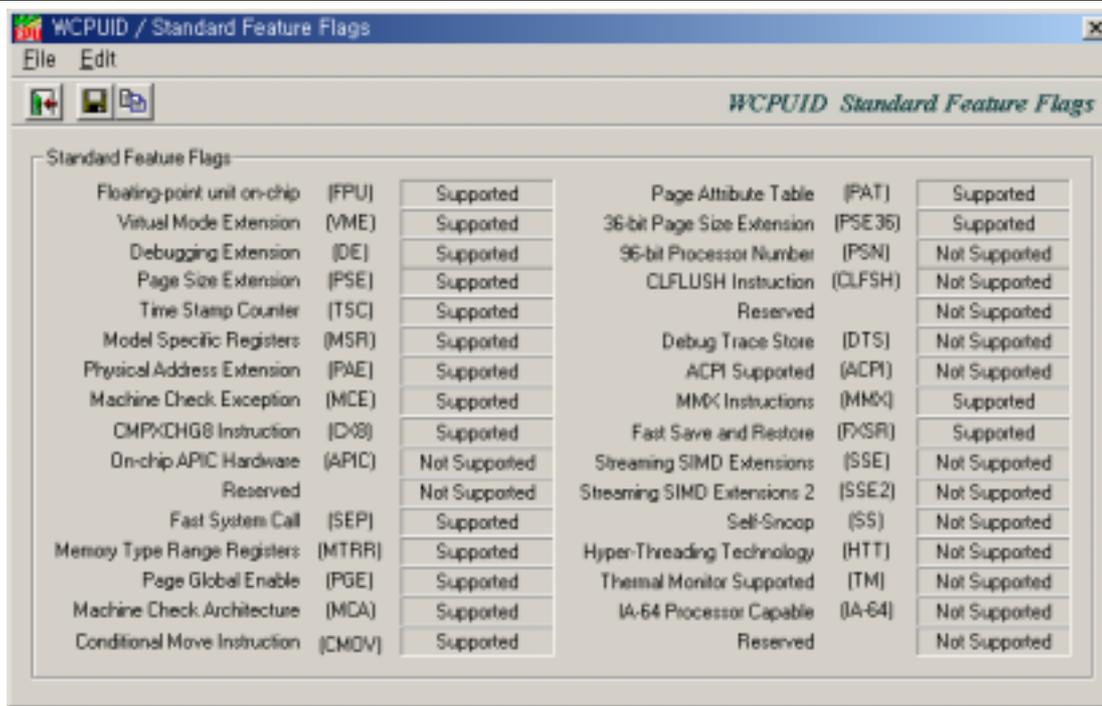
(Incident Response Scripts)

:   batch   .

                                          , Forensic   netcat

              .   NT/2000

            .

                              .

                  (baseline)   .

Windows NT/2000/XP

:   ,   OS

ir.bat   .

```
set path=.
cd ..\ windows\ ir
..\ WinNT\ doskey /history
time /t
date /t
REM request user to input date time
REM datetime
REM network state
..\ WinNT\ ipconfig /all
promiscdetect
netstat - an
route print
fport
pslist
nbtstat - c
psloggedon
time /t
date /t
..\ WinNT\ doskey /history
cd ..\ ..\
echo "completed!"
```

:   ,   ,   ,

OS   ir2.bat   .

```
cd ..\ Windows\ ir2
date /t
time /t

REM dump log files
dumpel - l security
dumpel - l application
dumpel - l system
date /t
time /t
REM last sucessful interactive logon
ntlast - l:i - null - n 100
REM last sucessful remote logon
```

```
ntlast - l:r - null - n 100
REM last failed logon
ntlast - f - null - n 100


REM get user info
reg query "HKLM\ SOFTWARE\ Microsoft\ Windows NT\ CurrentVersion\ RegisteredOwner"
reg query "HKLM\ SOFTWARE\ Microsoft\ Windows NT\ CurrentVersion\ RegisteredOrganization"
reg query "HKLM\ SOFTWARE\ Microsoft\ Windows NT\ CurrentVersion\ ProductID"
reg query "HKLM\ SOFTWARE\ Microsoft\ Windows NT\ CurrentVersion\ ProfileList"
reg query "HKLM\ SAM\ SAM\ Domains\ Account\ Users\ Names


REM users/groups
net user
net localgroup
REM admins list
REM local administrators



reg query "HKLM\ SOFTWARE\ Microsoft\ Windows NT\ CurrentVersion\ Winlogon"


REM get system info
reg query "HKLM\ System\ Controlset001\ Control\ ComputerName\ ComputerName"
reg query "HKLM\ System\ Controlset001\ Control\ ActiveComputerName"
reg query "HKLM\ SOFTWARE\ Microsoft\ Windows NT\ CurrentVersion\ Currentversion"
reg query "HKLM\ SOFTWARE\ Microsoft\ Windows NT\ CurrentVersion\ CSDVersion"
reg query "HKLM\ SOFTWARE\ Microsoft\ Windows NT\ CurrentVersion\ WinLogon\ LegalNoticeText"


REM get timezone info


reg query "HKLM\ System\ CurrentControlSet\ Control\ TimeZoneInformation\ StandardName"


REM swap file setting
reg query "HKLM\ System\ CurrentControlSet\ Control\ Session Manager\ Memory
Management\ ClearPageFileAtShutDown"
reg query "HKLM\ System\ CurrentControlSet\ Services\ LanmanServer\ Shares"


REM recent files
reg query "HKLM\ Software\ Microsoft\ Windows\ CurrentVersion\ Explorer\ RecentDocs"


REM startup programs
```

```
reg query "HKLM\ Software\ Microsoft\ Windows\ CurrentVersion\ run"
reg query "HKLM\ Software\ Microsoft\ Windows\ CurrentVersion\ runonce"
reg query "HKLM\ Software\ Microsoft\ Windows\ CurrentVersion\ runonceEx"
reg query "HKLM\ Software\ Microsoft\ Windows\ CurrentVersion\ runServices"
reg query "HKLM\ Software\ Microsoft\ Windows\ CurrentVersion\ runServicesOnce"
reg query "HKLM\ Software\ Microsoft\ Windows NT\ CurrentVersion\ Windows\ Load"
reg query "HKLM\ Software\ Microsoft\ Windows NT\ CurrentVersion\ WinLogon\ Userinit"

REM query Network Interface
REM reg query "HKLM\ System\ CurrentControlSet\ Services\ Tcpip\ Parameters\ Interfaces" /S
reg query "HKLM\ System\ CurrentControlSet\ Services\ Tcpip\ Parameters" /S
REM query Telnet Services
reg query "HKLM\ System\ CurrentControlSet\ Services\ Tlntsvr" /S

REM browser proxy setting
reg query "HKCU\ Software\ Microsoft\ Windows\ CurrentVersion\ Internet Settings"

REM explorer history and settings
reg query "HKCU\ Software\ Microsoft\ Windows\ CurrentVersion\ Explorer\ ComDlg32\ OpenSaveMRU" /S
reg query "HKCU\ Software\ Microsoft\ Windows\ CurrentVersion\ Explorer\ RunMRU" /S
reg query "HKCU\ Software\ Microsoft\ Windows\ CurrentVersion\ Explorer\ Shell Folders" /S
reg query "HKCU\ Software\ Microsoft\ Windows\ CurrentVersion\ Explorer\ User Shell Folders" /S
cd ..\ ..\
```

```
CURDIR=`./linux2.2_x86/pwd`
BINDIR="$CURDIR/linux2.2_x86"
$BINDIR/echo "All output can be redirected to your choice of storage or netcat pipe."

$BINDIR/echo "========"
$BINDIR/echo "hostname:"
$BINDIR/echo "========"
$BINDIR/hostname
$BINDIR/echo

$BINDIR/echo "========"
$BINDIR/echo "cpu info:"
$BINDIR/echo "========"
$BINDIR/cat /proc/cpuinfo
```

```
$BINDIR/echo

$BINDIR/echo "========="
$BINDIR/echo "disk use:"
$BINDIR/echo "========="
$BINDIR/df - h
$BINDIR/echo

$BINDIR/echo "============="
$BINDIR/echo "fdisk output:"
$BINDIR/echo "============="
fdisk - l
# need a binary for this
$BINDIR/echo

$BINDIR/echo "========="
$BINDIR/echo "version:"
$BINDIR/echo "========="
$BINDIR/cat /proc/version
$BINDIR/echo

$BINDIR/echo "=================="
$BINDIR/echo "kernel boot params:"
$BINDIR/echo "=================="
$BINDIR/cat /proc/cmdline
$BINDIR/echo

$BINDIR/echo "================================="
$BINDIR/echo "Local shell environment variables:"
$BINDIR/echo "================================="
$BINDIR/env
$BINDIR/echo

$BINDIR/echo "========================="
$BINDIR/echo "currently logged in users:"
$BINDIR/echo "========================="
$BINDIR/who
$BINDIR/echo

$BINDIR/echo "========================="
```

```
$BINDIR/echo "List of running processes:"
$BINDIR/echo "=========================="
ps - efl
# $BINDIR/ps - efl ; need static ps command

$BINDIR/echo
$BINDIR/echo "====================="
$BINDIR/echo "Network interface info"
$BINDIR/echo "====================="
$BINDIR/ifconfig - a
$BINDIR/echo
$BINDIR/ifconfig - s
$BINDIR/echo

$BINDIR/echo
$BINDIR/echo "=================="
$BINDIR/echo "arp table entries:"
$BINDIR/echo "=================="
$BINDIR/arp - n
$BINDIR/echo

$BINDIR/echo
$BINDIR/echo "=================="
$BINDIR/echo "/etc/hosts file:"
$BINDIR/echo "=================="
$BINDIR/cat /etc/hosts
$BINDIR/echo

$BINDIR/echo
$BINDIR/echo "====================="
$BINDIR/echo "/etc/resolv.conf file:"
$BINDIR/echo "====================="
$BINDIR/cat /etc/resolv.conf
$BINDIR/echo

$BINDIR/echo
$BINDIR/echo "====================="
$BINDIR/echo "/etc/passwd file:"
$BINDIR/echo "====================="
$BINDIR/cat /etc/passwd
```

```
$BINDIR/echo


$BINDIR/echo
$BINDIR/echo "====================="
$BINDIR/echo "/etc/shadow file:"
$BINDIR/echo "====================="
$BINDIR/cat /etc/shadow
$BINDIR/echo


$BINDIR/echo
$BINDIR/echo "================================="
$BINDIR/echo "netstat output(current connections)"
$BINDIR/echo "================================="
$BINDIR/netstat - anp
$BINDIR/echo


$BINDIR/echo "============="
$BINDIR/echo "routing table:"
$BINDIR/echo "============="
$BINDIR/netstat - rn
$BINDIR/echo


$BINDIR/echo "==========================="
$BINDIR/echo "listening ports (via lsof):"
$BINDIR/echo "==========================="
$BINDIR/lsof - P - i - n
$BINDIR/echo


$BINDIR/echo "==========="
$BINDIR/echo "lsof output:"
$BINDIR/echo "==========="
$BINDIR/lsof
$BINDIR/echo


$BINDIR/echo "==========="
$BINDIR/echo "Memory info:"
$BINDIR/echo "==========="
$BINDIR/cat /proc/meminfo
$BINDIR/echo
$BINDIR/echo
```

```
$BINDIR/echo "============"
$BINDIR/echo "Module info:"
$BINDIR/echo "============"
$BINDIR/cat /proc/modules
$BINDIR/echo
$BINDIR/echo

$BINDIR/echo "=========="
$BINDIR/echo "Mount info:"
$BINDIR/echo "=========="
$BINDIR/cat /proc/mounts
$BINDIR/echo
$BINDIR/echo "Swap info:"
$BINDIR/echo "========="
$BINDIR/cat /proc/swaps
$BINDIR/echo
$BINDIR/echo "=========="
$BINDIR/echo "   fstab   "
$BINDIR/echo "=========="
$BINDIR/cat /etc/fstab
$BINDIR/echo
$BINDIR/echo


$BINDIR/echo
"================================================================="
$BINDIR/echo "Running Process info:"
$BINDIR/echo
"================================================================="
$BINDIR/ls /proc | sort -n | grep -v [a-z,A-Z] | while read PID
  do
        $BINDIR/echo "Process ID $PID:"
        $BINDIR/echo "/proc/$PID/cmdline:"
        $BINDIR/cat /proc/$PID/cmdline
        $BINDIR/echo
        $BINDIR/echo
        $BINDIR/echo "/proc/$PID/environ:"
        $BINDIR/cat /proc/$PID/environ
        $BINDIR/echo
```

```
        $BINDIR/echo
        $BINDIR/echo "/proc/$PID/maps:"
        $BINDIR/cat /proc/$PID/maps
        $BINDIR/echo
        $BINDIR/echo
        $BINDIR/echo "/proc/$PID/stat:"
        $BINDIR/cat /proc/$PID/stat
        $BINDIR/echo
        $BINDIR/echo
        $BINDIR/echo "/proc/$PID/statm:"
        $BINDIR/cat /proc/$PID/statm
        $BINDIR/echo
        $BINDIR/echo
        $BINDIR/echo "/proc/$PID/status:"
        $BINDIR/cat /proc/$PID/status
        $BINDIR/echo
        $BINDIR/echo
        $BINDIR/echo "/proc/$PID/mem:"
        $BINDIR/cat /proc/$PID/mem
        $BINDIR/echo
        $BINDIR/echo
        $BINDIR/echo "/proc/$PID/root:"
        $BINDIR/ls - ld /proc/$PID/root
        $BINDIR/echo
        $BINDIR/echo "/proc/$PID/cwd:"
        $BINDIR/ls - ld /proc/$PID/cwd
        $BINDIR/echo
        $BINDIR/echo "/proc/$PID/exe:"
        $BINDIR/ls - ld /proc/$PID/exe
        $BINDIR/echo
        $BINDIR/echo "/proc/$PID/fd/*:"
        $BINDIR/ls - lrta /proc/$PID/fd/
        $BINDIR/echo
        $BINDIR/echo "========================================================="
        $BINDIR/echo
    done

$BINDIR/echo "================="
$BINDIR/echo "SUID/SGID search:"
$BINDIR/echo "================="
```

```
$BINDIR/echo
find / - perm - 2000 - o - perm - 4000 - print | xargs $BINDIR/ls - l { }


$BINDIR/echo "================="
$BINDIR/echo "File permissions:"
$BINDIR/echo "================="
$BINDIR/echo "/etc:"
$BINDIR/echo "- - - - -"
$BINDIR/ls - lrta /etc
$BINDIR/echo
$BINDIR/echo "/bin:"
$BINDIR/echo "- - - - -"
$BINDIR/ls - lrta /bin
$BINDIR/echo
$BINDIR/echo "/sbin:"
$BINDIR/echo "- - - - - -"
$BINDIR/ls - lrta /sbin
$BINDIR/echo
$BINDIR/echo "/usr:"
$BINDIR/echo "- - - - -"
$BINDIR/ls - Rlrta /usr
$BINDIR/echo
$BINDIR/echo "/var:"
$BINDIR/echo "- - - - -"
$BINDIR/ls - Rlrta /var
$BINDIR/echo
$BINDIR/echo "/dev:"
$BINDIR/echo "- - - - -"
$BINDIR/ls - Rlrta /dev
$BINDIR/echo
$BINDIR/echo "/home:"
$BINDIR/echo "- - - - - -"
$BINDIR/ls - Rlrta /home
$BINDIR/echo
$BINDIR/echo "/lib:"
$BINDIR/echo "- - - - - -"
$BINDIR/ls - Rlrta /lib
$BINDIR/echo
$BINDIR/echo "========================================================="
```

```
$BINDIR/echo "================"
$BINDIR/echo "MD5SUMs:"
$BINDIR/echo "================"
$BINDIR/echo "/etc:"
$BINDIR/echo "- - - - -"
$BINDIR/md5sum /etc/*
$BINDIR/echo
$BINDIR/echo "/bin:"
$BINDIR/echo "- - - - -"
$BINDIR/md5sum /bin/*
$BINDIR/echo
$BINDIR/echo "/sbin:"
$BINDIR/echo "- - - - - -"
$BINDIR/md5sum /sbin/*
$BINDIR/echo
$BINDIR/echo "/usr:"
$BINDIR/echo "- - - - -"
$BINDIR/md5sum /usr/*
$BINDIR/echo
$BINDIR/echo "/var:"
$BINDIR/echo "- - - - -"
$BINDIR/md5sum /var/*
$BINDIR/echo
$BINDIR/echo "========================================================"

# $BINDIR/echo "Make sure to grab /proc/kcore"
```

:   .

```
CURDIR=`./solaris_2.7/pwd`
BINDIR="$CURDIR/solaris_2.7"
$BINDIR/echo "All output can be redirected to your choice of storage or netcat pipe."

$BINDIR/echo "========"
$BINDIR/echo "hostname:"
$BINDIR/echo "========"
$BINDIR/hostname
$BINDIR/echo
```

```
$BINDIR/echo "========"
$BINDIR/echo "disk use:"
$BINDIR/echo "========"
$BINDIR/df
$BINDIR/echo

$BINDIR/echo "==================="
$BINDIR/echo "disk format output:"
$BINDIR/echo "==================="
$BINDIR/echo "Need to add format output"
# fdisk - l
# need a binary for this
$BINDIR/echo

$BINDIR/echo "================================="
$BINDIR/echo "Local shell environment variables:"
$BINDIR/echo "================================="
$BINDIR/env
$BINDIR/echo

$BINDIR/echo "========================="
$BINDIR/echo "currently logged in users:"
$BINDIR/echo "========================="
$BINDIR/who
$BINDIR/echo

$BINDIR/echo "========================="
$BINDIR/echo "List of running processes:"
$BINDIR/echo "========================="
ps - efl
# $BINDIR/ps - efl ; need static ps command

$BINDIR/echo
$BINDIR/echo "===================="
$BINDIR/echo "Network interface info"
$BINDIR/echo "===================="
$BINDIR/ifconfig - a
$BINDIR/echo
$BINDIR/ifconfig - s
$BINDIR/echo
```

```
$BINDIR/echo
$BINDIR/echo "================="
$BINDIR/echo "arp table entries:"
$BINDIR/echo "================="
$BINDIR/arp - n
$BINDIR/echo

$BINDIR/echo
$BINDIR/echo "================="
$BINDIR/echo "/etc/hosts file:"
$BINDIR/echo "================="
$BINDIR/cat /etc/hosts
$BINDIR/echo

$BINDIR/echo
$BINDIR/echo "====================="
$BINDIR/echo "/etc/resolv.conf file:"
$BINDIR/echo "====================="
$BINDIR/cat /etc/resolv.conf
$BINDIR/echo

$BINDIR/echo
$BINDIR/echo "====================="
$BINDIR/echo "/etc/passwd file:"
$BINDIR/echo "====================="
$BINDIR/cat /etc/passwd
$BINDIR/echo

$BINDIR/echo
$BINDIR/echo "====================="
$BINDIR/echo "/etc/shadow file:"
$BINDIR/echo "====================="
$BINDIR/cat /etc/shadow
$BINDIR/echo

$BINDIR/echo
$BINDIR/echo "================================"
$BINDIR/echo "netstat output(current connections)"
$BINDIR/echo "================================"
```

```
$BINDIR/netstat - an
$BINDIR/echo


$BINDIR/echo "=============="
$BINDIR/echo "routing table:"
$BINDIR/echo "=============="
$BINDIR/netstat - rn
$BINDIR/echo


$BINDIR/echo "=========================="
$BINDIR/echo "listening ports (via lsof):"
$BINDIR/echo "=========================="
$BINDIR/lsof - P - i - n
$BINDIR/echo


$BINDIR/echo "============"
$BINDIR/echo "lsof output:"
$BINDIR/echo "============"
$BINDIR/lsof
$BINDIR/echo


$BINDIR/echo "=========="
$BINDIR/echo "Mount info:"
$BINDIR/echo "=========="
mount
$BINDIR/echo
$BINDIR/echo "=========="
$BINDIR/echo "    fstab    "
$BINDIR/echo "=========="
$BINDIR/cat /etc/vfstab
$BINDIR/echo
$BINDIR/echo


$BINDIR/echo "================="
$BINDIR/echo "SUID/SGID search:"
$BINDIR/echo "================="
$BINDIR/echo
find / - perm - 2000 - o - perm - 4000 - print | xargs $BINDIR/ls - l {}


$BINDIR/echo "================="
```

```
$BINDIR/echo "File permissions:"
$BINDIR/echo "================="
$BINDIR/echo "/etc:"
$BINDIR/echo "- - - - -"
$BINDIR/ls - lrta /etc
$BINDIR/echo
$BINDIR/echo "/bin:"
$BINDIR/echo "- - - - -"
$BINDIR/ls - lrta /bin
$BINDIR/echo
$BINDIR/echo "/sbin:"
$BINDIR/echo "- - - - - -"
$BINDIR/ls - lrta /sbin
$BINDIR/echo
$BINDIR/echo "/usr:"
$BINDIR/echo "- - - - -"
$BINDIR/ls - Rlrta /usr
$BINDIR/echo
$BINDIR/echo "/var:"
$BINDIR/echo "- - - - -"
$BINDIR/ls - Rlrta /var
$BINDIR/echo
$BINDIR/echo "/dev:"
$BINDIR/echo "- - - - -"
$BINDIR/ls - Rlrta /dev
$BINDIR/echo
$BINDIR/echo "/home:"
$BINDIR/echo "- - - - - -"
$BINDIR/ls - Rlrta /home
$BINDIR/echo
$BINDIR/echo "/lib:"
$BINDIR/echo "- - - - - -"
$BINDIR/ls - Rlrta /lib
$BINDIR/echo
$BINDIR/echo "========================================================"
$BINDIR/echo "================="
$BINDIR/echo "MD5SUMs:"
$BINDIR/echo "================="
$BINDIR/echo "/etc:"
$BINDIR/echo "- - - - -"
```

```
$BINDIR/md5sum /etc/*
$BINDIR/echo
$BINDIR/echo "/bin:"
$BINDIR/echo "- - - - -"
$BINDIR/md5sum /bin/*
$BINDIR/echo
$BINDIR/echo "/sbin:"
$BINDIR/echo "- - - - - -"
$BINDIR/md5sum /sbin/*
$BINDIR/echo
$BINDIR/echo "/usr:"
$BINDIR/echo "- - - - -"
$BINDIR/md5sum /usr/*
$BINDIR/echo
$BINDIR/echo "/var:"
$BINDIR/echo "- - - - -"
$BINDIR/md5sum /var/*
$BINDIR/echo
$BINDIR/echo "======================================================"


# $BINDIR/echo "Make sure to grab /proc/kcore"
```

　　　　Live　　　　　　　　　　　　　　　　　　　,　　　　　　　　　　　　　　　　　　　　　　　Biatchux
　　　　　　　.　　　　off- line　　　　　　　　　　　　　　　　　　　　　　　　　　Biatchux
　　　　　　　.　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　.

　　1.　CD- ROM
　　　-.　　　　　　　　　　　　　　　　CD- ROM　　　　　　　　　BIOS　　　　　　　.
　　　-. Biatchux CD　CD- ROM　　　　　　　　　　　　.
　　2.
　　　-. CD- ROM　　　　　　　　　　　　　　1, 3, 4　　　　　　　.
　　　-.　　　　　　　　　　　　　　　　　　　　　　(　　　　　　3　　).
　　3.
　　　-. Biatchux　　　　　　　　　　　　　　　　　.
　　　-.　　　　　　　　　　　　　　　　　　　　　　　　　　.

(   )
Forensics   IP   192.168.10.110
Forensics# nc –l –p 3147 > victim_sda1.img
Biatchux CD- ROM
[root@ FIRE] root> ifconfig eth0 192.168.10.111 netmask 255.255.255.0 broadcast 192.168.10.255
[root@ FIRE] root> route add –net default gw 192.168.10.1
[root@ FIRE] root> cd /data
[root@ FIRE] root>dd if=/dev/sda1	nc –nv 192.168.10.110 3147

- .   (victim_sda1.img)
.

4.

- .   .

     3   .

Forensics# md5sum victim_sda1.img
c8f201b2ffb65595a6c2af6a1c51bb66
Biatchux CD- ROM
[root@ FIRE] root>md5sum /dev/sda1
c8f201b2ffb65595a6c2af6a1c51bb66

5.

- .   off- line

           .   Biatchux

                        .

Biatchux CD- ROM
[root@ FIRE] root>mount –ro,noatime,nosuid,nodev,noexec /dev/sda1 /mnt/sda1
[root@ FIRE] root> mount

6.   SSHD(SecureShell Daemon)

   :   SSHD   /sbin/   ,   /etc/ssh/sshd_config   .

   2222/tcp   .

Biatchux CD- ROM
[root@ FIRE] root> start- sshd.sh
[root@ FIRE] root> netstat - ntl

```
[root@FIRE] sbin> netstat -ntl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp       0      0 0.0.0.0:2222           0.0.0.0:*              LISTEN
tcp       0      0 0.0.0.0:6000           0.0.0.0:*              LISTEN
[          18:21:19]
[root@FIRE] sbin> ps -ef | grep sshd
root       606     1  0 18:05 ?         00:00:00 /usr/sbin/sshd -f /etc/ssh/sshd_
root       634     1  0 18:21 ?         00:00:00 /usr/sbin/sshd -f /etc/ssh/sshd_
[          18:21:23]
[root@FIRE] sbin> cat /sbin/start-sshd.sh
#!/bin/sh
echo "creating sshd keys"
ssh-keygen -b 1024 -f /etc/ssh/ssh_host_dsa_key -t dsa -P ""
ssh-keygen -b 1024 -f /etc/ssh/ssh_host_rsa_key -t rsa -P ""
#ssh-keygen -b 1024 -f /etc/ssh/ssh_host_key -t rsal -P ""

echo "Starting sshd server listening on port 2222"
/usr/sbin/sshd -f /etc/ssh/sshd_config &

[          18:22:02]
[root@FIRE] sbin>
```

7. VNCServer(vncserver)

   : VNC   (Virtual Network Computing)   .

   "   "   . VNC

   OS   OS   , JAVA

   . VNC   http://www.realvnc.com/   . Biatchux   VNC   .

Biatchux CD-ROM
[root@ FIRE] root> vncpasswd
[root@ FIRE] root> vncserver :0 –geometry 1024x768 - depth 16
[root@ FIRE] root> netstat - ntl

```
[root@FIRE] root> vncpasswd
Password:
Verify:
[          10:09:13]
[root@FIRE] root> vncserver :0 -geometry 1024x768 -depth 16

New 'X' desktop is prometheus:0

Starting applications specified in /home/root/.vnc/xstartup
Log file is /home/root/.vnc/prometheus:0.log

[          10:10:51]
[root@FIRE] root> netstat -ntl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp       0      0 0.0.0.0:5800           0.0.0.0:*              LISTEN
tcp       0      0 0.0.0.0:5900           0.0.0.0:*              LISTEN
tcp       0      0 0.0.0.0:2222           0.0.0.0:*              LISTEN
tcp       0      0 0.0.0.0:6000           0.0.0.0:*              LISTEN
[          10:10:58]
[root@FIRE] root>
```

VNC
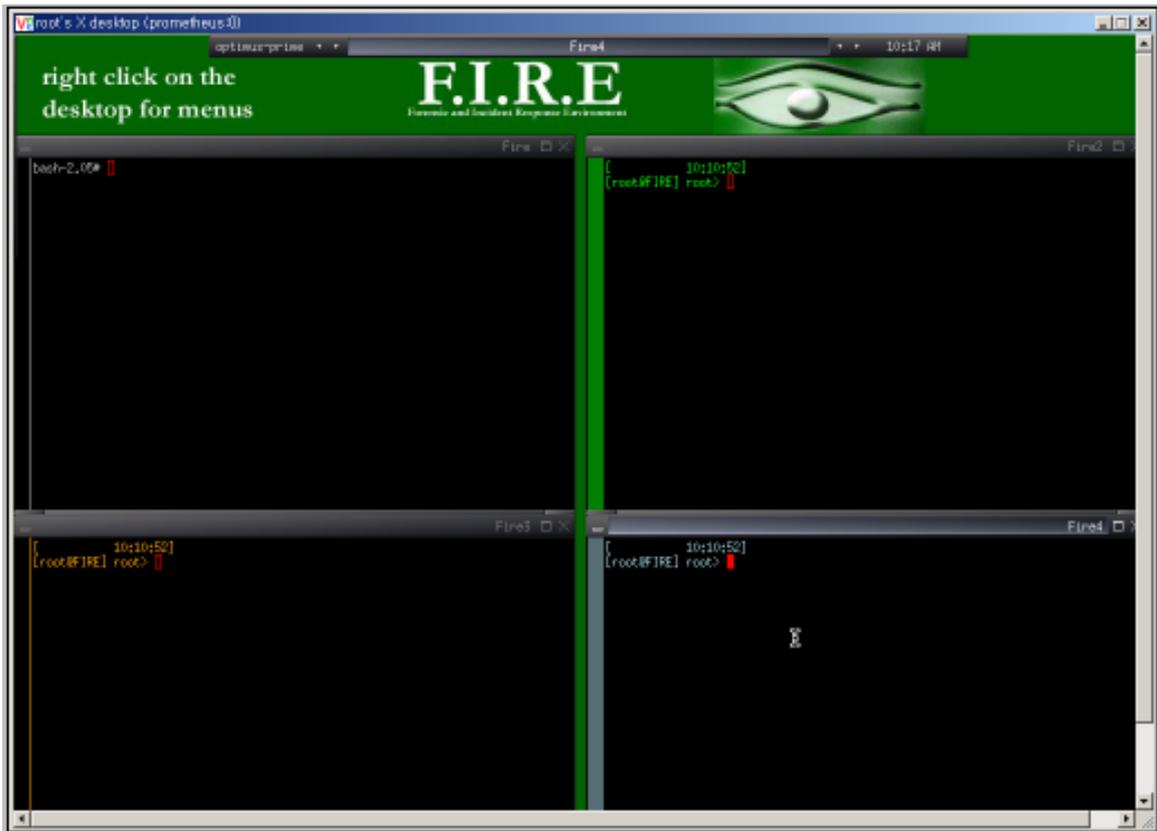
9. Vncviewer   Biatchux 0.4a   X- Windows

Biatchux

10. Biatchux 0.4a

Administrivia	services	start-em
services ▸	start-em ▸	Start TelnetD -single session
calculator	stop-em ▸	Start SSHD
PCMCIA start		Start TFTPD-RW
start Xscreensaver		Start TFTPD-RO
		Start Apache v1.3.27
		Start irc server
		Start FTPD -not enabled yet
		Start PXE-Server -not enabled yet
		Start DHCP-Server -not enabled yet

Shells/Consoles	logging
logging ▸	respawn all logging xterms
non-logging ▸	

Network	dhcp net config
dhcp net config ▸	dhcp on eth0
Etherape	dhcp on eth1
gabber	dhcp on eth2
xchat	

Virus Scan

Virus Scan mounted filesystems
Update Signatures from Net
Update Signatures from Floppy

Forensics	Local Drives
Local Drives ▸	Mount local partitions
rescan scsi bus	Unmount local partitions
Firewire Devices ▸	**Firewire Devices**
USB Devices ▸	Mount FireWire partitions
Autopsy	UnMount FireWire partitions
Outlook .pst exam -not yet	**USB Devices**
OutlookExpress .dbx exam -not yet	USB 1.1 Devices ▸
	USB 2.0 Devices - experimental ▸

Docs	PenTest Tools
MS Fat spec	Xnmap
Another Fat spec	@stake WebProxy
iso9660 spec	Nessusd+client
Another iso9660 spec	Nessus client
Open Source Security Testing Methodology Manual	ip sorcery
	VNCviewer
	rdesktop - MS Term Client
	Netware Tools ▸
	Exploits ▸
	DoS ▸

Sniffers	Editors
Ethereal	hexedit
sniffit	vi
ettercap	pico-nano
dsniff	
p0f	
PHoss	
hunt	

11. Biatchux 0.4a

12. Biatchux 0.4a   Mozilla

Biatchux

. Biatchux   find, grep

:

chkrootkit –   .
The Coroner's Toolkit(TCT) –   .
tctutils - Brian Carrier   , TCTUtils   TCT   .
Autopsy – TCT   TCTUtils   GUI   .
                                                                      ,   , inode   .
                      ,   .
mac- robber -   ,   inode   (MAC),   ,
                      timeline   (grave- robber   - m   ).
stegdetect –   JPEG
                      .

                      Examples: $ stegdetect *.jpg

                                  cold_dvd.jpg : outguess(old)(***) jphide(*)

                                  dscf0001.jpg : negative

                                  dscf0002.jpg : jsteg(***)

                                  dscf0003.jpg : jphide(***)

                                  [...]

                                  $ stegbreak - tj dscf0002.jpg

                                  Loaded 1 files...

                                  dscf0002.jpg : jsteg(wonderland)

Processed 1 files, found 1 embeddings.

Time: 36 seconds: Cracks: 324123,   8915 c/s

hexedit –   hex   .

LDE –   – inode   ,   ,   .

OpenOffice 1.0.1 –   .

Biatchux

Biatchux   .   :

            : nmap, whisker, hping, firewalk, fragrouter, John-the-Ripper, nbtscan, nemesis,

              screamingCobra, onesixtyone, isnprober, hunt, pOf, THC-Hydra

                        : ethereal, tcpdump, dig, dsniff, netcat, hunt, ncftp, ngrep, pOf, arena, Sniffit,

                  Phoss, Wireless, airsnort, kismet, xchat, gabber

          : hammerhead, apachebench

    /   : hexedit, LDE

      : snort

    : ipchains, iptables

          : telnetd, sshd, ftpd(   ), tftpd, PXE-Server(   ), Apache v1.3.27, irc server,

              DHCP-Server(   ),   , PCMCIA, X-screensaver

          : Mozilla

          : Xnmap, @stake WebProxy, Nessusd+client, ip sorcery, VNC Viewer, Netware Tools(Pandora),

              rdesktop(MS Term Client), Exploits(Unicode, jill, holygrail – solaris teleted),

              Denial Of Service Attack tool(SMBdie-kills NT/2k/XP))

Exploit: bind   , bsd   , flood   , holygrail, jill, local   , rpc   , sendmail   , sparc   , ssh   ,

          unencoded-stuff   , win32   , wuftp   , random   (exploit)

      : hexedit, vi, pico-nano

Biatchux, PLAC, Trinux

	Trinux v. 0.80rc2	PLAC v. 2.9.5	Biatchux v. 0.4a
CD-ROM ?			
floppy ?			
	1.44 MB*	47 MB	117 MB
?		**	X
	X		X
?			
?	X	X	
?			
TCT	***		
tctutils	***	X	
Autopsy browser	X	X	
Ethereal		X	
tcpdump			
mac-robber	X	X	
chkrootkit	X		
LDE			
hexedit	X	X	
md5sum			
netcat			
StegDetect	X	X	
static binaries ?	X	X	X
Windows	X	X	
Linux x86	X	X	
Solaris Sparc	X	X	
?	X	X	

Biatchux

F.I.R.E.   Q&A

Q: F.I.R.E.   ?

A: F.I.R.E.   CD- ROM   .

. CD- ROM

. F.I.R.E.   William Salusky

.   .

Q: F.I.R.E.   ?

A: .

-   .

-   .

-   .

-   .

-   .

F.I.R.E.   X- Windows   CD- ROM   .

.

Q: /   F.I.R.E.   ?

A: CD- ROM

- Knoopix

- Trinux

- PLAC

Knoopix   .

F.I.R.E.   .

Trunux   3   .

F.I.R.E.

X- Windows   .

PLAC   CD- ROM   .   ,   ,   .

. F.I.R.E.

,   .

Q: ?

A: F.I.R.E.   ,   .

- Nessus, Nmap, Whisker, hping2, hunt, fragrouter
- Ethereal, Snort, tcpdump, ettercap, dsniff, airsnort
- chkrootkit, F-Prot
- tct, tctutils, Autopsy
- Testdisk, fdisk, gpart
- SSH (client and Server), VNC (client and server)
- Mozilla, ircII, mc, Perl, biew, fenris, gpg

                                                  .

Q: F.I.R.E.   **?**
A: F.I.R.E.   48MB   x86   PC   . X-Windows   800X600
                                                              .
            .

Q: F.I.R.E.   **?**
A: .
          ,   .   F.I.R.E.
            .

        F.I.R.E.

Q: F.I.R.E.   CD-ROM   **?**
A: F.I.R.E.   (*.iso)   .   , CD-
ROM   (ISDN
                    .   200MB   ).

Q: OK, ISO   **.**   **?**
A: 1. Sourceforge   MD5   .
2.   iso   CD-ROM   .   CD-ROM
          .
3.   BIOS   CD-ROM   .
4. F.I.R.E. CD   CD-ROM
            .   (3)   (4)   .

Q: MD5   **?**
A: "md5sum"   .iso   MD5   .

GNU   .

$ md5sum fire-0.4a.iso

ae810533dc3ae95e4036b2d665bd5f1a *fire-0.4a.iso

md5sum   .

                          MD5   DPASHA   .

              ,   (, fire-0.4a.iso.md5sum.txt)
                                                    .

$cat fire-0.4a.iso.md5sum.txt(   )
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

ae810533dc3ae95e4036b2d665bd5f1a *fire-0.4a.iso

-----BEGIN PGP SIGNATURE-----
Version: PGP 7.0.1

iQA/AwUBPearEQCUWsrxYo1REQKSdQCg5Dxsok4GFDLxZQchQs7q79TZLYcAn1I8
nNJ4BWGAfGsvpPOPsydI2HzQ
=iUvO
-----END PGP SIGNATURE-----

              ,   ("ae810533dc3ae95e4036b2d665bd5f1a")
                          .   sourceforge
        .

Q: CD-ROM   ?
A: iso   CD-ROM   CD-R/W   .

Q: F.I.R.E.   root   ?
A: root   "firefire"   .

Q: X-windows   .   ?
A: .

/sbin/dlg/startmenu

Q: /data   ?

A: .

                                                                 .

                   netcat   :

[Shim@REMOTE]$ nc - l - p 3147 > data.tar

F.I.R.E.   (IP Address

192.168.1.100   ):

[root@FIRE]# cd /data
[root@FIRE] tar cf - . | nc - nvv 192.168.1.100 3147

                   tar   .

[Shim@REMOTE]# tar - xvf data.tar

Q: .
A: "autoexec.sh"   FAT

      .

             F.I.R.E.   :

nano autoexec.sh
mcopy autoexec.sh a:

"autoexec.sh"   F.I.R.E.   .

               :

- - -   - - - -
#!/bin/sh
insmod 8390
insmod ne2k- pci
ifconfig eth0 192.168.1.100 up
echo nameserver 192.168.1.254 > /etc/resolv.conf
loadkeys it
- - -   - - -

             F.I.R.E.   /sbin/checkfloppy.sh   .

Q: **F.I.R.E.**   **?**   **,**   **PC**
F.I.R.E.   **.**
A: CD- ROM   . F.I.R.E.   statically
            ,   .

        F.I.R.E.

Q: **CD- ROM**   **.**
A: 4   .
1.   .iso   . MD5   .
2. CD- ROM   . iso   CD- ROM   .
3. CD- ROM   BIOS   .   BIOS   CD- ROM
                        .

4. F.I.R.E.   .   RAM   x86   PC   .

Q: **CD- ROM**   **BIOS**   **.**
A: "Smart Boot Manager"   .   CD- ROM
                .   , BIOS   CD- ROM
                    .   BIOS   CD- ROM   .

Q: **i815**   **. x- Windows**   **.**
A: F.I.R.E.   x11   VESA   . i815   VESA
        .

Q: **.**   **.**
A: vi   Bash   .

set - o emacs

            Emacs   .   .

Q: **?**
A: :

loadkeys de

                        .   .
                    :

```
# loadkeys it
```

.

Q: **NE 2000**   **PCI**   (**RealTek 8029**   ).

.

A: :

```
# insmod 8390
# insmod ne2k-pci
```

IP   (DHCP   IP   ).

Q: **"autoexec.sh"**   .
A: :

```
# /sbin/chkfloppy.sh
```

Q: **?**
A: Sourceforge   .

.

F.I.R.E.

Q: **?**
A: Joe Lofshult   FIRE   , Biatchux   . Winword   .

      F.I.R.E.   Sourceforge   .

Q: .
A: , Biatchux

      .

(References)

@ Stake. @ stake Research Labs – Tools.
<http://www.atstake.com/research/tools/index.html#forensic>.

Bajusz, Richard. Security Applications of Bootable Linux CD-ROMs. <http://rr.sans.org/linux/sec_apps.php>.

Dittrich, David. Basic Steps in Forensic Analysis of Unix Systems.
<http://staff.washington.edu/dittrich/misc/forensics/>.

Dittrich, David. "Root Kits" and hiding files/directories/processes after a break- in. January 5, 2002.
<http://staff.washington.edu/dittrich/misc/faqs/rootkits.faq>.

Foundstone - Free Tools. <http://www.foundstone.com/knowledge/free_tools.html>.

Franz, Matthew. Trinux homepage. <http://trinux.sourceforge.net/>.

Lee, Rob. Incident- Response homepage. <http://incident- response.org/>.

Mandia, Kevin and Chris Prosise. Incident Response: Investigating Computer Crime. Berkeley:
Osborne/McGraw Hill, 2001.

Project: Portable Linux Auditing CD. <http://sourceforge.net/projects/plac>.

Salusky, William and David Zendzian. Biatchux. <http://biatchux.dmzs.com/>.

Showalter, Brad. Trinux – A Digital Tool Belt. October 10, 2001. <http://rr.sans.org/unix/trinux.php>.

Somer, Lord. Linux Rootkit. <http://online.securityfocus.com/tools/1489>.

Vidstrom, Arne. Security Toolbox. <http://ntsecurity.nu/toolbox>.

Joe Lofshult < www.giac.org/practical/Joe_Lofshult_GSEC.doc >.

         "   " <http://www.securitymap.net/sp/docs/FreewareUnixForensicToolkit.pdf>.

         "   NT/2000   "
<http://www.securitymap.net/sp/docs/InitialResponseToWindowsNT_2000.pdf>.

Biatchux   .

2003   5   14   0.35b   0.4a   .

.   Biatchux

,   (SRC IP   , DST IP   ,   ,

)   (.   ;).   IP

.

,   .

/   ,

,   .

.

www.securitymap.net   .

E- Mail   .

jjshim AT hanaro.com