Extração de vestígios do *Windows Live Messenger 2009*

Marcelo Henrique Ferreira de Medeiros
Galileu Batista de Sousa
Departamento de Polícia Federal

Abstract – ***Windows Live Messenger - WLM - remains the most popular instant messenger on the Internet. In current version, Microsoft has changed totally the local storage cache for contact lists, in order to provide robustness and reliability. The new features, internal structures and relevant characteristics of this cache are presented in this paper. Following the steps of another tool, WMM, we present a new tool, WMM 2009, to help forensic analysts to get traces left by WLM 2009 in a fully automatic manner.***

Index terms – **Instant Messaging, Windows Live Messenger, MSN Messenger, Extensible Storage Engine, Conversation content, contact list. ESENT. WLM. WMM.**

I. INTRODUÇÃO

NO contexto de investigação policial e perícia criminal, recuperar vestígios deixados por programas de comunicação instantânea tem adquirido uma importância crescente, especialmente porque esse modo de comunicação é cada vez mais frequente e, muitas vezes, tem substituído as ligações telefônicas convencionais. O *Microsoft Windows Live Messenger* (WLM), ou simplesmente MSN, continua sendo o programa mais usado atualmente, com mais 40 milhões de usuários somente no Brasil [3]. Apesar disso, esse tema ainda tem sido pouco estudado, sob a perspectiva forense. Em 2008, [1] indicou o suporte das principais ferramentas forenses à recuperação de vestígios do MSN, mencionando a ausência dessa funcionalidade no FTK, uma rudimentar forma de recuperação de conversações no *Encase* e o suporte a antigas versões no *Paraben Chat Examiner*.

Uma ferramenta nomeada WMM foi apresentada em [1], com o objetivo de automatizar todo o processo de extração e apresentação dos vestígios deixados pelo WLM 8.X. No mesmo artigo, [1] faz uma análise aprofundada sobre a localização, a decifragem e a interpretação de tais vestígios. Em [4], referência clássica sobre artefatos forenses associados ao WLM, pode-se encontrar uma visão mais geral sobre os demais artefatos deixados pelo WLM 8.X. No corrente ano, peritos da polícia belga desenvolveram uma ferramenta, que apesar de não possuir a abrangência do WMM, disponibiliza uma interface de integração com o *WinHex Forensics*.

Na sua versão WLM 2009, o MSN armazena o *cache* local dos contatos de uma maneira completamente diferente. O presente trabalho visa a interpretar esta nova arquitetura, baseada na tecnologia *Microsoft ESENT* (*Extensible Storage Engine*). Com essa interpretação é possível atualizar o trabalho de desenvolvimento da ferramenta WMM proposta por [1], demonstrando as mudanças ocorridas entre versões do WLM e propondo a versão WMM 2009, como complementação da ferramenta inicial. Adicionalmente são mantidas as mesmas funcionalidades para rastreamento de conversações encontradas na versão anterior do WMM.

Este trabalho está organizado como segue: na seção II discute-se a evolução das formas de armazenamento de alguns dos artefatos deixados pelo WLM em suas várias versões, até chegar à versão atual. Além disso, discute-se a metodologia de pesquisa e desenvolvimento utilizada. A principal contribuição deste artigo está à seção III, no qual é apresentado detalhadamente o modelo para o banco de dados de contatos do WLM 2009. Na seção IV, apresenta-se uma versão do WMM para a extração dos vestígios descritos na seção III, o WMM 2009. Sugestões para trabalhos futuros estão na seção V e a conclusão na seção VI.

II. O BANCO DE DADOS DE CONTATOS

A Evolução da armazenagem de informações pelo WLM

A gravação local da lista de contatos de um usuário do MSN tem mudado significativamente entre as versões do *software*. Na versão 7.X, os dados eram cifrados usando a *Microsoft Data Protection* API (DPAPI), a qual dificultava sobremaneira análises *off-line*. Na versão 8.X, os dados passaram a ser cifrados com o algoritmo AES, com uma chave derivada do nome do passaporte [1].

Na versão 2009 (WLM 2009), não há mais cifragem dos dados e, seguindo a tendência de outras ferramentas da *Microsoft*, como o *Exchange Server* e o *Active Directory,* os dados do WLM 2009 estão organizados sob a arquitetura de um banco de dados *ESENT* (*Extensible Storage Engine*), também conhecida como *Jet Blue.* Trata-se de uma implementação de base de dados *ISAM,* nativa no Windows, que habilita aplicações a armazenarem a recuperarem dados de tabelas usando cursores de navegação indexados ou sequenciais de maneira rápida, em uma estrutura leve e hierárquica [2].

Apesar de implementar um sofisticado mecanismo de banco de dados, a *ESENT* não possui *drivers* de acesso com interfaces ODBC ou JDBC, o que significa um desafio adicional à implementação do WMM 2009.

Marcelo Henrique Ferreira de Medeiros é Papiloscopista Policial Federal, lotado no Núcleo de Tecnologia da Informação da Superintendência Regional do Departamento de Polícia Federal no Estado do Rio Grande do Norte.

Galileu Batista de Souza é Perito Criminal Federal, lotado no Setor Técnico-Científico da Superintendência Regional do Departamento de Polícia Federal no Estado do Rio Grande do Norte.

B Metodologia

O processo de engenharia reversa da base de dados de contatos armazenados pelo WLM 2009 resumiu-se, inicialmente, à execução de *dump* dos nomes das tabelas do banco de dados *contacts.edb*, utilizando-se a ferramenta de linha de comando *esentutl.exe (Microsoft Windows Database Utilities, Version* 5.1 para *Windows XP*; *Extensible Storage Engine Utilities for Microsoft Windows Version* 6.0 para *Windows Vista*). Todos os experimentos foram feitos em instalações reais do *Microsoft Windows XP* com *Service Pack* 3 e *Microsoft Windows Vista* com *Service Pack* 1, O software WLM 2009 instalado para análise tem seu número de versão: 2009 (14.0.8064.206). Além desses, é necessário instalar o *Microsoft .NET Framework 3.5* [6].

A partir do estudo da ferramenta *esentutl.exe,* conseguiu-se extrair metadados de tabelas e índices da base de dados de contatos, porém a ferramenta não permite a extração do esquema completo, nem dos dados em si. A falta de suporte a JDBC (e ODBC) e a dificuldade de programação usando a própria API do ESENT, conduziu ao uso da interface *ESENT Managed Interop* distribuída livremente em [5] e que tem como linguagem nativa *Microsoft* C#. Essa API funciona como um encapsulamento para a ESENT Win32 API e é disponível através de uma DLL (*Esent.Interop.dll)*, compatível com todas as versões do *Windows*, a partir do *XP*.

A partir da utilização da API *ESENT Managed Interop*, toda a extração de dados passou a ser realizada por protótipos que evoluíram até chegar à versão proposta do WMM 2009, descrita na seção IV.

C A Base de Dados contacts.edb

Ainda que a estrutura de armazenamento de conversações tenha sido mantida na versão 2009, não sendo por isso discutido no presente texto, o armazenamento local das listas de contatos mudou completamente. A mudança é tão significativa que toda a base de dados dos contatos, antes distribuída em vários arquivos, torna-se reduzida ao arquivo ***contacts.edb*** e seus *logs* de controle. É importante frisar que para cada usuário logado no WLM 2009 é criada uma nova instância da base de dados *contatcs.edb,* exclusiva para aquele usuário.

O arquivo *contacts.edb* é encontrado, por padrão, no diretório (em português): **"C:\Documents and Settings\<WindowsUserName>\Configurações locais\Dados de *aplicativos\Microsoft\WindowsLiveContacts\<DBINST>\DBStore"*.** O parâmetro <*DBINST*> é denominadado *Global Unique identifier (GUID)* [4]. O *GUID* é um inteiro de 128 *bits* (16 *bytes*), gerado através uma função com baixa probabilidade de colisão, a partir de uma semente. Existem vários algoritmos de geração de *GUID,* mas até o momento, não foi determinado qual deles é utilizado pelo WLM 2009, nem a semente usada, embora os autores acreditem ser esta baseada no passaporte do usuário.

No mesmo diretório do arquivo principal há, tipicamente, um subdiretório **"LogFiles",** contendo arquivos de controle e "redo" da base de dados**.** Inicialmente estes arquivos são nomeados por: **edb.log**, **res1.log** e **res2.log**. Outros arquivos de controle são gerados no decorrer do uso do WLM 2009, porém são vinculados ao banco de dados em si, não tendo vinculação específica ao WLM 2009.

III. OS DADOS EM *CONTACTS.EDB*

A base de dados **contacts.edb** guarda em sua estrutura interna vinte e nove tabelas e seus respectivos índices. Observando essas tabelas e seus relacionamentos, verificou-se a existência de quatro domínios de informações, que orbitam a tabela principal do WLM: *WindowsLiveID.*

Importante observar que no decorrer desta seção utilizaremos um nome simplificado para cada tabela. Na base de dados, as tabelas têm seus nomes simplificados e seguidos por um sufixo que é a versão do modelo de dados utilizado pelo WLM. Verificou-se, por exemplo, que a tabela *GroupView* tem campos extras em diferentes versões menores do WLM 2009. Nos casos analisados, encontraram-se, nas tabelas, os seguintes sufixos de versões: "-v080826-1607-1288" e "-v01111-0856-1203".

Os domínios são definidos como: **Contatos**, **Categorias**, **Circle** e **Sistema**, cujas tabelas, suas características e campos relevantes serão discutidos mais adiante.

A Fig. 1 apresenta graficamente os domínios, sem nomes das tabelas neles contidas, para melhor visualização.

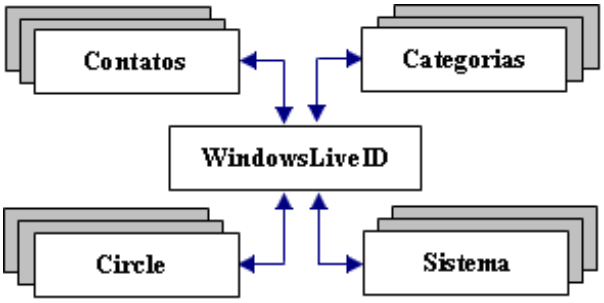

Fig. 1. Representação dos domínios de informação em contacts.edb.

A Tabela I apresenta as tabelas do banco de dados dentro de seus respectivos domínios de informação. Pode ser observado que a tabela *WindowsLiveID* fará relacionamentos com todos os domínios, contudo, ela ficará agrupada no domínio **Contatos** para melhor entendimento.

TABELA I
ENUMERAÇÃO DAS TABELAS E SEUS DOMÍNIOS

Domínios	Tabelas
Contatos	*WindowsLiveID, Member, Name, SimpleContact, StreamTable, ContactID, ContactIdTable, Certificate, Date, Email, IMAddress, Level1Properties, Person, PhoneNumber, PresenceData, Photo, SimpleContactWrite, PhysicalAddress, Position e Url*
Categorias	*GroupView, Group e GroupSpecific*
Circle	*CircleSpecific, CircleView e CircleContactView*
Sistema	*Changetable, Updatetickettable e SyncItem*

A Domínio Contatos

As tabelas do domínio **Contatos** armazenam todas as informações relativas aos contatos de um usuário WLM, como por exemplo: nome completo, endereços residencial e

comercial, telefones, sites, e-mail, dentre outros. A Fig. 2 mostra as suas tabelas principais em negrito e sombreado, além das tabelas auxiliares. Em seguida, serão dadas explicações sobre as principais tabelas e seus respectivos campos.

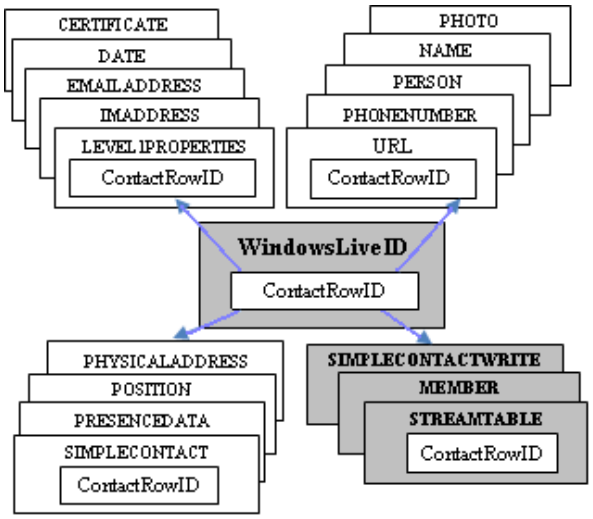

Fig. 2. Principais tabelas do domínio Contatos

Relacionamentos do domínio Contatos

WindowsLiveID é a tabela central de todos os relacionamentos encontrados no WLM 2009. Nela encontramos cadastrados todos os contatos e categorias de um usuário WLM. Seus campos principais são: CID (*ContactID*), que faz vinculação direta ao usuário de contato identificando-o unicamente; *ContactRowID*, que é chave estrangeira de todos os relacionamentos encontrados nas tabelas deste e de outros domínios de informação; e, *Value*, que, se preenchido, indica o *passport* de um contato, ou, senão, representa uma Categoria.

SimpleContact armazena os dados mais significativos do cadastro de um contato. É desse relacionamento com *WindowsLiveID* que se obtém as informações sobre um contato cadastrado. Os campos chaves para relacionamentos são: CID e *ContactRowID*, os quais identificam o usuário e os relacionamentos com tabelas auxiliares, respectivamente. Existe, também, o campo *UniqueID*, que faz ligação com a tabela *SimpleContactWrite* – uma redundância de *SimpleContact,* adicionada de campos de controles. Os dados em *SimpleContact* são utilizados pelo WMM 2009 para gerar o relatório de contatos de um usuário do WLM 2009.

Member cadastra informações de convites enviados ou recebidos para fazer parte da lista de contatos. Encontra-se, também, o histórico de negociação de permissão, bloqueio e pendência. Seus principais campos são: CID, *DisplayName, Passport* (*emails MSN* e *Hotmail,* entre outros) e *Role* (Histórico de negociação). Particularmente, essa tabela faz relacionamento usando o campo CID e não o campo *ContactRowID*, como nos outros relacionamentos.

StreamTable armazena duas colunas: *streamData* e *streamName*. O campo *streamData* guarda em seu conteúdo texto em XML, sem qualquer cifragem, no formato já apresentado em [1]. Basicamente, o XML contém dados sumarizados do usuário WLM, como: CID, *Name*, *UniqueID*, *QuickName* (nome simplificado), *FirstName*, *LastName*, *MsnAddress*, *PassportCategory*, *StatusMessage* (Mensagem de apresentação), *UserTileLocation*, dentre outros. Além disso, contém informações de controle de sincronização dos contatos do WLM. No WLM 8.X esses dados apresentavam-se nos seguintes arquivos: *".MeContact" e ".AddressBook".* Para maior detalhamento sobre esse processo, vide [1], seção "III-B. Conteúdo dos arquivos".

Na Tabela I têm-se referências a outras tabelas, não discutidas em detalhes aqui. Por exemplo, a tabela *PresenceData,* armazena a mensagem inicial do usuários, e, a *Url,* guarda os sítios que o usuário informou em seu cadastro de MSN.

B Domínio Categorias

O domínio **Categorias** referencia as categorias que o usuário criou para organizar sua lista de contatos na interface do WLM 2009. Os nomes das tabelas desse domínio de informações contêm a expressão *group,* o que pode causar confusão. Nas interfaces visuais do *Messenger* (MSN/WLM) até a versão 8.X, a denominação **Categorias** não existia, e sim a palavra **Grupos**, significando o agrupamento de contatos que um usuário identifica como tendo características em comum. A partir da versão 9.X e posteriores, o termo **Grupos** passou a ter outra semântica – refere-se aos conjuntos de contatos que fazem parte de "grupos de discussão" em *groups.live.com* dos quais o usuário principal participa, como convidado ou criador - melhor se vinculando ao domínio **Circle**, descrito mais adiante. Ou seja, embora no nome das tabelas do domínio **Categorias** conste o termo *group*, essas nada se associam a grupos de discussão, mas apenas às classes de organização dos contatos na interface visual, que agora se denominam Categorias.

A Fig. 3 representa simplificadamente o domínio Categorias com suas tabelas e seus relacionamentos. Na Tabela I, encontram-se as tabelas que compõem o domínio Categorias.

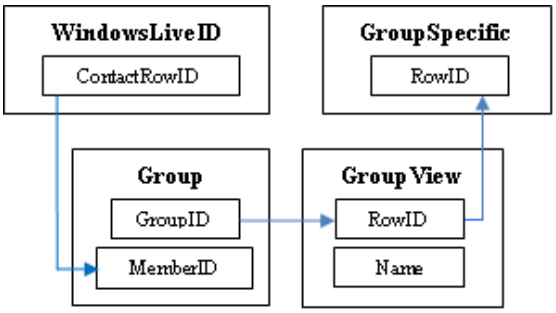

Fig. 3. Principais tabelas do domínio Categorias

Relacionamentos do domínio Categorias

Group é a tabela principal do domínio Categorias. É através dela que acontece o relacionamento de um contato com as Categorias *default* do próprio WLM ou com as categorias que o usuário WLM criar. As chaves de relacionamento são *GroupId* que se liga à tabela *GroupView*; e *MemberID* que se liga à tabela *WindowsLiveId*.

GroupView armazena primordialmente as características de uma categoria como o seu nome (campo

Name). O campo chave é *RowID*, que se relaciona à tabela *Group* através do campo *GroupID* desta e, relaciona-se com a tabela *GroupSpecific* através do campo GroupID.

GroupSpecific armazena dados extras de controle interno do WLM, não significativos para o estudo corrente. O campo chave dessa tabela é o *RowId*. Seu relacionamento é mostrado na Fig. 3.

A Fig. 6, na seção IV, exemplifica a divisão em Categorias e os respectivos contatos das mesmas, além de agrupar os contatos sem categorias em uma categoria denominada, pelo próprio WLM, de "Outros Contatos".

C Domínio Circle

O domínio **Circle** referencia os grupos de discussão que foram criados pelo próprio usuário WLM no *groups.live.com* ou aqueles em que ele participa como convidado. A Fig. 4 representa o domínio *Circle* de maneira simplificada; na Tabela I encontram-se os nomes de todas as suas tabelas componentes.

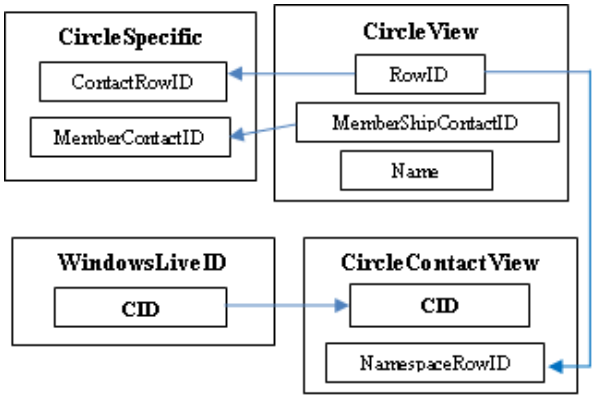

Fig. 4. Principais tabelas do domínio **Circle**.

Relacionamentos do domínio Circle

CircleContactView armazena os dados referentes aos convites efetuados para participação em um grupo de discussão no *groups.live.com*. Os campos (chaves estrangeiras) são: CID e *NamespaceRowID*. Essa tabela se relaciona com *WindowsLiveID* e *CircleView,* vide Fig. 4.

CircleView contém, entre outros campos, o nome do grupo de discussão em *Name*. Essa tabela se relaciona com *CircleContactView* e *CircleSpecific*. Esses relacionamentos têm o objetivo de recuperar dados complementares como por exemplo a personalização do ambiente gráfico do WLM, o esquema de cores e os dados de sincronização entre os participantes do *Circle*. Os relacionamentos são apresentados graficamente na Fig. 4.

CircleSpecific guarda informações sobre os convites aceitos ou não, e outros dados de controle de sincronização do programa local com o *groups.live.com*. Seus principais campos são *ContactRowID*, *MembershipContactID*. Seu relacionamento é visualizado na Fig. 4.

D Domínio Sistema

O domínio **Sistema** representa tabelas que guardam dados utilizados pelo próprio WLM. Os autores acreditam que esses não estão diretamente relacionados à Lista de Contatos, mas aos dados de controle de versões, atualizações, modificação de estrutura de tabelas, dentre outros. Suas tabelas são *Changetable, Updatetickettable e SyncItem.* Essas tabelas não serão discutidas aqui, pois não apresentaram dados relevantes de investigação.

E Codificação de campos chaves

Durante o processo de engenharia reversa dos relacionamentos das tabelas *GroupView* e *GroupSpesific* com a tabela *Group* , verificou-se a necessidade de uma inversão de *bytes* de *little-endian* para *big-endian,* no campo *RowID,* para que se concretizassem os relacionamentos em si. Contudo, apenas os 16 *bytes* iniciais desta chave devem ser invertidos e não todos os 32 *bytes.*

Mais precisamente, nos relacionamentos demonstrados na Fig. 3, os campos *RowID* das tabelas *GroupView* e *GroupSpesific* têm o seguinte formato "**ABCDEFGH-IJKL-MNOP**-QRST-UVWXYZ012345" (32 caracteres hexadecimais, com quatro separadores "-", somando 36 *bytes*). Na tabela *Group*, os campos *GroupID* e *MemberID* têm o formato "**GHEFCDABKLIJOPMN**QRSTUVWXYZ012345" (32 caracteres hexadecimais sem separadores). Observam-se, em destaque, os 16 primeiros *bytes* em ordem diferente e todo o campo em formato diferente, tornando, assim, impossível o relacionamento direto entre essas tabelas. A inversão necessária é expressa na forma de um pseudocódigo, apresentado na Fig. 5.

```
internal static string ConvertKey16(string t){
String[] V{};
  V[0] = t[6];        V[1] = t[7];        V[2] = t[4];
  V[3] = t[5];        V[4] = t[2]         V[5] = t[3];
  V[6] = t[0];        V[7] = t[1];        V[8] = "-";
  V[9] = t[10];       V[10] = t[11];      V[11] = t[8];
  V[12] = t[9];       V[13] = "-";  V[14] = t[14];
  V[15] = t[15];      V[16] = t[12];  V[17] = t[13];
  …
  Return V;
}
```

Fig. 5. Pseudocódigo para inversão de campos chaves.

IV. O WMM 2009

Para validar os conceitos e oferecer às forças policiais uma ferramenta para coleta de vestígios do WLM 2009, os autores buscaram implementar uma evolução do WMM, contudo, conforme explicado em seção precedente, a *Microsoft* vem, gradativamente, convergindo seus produtos para a utilização da arquitetura de armazenamento de informações *ESENT*, dando, nesse caso, maior capacidade ao WLM, a partir da versão 9.X.

Embora a integração do WMM 2009 ao WMM ainda seja uma meta dos autores, ela se mostrou complicada de início, por não existirem, até o momento, APIs Java para o ESENT. Portanto, o desenvolvimento da nova versão foi executado em linguagem C#, para a qual existe uma *interface* (API) para o *ESENT*, permitindo experimentação, decodificação do modelo de dados e, ao mesmo tempo, viabilizando o desenvolvimento da ferramenta mais rapidamente.

O WMM 2009 tem um padrão de operação similar ao WMM [1]. O protótipo tenta recuperar os contatos de um usuário através de acesso direto ao banco de dados *contacts.edb* (e seus arquivos de *log*). As conversações (*chat logs*), se armazenadas, também são recuperadas. Em sua atual versão, WMM 2009 não faz o rastreamento da

estrutura de diretórios, identificando os arquivos associados a todos os usuários, nem tampouco consulta o *Registry* para descobrir bancos de dados de contatos armazenados fora dos diretórios padrões.

Passado um banco de dados *contact.edb* como parâmetro, o resultado da execução do WMM 2009 é um conjunto de arquivos HTML's contendo os contatos, seus grupos de contatos (categorias, no jargão WLM 2009) e demais propriedades. Os arquivos de conversações, quando existentes, são apresentados sem nenhum tipo de modificação, uma vez que já são legíveis.

O WMM 2009 funciona sem que seja necessária a execução do sistema operacional onde o WLM estava originalmente instalado. Diferentemente da versão anterior, não é necessário o mapeamento de uma unidade de disco do sistema hospedeiro, apenas são necessários que os arquivos *contacts.edb, edb.log, res1.log e res2.log* sejam acessíveis ao programa. Esses três últimos em um subdiretório chamado *LogFiles*.

O resultado da execução do WMM 2009 pode ser observado na Fig. 6, onde nomes de usuários e fotografia foram riscados por motivo de preservação de privacidade.

WMM 2009

WLM User Main	PassportID	Actual Photo
[redacted]@hotmail.com	1388252269	

MSN Groups (Categories)	Contacts
'Favoritos'	[redacted]@hotmail.com' - '[redacted]' [Log Chat] [redacted]@hotmail.com' - '' [Log Chat]
'Colegas de trabalho'	[redacted]@hotmail.com' - '[redacted]' [redacted]@hotmail.com' - '[redacted]' [Photo] [redacted]@hotmail.com' - '[redacted]'
'Categoria de Desconhecidos'	[redacted]@hotmail.com' - '[redacted]' '' - '[redacted]'
'Amigos'	[redacted]@gmail.com' - '[redacted]' [redacted]@hotmail.com' - '[redacted]' [redacted]@hotmail.com' - '[redacted]' [redacted]@gmail.com' - '[redacted]'
Others Contacts (Anyone Categories)	'' - '[redacted]' [redacted]@hotmail.com' - '[redacted] [Photo]' [redacted]@gmail.com' - '[redacted]' [redacted]@hotmail.com' - '[redacted]' '' - '[redacted]' [redacted]@hotmail.com' - '[redacted] [Photo] [Log Chat]' '' - '[redacted]' [redacted]@gmail.com' - '[redacted]' '' - '[redacted]'

Files found in "HISTORY"
C:\Documents and Settings\[redacted]\Meus Documentos\Meus Arquivos Recebidos\[redacted]1388252269\Histórico
C:\Documents and Settings\[redacted]\Meus Documentos\Meus Arquivos Recebidos\[redacted]1388252269\Histórico\[redacted]28629012.xml
C:\Documents and Settings\[redacted]\Meus Documentos\Meus Arquivos Recebidos\[redacted]1388252269\Histórico\[redacted]601210121.xml
C:\Documents and Settings\[redacted]\Meus Documentos\Meus Arquivos Recebidos\[redacted]1388252269\Histórico\[redacted]230492323.xml

Fig. 6. Resultado da execução do WMM 2009

Ao clicarmos em qualquer *QuickName* de contatos, vide Fig. 6, será visualizada uma nova página no navegador com maior detalhamento de informações sobre aquele contato. Existindo *log* de conversação, tem-se *link* a partir de "[Log Chat]", vide Fig. 6, para arquivo correspondente; existindo fotografia ou *avatar* de um contato, tem-se *link* a partir de "[Photo]", vide Fig. 6, para o relatório de detalhamento do contato. A fotografia do contato, se existir, será apresentada nesse relatório. Vê-se um exemplo na Fig. 7.

User Contact

Photo:	
MSN Address:	'[redacted]@hotmail.com'
Quick Name:	'[redacted]'
Initial Message:	''
Talk Mensage:	'[redacted]'
Identification Name:	''
MSN Passport:	''
Single Identification:	'f02b0d1193eade44911eff00dbfa396c'
Contact Identification:	''
First Contact at:	'2009-05-07T19:23:27.23-07:00'
Contact Status:	''
Asking Status from Contact:	''
Calculated Buddy Identifier:	'[redacted]@hotmail.com'
Home Email:	''
Home Phone:	''
Mobile Phone:	''
Other Email:	''
Othe IM Email:	''

Fig. 7. Informações detalhadas de um contato

O WMM 2009, em sua interface, disponibiliza campos para preenchimento com o caminho de diretórios para auxiliá-lo na busca pelos *logs* de conversações e fotografias dos contatos e usuário WLM. Há, por motivos de praticidade, uma funcionalidade de preenchimento automatizado que sugere a localização desses diretórios. Encontra-se também, na versão atual do WMM 2009, funcionalidade para localização automática de todas as listas de contatos (bancos de dados *contacts.edb*) dos diversos usuários de WLM em um mídia específica;

Como não há necessidade de *mount* da partição a extração de vestígios é feita em modo *off-line*. Além disso, a estrutura de diretórios pesquisados pode ter uma *language* diferente da sugerida inicialmente. Assim, se os *logs* existirem, serão criados *links* de acesso no formato Conversações. Observa-se os links dos *logs* de conversações de cada um dos contatos na Fig. 6.

V. TRABALHOS FUTUROS

Os autores apresentam neste trabalho uma ferramenta para extração de vestígios deixados pelo WLM 2009, porém vários trabalhos adicionais necessitam ser considerados, entre eles:

- Integração ao WMM 8.X;
- Identificação de localização dos bancos de dados usando acesso *off-line* ao *Registry* da mídia questionada;

- *Carving* de arquivos e conversações, no padrão do WMM;

É de suma importância também o acompanhamento da evolução do WLM 2009, para garantir que a ferramenta desenvolvida se mantenha compatível com esse *software*.

VI. CONCLUSÃO

Desde a sua publicação, o WMM vem sendo usado por várias forças policiais e tem se mostrado útil na investigação forense e na materialização de delitos. Este trabalho apresenta uma evolução nesse caminho e representa uma nova e inédita vertente na recuperação de vestígios deixados pelo WLM, ao identificar e extrair contatos e seus relacionamentos da sua versão 2009.

No texto decodifica-se a arquitetura de armazenamento dos dados de contatos do WLM 2009 e apresenta-se um protótipo de ferramenta (o WMM 2009), que será integrado, no futuro ao WMM para que esse continue "um passo adiante na identificação da localização e apresentação dos vestígios deixados pelo WLM" [1].

REFERÊNCIAS

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

[2] *Microsoft. Extensible Storage Engine*. Disponível *online* em http://msdn.microsoft.com/en-us/library/ms684493(VS.85).aspx.

[3] *Microsoft*. Disponível online em http://advertising.microsoft.com/brasil/windows-live-messenger

[4] Wouter S. van Dongen. *Forensic artefacts left by Windows Live Messenger 8.0*

[5] *ESENT Managed Interop*. Disponível online em http://www.codeplex.com/ManagedEsent.

[6] *Microsoft .NET Framework 3.5*. Disponível online em http://download.microsoft.com/download/6/0/f/60fc5854-3cb8-4892-b6db-bd4f42510f28/dotnetfx35.exe