UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

ESTUDO DE RÓTULOS DE TEMPO EM SISTEMAS NTFS BASEADO EM ESTRUTURAS DO SISTEMA DE ARQUIVOS E DO SISTEMA OPERACIONAL WINDOWS

CLEBER SCORALICK JÚNIOR

ORIENTADOR: ANDERSON CLAYTON ALVES NASCIMENTO

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA
ÁREA DE CONCENTRAÇÃO INFORMÁTICA FORENSE E SEGURANÇA DA INFORMAÇÃO

PUBLICAÇÃO: PPGENE.DM-093/12

BRASÍLIA/DF: 01/2012.

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

ESTUDO DE RÓTULOS DE TEMPO EM SISTEMAS NTFS BASEADO EM ESTRUTURAS DO SISTEMA DE ARQUIVOS E DO SISTEMA OPERACIONAL WINDOWS

CLEBER SCORALICK JÚNIOR

DISSERTAÇÃO DE MESTRADO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE PROFISSIONAL EM INFORMÁTICA FORENSE E SEGURANÇA DA INFORMAÇÃO.

APROVADA POR:

ANDERSON CLAYTON A. NASCIMENTO, PhD. UNIVERSITY OF TOKYO
(ORIENTADOR)

FLAVIO ELIAS DE DEUS, Dr. UnB
(EXAMINADOR INTERNO)

GEORGES DANIEL ANVAME NZE, Dr. UnB
(EXAMINADOR EXTERNO)

BRASÍLIA/DF, 31 DE JANEIRO DE 2012.

FICHA CATALOGRÁFICA

SCORALICK JÚNIOR, CLEBER

Estudo de rótulos de tempo em sistemas NTFS baseado em estruturas do sistema de arquivos e do sistema operacional Windows [Distrito Federal] 2012.

xvi, 89p., 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2012).

Dissertação de Mestrado - Universidade de Brasília, Faculdade de Tecnologia.

Departamento de Engenharia Elétrica.

1. rótulos de tempo
2. sistemas de arquivos
3. computação forense
4. NTFS

I. ENE/FT/UnB
II. Título (Série)

REFERÊNCIA BIBLIOGRÁFICA

SCORALICK JÚNIOR, C. (2012). Estudo de rótulos de tempo em sistemas NTFS baseado em estruturas do sistema de arquivos e do sistema operacional Windows. Dissertação de Mestrado, Publicação PPGENE.DM-093/12, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 89p.

CESSÃO DE DIREITOS

NOME DO AUTOR: Cleber Scoralick Júnior.

TÍTULO DA DISSERTAÇÃO: Estudo de rótulos de tempo em sistemas NTFS baseado em estruturas do sistema de arquivos e do sistema operacional Windows.

GRAU / ANO: Mestre / 2012

Cleber Scoralick Júnior

Instituto de Criminalística - PCDF - SAISO, Bloco C

CEP:70610-200 - Brasília - DF - Brasil.

Dedico este trabalho aos meus pais,
Cleber e Beatriz, por acreditarem que
o melhor presente que poderiam me dar
seria uma educação de qualidade.
Este trabalho é um resultado desse esforço.

À minha irmã, Ana Luiza, pelo carinho,
amizade e exemplo de perseverança
em buscar nossos objetivos.

À minha querida esposa, Raquel,
por me incentivar a iniciar este trabalho e
por estar sempre pronta a me apoiar.
Seu amor, carinho e companhia
foram essenciais nessa caminhada.
Esta vitória também é sua.

AGRADECIMENTOS

Agradeço ao amigo Angelo Shimabuko, pelo exemplo de profissional, pelos inúmeros conhecimentos transmitidos e contribuições valiosas para este trabalho.

Ao amigo Rafael Farnese, pelo companheirismo, pela amizade, pelo exemplo de dedicação à profissão e por contribuir diariamente para meu aperfeiçoamento.

Aos orientadores Lucas Ferreira e Prof. Anderson Nascimento, pelo direcionamento e contribuição na elaboração desse trabalho.

Aos colegas do Instituto de Criminalística, pelo excelente convívio diário e amizade, em especial aos companheiros da Seção de Perícias de Informática, pelos conhecimentos transmitidos, e à Seção de Delitos de Trânsito, por onde iniciei minha carreira pericial.

Agradeço à direção do Instituto de Criminalística, em especial ao Wagner Santos, por ajustar minha escala de plantão de forma a viabilizar meus estudos, à Ivete Shimabuko, pelo incentivo e apoio na minha carreira na área de informática forense, e ao Mauro Yared e Celso Nenevê, por acreditarem neste projeto e o apoiarem.

Agradeço aos colegas do programa de mestrado em informática forense pelo convívio agradável, pelas experiências e conhecimentos compartilhados.

A todos, que direta ou indiretamente fizeram parte deste trabalho, os meus sinceros agradecimentos.

Agradeço também ao Departamento Polícia Federal - DPF, ao Instituto de Criminalística da Polícia Civil do Distrito Federal e aos gestores do Programa Nacional de Segurança Pública com Cidadania - PRONASCI, do Ministério da Justiça, por investirem em seus profissionais e acreditarem no potencial deles.

RESUMO

ESTUDO DE RÓTULOS DE TEMPO EM SISTEMAS NTFS BASEADO EM ESTRUTURAS DO SISTEMA DE ARQUIVOS E DO SISTEMA OPERACIONAL WINDOWS

Autor: Cleber Scoralick Júnior

Orientador: Anderson Clayton Alves Nascimento

Programa de Pós-graduação em Engenharia Elétrica

Brasília, 31 de janeiro de 2012

Metadados de arquivos e pastas em sistemas de arquivos armazenam informações relevantes para a análise pericial, com destaque para os rótulos de tempo. No entanto, esses rótulos podem ser afetados por configurações erradas do relógio, problemas de alimentação elétrica ou alterações intencionais dos rótulos de tempo ou do relógio do sistema, exigindo do examinador maior cuidado em sua análise. Dessa forma, este trabalho tem como objetivo determinar procedimentos periciais de informática em sistemas de arquivos NTFS (*New Techonologies File System*), na plataforma Windows XP, que permitam afirmar acerca do grau de confiabilidade dos rótulos de tempo, indicar a quais operações os arquivos e pastas de interesse foram submetidos, bem como elaborar uma linha de tempo. Em uma máquina virtual Windows XP, foram realizadas simulações de operações com arquivos e pastas e um estudo de seus efeitos nos rótulos de tempo. Além das simulações de operações comuns, foram testadas alterações intencionais nos rótulos de tempo e no relógio do sistema, o efeito de varreduras do Windows Media Player e de programas antivírus, além de transferências de arquivos e pastas de um sistema FAT (*File Allocation Table*) para o sistema NTFS. Investigou-se também como a geração de pontos de restauração pelo Windows pode contribuir para a análise temporal. Para exposição dos resultados dos experimentos, foram elaboradas tabelas que apresentam relações cronológicas entre os rótulos de tempo dos atributos analisados, relações de igualdade e desigualdade entre rótulos de atributos diferentes e características dos rótulos de tempo para cada operação analisada. Esses resultados permitem, na maioria dos casos, individualizar as operações. Os programas para manipulação dos rótulos de tempo avaliados mostraram-se ineficazes, pois não impediram que, no exame pericial, tanto a alteração quanto o instante em que ocorreram fossem detectados. Constatou-se também que é possível detectar arquivos alterados com o relógio do sistema manipulado, sendo necessário avaliar o campo LSN (*$LogFile Sequence Number*) dos arquivos de interesse e os que apresentam valores próximos, juntamente com seus rótulos de tempo. A análise do Registro ativo e de suas cópias armazenadas nos pontos de restauração mostrou-se importante para determinar configurações relevantes para a análise temporal. Finalmente, os resultados obtidos foram aplicados em um caso real, permitindo a afirmação da autenticidade dos arquivos questionados e a elaboração de suas linhas de tempo.

ABSTRACT

NTFS FILE SYSTEM TIMESTAMP STUDY BASED ON FILE SYSTEM AND WINDOWS OPERATING SYSTEM STRUCTURES

Author: Cleber Scoralick Júnior

Supervisor: Anderson Clayton Alves Nascimento

Programa de Pós-graduação em Engenharia Elétrica

Brasília, 31st January 2012

Timestamps within file system metadata hold important forensic information. However, their analysis is not straightforward, as they can be unwittingly tampered as a result of the computer clock being incorrect, low clock battery or time zone/day-light saving time misconfiguration. They can also be deliberately manipulated with direct tampering of timestamps or of the computer clock. This study intends to determine digital forensic procedures for NTFS (New Techonologies File System) file systems on Windows XP. These procedures would allow investigators to assess the reliability of timestamps and determine the operations to which files and folders were submitted to and generate their timeline. The most common operations on files and folders were performed on a Windows XP virtual machine and their effects on NTFS timestamps were evaluated. Direct timestamp and computer clock tampering, scans by Windows Media Player and antivirus programs and FAT (File Allocation Table) to NTFS file transfers were also evaluated. Files generated by restore point were also forensically investigated. As a result, we developed tables containing chronological relationships between timestamps, comparisons of timestamps between attributes and timestamp characteristics of some operations, allowing distinguishing among most of the analyzed operations. Several timestamp manipulation programs were tested and proved to be ineffective because a forensic analysis is capable to identify the manipulation and also to find out its time of occurrence. Computer clock tampering can also be detected by evaluating the LSN ($LogFile Sequence Number) and timestamps of the files under investigation and also of the ones with close LSN values. The operating system Registry and its backup copies stored on restore points should be examined to determine system configurations at the time of analysis. The results from this study were applied to a real case and allowed the determination of the authenticity of files and supported the creation of their timeline.

Sumário

Lista de Tabelas

Lista de Figuras

LISTA DE SÍMBOLOS, NOMENCLATURA E ABREVIAÇÕES

BIOS: Basic Input Output System

DNS: Domain Name System

DOS: Disk Operating System

FAT: File Allocation Table

GUID: Globally Unique Identifier

IP: Internet Protocol

IRQ: Interrupt Request Line

LSN: $LogFile Sequence Number

MFT: Master File Table

NTFS: New Techonologies File System

NTP: Network Time Protocol

POSIX: Portable Operating System Interface for Unix

RTC: Real Time Clock

SNTP: Simple Network Time Protocol

TSK: The Sleuth Kit

UTC: Coordinated Universal Time

UTF: Unicode Transformation Format

1 INTRODUÇÃO

Em exames periciais de informática, muitas vezes a determinação das informações temporais de um arquivo são tão ou mais importantes que a extração de seu conteúdo. No entanto, devido aos rótulos de tempo serem dependentes de diversos fatores, como o sistema de arquivos utilizado, o sistema operacional em execução e suas configurações, geralmente a determinação das informações temporais não é direta. Isso ocorre porque sua exatidão pode ser afetada por fatores não intencionais, como imprecisão do relógio do computador, carga baixa da bateria que alimenta esse relógio e configurações erradas de fuso horário e de horário de verão, ou por fatores intencionais, como manipulação desses metadados ou do relógio do sistema por um usuário mal intencionado visando alterar rótulos de tempo de arquivos para incluí-los ou excluí-los do intervalo de tempo sob investigação.

É importante, portanto, determinar procedimentos para exames pericias de informática que possibilitem ao perito criminal afirmar com determinado grau de certeza a confiabilidade dos rótulos de tempo analisados. Dessa forma, seria factível descartar ou corroborar a possibilidade de alteração intencional de metadados ou mesmo da inserção de arquivos no sistema, em especial naqueles exames em que as informações temporais relativas à criação, modificação ou acesso de determinado arquivo são essenciais. Essas informações trariam maior robustez às conclusões apresentadas nos laudos periciais. Outro resultado esperado deste estudo é a possibilidade de elaboração de uma linha de tempo dos arquivos e pastas examinados, a qual indicaria as operações realizadas sobre eles em um determinado espaço de tempo, como por exemplo, a forma como foram inseridos no sistema de arquivos, a ocorrência de cópias, movimentações, alterações de conteúdo.

O sistema de arquivos NTFS (*New Technologies File System*) é o sistema de arquivos padrão da família Windows NT, que inclui o Windows 2000, o Windows XP e seus sucessores (CARRIER, 2005). Por sua vez, os sistemas Windows representam de 78% (W3COUNTER, 2004-2012) a 92% (NETMARKETSHARE, 2006-2012) dos sistemas operacionais que acessam a Internet[1]. Logo, a determinação de procedimentos relati-

[1]Essas estatísticas referem-se a números absolutos coletados de amostras diferentes - o W3Counter considera dispositivos móveis, enquanto que o Netmarketshare contabiliza somente computadores - sendo citadas por serem um indicativo da distribuição dos sistemas operacionais mundialmente.

vos às informações temporais para esse sistema de arquivos seria a que traria maior benefício para a perícia de informática.

Tendo em vista a diferença de comportamento na alteração dos rótulos de tempo para os diversos sistemas operacionais Windows, foi necessário escolher um sistema para realização dos experimentos. Segundo Netmarketshare (2006-2012), o Windows XP é o sistema mais utilizado atualmente, representando 47,2% das máquinas que acessam a Internet, enquanto que o segundo sistema mais usado, o Windows 7, representa 36,4%. A tendência é que ocorra uma inversão entre esses dois sistemas, fato esse indicado pelas dados de 2011 (NETMARKETSHARE, 2006-2012), em que o Windows XP apresenta redução gradual, possuindo 56,8% em março de 2011 e 47,2% em janeiro de 2012, enquanto que o Windows 7 apresentava 25,2% e atualmente possui 36,4%, e pelos dados de W3Counter (2004-2012), que indica que em janeiro de 2012 o Windows 7 possui 38,5% do mercado enquanto que o Windows XP apresenta 30,5%. Mesmo diante dessa tendência de inversão para 2012, o Windows XP ainda possui uma fatia importante do mercado e, se analisarmos um horizonte de dois anos para trás, o Windows XP possuía uma liderança isolada, representando, em fevereiro de 2010, 66,7% do mercado, enquanto que o segundo colocado, o Windows Vista, representava somente 16,8%. Considerando os dados apresentados e o fato de a análise temporal ser muito utilizada em respostas a quesitos, que normalmente são feitos dois anos após a emissão do laudo, optou-se por realizar os experimentos, neste trabalho, com o Windows XP, e expandi-los para outros sistemas operacionais em trabalhos futuros.

1.1 Objetivo

Este trabalho tem por objetivo a determinação de procedimentos a serem adotados em exames periciais de informática em sistemas de arquivos NTFS, na plataforma Windows XP, que permitam a afirmação acerca da confiabilidade dos rótulos de tempo dos arquivos e pastas analisados e das operações a que esses arquivos e pastas foram submetidos, bem como a elaboração de uma linha de tempo provável.

1.2 Hipótese e Justificativa

Acredita-se que é possível realizar afirmações objetivas em relação aos rótulos de tempo de arquivos e pastas armazenados em sistema NTFS, na plataforma Windows XP, além de elaborar uma linha de tempo dos arquivos de interesse, analisando-se estruturas do sistema de arquivos e do sistema operacional Windows.

Os rótulos de tempo de arquivos e pastas, analisados individualmente e em conjunto com os rótulos de outros arquivos, podem fornecer elementos que aumentem ou diminuam o grau de confiabilidade desses rótulos de tempo, bem como propiciar a determinação das operações realizadas sobre arquivos e pastas de interesse e a consequente elaboração de uma linha de tempo. Como exemplo de informações a serem verificadas estão os conteúdos das entradas da MFT[2] (*Master File Table*) referentes aos arquivos e pastas de interesse e de arquivos de sistema, as entradas de diretório correspondentes, dentre outros.

Estruturas do sistema operacional como o Registro e pontos de restauração, podem fornecer, também, dados importantes para a análise temporal, como lista de dispositivos móveis utilizados, configurações de fuso horário e horário de verão, configurações de sincronização do relógio do sistema, informações de modificação em arquivos que possuam extensões monitoradas, dentre outros.

1.3 Metodologia

A metodologia adotada neste trabalho será a simulação, em um sistema operacional Windows XP, de operações comuns de usuários na manipulação de arquivos e pastas, como copiar, mover, renomear, criar, dentre outros, além da simulação de alterações intencionais de rótulos de tempo e do relógio do sistema. A análise das alterações na estrutura do sistema de arquivos e dos mecanismos de monitoramento do sistema operacional, relativas a essas operações, servirá de base para a definição dos procedimentos periciais, permitindo a avaliação da confiabilidade dos rótulos de tempo armazenados nas mídias examinadas, a determinação da natureza das operações realizadas sobre esses arquivos e a elaboração da uma linha de tempo.

Os procedimentos elaborados serão então utilizados em um caso real para verificar a eficácia do método adotado em responder questionamentos sobre a integridade das informações armazenadas em mídia digital.

1.4 Trabalhos correlatos

O comportamento de rótulos de tempo em um sistema NTFS foi investigado inicialmente por Chow et al. (2007), que apresentaram regras gerais baseadas em alguns dos rótulos de tempo existentes. Posteriormente, Bang et al. (2009) e Bang, Yoo e Lee

[2]Estrutura do sistema de arquivo NTFS que possui pelo menos uma entrada por arquivo onde são armazenados os metadados e lista dos blocos de dados.

(2011) realizaram um estudo mais detalhado, avaliando mais rótulos de tempo e um número maior de operações. Este trabalho busca expandir esses estudos, realizando uma análise mais aprofundada do comportamento dos rótulos de tempo de arquivos e pastas, e complementá-los, avaliando outras estruturas do sistema de arquivos e do sistema operacional, bem como investingando alterações intencionais nos rótulos de tempo e no relógio do sistema, visando, dessa forma, obter resultados mais completos e abrangentes.

1.5 Resultados esperados

Com a realização deste trabalho, espera-se que seja possível a definição de procedimentos que permitam ao perito criminal afirmar acerca da confiabilidade dos rótulos de tempo presentes nos metadados de arquivos e pastas armazenados no sistema de arquivos NTFS com sistema operacional Windows XP, determinar quais operações foram realizadas sobre essas estruturas e, consequentemente, elaborar uma linha de tempo das ações executadas. Essas informações darão maior robustez aos laudos periciais, permitindo inclusive responder objetivamente quesitos que possam surgir durante o processo judicial.

1.6 Descrição dos Capítulos

No capítulo 2 são apresentados conceitos e trabalhos relevantes nos tópicos de sistema de arquivos NTFS e FAT (*File Allocation Table*), relógio do sistema e suas formas de sincronização, chaves relevantes do Registro do Windows e pontos de restauração do sistema. No capítulo 3 é detalhada a metodologia adotada nos testes realizados, juntamente com a apresentação das ferramentas desenvolvidas para auxiliá-los. Na sequência, no capítulo 4, detalham-se os resultados obtidos nos testes e apresentam-se tabelas com a compilação desses resultados. No capítulo 5 os resultados obtidos são discutidos e no capítulo 6 é apresentado um estudo de caso, baseado em um caso real, o qual foi solucionado aplicando-se os resultados deste trabalho. Finalmente, no capítulo 7 é realizada a conclusão do trabalho e são sugeridos trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo serão apresentados conceitos referentes ao relógio do computador, as chaves de interesse do Registro do Windows e o mecanismo de criação de pontos de restauração. Serão detalhados, também, conceitos dos sistemas de arquivos NTFS e FAT. Esses conceitos são importantes para a compreensão dos trabalhos correlados, apresentados nesse capítulo, e dos experimentos e resultados deste trabalho.

2.1 Relógio da BIOS

O relógio da BIOS (*Basic Input Output System*), também chamado de RTC (*Real Time Clock*), é utilizado para contar o tempo enquanto o computador está desligado, sendo alimentado, portanto, por uma bateria. O RTC pode, utilizando o IRQ8 (*Interrupt Request Line*), informar o tempo atual ao sistema operacional periodicamente. Além do RTC, há também um contador (*timer*) programável que informa ao sistema operacional que um determinado intervalo de tempo decorreu, via IRQ0. Em sistemas mais recentes (*hardware* e sistema operacional), usa-se um mecanismo assíncrono para controle do tempo, no qual o sistema operacional lê o valor armazenado em um contador quando lhe for mais conveniente, em vez de ser interrompido periodicamente. Em sistemas UNIX e Windows 2000 e superiores, o tempo informado pelo RTC é utilizado como tempo inicial no processo de inicialização (*boot*). Deve-se atentar para a forma com a qual o RTC é utilizado pelos sistemas operacionais, visto que nos sistemas Windows, o RTC é interpretado como o tempo local, enquanto que em sistemas Linux, ele pode ser interpretado como tempo local ou como tempo UTC (*Coordinated Universal Time*) (SCHATZ; MOHAY; CLARK, 2006) (BOVET; CESATI, 2006).

Devido ao relógio do sistema basear-se em osciladores de quartzo, que apresentam instabilidade conhecida, apresentando variações devido a temperatura, tensão e barulho, o tempo registrado pelo relógio é impreciso (MILLS, 2003). Aliado a essa imprecisão, há a possibilidade de o sistema estar mal configurado no que se refere a configuração equivocada de fuso horário, horário de verão e do próprio RTC (SCHATZ; MOHAY; CLARK, 2006).Para que se tenha uma fonte de tempo confiável nos computadores, foi desenvolvido o protocolo NTP (*Network Time Protocol*), possibilitando a computado-

res que utilizam a plataforma UNIX apresentarem sincronismo de nanosegundos com servidores de tempo confiáveis.

Em sistemas Windows 2000 e posteriores foi incluído uma versão simplificada do NTP, chamada de SNTP (*Simple Network Time Protocol*), não apresentando a precisão do protocolo original. Em sistemas Windows XP o protocolo SNTP é habilitado por padrão, sendo configurado para acessar o servidor de tempo uma vez por semana. No entanto, quando inserido em um domínio, a máquina é configurada para realizar a sincronização com o controlador do dominio (SCHATZ; MOHAY; CLARK, 2006). Schatz, Mohay e Clark (2006) apresentam um estudo no qual um controlador de domínio Windows é configurado para não realizar sincronização com um servidor de tempo externo enquanto que as máquinas Windows dentro do domínio são configuradas para sincronizar com esse controlador. Foi constatado que tanto o controlador quanto as demais máquinas do domínio apresentaram um desvio crescente e constante em relação ao tempo real, sendo que em aproximadamente dois meses e meio foi medido um aumento de 2 segundos no desvio em relação ao tempo real.

2.2 Registro do Windows

O Registro do Windows é um banco de dados hierárquico que armazena configurações do sistema operacional como um todo e de preferências de usuários, desempenhando um papel primordial no funcionamento de um sistema Windows. Ele é organizado em chaves e valores, sendo que as chaves, que contém subchaves e valores, são semelhantes a pastas, enquanto que os valores, que armazenam os dados, são semelhantes a arquivos. O Registro possui seis chaves principais, que contém as demais, (HKEY_CURRENT_USER, HKEY_USERS, HKEY_CLASSES_ROOT, HKEY_LOCAL_MACHINE, HKEY_PERFORMANCE_DATA e HKEY_CURRENT_CONFIG), e que podem ser acessadas, no Windows XP, pelo aplicativo Regedit.exe. Cada uma dessas chaves principais são armazenadas em arquivos de suporte no sistema de arquivos, localizados, no Windows XP, nas pastas %SystemRoot%\System32\Config e %SystemRoot%\Profiles\Username (Microsoft Support, 2008) (RUSSINOVICH; SOLOMON, 2004).

Por centralizar as configurações do sistema operacional o Registro do Windows é uma fonte de informação importante em uma análise forense apresentando dados relativos ao sistema, como configurações e informações de dispositivos, aplicativos e usuários, os quais podem ser correlacionados com dados obtidos no sistema de arquivos (CARVEY,

2005). Diversas chaves do Registro de interesse pericial são citadas na literatura (CARVEY, 2005) (BOYD; FORSTER, 2004) (Microsoft MSDN, 2006) (Microsoft TechNet, 2010) (Microsoft Support, 2011), sendo apresentadas a seguir as chaves de interesse para este trabalho:

- *HKEY_LOCAL_MACHINE\SYSTEM\ControlSet\Enum\USBSTOR*: Essa entrada do Registro armazena o rótulo de tempo referente à ultima vez que um determinado dispositivo removível USB, como *pen drives* e câmeras, foi conectado à máquina. Cada dispositivo conectado ao computador recebe uma entrada referenciada pelo seu número de série ou, caso não possua, pelo seu *instance ID*[3] (CARVEY, 2005).

- *HKEY_LOCAL_MACHINE\SYSTEM\Current ControlSet\Control\TimeZoneInformation\ActiveTimeBias*: Apresenta o deslocamento de fuso horário configurado para o sistema. Um dos valores armazena o número de minutos positivos ou negativos que devem ser adicionados ao tempo UTC e outro armazena o nome do fuso horário utilizado (BOYD; FORSTER, 2004).

- *HKEY_LOCAL_MACHINE\SYSTEM\Current ControlSet\Control\TimeZoneInformation\DaylightBias*: Apresenta o deslocamento relativo ao horário de verão. As chaves *DaylightStart* e *StandardStart*, presentes também no diretório *TimeZoneInformation* apresentam a configuração do início e fim do horário de verão (BOYD; FORSTER, 2004).

- *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate*: Desabilita a atualização do rótulo de tempo de último acesso de arquivos e pastas no sistema NTFS quando apresenta o valor igual a 1. Esta chave influencia diretamente a análise de rótulos de tempo, pois quando a atualização do tempo de acesso está desabilitada o instante de acesso a arquivos e pastas não é mais registrado (Microsoft MSDN, 2006) (Microsoft TechNet, 2005).

- *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\Type*: Indica de qual tipo de fonte externa o sistema irá aceitar sincronização de tempo. As opções são: **NoSync**, não aceita sincronização com fontes externas; **NTP**, sincroniza com os servidores especificados na chave *NtpServer*, mostrada a seguir; **NT5DS**, sincroniza dentro da hierarquia do domínio;

[3] O *instance ID* é uma *string* de identificação gerada pelo sistema que individualiza um dispositivo nesse sistema, sendo preservado durante reinicialiações (http://msdn.microsoft.com/en-us/library/ff541327(v=vs.85).aspx).

AllSync, utiliza todos os meios de sincronização disponíveis. O valor padrão para membros do domínio é *NT5DS* e para servidores e clientes autônomos é *NTP* (Microsoft TechNet, 2010).

- *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpServer\Enabled*: Indica se o servidor NTP está habilitado. O valor padrão dessa chave é 1 para membros de domínio e para servidores e clientes autônomos (Microsoft TechNet, 2010) (Microsoft Support, 2011).

- *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\NtpServer*: Contém uma lista de servidores de tempo na forma de nomes DNS (*Domain Name System*) ou endereços IP (*Internet Protocol*), com os quais a máquina irá realizar a sincronização de tempo. Apresenta também *flags* de configuração do modo de sincronização, dentre elas a *flag SpecialInterval* (0x01), que habilita a chave *SpecialPoolInterval*, mostrada a seguir. Para membros de domínio não há um valor definido para a chave *NtpServer*, enquanto que para servidores e clientes autônomos o valor padrão é *time.windows.com,0x1* (Microsoft TechNet, 2010).

- *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config\MaxPollInterval*: Especifica o valor máximo em log_2 segundos permitido entre solicitações de sincronização com o servidor de tempo. O valor padrão para controladores de domínio é 10, o que equivale a 17 minutos, e para os demais é 15, o que equivale a aproximamente 9 horas (Microsoft TechNet, 2010).

- *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config\MinPollInterval*: Especifica o valor mínimo em log_2 segundos permitido entre solicitações de sincronização com o servidor de tempo. O valor padrão para controladores de domínio é 6, o que equivale a 64 segundos, e para os demais é 10, o que equivale a 17 minutos (Microsoft TechNet, 2010).

- *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpClient\SpecialPollInterval*: Especifica, em segundos, o intervalo de sincronização especial com o servidor de tempo. Este valor é utilizado ao invés dos tempos mínimos e máximos especificados nas duas chaves acima sempre que a *flag SpecialInterval* estiver habilitada na chave *NtpServer*. O valor padrão para membros de domínio é 3600, o que equivale a uma hora, e para servidores e clientes autônomos é de 604800, o que equivale a 7 dias (Microsoft TechNet, 2010) (Microsoft Support, 2011).

- *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config\AnnounceFlags*: *Flags* que indicam se a máquina se anuncia como um servidor de tempo confiável no domínio, podendo ser configurado para anunciar sempre (valor igual a 5), indicado para servidores de domínio, ou de maneira automática (valor igual a 10), indicado para membros do domínio ou máquinas autônomas (Microsoft TechNet, 2010) (Microsoft Support, 2011).

2.3 Pontos de Restauração

Pontos de restauração foram introduzidos a partir do Windows ME com o objetivo de propiciar a restauração de arquvios críticos do sistema operacional e de aplicativos, em diversos instantes de tempo, na eventualidade de serem corrompidos por uma falha do sistema. No Windows XP, a criação de pontos de restauração é habilitada como padrão e é realizada quando da ocorrência dos seguintes eventos (HARMS, 2006):

- Primeira execução do sistema;
- A cada 24 horas de atividade;
- Antes da instalação de programas;
- Antes de atualizações automáticas;
- Antes da restauração de um ponto de restauração;
- Antes que um *driver* não reconhecido seja instalado;
- Antes da restauração de dados pelo aplicativo *Backup tool*;
- Por seleção manual.

Por padrão, o espaço utilizado pelos pontos de restaução é de no máximo 12% do volume para volumes maiores que 4 GiB[4], ficando limitado pela quantidade de espaço livre, visto que é dado prioriade ao sistema e não aos pontos de restauração. Pontos de restauração são apagados em um política FIFO (*first in first out*) quando o espaço

[4]Quando trabalha-se com quantidades baseadas em *bytes*, que é uma potência de 2, o correto é utilizar prefixos binários. Dessa forma, neste trabalho será utilizado o prefixo Gi (gibi), que equivale a $2^{30} = 1024^3$. Quando utilizado com prefixos decimais, o termo *byte* não deve ser abreviado, para que não seja confundido com a unidade bel do sistema internacional.

destinado aos pontos de restauração atige 90% de ocupação ou quando são passados 90 dias da realização do ponto de restauração (HARMS, 2006).

Por serem habilitados por padrão no Windows XP e armazenarem informações úteis em diversos instantes de tempo, os pontos de restauração são uma ferramenta muito importante para a área forense. Em seguida será detalhado o funcionamento dos pontos de restauração e apresentadas algumas de suas aplicações.

No Windows XP há uma pasta na raiz do sistema de arquivos chamada *System Volume Information*. Caso a criação dos pontos de restauração esteja habilitada, dentro dessa pasta haverá outra pasta, chamada *_restore{(System GUID (Globally Unique Identifier))}*, na qual serão armazenados os pontos de restauração. Cada ponto de restauração recebe uma pasta chamada *RP#*, onde # são números sequenciais (HARMS, 2006).

Os pontos de restauração armazenam um cópia integral do Registro do Widows na pasta *snapshot*, localizada dentro de cada pasta *RP#*. Esta cópia é comprimida por uma ferramenta do próprio NTFS. Além do resgistro, algumas extensões de arquivos e pastas também são copiados para a pasta *RP#* caso tenham sido modificados entre o instante de criação do ponto de restauração atual e o anterior. A lista de arquivos e diretórios monitorados é determinada por diretrizes de inclusão e exclusão presentes no arquivo *C:\Windows\system32\Restore\filelist.xml*. Os arquivos copiados para a pasta *RP#* recebem nomes sequenciais, sendo que o seus nomes e caminhos originais são armazenados em arquivos binários com nome *change.log* localizados nesse diretório. Cabe ressaltar que os metadados dos arquivos monitorados não são alterados quando da criação do ponto de restauração, logo os arquivos contidos na pasta *RP#* possuem os mesmos metadados dos arquivos originais (HARMS, 2006).

As configurações de pontos de restauração são definidas no Registro, dentro do caminho *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SystemRestore*, onde podem ser configurados a quantidade de espaço reservado no volume, o tempo de operação contínua entre pontos de restauração, o tempo máximo de armazenamento, dentre outros. Um aspecto importante sobre as configurações é que, quando a criação dos pontos de restauração é desabilitada, os dados dos pontos de restauração armazenados no disco rígido são apagados (HARMS, 2006).

No estudo de caso apresentado por Harms (2006) são utilizados pontos de restauração para obteção de diversas versões de um arquivo de interesse que possuía extensão monitorada. Utilizando-se os rótulos de tempo desses arquivos e a numeração dos pontos de restauração nos quais estavam armazenados, foi possível criar uma linha de tempo de modificação do arquivo, além de obter o seu conteúdo nesses instantes de tempo.

Quando pontos de restauração são utilizados em análise forense, deve-se atentar para o fato de que, quando um evento de interesse é encontrado, pode-se somente afirmar que esse evento ocorreu pelo menos uma vez entre o instante de registro do evento (rótulos de tempo de arquivos ou tempo de modificação de uma entrada do Registro), o qual está armazenado em um ponto de restauração, e o tempo de criação do ponto de resturação anterior. Como o tempo de registro de evento somente marca o instante da última operação, pode ocorrer de o evento ter acontecido mais de uma vez nesse intervalo de tempo. Outra possibilidade é a de um evento ocorrer e ter seus traços removidos em um espaço de tempo entre pontos de restauração. Nesse caso, não será encontrado registro desse evento analisando-se os pontos de restauração (ZHU; JAMES; GLADYSHEV, 2009).

No estudo de caso apresentado por Zhu, James e Gladyshev (2009) é apresentada uma situação na qual, analisando-se cópias do Registro armazenadas em pontos de restauração, foi possível identificar uma conexão remota para outro computador na rede local dentro de um espaço de tempo restrito, possibilitando, dessa forma, identificar quem operava a máquina durante essa conexão não permitida.

2.4 NTFS - *New Techonologies File System*

O sistema de arquivos NTFS foi desenvolvido pela Microsoft para se tornar o sistema padrão para os novos sistemas operacionais da empresa a partir do Windows NT, substituindo o sistema FAT, utilizado anteriormente. Ele foi desenvolvido com o objetivo de ser confiável, seguro e suportar dispositivos de armazenamento grandes (CARRIER, 2005).

Um conceito fundamental do NTFS é que todos os dados armazenados no sistema são alocados em arquivos, inclusive os dados necessário à administração do sistema operacional (arquivos de metadados), podendo ser alocados em qualquer parte do volume. As únicas exceções são os primeiros setores do volume, que são ocupados pelo setor

de *boot* e pelo código de *boot*, necessários para a inicialização do sistema (CARRIER, 2005).

2.4.1 MFT - *Master File Table*

A principal estrutura do NTFS é a MFT, que consiste de uma tabela com informações sobre todos os arquivos e diretórios do sistema de arquivos, inclusive dela mesma, pois, como todas as estruturas do NTFS, a MFT também é um arquivo. A primeira entrada da MFT, chamada de $MFT, corresponde à entrada relativa à própria MFT e possui a informação de quais blocos estão alocados para ela. Para o sistema de arquivos localizar qualquer arquivo é necessário que ele acesse sua entrada MFT correspondente. E para que o sistema de arquivos localize inicialmente a MFT, o endereço do seu primeiro bloco encontra-se no primeiro setor do volume (setor de *boot*), como pode ser visto na figura 2.1 (CARRIER, 2005).

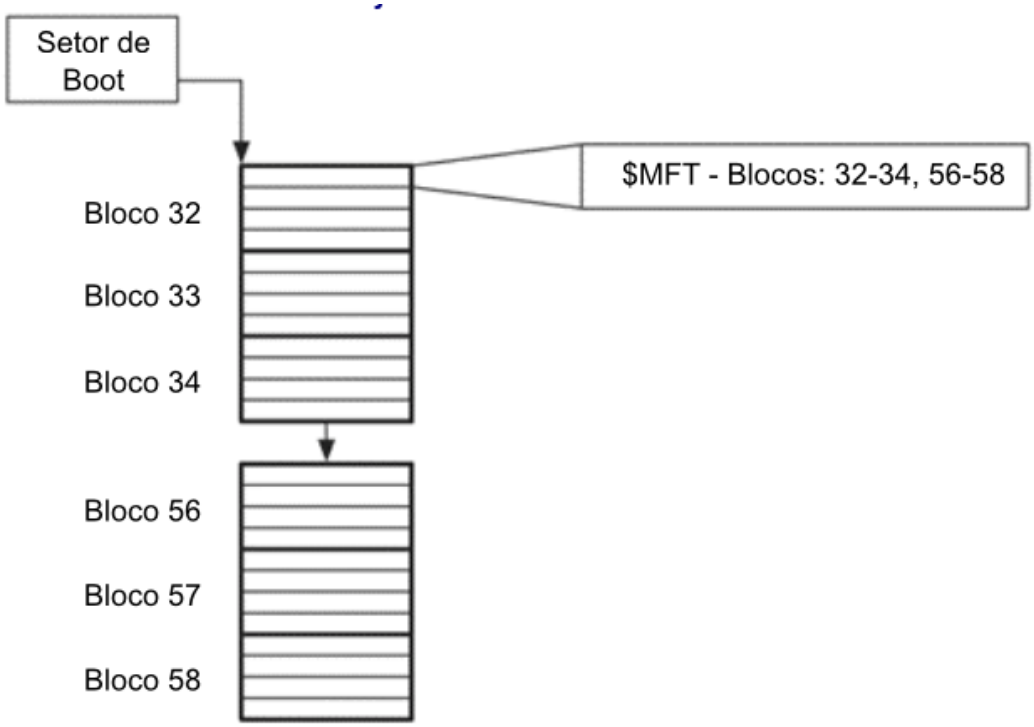


Figura 2.1: Setor de *boot* e estrutra de blocos da MFT (*Adaptado de:* Carrier (2005))

O número de cada entrada MFT é sequencial e é determinado dividindo-se o endereço do início da entrada, relativo ao início do arquivo $MFT, pelo tamanho da entrada. Por exemplo, a entrada com início no byte 12288 do arquivo $MFT corresponde à entrada de número 12 para um tamanho de entrada de 1024 bytes, pois 12288 por 1024 resulta 12. Todas as entradas MFT têm um mesmo tamanho, definido no setor de *boot*, sendo o valor padrão utilizado pela Microsoft de 1024 bytes. São utilizados 48 bits para referenciar o número da entrada MFT, chamado pela Microsoft de *file number*. Dentro

de cada entrada MFT há um contador de 16 bits chamado de número de sequência (*sequence number*) que é incrementado toda vez que a entrada MFT é realocada. Por exemplo, um entrada alocada a um arquivo possui um número de sequência igual a 5. Quando o arquivo é apagado esse número permanece e a entrada é marcada como livre. No momento da realocação dessa entrada para outro arquivo o número de sequência é incrementado para 6. O sistema NFTS, ao se referir a uma entrada MFT, utiliza o número da entrada MFT concatenado com o número de sequência, resultando em um número de 64 bits chamado de *file reference address*. O número de sequência é utilizado juntamente com o número da entrada MFT para facilitar a verificação de integridade da entrada em caso ocorra alguma pane no sistema durante operações de alocações de arquivos (CARRIER, 2005).

Apesar da entrada MFT possuir um tamanho fixo, ela é composta por estruturas de tamanho variável chamadas de atributos. Os atributos se localizam logo após um cabeçalho de tamanho fixo posicionado no início da entrada, conforme pode ser observado na figura 2.2. Existem diversos tipos de atributos que podem compor uma entrada MFT, sendo cada um destinado a um propósito específico como, por exemplo, armazenar rótulos de tempo, nome, blocos alocados ao arquivo, dentre outros. Caso um entrada possua muitos atributos e o tamanho da entrada não seja suficiente para armazená-los são utilizadas mais entradas para o mesmo arquivo ou pasta. Nesse caso, a entrada principal, chamada de entrada base, possuirá um tipo de atributo ($ATTRIBUTE_LIST) que lista todos os atributos do arquivo ou pasta e correlaciona-os com o número da entrada MFT em que estão localizados. As demais entradas, chamadas de não base, possuirão uma referência ao número da entrada base (CARRIER, 2005). Como exemplo temos a figura 2.3 na qual a entrada 5009 é a entrada base, possuindo quatro atributos e mais duas entradas não base, que são referenciadas pelo atributo $ATTRIBUTE_LIST.

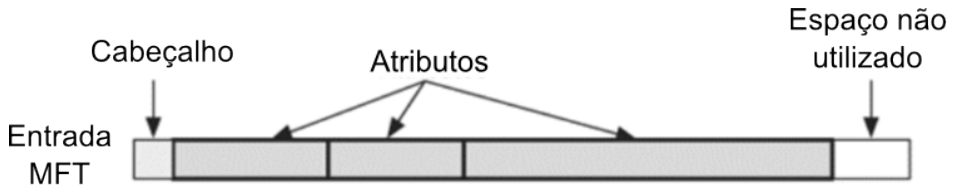


Figura 2.2: Estrutura de uma entrada MFT (*Adaptado de:* Carrier (2005))

2.4.2 Atributos

Cada tipo de atributo possui uma estrutura própria, no entanto, todo atributo possui um cabeçalho padrão. Nesse cabeçalho, temos o tipo do atributo, seu nome, seu

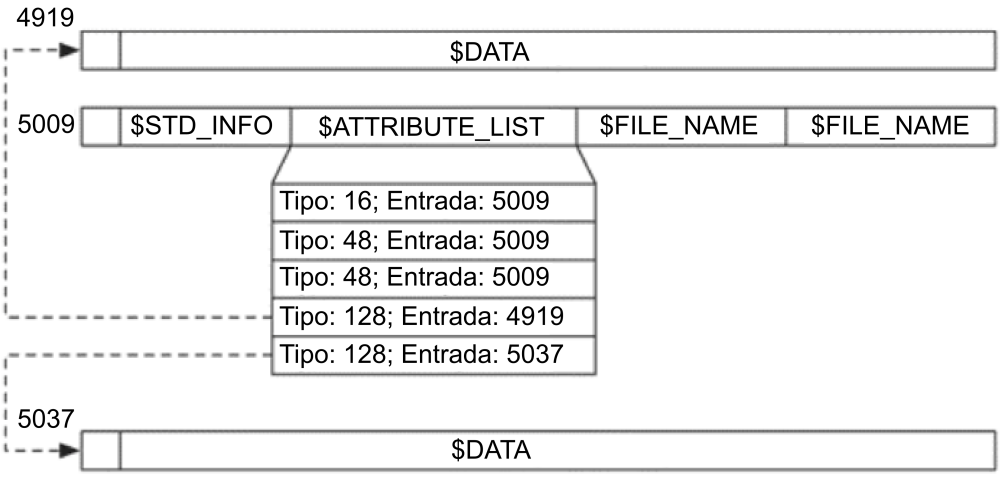


Figura 2.3: Entradas MFT base e não base (*Adaptado de:* Carrier (2005))

tamanho, algumas *flags* e um identificador. Para individualização de cada atributo, visto que uma entrada pode possuir mais de um atributo do mesmo tipo, é utilizada a combinação do número referente ao tipo com um identificador, que é um número único dentro de cada entrada MFT. O sistema possui tipos de atributos padrão, que podem ser redefinidos no arquivo de sistema $AttrDef (CARRIER, 2005).

Como os atributos podem possuir qualquer formato e tamanho, não seria viável que um arquivo que possuísse um atributo grande ocupasse diversas entradas MFT para armazenar seu conteúdo. Para tanto, os atributos são divididos em atributos residentes e não-residentes. Os atributos residentes são atributos pequenos e são armazenados integralmente na própria entrada MFT. Já os não-residentes, armazenam seu conteúdo em blocos do disco alocados para tal fim. Nesse caso, os atributos não residentes armazenam na MFT somente o seu cabeçalho e uma lista que indica em quais blocos o seu conteúdo está armazenado (RUSSINOVICH; SOLOMON, 2004).

A seguir serão listados os principais atributos padrão de interesse:

1. $STANDARD_INFORMATION: Presente em toda entrada MFT, com exceção das não base, possui informações de propriedade, segurança e informações de quota, além de possuir quatro campos destinados aos rótulos de tempo. Os rótulos de tempo se referem ao tempo de criação, tempo de última modificação do conteúdo, tempo de última modificação da entrada MFT e tempo de último acesso. Cada campo é formado por 64 bits e representa a quantidade de centenas de nanosegundos a partir de zero hora do dia primeiro de janeiro de 1601, em UTC (CARRIER, 2005) (Microsoft MSDN, 2011).

2. $FILE_NAME: Assim como o atributo anterior, está presente em toda entrada MFT, com exceção das não base, e possui o nome do arquivo ou diretório, informação de seu tamanho, referência do diretório pai e também quatro campos para os rótulos de tempo. O sistema NTFS admite três formatos para nomes, formato DOS (*Disk Operating System*) 8.3, formato Win 32 e formato POSIX (*Portable Operating System Interface for Unix*) (CARRIER, 2005). O formato padrão, Win 32, é não sensível à caixa, utiliza codificação UTF-16 (*Unicode Transformation Format*) (UNICODE, 2011), admite nomes longos com até 255 caracteres e suporta quase todos os caracteres Unicode[5], com exceção de alguns caracteres especiais como "/", "\", "?", "*", ":"(Microsoft Support, 2007). Quando uma entrada MFT é criada com um nome maior do que o suportado pelo formato DOS 8.3, ou contendo caracteres Unicode, ou com espaços no nome, ou com múltiplos caracteres ".", ou iniciando com esse caractere, é criado automaticamente outro atributo $FILE_NAME com um nome alternativo que atenda ao formato DOS 8.3. A criação desse nome alternativo ocorre para que aplicações MS-DOS e Windows 16 bits possam trabalhar com esses arquivos ou pastas. O sistema NTFS é compatível, também, com nomes no formato POSIX[6], sendo necessário, portanto, um atributo $FILE_NAME para armazenar o nome nesse padrão. Devido às essas características de formatos de nome é comum que uma entrada MFT possua mais de um atributo $FILE_NAME (RUSSINOVICH; SOLOMON, 2004) (Microsoft TechNet, 2005).

3. $DATA: Armazenam o conteúdo do arquivo ou diretório a qual pertencem. Se forem residentes, o conteúdo seguirá logo após o cabeçalho dentro da entrada MFT. Se forem não-residentes possuirão as listas dos blocos alocados para armazenamento. Um arquivo pode possuir mais de um atributo $DATA (CARRIER, 2005).

4. $ATTRIBUTE_LIST: É utilizado quando uma entrada MFT não é suficiente para armazenar todos os cabeçalhos de seus atributos. Nesse caso, esse atributo enumera todos os atributos do arquivo, referenciando em qual entrada MFT ele está localizado (CARRIER, 2005).

5. $BITMAP: Armazena um mapa de bits, em que cada bit indica se o elemento a que se refere está alocado (bit igual a 1) ou não (bit igual a 0). É utilizado

[5]Unicode é um padrão internacional para representação de caracteres de todas as linguagens, podendo ser representado por três codificações diferentes: UTF-8, UTF-16 e UTF-32 (UNICODE, 2011).

[6]POSIX é uma família de padrões para interoperabilidade de sistemas operacionais, dentre os quais há um formato para codificação de nomes (IEEE, 2008).

no arquivo $MFT, para controlar quais entradas MFT encontram-se alocadas e quais estão disponíveis para uso, e em entradas MFT de diretórios com muitos itens, para controlar a alocação das entradas de diretório (detalhado no item 2.4.4) (CARRIER, 2005).

6. $INDEX_ROOT: Utilizado na estrutura de diretórios. Será detalhado no item 2.4.4.

7. $INDEX_ALLOCATION: Utilizado na estrutura de diretórios. Será detalhado no item 2.4.4.

2.4.3 Arquivos de metadados do sistema

Como, no NTFS, todas as estruturas são armazenadas como arquivos, as dezesseis primeiras entradas da MFT são reservadas para arquivos relativos à administração do sistema de arquivos, sendo os principais listados na tabela 2.1 (Microsoft TechNet, 2005):

Tabela 2.1: Principais arquivos de metadados do sistema de arquivos NTFS

Entrada	**Nome**	**Descrição**
0	$MFT	Entrada referente à MFT.
1	$MFTMirr	Contém uma cópia das primeiras entradas da MFT.
2	$LogFile	Contém o diário (*journal*) referente às operações de metadados.
3	$Volume	Contém informações do volume.
4	$AttrDef	Contém informações sobre os atributos do sistema de arquivos.
5	.	É a entrada referente ao diretório raiz do sistema de arquivos.
6	$Bitmap	Contém o mapeamento de alocação dos blocos no volume.
7	$Boot	Contém o setor de *boot* e código de *boot*.
8	$BadClus	Lista os blocos com setores defeituosos.

2.4.4 Estrutura de diretórios

Outro componente importante do sistema de arquinos NTFS é a estrutura de diretórios. O NTFS utiliza índices para organizar atributos em diversas situações. No caso dos diretórios, os índices são utilizados para ordenar atributos $FILE_NAME dos arquivos e diretórios do volume. O NTFS utiliza estrutras de árvore-B (*B-trees*) para ordenar os arquivos e pastas alfabeticamente. Uma árvore é um grupo formado por estruturas de dados chamadas nós que são ligadas em um formato de árvore, na qual há um nó raiz que se ramifica em vários nós. Os nós que não possuem ramificações para baixo, são chamados de folhas. Árvores-B, ao contrário de árvores bínárias, em que cada nó

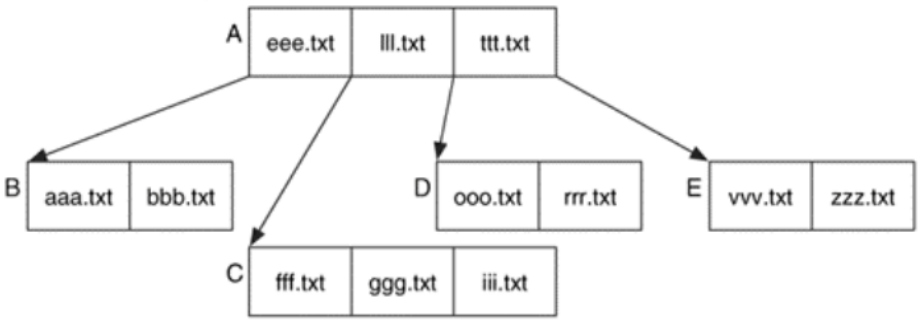


Figura 2.4: Exemplo de árvore-B ordenada alfabeticamente (*Adaptado de:* Carrier (2005))

pode ter no máximo dois filhos, admitem mais de dois filhos por nó. Segue na figura 2.4 um exemplo de árvore-B ordenada alfabeticamente (CARRIER, 2005).

No NTFS, o nó raiz de qualquer volume é a entrada MFT número 5, cujo nome é ".". A partir desse diretório é possível localizar qualquer arquivo dentro desse volume (CARRIER, 2005).

Os índices de diretório de arquivos e pastas são armazenados nas entradas MFT de seus diretórios pais, mais especificamente em dois tipos de atributos, o $INDEX_ROOT e o $INDEX_ALLOCATION. O atributo $INDEX_ROOT é sempre residente e sempre corresponde ao nó raiz do diretório em questão. Por ser residente, o $INDEX_ROOT não pode ocupar muito espaço, logo, quando o diretório possui muitas entradas, é utilizado o atributo $INDEX_ALLOCATION, que é sempre não residente, para armazenar as demais entradas (CARRIER, 2005).

O atributo $INDEX_ROOT é composto por um cabeçalho próprio, por um cabeçalho do nó e por entradas de índice, que são estruturas formados por um cabeçalho seguido do atributo $FILE_NAME, conforme figura 2.5. Já o atributo $INDEX_ALLOCATION é composto por vários registros de índice, equivalentes a nós, possuindo um cabeçalho próprio, um cabeçalho do nó e de entradas de índice, como pode ser visto na figura 2.6. Cada entrada de índice possui, além do atributo $FILE_NAME, *flags* que indicam se a entrada é a última da lista naquele nó e se possui algum filho. Caso tenha filho, a entrada possui um apontador para o nó filho (CARRIER, 2005).

O atributo $FILE_NAME presente nas entradas de índice possuem os mesmos campos existentes no atributo $FILE_NAME presente nas entradas MFT (CARRIER, 2005).

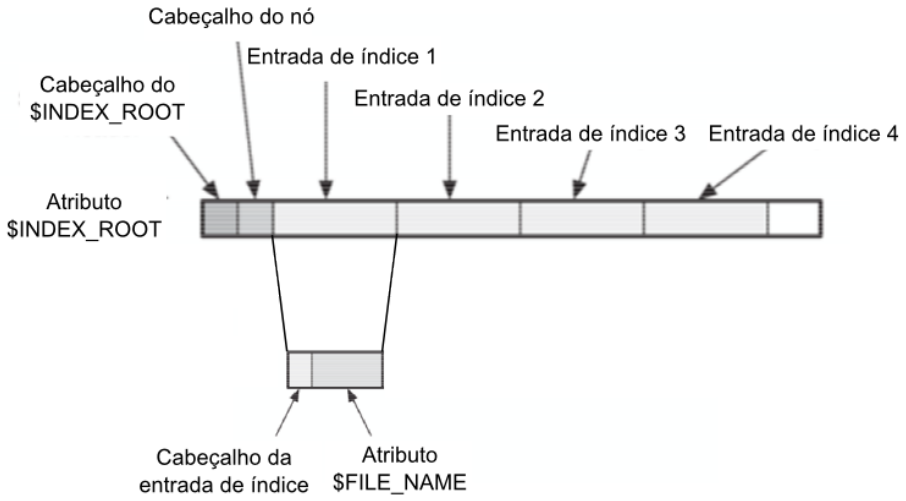


Figura 2.5: Estrutura do atributo $INDEX_ROOT (*Adaptado de:* Carrier (2005))

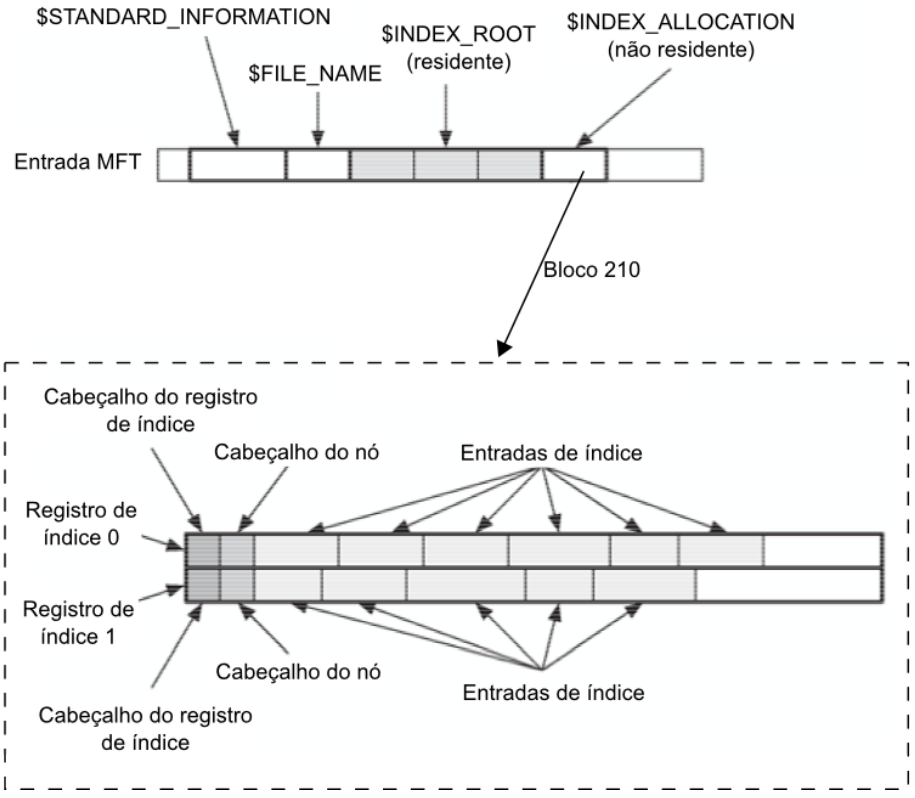


Figura 2.6: Estrutura do atributo $INDEX_ALLOCATION (*Adaptado de:* Carrier (2005))

2.4.5 Características de interesse para análise temporal

Após a apresentação das estruturas principais do sistema NTFS, serão detalhadas, nesta seção, características de alocação e estruturas do sistema que possuem relevância para a análise temporal.

2.4.5.1 Características de alocação

O Windows XP aloca o arquivo $Boot nos primeiros blocos do volume, os arquivos $LogFile, $AttrDef, $MFT e $Secure a um terço do início do volume e os arquivos $MFTMirr, $Root e $Bitmap na metade do volume. Normalmente, os rótulos de tempo nesses arquivos de metadados correspondem ao instante em que o sistema de arquivos foi criado (CARRIER, 2005).

No NTFS, a MFT é criada com o menor tamanho possível, sendo expandida de acordo com a necessidade do sistema. Para que não ocorra uma fragmentação da MFT em um curto espaço de tempo, o Windows reserva um espaço contíguo de aproximadamente 12,5% do sistema de arquivos para a MFT, espaço esse que permanece não alocado para conteúdo de arquivos ou diretórios até que o volume esteja cheio (CARRIER, 2005).

A MFT é alocada de acordo com uma política de primeira entrada disponível, a partir da entrada número 24, já que as anteriores são reservadas pelo sistema. Quando uma entrada em uso deixa de estar alocada, o seu conteúdo permanece inalterado, sendo somente alterado um flag em seu cabeçalho e um bit no atributo $Bitmap da MFT. Já no momento da alocação de uma entrada, o seu conteúdo é apagado antes dos novos dados serem escritos. Devido a essa política de alocação, normalmente as entradas da MFT mais próximas do início são mais reutilizadas e as mais distantes menos. Dessa forma, é mais provável que entradas marcadas como não alocadas, mas que possuam dados da entrada prévia, sejam encontradas mais distantes do início da MFT (CARRIER, 2005).

Diferentemente da alocação de entradas MFT, a alocação de blocos no Windows XP, segue o algoritmo *best fit*. Segundo esse algoritmo, quando é necessário alocar um arquivo que possui um determinado número de blocos, procura-se nos blocos não alocados um intervalo contíguo de blocos livres com tamanho igual ou ligeiramente maior que o necessário, visando, dessa forma, deixar o menor espaço não ocupado entre o novo arquivo e o próximo bloco alocado (CARRIER, 2005).

2.4.5.2 Estruturas de interesse

No NFTS, encontramos rótulos de tempo em diversas estruturas do sistema de arquivos. Para um mesmo arquivo ou diretório, temos rótulos de tempo no atributo $STANDARD_INFORMATION e nos atributos $FILE_NAME presentes tanto na própria en-

trada MFT quanto no índice de seu diretório pai. Há também um campo relevante para análise temporal, chamado de LSN (*$LogFile Sequence Number*), presente nos cabeçalhos das entradas MFT. Esse campo, que possui 64 bits e é único para todo o sistema de arquivos, refere-se ao último registro daquela entrada MFT no *journal*. O LSN é sempre crescente e é atribuído a cada entrada MFT sempre que essa passar por alguma alteração. Dessa forma, o LSN pode ser utilizado para determinação da ordem em que dois arquivos foram alterados (CARRIER, 2005) (RUSSINOVICH; SOLOMON, 2004).

2.5 FAT - *File Allocation Table*

O sistema de arquivos FAT foi utilizado como padrão nos sistemas operacionais Microsoft DOS e Windows 9x. Por ser um sistema muito simples e reconhecido em diversas plataformas, é muito utilizado atualmente em mídias removíveis, como pen drives e cartões de memória de câmeras e celulares. Ele possui duas estruturas principais, a FAT e as entradas de diretório. A FAT é uma tabela onde cada célula corresponde a um *cluster* (conjunto de setores consecutivos) e é utilizada como um lista encadeada para localização os *clusters* alocados a cada arquivos e pasta. Já a entrada de diretório é uma estrutura que é alocada para cada arquivo e diretório do sistema e armazena informações de metadados, como atributos, tamanho, nome, rótulos de tempo e endereço inicial dos dados (CARRIER, 2005).

Os rótulos de tempo no sistema FAT são armazenados nas entradas de diretório e referem-se aos tempos de criação, modificação e acesso. Ao contrário da maioria dos sistemas de arquivos, o sistema FAT não registra os rótulos de tempo armazenando a quantidade de segundos decorridos a partir de uma determinada data. Ao invés dessa técnica, ele armazena os dígitos correspondentes à data e à hora informadas pelo sistema (seja pelo sistema operacional do computador, ou pela configuração da máquina fotográfica ou celular, por exemplo). Em função disso, o rótulo de tempo armazenado já está convertido para o fuso horário configurado para o dispositivo (CARRIER, 2005).

O sistema FAT apresenta resolução de horário diferente para cada rótulo de tempo analisado. O tempo de criação possui resolução de centésimos de segundo, o tempo de modificação tem resolução de dois em dois segundos e o tempo de acesso possui resolução de dias. Essa diferença se deve à quantidade de bytes disponibilizada para cada rótulo de tempo. O tempo de acesso possui somente 2 bytes, que são utilizados para data. Já o tempo de modificação possui 4 bytes, sendo 2 para a data e 2 para a

hora, enquanto que o tempo de criação possui 5 bytes, 2 para a data e 3 para a hora. Os 2 bytes utilizados para a data nos três rótulos de tempo apresentam a seguinte distribuição: 5 bits para o dia, 4 bits para o mês e 7 bits para o ano, possuindo intervalos válidos de 1 a 31, 1 a 12 e 0 a 127, respectivamente, conforme figura 2.7. A interpretação do valor do dia e do mês são diretas, enquanto que para o ano deve-se adicionar ao valor armazenado o número 1980. No rótulo de modificação são utilizados 2 bytes para a hora, divididos da seguinte forma: 5 bits para os segundos, 6 bits para os minutos e 5 bits para a hora, com intervalos válidos de 0 a 29, 0 a 59 e 0 a 23, respectivamente, conforme figura 2.8. A tradução dos campos referentes às horas e aos minutos é direta. Para os segundos, como o intervalo válido não abrange todo o intervalo real, o valor armazenado é multiplicado por 2, resultando, portanto, em uma resolução de 2 em 2 segundos para o tempo de modificação, registrando somente os segundos pares. Já o tempo de criação utiliza o mesmo esquema do tempo de modificação, no entanto, por possuir um byte a mais, apresenta uma melhor resolução temporal, de centésimos de segundo. Ela é alcançada adicionando-se ao valor referente aos segundos, obtidos dos 5 bits indicados acima, os centésimos de segundo armazenados no byte adicional, que possui intervalo válido de 0 a 199 (MICROSOFT, 2000).

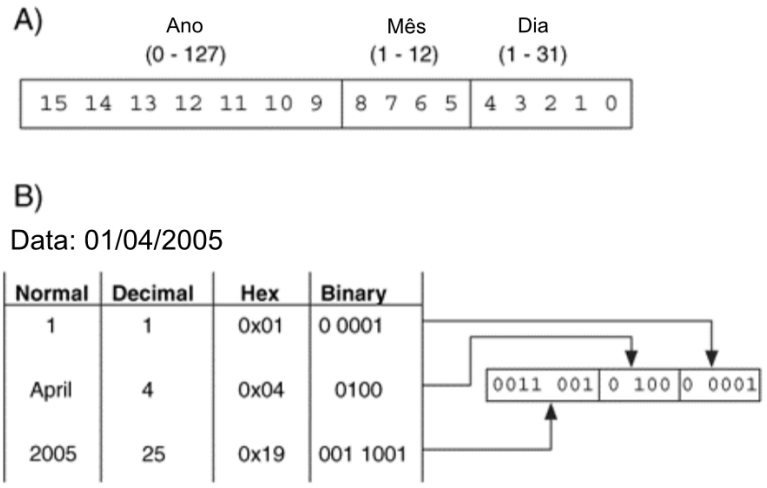


Figura 2.7: A) Divisão dos bits entre os campos da data e respectivos intervalos válidos; B) Conversão da data 01/04/2005 para formato do FAT (*Adaptado de:* Carrier (2005))

2.6 Trabalhos correlatos

Em uma análise forense em que a informação temporal é relevente, é recomendável que sejam analisados os rótulos de tempo de um conjunto de arquivos e pastas que apresentem relação com o caso examinado. Dessa forma, obtem-se maior robustez na reconstrução de eventos do que se baseados somente em metadados de um único arquivo (CHOW et al., 2007). Nesse contexto, Chow et al. (2007) apresentam propostas de

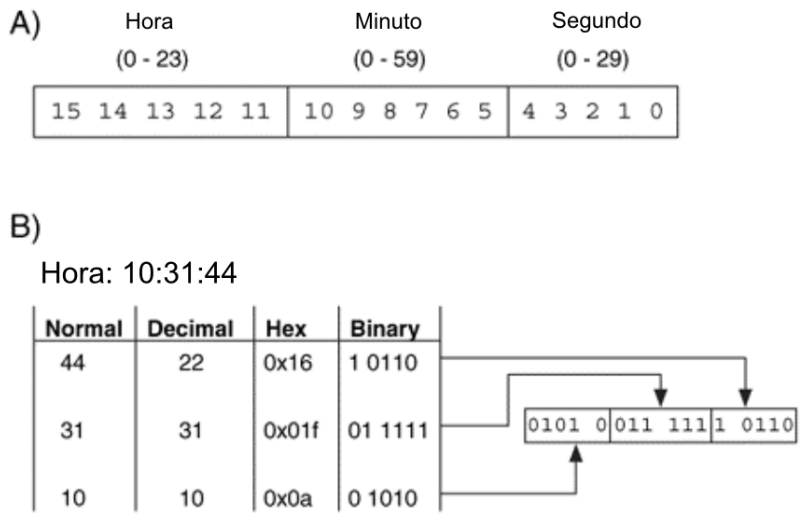


Figura 2.8: A) Divisão dos bits entre os campos da hora e respectivos intervalos válidos; B) Conversão da hora 10:31:44 para formato do tempo de modificação (*Adaptado de:* Carrier (2005))

regras de comportamento de rótulos de tempo em um sistema NTFS para algumas ações comuns de manipulação em arquivos. Essas regras foram validadas com experimentos realizados em sistemas Windows XP e, posteriormente, aplicadas em dois estudos de caso. Outro recomendação é que seja verificado se o relógio da BIOS está sincronizado com o horário real e, em sistemas Windows, se a atualização do tempo de último acesso está habilitada no Registro.

A seguir serão apresentadas as regras citadas em Chow et al. (2007), as quais serão discutidas, posteriormente, no capítulo 5, com os resultados obtidos nos experimentos.

1. Quando o tempos de modificação e criação são iguais, os arquivos não foram modificados nem copiados de outra porção do disco;

2. Quando o tempo de modificação é anterior ao tempo de criação, o arquivo foi copiado do mesmo volume ou de outro volume ou então foi movido de um volume diferente. Um arquivo movido no mesmo volume não apresenta alterações em seus tempos de modificação e criação;

3. Quando arquivos em uma pasta apresentam tempos de modificação anteriores ao tempo de criação e seus tempos de criação são muito próximos, então os arquivos foram copiados do mesmo volume ou de outro em lote ou foram movidos de outro volume em lote ou foram extraídos de um arquivo comprimido;

4. Quando uma grande quantidade de arquivos no volume apresentam tempos de acesso próximos, é provável que tenham sido varridos por alguma ferramenta, como anti-vírus ou aplicativos de busca;

5. Se arquivos de vídeo/imagens em uma pasta apresentarem tempos de acesso próximos e outros arquivos do mesmo tipo não possuírem tempos de acesso nesse intervalo, é provável que tenham sido acessados por alguma ferramenta de pré-visualização, como por exemplo por meio do modo miniatura do *Windows Explorer*;

6. Quando arquivos em uma pasta possuem tempos de acesso aleatórios é provável que tenham sido acessados individualmente;

7. Quando arquivos em uma pasta possuírem tempos de modificação e criação iguais e quando esses tempos forem muito próximos entre cada arquivo, é possível que eles tenham sido baixados em lote de um outro sistema via rede.

A análise do comportamento de rótulos de tempo em sistemas NTFS foi expandida por outro autor em dois trabalhos. No primeiro, Bang et al. (2009) apresentam resultados preliminares, enquanto que no segundo, Bang, Yoo e Lee (2011) apresentam resultados mais detalhados e para uma maior variedade de operações com arquivos e pastas. Esses trabalhos inovaram, também, em relação ao anterior, quando incluiram na análise o tempo de última modificação da MFT e os quatro rótulos de tempo do atributo $FILE_NAME. O tempo de última modificação da MFT, apesar de não ser mostrado pelo sistema operacional, pode ser visualizado por diversas ferramentas forenses e seu comportamento varia de acordo com a operação realizada no arquivo ou pasta. A inclusão dos rótulos de tempo do atributo $FILE_NAME, além de auxiliar na individualização das operações estudadas, traz uma maior confiabilidade, pois não foi encontrada ferramenta capaz de alterar seus valores, ao contrário dos rótulos do atributo $STANDARD_INFORMATION. O detalhamento dos resultados de Bang, Yoo e Lee (2011) será apresentando no capítulo 5, onde serão discutidas suas divergências e convergências com os experimentos deste trabalho.

3 METODOLOGIA

Neste capítulo será apresentado inicialmente o procedimento geral utilizado nos experimentos. Em seguida, serão detalhados os testes referentes a operações com arquivos e pastas no sistema NTFS, varreduras de aplicativo de mídia e de antivírus, manipulações dos rótulos de tempo e do relógio do sistema, pontos de restauração e tranferência de arquivos do sistema FAT para o NTFS.

3.1 Procedimento geral

De forma a alcançar o objetivo proposto foram realizadas análises de rótulos de tempo de arquivos e pastas contidos em um sistema de arquivos NTFS com sistema operacional Windows XP Professional (Service Pack 3) e configurações padrão. O referido sistema foi criado em uma máquina virtual utilizando-se o aplicativo *VirtualBox* (ORACLE, 2004-2011) em uma máquina hospedeira Ubuntu/Linux. Foi utilizado um disco virtual de tamanho fixo de 8 GiB, possuindo a partição do sistema operacional um tamanho de 6 GiB e uma segunda partição um tamanho de 2 GiB. Ressalta-se que a utilização da máquina virtual não influencia o experimento, tendo sido utilizada somente para facilitar o procedimento de processamento dos dados descrito a seguir.

Para realização da análise é necessário que se conheça os valores dos rótulos de tempo antes e após cada operação avaliada. Para tanto, foi adotado o procedimento de iniciar a máquina virtual, configurar os arquivos e pastas de acordo com o teste a ser realizado, desligar a máquina virtual, realizar uma cópia do arquivo do disco virtual, iniciar novamente a máquina virtual, realizar as operação planejadas, anotando o instante de cada operação, desligar a máquina e, finalmente, realizar nova cópia do disco virtual. A partir dos arquivos do disco virtual referentes aos instantes anterior e posterior às operações foram realizadas as análises pertinentes.

Para analisar os rótulos de tempo armazenados nos arquivos dos discos virtuais, foi desenvolvida pelos autores uma ferramenta em *Shell Script*, chamada *proc_time_mft*, cujo código fonte é apresentado no apêndice B. Essa ferramenta foi executada na máquina hospedeira Ubuntu/Linux e utiliza como entrada uma lista gerada pelo aplicativo *fls* do pacote *sleuthkit* (CARRIER, 2003-2012). Essa lista é gerada pelo processamento de

diretórios, referenciados pelo número de suas entradas MFT na chamada do programa, e apresenta, em cada linha, uma entrada referente aos arquivos e pastas contidos nesse diretório, sendo que cada linha contém o nome, número da entrada MFT e tipo da entrada (arquivo ou pasta). A partir do número das entradas MFT obtidas pelo aplicativo *fls*, a ferramenta *proc_time_mft* obtém o LSN de cada entrada, utilizando-se a ferramenta *istat* do pacote *sleuthkit* (CARRIER, 2003-2012), extrai os rótulos de tempo dos atributos $STANDARD_INFORMATION e $FILE_NAME, utilizando-se a ferramenta *icat* do pacote *sleuthkit* (CARRIER, 2003-2012), e os processa, convertendo-os para tempo UTC com resolução de segundos e habilitando uma flag caso as frações de segundo estejam zeradas. Finalmente, a ferramenta gera um arquivo texto de saída que contém em cada linha o número da entrada MFT, o nome, o LSN, o tipo da entrada, e o identificador dos atributos com os respectivos rótulos de tempo e flags referentes às frações de segundo.

Os arquivos texto gerados pela ferramenta descrita referentes aos instantes anterior e posterior às operações analisadas foram importados em uma tabela do aplicativo *Calc* do pacote *OpenOffice*. Nessa tabela, as entradas foram ordenadas de modo que cada entrada de um arquivo ou pasta referente ao instante anterior às operações fique imediatamente posicionado primeiro que sua entrada referente ao instante posterior. Após a ordenação, foram realizadas comparações entre os rótulos de tempo anterior e posterior de um arquivo ou pasta, utilizando-se funções nativas do aplicativo, sendo apresentado na referida tabela se houve variação entre eles. Foram realizadas, também, comparações entre os rótulos de tempo (criação, modificação, modificação da MFT e acesso) dos atributo de cada entrada referentes aos instantes posteriores, sendo apresentado os nomes dos rótulos ordenados cronologicamente e separados pelo sinal de maior quando diferentes. A partir do processamento realizado nas tabelas do aplicativo *Calc*, foram feitas as análises de cada operação para determinação do comportamento dos rótulos de tempo em cada uma das situações em estudo. Em todos os casos nos quais foram constadas inconsistências em relação à literatura, as operações foram refeitas utilizando-se outros arquivos e pastas.

Ressalta-se que a ferramenta desenvolvida pelos autores para processamento dos rótulos de tempo foi validada antes dos experimentos com a ferramenta *istat* do pacote *sleuthkit* (CARRIER, 2003-2012) e por verificação manual das entradas MFT. Foi necessário desenvolver a ferramenta pois o aplicativo *istat* apresenta o rótulos de tempo no horário local, não informa as frações de segundo e seu formato de saída não é adequado para importação em tabelas do aplicativo *Calc*. O processamento realizado nessas tabelas

também foi validado antes dos experimentos por verificação manual.

Antes do início dos testes com a ferramenta *proc_time_mft* e tabelas do *Calc*, foi avaliada a necessidade de se considerar também os rótulos de tempo de arquivos e pastas armazenados nas entradas de índice dos seus diretórios pais (atributos $INDEX_ROOT e $INDEX_ALLOCATION). Nessa avaliação utilizou-se as ferramentas *dd* (The IEEE and The Open Group, 2001-2008) e *xxd* (WEIGERT, 1996), nativas do Linux, para observar os bytes referentes à esses rótulos de tempo e aos armazenados nos atributos $FILE_NAME e $STANDARD_INFORMATION, com o objetivo de compará-los. Essa comparação foi realizada com a máquina virtual em execução e as verificações foram feitas à medida que eram realizadas alterações em determinados arquivos e pastas. Outra etapa da avaliação consistiu na alteração, com a máquina virtual desligada, utilizando-se a ferramenta *dd*, de bytes referentes a rótulos de tempo de índices de diretório de alguns arquivos para valores distintos dos armazenados originalmente. Em seguida a máquina virtual foi executada e esses rótulos foram monitorados, com as ferramentas *dd* e *xxd*, antes e após à exibição dos arquivos e pastas em questão no *Windows Explorer*.

3.2 Operações no sistema NTFS

Baseando-se na literatura (CHOW et al., 2007; BANG et al., 2009; BANG; YOO; LEE, 2011), foram selecionadas operações sobre arquivos e pastas, detalhadas nesta seção, para avaliação do comportamento de seus rótulos de tempo.

3.2.1 Criação de arquivos e pastas

Para criação de arquivos digitou-se um texto no aplicativo *Notepad* e, em seguinda, salvou-se esse conteúdo em um novo arquivo na pasta desejada. Para a criação de pastas foi utilizada a opção de criar nova pasta no menu do aplicativo *Windows Explorer*.

3.2.2 Cópia de arquivos e pastas

Arquivos e pastas foram copiados de um local para outro no mesmo volume e entre volumes (entre as duas partições do disco) por meio do método de copiar e colar, utilizando-se os atalhos do teclado (Ctrl-C e Ctrl-V), e do método "*drag and drop*", utilizando-se o mouse. Ressalta-se que nos testes de cópia no mesmo volume com o método "*drag and drop*"foi necessário manter a tecla Shift pressionada enquanto o objeto era arrastado pelo mouse, pois, caso contrário, seria realizada movimentação.

No teste de cópia de pastas foi realizado o procedimento com pastas que continham arquivos e subpastas para verificação do comportamento dos rótulos de tempo desses objetos.

3.2.3 Movimentação de arquivos e pastas

Na movimentação de arquivos e pastas foram utilizados o método de copiar e colar, utilizando-se os atalhos do teclado (Ctrl-X e Ctrl-V), e o método "*drag and drop*", utilizando-se o mouse. Arquivos e pastas foram movimentados dentro do mesmo volume e entre volumes (entre as partições do disco). As operações foram realizadas com arquivos residentes e não residentes[7]. No teste de movimentação entre volumes diferentes com o método "*drag and drop*"foi necessário manter a tecla Shift pressionada enquanto o objeto era arrastado com o mouse para que fosse realizada a movimentação e não a cópia. Da mesma forma como no teste de cópia de pastas, foram realizadas movimentações com pastas que continham arquivos e subpastas para avaliar o comportamento de seus rótulos de tempo.

3.2.4 Alteração de propriedades de arquivos e pastas

Foram realizadas alterações nas propriedades "somente leitura"e "oculto"de arquivos e pastas por meio da opção "Propriedades"do menu de contexto do *Windows Explorer*.

3.2.5 Renomeio de arquivos e pastas

No operação de renomeio foi utilizado o teclado (tecla F2) para alterar o nome de arquivos e pastas listados no *Windows Explorer* e o acionamento da tecla Enter para concluir a operação.

3.2.6 Alteração de conteúdo de arquivos e pastas

Nos testes de alteração de conteúdo de arquivos foram utilizados arquivos texto os quais foram manipulados pelos aplicativos *Notepad* e *Wordpad*. As alterações foram realizadas em arquivos residentes e não residentes, acrescentando-se e excluindo-se informações. Foi investigada a situação de arquivos residentes serem aumentados e tornarem-se não residentes assim como a redução de arquivos não residentes.

[7]Arquivos residentes possuem seu conteúdo armazenado na própria MFT, enquanto que arquivos não residentes têm seu conteúdo armezados em blocos referenciados na MFT. (RUSSINOVICH; SOLOMON, 2004)

A alteração de conteúdo de pastas foi testada por meio da inclusão e da exclusão de arquivos e subpastas.

3.2.7 Sobrescrita de arquivos e pastas

Para realização dos testes de sobrescrita de arquivos, foi necessário, inicialmente, copiar arquivos para pastas diferentes das pastas originais. Em seguida, esses arquivos foram alterados, para depois sobrescreverem os arquivos originais. Os testes de sobrescrita foram realizados com o arquivo que sobrescreveu presente na mesma partição e em partição diferente do arquivo sobrescrito. As operações de sobrescrita foram realizadas tanto por meio da cópia quanto da movimentação do arquivo alterado para a pasta do arquivo original.

Na sobrescrita de pastas foram avaliadas as situações de sobrescrita por meio de movimentação e cópia. Foram avaliados cenários em que a pasta que sobrescreveu possuía mais arquivos e menos arquivos que a pasta sobrescrita. Em todos esses cenários, dentro da pasta que sobrescreveu havia arquivos com o mesmo nome de arquivos da pasta original mas com conteúdo alterado.

3.2.8 Extração de arquivos e pastas compactados

Foram criados arquivos compactados no formato *zip* na máquina hospedeira, os quais foram inseridos na máquina virtual por meio de um *pendrive* formatado com sistema FAT. Foram criados arquivos *zip* contendo somente arquivos e outros contendo pastas com arquivos dentro. Esses arquivos compactados foram extraídos para a pasta em que se encontravam utilizando-se a ferramenta nativa do sitema operacional Windows.

3.2.9 *Download* de arquivos e pastas

Utilizou-se o navegador *Internet Explorer* para realizar o *download* de arquivos hospedados em *sites* na Internet. Foi realizado, também, o mapeamento de uma unidade de rede via *Windows Explorer* para avaliar a transferência de arquivos de uma pasta compartilhada para a máquina em estudo. No caso em questão, a unidade mapeada referiu-se a uma pasta da máquina hospedeira que foi compartilhada utilizando-se a ferramenta *Samba* (SAMBA, 1992-).

3.2.10 Pré-visualização de arquivos de imagem

Para realizar a pré-visualização de arquivos de imagem, utilizou o *Windows Explorer*, o qual apresentava o modo de visualização configurado para o modo "detalhes", para navegar até a pasta de interesse. Em seguida, alterou-se o modo de visualização dessa pasta para o modo "miniaturas".

3.3 Varredura com Windows Media Player

Para varrer uma pasta com arquivos de mídia para incluí-los na biblioteca do *Windows Media Player* primeiramente configurou-se esse aplicativo para não incluir arquivos em sua biblioteca automaticamente. Em seguida, copiou-se uma pasta com arquivos de áudio para o sistema em questão via *pendrive*. Finalmente selecionou-se manualmente essa pasta, dentro do *Windows Media Player*, para inclusão na biblioteca do aplicativo.

3.4 Varredura com antivírus

Para os testes de varredura de programas antivírus, foram instalados os aplicativos AVG (AVG Technologies, 2012), Avast (AVAST Software, 1988-2012) e Avira (Avira Operations, 2012), os quais foram configurados para não realizar varredura automática. Em seguida, selecionou-se, em cada aplicativo, algumas pastas para serem submetidas a varredura manual.

3.5 Manipulações intencionais dos rótulos de tempo

Para alteração intencional de rótulos de tempo de arquivos foram instalados na máquina em estudo os aplicativos *SKTimeStamp* (KüNG, 2011), *eXpress TimeStamp Toucher (XTST)* (HALIULLIN, 2004), *NewFile Time* (NENAD, 2010) e *Febooti File Tweak* (Febooti Software, 2011). Em cada aplicativo foram selecionados arquivos ou pastas inteiras (no caso do *Time Stamp Toucher*) para que tivessem seus rótulos de tempo alterados para 6h01min01s do dia 01/01/2010. Deve-se ressaltar que esse horário corresponde ao horário local, o que equivale a 9h01min01s em UTC. Nenhum dos aplicativos testados apresentava opção para alteração do tempo de modificação da MFT, sendo possível somente alterar os rótulos de criação, modificação e acesso.

3.6 Manipulação do relógio do sistema

O *VirtualBox* (ORACLE, 2004-2011), programa utilizado para gerenciar a máquina virtual do sistema operacional em estudo, possui alguns parâmetros que configuram a sincronização entre o relógio da máquina hospedeira e o da máquina hóspede. Esses parâmetros determinam o intervalo de sincronização, o limite mínimo de diferença temporal entre os dois relógios, dentre outras opções. Foi necessário, portanto, alterar essas configurações para possibilitar a realização dos testes de manipulação do relógio do Windows, caso contrário o relógio seria reajustado automaticamente para o horário correto. Foi alterado, então, o parâmetro *–timesync-interval*, que determina o intervalo entre as sincronizações dos dois relógios[8].

Após essas configurações, foram realizadas operações sequenciais de alteração, cópia e renomeio de arquivos inicialmente com o relógio no tempo correto. Em seguida, as mesmas operações foram realizadas com o relógio atrasado. Na sequência, essas operações foram realizadas novamente com o relógio no tempo correto. Em seguida, repetiu-se as operações com o relógio adiantado e, finalmente, com o relógio no tempo correto. Ao fim dessas operações a máquina virtual foi desligada e as pastas de interesse foram processadas de acordo com o procedimento geral, descrito na seção 3.1. Finalmente, os arquivos que foram submetidos a algum tipo de alteração foram ordenados de acordo com o seu campo LSN para avaliar o comportamento desse campo em virtude da alteração do relógio.

3.7 Pontos de restauração

Foram realizados testes com pontos de restauração para avaliar sua forma de funcionamento e de que maneira eles podem fornecer informações relevantes para a análise de rótulos de tempo.

Realizou-se, então, operações de alteração de conteúdo, deleção, cópia, movimentação, renomeio e criação de arquivos. Após a realização dessas operações foram criados pontos de restaurações manualmente utilizando-se a ferramenta gráfica nativa do sistema. Após a criação do ponto de restauração, a máquina virtual era desligada e os diretórios referentes às pastas que continham os arquivos alterados e a pasta referente ao ponto de restauração eram processadas conforme o procedimento geral, citado na seção 3.1. Nos

[8]Para realizar a configuração dos parâmetros de sincronização no VirtualBox deve-se executar o comando *VBoxManage guestproperty set "NOME DA MÁQUINA VIRTUAL" "/VirtualBox/GuestAdd/VBoxService/PARAMETRO" VALOR*.

testes de alteração de arquivos foram realizadas mais de uma alteração por aquivo entre dois pontos de restauração, para avaliar quais dessas alterações seriam registradas. Adicionalmente, entre alterações sequenciais em um mesmo arquivo e antes da geração do ponto de restauração, foi realizado a reinicialização da máquina para verificar se o desligamento exercia alguma influência sobre qual versão do arquivo seria registrada.

Como na criação do ponto de restauração os arquivos monitorados são copiados para a pasta do ponto de restauração com um nome diferente do seu nome original, foi necessário fazer o mapeamento entre esses nomes. Para isso foi utilizada a ferramenta *MANDIANT Restore Point Analyzer*[9](HARMS, 2006), que processa o arquivo *change.log* e apresenta o nome original do arquivo, com seu caminho, e o nome utilizado pelo ponto de restauração. Essa ferramenta foi instalada em outra máquina virtual Windows, diferente da utilizada para os experimentos. Mountou-se, então, na máquina Linux hospedeira, o arquivo de imagem da máquina virtual utilizada nos experimentos em modo somente leitura e copiou-se o arquivo *change.log* para a máquina hospedeira. Em seguida, esse arquivo foi transferido para a máquina virtual Windows por meio de um *pendrive*. Finalmente esse arquivo foi processado pela ferramenta, permitindo, assim, mapear os arquivos gerados pelo ponto de restauração com os arquivos de interesse.

Para realização dos testes foi realizada a alteração do arquivo de configuração *filelist.xml*, que determina quais diretórios e extensões de arquivos são incluídos ou excluídos do monitoramento. No primeiro teste, foi incluído o diretório no qual as operações foram realizadas. No segundo teste, foi adicionada no monitoramento de arquivos a extensão dos arquivos testados e, no terceiro teste, o diretório de trabalho foi acrescentado na lista de diretórios excluídos do monitoramento.

3.8 Operações entre sistema FAT e sistema NTFS

Além da análise de operações de arquivos e pastas no sistema NTFS, foram realizados, também, estudos em arquivos e pastas transferidos de um sistema FAT para o sistema NTFS. Não foram realizados estudos para arquivos transferidos do sistema NTFS para o sistema FAT, visto que o escopo do trabalho limita-se ao sistema NTFS.

Para determinação dos valores dos rótulos de tempo dos arquivos e pastas, ainda no sistema FAT, no instante anterior à transferência para o sistema NTFS, foi adotado o

[9]Disponível em http://www.mandiant.com/products/free_software

procedimento descrito a seguir. Montou-se na máquina hospedeira, em modo somente leitura, o *pendrive* formatado no sistema FAT utilizado nos testes. Em seguida, foi utilizado tanto as ferramentas *dd* (The IEEE and The Open Group, 2001-2008) e *xxd* (WEIGERT, 1996), nativas do Linux, para processamento manual dos rótulos de tempo, quanto a ferramenta *istat* do pacote *sleuthkit* (CARRIER, 2003-2012). Já o processamento dos rótulos de tempo dos arquivos e pastas após a tranferência para o sistema NTFS, juntamente com a sua comparação com os rótulos do instante anterior às operações de tranferência, foram realizados conforme o procedimento geral, descrito na seção 3.1.

3.8.1 Cópia de arquivos e pastas

As cópias do sitema FAT para o sistema NTFS foram realizadas pelos métodos de copiar e colar, utilizando-se os atalhos do teclado (Ctrl-C e Ctrl-V), e pelo método "*drag and drop*", utilizando-se o mouse. As cópias foram realizadas de um *pendrive* para a máquina em estudo. As pastas copiadas continham arquivos e subpastas em seu interior.

3.8.2 Movimentação de arquivos e pastas

Da mesma forma, como no teste de cópia entre os sistemas de arquivos, foram realizados também testes de movimentação de arquivos e pastas de um *pendrive* para a máquina em estudo. As movimentações foram feitas pelo método de copiar e colar, utilizando-se os atalhos do teclado (Ctrl-X e Ctrl-V), e pelo método "*drag and drop*", utilizando-se o mouse. Nesse último foi necessário manter a tecla Shift pressionada para que fosse realizada movimentação ao invés de cópia. Ressalta-se que as pastas movidas continham arquivos e subpastas em seu interior.

4 RESULTADOS OBTIDOS

Neste capítulo são apresentados os resultados obtidos nos experimentos realizados em uma máquina virtual com sistema operacial Windows XP e sistema de arquivos NTFS. Ressalta-se que, quando os resultados obtidos apresentaram diferenças em relação à bibliografia utilizada, os testes foram repetidos.

Para fins didáticos, será adotada uma convenção de abreviatura para nomes dos rótulos de tempo e dos atributos do NTFS deste ponto até o final do texto, a saber:

- CrT: Tempo de criação;
- MT: Tempo de última modificação;
- ChT: Tempo de última modificação da MFT;
- AT: Tempo de último acesso;
- SI: $STANDARD_INFORMATION;
- FN: $FILE_NAME.

Na figura 4.1, é apresentada a localização na entrada MFT dos citados rótulos de tempo e atributos, acompanhados da abreviatura adotada.

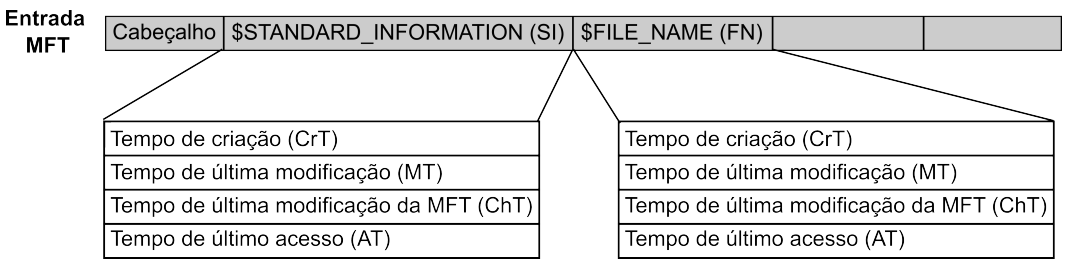


Figura 4.1: Rotulos de tempo contidos nos atributos $STANDARD_INFORMATION e $FILE_NAME de uma entrada MFT

4.1 Operações com arquivos

Nesta seção serão apresentados os resultados referentes ao comportamento dos rótulos de tempo de arquivos quando submetidos às operações detalhadas a seguir.

4.1.1 Criação de arquivos

Foi verificado que, quando um arquivo é criado, todos os rótulos de tempo dos atributos SI e FN armazenam o tempo de criação.

4.1.2 Cópia de arquivos

Quando um arquivo é copiado, os rótulos MT e ChT do SI preservam os tempos do arquivo original. Os demais rótulos do SI e todos do FN armazenam o tempo da cópia. O procedimento foi realizado copiando-se arquivos provenientes do mesmo volume e de volumes diferentes por meio dos métodos "copiar e colar"e "*drag and drop*". Foram obtidos resultados idênticos para todos esses cenários.

4.1.3 Movimentação de arquivos

O comportamento dos rótulos de tempo de arquivos movimentados dentro do mesmo volume e entre volumes difere. Nos tópicos seguintes serão detalhados esses dois cenários.

4.1.3.1 Movimentação no mesmo volume

Quando um arquivo é movimentado de uma pasta para outra dentro do mesmo volume, os rótulos de tempo do atributo SI são copiados para o atributo FN. Deve-se ressaltar que, quando o arquivo é acessado, instantes antes da movimentação, o AT do SI é atualizado, sendo copiado para o FN. Após o termino da movimentação o ChT do SI é alterado para o tempo da movimentação, permanecendo os demais rótulos desse atributo inalterados. Dessa forma, o tempo da movimentação pode ser recuperado tanto pelo ChT (SI) quando pelo AT (FN), os quais apresentarão alguns segundos de diferença. Foram realizados testes com arquivos residentes e não residentes[10] e utilizando-se os métodos "recortar e colar"e *drag and drop*, sendo observado o mesmo resultado em todos os casos.

4.1.3.2 Movimentação entre volumes diferentes

Na movimentação de arquivos entre volumes diferentes, o rótulo AT do SI e todos os rótulos do FN armazenam o tempo da movimentação, enquanto que os demais mantêm o tempo original. Os resultados se repetiram para arquivo residentes e não residentes e para os dois métodos de cópia.

[10] Arquivos residentes possuem seu conteúdo armazenado na própria MFT, enquanto que arquivos não residentes têm seu conteúdo armezados em blocos referenciados na MFT. (RUSSINOVICH; SOLOMON, 2004)

4.1.4 Alteração de propriedades de arquivos

Foi constatado que, quando é alterada alguma propriedade de um arquivo, o ChT (SI) armazena o tempo de alteração e o AT (SI) armazena um tempo imediatamente anterior ao do ChT, correspondendo ao instante que o arquivo é selecionado com o botão direito do mouse para alteração das propriedades. Os demais rótulos de tempo permanecem inalterados.

4.1.5 Renomeio de arquivos

A operação de renomear arquivos obedece às mesmas regras de movimentação de arquivos dentro do mesmo volume, ou seja, ChT do SI armazena o tempo da operação, o AT do SI armazena um valor próximo e um pouco anterior ao ChT, enquanto que os demais rótulos do SI permanecem inalterados. Já os rótulos do atributo FN são alterados para os valores constantes no atributo SI no instante imediatamente anterior ao renomeio.

4.1.6 Alteração de conteúdo de arquivos

Foram investigadas alterações de conteúdo de arquivos com os aplicativos *Wordpad* e *Notepad*. Arquivos residentes tiveram seu conteúdo reduzido para permanecerem residentes e aumentado para tornarem-se não residentes. Já arquivos não residentes foram aumentados e reduzidos, permanecendo não residentes, visto que após virar não residente, um arquivo não retorna para o estado residente. Para todas as situações os rótulos MT, ChT e AT do SI foram atualizados para o instante da alteração, permanecendo os demais inalterados.

4.1.7 Sobrescrita de arquivos

O comportamento dos rótulos de tempo de arquivos sobrescritos variam de acordo com a forma na qual a operação foi realizada. Nos subtópicos serão detalhados os resultados para sobrescrita efetuada por meio de cópia e por meio de movimentação de arquivos.

4.1.7.1 Sobrescrita por meio de cópia

Quando arquivos são sobrescritos pela cópia de arquivos oriundos do mesmo volume ou de volume diferente, o rótulo AT (SI) armazena o instante da operação, os rótulos MT e ChT do SI são copiados do arquivo que sobrescreveu e o rótulo CrT (SI) é mantido. Os rótulos do FN do arquivo sobrescrito não são alterados.

4.1.7.2 Sobrescrita por meio de movimentação

1. *Movimentação no mesmo volume*: Quando um arquivo é sobrescrito por meio da movimentação de um arquivo proveniente do mesmo volume, o rótulo ChT (SI) armazena o tempo da operação, o AT (SI) apresenta rótulo com alguns segundos anteriores ao ChT, o rótulo MT (SI) é copiado do arquivo que sobrescreveu e o rótulo CrT (SI) é mantido. Os rótulos do FN do arquivo sobrescrito são copiados do atributo SI do arquivo que sobrescreveu.

2. *Movimentação entre volumes diferentes*: Já quando a sobrescrita ocorre por meio da movimentação de um arquivo proveniente de um volume diferente, o rótulo AT (SI) armazena o tempo da operação, enquanto os demais rótulos do SI são copiados do arquivo que sobrescreveu. Os rótulos do FN não são alterados.

4.1.8 Extração de arquivos compactados

Foi realizada a extração de arquivos compactados em formato *zip* utilizando-se a ferramenta nativa do sistema operacional Windows, sendo constatado que o ChT do SI e todos os rótulos do FN armazenam o tempo da extração dos arquivos. Os demais rótulos do SI são alterados com o valor presente no rótulo de última modificação do arquivo original. É importante ressaltar que o valor armazenado nos rótulos CrT, MT e AT do SI apresentam as frações de segundo zeradas e somente segundos pares, semelhante aos rótulos de modificação do sistema FAT. Quando os arquivos originais apresentam segundos ímpares em seu rótulo MT (SI), estes valores são arredondados para cima quando copiados para os rótulos CrT, MT e AT dos arquivos extraídos.

4.1.9 *Download* de arquivos

Arquivos copiados de *sites* na Internet por meio do navegador *Internet Explorer* apresentam rótulos de tempo compatíveis com operações sequenciais de criação, alteração de conteúdo e renomeio. Portanto, possuem rótulos de tempo semelhantes ao renomeio de arquivos, última operação executada, apresentando o ChT do SI com valor superior aos demais e os rótulos CrT, MT e AT do FN iguais aos do SI. No entanto, em decorrência das operações anteriores, temos o MT e o AT do SI iguais entre si e superiores ao CrT (SI) e o MT, ChT e AT do FN iguais entre si, devido à alteração de conteúdo. Temos também todos os rótulos de tempo com diferenças de segundos, pois as operações de criação, modificação de conteúdo e renomeio ocorreram entre o início e término do *download* dos arquivos.

Arquivos e pastas copiados via rede local através de compartilhamento de pastas com a ferramenta *Samba* (SAMBA, 1992-) apresentaram alterações nos seus rótulos de tempo iguais às operações de cópia de arquivos e pastas dentro do volume.

4.1.10 Pré visualização de arquivos de imagem

Quando arquivos de imagem contidos em uma pasta são visualizados por uma aplicativo de pré-visualização, como o Windows Explorer no modo miniatura, seus rótulos AT (SI) apresentam valores iguais ou com diferença de segundos.

4.2 Operações com pastas

Nesta seção será detalhado o comportamento dos rótulos de tempo de pastas submetidas às operações detalhadas a seguir.

4.2.1 Criação de pastas

Quando da criação de uma pasta, os rótulos CrT, MT e AT do atributo SI e todos os rótulos de tempo do atributo FN armazenam o mesmo valor, enquanto que o rótulo ChT do SI armazena um tempo um pouco superior em relação aos demais rótulos. Foi constatado que o tempo armazenado no CrT, MT e AT do SI e nos rótulos do FN correspondem ao tempo no qual a opção de criar nova pasta é selecionada no Windows Explorer e que o tempo armazenado no ChT do SI corresponde ao tempo no qual o usuário atribui um nome para a pasta e aperta a tecla Enter. Esse comportamento permite inferir que, quando da seleção da opção de criação da uma nova pasta, o Windows cria uma pasta com um nome padrão e, quando o usuário atribui o nome, a pasta é renomeada.

4.2.2 Cópia de pastas

Foi observado que, quando uma pasta é copiada, independentemente se proveniente do mesmo volume ou de volume diferente e do método de cópia ("copiar e colar"ou "*drag and drop*"), todos os seus rótulos de tempo em ambos os atributos armazenam o tempo da operação.

Para subpastas e arquivos dentro das subpastas, valem as mesmas regras para cópia de pasta e cópia de arquivo, respectivamente.

4.2.3 Movimentação de pastas

O comportamento dos rótulos de tempo de pastas movimentadas dentro do mesmo volume e entre volumes é diferente. Nos subtópicos seguintes serão detalhados esses dois cenários.

4.2.3.1 Movimentação no mesmo volume

Em movimentação de pastas dentro do mesmo volume os rótulos ChT e AT do SI armazenam o tempo da movimentação, enquanto que os rótulos CrT e MT mantêm o valor original. Já os rótulos do FN são alterados para os valores armazenados no SI antes da operação.

Para subpastas dentro da pasta movida, somente o AT do SI é alterado para o instante da cópia, ficando os demais rótulos inalterados. Para arquivos dentro dessas subpastas, o ChT do SI é alterado para o instante da movimentação, permanecendo os demais rótulos inalterados.

Os resultados obtidos são independentes do método de movimentação utilizado ("recortar e colar"ou "*drag and drop*").

4.2.3.2 Movimentação entre volumes diferentes

Para movimentação de pastas entre volumes diferentes, todos os rotulos de tempo de ambos os atributos são alterados para o instante da operação, independente do método de movimentação utilizado.

Para subpastas contidas dentro dessas pastas, o comportamento é idêntico. Para arquivos dentro dessas subpastas o resultado é igual ao observado na movimentação de arquivos entre volumes.

4.2.4 Alteração de propriedades de pastas

Quando da alteração das propriedades de uma pasta, os rótulos ChT e AT do SI são atualizados com o tempo da operação, enquanto que os demais permanecem inalterados.

4.2.5 Renomeio de pastas

A operação de renomear pastas obedece às mesmas regras de movimentação de pastas dentro do mesmo volume, ou seja, ChT e AT do SI armazenam o tempo da operação enquanto que os demais rótulos do SI permanecem inalterados. Já os rótulos do atributo FN são alterados para os valores constantes no atributo SI no instante anterior ao renomeio.

4.2.6 Alteração de conteúdo de pastas

Quando o conteúdo de uma pasta é alterado, ou seja, arquivos ou subpastas são criados ou apagados, os rótulos MT, ChT e AT do SI são alterados para o instante da operação, ficando os demais rótulos inalterados.

4.2.7 Modificação de arquivos dentro de uma pasta

Foi constatado que, quando o conteúdo de um arquivo é alterado, a pasta na qual ele está contido apresenta atualização do AT do SI para o instante da alteração. Em alguns casos, no entanto, foi constatado também a alteração do ChT do SI para o mesmo valor do AT (SI). Foram testados casos em que arquivos residentes e não residentes foram aumentados ou reduzidos, não sendo possível identificar um padrão que resulte na alteração do ChT.

4.2.8 Sobrescrita de pastas

Os experimentos de sobrescrita de pastas foram realizados com operações de cópia e de movimentação de pastas. Foram testados os cenários em que a pasta de origem possuía mais arquivos e menos arquivos que a pasta de destino. Nos casos em que a pasta de origem possuía mais arquivos que a destino, o resultado obtido foi o mesmo, independente se realizada cópia ou movimentação. Nesses casos, os rótulos MT, ChT e AT do SI apresentaram o tempo correspondente ao momento da sobrescrita, permanecendo os demais inalterados. Já nos casos em que a pasta de origem possuía menos arquivos que a de destino, para a operação de movimentação os resultados foram iguais aos obtidos com mais arquivos na pasta de origem. Para a operação de cópia, os rótulos de SI e de FN não sofreram alteração.

Os arquivos sobrescritos contidos dentro das pastas examinadas apresentaram o mesmo comportamento de sobrescrita de arquivos.

4.2.9 Extração de pastas compactadas

Pastas extraídas de arquivos em formato *zip* apresentam todos os rótulos de tempo do SI e do FN com valor igual ao tempo de extração da pasta. Os arquivos contidos dentro das pastas se comportam como arquivos extraídos de arquivos compactados. Foi utilizada a ferramenta nativa do sitema operacional Windows para extração das pastas.

4.3 Varredura com *Windows Media Player*

Foi constatado que, quando o aplicativo *Windows Media Player* varre uma pasta para adicioná-la à sua biblioteca, os arquivos multimídia (WMV, WMA, MP3, AVI, MPG, etc) têm os rótulos ChT e AT do SI atualizados para esse instante, permanecendo os demais inalterados. Verificou-se também que a pasta que contém esses arquivos e outros tipos de arquivos constates na pasta, como imagens JPG, não são alterados. Os arquivos adicionados na biblioteca do *Windows Media Player* têm seus nomes inseridos no arquivo "CurrentDatabase_59R.wmdb"localizado na pasta "Documents and Settings\<usuário>\Local Settings\Application Data\Microsoft\Media Player".

4.4 Varredura com antivírus

A varredura de pastas selecionadas com os aplicativos antivírus AVG (AVG Technologies, 2012) e Avast (AVAST Software, 1988-2012) mostrou que os arquivos verificados por esses dois aplicativos não apresentaram alteração nos seus rótulos de tempo. No entanto, arquivos e pastas varridos pelo antivírus Avira (Avira Operations, 2012) apresentaram AT (SI) atualizados para o instante dessa operação.

4.5 Manipulações intencionais dos rótulos de tempo

Foram efetuadas alterações intencionais no rótulos de tempo de arquivos por meio dos aplicativos *SKTimeStamp* (KüNG, 2011), *eXpress TimeStamp Toucher (XTST)* (HALIULLIN, 2004), *NewFile Time* (NENAD, 2010) e *Febooti File Tweak* (Febooti Software, 2011). Em todos os programas foi selecionado para que os arquivos tivessem suas datas alteradas para as 9h01min01s (UTC) do dia 01/01/2010. Os resultados dessas operações são apresentados na tabela 4.1. Para cada rótulo de tempo, a primeira linha apresenta o valor original do arquivo e a segunda o valor posterior à execução dos aplicativos.

Tabela 4.1: Rótulos de tempo do atributo $STANDARD_INFORMATION alterados intencionalmente com diversos programas

	SKTimeStamp	XTST	NewFile Time	Febooti File Tweak
Tempo de criação	2011-05-05;13:25:47 2010-01-01;08:01:01	2011-05-05;13:43:54 2010-01-01;09:01:01	2011-06-07;13:11:45 2010-01-01;09:01:01	2011-06-07;13:12:36 2010-01-01;09:01:01
Tempo de modificação	2011-05-05;13:25:48 2010-01-01;08:01:01	2011-05-10;17:23:43 2010-01-01;09:01:01	2011-06-07;13:11:45 2010-01-01;09:01:01	2011-06-07;13:12:36 2010-01-01;09:01:01
Tempo de modificação MFT	2011-05-10;13:35:09 2011-06-06;21:03:37	2011-05-10;17:23:43 2011-06-06;21:07:27	2011-06-07;13:11:45 2011-06-07;13:25:40	2011-06-07;13:12:36 2011-06-07;13:26:54
Tempo de acesso	2011-05-10;13:34:17 2010-01-01;08:01:01	2011-05-10;17:23:43 2010-01-01;09:01:01	2011-06-07;13:11:45 2011-06-07;13:25:41	2011-06-07;13:12:36 2011-06-07;13:26:56

Como pode ser observado na tabela 4.1, os programas *SKTimeStamp* e *eXpress TimeStamp Toucher* alteraram para a data selecionada os rótulos de tempo de criação, modificação e acesso, enquanto que os programas *NewFile Time* e *Febooti File Tweak* alteraram somente os rótulos de criação e modificação. De todos os programas somente o *SKTimeStamp Toucher* alterou o horário incorretamente (uma hora a menos), o que é compatível com a não consideração do horário de verão pelo aplicativo.

Todos os programas testados, além de não alterarem o rótulo de tempo de modificação da MFT para o tempo selecionado, atualizaram esse rótulo de tempo para o instante em que os arquivos tiveram seus rótulos de tempo intencionalmente alterados. Para os programas *NewFile Time* e *Febooti File Tweak*, o tempo de acesso dos arquivos também foi atualizado para instantes imediatamente após a alteração intencional dos arquivos. Deve-se ressaltar os rótulos de tempo do atributo $FILE_NAME não foram alterados por nenhum aplicativo.

4.6 Manipulação do relógio do sistema

Os testes de manipulação de arquivos com alteração do relógio mostraram que os rótulos que sofreram alterações registravam o horário indicado pelo relógio, mesmo esse estando alterado. Em virtude desse fato, nas operações em que não ocorre alteração de todos os rótulos de tempo do arquivo, podem haver inconsistências temporais entre seus rótulos de tempo, principalmente nos casos de atraso do relógio. Observou-se também que, independente de o relógio ter sido atrasado ou adiantado, o valor do campo LSN, que é alterado sempre que ocorre uma alteração na entrada MFT, é sempre crescente. Ou seja, quando foi feita a ordenação dos arquivos alterados, inclusive aqueles alterados antes da manipulação do relógio, pelo campo LSN pode-se verificar que essa ordenação refletia a cronologia das operações realizadas, mesmo que os rótulos de tempo não o fizessem.

4.7 Pontos de restauração

O arquivo *filelist.xml*, contido no diretório *C:\WINDOWS\system32\Restore*, por meio de diretivas de inclusão e exclusão, determina o monitoramento de diretórios e extensões de arquivos pela ferramenta de geração de pontos de restauração. Foi constatado, nos testes realizados, que a inclusão de um diretório nesse arquivo não faz com que todos os arquivos contindos nele seram monitorados. Os resultados indicaram que somente os arquivos que possuíam extensões na lista de extensões monitoradas eram processados pela ferramenta de ponto de restauração, mesmo o diretório estando na lista de monitoração. No entanto, quando o diretório de trabalho foi acrescentado na lista de exclusão, nenhum arquivo dentro dele foi monitorado, até mesmo aqueles que possuíam extensões na lista de monitoração.

Dentre os arquivos monitorados, somente foram gravadas cópias dos arquivos que sofreram alterações em seu conteúdo. Arquivos que foram apagados, renomeados, copiados ou movidos para outra pasta e os arquivos que foram criados não geraram registro no ponto de restauração. Dentre os arquivos que tiveram seu conteúdo alterado, foi constatado que a cópia armazenada no ponto de restauração correspondia à ultima modificação do arquivo anterior ao último desligamento. Ou seja, as modificações realizadas antes do desligamento, excetuando-se a última, não foram registradas. Da mesma forma, as alterações posteriores, que ocorreram entre a inicialização da máquina e a criação do ponto de restauração, também não foram registradas. Quanto aos rótulos de tempo desses arquivos, os rótulos do SI apresentavam valor igual aos anteriores à sua alteração. Deve-se ressaltar que o AT (SI) apresentava valor próximo e anterior ao instante da modificação, indicando a atualização desse rótulo de tempo quando da seleção do arquivo, imediatamente antes de sua alteração. Já os rótulos do FN apresentavam conteúdo diverso do arquivo original, possuindo todos o valor igual ao instante da alteração do arquivo.

Foi observado que os arquivos monitorados e copiados para o ponto de restauração encontravam-se sempre no penúltimo ponto de restauração (as pastas referentes aos pontos de restauração tem o formato *RP#*, onde # é um número sequencial) e não no último, como era esperado. As pastas referentes aos pontos de restauração, além de conter a cópia no instante anterior à modificação dos arquivos monitorados, apresentam também uma cópia do Registro, o qual possui informações relevantes da configuração do computador naquele instante bem como outras informações, como por exemplo, dados referentes a dispositivos removíveis inseridos na máquina.

4.8 Transferências de arquivos e pastas do sistema FAT para o sistema NTFS

Em razão da grande maioria dos dispositovos removíveis (*pendrives*, câmeras, celulares, cartões de memória) utilizarem o sistema de arquivos FAT, foram realizados experimentos de transferência de arquivos desse sistema para o sistema de arquivos em estudo, o NTFS. Ressalta-se que não foram realizados estudos referentes à transferência de arquivos do sistema NTFS para o sistema FAT pois foge ao escopo deste trabalho.

4.8.1 Cópia de arquivos e pastas

Arquivos copiados do sistema FAT para o sistema NTFS preservam o tempo de modificação do arquivo original no MT (SI), enquanto que os demais rótulos de tempo armazenam o instante da operação. Já a cópia de pastas faz com que todos os rótulos de tempo da pasta copiada apresentem o tempo da operação. Os arquivos contidos dentro das pastas se comportam da mesma forma como na cópia de arquivos.

Deve-se destacar que nos arquivos copiados de um sistema FAT o rótulo MT (SI), o qual preserva o valor do arquivo original, apresenta as frações de segundo zeradas e o valor dos segundos par.

4.8.2 Movimentação de arquivos e pastas

Na movimentação de arquivos de um sistema FAT para o sistema NTFS foi constatado que o CrT e o MT do SI preservam o valor armazenado no arquivo original, enquanto que os demais rótulos do SI e todos os rótulos do FN apresentam o tempo da movimentação. Da mesma forma como ocorre na cópia de pastas entre esses sistemas de arquivos, pastas movidas do sistema FAT para o sistema NTFS armazenam em todos os seus rótulos de tempo o instante da operação, enquanto que os arquivos nelas contidos se comportam como arquivos movidos.

Foi constatado também que os rótulos de tempo de arquivos que preservam os valores originais (CrT e MT do SI) apresentam as frações de segundo zeradas, sendo que o MT (SI) apresenta o valor dos segundos par.

4.8.3 Ferramenta *SleuthKit*

Durante o processamento dos rótulos de tempo do sistema FAT, alguns arquivos foram processados manualmente e os resultados foram comparados com os obtidos com

a ferramenta *istat* do pacote *sleuthkit* (CARRIER, 2003-2012). Nos casos nos quais o processamento manual resultava em um valor de segundos ímpar para o tempo de criação, a ferramenta *istat* apresentava resultado com um segundo a menos. Nesses casos foram utilizadas a ferramenta *ls* (Free Software Foundation, 1994-1996, 2000-2012) nativa do Linux em uma partição FAT montada e a ferramenta *FTK Imager* (ACCESSDATA, 2010). Ambas forneceram resultados iguais aos obtidos no processamento manual.

Em virtude das inconsistências encontradas foi realizado um estudo mais detalhado do byte referente aos centésimos de segundo do tempo de criação. Foi constatado que, tanto na especificação do sistema FAT (MICROSOFT, 2000) quanto em Carrier (2005), é afirmado que este byte refere-se a décimos de segundo quando na verdade armazena centésimos de segundo. Apesar da nomenclatura estar errada na espeficicação (MICROSOFT, 2000), o intervalo válido indicado, de 0 a 199, está correto. Foi analisado, em seguida, o código fonte da ferramenta *istat* do pacote *sleuthkit* (CARRIER, 2003-2012), versão 3.2.3. Verificou-se que a rotina de tratamento do tempo de criação do sistema FAT testa se o valor armazenado no byte referente aos centésimos de segundo é maior que 100, somando um segundo no tempo de criação em caso positivo. No entanto, deveria ser acrescentado um segundo se o valor fosse maior que 99 e não maior que 100. O autor da ferramenta foi contactado e informado dessa falha.

A análise dos bytes refentes ao tempo de criação mostrou que o byte referente aos centésimos de segundo apresentava somente os valores 0 (0x00) ou 100 (0x64), ou seja, adiciona 0 segundo ou 1 segundo ao tempo de criação. Não foi realizado um estudo mais detalhado, por fugir ao escopo do trabalho, para verificar se sistemas de arquivo FAT criados em outros sistemas operacionais apresentam valores diferentes de 0 ou 100 no referido byte, o que proporcionaria a existência de frações de segundo no tempo de criação.

4.9 Da análise dos índices de diretório

Além da análise dos rótulos de tempo armazenados nos atributos $STANDARD_INFORMATION e $FILE_NAME das entradas MFT, referentes aos arquivos e pastas analisados, foram estudados também os rótulos constantes nos atributos $FILE_NAME das entradas de índice de seus diretórios pais (atributos $INDEX_ROOT e $INDEX_ALLOCATION). Foram comparados os valores constantes nessas entradas com dos demais rótulos de tempo presentes na entrada MFT de cada arquivo ou pasta analisado,

sendo constatado que os valores sempre coincidem com os rótulos do atributo $STANDARD_INFORMATION. Foram realizadas, também, alterações intencionais nos rótulos das entradas de índice de algumas pastas, por meio da alteração dos bytes correspondentes na imagem da máquina virtual do sistema operacional em estudo. Foi verificado, nesse caso, que quando as pastas com entradas de índice alteradas eram acessadas pelo sistema operacional, esses rótulos eram atualizados para os valores constantes no atributo $STANDARD_INFORMATION correspondente. Portanto, foi constatado que o estudo dos rótulos de tempo armazenados nas entradas de índice não traria nenhuma informação nova, pois são cópias fiéis do atributo $STANDARD_INFORMATION das entradas MFT a que se referem.

4.10 Síntese dos resultados das operações com arquivos e pastas

É apresentada nas tabelas 4.2, 4.3, 4.4 e 4.5 uma síntese dos resultados referentes ao comportamento dos rótulos de tempo em operações com arquivos e pastas, detalhados nas seções 4.1, 4.2 e 4.8. Com o intuito de facilitar a consulta por uma operação específica como também possibilitar a comparação de operações com comportamentos semelhantes nos rótulos de tempo, são apresentadas duas tabelas para operações com arquivos, uma ordenada por operação (tabela 4.2) e outra pelos rótulos de tempo (tabela 4.3), e duas tabelas para operações com pastas, uma ordenada por operação (tabela 4.4) e outra pelos rótulos de tempo (tabela 4.5). São apresentadas, também, duas tabelas, uma para arquivos (tabela 4.6) e outra para pastas (tabela 4.7), com características dos rótulos de tempo para cada operação. Essas tabelas são apresentadas, também, em formato maior (paisagem), no apêndice A para facilitar sua visualização e consulta.

Deve-se ressaltar que os resultados apresentados consideram desabilitada a chave do Registro que inibe a atualização do AT (SI), que é a configuração padrão no Windows XP. Caso seja verificado que essa chave esteja habilitada deve-se desconsiderar o AT nas tabelas 4.1 a 4.7.

As colunas "SI"e "FN"apresentam os rótulos de tempo referentes aos atributos $STANDARD_INFORMATION e $FILE_NAME, respectivamente, separados pelo símbolo > quando é possível afirmar que um rótulo possui valor cronologicamente superior a outro e por vírgulas quando não é possível. A coluna "SI x FN"apresenta relações de igualdade ou desigualdade entre os rótulos de tempos dos dois atributos. Na coluna "Tipo"é especificado se os rótulos de tempo se referem a arquivo e pastas ou a subarquivos e

subpastas, ou seja, arquivos e pastas contidos em pastas nais quais foram executadas as operações. A coluna "Operação"determina a operação em questão enquanto que a coluna "Sub operação"especifica alguma subdivisão dessa operação como, por exemplo, movimentação entre volumes diferentes ou no mesmo volume.

Tabela 4.2: Síntese do comportamento dos rótulos de tempo em operações com arquivos - ordenação por operação

SI	FN	SI x FN	Tipo	Operação	Sub operação
Ch>A>Cr,M	Cr,M,Ch,A	Ch,A≠Ch,A	Arquivo	Altera propriedades	
M=Ch=A>Cr	Cr,M,Ch,A	M,Ch,A≠M,Ch,A	Arquivo	Alterar conteúdo	
Cr=A>M,Ch	Cr=M=Ch=A	Cr,A=FN	Arquivo	Cópia	Independente volume
Cr=A>M,Ch	Cr=M=Ch=A	Cr,A=FN	Subarquivo	Cópia	Independente volume
Cr=Ch=A>M	Cr=M=Ch=A	Cr,Ch,A=Cr,Ch,A; M≠M	Arquivo	Cópia	Volume diferente (FAT)
Cr=Ch=A>M	Cr=M=Ch=A	Cr,Ch,A=Cr,Ch,A; M≠M	Subarquivo	Cópia	Volume diferente (FAT)
Cr=M=Ch=A	Cr=M=Ch=A	SI=FN	Arquivo	Criação	
Ch>M=A>Cr	M=Ch=A>Cr	Cr,M,A=Cr,M,A; Ch≠Ch	Arquivo	Download	
Ch>Cr=M=A	Cr=M=Ch=A	Ch=FN	Arquivo	Extração zip	
Ch>A>Cr,M	Cr,M,Ch,A	Cr,M,A=Cr,M,A; Ch≠Ch	Arquivo	Movimentação	Mesmo volume
Ch>Cr,M,A	Cr,M,Ch,A	Ch≠Ch	Subarquivo	Movimentação	Mesmo volume
A>Cr,M,Ch	Cr=M=Ch=A	A=FN	Arquivo	Movimentação	Volume diferente
A>Cr,M,Ch	Cr=M=Ch=A	A=FN	Subarquivo	Movimentação	Volume diferente
Ch=A>Cr,M	Cr=M=Ch=A	Ch,A=Ch,A; Cr,M≠Cr,M	Arquivo	Movimentação	Volume diferente (FAT)
Ch=A>Cr,M	Cr=M=Ch=A	Ch,A=Ch,A; Cr,M≠Cr,M	Subarquivo	Movimentação	Volume diferente (FAT)
Ch>A>Cr,M	Cr,M,Ch,A	Cr,M,A=Cr,M,A; Ch≠Ch	Arquivo	Renomear	
A>Cr,M,Ch	Cr,M,Ch,A	M,Ch,A≠M,Ch,A	Arquivo	Sobrescrita	Cópia (independente volume)
Ch>A>Cr,M	Cr,M,Ch,A	M=M; Ch,A≠Ch,A	Arquivo	Sobrescrita	Move (mesmo volume)
A>Cr,M,Ch	Cr,M,Ch,A	SI≠FN	Arquivo	Sobrescrita	Move (volume diferente)

Tabela 4.3: Síntese do comportamento dos rótulos de tempo em operações com arquivos - ordenação por rótulos de tempo

SI	FN	SI x FN	Tipo	Operação	Sub operação
A>Cr,M,Ch	Cr,M,Ch,A	M,Ch,A≠M,Ch,A	Arquivo	Sobrescrita	Cópia (independente volume)
A>Cr,M,Ch	Cr,M,Ch,A	SI≠FN	Arquivo	Sobrescrita	Move (volume diferente)
A>Cr,M,Ch	Cr=M=Ch=A	A=FN	Arquivo	Movimentação	Volume diferente
A>Cr,M,Ch	Cr=M=Ch=A	A=FN	Subarquivo	Movimentação	Volume diferente
Ch=A>Cr,M	Cr=M=Ch=A	Ch,A=Ch,A; Cr,M≠Cr,M	Arquivo	Movimentação	Volume diferente (FAT)
Ch=A>Cr,M	Cr=M=Ch=A	Ch,A=Ch,A; Cr,M≠Cr,M	Subarquivo	Movimentação	Volume diferente (FAT)
Ch>A>Cr,M	Cr,M,Ch,A	Ch,A≠Ch,A	Arquivo	Altera propriedades	
Ch>A>Cr,M	Cr,M,Ch,A	Cr,M,A=Cr,M,A; Ch≠Ch	Arquivo	Movimentação	Mesmo volume
Ch>A>Cr,M	Cr,M,Ch,A	Cr,M,A=Cr,M,A; Ch≠Ch	Arquivo	Renomear	
Ch>A>Cr,M	Cr,M,Ch,A	M=M; Ch,A≠Ch,A	Arquivo	Sobrescrita	Move (mesmo volume)
Ch>Cr,M,A	Cr,M,Ch,A	Ch≠Ch	Subarquivo	Movimentação	Mesmo volume
Ch>Cr=M=A	Cr=M=Ch=A	Ch=FN	Arquivo	Extração zip	
Ch>M=A>Cr	M=Ch=A>Cr	Cr,M,A=Cr,M,A; Ch≠Ch	Arquivo	Download	
Cr=A>M,Ch	Cr=M=Ch=A	Cr,A=FN	Arquivo	Cópia	Independente volume
Cr=A>M,Ch	Cr=M=Ch=A	Cr,A=FN	Subarquivo	Cópia	Independente volume
Cr=Ch=A>M	Cr=M=Ch=A	Cr,Ch,A=Cr,Ch,A; M≠M	Arquivo	Cópia	Volume diferente (FAT)
Cr=Ch=A>M	Cr=M=Ch=A	Cr,Ch,A=Cr,Ch,A; M≠M	Subarquivo	Cópia	Volume diferente (FAT)
Cr=M=Ch=A	Cr=M=Ch=A	SI=FN	Arquivo	Criação	
M=Ch=A>Cr	Cr,M,Ch,A	M,Ch,A≠M,Ch,A	Arquivo	Alterar conteúdo	

Tabela 4.4: Síntese do comportamento dos rótulos de tempo em operações com pastas - ordenação por operação

SI	FN	SI x FN	Tipo	Operação	Sub operação
A>Cr,M,Ch	Cr,M,Ch,A	A≠A	Pasta	Altera conteúdo arquivo	
Ch=A>Cr,M	Cr,M,Ch,A	Ch,A≠Ch,A	Pasta	Altera propriedades	
M=Ch=A>Cr	Cr,M,Ch,A	M,Ch,A≠M,Ch,A	Pasta	Alterar conteúdo	
Cr=M=Ch=A	Cr=M=Ch=A	SI=FN	Pasta	Cópia	Independente volume
Cr=M=Ch=A	Cr=M=Ch=A	SI=FN	Subpasta	Cópia	Independente volume
Cr=M=Ch=A	Cr=M=Ch=A	SI=FN	Pasta	Cópia	Volume diferente (FAT)
Ch>Cr=M=A	Cr=M=Ch=A	Cr,M,A=FN	Pasta	Criação	
Cr=M=Ch=A	Cr=M=Ch=A	SI=FN	Pasta	Extração zip	
Ch=A>Cr,M	Cr,M,Ch,A	Cr,M=Cr,M; Ch,A≠Ch,A	Pasta	Movimentação	Mesmo volume
A>Cr,M,Ch	Cr,M,Ch,A	A≠A	Subpasta	Movimentação	Mesmo volume
Cr=M=Ch=A	Cr=M=Ch=A	SI=FN	Pasta	Movimentação	Volume diferente
Cr=M=Ch=A	Cr=M=Ch=A	SI=FN	Subpasta	Movimentação	Volume diferente
Cr=M=Ch=A	Cr=M=Ch=A	SI=FN	Pasta	Movimentação	Volume diferente (FAT)
Ch=A>Cr,M	Cr,M,Ch,A	Cr,M=Cr,M; Ch,A≠Ch,A	Pasta	Renomear	
M=Ch=A>Cr	Cr,M,Ch,A	M,Ch,A≠M,Ch,A	Pasta	Sobrescrita	Cópia (mais arquivos origem)
Cr,M,Ch,A	Cr,M,Ch,A		Pasta	Sobrescrita	Cópia (menos arquivos origem)
M=Ch=A>Cr	Cr,M,Ch,A	M,Ch,A≠M,Ch,A	Pasta	Sobrescrita	Movimentação (mais arquivos origem)
M=Ch=A>Cr	Cr,M,Ch,A	M,Ch,A≠M,Ch,A	Pasta	Sobrescrita	Movimentação (menos arquivos origem)

Tabela 4.5: Síntese do comportamento dos rótulos de tempo em operações com pastas - ordenação por rótulos de tempo

SI	FN	SI x FN	Tipo	Operação	Sub operação
A>Cr,M,Ch	Cr,M,Ch,A	A≠A	Pasta	Altera conteúdo arquivo	
A>Cr,M,Ch	Cr,M,Ch,A	A≠A	Subpasta	Movimentação	Mesmo volume
Ch=A>Cr,M	Cr,M,Ch,A	Ch,A≠Ch,A	Pasta	Altera conteúdo arquivo	
Ch=A>Cr,M	Cr,M,Ch,A	Ch,A≠Ch,A	Pasta	Altera propriedades	
Ch=A>Cr,M	Cr,M,Ch,A	Cr,M=Cr,M; Ch,A≠Ch,A	Pasta	Movimentação	Mesmo volume
Ch=A>Cr,M	Cr,M,Ch,A	Cr,M=Cr,M; Ch,A≠Ch,A	Pasta	Renomear	
Ch>Cr=M=A	Cr=M=Ch=A	Cr,M,A=FN	Pasta	Criação	
Cr,M,Ch,A	Cr,M,Ch,A		Pasta	Sobrescrita	Cópia (menos arquivos origem)
Cr=M=Ch=A	Cr=M=Ch=A	SI=FN	Pasta	Cópia	Independente volume
Cr=M=Ch=A	Cr=M=Ch=A	SI=FN	Subpasta	Cópia	Independente volume
Cr=M=Ch=A	Cr=M=Ch=A	SI=FN	Pasta	Cópia	Volume diferente (FAT)
Cr=M=Ch=A	Cr=M=Ch=A	SI=FN	Pasta	Extração zip	
Cr=M=Ch=A	Cr=M=Ch=A	SI=FN	Pasta	Movimentação	Volume diferente
Cr=M=Ch=A	Cr=M=Ch=A	SI=FN	Subpasta	Movimentação	Volume diferente
Cr=M=Ch=A	Cr=M=Ch=A	SI=FN	Pasta	Movimentação	Volume diferente (FAT)
M=Ch=A>Cr	Cr,M,Ch,A	M,Ch,A≠M,Ch,A	Pasta	Alterar conteúdo	
M=Ch=A>Cr	Cr,M,Ch,A	M,Ch,A≠M,Ch,A	Pasta	Sobrescrita	Cópia (mais arquivos origem)
M=Ch=A>Cr	Cr,M,Ch,A	M,Ch,A≠M,Ch,A	Pasta	Sobrescrita	Movimentação (mais arquivos origem)
M=Ch=A>Cr	Cr,M,Ch,A	M,Ch,A≠M,Ch,A	Pasta	Sobrescrita	Movimentação (menos arquivos origem)

Tabela 4.6: Detalhamento dos rótulos de tempo em operações com arquivos

Tipo	Operação	Sub operação	Características
Arquivo	Altera propriedades		Ch(SI),AT(SI) = tempo alteração
Arquivo	Alterar conteúdo		M(SI),Ch(SI),A(SI) = tempo modificação
Arquivo	Cópia	Independente volume	Cr(SI),A(SI),FN = tempo cópia
Subarquivo	Cópia	Independente volume	Cr(SI),A(SI),FN = tempo cópia
Arquivo	Cópia	Volume diferente (FAT)	Cr(SI),Ch(SI),A(SI),FN = tempo copia; M(SI) igual arquivo original (frac. seg. zeradas)
Subarquivo	Cópia	Volume diferente (FAT)	Cr(SI),Ch(SI),A(SI),FN = tempo copia; M(SI) igual arquivo original (frac. seg. zeradas)
Arquivo	Criação		SI,FN = tempo criação
Arquivo	Download		M(SI e FN),Ch(SI e FN),A(SI e FN) = fim do download
Arquivo	Extração zip		Ch(SI),FN = tempo extração; Cr(SI),M(SI),A(SI) = M(SI) do arquivo original arrendondado para cima quando ímpares
Arquivo	Movimentação	Mesmo volume	Ch(SI),AT(SI e FN) = tempo movimentação
Subarquivo	Movimentação	Mesmo volume	Ch(SI) = tempo movimentação
Arquivo	Movimentação	Volume diferente	A(SI),FN = tempo movimentação
Subarquivo	Movimentação	Volume diferente	A(SI),FN = tempo movimentação
Arquivo	Movimentação	Volume diferente (FAT)	Ch(SI),A(SI),FN = tempo movimentação; Cr(SI),M(SI) iguais arquivo original (frac. seg. zeradas)
Subarquivo	Movimentação	Volume diferente (FAT)	Ch(SI),A(SI),FN = tempo movimentação; Cr(SI),M(SI) iguais arquivo original (frac. seg. zeradas)
Arquivo	Renomear		Ch(SI),AT(SI e FN) = tempo renomeio
Arquivo	Sobrescrita	Cópia (independente volume)	A(SI) = tempo copia; M(SI),Ch(SI) = arquivo que sobrescreveu
Arquivo	Sobrescrita	Move (mesmo volume)	Ch(SI) = tempo movimentação; M(SI),FN = arquivo que sobrescreveu
Arquivo	Sobrescrita	Move (volume diferente)	A(SI) = tempo movimentação; Cr(SI),M(SI),Ch(SI) = arquivo que sobrescreveu

Tabela 4.7: Detalhamento dos rótulos de tempo em operações com pastas

Tipo	Operação	Sub operação	Características
Pasta	Altera conteúdo arquivo		A(SI) = tempo alteração
Pasta	Altera conteúdo arquivo		Ch(SI),A(SI) = tempo alteração
Pasta	Altera propriedades		Ch(SI),A(SI) = tempo alteração
Pasta	Alterar conteúdo		M(SI),Ch(SI),A(SI) = tempo modificação
Pasta	Cópia	Independente volume	SI,FN = tempo cópia
Subpasta	Cópia	Independente volume	SI,FN = tempo cópia
Pasta	Cópia	Volume diferente (FAT)	SI,FN = tempo cópia
Pasta	Criação		Cr(SI),M(SI),A(SI),FN = tempo criação
Pasta	Extração zip		SI,FN = tempo extração
Pasta	Movimentação	Mesmo volume	Ch(SI),A(SI) = tempo movimentação
Subpasta	Movimentação	Mesmo volume	A(SI) = tempo movimentação
Pasta	Movimentação	Volume diferente	SI,FN = tempo movimentação
Subpasta	Movimentação	Volume diferente	SI,FN = tempo movimentação
Pasta	Movimentação	Volume diferente (FAT)	SI,FN = tempo movimentação
Pasta	Renomear		Ch(SI),A(SI) = tempo renomeio
Pasta	Sobrescrita	Cópia (mais arquivos origem)	M(SI),Ch(SI),A(SI) = tempo cópia
Pasta	Sobrescrita	Cópia (menos arquivos origem)	
Pasta	Sobrescrita	Movimentação (mais arquivos origem)	M(SI),Ch(SI),A(SI) = tempo movimentação
Pasta	Sobrescrita	Movimentação (menos arquivos origem)	M(SI),Ch(SI),A(SI) = tempo movimentação

5 DISCUSSÃO DOS RESULTADOS

O conhecimento da forma como se comportam rótulos de tempo em um sistema de arquivos é de fundamental importância para se estabelecer uma linha de tempo de arquivos e pastas de interesse, bem como para confirmar ou refutar a possibilidade de adulteração em evidências digitais. Os experimentos realizados que envolveram operações com arquivos e pastas, simulando comportamentos comuns a usuários e a certas rotinas do sistema operacional, apresentaram resultados compatíveis com estudos anteriores.

No entanto, foram constadas divergências da literatura (CHOW et al., 2007; BANG et al., 2009; BANG; YOO; LEE, 2011) em algumas operações, bem como, em outras, foram analisadas subdivisões dessas operações, o que não havia sido detalhado nesses trabalhos. Nos casos nos quais os experimentos mostraram resultados diferentes daqueles encontrados na literatura, os testes foram repetidos, sendo confirmados, em todos os casos, os resultados iniciais. Por apresentarem repetibilidade dos resultados e, em algumas situações, simularem mais possibilidades do que os estudos anteriores, acredita-se que os resultados obtidos neste trabalho relativos a operações de arquivos e pastas representam de forma mais completa o comportamento dos rótulos de tempo em um sistema NTFS com Windows XP.

Chow et al. (2007) apresentam regras genéricas para operações com arquivos, não detalhando o comportamento dos rótulos de tempo para cada caso específico, mas sugerindo um conjunto de regras para serem aplicadas em qualquer situação para determinadas operações. Além de ser mais genérico, o referido estudo deixou de contemplar o rótulo de tempo de última modificação da MFT (ChT), o qual foi criado somente quando da migração do sistema FAT para o NTFS, além de analisar somente os rótulos presentes no atributo $STANDARD_INFORMATION. Mesmo deixando de analisar essas importantes fontes de informação e o comportamento dos rótulos de tempo das pastas, o estudo de Chow et al. (2007) se presta a ser um balizador para experimentos mais detalhados, os quais foram realizados em Bang et al. (2009) e Bang, Yoo e Lee (2011) e no presente trabalho, sendo cada operação específica discutida a seguir.

5.1 Criação de arquivos e pastas

A criação de arquivos gera uma configuração muito característica nos rótulos de tempo, em que todos apresentam o mesmo valor nos dois atributos analisados. Esse resultado e os referentes à alteração de arquivos e cópia de arquivos estão de acordo com a primeira regra de Chow et al. (2007), a qual afirma que, quando o CrT e o MT do SI são iguais, o arquivo não foi modificado nem copiado. No entanto, com os resultados obtidos neste trabalho, compatíveis com os mostrados em Bang, Yoo e Lee (2011), constatou-se que a configuração dos rótulos de tempo, quando da criações de um arquivo, apresenta uma configuração única, possibilitando uma afirmação conclusiva sobre o seu estado.

No que se refere à criação de pastas, o resultado obtido é semelhante ao da criação de arquivos, com a diferença que o ChT (SI) apresenta alguns segundos a mais que os demais rótulos. Bang, Yoo e Lee (2011) afirmam que o comportamento é igual ao da criação de arquivos. O comportamento simulado em nosso estudo, que nos parece mais natural ao usuário, efetua a criação de uma pasta no Windows Explorer por meio do mouse, nomeando-a na sequência e finalizando a operação. Foi constatado que a diferença observada no ChT (SI) deve-se justamente ao intervalo em que o usuário escreve o nome da pasta e aperta a tecla Enter. Conclui-se, portanto, que Bang, Yoo e Lee (2011) simularam a criação de pastas com o nome padrão o que não causa a alteração do rótulo ChT (SI).

5.2 Cópia de arquivos e pastas

O comportamento dos rótulos de tempo em cópias de arquivos não se modifica pelo método de cópia (copiar e colar ou *drag and drop*) nem pela origem do arquivo (mesmo volume ou entre volumes), sendo os resultados obtidos compatíveis com os de Bang, Yoo e Lee (2011). Apesar de, na cópia de arquivos, o CrT (SI) ser superior ao MT (SI), deve-se ter cautela em relação às regras propostas por Chow et al. (2007) (segunda e terceira regras), que atribuem esse cenário à movimentação de outro volume ou à cópia de arquivos. Na seção 5.3, será mostrado que essas regras não se aplicam a movimentação de outro volume e, para o caso de cópia, essa situação somente indica que o arquivo foi copiado, não sendo necessariamente a última operação executada sobre o arquivo como, por exemplo, no caso em que um arquivo foi copiado e em seguida movimentado. A análise de todos os rótulos de tempo disponíveis nos permite identificar uma configuração única de rótulos de tempo que configura uma cópia, que se caracteriza pela igualdade entre os rótulos do FN e os rótulos CrT e AT do SI, além destes serem superiores aos demais.

No caso de cópia de pastas e subpastas, os resultados obtidos foram indiferentes em relação ao método de cópia e à origem da pasta. Todos os rótulos de tempo dos atributos SI e FN apresentam o mesmo valor, situação semelhante à observada quando da movimentação de pastas e subpastas provenientes de um volume diferente (seção 5.3) e da extração de um arquivo *zip* (seção 5.6). Em vista desse resultado, somente é possível distinguir se uma pasta foi copiada, movimentada de outro volume ou extraída de um arquivo compactado pela observação dos rótulos de tempo de seus arquivos. O comportamento dos rótulos de tempo em cópia de pastas é muito semelhante à da criação de pastas, o qual se destaca pela ligeira diferença do ChT (SI) quando o usuário atribui um nome à pasta. Os resultados obtidos neste estudo divergem de Bang, Yoo e Lee (2011) em relação à cópia de subpasta no mesmo volume e de cópia de pastas provenientes de outro volume, no qual é afirmado que as pastas mantêm o tempo original nos rótulos MT e ChT do SI no primeiro caso e nos ChT e AT do SI no último. É afirmado por Bang, Yoo e Lee (2011), também, que o AT (SI) da pasta original é atualizado para o tempo de cópia, o que não foi observado nos testes realizados.

5.3 Movimentação e renomeio de arquivos e pastas

Arquivos movimentados apresentam comportamentos diferentes para operações no mesmo volume e entre volumes diferentes. Os experimentos realizados mostraram que o comportamento dos rótulos de tempo nas operações de movimentação no mesmo volume e de renomeio alteram os rótulos de tempo da mesma maneira, o que seria esperado, pois em uma movimentação somente são alterados os metadados do arquivo. Nessa situação ocorre um fato interessante para a análise forense, pois o AT (SI) do arquivo é atualizado quando o arquivo é acessado, instantes antes da movimentação, sendo copiado, juntamente com o restante dos rótulos do SI, para o atribulo FN. Dessa forma, o tempo da movimentação fica registrado tanto nos AT do SI e do FN, quanto no ChT do SI, com alguns segundos de diferença. A cópia dos rótulos do SI para o FN permite separar as operações de movimentação no mesmo volume e de renomeio das operações de alteração de propriedades (seção 5.4) e sobrescrita por meio de movimentação no mesmo volume (seção 5.5), que apresentam comportamento igual se analisarmos somente o atributo SI. Deve-se atentar para o fato de que arquivos contidos dentro de pastas movidas somente têm alterado seu ChT (SI), mantendo os demais rótulos inalterados. Os resultados de Bang, Yoo e Lee (2011) relativos ao renomeio de arquivos e a arquivos dentro de pastas movidas corroboram os obtidos neste trabalho. No entanto, quando refere-se à movimentação de arquivos no mesmo volume, não é assinalado que os rótulos de tempo do atributo SI são copiados para o atributo FN. Além

disso, é dito que a alteração do AT (SI) somente ocorre para arquivos não residentes, e não para ambos os casos, como foi constatado neste trabalho.

O comportamento dos rótulos de tempo na movimentação de arquivo entre volumes diferentes é muito similar ao observado na cópia de arquivos. No entanto, arquivos movidos não têm seu CrT (SI) alterado para o instante da cópia, fato esse que permite diferenciar entre as duas situações, visto que, na cópia, o CrT (SI) será posterior ao MT (SI), o que não ocorrerá na movimentação. Diferentemente da movimentação no mesmo volume, o comportamento de arquivos dentro de pastas movidas entre volumes apresentam o mesmo comportamento de arquivos movidos entre volumes. Os resultados obtidos foram iguais para arquivos residentes e não residentes e para diferentes métodos de movimentação. Bang, Yoo e Lee (2011) dividem o teste de movimentação de arquivos entre volumes diferentes em dois métodos: *drag and drop* e recortar e colar. Os resultados para o método *drag and drop* foram compatíveis com os obtidos neste estudo para a cópia de arquivos e não para movimentação. No Windows XP, quando arquivos são arrastados de um volume para outro, o comportamento padrão é a realização de cópia e não a movimentação, ao contrário do que ocorre entre arquivos no mesmo volume. Para alterar esse comportamento é necessário que o usuário mantenha pressionanda a tecla *Shift*. Considerando esse comportamento padrão do sistema e os resultados apresentados por Bang, Yoo e Lee (2011), pode-se concluir que a operação de movimentação entre volumes realizada por Bang, Yoo e Lee (2011) foi feita de forma incorreta. Já os resultados referentes ao método recortar e colar estão incompletos, pois apesar do autor citar que os rótulos CrT e MT do SI se mantêm, não informa que o ChT (SI) também se mantém e que os rótulos do atributo FN são alterados para o tempo da movimentação.

Assim como arquivos, pastas também se comportam de maneira diferente quando movidas no mesmo volume e entre volumes diferentes. O comportamento dos rótulos de tempo de pastas movidas no mesmo volume é igual ao de pastas renomeadas. Nesses dois casos, os rótulos do SI são copiados para o FN, da mesma forma como ocorre no caso de movimentação no mesmo volume e renomeio de arquivos. No entanto, para pastas, o AT (SI) copiado para o FN não é o atualizado, portanto não reflete o tempo da operação. Para determinar o tempo da movimentação ou renomeio, deve-se consultar o ChT e o AT do SI. Esse comportamento dos rótulos de tempo é único para as operações de movimentação e renomeio e para fazer a distinção entre uma e outra deve-se verificar outros elementos, como por exemplo os rótulos de arquivos e subpastas da pasta analisada. As subpastas contidas em pastas movidas somente têm

alterado o seu AT (SI), mantendo os demais rótulos inalterados, enquanto que arquivos contidos nas pastas somente têm atualizado seu ChT (SI), conforme já dito no início desta seção. Os resultados obtidos por Bang, Yoo e Lee (2011) para os casos de movimentação e renomeio de pastas foram compatíveis com os obtidos neste trabalho. No entanto, o referido estudo ficou limitado à movimentação dentro do mesmo volume, não apresentando resultados para volumes diferentes.

Os resultados para movimentação de pastas entre volumes diferentes assemelha-se à cópia de pastas, conforme citado na seção 5.2.

5.4 Alteração de propriedades e conteúdos de arquivos e pastas

A alteração das propriedades de arquivos no NTFS gera modificações nos rótulos de tempo do atributo SI da mesma forma como ocorre na movimentação no mesmo volume, no renomeio (seção 5.3) e na sobrescrita por meio de movimentação no mesmo volume (seção 5.5). No entanto, na operação de alteração de propriedades, os rótulos do FN não são alterados, o que permite diferenciá-la das demais. Deve-se atentar para o caso de arquivos contidos dentro de pastas movimentadas no mesmo volume (seção 5.3), que só se diferenciam deste caso pela não alteração do AT (SI), o que pode ser de difícil detecção quando o arquivo é acessado posteriormente. Os resultados deste trabalho referentes a esse tópico foram compatíveis com os de Bang, Yoo e Lee (2011).

Similarmente ao que ocorre com arquivos, o comportamento dos rótulos de tempo do SI na alteração de propriedades de pastas é igual ao renomeio e à movimentação de pastas no mesmo volume (seção 5.3). Para diferenciar o caso de alteração de propriedade dos demais devemos verificar os rótulos do FN, pois, nesse caso, eles não são alterados, enquando que nos outros dois casos os valores constantes do SI antes da operação são armazenados no FN. A alteração de conteúdo de arquivos dentro de pastas provoca alterações nos rótulos de tempo, em alguns casos, idênticas às observadas na alteração de propriedades de pasta, sendo necessário verificar se há algum arquivo com características de alteração de conteúdo no instante de tempo avaliado para distinguir os dois casos. Os resultados para alteração de propriedades de pastas deste trabalho foram compatíveis com os de Bang, Yoo e Lee (2011).

Nos experimentos com os aplicativos *Notepad* e *Wordpad* foram constatados que o MT, ChT e AT do SI são atualizados para o instante da alteração do conteúdo do arquivo, permanecendos os demais inalterados. Esse configuração de rótulos de tempo

é única, permitindo distiguir esse caso dos demais. Bang, Yoo e Lee (2011) afirmam que o comportamento dos rótulos de tempo na modificação de arquivos varia com o aplicativo, não informando um comportamento para nenhum caso específico.

A alteração de conteúdo de arquivos gera alterações nos rótulos de tempo das pastas em que estão contidas. Foi observado dois comportamentos distintos para essa situação. Em um caso, somente o AT do SI é alterado para o tempo da modificação enquanto que, em outro, ambos AT e ChT do SI são atualizados. Foram testadas situações de aumento e redução de conteúdo de arquivos residentes e não residentes, não sendo obtido êxito em descobrir o que provoca essa diferença de comportamento. A modificação dos rótulos de tempo no primeiro caso citado é igual ao da movimentação de subpastas no mesmo volume (seção 5.3), enquanto que, no segundo caso, é igual ao da alteração de propriedades da pasta, conforme apresentado no início desta seção. Os resultados de Bang, Yoo e Lee (2011) citam somente o caso de alteração do ChT e AT do SI para o tempo da alteração.

A alteração de conteúdo de pastas, ou seja, adição ou remoção de arquivos ou subpastas, provoca alterações nos rótulos de tempo da mesma forma como ocorre em alguns casos de sobrescrita de pasta, os quais serão discutidos na seção 5.5. Esses resultados são compatíveis com os obtidos por Bang, Yoo e Lee (2011).

5.5 Sobrescrita de arquivos e pastas

Arquivos sobrescritos apresentam comportamentos diferentes em seus rótulos de tempo dependendo do modo de sobrescrita e se provenientes de volumes diferentes ou do mesmo volume. No caso de sobrescrita por meio de cópia, independentemente da origem do arquivo, o AT (SI) armazena o tempo da operação e o MT e o ChT do SI são copiados do arquivo que sobrescreveu, enquanto que o FN não é alterado. Nessa situação, teremos uma diferença entre os valores dos rótulos MT e ChT dos dois atributos, o que a diferencia da movimentação de arquivos entre volumes diferentes (seção 5.3), já que os dois casos possuem cronologia dos rótulos de tempo iguais em ambos atributos. No caso de o MT e o ChT do SI serem iguais e superiores ao CrT, a sobrescrita de arquivos por meio de cópia pode ser confundida com a alteração de conteúdo de arquivo (seção 5.4) seguida de um acesso posterior, o que atualizaria o AT (SI). Para descartar essa possibilidade seria necessário encontrar outro arquivo com o mesmo nome e rótulos MT e ChT do SI. Nesse caso, confirma-se a sobrescrita apesar de não ser possível determinar qual arquivo foi sobrescrito, pois o AT do arquivo que

sobrescreveu pode ter sido atualizado posteriormente, apresentando um valor superior ao do arquivo sobrescrito.

A sobrescrita por meio de movimentação de arquivos proveniente de volumes diferentes apresenta comportamento similar ao da sobrescrita por meio de cópia, diferenciando-se desta pela cópia do CrT (SI) do arquivo de origem. Esse fato permite diferenciar as duas situações, pois na sobrescrita por meio de movimentação teremos diferença entre todos os rótulos do SI e do FN, enquanto que na sobrescrita por meio de cópia o CrT dos dois atributos é igual.

A sobrescrita por meio de movimentação de arquivos no mesmo volume apresenta alteração dos rótulos de tempo muito semelhante aos casos de renomeio, movimentação no mesmo volume e alteração de propriedades (seções 5.3 e 5.4). O que diferencia esse caso da alteração de propriedades é a igualdade entre o MT do SI e do FN, que são copiados do arquivo que sobrescreveu, o que não ocorre na alteração de propriedades. Já o que a diferencia dos outros dois casos e torna-a singular é a manutenção do CrT (SI) do arquivo sobrescrito, o qual fica diferente do CrT do FN, que é copiado do arquivo que o sobrescreveu, e a diferença entre o tempo de acesso do SI e do FN.

Os experimentos de Bang, Yoo e Lee (2011) relativos à sobrescrita de arquivos somente contemplaram as situações de movimentação, não sendo informada se entre volumes diferentes ou no mesmo volume. É afirmado que os rótulos AT e ChT do arquivo que sobrescreveu são copiados para o arquivo sobrescrito e que o AT indica o tempo da operação. Neste trabalho foi constatado que o AT (SI) somente armazena o tempo da operação na movimentação entre volumes diferentes e que, nesse caso, os demais rótulos do SI são copiados do arquivo que sobrescreveu e não somente o ChT. Na movimentação dentro do mesmo volume os resultados obtidos não são compatíveis com essas afirmações.

A sobrescrita de pastas por meio de movimentação, independente se a pasta de origem possui mais ou menos arquivos, e por meio de cópia, com mais arquivos na pasta de origem, apresentam alterações dos rótulos de tempo iguais ao caso de alteração de conteúdo de pastas (seção 5.4). A sobrescrita pode ser diferenciada da alteração de conteúdo pela análise dos arquivos constantes nas pastas, pois no caso de sobrescrita, os arquivos apresentam comportamento igual ao caso de sobrescrita de arquivos, enquanto que na alteração de pastas ou haverão arquivos ou pastas com rótulos característicos de criação, com valores iguais aos MT, ChT e AT do SI da pasta, ou não haverá

arquivos com rótulos iguais aos da pasta, indicando deleção. Já a diferenciação entre a sobrescrita por meio de movimentação ou cópia de pastas pode ser feita pela análise dos rótulos dos arquivos dentro da pasta, pois os arquivos se comportam diferentemente quando da sobrescrita por cópia ou movimentação.

Para o caso de sobrescrita por meio de cópia com menos arquivos na origem não foram constatadas alterações nos rótulos de tempo da pasta, não sendo possível, portanto, afirmar acerca de operações pela análise de seus rótulos de tempo, restando somente a possibilidade de análise de seus arquivos.

Os resultados de Bang, Yoo e Lee (2011) afirmam não haver alteração nos rótulos de tempo das pastas, o que indica que foram realizados somente testes de sobrescrita por meio de cópia com menos arquivos na origem.

5.6 Extração de arquivos e pastas compactados

Arquivos extraídos de *containers* compactados em formato *zip* apresentam alterações em seus rótulos de tempo que permitem determinar o instante da extração, bem como o valor do tempo de modificação do arquivo original. A configuração dos rótulos de tempo desses arquivos é única, comparada com os demais testes realizados, o que permite identificar essa operação específica. Um fato interessante a ser ressaltado é que os rótulos CrT, MT e AT do SI, os quais armazenam o tempo de modificação do arquivo original, apresentam as frações de segundo zeradas e segundos pares, o que facilita a identificação desses arquivos. Essa característica dos rótulos de tempo de possuírem as frações zeradas e os segundos pares, também ocorre na transferência de arquivos de um sistema FAT para o NTFS, no entanto no segundo caso, detalhado na seção 5.12, o AT não possui essa configuração e os rótulos CrT e MT não são necessariamente iguais. Os resultados obtidos neste estudo divergem dos resultados apresentandos por Chow et al. (2007), quando ele afirma que o tempo de modificação é anterior ao de criação e que os arquivos apresentam tempo de criação próximos. Nos resultados obtidos, o CrT e o MT do SI de um arquivo são iguais e os arquivos extraídos de um *container zip* apresentam ChT (SI) iguais ou próximos. Já pastas extraídas de um arquivo *zip* apresentam alterações dos rótulos de tempo semelhante à criação de pastas, enquanto que os arquivos contidos nessas pastas se comportam como arquivos extraídos de um arquivo *zip*.

5.7 *Download* de arquivos e pastas

Arquivos baixados da Internet utilizando-se um navegador apresentam rótulos de tempo compatíveis com operações sequenciais de criação, alteração de conteúdo e renomeio, o que é compreensível, pois no início do *download* o arquivo é criado com um nome temporário. A medida que o conteúdo é baixado o arquivo tem seu conteúdo alterado e ao fim do *download* o arquivo é renomeado para o nome correto. As alterações nos rótulos de tempo causadas por essas operações sequenciais realizadas em curto espaço de tempo permite individualizar esses arquivos em relação às demais operações. Arquivos e pastas transferidos de compartilhamentos na rede se comportam como arquivos e pastas copiados de outro volume (seção 5.2). Os resultados de *download* de arquivos da Internet não foram compatíveis com os resultados de Chow et al. (2007) que afirmam que o CrT e o MT do SI são iguais nessa operação.

5.8 Pré visualização de arquivos de imagem e varredura com antivírus e com *Windows Media Player*

A pré visualização de arquivos de imagem e de vídeo causa a atualização de seus rótulos AT (SI). Quando essa pré visualização é realizada em uma pasta que contém mais de um arquivo desse tipo, seus tempos de atualização serão muito próximos, o que nos permite identificar essa situação se esse comportamento não se repetir em outros arquivos multimídia, conforme a regra 5 de Chow et al. (2007). Caso vários arquivos de multimídia no volume possuam valores próximos de AT (SI), e também de ChT (SI), é possível que tenham sido varridos por aplicativos que criam bibliotecas de multimídia como, por exemplo, o *Windows Media Player*. Esse aplicativo especificamente possui um arquivo com o nome de todos os arquivos adicionados à sua biblioteca, o que pode reforçar essa suposição. Já a varredura de arquivos por programas antivírus apresentou resultados diferentes dependendo do aplicativo analisado. Para um caso foi observado o comportamento descrito por Chow et al. (2007), que afirma que ocorre atualização do AT (SI) quando da varredura pelo antivírus. No entanto, em outros casos não foram contantadas alterações nos rótulos de tempo em função da varredura por antivírus. Portanto, a alteração de arquivos por antivírus não apresenta um comportamento determinístico, sendo dependente do aplicativo.

5.9 Considerações sobre o tempo de último acesso

Deve-se ressaltar que os resultados e análises referentes às operações de arquivos e pastas apresentados neste trabalho consideram que a chave do Registro que inibe a

atualização do AT (SI) está desabilitada, que é a configuração padrão no Windows XP. Portanto, é importante que, antes da análise dos rótulos de tempo, seja verificada essa chave do Registro para confirmar seu valor. Caso seja constatado que a atualização do AT (SI) esteja desabilitada deve-se desconsiderar esse rótulo de tempo na análise. No entanto, caso essa situação ocorra, ainda é possível realizar a análise temporal, pois a maioria das características que individualizam uma operação da outra não dependem do AT (SI). E mesmo que a atualização do AT (SI) esteja ativa, deve-se ter cautela com esse rótulo de tempo, pois devido à facilidade com que ele é atualizado, o seu valor pode corresponder ao instante de um acesso relativo a uma visualização posterior à última operação realizada sobre o arquivo ou pasta e não à operação à propriamente dita.

5.10 Manipulações intencionais dos rótulos de tempo e do relógio do sistema

Os programas destinados à manipulação intencional de arquivos avaliados neste estudo apresentam limitações na manipulação dos rótulos de tempo. Dois deles possibilitaram a alteração dos rótulos CrT, MT e AT do SI, enquanto que os outros dois possibilitaram somente a alteração dos rótulos CrT e MT do SI. Além disso, todos registram no ChT (SI) e alguns também no AT (SI) o instante da alteração intencional. Nenhum deles possibilitou a alteração dos rótulos de tempo do atributo FN.

Para que uma alteração intencional não seja detectada por uma análise temporal, ela deveria obedecer algum dos padrões referentes às operações de arquivos detalhandos neste estudo. Em quase todas essas operações há relações de igualdade entre alguns rótulos do SI e do FN, o que impossibilitaria o mascaramento de alguma dessas operações por um impostor, pois não é possível alterar os rótulos do FN com essas ferramentas. Além disso, a alteração automática do rótulo ChT (SI) (e em alguns casos do AT do SI) para o instante da operação, influencia a ordem cronológica entre os rótulos do SI, que também deveria obedecer o padrão referente a uma das operações. Finalmente, a alteração dos rótulos de tempo para um instante anterior à criação do arquivo não seria viável, pois os rótulos do FN seriam posteriores aos do SI, o que é impossível. Por esses motivos, acredita-se que seja possível detectar, em uma análise temporal, arquivos com rótulos de tempo alterados intencionalmente por essas ferramentas.

Os resultados de manipulação de arquivos com alterações do relógio do sistema mostraram que uma análise do LSN dos arquivos analisados é de extrema importância. A

comparação dos rótulos de tempo de arquivos sob análise com outros arquivos que possuam LSN próximos serve para verificar se esses arquivos estão com rótulos de tempo consistentes com os demais arquivos do sistema. Como o LSN é atualizado sempre que a MFT é alterada, ele reflete o instante de alteração do rótulo de tempo alterado mais recentemente, sendo um indicador da ordem de alteração de arquivos, conforme indicado por Carrier (2005). Dessa forma, caso o arquivo tenha sido alterado com o relógio manipulado, o LSN desse arquivo não estará de acordo com os demais arquivos com LSN próximos, pois o seu rótulo de tempo mais recente não será próximo dos rótulos mais recentes dos demais arquivos. Outra forma de detecção de arquivos manipulados pela alteração do relógio é verificar se os rótulos de tempo do arquivo estão compatíveis temporalmente entre si, ou seja, se não apresentam inconsistências entre seus rótulos de tempo. No entanto, essa é uma análise mais trabalhosa e sua viabilidade depende da operação à qual o arquivo foi submetido enquanto o relógio estava alterado.

5.11 Pontos de restauração

A análise do funcionamento dos pontos de restauração mostrou que as diretivas de inclusão e exclusão de monitoramento de diretórios e de extensões de arquivos, presentes no arquivo *filelist.xml*, não são diretas. Pelos resultados obtidos, as diretivas de exclusão de diretório têm precedência sobre as de inclusão de extensões de arquivos, enquanto que as diretivas de inclusão de diretórios estão condicionadas às diretivas de inclusão de extensões de arquivos. Ou seja, para que um arquivo seja monitorado não basta que a pasta em que ele se encontra esteja na lista de pastas monitoradas, é necessário também que a sua extensão esteja entre as extensões monitoradas. Da mesma forma, arquivos presentes em diretórios contidos na lista de exclusão não serão monitorados, mesmo que sua extensão esteja entre as monitoradas. A conclusão sobre o funcionamento das diretivas do arquivo *filelist.xml*, obtida neste trabalho, está aparentemente de acordo com a estrutura do arquivo *filelist.xml* padrão do Windows. Nele é possível observar que inúmeras extensões de arquivos estão incluídas no monitoramento e nenhuma está presente na lista de excluídas. Já na lista de diretórios, a maioria está presente na lista de exclusão, enquanto que poucos estão na lista de inclusão. Essa configuração padrão do arquivo reforça nossa hipótese que o monitoramento é realizado por extensão de arquivo e que as diretivas de diretório se prestam a excluir alguns diretórios desse monitoramento, como por exemplo pastas de dados dos usuários. Na literatura estudada (HARMS, 2006) (ZHU; JAMES; GLADYSHEV, 2009), não há um aprofundamento sobre a lógica de funcionamento das diretivas do arquivo *filelist.xml*, limitando-se somente a informar que esse arquivo possui diretivas de inclusão e exclusão

que governam o processo de monitoramento dos pontos de restauração.

Os arquivos copiados para as pastas dos pontos de restauração apresentam alguns dados relevantes para a análise temporal. Em cada uma dessas pastas há uma cópia do Registro, que pode proporcionar informações importantes sobre a configuração do computador em um instante próximo da janela de tempo sob análise, como por exemplo configurações de sincronização de relógio, de fuso horário e de horário de verão, além de informações sobre dispositivos removíveis inseridos no computador. Além da cópia do Registro, arquivos monitorados que tiverem seu conteúdo alterado antes da criação do ponto de restauração terão seus rótulos de tempo do atributo SI preservados, juntamente com o seu conteúdo referente ao instante monitorado.

Esse arquivos, além de propiciarem informações que complementam a criação de suas linhas de tempo, informações essas que poderiam se perder caso o arquivo sofresse muitas modificações até a data do exame, proporcionam, também, um componente extra à análise temporal. Esse componente extra é a possibilidade de recuperação do conteúdo do arquivo antes de uma modificação, que pode trazer informações importantes para o caso analisado. Deve-se atentar, no entanto, conforme salientado por Zhu, James e Gladyshev (2009), que os arquivos registrados pelo ponto de restauração correspondem à ultima alteração do arquivo no intervalo de tempo entre o ponto de restauração anterior e o horário de criação do arquivo (armazenado no atributo FN do arquivo presente no ponto de restauração), sendo possível que tenham ocorridas outras modificações não registradas nesse intervalo. Além desse fato, por padrão, arquivos de usuário não são monitorados pelos pontos de restauração, o que torna sua aplicação para a área forense mais limitada àqueles casos nos quais o interesse seja na alteração de arquivos de sistema ou que o arquivo *filelist.xml* tenha sido alterado.

5.12 Transferências de arquivos e pastas do sistema FAT para o sistema NTFS

Os resultados obtidos na cópia e movimentação de arquivos de um sistema FAT para o sistema NFTS apresentaram resultados de interesse, pois foram constatadas características capazes de individualizar essas operações. O padrão de alteração dos rótulos de tempo não se assemelha a nenhuma outra operação analisada, nem mesmo às operações equivalentes de transferência de arquivos entre volumes NTFS distintos, permitindo a sua individualização. Deve-se resssaltar o fato de as frações de segundo apresentarem-se zeradas no MT (SI), no caso de movimentação, e nos CrT e MT do

SI, no caso de cópia, característica essa que pode permanecer após a realização de alguns tipos de operações, como foi apresentado no estudo de caso. Nessas situações é possível afirmar que determinados arquivos foram provenientes de um sistema FAT, mesmo após certas manipulações, o que pode ser relevante para o caso analisado.

5.13 Considerações finais

A pesquisa relativa aos rótulos de tempo armazenados nas entradas dos diretórios pais de arquivos e pastas analisados mostrou que elas refletem as informações constantes no atributo SI, não sendo, portanto, necessário o seu processamento e análise.

Um dos principais resultados deste trabalho foi a elaboração de tabelas com a compilação, por operação, das cronologias temporais dos rótulos de tempo por atributo e das relações entre os rótulos de tempo de atributos distintos, além de tabelas com características dos rótulos de tempo para cada operação. Essas tabelas foram utilizadas no estudo de caso apresentado no capítulo 6 e, por esse motivo, acredita-se que serão muito úteis quando aplicadas em um caso real, pois apresentam de maneira sintética e completa os resultados obtidos neste estudo.

6 ESTUDO DE CASO

O estudo de caso apresentado neste capítulo é baseado em uma situação real em que quesitos foram enviados para a perícia criminal de informática, a fim de que questionamentos da defesa sobre a integridade de alguns vídeos encontrados no disco rígido de um notebook, previamente examinado, fossem respondidos. Nesse estudo de caso foram utilizados os resultados obtidos neste trabalho. Ressalta-se que os dados a seguir apresentados foram alterados para preservar a privacidade dos envolvidos.

A defesa do acusado alegou que os vídeos de pornografia infantil localizados no disco rígido do notebook foram inseridos na mídia por um terceiro que queria prejudicar seu cliente. Foi solicitado, então, que a perícia examinasse o disco rígido para verificar se essas alegações tinham fundamento.

O disco rígido analisado possuía uma partição de ∼56 GiB, formatada com sistema de arquivos NTFS e com sistema operacional Windows XP Professional instalado.

Os exames foram realizados sobre uma imagem do disco rígido em um sistema Linux utilizandos-se ferramentas nativas (dd, grep, strings, ls, etc.), o conjunto de aplicativos *The Sleuth Kit* (TSK) (CARRIER, 2003-2012) e ferramentas desenvolvidas em *Shell Script*.

6.1 Análise

Uma análise dos rótulos de tempo de arquivos que armazenam metadados do sistema ($MFT, $MFTMirr, $Boot) indicou que o sistema de arquivos foi criado na data de 16/03/2007, às 13:27:05, como pode ser observado, por exemplo, nos rótulos de tempo dos atributos $STANDARD_INFORMATION e $FILE_NAME do arquivo $MFT (tabela 6.1).

Os arquivos de vídeo questionados encontravam-se na pasta *C:\Documents and settings\Fulano\Documentos\Vídeos xxx* e seus rótulos de tempo são apresentados nas tabelas 6.2 e 6.3. Para facilitar a apresentação, serão analisados somente três arquivos de vídeo.

Tabela 6.1: Rótulos de tempo do arquivo $MFT

	$STANDARD_INFORMATION	**$FILE_NAME**
Criação	2007-03-16;13:27:05	2007-03-16;13:27:05
Modificação	2007-03-16;13:27:05	2007-03-16;13:27:05
Modificação da MFT	2007-03-16;13:27:05	2007-03-16;13:27:05
Acesso	2007-03-16;13:27:05	2007-03-16;13:27:05

Tabela 6.2: Rótulos de tempo do atributo $STANDARD_INFORMATION dos arquivos de vídeo

	$STANDARD_INFORMATION			
Arquivos	**CrT**	**MT**	**ChT**	**AT**
VIDEO1.WMV	2007-03-16;19:00:00	2006-09-14;16:55:50	2007-03-17;01:21:23	2008-06-13;13:19:23
VIDEO2.WMV	2007-03-16;19:00:01	2006-07-27;09:31:44	2007-03-17;01:21:23	2008-06-13;13:19:23
VIDEO3.WMV	2007-03-16;19:00:03	2006-07-28;10:13:20	2007-03-17;01:21:23	2008-06-13;13:19:23

Tabela 6.3: Rótulos de tempo do atributo $FILE_NAME dos arquivos de vídeo

	$FILE_NAME			
Arquivos	**CrT**	**MT**	**ChT**	**AT**
VIDEO1.WMV	2007-03-16;19:00:00	2007-03-16;19:00:00	2007-03-16;19:00:00	2007-03-16;19:00:00
VIDEO2.WMV	2007-03-16;19:00:01	2007-03-16;19:00:01	2007-03-16;19:00:01	2007-03-16;19:00:01
VIDEO3.WMV	2007-03-16;19:00:03	2007-03-16;19:00:03	2007-03-16;19:00:03	2007-03-16;19:00:03

Verificando-se os rótulos de última modificação do atributo $STANDARD_INFORMATION dos arquivos, foi observado que todos apresentavam segundos pares, como pode ser observado na tabela 6.2. Foi utilizada, então, uma ferramenta para verificar as frações de segundo desses rótulos de tempo, sendo constatado que todos apresentavam as frações de segundo zeradas. O fato de os tempos de modificação do $STANDARD_INFORMATION serem pares, terem suas frações de segundos zeradas e serem anteriores à data de criação do volume, indica que esses arquivos foram armazenados em um sistema FAT, em um instante anterior à criação do sistema de arquivos do notebook, instante esse em que foram criados ou modificados pela última vez.

Em seguida, foram verificados os rótulos de tempo e os números das entradas MFT de cada pasta que compõe o caminho até os arquivos. Esses dados são apresentados na tabela 6.4. Com excessão da pasta *Vídeos xxx*, todas as demais apresentavam os rótulos do atributo $FILE_NAME iguais entre si e iguais ao tempo da criação do atributo $STANDARD_INFORMATION. Esse comportamento indica que as pastas que apresentam essa característica foram criadas, copiadas ou movidas (de outro volume) e não sofreram movimentação posterior. Além disso, considerando-se o nome, caminho e tempo de criação das pastas *Documents and Settings* e *Fulano*, pode-ser afirmar que elas foram criadas no volume, pois são pastas comumente criadas durante a instalação do sistema. O motivo do comportamento diferenciado da pasta *Vídeos xxx* será

detalhado mais adiante.

Tabela 6.4: Tempos de criação e número das entradas MFT de cada pasta do caminho

Entrada MFT	**Pasta**	**Tempo de Criação**
0	C:	2007-03-16;13:27:05
3475	Documents and Settings	2007-03-16;13:34:25
10128	Fulano	2007-03-16;17:42:19
16423	Documentos	2007-03-16;20:03:00
11216	Vídeos xxx	2007-03-16;19:00:00

A pasta *Vídeos xxx*, apesar de estar contida na pasta *Documentos*, apresenta entrada MFT e tempo de criação anteriores à esta. Ordenando-se os arquivos e pastas do disco rígido pelo tempo de criação e pelo número da entrada MFT, foi constatada a criação de vários arquivos e pastas de usuário com tempo de criação e número da entrada MFT muito próximos dos da pasta *Vídeos xxx*, inclusive com poucos segundos de diferença entre um arquivo e outro, estando muitos destes contidos na pasta *Fulano*. Alguns exemplos são mostrados na tabela 6.5. Esse fato indica que a pasta *Vídeos xxx* foi criada no sistema, juntamente com outros arquivos de usuário, às 19h do dia 16/03/2007, provavelmente dentro da pasta *Fulano* ou de alguma subpasta como, por exemplo, a subpasta *Desktop*, e que a pasta *Documentos* foi criada em um instante posterior.

Tabela 6.5: Arquivos e pastas com tempos de criação e entradas MFT próximos de *Vídeos xxx*

Entrada MFT	**Arquivo ou pasta**	**Tempo de Criação**
11216	C:\Documents and Settings\Fulano\Documentos\Vídeos xxx	2007-03-16;19:00:00
11268	C:\Documents and Settings\Fulano\Musicas	2007-03-16;19:00:13
11269	C:\Documents and Settings\Fulano\Musicas\Musica1.mp3	2007-03-16;19:00:13
11285	C:\Documents and Settings\Fulano\Documentos\Fotos	2007-03-16;19:00:17
11349	C:\Documents and Settings\Fulano\Desktop\Documentos	2007-03-16;19:00:24
11363	C:\Documents and Settings\Fulano\Desktop\Doc1.doc	2007-03-16;19:00:38

Verificando-se os rótulos de tempo da pasta *Vídeos xxx* (tabela 6.6) podemos observar que os rótulos do atributo $FILE_NAME não são iguais entre si. Além disso, seus rótulos de criação e modificação são iguais aos do atributo $STANDARD_INFORMATION. Quando uma pasta é movida dentro do mesmo volume ou renomeada, os rótulos do atributo $STANDARD_INFORMATION são copiados para o atributo $FILE_NAME, sendo que, na maioria dos casos, o tempo de acesso copiado para o atributo $FILE_NAME corresponde ao tempo da movimentação, visto que a pasta tem o seu tempo de acesso atualizado quando é acessada instantes antes da realização da operação de movimentação. Como, nesse caso, já foi mostrado que a pasta *Vídeos xxx* não foi criada ou copiada originalmente para *Documentos*, podemos excluir a possibilidade de renomeio e concluir que, em 16/03/2007 às 20:11:58, a pasta *Vídeos xxx* foi movida para dentro da pasta *Documentos*, a qual havia sido criada em 16/03/2007 às 20:03:00.

No entanto, os arquivos de vídeo dentro da pasta *Vídeos xxx* deveriam ter seu tempo de modificação da MFT do atributo $STANDARD_INFORMATION atualizado para o tempo da movimentação da pasta, enquanto que os demais deveriam permanecer inalterados. De fato, os demais não foram alterados (com excessão dos de último acesso), mas o tempo de modificação da MFT, ao invés de marcar o instante da movimentação, mostra um instante posterior (2007-03-17;10:28:58). Os arquivos do volume foram, então, ordenados pelo seu tempo de modificação da MFT, sendo constatados centenas de arquivos com horário de modificação da MFT entre 01:21:00 e 01:27:00 do dia 17/03/2007, em quase sua totalidade arquivos de áudio e vídeo (MP3, WAV, MPEG, WMV). Foi localizado, também, o arquivo *C:\Documents and Settings\Fulano\Local Settings\Application Data\Microsoft\Media Player\CurrentDatabase_59R.wmdb*. Esse arquivo é uma base de dados do aplicativo *Windows Media Player* e seu tempo de última modificação é 01:39:33 do dia 17/03/2007. No conteúdo desse arquivo foram encontrados os nomes dos arquivos de vídeo analisados. Portanto, o tempo de modificação da MFT encontrado nos arquivos de vídeo, com instante posterior ao de sua movimentação, corresponde à varredura por arquivos de mídia efetuada pelo aplicativo *Windows Media Player*, que altera esse rótulo de tempo para o instante no qual o arquivo é adicionado à sua base de dados.

Tabela 6.6: Rótulos de tempo da pasta *Vídeos xxx*

	$STANDARD_INFORMATION	**$FILE_NAME**
Criação	2007-03-16;19:00:00	2007-03-16;19:00:00
Modificação	2007-03-16;19:00:03	2007-03-16;19:00:03
Modificação da MFT	2007-03-17;10:28:58	2007-03-16;19:00:03
Acesso	2008-02-12;15:44:00	2007-03-16;20:11:58

6.2 Resultados e conclusão

Recapitulando, foi possível, através da análise dos rótulos de tempo e de estruturas do sistema de arquivos NTFS, montar a linha de tempo da pasta *Vídeos xxx* e de seus arquivos, a qual é apresentada a seguir e na figura 6.1:

1. Arquivos de vídeo são criados ou modificados pela última vez em um sistema FAT no ano de 2006 - Rótulos de última modificação são anteriores aos de criação e apresentam os segundos pares, com as centenas de segundo zeradas;

2. Sistema de arquivo do volume criado em 16/03/2007 - 13:27:05 - Instante presente nos rótulos de tempo dos arquivos de metadados do sistema;

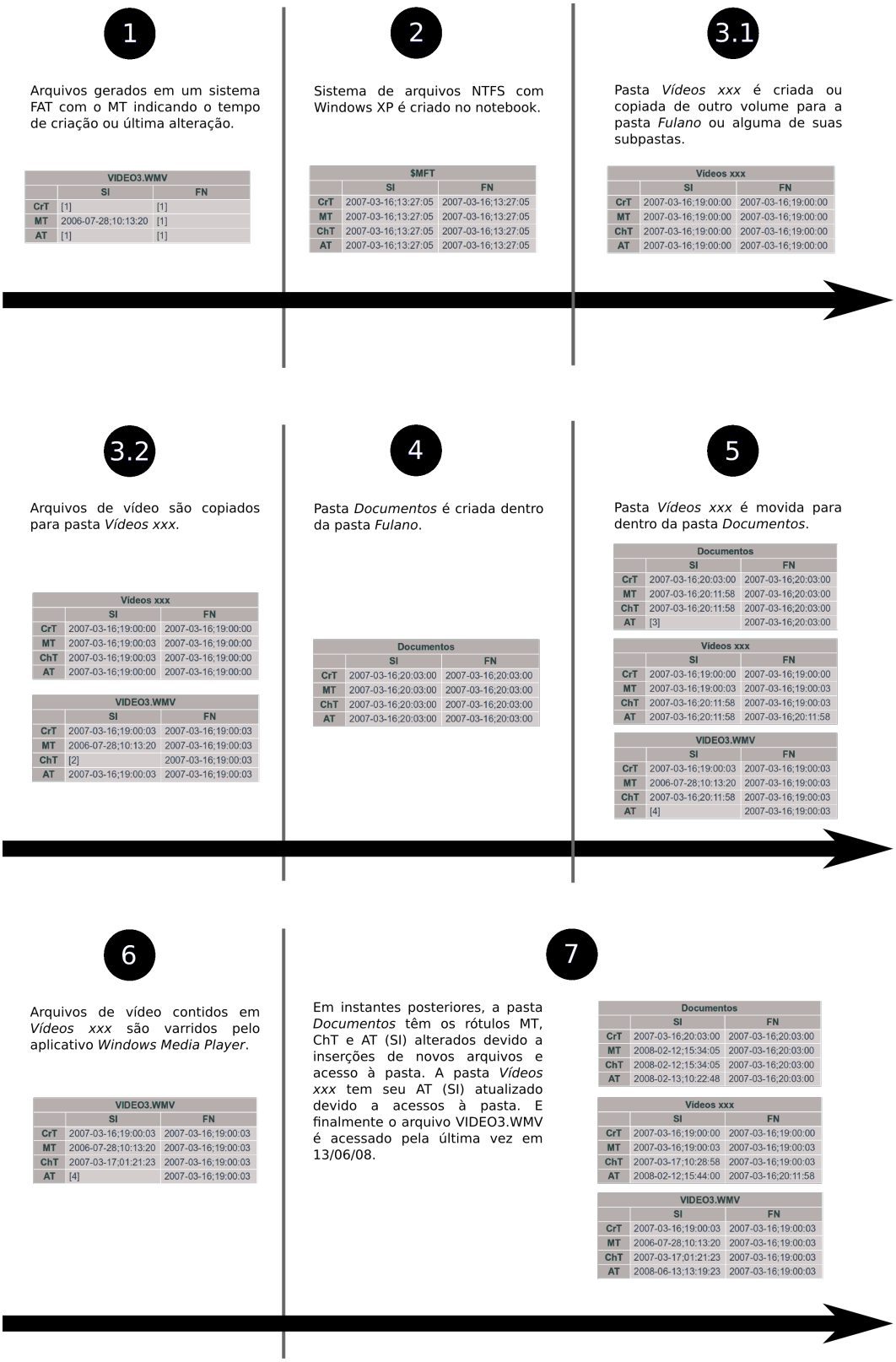
3. Pasta *Vídeos xxx* é criada ou copiada de outro volume, às 19:00:00 do dia 16/03/2007, para a pasta *Fulano* ou alguma de suas subpastas. Os arquivos de vídeo são copiados de um sistema FAT para a pasta *Vídeos xxx*. Pasta *Vídeos xxx* apresenta todos os rótulos de tempo iguais ao instante da operação. À medida que os arquivos de vídeo são copiados para o seu interior, seus tempos de modificação e modificação da MFT são atualizados, coincidindo, ao final da operação, com o tempo de criação (SI) e rótulos em $FILE_NAME do último arquivo a ser inserido na pasta (2007-03-13;22:00:03);

4. Pasta *Documentos* é criada em 16/03/2007 às 20:03:00 - Instante armazenado no tempo de criação (SI) e rótulos do $FILE_NAME;

5. Pasta *Vídeos xxx* é movida para dentro da pasta *Documentos* em 16/03/2007 às 20:11:58. Rótulos em $STANDARD_INFORMATION são copiados para atributo $FILE_NAME, sendo que o tempo de último acesso (FN) indica o tempo de cópia, assim como os tempo de modificação da MFT (SI) dos arquivo de vídeo;

6. Aplicativo *Windows Media Player* inicia varredura por arquivos de mídia em 17/03/2007 às 01:21:00 e termina às 01:39:33, alterando nesse intervalo os tempo de modificação da MFT (SI) dos arquivos de vídeo e inserindo-os em seu arquivo de banco de dados.

Concluindo, foi possível, através do conhecimento do comportamento dos rótulos de tempo em um sistema Windows XP com NTFS, traçar uma linha tempo dos arquivos de vídeo de interesse no sistema analisado, além de determinar que foram gerados, inicialmente, em um sistema FAT, característico de dispositivos de armazenamento portáteis e de equipamentos de gravação. A complexidade encontrada na linha de tempo dos arquivos, aliado ao fato de terem sido submetidos a um procedimento automático de varredura por um aplicativo e de suas datas de inserção no sistema estarem próximas a data de criação do volume, refuta a alegação de que os arquivos foram inseridos intencionalmente no sistema por um terceiro com intuito de incriminar o proprietário do notebook.



[1] Não há como precisar o valor desses rótulos de tempo pois foram sobrescritos quando o arquivo foi copiado para o volume analisado e nas operações subsequentes.
[2] O rótulo ChT (SI) é preservado na cópia do sistema FAT para o volume em estudo, no entanto, a movimentação posterior para a pasta Documentos alterou o valor anterior.
[3] Não há como precisar o valor de AT nesse instante, pois esse rótulo poderia ter sido atualizado entre os passos 4 e 7, e depois foi atualizado para o valor apresentado em 7.
[4] Não há como precisar o valor de AT nesse instante, pois esse rótulo poderia ter sido atualizado entre os passos 3.2 e 7, e depois foi atualizado para o valor apresentado em 7.

Figura 6.1: Linha de tempo do estudo de caso

7 CONCLUSÕES

Este trabalho propôs e cumpriu o objetivo de determinar procedimentos a serem adotados em exames periciais de informática de análise temporal em sistemas de arquivos NFTS, na plataforma Windows XP. Foi realizada uma análise mais aprofundada, com expansão dos casos testados, em relação aos trabalhos correlatos que avaliaram rótulos de tempo (CHOW et al., 2007; BANG et al., 2009; BANG; YOO; LEE, 2011), além de incorporar a essa análise outros elementos do sistema de arquivos e do sistema operacional, obtendo, dessa forma, resultados mais robustos.

Foram realizados testes nos quais arquivos e pastas foram submetidos a operações rotineiras de usuários do sistema, o que resultou na elaboração de tabelas que apresentam relações cronológicas entre os rótulos de tempo armazenados em um atributo da MFT e relações de igualdade e desigualdade entre os rótulos de atributos diferentes. Elaborou-se, também, tabelas com características dos rótulos de tempo para cada operação analisada. Organizando-se os dados nessas tabelas, foi possível determinar que a maioria das operações apresentavam características individualizadoras, o que possibilita a indentificação precisa da ocorrência de uma determinada operação pela observação dos rótulos de tempo de determinado arquivo ou pasta.

Realizou-se, também, experimentos de transferência de arquivos entre o sistema FAT e o sistema NTFS. Constatou-se que arquivos oriundos do sistema FAT possuem características individualizadoras que são as presenças de segundos pares no rótulo MT (SI) e de frações de segundo zeradas nesse rótulo e, para o caso da operação de movimentação, também no CrT (SI). Essas características permitem individualizar os arquivos oriundos de um sistema FAT, muito utilizado em *pendrives*, cartões de memória, câmeras fotográficas, dentre outros. Além da determinação dessas caracteríticas individualizadoras, foi realizado a análise temporal da mesma forma como nas operações do sistema NTFS e o resultado incluído nas tabelas construídas.

Foram feitos, também, testes simulando manipulações intencionais por meio de programas destinados a alteração de rótulos de tempo e de alterações intencionais no relógio do sistema. No caso de manipulações dos rótulos de tempo, foi constatado que os programas testados não são eficazes em mascarar rótulos de tempo de arquivos subme-

tidos a uma análise temporal forense, visto que deixam rastros da alteração, inclusive do instante no qual ela ocorreu. Já o caso de alterações intencionais do relógio do sistema para forjar rótulos de tempo, constatou-se que há dois modos de se detectar essa situação. No primeiro, é necessário analisar em conjunto todos os rótulos de tempo do arquivo ou pasta em questão, pois, como na maioria das operações não há alterações em todos os rótulos de tempo, é esperado que ocorra inconsistências temporais entre os rótulos de tempo do objeto em questão. O segundo método, que é mais simples, consiste na comparação do LSN do arquivo em análise com arquivos que possuam LSN próximos, buscando verificar incompatibilidades entre o rótulo de tempo mais recente do arquivo suspeito com o dos demais.

Verificou-se, também, o mecanismo de geração de pontos de restauração e o conteúdo dos pontos gerados por essa ferramenta. Foi determinada a forma de processamento do arquivo que estabelece a configuração dos diretórios e extensões de arquivos monitorados. Esses resultados indicaram que as diretivas de exclusão de diretório têm precedência sobre as de inclusão de extensões de arquivos, enquanto que as diretivas de inclusão de diretórios estão condicionadas às diretivas de inclusão de extensões de arquivos. Constatou-se também que a única operação monitorada é a de alteração de conteúdo de arquivos e que a cópia do arquivo armazenada no ponto de restauração corresponde à versão do arquivo antes do último desligamento da máquina. Esses resultados foram importantes para entender o funcionamento da referida ferramenta, não sendo encontradas essas informações na literatura referente a esse assunto. Os arquivos monitorados pelos pontos de restauração, caso estejam entre os arquivos de interesse, são vestígios importantes na análise temporal, pois além de armazenarem os rótulos de tempo anteriores à alteração do arquivos, o que auxilia na geração de sua linha de tempo, também armazenam o seu conteúdo anterior, o que pode ser relevante ao caso. Outra contribuição dos pontos de restauração para a análise temporal é o armazenamento do Registro nos instantes nos quais os pontos são gerados. Dessa forma, pode ser possível recuperar o Registro em um instante próximo ao do evento investigado, o que possibilita a recuperação de configurações relevantes para a análise temporal, como configurações de sincronização do relógio, horário de verão, fuso horário, dipositivos removíveis inseridos na máquina, dentre outros. Essa cópia do Registro, quando existente em um instante próximo ao investigado, complementa a análise do Registro atual do sistema.

Os resultados obtidos neste trabalho foram aplicados em um caso real, apresentando no capítulo 6, no qual foram feitos questionamentos sobre a autenticidade de determinados

arquivos. Foi possível concluir positivamente sobre a autenticidade dos arquivos, bem como gerar uma linha de tempo dos arquivos em questão, sendo cumprido o objetivo de validação dos resultados em um caso real. Esse estudo de caso foi apresentado no XXI Congresso Nacional de Criminalística em novembro de 2011 e publicado na íntegra na página oficial do evento (SCORALICK JUNIOR; SHIMABUKO; FERREIRA, 2011).

Ressalta-se que os procedimentos para avaliação temporal de arquivos e pastas apresentados neste trabalho são complementares e sempre que possível devem ser aplicados em conjunto, pois quanto maior a quantidade de evidências coletadas mais consistente fica a conclusão do caso. Recapitulando, é importante analisar o Registro, verificando configurações da máquina, principalmente relativas ao relógio e os pontos de restauração. Deve-se analisar os rótulos de tempo dos arquivos e pastas de interesse, baseando-se nos resultados apresentados nas tabelas (seção 4.10), verificando se apresentam indícios de manipulação direta ou indireta, via alteração do relógio. Finalmente, havendo pontos de restauração próximos ao instante de tempo em questão, deve ser verificado se algum dos arquivos de interesse foi monitorado e deve-se analisar as cópias do Registro, presentes nos pontos de restauração.

Como resultado complementar deste trabalho foram elaboradas ferramentas em *Shell Script* para processamento das entradas MFT dos arquivos e pastas de interesse e sua formatação para utilização em planilhas do aplicativo *Calc* do pacote *OpenOffice*. Foram elaboradas funções nas planilhas que recebem os dados e geram uma ordem cronológica entre os rótulos de tempo de cada atributo da MFT dos arquivos e pastas. Ressalta-se que a ferramenta desenvolvida em *Shell Script* deve ser utilizada em conjunto com a ferramente *fls* do pacote *sleuthkit* (CARRIER, 2003-2012).

Outro resultado complementar do trabalho foi a descoberta de uma falha no aplicativo *istat* do pacote *sleuthkit* (CARRIER, 2003-2012) no processamento do rótulo de última modificação do sistema FAT. A falha foi informado ao desenvolvedor do aplicativo para correção. Constatou-se também uma falha de nomenclatura de um campo referente à esse rótulo de tempo no documento de especificação do sistema FAT (MICROSOFT, 2000).

Como trabalho futuro é sugerido a realização dos experimentos referentes a operações com arquivos e pastas, para elaboração de tabelas com o comportamento de seus rótulos de tempo, em máquinas com outros sistemas operacionais Windows, principalmente o Windows 7, haja visto a tendência desse sistema de superar o Windows XP como sis-

tema operacional mais utilizado (NETMARKETSHARE, 2006-2012; W3COUNTER, 2004-2012).

Outra sugestão de trabalho futuro é automatizar o processo de análise dos rótulos de tempo. Sugere-se que seja desenvolvida uma ferramenta que receba como entrada o arquivo texto com os rótulos de tempo, proveniente da ferramenta já desenvolvida em *Shell Script*. Processando esses rótulos de tempo e utilizando-se dos dados sintetizados nas tabelas apresentadas no apêndice A, a ferramenta apresentaria quais operações poderiam ter sido realizadas sobre os arquivos e pastas de interesse.

REFERÊNCIAS BIBLIOGRÁFICAS

ACCESSDATA. *FTK Imager*. 2010. http://accessdata.com/support/adownloads#FTKImager. Acesso em: 27 dez 2011.

AVAST Software. *avast! Internet Security*. 1988–2012. http://www.avast.com/pt-br/products. Acesso em: 01 fev 2012.

AVG Technologies. *AVG Anti-Virus*. 2012. http://www.avg.com/. Acesso em: 01 fev 2012.

Avira Operations. *Avira Free Antivirus*. 2012. http://www.avira.com/en/for-home. Acesso em: 01 fev 2012.

BANG, J. et al. Analysis of time information for digital investigation. *Networked Computing and Advanced Information Management, International Conference on*, IEEE Computer Society, Los Alamitos, CA, USA, v. 0, p. 1858–1864, 2009.

BANG, J.; YOO, B.; LEE, S. Analysis of changes in file time attributes with file manipulation. *Digital Investigation*, v. 7, n. 3-4, p. 135–144, 2011.

BOVET, D. P.; CESATI, M. *Understanding the Linux Kernel, Third Editon*. [S.l.]: O'Reilly, 2006. ISBN 0596005652.

BOYD, C.; FORSTER, P. Time and date issues in forensic computing - a case study. *Digital Investigation*, v. 1, n. 1, p. 18–23, 2004.

CARRIER, B. *sleuthkit.org*. 2003–2012. http://www.sleuthkit.org/. Acesso em: 27 dez 2011.

CARRIER, B. *File System Forensic Analysis*. [S.l.]: Addison-Wesley Professional, 2005. ISBN 0321268172.

CARVEY, H. The windows registry as a forensic resource. *Digital Investigation*, v. 2, n. 3, p. 201 – 205, 2005. ISSN 1742-2876. Disponível

em: <http://www.sciencedirect.com/science/article/B7CW4-4GX1J3B-1/2/6f94db2adc419ceacce8e366614ad34f>.

CHOW, K. et al. The rules of time on ntfs file system. *Systematic Approaches to Digital Forensic Engineering, IEEE International Workshop on*, IEEE Computer Society, Los Alamitos, CA, USA, v. 0, p. 71–85, 2007.

Febooti Software. *Febooti fileTweak - change file date, time and attributes.* 2011. `http://www.febooti.com/products/filetweak/`. Acesso em: 15 ago 2011.

Free Software Foundation. *ls: List directory contents.* 1994–1996, 2000–2012. `http://www.gnu.org/software/coreutils/manual/html_node/ls-invocation.html`. Acesso em: 27 dez 2011.

HALIULLIN, I. *eXpress TimeStamp Toucher.* 2004. `http://www.irnis.net/soft/xtst/`. Acesso em: 15 ago 2011.

HARMS, K. Forensic analysis of system restore points in microsoft windows xp. *Digital Investigation*, v. 3, n. 3, p. 151 – 158, 2006. ISSN 1742-2876. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1742287606000971>.

IEEE. *POSIX - Austin Joint Working Group.* 2008. `http://standards.ieee.org/develop/wg/POSIX.html`. Acesso em: 10 mai 2011.

KüNG, S. *Stefan's Tools - SKTimeStamp.* 2011. `http://tools.tortoisesvn.net/SKTimeStamp.html`. Acesso em: 15 ago 2011.

MICROSOFT. Microsoft extensible firmware initiative fat32 file system specification. *Hardware White Paper*, 2000.

Microsoft MSDN. *Disabling Last Access Time Stamps.* 2006. `http://msdn.microsoft.com/en-us/library/ms940846(v=winembedded.5).aspx`. Acesso em: 06 set 2011.

Microsoft MSDN. *File Times.* 2011. `http://msdn.microsoft.com/en-us/library/windows/desktop/ms724290(v=vs.85).aspx`. Acesso em: 10 mai 2011.

Microsoft Support. *Overview of FAT, HPFS, and NTFS File Systems.* 2007. `http://support.microsoft.com/kb/100108`. Acesso em: 10 mai 2011.

Microsoft Support. *Windows registry information for advanced users.* 2008. `http://support.microsoft.com/kb/256986`. Acesso em: 22 abr 2011.

Microsoft Support. *How to configure an authoritative time server in Windows XP*. 2011. http://support.microsoft.com/kb/314054. Acesso em: 08 set 2011.

Microsoft TechNet. *Windows XP Professional Resource Kit Documentation*. 2005. http://technet.microsoft.com/en-us/library/cc780838(WS.10).aspx. Acesso em: 10 mai 2011.

Microsoft TechNet. *Windows Time Service Tools and Settings*. 2010. http://technet.microsoft.com/en-us/library/cc773263(WS.10).aspx. Acesso em: 08 set 2011.

MILLS, D. L. A brief history of ntp time: Confessions of an internet timekeeper 1,2. *Computer Communication Review*, 2003.

NENAD, H. *NewFileTime 1.51*. 2010. http://www.softwareok.com/?seite=Microsoft/NewFileTime. Acesso em: 15 ago 2011.

NETMARKETSHARE. *Desktop Operating System Market Share*. 2006–2012. http://netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0. Acesso em: 03 fev 2012.

ORACLE. *VirtualBox*. 2004–2011. https://www.virtualbox.org/. Acesso em: 27 dez 2011.

RUSSINOVICH, M. E.; SOLOMON, D. A. *Microsoft Windows Internals, Fourth Edition: Microsoft Windows Server(TM) 2003, Windows XP, and Windows 2000 (Pro-Developer)*. Redmond, WA, USA: Microsoft Press, 2004. ISBN 0735619174.

SAMBA. *Samba - opening windows to a wider world*. 1992–. http://www.samba.org/samba/. Acesso em: 01 fev 2012.

SCHATZ, B.; MOHAY, G. M.; CLARK, A. J. A correlation method for establishing provenance of timestamps in digital evidence. *Digital Investigation*, Elsevier, v. 3, n. Supplement 1, p. S98–S107, September 2006. Disponível em: <http://eprints.qut.edu.au/20576/>.

SCORALICK JUNIOR, C.; SHIMABUKO, A.; FERREIRA, L. C. Linha de tempo na análise pericial de informações em meios digitais. *XXI Congresso Nacional de Criminalística*, Gramado, 2011. Disponível em: <http://www.xxicnc.com.br/userfiles/file/oral_18.pdf>.

The IEEE and The Open Group. *dd - convert and copy a file - Commands & Utilities Reference, The Single UNIX Specification, Issue 7*. 2001–2008.

http://pubs.opengroup.org/onlinepubs/9699919799/utilities/dd.html. Acesso em: 27 dez 2011.

UNICODE. *The Unicode Standard, Version 6.0.0*. 2011. http://www.unicode.org/versions/Unicode6.0.0/. Acesso em: 10 mai 2011.

W3COUNTER. *Global Web Stats*. 2004–2012. http://www.w3counter.com/globalstats.php. Acesso em: 03 fev 2012.

WEIGERT, J. *Manual page for xxd*. 1996. http://linuxcommand.gds.tuwien.ac.at/man_pages/xxd1.html. Acesso em: 27 dez 2011.

ZHU, Y.; JAMES, J.; GLADYSHEV, P. A comparative methodology for the reconstruction of digital events using windows restore points. *Digital Investigation*, v. 6, n. 1-2, p. 8 – 15, 2009. ISSN 1742-2876. Disponível em: <http://www.sciencedirect.com/science/article/B7CW4-4W09GKW-1/2/0ca2fea4fb1ae61af72f87557f346745>.

APÊNDICES

A TABELAS DOS RESULTADOS DAS OPERAÇÕES COM ARQUIVOS E PASTAS

Tabela A.1: Síntese do comportamento dos rótulos de tempo em operações com arquivos - ordenação por operação

SI	FN	SI x FN	Tipo	Operação	Sub operação
Ch>A>Cr,M	Cr,M,Ch,A	Ch,A≠Ch,A	Arquivo	Altera propriedades	
M=Ch=A>Cr	Cr,M,Ch,A	M,Ch,A≠M,Ch,A	Arquivo	Alterar conteúdo	
Cr=A>M,Ch	Cr=M=Ch=A	Cr,A=FN	Arquivo	Cópia	Independente volume
Cr=A>M,Ch	Cr=M=Ch=A	Cr,A=FN	Subarquivo	Cópia	Independente volume
Cr=Ch=A>M	Cr=M=Ch=A	Cr,Ch,A=Cr,Ch,A; M≠M	Arquivo	Cópia	Volume diferente (FAT)
Cr=Ch=A>M	Cr=M=Ch=A	Cr,Ch,A=Cr,Ch,A; M≠M	Subarquivo	Cópia	Volume diferente (FAT)
Cr=M=Ch=A	Cr=M=Ch=A	SI=FN	Arquivo	Criação	
Ch>M=A>Cr	M=Ch=A>Cr	Cr,M,A=Cr,M,A; Ch≠Ch	Arquivo	Download	
Ch>Cr=M=A	Cr=M=Ch=A	Ch=FN	Arquivo	Extração zip	
Ch>A>Cr,M	Cr,M,Ch,A	Cr,M,A=Cr,M,A; Ch≠Ch	Arquivo	Movimentação	Mesmo volume
Ch>Cr,M,A	Cr,M,Ch,A	Ch≠Ch	Subarquivo	Movimentação	Mesmo volume
A>Cr,M,Ch	Cr=M=Ch=A	A=FN	Arquivo	Movimentação	Volume diferente
A>Cr,M,Ch	Cr=M=Ch=A	A=FN	Subarquivo	Movimentação	Volume diferente
Ch=A>Cr,M	Cr=M=Ch=A	Ch,A=Ch,A; Cr,M≠Cr,M	Arquivo	Movimentação	Volume diferente (FAT)
Ch=A>Cr,M	Cr=M=Ch=A	Ch,A=Ch,A; Cr,M≠Cr,M	Subarquivo	Movimentação	Volume diferente (FAT)
Ch>A>Cr,M	Cr,M,Ch,A	Cr,M,A=Cr,M,A; Ch≠Ch	Arquivo	Renomear	
A>Cr,M,Ch	Cr,M,Ch,A	M,Ch,A≠M,Ch,A	Arquivo	Sobrescrita	Cópia (independente volume)
Ch>A>Cr,M	Cr,M,Ch,A	M=M; Ch,A≠Ch,A	Arquivo	Sobrescrita	Move (mesmo volume)
A>Cr,M,Ch	Cr,M,Ch,A	SI≠FN	Arquivo	Sobrescrita	Move (volume diferente)

Tabela A.2: Síntese do comportamento dos rótulos de tempo em operações com arquivos - ordenação por rótulos de tempo

SI	**FN**	**SI x FN**	**Tipo**	**Operação**	**Sub operação**
A>Cr,M,Ch	Cr,M,Ch,A	M,Ch,A≠M,Ch,A	Arquivo	Sobrescrita	Cópia (independente volume)
A>Cr,M,Ch	Cr,M,Ch,A	SI≠FN	Arquivo	Sobrescrita	Move (volume diferente)
A>Cr,M,Ch	Cr=M=Ch=A	A=FN	Arquivo	Movimentação	Volume diferente
A>Cr,M,Ch	Cr=M=Ch=A	A=FN	Subarquivo	Movimentação	Volume diferente
Ch=A>Cr,M	Cr=M=Ch=A	Ch,A=Ch,A; Cr,M≠Cr,M	Arquivo	Movimentação	Volume diferente (FAT)
Ch=A>Cr,M	Cr=M=Ch=A	Ch,A=Ch,A; Cr,M≠Cr,M	Subarquivo	Movimentação	Volume diferente (FAT)
Ch>A>Cr,M	Cr,M,Ch,A	Ch,A≠Ch,A	Arquivo	Altera propriedades	
Ch>A>Cr,M	Cr,M,Ch,A	Cr,M,A=Cr,M,A; Ch≠Ch	Arquivo	Movimentação	Mesmo volume
Ch>A>Cr,M	Cr,M,Ch,A	Cr,M,A=Cr,M,A; Ch≠Ch	Arquivo	Renomear	
Ch>A>Cr,M	Cr,M,Ch,A	M=M; Ch,A≠Ch,A	Arquivo	Sobrescrita	Move (mesmo volume)
Ch>Cr,M,A	Cr,M,Ch,A	Ch≠Ch	Subarquivo	Movimentação	Mesmo volume
Ch>Cr=M=A	Cr=M=Ch=A	Ch=FN	Arquivo	Extração zip	
Ch>M=A>Cr	M=Ch=A>Cr	Cr,M,A=Cr,M,A; Ch≠Ch	Arquivo	Download	
Cr=A>M,Ch	Cr=M=Ch=A	Cr,A=FN	Arquivo	Cópia	Independente volume
Cr=A>M,Ch	Cr=M=Ch=A	Cr,A=FN	Subarquivo	Cópia	Independente volume
Cr=Ch=A>M	Cr=M=Ch=A	Cr,Ch,A=Cr,Ch,A; M≠M	Arquivo	Cópia	Volume diferente (FAT)
Cr=Ch=A>M	Cr=M=Ch=A	Cr,Ch,A=Cr,Ch,A; M≠M	Subarquivo	Cópia	Volume diferente (FAT)
Cr=M=Ch=A	Cr=M=Ch=A	SI=FN	Arquivo	Criação	
M=Ch=A>Cr	Cr,M,Ch,A	M,Ch,A≠M,Ch,A	Arquivo	Alterar conteúdo	

Tabela A.3: Síntese do comportamento dos rótulos de tempo em operações com pastas - ordenação por operação

SI	FN	SI x FN	Tipo	Operação	Sub operação
A>Cr,M,Ch	Cr,M,Ch,A	A≠A	Pasta	Altera conteúdo arquivo	
Ch=A>Cr,M	Cr,M,Ch,A	Ch,A≠Ch,A	Pasta	Altera propriedades	
M=Ch=A>Cr	Cr,M,Ch,A	M,Ch,A≠M,Ch,A	Pasta	Alterar conteúdo	
Cr=M=Ch=A	Cr=M=Ch=A	SI=FN	Pasta	Cópia	Independente volume
Cr=M=Ch=A	Cr=M=Ch=A	SI=FN	Subpasta	Cópia	Independente volume
Cr=M=Ch=A	Cr=M=Ch=A	SI=FN	Pasta	Cópia	Volume diferente (FAT)
Ch>Cr=M=A	Cr=M=Ch=A	Cr,M,A=FN	Pasta	Criação	
Cr=M=Ch=A	Cr=M=Ch=A	SI=FN	Pasta	Extração zip	
Ch=A>Cr,M	Cr,M,Ch,A	Cr,M=Cr,M; Ch,A≠Ch,A	Pasta	Movimentação	Mesmo volume
A>Cr,M,Ch	Cr,M,Ch,A	A≠A	Subpasta	Movimentação	Mesmo volume
Cr=M=Ch=A	Cr=M=Ch=A	SI=FN	Pasta	Movimentação	Volume diferente
Cr=M=Ch=A	Cr=M=Ch=A	SI=FN	Subpasta	Movimentação	Volume diferente
Cr=M=Ch=A	Cr=M=Ch=A	SI=FN	Pasta	Movimentação	Volume diferente (FAT)
Ch=A>Cr,M	Cr,M,Ch,A	Cr,M=Cr,M; Ch,A≠Ch,A	Pasta	Renomear	
M=Ch=A>Cr	Cr,M,Ch,A	M,Ch,A≠M,Ch,A	Pasta	Sobrescrita	Cópia (mais arquivos origem)
Cr,M,Ch,A	Cr,M,Ch,A		Pasta	Sobrescrita	Cópia (menos arquivos origem)
M=Ch=A>Cr	Cr,M,Ch,A	M,Ch,A≠M,Ch,A	Pasta	Sobrescrita	Movimentação (mais arquivos origem)
M=Ch=A>Cr	Cr,M,Ch,A	M,Ch,A≠M,Ch,A	Pasta	Sobrescrita	Movimentação (menos arquivos origem)

Tabela A.4: Síntese do comportamento dos rótulos de tempo em operações com pastas - ordenação por rótulos de tempo

SI	**FN**	**SI x FN**	**Tipo**	**Operação**	**Sub operação**
A>Cr,M,Ch	Cr,M,Ch,A	A≠A	Pasta	Altera conteúdo arquivo	
A>Cr,M,Ch	Cr,M,Ch,A	A≠A	Subpasta	Movimentação	Mesmo volume
Ch=A>Cr,M	Cr,M,Ch,A	Ch,A≠Ch,A	Pasta	Altera conteúdo arquivo	
Ch=A>Cr,M	Cr,M,Ch,A	Ch,A≠Ch,A	Pasta	Altera propriedades	
Ch=A>Cr,M	Cr,M,Ch,A	Cr,M=Cr,M; Ch,A≠Ch,A	Pasta	Movimentação	Mesmo volume
Ch=A>Cr,M	Cr,M,Ch,A	Cr,M=Cr,M; Ch,A≠Ch,A	Pasta	Renomear	
Ch>Cr=M=A	Cr=M=Ch=A	Cr,M,A=FN	Pasta	Criação	
Cr,M,Ch,A	Cr,M,Ch,A		Pasta	Sobrescrita	Cópia (menos arquivos origem)
Cr=M=Ch=A	Cr=M=Ch=A	SI=FN	Pasta	Cópia	Independente volume
Cr=M=Ch=A	Cr=M=Ch=A	SI=FN	Subpasta	Cópia	Independente volume
Cr=M=Ch=A	Cr=M=Ch=A	SI=FN	Pasta	Cópia	Volume diferente (FAT)
Cr=M=Ch=A	Cr=M=Ch=A	SI=FN	Pasta	Extração zip	
Cr=M=Ch=A	Cr=M=Ch=A	SI=FN	Pasta	Movimentação	Volume diferente
Cr=M=Ch=A	Cr=M=Ch=A	SI=FN	Subpasta	Movimentação	Volume diferente
Cr=M=Ch=A	Cr=M=Ch=A	SI=FN	Pasta	Movimentação	Volume diferente (FAT)
M=Ch=A>Cr	Cr,M,Ch,A	M,Ch,A≠M,Ch,A	Pasta	Alterar conteúdo	
M=Ch=A>Cr	Cr,M,Ch,A	M,Ch,A≠M,Ch,A	Pasta	Sobrescrita	Cópia (mais arquivos origem)
M=Ch=A>Cr	Cr,M,Ch,A	M,Ch,A≠M,Ch,A	Pasta	Sobrescrita	Movimentação (mais arquivos origem)
M=Ch=A>Cr	Cr,M,Ch,A	M,Ch,A≠M,Ch,A	Pasta	Sobrescrita	Movimentação (menos arquivos origem)

Tabela A.5: Detalhamento dos rótulos de tempo em operações com arquivos

Tipo	**Operação**	**Sub operação**	**Características**
Arquivo	Altera propriedades		Ch(SI),AT(SI) = tempo alteração
Arquivo	Alterar conteúdo		M(SI),Ch(SI),A(SI) = tempo modificação
Arquivo	Cópia	Independente volume	Cr(SI),A(SI),FN = tempo cópia
Subarquivo	Cópia	Independente volume	Cr(SI),A(SI),FN = tempo cópia
Arquivo	Cópia	Volume diferente (FAT)	Cr(SI),Ch(SI),A(SI),FN = tempo copia; M(SI) igual arquivo original (frac. seg. zeradas)
Subarquivo	Cópia	Volume diferente (FAT)	Cr(SI),Ch(SI),A(SI),FN = tempo copia; M(SI) igual arquivo original (frac. seg. zeradas)
Arquivo	Criação		SI,FN = tempo criação
Arquivo	Download		M(SI e FN),Ch(SI e FN),A(SI e FN) = fim do download
Arquivo	Extração zip		Ch(SI),FN = tempo extração; Cr(SI),M(SI),A(SI) = M(SI) do arquivo original arrendondado para cima quando ímpares
Arquivo	Movimentação	Mesmo volume	Ch(SI),AT(SI e FN) = tempo movimentação
Subarquivo	Movimentação	Mesmo volume	Ch(SI) = tempo movimentação
Arquivo	Movimentação	Volume diferente	A(SI),FN = tempo movimentação
Subarquivo	Movimentação	Volume diferente	A(SI),FN = tempo movimentação
Arquivo	Movimentação	Volume diferente (FAT)	Ch(SI),A(SI),FN = tempo movimentação; Cr(SI),M(SI) iguais arquivo original (frac. seg. zeradas)
Subarquivo	Movimentação	Volume diferente (FAT)	Ch(SI),A(SI),FN = tempo movimentação; Cr(SI),M(SI) iguais arquivo original (frac. seg. zeradas)
Arquivo	Renomear		Ch(SI),AT(SI e FN) = tempo renomeio
Arquivo	Sobrescrita	Cópia (independente volume)	A(SI) = tempo copia; M(SI),Ch(SI) = arquivo que sobrescreveu
Arquivo	Sobrescrita	Move (mesmo volume)	Ch(SI) = tempo movimentação; M(SI),FN = arquivo que sobrescreveu
Arquivo	Sobrescrita	Move (volume diferente)	A(SI) = tempo movimentação; Cr(SI),M(SI),Ch(SI) = arquivo que sobrescreveu

Tabela A.6: Detalhamento dos rótulos de tempo em operações com pastas

Tipo	**Operação**	**Sub operação**	**Características**
Pasta	Altera conteúdo arquivo		A(SI) = tempo alteração
Pasta	Altera conteúdo arquivo		Ch(SI),A(SI) = tempo alteração
Pasta	Altera propriedades		Ch(SI),A(SI) = tempo alteração
Pasta	Alterar conteúdo		M(SI),Ch(SI),A(SI) = tempo modificação
Pasta	Cópia	Independente volume	SI,FN = tempo cópia
Subpasta	Cópia	Independente volume	SI,FN = tempo cópia
Pasta	Cópia	Volume diferente (FAT)	SI,FN = tempo cópia
Pasta	Criação		Cr(SI),M(SI),A(SI),FN = tempo criação
Pasta	Extração zip		SI,FN = tempo extração
Pasta	Movimentação	Mesmo volume	Ch(SI),A(SI) = tempo movimentação
Subpasta	Movimentação	Mesmo volume	A(SI) = tempo movimentação
Pasta	Movimentação	Volume diferente	SI,FN = tempo movimentação
Subpasta	Movimentação	Volume diferente	SI,FN = tempo movimentação
Pasta	Movimentação	Volume diferente (FAT)	SI,FN = tempo movimentação
Pasta	Renomear		Ch(SI),A(SI) = tempo renomeio
Pasta	Sobrescrita	Cópia (mais arquivos origem)	M(SI),Ch(SI),A(SI) = tempo cópia
Pasta	Sobrescrita	Cópia (menos arquivos origem)	
Pasta	Sobrescrita	Movimentação (mais arquivos origem)	M(SI),Ch(SI),A(SI) = tempo movimentação
Pasta	Sobrescrita	Movimentação (menos arquivos origem)	M(SI),Ch(SI),A(SI) = tempo movimentação

B CÓDIGO FONTE DA FERRAMENTA

```
# proc_time_mft - Processa arquivo gerado pelo  aplicativo fls do pacote
# sleuthkt e gera tabela com campos de interesse dos atributos $DATA,
# $FILE_NAMEs, $INDEX_ROOT e $INDEX_ALLOCATION.
#
# Copyright (C) - 2011 - Cleber Scoralick Junior <scoralick@gmail.com> e
# Copyright (C) - 2010 - Angelo Shimabuko <angeloshimabuko@gmail.com>
# (função conv_time)
#
# Este programa é um software livre; pode ser redistribuído e/ou modificado
# sob os termos da Licença Pública Geral GNU (GPL -- General Public License)
# na versão 2 (GPL v2) exclusivamente.
#
# Este programa é distribuído no intuito de ser útil, sem qualquer garantia,
# mesmo que implícita.
#
# Uma cópia da GPL pode ser obtida escrevendo-se par a Free Software
# Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
# http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
#
# Descrição dos parâmetros necessários à execução do programa:
#
# Primeiro parametro: arquivo gerado pelo fls, em formato extendido (-p)
# para os arquivos e diretórios de interesse
# Segundo parametro: arquivo da imagem .dd
# Terceiro parametro: offset do arquivo
# Quarto parametro: nome arquivo de saída


#/bin/bash

#Função de conversão dos bytes de rotulo de tempo em formato legível (UTC)
#Input: Array com bytes na ordem de leitura convertidos para decimal
#Output: String com data formatada e flag indicando se os nano segundos são
#nulos (0) ou não (1)

      function conv_time {
        b=($1 $2 $3 $4 $5 $6 $7 $8)
        time_ns=0
        for ((i = 0; i < 8; i++))
```

```
do
  let time_ns=$time_ns+${b[$i]}*256**$i
done
let time_70=$time_ns-116444736000000000
let time_s=$time_70/10000000
let remain=$time_70%10000000
if [ $remain -gt 0 ]
then
  flag=1
else
  flag=0
fi
let dias=$time_s/86400      # dias desde 1970
let segs=$time_s%86400      # segundos no ultimo dia
let mins=$segs/60         # minutos no ultimo dia
let ss=segs%60            # segundos - ultimo minuto
if [ "$ss" -lt "10" ]     # normaliza os segundos (2 digitos)
then
  ss=0$ss
fi
let mm=mins%60            # minutos - ultima hora
if [ "$mm" -lt "10" ]     # normaliza os minutos (2 digitos)
then
  mm=0$mm
fi
let hh=mins/60            # horas - ultimo dia
if [ "$hh" -lt "10" ]     # normaliza as horas (2 digitos)
then
  hh=0$hh
fi
# ano
if [ "$dias" -lt "730" ]
then
  fev=28
  let dias=$dias%365
  let ano0=$dias/365
  let ano=$ano0+1970      # 1970 ou 1971
else
  let dias=$dias-730
  let quad=$dias/1461
  let dias=$dias%1461
  let ano0=$quad*4
  if [ "$dias" -lt "366" ]
  then
    let fev=29
```

```
    let ano=$ano0+1972    # anos bissextos desde 1972
  else
    let fev=28
    let dias=$dias-366
    let ano1=$dias/365
    let dias=$dias%365
    let ano=$ano0+$ano1+1973  # anos comuns apos 1972
  fi
fi
# mes e dia
if [ "$dias" -lt "31" ]
then
  mes=1
  let dia=$dias+1 # dias em janeiro
else
  let dias=$dias-31
  if [ "$dias" -lt "$fev" ]
  then
    mes=2
    let dia=$dias+1 # dias em fevereiro
  else
    let dias=$dias-$fev
    let quim=$dias/153  # $quim=0 => mar, abr, mai, jun, jul
    let quim=$quim*5    # $quim=5 => ago, set, out, nov, dez
    let dias=$dias%153
    let bim=$dias/61    # $bim=0 => mar, abr, ago, set
    let bim=$bim*2      # $bim=2 => mai, jun, out, nov
    let dias=$dias%61   # $bim=4 => jul, dez
    if [ "$dias" -lt "31" ]
    then
      let mes=3+$quim+$bim # mar, mai, jul, ago, out, dez
      let dia=$dias+1
    else
      let mes=4+$quim+$bim # abr, jun, set, nov
      let dia=$dias-30
    fi
  fi
fi
# normaliza o mes (2 digitos)
if [ "$mes" -lt "10" ]
then
  mes=0$mes
fi
# normaliza o dia (2 digitos)
if [ "$dia" -lt "10" ]
```

```
        then
          dia=0$dia
        fi
        echo "$ano-$mes-$dia;$hh:$mm:$ss|$flag|"
      }
      #////////////////////////////////////////////////////

#Definição de constantes:
OUT_DIR="/output" #Diretório dentro do PWD onde serão salvos os arquivos

#Testa se os parametros são válidos
if !( [ -f $1 ] && [ -f $2 ] && [ $3 -ge 0 ] && [ -n $4 ])
then
  echo "Parâmetros inválidos!"
  exit 0
else
  #Cria diretório de saída
  if [ -d "${PWD}${OUT_DIR}" ]
  then
    dir="${PWD}${OUT_DIR}"
  else
    mkdir "${PWD}${OUT_DIR}"
    dir="${PWD}${OUT_DIR}"
  fi

  #Cabeçalho tabela de saída
  header="MFT_num|Nome|LSN|f/d|Att_num|$SI(CrT)|ns_flag|$SI(MT)|ns_flag|
  $SI(ChT)|ns_flag|$SI(AT)|ns_flag|Att_num|$FN1(CrT)|ns_flag|$FN1(MT)|
  ns_flag|$FN1(ChT)|ns_flag|$FN1(AT)|ns_flag|Att_num|$FN2(CrT)|ns_flag|
  $FN2(MT)|ns_flag|$FN2(ChT)|ns_flag|$FN2(AT)|ns_flag|Att_num|$FN3(CrT)|
  ns_flag|$FN3(MT)|ns_flag|$FN3(ChT)|ns_flag|$FN3(AT)|ns_flag|"

  #Apaga arquivo de saída de existir e acrescenta cabeçalho
  echo $header > "$dir/$4"

  while read entrada
  do
    #Obtem número da entrada mft
    mft=`echo $entrada | cut -d " " -f2 | cut -d "-" -f1`
    #Inicializa string saída
    saida=""
    #Insere número entrada MFT
    saida="$saida$mft|"
    #Insere nome retirando espaços em branco no início do nome
    nome=`echo $entrada | cut -d ":" -f2 | sed 's/^ *//'`
```

```
saida="$saida$nome|"
#Insere LSN
lsn=‘istat -o $3 $2 $mft | grep "LogFile Sequence Number" | cut -d ":"
 -f2‘
saida="$saida$lsn|"
#Flag de diretório ou arquivo
d_f=‘echo $entrada | cut -d "/" -f1‘
saida="$saida$d_f|"
#Processa attributos do arquivo
IFS_OLD=$IFS
IFS=$’\n’
#Inicia variaveis
SI="|||||||||"
FN1="|||||||||"
FN2="|||||||||"
FN3="|||||||||"
fn_count=0
for linha in ‘istat -o $3 $2 $mft | grep "Type: "‘
do
  #Captura nome do atributo
  att_name=‘echo $linha | cut -d " " -f2‘
  case $att_name in
  #$STANDARD_INFORMATION
  \$STANDARD_INFORMATION)
    #Número do atributo
    att_num=‘echo $linha | cut -d "(" -f2 | cut -d ")" -f1‘
    SI="$att_num|"
    #Creation time (extrai byte a byte e chama função para conversão)
    for ((i = 0; i < 8; i++))
    do
      b[$i]=$(icat -o $3 $2 $mft-$att_num | dd bs=1 count=1 skip=$i
      2>/dev/null | xxd -ps)
      let b[$i]=0x${b[$i]}
    done
    SI="$SI‘conv_time ${b[0]} ${b[1]} ${b[2]} ${b[3]} ${b[4]} ${b[5]}
     ${b[6]} ${b[7]}‘"
    #Modified time (extrai byte a byte e chama função para conversão)
    for ((i = 0; i < 8; i++))
    do
      b[$i]=$(icat -o $3 $2 $mft-$att_num | dd bs=1 count=1 skip=
      $[$i+8] 2>/dev/null | xxd -ps)
      let b[$i]=0x${b[$i]}
    done
    SI="$SI‘conv_time ${b[0]} ${b[1]} ${b[2]} ${b[3]} ${b[4]} ${b[5]}
     ${b[6]} ${b[7]}‘"
```

```
  #Change time (extrai byte a byte e chama função para conversão)
  for ((i = 0; i < 8; i++))
  do
    b[$i]=$(icat -o $3 $2 $mft-$att_num | dd bs=1 count=1 skip=
    $[$i+16] 2>/dev/null | xxd -ps)
    let b[$i]=0x${b[$i]}
  done
  SI="$SI`conv_time ${b[0]} ${b[1]} ${b[2]} ${b[3]} ${b[4]} ${b[5]}
   ${b[6]} ${b[7]}`"
  #Access time (extrai byte a byte e chama função para conversão)
  for ((i = 0; i < 8; i++))
  do
    b[$i]=$(icat -o $3 $2 $mft-$att_num | dd bs=1 count=1 skip=
    $[$i+24] 2>/dev/null | xxd -ps)
    let b[$i]=0x${b[$i]}
  done
  SI="$SI`conv_time ${b[0]} ${b[1]} ${b[2]} ${b[3]} ${b[4]} ${b[5]}
   ${b[6]} ${b[7]}`"
  ;;
#$FILE_NAME
\$FILE_NAME)
  #Número do atributo
  att_num=`echo $linha | cut -d "(" -f2 | cut -d ")" -f1`
  FN_temp="$att_num|"
  #Creation time (extrai byte a byte e chama função para conversão)
  for ((i = 0; i < 8; i++))
  do
    b[$i]=$(icat -o $3 $2 $mft-$att_num | dd bs=1 count=1 skip=
    $[$i+8] 2>/dev/null | xxd -ps)
    let b[$i]=0x${b[$i]}
  done
  FN_temp="$FN_temp`conv_time ${b[0]} ${b[1]} ${b[2]} ${b[3]} ${b[4]}
   ${b[5]} ${b[6]}
  ${b[7]}`"
  #Modified time (extrai byte a byte e chama função para conversão)
  for ((i = 0; i < 8; i++))
  do
    b[$i]=$(icat -o $3 $2 $mft-$att_num | dd bs=1 count=1 skip=
    $[$i+16] 2>/dev/null | xxd -ps)
    let b[$i]=0x${b[$i]}
  done
  FN_temp="$FN_temp`conv_time ${b[0]} ${b[1]} ${b[2]} ${b[3]} ${b[4]}
   ${b[5]} ${b[6]}
  ${b[7]}`"
  #Change time (extrai byte a byte e chama função para conversão)
```

```
        for ((i = 0; i < 8; i++))
        do
          b[$i]=$(icat -o $3 $2 $mft-$att_num | dd bs=1 count=1 skip=
          $[$i+24] 2>/dev/null | xxd -ps)
          let b[$i]=0x${b[$i]}
        done
        FN_temp="$FN_temp`conv_time ${b[0]} ${b[1]} ${b[2]} ${b[3]} ${b[4]}
         ${b[5]} ${b[6]}
        ${b[7]}`"
        #Access time (extrai byte a byte e chama função para conversão)
        for ((i = 0; i < 8; i++))
        do
          b[$i]=$(icat -o $3 $2 $mft-$att_num | dd bs=1 count=1 skip=
          $[$i+32] 2>/dev/null | xxd -ps)
          let b[$i]=0x${b[$i]}
        done
        FN_temp="$FN_temp`conv_time ${b[0]} ${b[1]} ${b[2]} ${b[3]} ${b[4]}
         ${b[5]} ${b[6]}
        ${b[7]}`"
        let fn_count=$fn_count+1;
        case $fn_count in
        1)
          FN1=$FN_temp
        ;;
        2)
          FN2=$FN_temp
        ;;
        3)
          FN3=$FN_temp
        ;;
        esac
      ;;
      esac
    done
    saida="$saida$SI$FN1$FN2$FN3"
    echo $saida >> $dir/$4
    IFS=$IFS_OLD
  done < $1
fi

exit 0
```