A eficiência de soluções de recuperação de dados na geração de imagens periciais em discos rígidos com *badblocks* em detrimento de duplicadores forenses ou aplicativos específicos

Gilson Marques da Silva[a], Rogério de Freitas Ribeiro[b*]
[a]Polícia Federal, Uberlândia, MG, Brasil, CEP 38408-663
[b] SlackSpace, Uberlândia, MG, Brasil, CEP 38405-070
*rogerio@slackspace.com.br

Introdução

Não é raro, o recebimento de discos rígidos acometidos por problemas físicos para a realização de exames periciais, um tipo comum de problema físico é o *badblock*.
Também não é raro que a duplicação pericial realizada por técnicas forenses comuns não possa ser feita; ou seja feita de forma parcial, obtendo porção de dados menor do que a possível.
A impossibilidade de geração das imagens impede a realização dos exames periciais e acaba por potencializar a impunidade; ou a incompletude das imagens forenses limita o objeto a ser examinado, impedindo que o Perito tenha acesso a todas as informações, limitando suas análises e conclusões.

Objetivos

Demonstrar, na prática, a efetividade do uso de soluções especializadas na recuperação de dados e geração de imagens de HDs com *badblocks* em detrimento do uso de duplicadores forenses ou aplicativos específicos.

Metodologia

Para o desenvolvimento dos objetivos deste trabalho foram realizados testes com 3 (três) HDs com *badblocks* com diferentes níveis de comprometimento. Um quarto HD, sem defeitos foi usado como parâmetro inicial.
Cada HD foi duplicado por dois duplicadores forenses (Tableau TD3 e Logicube Dossier); por um aplicativo executado no sistema operacional Windows (Access Data FTK Imager); por um aplicativo executado no sistema operacional Linux (GNU dd_rescue); e por uma solução especializada na recuperação de dados (MRT Ultra).
Os resultados foram comparados em termos do sucesso na geração da imagem; do percentual de setores lidos e do tempo gasto na geração da imagem.

Resultados e Discussões

A tabela a seguir apresenta os resultados obtidos.

	TD3	Dossier	FTK Imager	dd_rescue	MRT
HD0 – sem defeitos – Toshiba – SATA – 320GB					
Imagem feita	Sim	Sim	Sim	Sim	Sim
% setores copiados	100%	100%	100%	100%	100%
Tempo	1h05min	1h	53min	58min	1h46min
HD1 – baixo índice de *badblock* – Western Digital – SATA – 250GB					
Imagem feita	Sim	Sim	Sim	Sim	Sim
% setores copiados	92%	92%	92%	94%	98%
Tempo	1h58min	1h50min	1h36min	2h10min	1h53min
HD2 – médio índice de *badblock* – Toshiba – SATA – 160GB					
Imagem feita	Não	Sim	Não	Sim	Sim
% setores copiados	0%	32%	0%	48%	69%
Tempo	n/a	43h	n/a	52h	76h
HD3 – alto índice de *badblock* – Saumsung – SATA – 320GB					
Imagem feita	Não	Não	Não	Não	Sim
% setores copiados	0%	0%	0%	0%	47%
Tempo	n/a	n/a	n/a	n/a	275h

Vale lembrar que dentre os equipamentos e ferramentas utilizadas apenas o dd_rescue e a MRT possuem mecanismos para retomar a geração da imagem caso o processamento seja interrompido.
Em muitas ocasiões, quando muitos *badblocks* existem na porção inicial do HD, os sistemas operacionais não conseguem tratar estes erros e abortam o acesso ao HD, gerando inclusive o completo desligamento do HD. Isso fez com que o duplicador TD3 e do aplicativo FTK Imager não terem conseguido sequer iniciar a geração da imagem do HD2.
Ainda resta esclarecer os motivos das diferenças de percentual de setores lidos no HD2 pelas soluções Dossier, dd_rescue e MRT. As informações são gravadas nos discos rígidos em *clusters* (grupos de setores), e por padrão, de controladores e sistemas

operacionais comuns, um setor defeituoso pode impedir a leitura de um *cluster* que ainda possua setores íntegros. Além do mais, os sistemas comuns fazem uma leitura antecipada de *clusters* a fim de melhorar a performance de leitura.

Soluções como a MRT não dependem do *hardware* controlador do disco rígido e nem dos *drivers*, isso permite funcionalidades adicionais como: a desativação de *buffers* ou *cache* de leitura, utilização de blocos menores, leitura nos dois sentidos e o principal: a possibilidade automática de reinicializar o disco rígido pois tem o completo controle de suas interfaces lógicas e elétricas. Assim, em situações que o HD é desligado em função das sucessivas tentativas malsucedidas, a própria solução pode religá-lo reiniciando o trabalho de leitura e geração da imagem; esse é um dos diferenciais que acabam por permitir que se consiga lidar com discos com alto índice de defeitos.

Conclusões:

Conclui-se diretamente que a adoção de ferramentas especializadas na recuperação de dados, como a MRT ou a PC-3000, podem melhorar em muito a qualidade das imagens geradas a partir de HDs com *badblocks*, o que em última instância melhora a qualidade dos exames periciais realizados e aprimora a execução da Justiça. Tais soluções ainda podem permitir o acesso aos dados em discos rígidos acometidos por outros problemas como o caso de falhas no *firmware*.