DOI: http://dx.doi.org/10.5769/C2011017

Busca de conversas do MSN utilizando os softwares WMM e EnCase

Klarissa de Souza Jerônimo
Polícia Federal
Klarissa.ksj@dpf.gov.br

***Abstract* — This paper compares positive results of searching for MSN conversations in real cases at SETEC/DPF/MA, obtained with WMM 0.2.0 and MSN_Extractor script in EnCase 6.18. This script extracts conversations obtained with an EnCase search for content compatible with MSN protocol messages.**

***Keywords*— Conversation; MSN; search; carving, WMM, EnCase.**

***Resumo* - Serão apresentados casos reais periciados no Setor Técnico Científico da Polícia Federal no Maranhão (SETEC/DPF/MA) em que foram obtidos resultados positivos com a busca de conversas do MSN através das ferramentas WMM 0.2.0 e do script MSN_Extractor no EnCase 6.18. Este script extrai as conversas após busca no EnCase de palavras-chave com conteúdo compatível com mensagens do protocolo MSN. Os resultados são confrontados neste artigo.**

***Palavras-chave*— Conversas; MSN; busca; carving, WMM, EnCase.**

1. Introdução

Ferramentas para busca de conversas de bate-papo são utilizadas pelos peritos de informática sempre que os casos em que eles estão envolvidos demandem busca por mensagens deste tipo de conversação, que é um meio de comunicação muito utilizado por usuários da Internet, inclusive criminosos que atuam utilizando a Internet como meio para suas fraudes.

Na Polícia Federal (PF) do Brasil foi desenvolvida uma ferramenta chamada WMM que possui duas versões diferentes:

- WMM 0.2.0 [1], para buscar conversas do Windows Live Messenger, ou simplesmente MSN, a partir da sua versão 8.0.
- WMM 2009 [2], para Windows Live Messenger 2009.

Neste trabalho, foi utilizada a versão WMM 0.2.0, porque foi ela que encontrou os vestígios de conversas do MSN nos materiais testados. Durante este artigo, esta versão do programa será referenciada simplesmente por WMM. Ele realiza opcionalmente a técnica de carving para busca de fragmentos deixados pelo protocolo MSN. Essa técnica é importante porque as conversas de MSN não são gravadas no disco do usuário por padrão, sendo comum identificar conversas apenas em forma de fragmentos encontrados pela técnica de carving.

Uma segunda ferramenta que permite programar a busca por padrões compatíveis com as conversas do protocolo MSN é o software EnCase. Depois de localizadas, podem-se extrair essas conversas para um formato legível e agrupadas por usuário. Uma programação desta extração de conversas para arquivos foi desenvolvida pelo Perito Criminal Federal Rogério Dourado (SETEC/BA), em formato de script do EnCase, denominado MSN_Extractor [3], transcrito no ANEXO I. Esse script utiliza como universo o resultado de uma busca (*Search Hits*) do EnCase por padrões de mensagens de entrada e de saída do MSN, que deve ser realizada sobre todas as entradas e registros do caso. É possível utilizar o EnCase para realizar previamente a recuperação de arquivos apagados - *Recover Folders* (não é carving, mas recuperação de arquivos apagados na área de clusters não alocados [4]) para incrementar o universo de arquivos para a busca por bate-papo.

Esse trabalho apresenta o resultado das duas ferramentas WMM e EnCase/MSN_Extractor na busca de conversas do MSN em discos rígidos (HDs) periciados no SETEC/DPF/MA. Verificou-se que há semelhanças de resultado entre elas, no entanto não foram obtidos resultados iguais. A análise do universo de arquivos utilizados na busca orienta a explicação para as diferenças encontradas.

Na Seção II são listados os materiais que foram utilizados nos experimentos e é apresentada a metodologia de trabalho, incluindo a preparação dos materiais e a utilização de cada ferramenta, com exemplos de resultados obtidos. Na Seção III são apresentados e analisados os resultados obtidos, que levam às conclusões presentes na Seção IV.

2. Exames E Metodologia

A. Identificação dos materiais utilizados

Na Tabela I é apresentada a identificação junto com uma descrição dos materiais que foram periciados e passaram pelas duas ferramentas de busca de conversas de bate-papo, cujos resultados serão apresentados na Seção III – Resultados. É informado também o número do Laudo relativo à perícia de cada material, que pode ser acessado pelos Peritos Criminais Federais através do sistema interno de Criminalística. Esses materiais são todos referentes a uma mesma apreensão.

TABELA I – Materiais utilizados		
Material	Descrição	Laudo
1. 1011/2010-SETEC/SR/DF	Um disco rígido (HD) de 500 GB e sistema Windows XP SP 3.	012/2011-SETEC/SR/DPF/MA
2. 1049/2010-SETEC/SR/DF	Um notebook com um HD de 100 GB e sistema Windows XP.	124/2011-SETEC/SR/DPF/MA
3. 936/2010-SETEC/SR/DF	Um disco rígido (HD) de 320 GB e sistema Windows XP SP 3.	128/2011-SETEC/SR/DPF/MA
4. 1012/2010-SETEC/SR/DF	Um disco rígido (HD) de 250 GB e sistema Windows XP SP 3.	139/2011-SETEC/SR/DPF/MA
5. 1014/2010-SETEC/SR/DF	Um disco rígido (HD) de 80 GB e sistema Windows XP SP 3.	144/2011-SETEC/SR/DPF/MA
6. 1015/2010-SETEC/SR/DF	Um disco rígido (HD) de 250 GB e sistema Windows XP SP 3.	163/2011-SETEC/SR/DPF/MA

Verificou-se a versão do Windows através do arquivo "software" que se encontrava na pasta "C:\WINDOWS\system32\config" e foi aberto utilizando o programa Mitec Windows Registry Recovery, seção Windows Instalation.

B. Preparação do material para o WMM

As informações do material periciado (Tabela 1) foram duplicadas por meio dos equipamentos *Solo III Forensics (Software Version 2.0.10.8f)* ou *Forensic Dossier (Software:V1.19RCx3)*, gerando arquivos imagens de tamanho 2GB e extensão iniciando por ".001". Outra forma de duplicação utilizada foi conectando o material ao sistema de análise através de interface USB protegida contra escrita via software Windows 7 SP1 e utilização do software FTK Imager 3.0.0.1442 com a opção de compressão "9" para geração dos arquivos imagens do tipo ".E01".

Em seguida, para utilização com o WMM, as imagens de cada material foram montadas utilizando o software AccessData® FTK® Imager 3.0.0.1442, nas opções: *Mount Type: Physical and Logical, Mount Method: Block Device/ Writable*. Após ter a unidade de disco montada, abre-se o programa WMM 0.2.0 para configuração das opções de busca. A interface do programa, com todas as opções de configuração, é ilustrada na Fig.1. Nessa interface, informa-se a unidade de disco para a busca e deve-se confirmar ou alterar as informações sugeridas para alguns diretórios na unidade de busca, como, por exemplo, *Documents and Settings* e *Local Settings* a respeito de Configuração do Windows ou *Received Files* para Configuração do WLM (MSN). Para solicitar a realização de carving, é preciso digitar "0" (*Carve all disk)* no campo *Max chat logs to carve*, em destaque na Fig. 1.

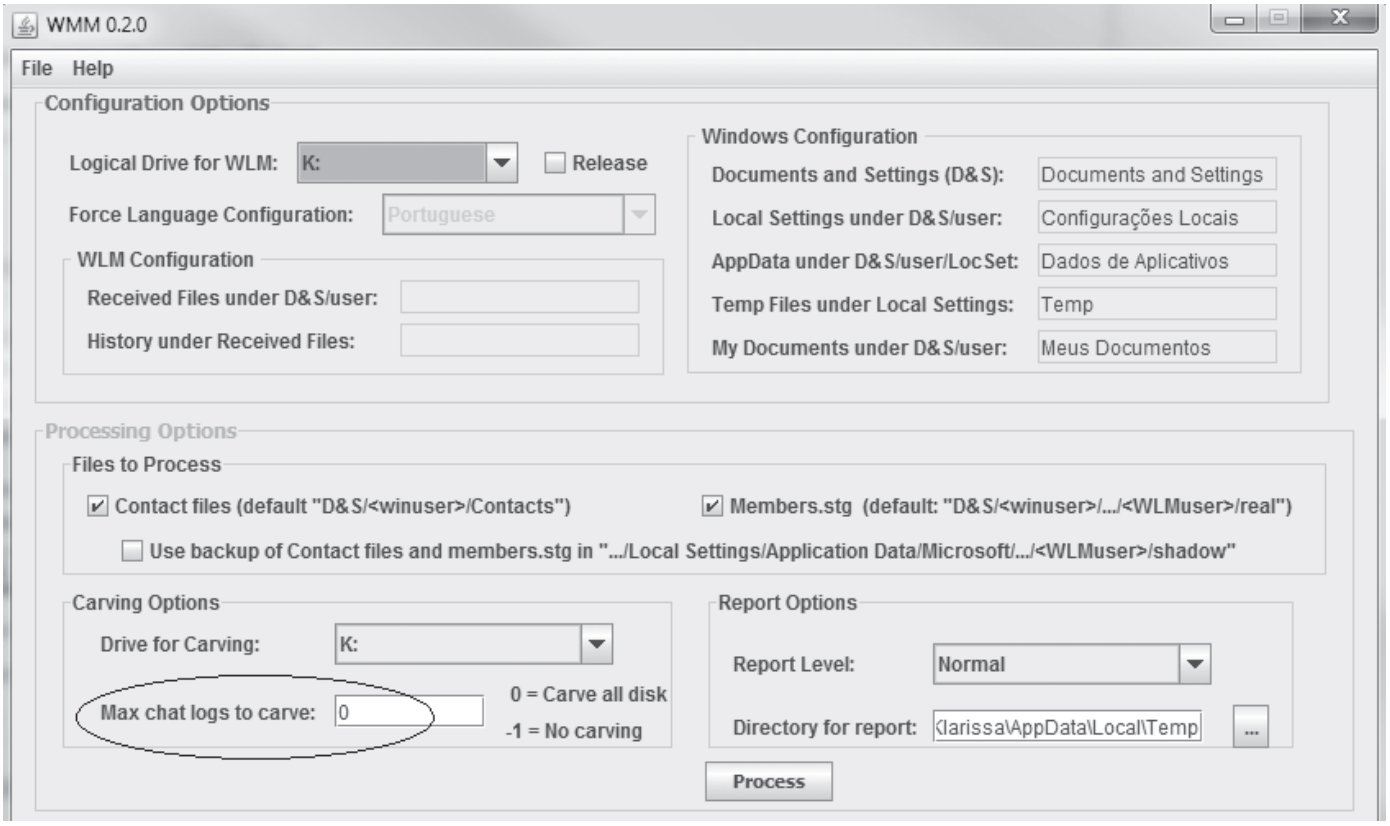

Fig. 1. Interface do programa WMM 0.2.0.

C. Preparação do material no EnCase

Para utilização com o EnCase, as imagens equivalentes aos materiais foram acrescentadas a um caso, através da opção *File/Add Raw Image*, *Image Type: Disk*, e selecionadas para inclusão todos os arquivos das imagens de um material, do último até o primeiro, de extensão ".001". No caso de imagem do tipo ".E01", ela foi aberta junto com o EnCase após duplo clique sobre o arquivo E01 no Windows Explorer.

Após o EnCase abrir o material, ele faz a busca por arquivos perdidos (*Lost Files*) e, na sequência, solicitou-se a recuperação de arquivos apagados, através do clique com o botão direito do mouse sobre letra indicativa da unidade de disco e escolha da opção *Recover Folders*. Feito isso, foram acrescentadas as duas palavras-chave que representam as assinaturas de mensagens de saída e de chegada do MSN:

• Outcoming MSN:	MSG #+ [A-Z] #+[^\x0D\x0A]+
• Incoming MSN:	MSG [a-z#~_\.!\#$%\^&*\(\)\-]+@[a-z#_\-]+\.[a-z#_\-\.]{2,3} [^\x0D\x0A]+

Essas duas palavras-chave devem ser criadas com a opção de GREP marcada e devem ser em seguida selecionadas para a busca, conforme ilustrado na Fig. 2.

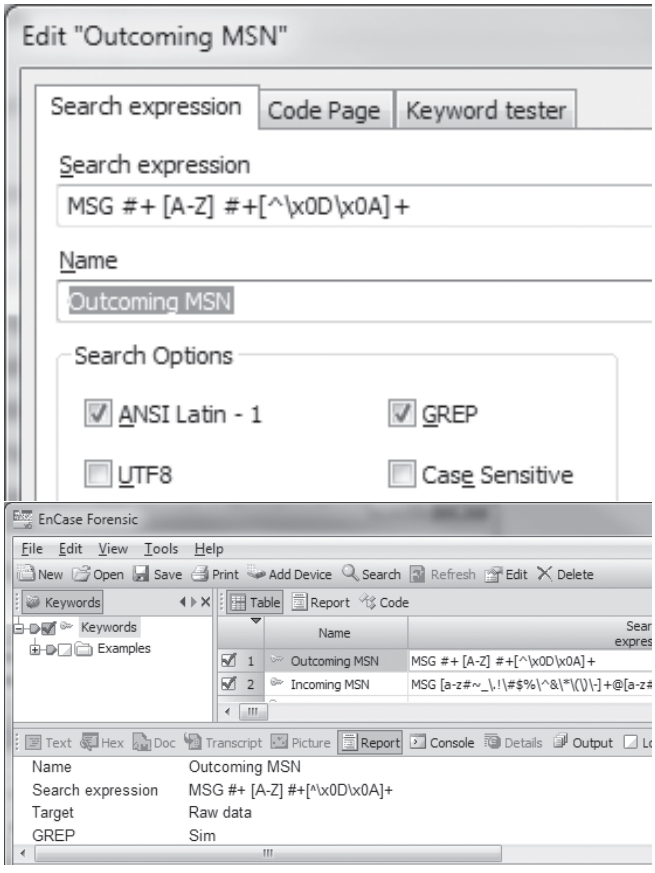

Fig. 2. Exemplo no EnCase da criação e seleção das palavras-chave da busca.

Em seguida, aciona-se a busca (menu *Tools/Search*) sobre todas as entradas do caso, à procura das mensagens compatíveis com as palavras-chave, conforme ilustrado na Fig. 3.

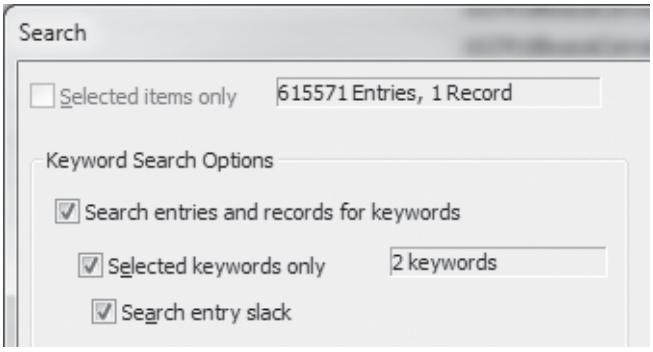

Fig. 3. Janela de busca do EnCase.

As mensagens resultantes da busca são apresentadas na aba *Search Hits* (Fig. 4). Havendo resultados nesta aba, deve-se acionar o script MSN_Extractor que processará o resultado disponível nos *Search Hits* para arquivos texto contendo as mensagens, conforme explicado na Seção D a seguir.

O acionamento do script é feito através do clique duplo no mesmo, que se encontra na aba EnScript, conforme destacado na Fig. 4. Antes o arquivo do script deve ser copiado no diretório EnScript do EnCase.

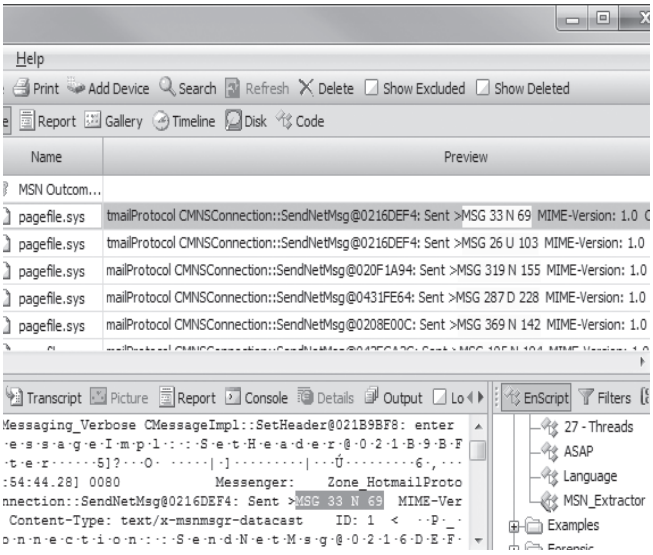

Fig. 4. Exemplo de resultado da busca do EnCase (Search Hits) e localização do script MSN_Extractor na aba EnScript.

D. Exemplo do resultado das ferramentas

O WMM apresenta seu resultado em forma de arquivos html, sendo sua saída como a exemplificada na Fig. 5. Para os materiais utilizados, não houve recuperação de Usuários de MSN e suas listas de contatos. As mensagens recuperadas são apresentadas agrupadas em dois tipos: Conversações entre usuários não identificados e Conversações extraídas do protocolo MSN, que neste trabalho serão chamadas de conversas recuperadas sem carving e com carving, respectivamente.

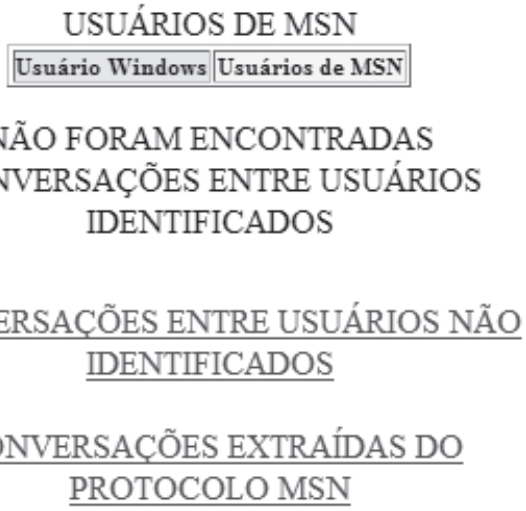

Fig. 5. Exemplo da saída do WMM em arquivo index.html.

Seguem, nas Tabelas II e III, exemplos dos dois tipos de mensagens recuperadas pelo WMM:

- Carved Não – mensagens extraídas diretamente dos arquivos deixados pelo MSN nos diretórios do Windows, sem carving e
- Carved Sim – mensagens obtidas pela busca do tipo carving na partição montada, contendo as pastas de usuários do Windows.

TABELA II – Exemplo de mensagens recuperadas pelo WMM sem utilização de carving (Carved Não)

Carved	Data	Hora	De	Para	Mensagem
Não	30/9/2009	11:10:29	Mulher	Doura	bom dia
Não	13/10/2009	22:15:52	Ramos	Lilo	23
Não	26/10/2009	15:03:48	Goiás	Bis	Como anda o jogo?

Os diálogos encontrados pelo WMM sem a utilização de carving possuem a identificação de remetente e destinatário da mensagem. Essa informação é apresentada nas colunas "De" e "Para" da Tabela II, onde os nomes foram modificados. Entretanto, dentre os participantes de cada mensagem, não é possível identificar qual estava conectado pelo programa MSN do computador analisado, se era o remetente ou o destinatário da mensagem. Consequentemente, no resultado das buscas do WMM sem carving não é possível identificar separadamente as *mensagens que saíram do computador*. Para agrupar os resultados dessa busca com fins de comparar com os resultados da outra ferramenta, nesses casos foram contados apenas o número de remetentes diferentes presentes na coluna De. No exemplo da Tabela II, são contados três *usuários remetentes de mensagens*.

Observou-se também que as identificações dos participantes dos diálogos correspondem aos apelidos utilizados no programa de conversação e não ao e-mail com o qual o usuário se conectou ao MSN, conhecido como MSN Passport.

As mensagens encontradas pelo WMM através de carving possuem a identificação apenas de um participante, informado na coluna Origem da Tabela III, onde os e-mails foram modificados. Cada usuário identificado por um e-mail diferente na coluna Origem foi contado como *usuário remetente de mensagens*. Nesse caso da Tabela III, são contados cinco *usuários remetentes*.

TABELA III – Exemplo de mensagens recuperadas pelo WMM através de carving (Carved Sim)

Carved	Origem	Destino	Mensagem
Sim	b@hotmail.com	-	eu nao sei pq
Sim	n@hotmail.com	-	vou te explicar
Sim	n@hotmail.com	-	Ok
Sim	h_2009@hotmail.com	-	p mim
Sim	c@hotmail.com	-	to ligando aqui ele ja ta na bola
Sim	?	-	kkkkkkkkkkkkkkkkkkk
Sim	?	-	Tudo
Sim	h_2009@hotmail.com	-	p mim
Sim	a@hotmail.com	-	Com certeza
Sim	?	-	Tudo

Algumas das mensagens são apresentadas com uma interrogação ("?") no campo de Origem. Para efeito de comparação do resultado das ferramentas, essas mensagens foram contadas separadamente como *mensagens que saíram do computador*. Foram observadas muitas mensagens repetidas no resultado da recuperação e cada uma delas foi contada apenas uma vez. Por exemplo, para a Tabela III, são contadas duas *mensagens que saíram do computador*.

Já no caso do script de busca MSN_Extractor, executado no EnCase, o resultado é apresentado em forma de arquivos texto contendo os diálogos recuperados, sendo criados:

- um arquivo para cada usuário do MSN identificado como remetente de mensagem, onde o nome do arquivo é o e-mail do usuário e o conteúdo são as mensagens desse usuário; e
- um arquivo para todas as mensagens que saíram do computador analisado, chamado de "outgoing".

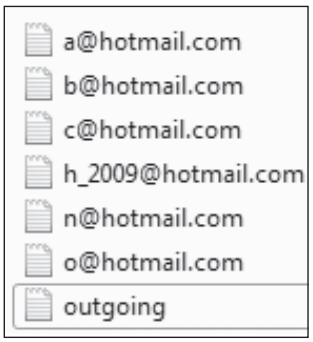

Fig. 6. Arquivos contendo mensagens MSN recuperadas pelo Script MSN_Extrator/EnCase.

Na Fig. 6 é apresentado um exemplo de arquivos resultantes do script MSN_Extractor, onde os e-mails foram modificados. Neste

caso de exemplo, existem seis arquivos cujos nomes são e-mails e para efeito de comparação de resultados, são contados, portanto, seis *usuários remetentes de mensagens*.

Já na Fig. 7, é apresentado o conteúdo do arquivo outgoing.txt, de onde são contadas as mensagens que saíram do computador, sem considerar as duplicatas, que também foram observadas no resultado desta ferramenta, em número nem sempre igual ao recuperado pelo WMM. Neste exemplo, são contadas cinco *mensagens que saíram do computador*.

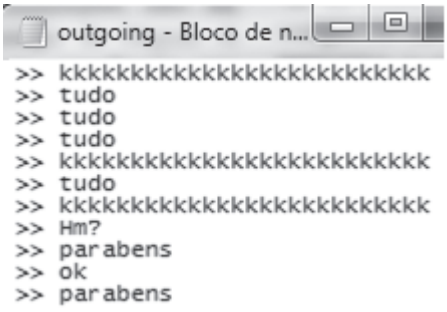

Fig. 7. Conteúdo de um arquivo outgoing.txt de exemplo contendo mensagens que saíram do computador.

A forma de apresentação dos resultados do script MSN_Extractor é semelhante aos resultados das mensagens recuperadas por carving pelo WMM, pelas seguintes coincidências:

- Identificação de apenas um dos dois participantes de uma mensagem;
- Identificação do remetente de mensagem pelo e-mail utilizado no MSN e não pelo apelido, que é recuperado pelo WMM nas buscas sem carving;
- Apresentação de uma mesma mensagem repetidas vezes.

3. Resultados

Para efeito de comparação das duas ferramentas, os resultados obtidos foram categorizados em três tipos:

- *Usuários remetentes de mensagens* – contou-se o número de usuários que tiveram mensagens recuperadas pelas ferramentas;

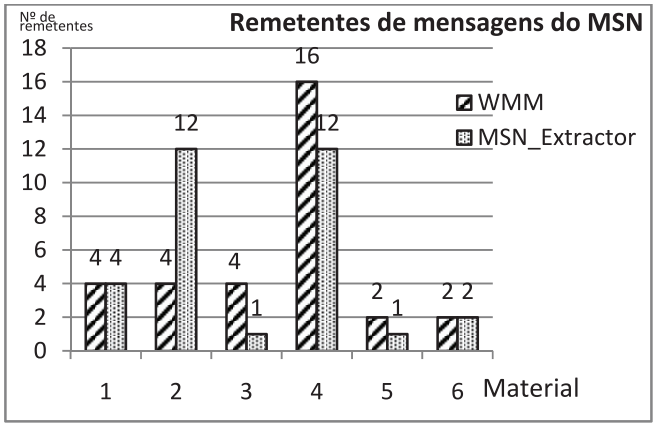

Fig. 8. Remetentes de mensagens do MSN recuperados pelo WMM e pelo MSN_Extractor/EnCase.

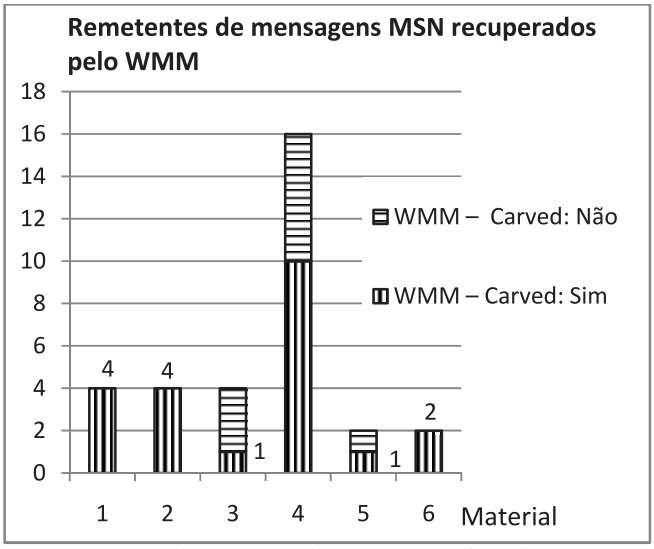

Fig. 9. Remetentes de mensagens do MSN recuperados pelo WMM com a distinção entre o resultado sem carving (Carved: Não) e com carving (Carved: Sim).

- *Mensagens que saíram do computador* – contou-se o número de mensagens originadas no computador analisado, ou seja, mensagens de saída. Nos materiais utilizados neste trabalho, as ferramentas não recuperaram o usuário do MSN que enviou cada uma dessas mensagens de saída.
- *Total de mensagens recuperadas* – contou-se o número total de mensagens que cada uma das ferramentas recuperou, tanto as mensagens dos *usuários remetentes de mensagens,* como as *mensagens que saíram do computador*.

Ambas as ferramentas apresentaram em seus resultados várias mensagens repetidas. Elas foram contadas apenas uma vez. Os resultados do WMM consideram a soma das mensagens ou remetentes encontrados pelas buscas sem carving e com carving.

Os resultados das recuperações de *Usuários remetentes de mensagens* são ilustrados na Fig. 8.

Na Fig. 9 é apresentada a quantidade de remetentes de mensagens do MSN que foram recuperadas apenas pelo

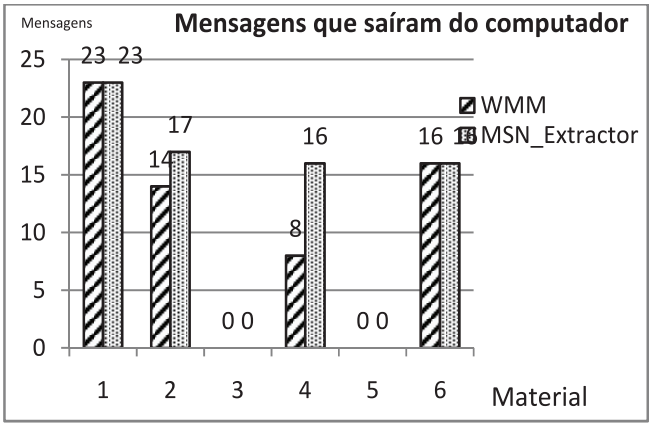

Fig. 10. Mensagens de saída recuperadas pelo WMM e MSN_Extractor/EnCase.

WMM, mostrando a participação do WMM sem carving e com carving para o resultado total obtido por esta ferramenta.

Na Fig. 10 são apresentados os resultados da contagem apenas de *Mensagens que saíram do computador*.

Uma consideração sobre o resultado da Fig. 10 é que as mensagens recuperadas pelo WMM sem carving não foram contadas nas *Mensagens que saíram do computador*, por não ser possível identificar no seu resultado as mensagens de saída separadamente, conforme explicado anteriormente na Seção *II.D*.

Na Fig. 11 é apresentado o total de mensagens que o WMM e que o MSN_Extractor/EnCase recuperaram.

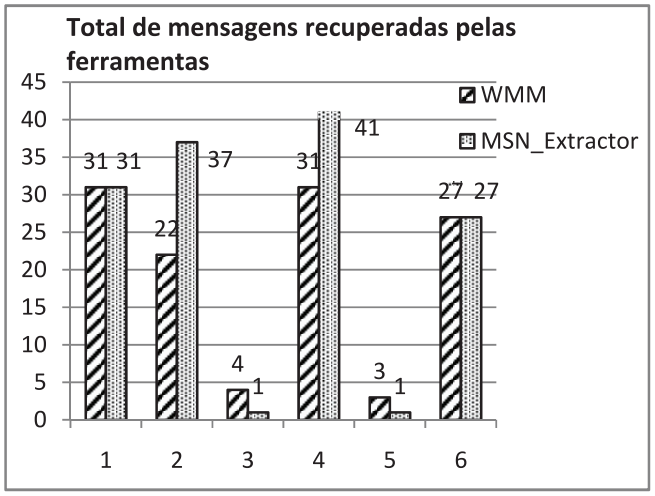

Fig. 11. Total de mensagens recuperadas pelo WMM e MSN_Extractor/EnCase.

Pelos resultados obtidos, observou-se que as duas ferramentas atuam diferentemente sobre os materiais. Na Tabela IV, são mostradas as áreas analisadas por cada ferramenta em busca de conversas do MSN.

TABELA IV – Atuação das ferramentas sobre os materiais	
WMM	Arquivos conhecidos deixados pelo MSN na área de usuários do Windows.
	Áreas livres do disco, utilizadas pelo carving.
EnCase	Todas as entradas de arquivos, incluindo aquelas recuperadas por *Recover Folders* em áreas não alocadas (*Unallocated Clusters*).

No caso do EnCase, foram encontrados resultados (*Search Hits*) em arquivos como pagefile.sys (arquivo de paginação do Windows), que pode não ser coberto pelo WMM. Nesse arquivo, podem ter sido encontradas as mensagens a mais que o MSN_Extractor/EnCase recuperou no caso dos materiais 2 e 4 na Fig. 11.

Por outro lado, dos casos em que o WMM encontrou mais remetentes ou mais mensagens, esse resultado pode ter sido graças à sua capacidade de interpretação dos arquivos deixados pelo MSN, como é o caso dos materiais 3 e 5 na Fig. 11, onde o WMM Sem Carving encontrou, respectivamente, três e duas mensagens a mais do que o MSN_Extractor, que só encontrou uma mensagem em cada material, a mesma encontrada pelo WMM com carving.

Além dos resultados já apresentados, em três dos materiais foram encontrados arquivos xml contendo gravações de conversas do MSN, no formato de quando este é configurado para gravar as conversações. Por exemplo, um diretório correspondente ao usuário MSN continha arquivos nomeados com a identificação de cada um dos contatos do usuário, no formato <QuickName + Passport_ID>.xml, onde o atributo *QuickName* é basicamente o e-mail do contato, sem o domínio [1]. Entretanto, essas conversas estavam gravadas em diretórios de backup e não faziam parte do MSN instalado nos computadores. Por isso, não foram encontradas pelo WMM, nem pelo MSN_Extractor/EnCase porque este só recupera os traços do protocolo eventualmente gravados no computador quando o MSN se conecta ao servidor da Microsoft pela porta 80, devido a um firewall, por exemplo [3].

Devido a esses achados, sugere-se utilizar as ferramentas de análise forense, como EnCase ou FTK, para análise de arquivos xml ou, mais especificamente, para busca do arquivo de folha de estilos Messagelog.xsl, que identifica a presença e favorece a leitura do conteúdo dos arquivos xml, encontrados geralmente na mesma pasta. Recomenda-se também procurar por arquivos HTML, que podem conter as gravações de conversas quando o "Messenger Plus!" está instalado. Por fim, sugere-se testar o WMM 2009 mesmo quando o WMM 0.2.0 encontrou resultado, para o caso de haver mais de uma versão do MSN instalada. Esse software encontrou usuários MSN e sua lista de contatos em um dos materiais examinados.

4. Conclusão

Pelos resultados obtidos, apesar de haver coincidência entre as mensagens recuperadas pelas duas ferramentas, nem sempre seus resultados foram iguais. Portanto, não é possível recomendar o uso de uma das ferramentas em detrimento da outra, porque houve casos em que o WMM 0.2.0 encontrou mais mensagens que o MSN_Extractor no EnCase, como também houve casos em contrário, onde o MSN_Extrator teve um melhor desempenho.

ANEXO I – script msn_extractor

```
/*
 Antes rodar este script é necessário executar uma busca (GREP)
pelas seguintes palavras chaves:

 Outcoming MSN: MSG #+ [A-Z] #+[^\x0D\x0A]+
 Incoming MSN: MSG [a-z#~_\.!\#$%\^&\*\(\)\-]+@[a-z#_\-]+\.
[a-z#_\-\.]{2,3} [^\x0D\x0A]+

 Os arquivos com as mensagens recuperadas serão gravados na
pasta MSN sob o diretório do caso.
 Qualquer dúvida: rogerio.rdsj@dpf.gov.br

*/
```

```
class MainClass {
  typedef String[] StringArray;
  StringArray command;
  String outPath;

  void Main(CaseClass c) {
    outPath = c.Path().GetFilePath()+"\\MSN\\";
    StringArray command(0, 0);
    LocalMachine.CreateFolder(outPath);

    int i = 0;
    forall (SearchHitClass hit in c.SearchHitRoot()) {

      if (!hit.IsFolder()) {
        if ((hit.KeywordName()==”Incoming MSN”) || (hit.
KeywordName()==”Outcoming MSN”)){
          //Console.WriteLine(“Hit Offset:” +  hit.FileOffset() + “
Length:” + hit.Length());
          //Console.WriteLine(“Hit Preview:” +  hit.Preview());
          //Console.WriteLine(“Hit KeywordName:” +  hit.
KeywordName());
          //Console.WriteLine(“Hit Text:” +  hit.HitText());
          EntryClass e = hit.GetEntry();
          //if (e)
            //Console.WriteLine(“Hit Entry:” +  e.FullPath());

          Tokenizer(“ “,hit.HitText(),command);
          if(command.Count()==4){
            int payload = int::Convert(command[3], int::DECIMAL);
            String content = getPacketContent(hit,e,payload);

            if(isMessage(content)){
              String msg = extractMessage(content);
              //Console.WriteLine(“Mensagem: “ + msg);
              writeToFile(msg,command[1]);
            }
          }
        }
      }
    }
    Console.WriteLine(“Arquivos gravados em “ + outPath);
  }


  bool isMessage(String content){
    int length = content.GetLength();
    uint index = content.Find(“Content-Type: text/plain”,0,length);
    if((index<length) && (index!=-1)) { return true; }
    else {return false; }
  }

  bool isEmail(String str){
    int length = str.GetLength();
    uint index = str.Find(“@”,0,length);
    if((index<length) && (index!=-1)) { return true; }
    else {return false; }
  }

  String extractMessage(String content){
    StringArray lines(0, 0);
    String msg = “”;
    //Console.WriteLine(“>>>”);
    //Console.WriteLine(content);
    //Console.WriteLine(“<<<”);

    Tokenizer(“\r\n”,content,lines);
    if(lines.Count()>=5){
      for(int i=4;i<lines.Count();i++){
        msg = msg + lines[i].SubString(1,lines[i].GetLength()-1) +
“\r\n”;
      }
    }
    return msg;
  }

  void writeToFile(String msg, String from){
    LocalFileClass lf();
    if(isEmail(from)){
      if (lf.Open(outPath+from+”.txt”,FileClass::APPEND)){
        lf.SetCodePage(CodePageClass::UTF8);
        lf.Write(“>> “+ msg);
      }
    }else{
      if (lf.Open(outPath+”outgoing.txt”,FileClass::APPEND)){
        lf.SetCodePage(CodePageClass::UTF8);
        lf.Write(“ >> “+ msg);
      }
    }
    lf.Close();
  }

  String getPacketContent(SearchHitClass hit, EntryClass e, int
payload){
    EntryFileClass ef();
    uint opts = 0;
    String msg;
    if (ef.Open(e, opts)) {
      ulong pos = hit.FileOffset() + hit.HitText().GetLength() + 2;
      ef.Seek(pos);
      ef.SetCodePage(CodePageClass::UTF8);
      ef.ReadString(msg,payload);
      ef.Close();
    }
    return msg;
  }

  void Tokenizer(String delimiter,String txt,StringArray array){
    uint start = 0;
    uint length = txt.GetLength();
    uint index = txt.Find(delimiter, start, length);
    uint count = 0;
    uint size = 0;
    while(true){
      if((index>length) || (index==-1))
        index = length;
      count++;
      array.SetCount(count);
      String token = txt.SubString(start,index-start);
      array[count-1] = token;
      start = index + 1;
      index = txt.Find(delimiter, start, length);
      if((index==length) || (start>length))
        break;
    }
  }
}
```

Referências

[1] Galileu Batista de Sousa. WMM – Uma ferramenta de extração de vestígios deixados pelo *Windows Live Messenger* - ICCyber 2008

[2] Marcelo Henrique Ferreira de Medeiros, Galileu Batista de Sousa. Extração de vestígios do *Windows Live Messenger 2009* - ICCyber 2009.

[3] Rogério Dourado. Código MSN_Extrator.EnScript. Comunicação interna.

[4] EnCase Forensic Version 6.18 User's Guide.

Klarissa de Souza Jerônimo é Perita Criminal da Polícia Federal, lotada no Setor Técnico Científico da Superintendência Regional da Polícia Federal no Maranhão (e-mail: Klarissa.ksj@dpf.gov.br).