REVELA
Periódico de Divulgação Científica da FALS
Ano VII - Nº XV-JUL/ 2013 - ISSN 1982-646X

Impacto das operações da linha do tempo em sistemas de arquivos UNIX

Marcelo Teixeira de Azevedo[1], Ana Lucia Pegetti[2] e Marco Antonio Quirio da Veiga[1]
[1]Escola Politécnica da Universidade de São Paulo
Av. Prof. Luciano Gualberto, Trav. 3 n° 158, CEP 05508-90 – São Paulo – SP - Brasil
{mdeazevedo, mquirino@usp.br}

[2]Faculdade do Litoral Sul Paulista
Praça Marechal Eduardo Gomes, 50 - Vila das Acácias CEP 12.228-900 – São José dos Campos – SP

Sumário: Este estudo descreve os impacto das operações da linha do tempo em sistemas de arquivos UNIX e tem como principal objetivo ser um auxilio para investigadores forenses fornecendo um estudo detalhado sobre as operações que podem ser realizados em sistemas de arquivos. Para isto será fornecido um estudo de caso simulado com as principais operacões e entre elas podemos destacar: criação, modificação, remoção, visualização, cópia e mudança de permissão em arquivos.

Palavras-chave: MACtimes, pericia forense, arquivos unix, linha do tempo

INTRODUÇÃO

A perícia forense computacional esta cada vez mais se desenvolvendo para que as instituições possam atuar no combate a crimes eletrônicos. As informações correm risco de serem perdidas, roubadas ou violadas, onde o sistema operacional pode também ser corrompido, a segurança do sistema e seus arquivos ficam entrelaçacados por quatro pontos: confidencialidade, disponibilidade, confiança e integridade das informações [1]. Atualmente métodos básicos para coleta e interpretação de data/hora são construídos essencialmente de pequenas máquinas do tempo, sendo assim os eventos de tempo em sua totalidade devem ser considerados isoladamente e seqüencialmente para que assim possamos interpretar os seus significados dentro de um contexto mais amplo [2].

Neste artigo é realizado o estudo das técnicas para localizar e utilizar os dados relacionados a linha do tempo, com o foco em *MACtimes* em sistemas *UNIX*, além de relacionar os impactos das operações na reconstrução de tais linhas do tempo, com o foco sempre em sistemas operacionais *UNIX*.

Objetivos

Nos dias atuais são freqüentes situações na qual são expostos de forma insegura servidores e o ambiente computacional como um todo de empresas, órgãos governamentais, instituições financeiras e indús-

trias dos mais variados setores da economia moderna. Sendo assim, a segurança torna-se uma preocupação constante de qualquer segmento do mercado atual [3].

Embora existam diversas ferramentas de reconstrução cronológica pouco se conhece a respeito dos impactos das diversas operações em sistemas de arquivos *Unix* nas marcações temporais dos arquivos e diretórios [4], [5], tais como:

- Criação de arquivo;
- Remoção de arquivo;
- Modificação de arquivo;
- Renomeação de arquivo;
- Cópia de arquivo;

O objetivo inicial deste estudo é mostrar que a seqüência de tempo fornece um contexto valioso e que dependendo de sua interpretação os seus significados podem ser alterados. Também é demonstrado como as informações de tempo podem ser úteis em um incidente de segurança, bem como mostrar locais incomuns onde tais informações podem ser localizadas em registros seqüenciais em sistemas de arquivos *Unix*. Para um melhor entendimento será analisado um estudo de caso na qual pretendemos demonstrar todas as interpretações possíveis dentro de um ambiente simulado que evidenciará os impactos de tais interpretações.

Desta forma o presente estudo tem como principal objetivo auxiliar uma investigação forense, fornecendo um estudo detalhado sobre o impacto das operações da linha do tempo em sistemas *Unix*.

METODOLOGIA

Para análise do impacto das operações de linha do tempo foi utilizado o utilitário forense *SleuthKit*, que nada mais é que uma coletânea de ferramentas que possibilita a interação e investigação em sistemas de arquivos [6]. As operações informadas abaixo foram realizadas dentro de um ambiente simulado, com o propósito de evidenciar as mudanças de parâmetros para cada operação.

- Criação de arquivo;
- Modificação de arquivo;
- Visualização do arquivo;
- Cópia de arquivo;
- Remoção de arquivo;

Periódico de Divulgação Científica da FALS
Ano VII - Nº XV-JUL/ 2013 - ISSN 1982-646X

- Renomeação de arquivo;
- Leitura de arquivo;
- Operação de *move*;
- Mudança de permissão de arquivos;
- Utilização de ferramentas de *backup tar*.

Para a coleta de evidências foi utilizado a ferramenta *grave-robber* que é o utilitário principal do *SleuthKit*. Tal utilitário somente coleta as informações não interpretando de nenhuma forma os dados obtidos [7]. Embora seja uma ferramenta completa e colete informações dos mais diversos gêneros, para o nosso propósito somente as informações do arquivo *body* serão analisadas, pois neste arquivo que são armazenados as informações de *MACtimes*. Segue abaixo figura 01 que ilustra a utilização de tal utilitário.

```
root@marcelo-laptop:/home/marcelo# grave-robber -c /home/marcelo/analise -d /forensic/data2 -m -o LINUX2
root@marcelo-laptop:/home/marcelo#
```

Figura 01 - Geração dos arquivos para análise

O comando *grave-robber* é informado para realizar a varredura de *MACtimes* a partir do diretório */home/marcelo/analise* colocando toda a análise no diretório de destino */forensic/data2* informando ainda tratar-se de arquivo do sistema operacional LINUX. A consequência desta coleta, em geral, serve de base para outras ferramentas, além de manter em um único lugar todas as informações relevantes para uma análise.

Já para a construção da linha do tempo foi utilizado outra ferramenta que também faz parte do conjunto principal do *SleuthKit*, que tem como principal função construir uma linha de tempo baseado nas informações criadas pelo utilitário *grave-robber*. Desta forma são mostrados os parâmetros do *MACtimes*, e como dito anteriormente somente é evidenciado os atributos, porém nenhuma análise é realizada pela ferramenta.

Na figura 02 podemos observar a linha do tempo das operações realizadas no diretório */home/marcelo/analise* que teve todas as informações de linha do tempo armazenadas no diretório de destino */forensic/data2*. Na terceira coluna são observados os *MACtimes* propriamente dito, já na quarta, quinta e sexta coluna os atributos de permissão, dono do arquivo e grupo são mostrados respectivamente. Finalmente na última coluna as operações realizadas no arquivo associada com a data na primeira coluna, como pode ser observado os horários são registrados de maneira descendente.

```
root@marcelo-laptop:/forensic/data2# /home/marcelo/forense/tct-1.18/bin/mactime -p /etc/passwd -g /etc/group -b body 2008-10-22
Oct 20 08 19:22:27          6 m.. -rw-r--r-- root     root     /home/marcelo/analise/b
Oct 20 08 19:26:03          6 ..c -rw-r--r-- root     root     /home/marcelo/analise/b
Oct 20 08 19:38:01        199 m.c -rw-r--r-- root     root     /home/marcelo/analise/ver
Oct 23 08 01:33:12          6 .a. -rw-r--r-- root     root     /home/marcelo/analise/b
                          199 .a. -rw-r--r-- root     root     /home/marcelo/analise/ver
Nov 06 08 19:24:41         37 m.c -rw-r--r-- root     root     /home/marcelo/analise/1
Nov 06 08 19:24:48         37 .a. -rw-r--r-- root     root     /home/marcelo/analise/1
Nov 06 08 19:24:53          0 mac -rw-r--r-- root     root     /home/marcelo/analise/c
Nov 06 08 19:25:29          0 mac -rw-r--r-- root     root     /home/marcelo/analise/error.log
                         1714 mac -rw-r--r-- root     root     /home/marcelo/analise/coroner.log
root@marcelo-laptop:/forensic/data2#
```

Figura 02 - Visualização da linha do tempo

Resultados obtidos

Em uma investigação forense os dados tradicionais não fornecem informação suficiente sobre um fato ocorrido. O agrupamento cronológico de tais informações, formando uma linha do tempo, pode fornecer informações essenciais para investigação. Desta forma o uso de *MACtimes* em forense computacional torna-se essencial [8], [9]. Para compreendermos como o uso de *MACtimes* contribui para a investigação do perito computacional é necessário entendermos o que ele significa. Portanto o *MACtimes* é constituído de três atributos:

- *Mtimes* (Tempo de modificação)
- *Atime* (Tempo de acesso)
- *Ctime* (Tempo de criação)

O atributo *mtime* armazena o último momento que foi modificado o conteúdo do arquivo. Já o atributo *atime*, informa o último momento que ocorreu acesso ao arquivo, por último o *ctime* que fornece o último momento que ocorreram modificações no conteúdo e meta-informação de um arquivo.

Para demonstração de tais atributos foi proposto um ambiente simulado para que as operações mencionadas no item 03 fossem realizadas de forma apropriada e os resultados podem ser observados nas próximas etapas:

Primeira etapa: Criação de um arquivo através do utilitário *vi*. Para este item foi criado o arquivo texto denominado *arq1* através do comando *vi arq1*, posteriormente foi digitado algumas frases para compor o arquivo para experimentação.

```
Nov 12 08 01:28:25       24 mac -rw-r--r-- root     root     /root/psi5007/arq1
```

Figura 03 – MACTimes na criação de arquivo

Como pode ser observado na figura 03, os três atributos: mtime, atime e ctime foram criados e associados ao arquivo denomiado *arq1*, desta forma toda criação de arquivo são criados os três atributos básicos.

Segunda etapa: Modificação do arquivo através do utilitário *vi*. Para esta etapa foi editado o arquivo e realizado alterações, ou seja, adição de frases, remoção de frases e por último, substituição de caracteres existentes por novos caracteres.

```
Nov 12 08 01:32:53       23 .a. -rw-r--r-- root     root     /root/psi5007/arq1
Nov 12 08 01:33:02       23 m.c -rw-r--r-- root     root     /root/psi5007/arq1
```

Figura 04 – MACTimes de modificação de arquivo.

Foi observado na figura 04 que no instante da criação do arquivo (12/11/2008) o atributo de *atime* foi atualizado, ou seja, na edição de um arquivo este atributo sempre será atualizado. Já na segunda etapa que foi a gravação das modificações o atributo *mtime* e *ctime* foi atualizado, evidenciado modificação no arquivo e posterior criação. Analisando como um todo, é compreensível que ocorreu primeiramente uma edição do arquivo e posteriormente as alterações foram gravadas.

Terceira etapa: Visualização do arquivo através do comando *cat*. Para esta etapa foi realizada uma leitura no arquivo com o intuito de ler as informações nele armazenado. Nenhum tipo de modificação foi realizado no arquivo somente a leitura.

```
Nov 12 08 01:35:35       23 .a. -rw-r--r-- root     root     /root/psi5007/arq1
```

Figura 05 – MACTimes na visualização de arquivo

Observou-se que durante uma operação de leitura somente o atributo *atime* é atualizado, caso não ocorra nenhum tipo de modificação no arquivo somente tal atributo será atualizado, não ocorrendo portanto modificações nos outros atributos, conforme ilustrado na figura 05.

Quarta etapa: Cópia do arquivo *arq1* para *arq2*. Para esta operação foi utilizado o comando de cópia: *cp*. Exemplo *cp arq1 arq2*. Onde *arq1* é o arquivo de origem e *arq2* o arquivo de destino.

```
Nov 12 08 01:33:02       23 m.c -rw-r--r-- root     root     /root/psi5007/arq1
Nov 12 08 01:35:35       23 .a. -rw-r--r-- root     root     /root/psi5007/arq1
Nov 12 08 01:37:37       23 mac -rw-r--r-- root     root     /root/psi5007/arq2
```

Figura 06 – MACTimes na cópia de arquivo

Durante a cópia do arquivo foi observado que os atributos de *mactimes* permanecem intactos para o arquivo de origem. Já para o arquivo de destino os atributos de *mactimes* são criados como na primeira etapa. Como pode ser observado na figura 06 os três atributos: *mtime*, *atime* e *ctime* foram criados e associados ao arquivo denominado *arq2*, desta forma para a cópia de arquivo no destino do arquivo são criados os três atributos básicos: *mtime*, *atime* e *ctime*.

Quinta etapa: Mudança de owner de root para marcelo

```
Nov 17 08 18:58:38       23 ..c -rwxrwxrwx marcelo  marcelo  /root/psi5007/arq2
```

Figura 07 – MACTimes na mudança de owner

Na mudança de *owner* do arquivo simulado, foi observado que somente o atributo de *ctime* é modificado, pois associasse ao atributo de criação e o mesmo fornece o último momento que ocorreram modificações no conteúdo e meta-informação de um arquivo, conforme ilustrado na figura 07.

Sexta etapa: Mudança de permissão 642 para 777

```
Nov 17 08 18:57:11      23 ..c -rwxrwxrwx root     root     /root/psi5007/arq2
```

Figura 08 – MACTimes na mudança de permissão

Da mesma forma que na mudança de *owner* do arquivo simulado na quinta etapa a mudança de permissão independente da permissão a ser mudada: 644, 777, 642 ou qualquer outra combinação de permissão foi observado que somente o atributo de *ctime* é modificado, conforme ilustrado na figura 08, pois também associasse ao atributo de criação e o mesmo fornece o último momento que ocorreram modificações no conteúdo e meta-informação de um arquivo.

Sétima etapa: *Move* de arquivo. Realizado o comando: mv arq2 arq3

```
Nov 19 08 01:15:40      23 ..c -rwxrwxrwx marcelo  marcelo  /root/psi5007/arq3
```

Figura 09 – MACTimes na mudança de arquivo

Foi observado que na execução do comando *mv* os atributos do arquivo de origem, denominado *arq2* não ocorreram mudanças de atributos, permanecendo de forma intacta. Já para o arquivo de destino o mesmo foi criado e o atributo de *ctime* foi o único que ocorreu modificação, diferentemente da operação de criação de arquivo onde os atributos *mtime*, *atime* e *ctime* foram criados. Na operação de move somente o atributo de ctime foi criado, conforme ilustrado na figura 09.

Oitava etapa: Backup de arquivo. Realizado o comando: *tar cvf backup arq2* e posteriormente *tar tvf backup* para visualização do arquivo.

```
Nov 19 08 00:57:07    10240 m.c -rw-r--r-- root     root     /root/psi5007/backup
                         23 .a. -rwxrwxrwx marcelo  marcelo  /root/psi5007/arq2
Nov 19 08 00:57:24    10240 .a. -rw-r--r-- root     root     /root/psi5007/backup
```

Figura 10 – MACTimes no backup do arquivo

Para a operação de backup foi utilizado o utilitário largamente usado, cujo nome é *tar*. Foi feito o backup de um arquivo texto e em seguida a visualização do backup. O arquivo de backup criado teve os atributos de *mtime* e *ctime* criados mostrando indícios que ocorreram mudanças no conteúdo do arquivo, ou se-

ja, a adição do arquivo *arq2*. Já para o comando de visualização do backup (*tar –tvf*) somente o atributo de *atime* foi atualizado demonstrando que logo após o backup teve uma operação de acesso ao arquivo, observa-se na figura 10 as mudanças.

Conclusão

Os MACtimes fornecem informações interessantes sobre um sistema comprometido. Deve-se entender, que, são fontes importantes em um processo de análise. A base para uma análise segura é a intervenção humana feita de modo correto. Sendo assim ao realizar cópias de arquivos para posterior analise forense é necessário ter certeza que os tempos de último acesso aos arquivos não foram sobrepostos pela cópia perdendo desta forma as informações anteriores, ou seja, o atributo *ctime* pode ser sobreposto de forma errada atrapalhando desta forma a investigação como um todo. Outro ponto também de atenção ao realizar uma investigação em sistemas é necessário verificar a possibilidade de desativar *atimes* para evitar que as informações de *atimes* sejam destruidas no caso de não ser possível montar um disco de leitura. A correta interpretação da linha do tempo é muito importante e para isto é necessário que a data/hora do sistema investigado esteja confiável para que não possam ser interpretadas informações de forma equivocada.

Para cada operação estudada os atributos de *MACtimes* são alteradas conforme as características descritas nos resultados esperados, porém a sua análise deve ser considerada como um todo, ou seja, desde a sua concepção até o momento final. As ferramentas estudadas mostraram ser capazes de construir uma linha do tempo demonstrando ser útil para percebemos que eventos isolados podem ter ação e reconstruir um fato ocorrido, porém é importante não só a linha do tempo como a correta interpretação das mais variadas operações executadas no sistema operacional.

Referências

[1] Farmer, Dan., Venema, Wietse., “Perícia Forense computacional – teoria e prática aplicada”, Pearson Prentice Hall, 2006.

[2] Eckstein, Knut., “Forensic for Advanced UNIX File System”, IEEE/USMA IA Workshop, 2004.

[3] C. Weil, Michael., “Dynamic Time & Date Stamp Analysis”, International Journal of Digital Evidence, 2002.

[4] Cardoso Guimarães, Célio., de Souza Oliveira, Flávio., Abdalla dos Reis, Marcelo., Lício de Geus, Paulo., “Forense Computacional: Aspectos Legais e Padronização”, Instituto de Computação – Unicamp.

[5] Pellegrini, Jerônimo., Ferreira Bertachhi, João Eduardo., Rechi Vita, João Paulo., “Forense Computacional” 2005.

[6] Carrier, Brian. The Sleuth Kit, 2004; http://www.sleuthkit.org

[7] Abdalla dos Reis, Marcelo.,Lício de Geus, Paulo., “Análise Forense de Intrusões em Sistemas Computacionais: Técnicas, Procedimentos e Ferramentas” , Instituto de Computação – Unicamp.

[8] Rodrigues de Freitas, Andrey., “Perícia Forense Aplicada à Informática”, Brasport, 2006.

[9] Böhm Argolo, Frederico Henrique., Análise Forense em sistemas GNU/Linux, 2005