**Brazilian Journal of Forensic Sciences, Medical Law and Bioethics**

Journal homepage: www.ipebj.com.br/forensicjournal


# Investigação Forense Digital em Redes Sociais: A Análise das Evidências de Crimes no *Facebook* e no *Twitter*

# Digital Forensic Investigation on Social Networks: The Analysis of Crime Evidences on Facebook and Twitter

Deivison Pinheiro Franco[1,a] e Nágila Magalhães Cardoso[2]

[1] *Mestrando em Inovação Tecnológica, Especialista em Ciências Forenses (Ênfase em Computação Forense), em Suporte a Redes de Computadores e Tecnologias Internet e em Redes de Computadores, Graduado em Tecnologia em Processamento de Dados*

[2] *Graduada em Tecnologia em Redes de Computadores e Especialista em Segurança Computacional*

[a] *E- mail: deivison.pfranco@gmail.com*

Received 22 November 2013

**Resumo.** As redes sociais se tornaram quase indispensáveis na vida de qualquer pessoa - são inúmeros acessos a todo instante. Seja por dispositivos móveis como *smartphones*, *tablets* ou por computadores, toda espécie de informação pode ser compartilhada através de redes sociais, assim tornaram-se ferramentas úteis para qualquer tipo de pessoa, entre os quais se destacam os criminosos de diversas espécies como traficantes, pedófilos, fraudadores, sequestradores, homicidas, ladrões entre outros que estão usando esses sites para fins ilícitos. Visto que o número crescente de organizações criminosas usando as redes sociais como apoio e meio para utilidades criminosas, surgiu desde então a necessidade de saber como analisar também essas promissoras fontes de vestígios, a fim de comprovar e desvendar um determinado crime. Autoridades investigadoras responsáveis pela aplicação da lei uma parte delas já estão utilizando redes sociais como o *Facebook* e *Twitter* para busca de evidências ou pistas correlacionadas ao delito. Entretanto pode-se perceber que ainda existe muito pouco de um modelo construído e difundido especificamente para investigação forense em redes sociais e agentes da lei devem ter a noção desses sites, bem como as técnicas para investigá-las. Dessa forma, este artigo vem contribuir na abordagem de um pequeno modelo voltado para este propósito com o foco nas redes *Facebook* e *Twitter*.

**Palavras-Chave:** Redes Sociais; Crime; Facebook; Twitter; Evidência.

http://dx.doi.org/10.17063/bjfs3(3)y2014233

**Abstract.** Social networks have become almost indispensable in any person's life - are innumerable access at all instant. Whether by mobile devices such as smartphones, tablets or computers, all species of information can be shared through social networks, so have become useful tools for any type of person, among which stand out the criminals of various species as traffickers, pedophiles , fraudsters, kidnappers, murderers, thieves and between others who are using these sites for illicit purposes. Viewed that the increasing number of criminal organizations using social networks as support and mean for utility criminal emerged since then the need to know how to analyze also these promising sources of vestiges in order to prove and unveil a determined crime. Investigating authorities responsible for law enforcement a part of them are already using social networks as Facebook and Twitter to search for evidence or clues correlated to the offense. However, it can be noticed that there is still much little of a model built and broadcast specifically for forensic research on social networks and law enforcement should have the notion of these sites, as well as the tools and techniques to investigate them. Thus, this paper contributes in a small model turned for this purpose with the focus on Facebook and Twitter networks.

**Keywords:** Social Networks; Crime; Facebook; Twitter; Evidence.

## 1. Introdução

Desde o surgimento dos computadores e, consequentemente, da *Internet*, novas formas de comunicação e tantas outras atividades foram promovidas e práticas comuns acabaram sendo incorporadas nesse meio, como é o caso dos crimes. Desde então surgiu a necessidade de uma ciência capaz de investigar e capacitar profissionais a fazer exames periciais nesses tipos de tecnologia.

Em decorrência do uso da *Internet* destacam-se com crescimento explosivo as redes sociais como *Facebook*, *Twitter*, *Google Plus*, *Linkedin*, *Instagram* entre tantas outras que se tornaram comuns na vida de qualquer pessoa, resultando, assim, em um aumento significativo de sua utilização como atrativo para atividades criminosas e consequentemente onde um grande manancial de informações é possível de serem encontradas em um determinado perfil de rede social e que, por sua vez, pode ter um grande valor na apuração de crimes em juízo, assim como qualquer outro meio de armazenamento de dados já habitualmente analisados pela pericia forense computacional.

Uma página do *Facebook*, por exemplo, pode ser usada para planejar um assalto, homicídio, ou grupo de malfeitores podem usa-lo para reunir novos membros e defender suas intenções criminais. Apresentar muitas informações a respeito de um suspeito, associadas a conhecidos, amigos, família, mensagens, grupos etc., através das quais é possível criar uma teia detalhada de

relacionamentos acerca do que, ou de quem, se está investigando, podendo colaborar na descoberta de um círculo criminoso inteiro.

O campo da perícia forense computacional e as agências policiais tem visto que as redes sociais não podem ser passadas despercebidas e devem ser incluídas nas investigações quando for preciso. A razão para investigar emerge com o valor para apresentar uma abordagem sistemática que pode ser usado por investigadores forenses digitais a fim de tentar resolver esses tipos de rede baseada em crime cibernético, para ajudar a garantir que a prova digital recuperada pode ser usada em um tribunal de direito[1].

A análise da prova nos crimes cometidos através dos meios virtuais é de suma importância, tendo em vista a crescente adesão do uso de computadores e dispositivos móveis conectados às redes sociais amplamente utilizadas para estreitar as distâncias entre pessoas.

## 2. Redes Sociais: as Fontes de Vestigios de Crimes para Perícia Forense Computacional

As redes sociais incrivelmente passaram a ser uns dos recursos mais utilizados e de grande gosto mundial pelas pessoas, onde inúmeras espécies de informações são depositadas na página frequentemente. Assim como celulares e em computadores, nas redes de relacionamento toda informação é armazenada, registrada e pode ser apagada a qualquer momento pela intervenção humana, ou seja, também pode se denominar como uma verdadeira fonte de dados sobre atividades pessoais de uma pessoa.

Os *sites* de redes sociais são muito mais do que “LOL”, “OMG”, “curtir”, *posts* engraçados, RT e *tweets* de 140 caracteres. Eles podem servir como provas importantes de registros de fotos, mensagens, localização podem ser encontradas[2].

A mídia social tornou-se o meio preferido de comunicação para muitos superando até mesmo o tão conhecido e-mail em sua popularidade e, portanto qualquer tipo de comunicação inevitavelmente leva à possibilidade de evidência[3]. Como consequência à popularidade dos meios de comunicações social, se encontram indivíduos dotados de má índole que veem a mídia social como uma ferramenta oportuna para estreitar a amizade entre criminosos e promover ações delitivas e a partir disso trouxe a necessidade de perícia em mídia social.

Por seguinte as abordagens de casos são exemplos das formas mais comuns da vida evidenciada em redes sociais como *Facebook* e *Twitter*, de como as

pessoas interagem com elas, e como suas informações podem ser usadas como prova.

### 2.1 *Facebook*

Para um investigador forense, uma análise do *Facebook* pode ser em grande grau uma riqueza de informações. Ele pode fornecer um histórico da vida de uma pessoa, sobre fotos, amigos, família, comentários, postagens na linha do tempo, informações de localização onde uma pessoa estava em uma data e hora específica, podendo revelar dados valiosos que irão permitir desvendar toda, ou boa parte, de um ato criminoso.

Um exemplo de caso real em que a análise do *Facebook* serviu para identificar um criminoso foi o de *Sarah Cafferkey* na cidade de *Melbourne*, na Austrália, no qual seu assassino, *Steven Hunter*, descrevia sua casa como sendo a "masmorra do estupro". Como ele já havia sido condenado por esfaquear uma jovem até a morte da mesma forma de *Sarah*, isso gerou indícios para um novo envolvimento de crime. Ao se realizar uma análise no perfil de *Sarah*, a policia descobriu que em 4 de novembro, cinco dias antes de *Sarah* desaparecer, ela havia tido uma pequena discussão com *Steven* no *Facebook*. Em um *post* (Figura 1) *Steven* e outro usuário, *Chris Stewart*, sugeriram fazer sexo a três com a garota. Irritada, ela criticou a maneira como a mente deles agia e pediu que o comportamento imaturo parasse ou ela iria excluir os dois de seu perfil. Com um pouco mais de investigação no alvo foi comprovado que o assassino era *Steven Hunter*[4].


**Figura 1.** Sarah Cafferkey em uma foto postada no *Facebook* (*print screen* do perfil).

### 2.2 *Twitter*

Esta rede social uma espécie de mistura de *blog* com mensagens de celular em apenas 140 caracteres, conhecida como *microblogging* que permite basicamente aos usuários enviar e receber atualizações pessoais de outros contatos em tempo real e também as enviadas a outros usuários[5] se tornou também meio utilizado por sujeitos praticantes do crime, sendo assim também um ótimo produtor de vestígios.

Caso de exemplo foi o *twee*t de *Jameg Blake* usado como prova de ter assassinado "amigo" dele chamado *Kwame Dancy*. Horas antes do assassinato, *Blake* teria discutido pelo *Twitter* com seu amigo e, em uns dos *tweets*, tuitou a seguinte frase: "*R.I.P Kwame*" ("*Rest in Peace*" expressão que significa "descanse em paz") a qual ocasionou em uma ótima prova-chave no julgamento do caso[6].

## 3. A Investigação Forense e as Redes Sociais *Twitter* e *Facebook*

Presente na vida de quase todas as pessoas, as redes sociais além de aproximar as pessoas, também se tornou local de encontro e ousadia entre criminosos de toda espécie entre eles pedófilos, traficantes, fraudadores, sequestradores, homicidas, terroristas, ladrões entre outros e servir a estes como *modus operandi* (modo de operação) para planejar e executar proezas ilegais.

Redes sociais foram inicialmente utilizadas com o propósito de promover a amizade. Entretanto, o crescimento da *Internet* e a sua popularização permitiu que elas se expandissem e crescessem rapidamente e, com isso, despertando o interesse de criminosos em utilizar mais essa ferramenta para praticar atos delituosos. Isso indica o quanto que esses *sites* podem se tornar hospedeiros de muitas pessoas que representam uma ameaça à segurança[7], evidenciando que redes sociais podem se tornar também redes sociais de crimes.

Diante do exposto, é possível observar que potenciais rastros de informações expostos publicamente ou não em uma página (perfil) se transformaram em novas fontes de vestígios que em muitos casos pode resultar em grandes fontes de evidências. Cabendo ressaltar que a pesquisa nesse assunto é algo novo que só agora está sendo mais estudado e analisado em relação a outras fontes de investigações periciais, já que muitas informações publicadas em páginas e perfis de redes sociais vêm servindo como prova e ajudando na solução de crimes.

Policias brasileira e americana, estão usando redes sociais como *Facebook, Twitter*, entre outros *sites* de relacionamentos, para buscar informações, provas e testemunhas que possam ajudar a solucionar processos criminais e até mesmo

rastrear suspeitos[8]. A NYPD (Departamento de Polícia de Nova Yorque) já possui unidades de análise e investigação de redes sociais[9].

Como toda e qualquer pessoa, criminosos também sentem a necessidade e a vontade de estarem nas redes sociais em qualquer hora, de qualquer lugar, mas o propósito não é simplesmente fazer amizades, é algo muito mais que isso - se trata de um lugar obscuro onde eles planejam crimes, trocam materiais obscenos e deixam vitimas pelo caminho. E enquanto aqueles mais experientes acham maneiras de mascarar e esconder suas mensagens, existem aqueles que simplesmente deixam as informações expostas e as agências de investigações e peritos forenses precisam trabalhar a fundo no que essas redes representam, a fim de descobrir evidências sobre uma pessoa, de toda uma rede criminosa, ou pelo menos uma parte dela.

### 3.1 Crimes Cometidos com o Uso de Redes Sociais

Com essa realidade apresentada, diversas formas de crimes são praticadas com o uso das redes sociais, e para que seja possível investigá-las é importante considerar e diferenciar a possibilidade de se evidenciar duas modalidades de prática de delitos: Redes Sociais como Apoio ao Crime e Redes Sociais como Meio do Crime, as quais serão detalhas e explicadas a seguir.

#### 3.1.1 Redes Sociais como Apoio ao Crime

Nesta modalidade de crime uma rede social é usada estrategicamente como mais uma utilidade de apoio ao delito, onde os criminosos utilizam este serviço para contatar e estreitar amizades com outros comparsas e futuras vítimas através de trocas de mensagens, publicações sobre planejamento, reuniões, discussões, sequestro, assassinato, estelionato, tráfico de drogas e pessoas, dentre outros.

Quanto ao crime de estelionato, por exemplo, pode-se citar o caso real em que uma quadrilha foi presa pela polícia de Manaus por vender falsas milhas de passagens aéreas pelo *Facebook*[10]. Este tipo de crime teve como apoio a rede social, mas também poderia ter sido realizada de outra forma, caso este recurso não existisse. Neste caso, o *Facebook* está associado ao modo de operação do crime.

Como qualquer outra ferramenta (agendas, veículos, telefones celulares etc.), a rede social é utilizada como uma utilidade auxiliar, ou seja, facilitadora para realização de um crime[11].

Se o crime for relacionado a tráfico de drogas, por exemplo, um traficante poderia utilizar o *Facebook* para contatar e vender drogas na página social ou poderia fazer esse mesmo processo pelo método tradicional sem o uso da tecnologia. A Figura 2 ilustra este caso.

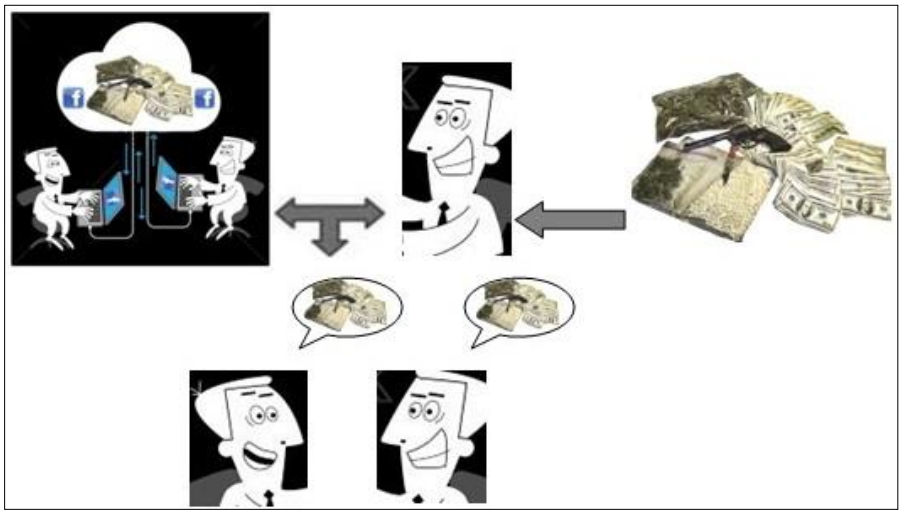

**Figura 2.** Representação de redes sociais como apoio do crime (criação dos autores).

### 3.1.2 Redes Sociais como Meio do Crime

Nesta modalidade de crime a rede social é a peça principal para a realização do delito, ou seja, caso a rede de relacionamento não existisse, o crime não seria praticado. Crimes como roubo de dados por meio de *malwares* proliferados pelo *Facebook*, induzimento e compartilhamento de imagens de pornografia infantil, são exemplos dessa modalidade.

A Figura 3, a seguir, demonstra um exemplo desse tipo de modalidade, onde um pedófilo cria um perfil falso no *Facebook* se passando por uma criança para atrair e induzir a vítima a adicioná-lo como amigo na rede social e, com isso, conseguir manter relações e obtenção e compartilhamento de fotos da vítima. Dessa forma, pode-se observar que o *Facebook* é o meio primordial para que o crime ocorra.

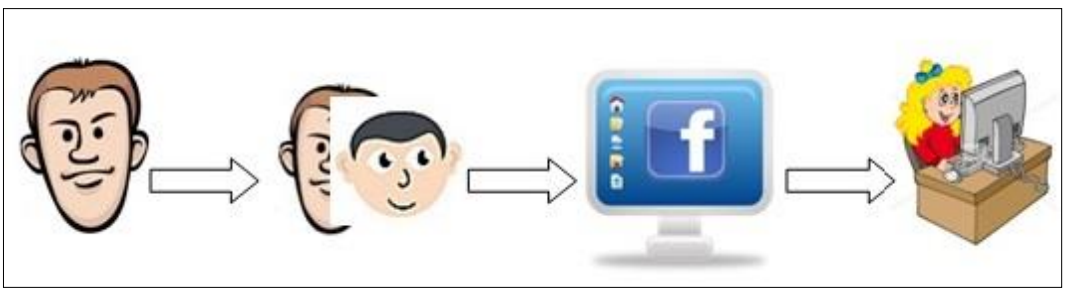

**Figura 3.** Representação de redes sociais como meio do Crime (criação dos autores).

### 3.2 Características Importantes a Serem Consideradas

#### 3.2.1 Sensibilidade a Tempo de Uso

As informações inseridas em qualquer rede social são sensíveis e podem ser apagadas pelo usuário a qualquer momento e, quando de sua exclusão, há poucas chances de recuperação. Mesmo assim, ainda é possível recuperá-las por meio de ferramentas forenses específicas.

#### 3.2.2 Facilidade de Cópia

Conteúdos no *Facebook* e *Twitter* como fotos, mensagens, vídeos, *links*, entre outros dados, podem ser facilmente copiados para um dispositivo de armazenamento através de *print screen* na evidência específica ou ainda via recurso que se encontra em "configurações da conta" do *Facebook* com a opção: "Baixe uma cópia dos seus dados do *Facebook*". O mesmo ocorre no *Twitter* ocorre de forma semelhante.

#### 3.2.3 Possibilidade a Inverídico

Informações publicadas podem ser manipuladas, como na criação de um perfil falso para fins ilegais, a fim de alguém se passar por quem que não é. Um pedófilo, por exemplo, pode criar um perfil falso no *Facebook* se passando por uma criança, ou um individuo pode fazer *check-in* em um determinado país estando em outro diferente, como mostrado na Figura 4, ou seja, é possível manipular essa informação, e isso vai da criatividade ou do objetivo de se dizer onde se está, seja no país de origem, ou fora dele, isto é, em qualquer lugar.

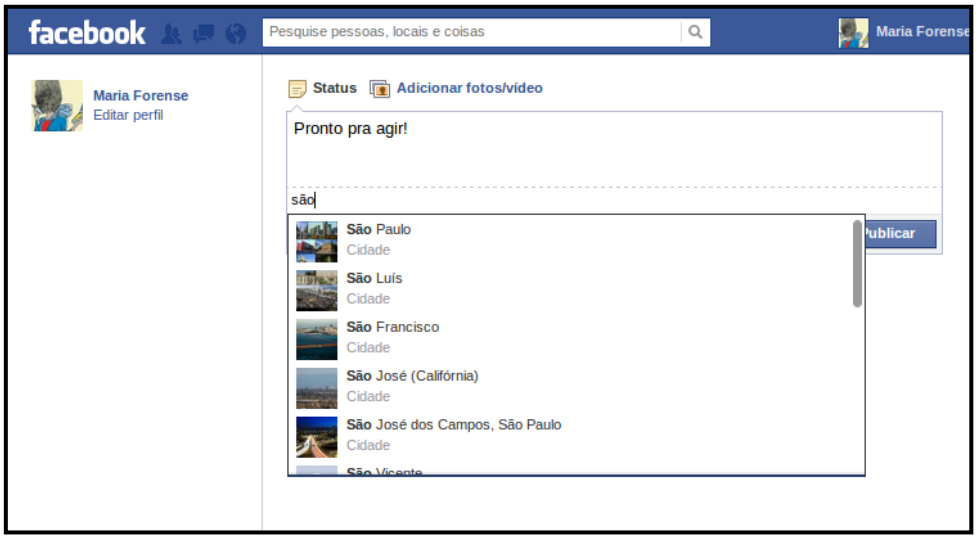


**Figura 4.** Exemplo de possibilidade a inverídico (*print screen* do perfil criado pelos autores no *Facebook*).

Dessa forma, é possível que o investigador obtenha informações a partir de um perfil criado no *Facebook* as quais não correspondam a real identidade real de quem criou e usa essa página. No entanto, é possível se obter outras informações relevantes tais como endereço IP de um titular de conta usada durante a sua criação original ou os endereços IP do titular da conta usada para acessá-la - que pode ser rastreado até uma conta de usuário suspeita[12].

### 3.3 Identificação do ID de um Perfil

#### 3.3.1 *Facebook*

A identificação do usuário no *Facebook* pode ocorrer em duas maneiras: a primeira representada numericamente por quinze dígitos após o ID (https://www.facebook.com/profile.php?id=números) ou simplesmente (https://www.facebook.com/números). Esta identificação é única e não pode ser alterada, ou seja, mesmo que o indivíduo mude seu nome de perfil, o ID continua o mesmo.

Na primeira, a visualização do ID é possível de ser verificado quando se posiciona o cursor do *mouse* em cima da foto de perfil ou da capa. O último bloco de números representa o ID, conforme é mostrado na Figura 5. Sendo que ainda é possível descobrir o ID de um usuário através de *sites* que oferecem serviço para tal como o *Find My Facebook* ID (http://findmyfacebookid.com).

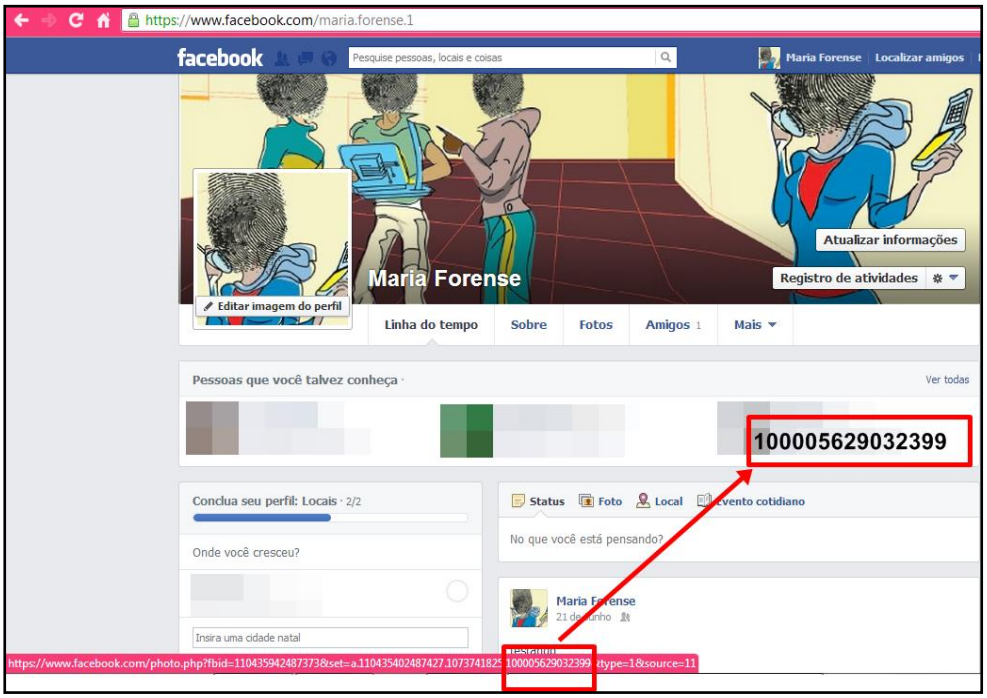


**Figura 5.** Identificação numérica (ID) (*print screen* do perfil criado pelos autores no *Facebook*).

Já a segunda maneira é a mais amigável e de fácil visualização, onde a identificação se dá através do nome do próprio usuário após o nome de domínio (https://www.facebook.com/nomedousuario), sendo possível alterar este nome apenas uma vez para a inclusão do nome verdadeiro.

Cabe ressaltar que as duas formas correspondem à identificação do usuário. Entretanto, a segunda é a mais utilizada devido sua facilidade de percepção, afinal basta estar no perfil do usuário para visualizá-la na barra de endereços do navegador.

### 3.3.2 *Twitter*

A identificação do usuário é caracterizada pelo *nickname,* logo após o nome de domínio do *Twitter* na barra de endereços no navegador (https://twitter.com/nickname).

O *Twitter* também possui uma identificação numérica composta de uma quantidade variável, porém essa identificação não é de fácil visualização, nem conhecida.

Pode-se encontrá-la através de sites que oferecem esse serviço, como o *My Twitter* ID (http://mytwitterid.com) e o *Get Twitter* ID (http://gettwitterid.com) que oferecem o serviço de encontrar o ID apenas digitando o *username* de um usuário. A Figura 6 exibe o site *My Twitter* ID em execução, onde foi digitado o *username* "*netnagila*", o qual retornou seu respectivo ID (241933097).


**Figura 6.** Identificação numérica (ID) (*print screen do My Twitter* ID em execução).

### 3.4 Localização de Evidências

#### 3.4.1 *Facebook*

**- Linha do Tempo (*Timeline*):** A *timeline* é onde está o chamado "poço de informações" para os investigadores forenses, nela se encontram todas as atividades de recursos que o *Facebook* oferece como, por exemplo, postagens e compartilhamento de outras redes sociais tais quais *Foursquare*, *Instagram*, *Twitter*, além de fotos, vídeos, localização, informações pessoais, interesses ("curtidas"), publicações de amigos, grupos etc..

**- *Timestamp* (Registro de Atividades e Identificação do Aparelho Eletrônico de Origem de uma Postagem):** O *Facebook* registra todas as atividades de data e hora em que um evento é registrado por um computador através do *timestamp* – informações de extrema importância para investigadores forenses, pois certificam exatamente quando um evento realmente ocorreu[13].

Outro ponto relevante é que o *Facebook* permite identificar se uma postagem na página foi originada por um computador via navegador *web* ou por um dispositivo móvel como um *smartphone* ou *tablet*.

A Figura 7 mostra o exemplo da postagem de localização da usuária Maria Forense na cidade do Rio de Janeiro na data de quinta-feira, 4 de abril, no horário de 17:56, ao se posicionar o *mouse* sobre a data localizada abaixo do nome de usuário.

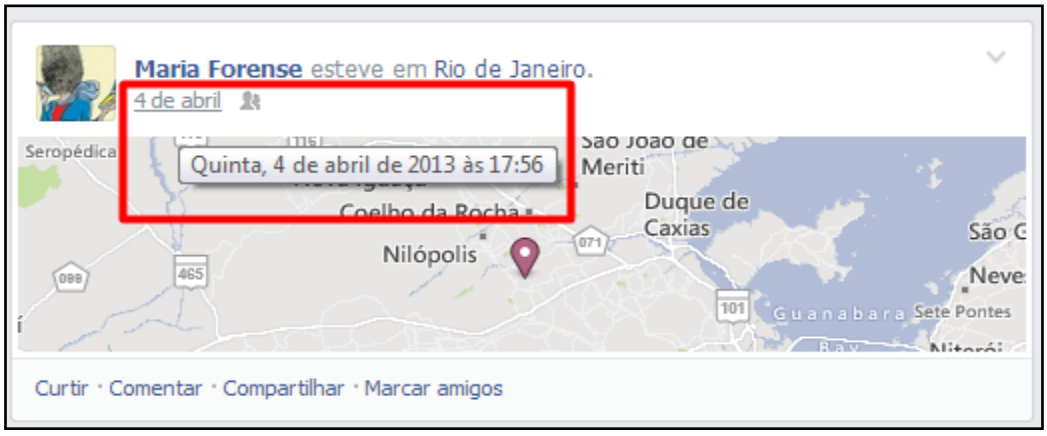


**Figura 7.** Registro de data e hora (*print screen* do perfil criado pelos autores no *Facebook*).

Já na Figura 8, a seguir, pode-se verificar de onde a postagem da foto em que a pessoa foi marcada foi enviada, mostrando exatamente que foi de um *smartphone Windows Phone*, o que facilita na identificação do dispositivo que deverá ser periciado caso seja necessário. Ressalta-se, ainda, que cada dispositivo varia de

acordo com seu modelo, em muitos casos é possível observar apenas "via dispositivo móvel".

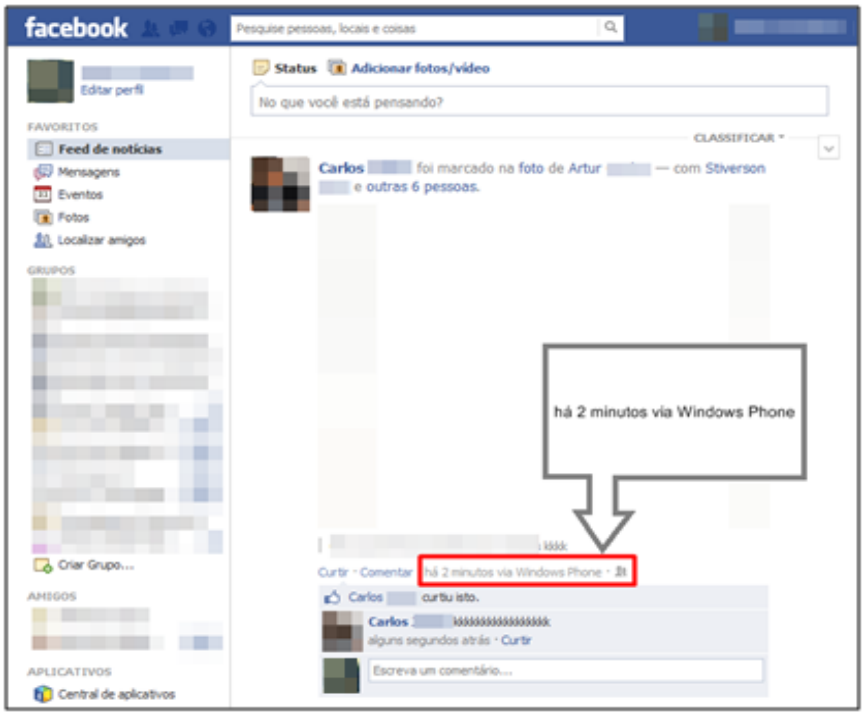


**Figura 8.** Postagem de marcação de fotos por meio de *Smartphone* (*print screen* do perfil criado pelos autores no *Facebook*).

**- Aba Sobre:** Clicando na opção "Sobre", é possível encontrar informações pessoais do indivíduo acerca de trabalho, instituição onde estudou, local onde mora atualmente, data de nascimento, família, número de celular, *e-mail* entre outras informações do contato, que podem ser importantes e colaborar em uma investigação. Incrivelmente há pessoas que expõem esses tipos de informações, o que favorece nas investigações.

**- Aba Fotos:** Nesta seção encontram-se todas as fotos postadas pelo próprio usuário ou nas quais ele foi marcado por algum amigo. Uma análise das fotos é de fundamental importância, elas podem esclarecer sobre certas situações e, às vezes, até servindo como prova de um crime. Em certos casos há possibilidades de o indivíduo ter adicionado o local de onde a foto foi tirada, o que possibilita sua localização.

**- Identificação de Fotos:** Todas as fotos publicadas carregam consigo uma identificação numérica (ID) após o "fbid" (https://www.facebook.com/photo.php?fbid=números) e que fica visível ao se passar o *mouse* por cima de uma foto, ou ao clicá-la, como mostrado na Figura 9.


**Análise na URL da imagem:**

https://www.facebook.com/photo.php?fbid=150119711852329&set=a.149094918621475.1073741828.100005629032399&type=1&theater

150119711852329 (ID da foto)

149094918621475.1073741828 (ID do álbum)

**Figura 9.** Identificação Numérica (ID) da foto (*print screen* do perfil criado pelos autores no *Facebook*).

A identificação permite saber de qual usuário do *Facebook* a imagem foi originada, sendo possível extrair esta informação através do *download* de uma foto do *Facebook*, na ocasião em que a mesma é salva, por padrão, com um nome que apresenta uma numeração específica para cada foto, a qual é composta por 3 blocos de números como, por exemplo, "1458609_576340899087364_1648760575_n", onde o segundo bloco ("576340899087364" neste caso) indica o ID da imagem. Quando este ID é recolocado na barra de endereços do navegador, é possível visualizar sua origem (para o exemplo em questão, dessa forma: https://www.facebook.com/576340899087364).

**- Aba Amigos:** Nesta aba se encontram todos os amigos adicionados pelo individuo dono da conta. Estar analisando os amigos em muitos casos ajuda na investigação, visto que eles têm muito a dizer sobre a pessoa investigada. Observando que em diversas ocasiões a realização de um crime não ocorre somente por uma única pessoa, pois quase sempre há mais alguém que fez parte do ato infracional ou pode indicar pistas na averiguação.

**- Aba Locais:** Esta seção mostra todos os locais onde o indivíduo esteve nos últimos dias ou meses, em um mapa, que foi publicado pela própria pessoa ou marcação de amigos na sua linha do tempo. A Figura, 10 a seguir, mostra a representação dessa aba, onde ao se clicar em “Locais” exibe todos os lugares, em um mapa, onde o indivíduo esteve ou possa estar atualmente. Sendo que em sua linha do tempo é possível ver cada local publicado.


**Figura 10.** Aba locais (*print screen* do perfil criado pelos autores no *Facebook*).

**- Músicas, Filmes, Programas de TV, Livros:** Essas informações descrevem basicamente a característica de determinada pessoa, o que pode auxiliar na identificação do suspeito e, consequentemente, do crime.

**- Aba Curtir:** As opções curtir também tem muito a dizer na identificação de um criminoso, pois são as páginas que um usuário curte, ou seja, tem interesse/empatia sobre um determinado assunto. Por exemplo, se a polícia está procurando por um criminoso de drogas e identifica seu suposto perfil no *Facebook* e vê suas opções de curtir relacionadas à droga, isso já se torna um grande indicio que aquele perfil é o que está sendo procurado ou indica como um apoio à forma pelo qual o crime foi praticado.

**- Grupos:** Pelo *Facebook* é possível se encontrar grupos com pessoas selecionadas para a troca aberta (público) ou fechada (privado) de informações sobre diversos assuntos, na linha do tempo do usuário. É possível se observar somente grupos abertos, pois grupos fechados estarão visíveis apenas na página inicial de um determinado usuário e da qual um investigador necessitará da posse.

Nesse espaço é possível postar fotos, vídeos, arquivos, fazer planos e acompanhar as conversas em andamento. Dessa forma, investigar os grupos dos quais o perfil investigado participa é de fundamental importância visto que, através destes, podem ser encontradas evidências sobre um crime e, possivelmente, a identificação de toda uma quadrilha criminosa que participa do grupo.

**- Identificação do Grupo:** Assim como em um perfil e nas suas fotos é possível encontrar a identificação de um usuário, em um grupo ocorre a mesma coisa.

A identificação do grupo no *Facebook* é representada também numericamente por quinze dígitos após "*groups*" (https://www.facebook.com/groups/números), ou pelo o nome do grupo (https://www.facebook.com/groups/nameofgroup).

Em muitos casos o investigador deve ter atenção ao analisar esse tipo de informação, pois grande parte dos grupos em que criminosos participam possuem disfarce. Por exemplo, em 2011, um grupo no *Facebook* com o nome: "Se tornar pai ou mãe, é o grande presente de vida" foi denunciado e descobriu-se que o mesmo havia sido criado por pedófilos para ter acesso às fotos de menores.

É importante analisar cada informação presente no grupo e suas abas como, por exemplo, a aba "procurar neste grupo" que possui o ícone de uma lupa, cujo objetivo é pesquisar uma determinada palavra ou frase postada dentro do grupo, o que pode facilitar na redução do tempo de pesquisa do perito. A Figura 11 mostra essa função, onde foi feita uma pesquisa pela palavra "crime", a qual retornou todas as postagens com este termo.

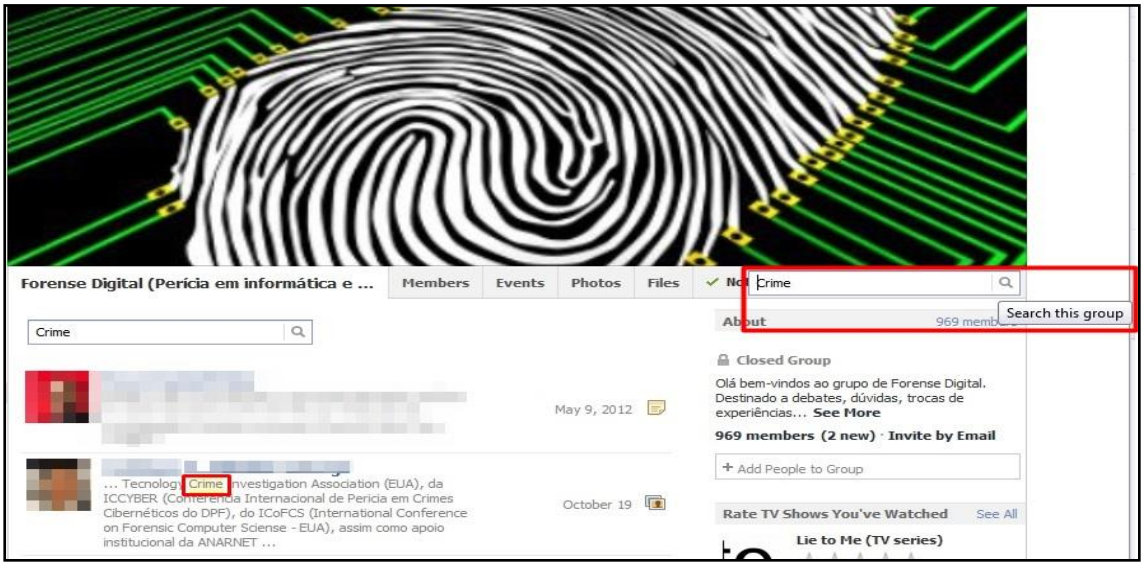


**Figura 11.** Recurso pesquisar (*print screen* do perfil criado pelos autores no *Facebook*).

**- Registro de Atividades:** O registro de atividades é a mina de ouro para investigadores, sendo possível, ainda, compará-lo a um histórico de *Web Browser* que salva todos os registros de navegação do usuário, ou seja, apresenta um verdadeiro dossiê com uma lista de todas as publicações e atividades desde a criação da conta até o dia atual em ordem decrescente, onde é possível visualizar

histórias e fotos em que foi marcado, conexões que fez, bem como quando o usuário curte algo e pesquisa por uma página, locais ou um amigo no *Facebook*. A Figura 12 ilustra o registro de atividades de um perfil.


**Figura 12.** Registro de atividades (*print screen* do perfil criado pelos autores no *Facebook*).

**- Mensagens:** Espaço onde se encontram as mensagens trocadas com outros participantes, sendo possível, inclusive, adicionar fotos e arquivos. Assim como as mensagens, também ficam registradas data e hora. Um ponto interessante ao se fazer a análise, é que é possível identificar de onde as mensagens foram enviadas, se de um dispositivo móvel ou através de um navegador *web* via bate-papo. No primeiro (enviada via *móbile*) é representada pelo ícone de um mini celular ou pelo ícone de localização quando está ativado no dispositivo. No segundo (via *web*) é representada pelo ícone de balão de diálogo. A Figura 13 mostra essas abordagens.

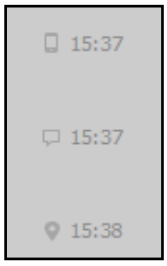


**Figura 13.** Ìcones em uma mensagem (*print screen* do perfil criado pelos autores no *Facebook*).

**- Recurso de Localização em Mensagens:** O uso de dispositivos móveis como *smartphones* e/ou *tablets* permite recursos de localização que muitas das vezes ficam ativados no *Facebook App* ou no *Facebook Messenger*, possibilitando se saber sua localização atual, inclusive com suporte a mapa.

A Figura 14, a seguir, representa o registro de dois usuários trocando mensagens. Ao se clicar na mini visualização do mapa é possível vê-lo em outra janela que se abrirá automaticamente.

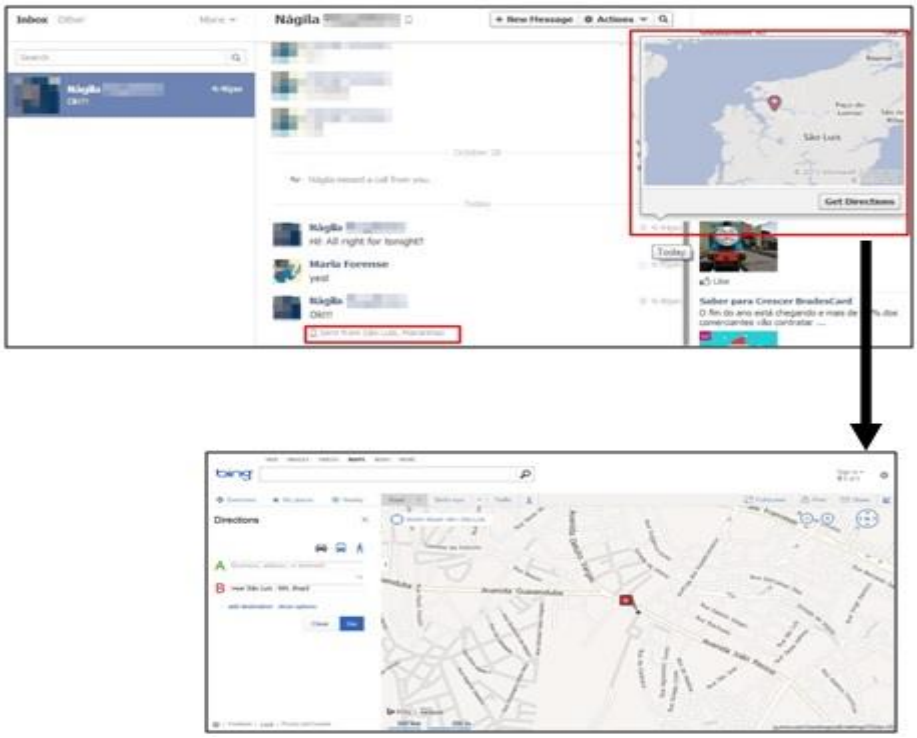

**Figura 14.** Recurso de localização em mensagens (*print screen* do perfil criado pelos autores no *Facebook*).

**- Mensagens - Caixa de Entrada:** Na caixa de entrada aparecem todas as mensagens do usuário, mas é preciso fazer uma análise minuciosa nas outras caixas como: “Outros” (mensagens de outras pessoas que não estão presentes na lista de amigos), “Não Lidas”, “Arquivado” (mensagens guardadas propositalmente pelo próprio usuário) e “*Spam*”, para que elas não passem despercebidas aos olhos do investigador. A Figura 15, a seguir, ilustra a Caixa de Entrada, bem como essas opções.


**Figura 15.** Caixa de entrada (*print screen* do perfil criado pelos autores no *Facebook*).

**- Recurso Pesquisar Conversas na Caixa de Entrada:** o recurso pesquisar tem o objetivo localizar com mais rapidez uma determinada conversa, através da busca por palavras e nomes específicos, o pode otimizar e facilitar o trabalho do perito. A Figura 16, a seguir, mostra esse recurso.


**Figura 16.** Recurso pesquisar em mensagens (*print screen* do perfil criado pelos autores no *Facebook*).

**- Comprovação de Visualização de Mensagens:** O acusado de um crime pode alegar que não viu a mensagem de um cúmplice ou vítima, porém o *Facebook* comprova se a mensagem foi visualizada. Na Figura 17 há a demonstração de um exemplo no qual a usuária Maria Forense envia uma mensagem às 20:06 para João, sendo esta visualizada pelo mesmo às 20:07. Ressalta-se que quem recebe a notificação de visualização é a usuária Maria Forense, já que foi ela quem enviou a mensagem.


**Figura 17.** Comprovação de visualização de mensagem (*print screen* do perfil criado pelos autores no *Facebook*).

Entretanto, existe um grande desafio anti-forense para o investigador, pois ao analisar uma mensagem é possível mostrar que ela não foi visualizada pelo acusado. Mas, isso não vale como prova pelo fato de que o registro "Visualizada - hora" só aparece quando o usuário recebe a notificação de que tem uma nova mensagem, a visualiza diretamente na caixa de entrada sem abri-la, ou simplesmente a marca como lida, como mostrado na Figura 18. Caso contrário, o *Facebook* entende que aquela mensagem ainda não foi lida.


**Figura 18.** Possibilidade e anti-forense (*print screen* do perfil criado pelos autores no *Facebook*).

Diante do exposto, é válido dizer que uma pessoa pode ter visto uma mensagem mesmo quando não está mostrando que foi visualizada. Para melhor entendimento desse processo, a Figura 19 ilustra a interação entre duas pessoas mostrando a ideia da possibilidade de manipulação de uma mensagem a fim de dificultar o trabalho de investigação caso seja descoberta.

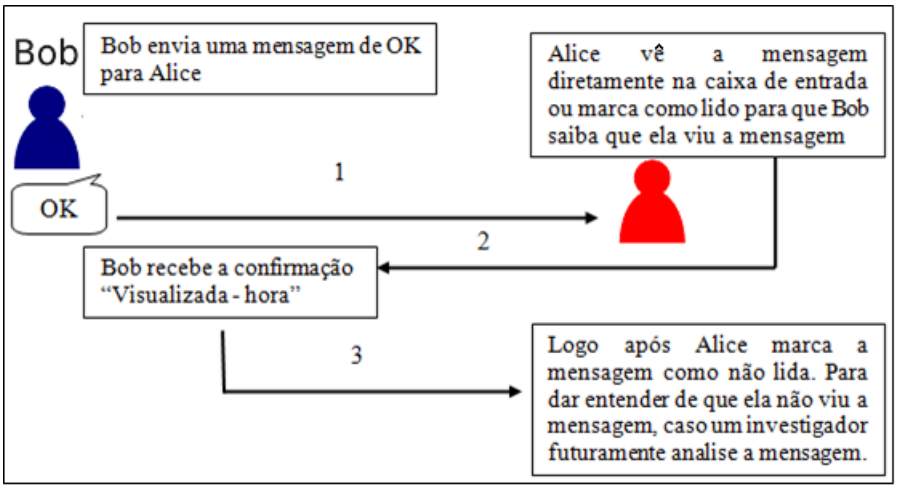


**Figura 19.** Possibilidade e anti-forense – manipulação de mensagem (criação dos autores)

Contudo, como mostrado acima, se Alice marcar a mensagem como não lida (último processo) a única forma de saber se ela está mentindo em dizer que não viu é comprovar, na mensagem original, o registro da hora que foi visualizada, pois o

mesmo permanece no remetente mesmo se o destinatário marcar a mensagem como não lida.

**- Eventos:** Recurso que permite organizar reuniões, responder a convites e manter atualizado sobre os que os amigos estão fazendo. Torna-se importante analisar visto que um individuo, por exemplo, pode ter criado um evento sobre um ato criminoso ou sido convidado por alguém.

### 3.4.2 *Twitter*

**- Perfil:** Em um perfil de uma pessoa no *Twitter* é possível verificar o nome do usuário o qual é sempre seguido pelo símbolo arroba "@", a quantidade de *Tweets*, a quantidade de pessoas que está seguindo e a quantidade de seguidores, dentre outras informações explanadas a seguir que são importantes em uma investigação.

**- *Tweets*:** Assim como no *Facebook*, o *Twitter* mantém o registro de data e hora da postagem de uma publicação, conforme pode-se observar na Figura 20. Sendo que um *tweet* pode-se publicar uma mensagem de até 140 caracteres, podendo incluir, fotos, videos, *links*, *hashtags*, localização e compartilhamento de outras redes sociais. Outra facilidade que pode ser encontrada é que na maioria das vezes as informações postadas (*tweets*) são, em grande parte, públicas e possibilitam que qualquer pessoa de fora possa visualizar as informações do perfil.


**Figura 20.** Registro de data e hora em *tweets* (*print screen* de perfil no *Twitter*).

**- Aba Conectar:** Permite, de forma rápida, visualizar todas as interações relacionadas a um determinado usuário. Ao se clicar em "@Conectar" é possível ver quais *tweets* foram marcados como favoritos, além dos últimos *retweets*, *tweets* (@respostas e menções), bem como novos seguidores. Caso se queira visualizar apenas as @respostas e menções de um usuário específico, basta clicar em menções (*mentions*) que fica logo abaixo de interações (*interactions*). Todas essas funcionalidades e recursos são mostrados na Figura 21 a seguir.

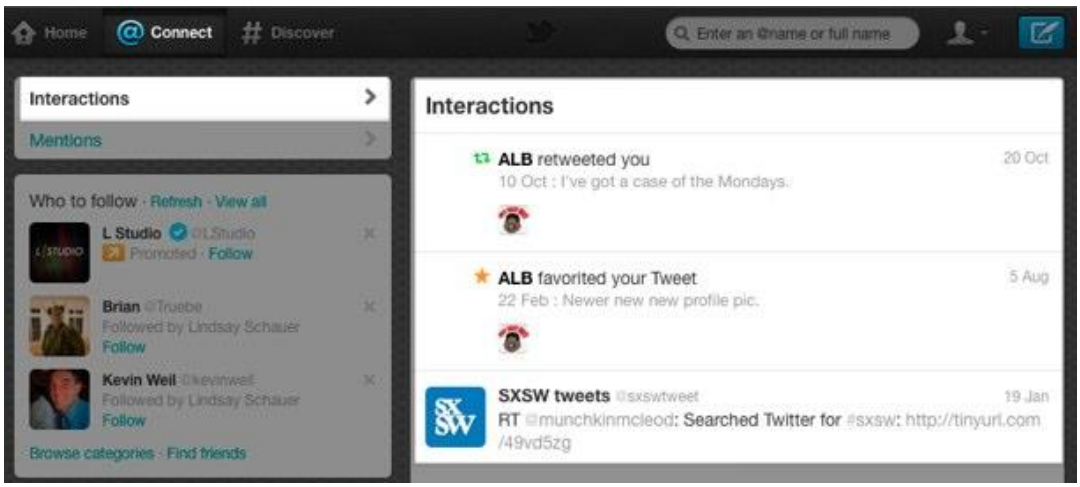


**Figura 21.** Aba conectar de um usuário (*print screen* de perfil no *Twitter*).

**- Mensagens Diretas:** As mensagens diretas, ou simplesmente DM, são mensagens privadas advindas de algum seguidor ou não do usuário, e que são extremamente relevantes no processo investigativo. A Figura 22 mostra esses tipos de mensagens.


**Figura 22.** Mensagem direta de um usuário (*print screen* de perfil no *Twitter*).

## 4. Ferramentas Existentes para Análise Forense em Redes Sociais

### 4.1 *Internet Evidence Finder* - IEF

*Software* da responsabilidade da empresa *Magnet Forensics* (Figura 23) projetado para examinadores forenses e investigadores treinados na aplicação da lei e do governo, bem como o pessoal de segurança de TI em empresas que estão realizando exames forenses completos de computadores *Windows* e *Mac*. Recupera dados de comunicações de redes sociais, artefatos baseados em nuvem, aplicativos P2P de compartilhamento de arquivos, cópias de segurança móvel, *webmail*, histórico do navegador *web*, imagens e vídeos. Pesquisa artefatos vivos e excluídos em discos rígidos e em captura de RAM in vivo. Na versão *Advanced* inclui exames em dispositivos móveis com a plataforma *Android* e *iOS*.


**Figura 23.** Tela de escolha de item de rede social a ser pesquisado no Internet Evidence Finder (*print screen* do programa em execução).

Ao se fazer uma pesquisa com IEF, os itens de redes sociais são identificados e classificados individual e separadamente dos artefatos comuns de navegação *web*, para posteriormente se proceder a análise em cada item recuperado. A Figura 24 mostra o IEF em execução.

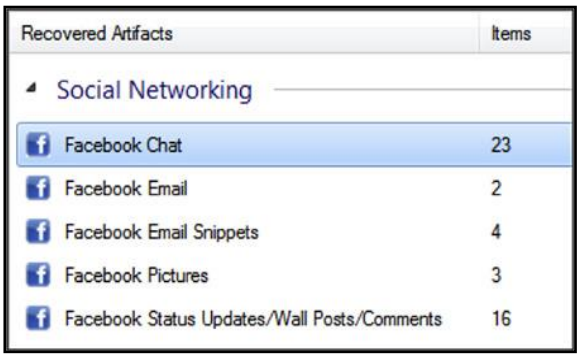


**Figura 24.** Artefatos do *Facebook* recuperados pelo IEF (*print screen* do programa em execução).

### 4.2 *Twitter Investigator*

*Software* forense da empresa *Afentis Forensics* destinado a investigadores forenses, empresas de auditoria e agências governamentais, o *Twitter Investigator* é uma solução importante para investigações em mídia social. É um poderoso motor de pesquisa de menção, palavras-chaves, mineração de dados, captura fotos, URLs do *tweet*, monitoração em tempo real, notificação por *e-mail* ou SMS e representação gráfica de atividades de conta, produção de laudos periciais em MS Word, HTML, ou PDF detalhando a investigação e preservando automaticamente os *logs* de auditoria

verificáveis para atender um tribunal ou requisitos processuais. A Figura 25 mostra o *Twitter Investigator* em execução.

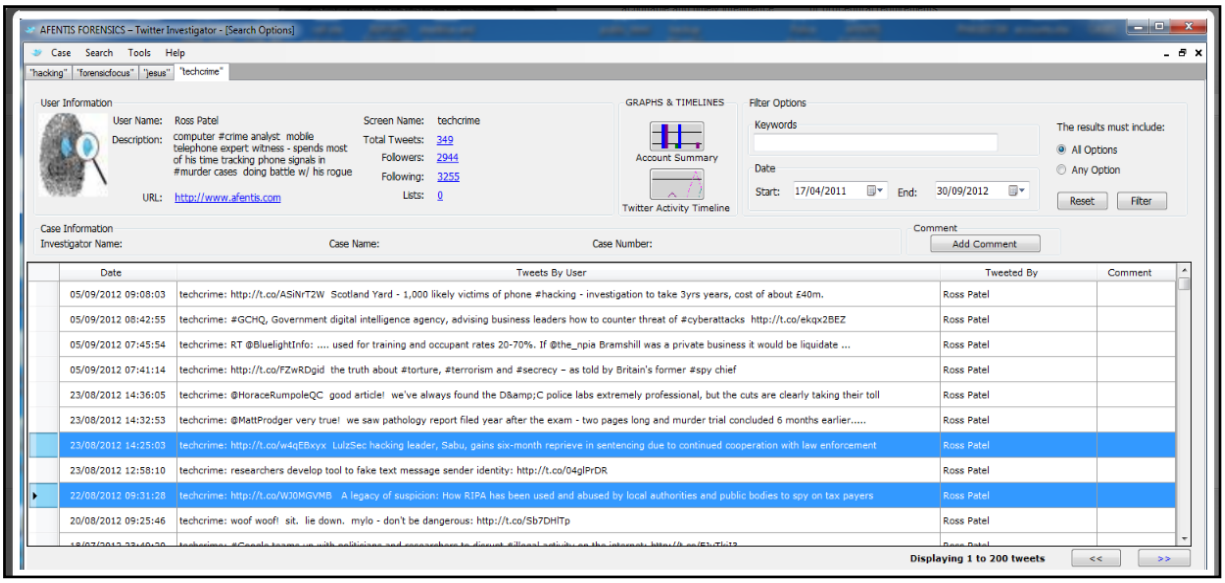


**Figura 25.** Tela do *Twitter Investigator* exibindo os *tweets* capturados de um usuário (*print screen* do programa em execução).

## 5. Considerações Finais

Neste artigo foram mencionados alguns casos importantes envolvendo evidências em redes sociais relacionados a crimes, entretanto há muitos outros casos semelhantes, como danos pessoais, direito de família, litígios empresariais, violação de marca, calúnia, concorrência desleal entre outros que envolvem provas de mídia social, em novembro de 2011 segundo publicação, a empresa *X1 Discovery,* procurou por bases de dados jurídicos online estaduais e federais de decisões judiciais nos Estados Unidos para identificar o número de casos a partir de 2010 até novembro de 2011, onde evidências de sites de redes sociais desempenharam um papel significativo [14].

O número de resultados veio em até 689 casos com uma planilha disponível em: (http://www.x1.com/products/x1_social_discovery/case_law_2011.html) e há também casos que cobrem o primeiro semestre de 2012, acessível em: (http://www.x1.com/products/x1_social_discovery/case_law_2012.html). Sendo que essa pesquisa é limitada nas quatro principais sites de redes sociais, computados da seguinte forma: *MySpace* (315 casos), *Facebook* (304), *LinkedIn* (39) *Twitter* (30).

Diante de tantos casos pode-se perceber o quanto a forense computacional em redes de relacionamentos é prospera na busca de evidências. Entretanto essa

especialidade ainda se encontra em fase ascensão, para se ter ideia uma pesquisa feita na base dados do Google por termos “Forense Computacional em Redes sociais” pode-se constatar que há uma escassez de pesquisa brasileira na área. Enquanto que na base de dados estrangeira possuem números mais relevantes.

## Referências


1. Zainudin NM, Merabti M, Jones, DL. A Digital Forensic Investigation Model and Tool for Online Social Networks. In: PGNET, 12th. 2011, Liverpool. Anais The Annual Postgraduate Symposium On The Convergence Of TelecomunicationS, Networking And Broadcasting. Liverpool: Reino Unido. The School of Computing and Mathematical Sciences, Liverpool John Moores University, 2011. p. 1-6.
2. Friedberg S. Social Networking Forensics. Services, Forensic & Investigations, 2010. Disponível em: <http://www.strozfriedberg.com/category/services/forensics-investigations-services/digital-forensics/social-networking-forensics>
3. Daniel L, Daniel L. Digital Forensics for Legal Professionals – Understanding Digital Evidence from the Warrant to the Courtroom. United States: Elsevier, 2011.
4. Barros T. Polícia usa Facebook para investigar assassinato de jovem de 22 anos. TechTudo, 25 nov. 2012. Notícias. Disponível em: <http://www.techtudo.com.br/noticias/noticia/2012/11/policia-usa-facebook-para-investigar-assassinato-de-jovem-de-22-anos.html>
5. Lima PMF. Crimes de Computador e Segurança Computacional. São Paulo: Atlas, 2011.
6. GALILEU. Twitter deve ser usado como prova em investigação de assassinato. 11 jan. 2010. Noticias. Disponível em: <http://revistagalileu.globo.com/Revista/Common/0,,EMI115479-17770,00-TWITTER+DEVE+SER+USADO+COMO+PROVA+EM+INVESTIGACAO+DE+ASSASSINATO.html>
7. Son J. Social Network Forensics: Evidence Extraction Tool Capabilities. 2012. 225 f. Tese (Mestre em Tecnologia da Informação Forense) - School of Computing and Mathematical Sciences, AUT University, 2012.
8. G1. FBI cria perfis em redes sociais para capturar criminosos. Globo, 17 mar. 2010. Tecnologias, Redes sociais. Disponível em: <http://g1.globo.com/Noticias/Tecnologia/0,,MUL1533470-6174,00.html>
9. Parascandola R. NYPD forms new social media unit to mine Facebook and Twitter for mayhem. Daily News, 10 ago. 2011. Local <http://www.nydailynews.com/new-york/nypd-forms-new-social-media-unit-facebook-twitter-mayhem-article-1.945242>
10. Severiano A. Suspeitos de vender passagens aéreas falsas são presos, em Manaus. G1 Amazônas, 29 nov. 2012. Notícia. Disponível em:

<http://g1.globo.com/am/amazonas/noticia/2012/11/suspeitos-de-vender-passagens-aereas-falsas-sao-presos-em-manaus.html>

11. Eleutério P, Machado MP. Desvendando a Computação Forense. São Paulo: Novatec, 2010.
12. Wiles J, Reyes A. The Best Damm Cybercrime and Digital Forensics Book Period. United States of America: Elsevier, 2007.
13. X- ACT FORENSICS. Social network investigations by a computer forensic expert. X-Act Forensics, 03 fev. 2012. Disponível em: <http://socialnetworkinvestigations.blogspot.com.br/2012/02/social-network-investigations-by.html>
14. Patzakis J. 689 Published Cases Involving Social Media Evidence (with full case listing). 16 Abr. 2012. Article. Forensic Focus. Disponível em: <http://articles.forensicfocus.com/2012/04/16/689-published-cases-involving-social-media-evidence-with-full-case-listing>