DOI: http://dx.doi.org/10.5769/C2011018

Uma Nova Abordagem em Apreensão de Computadores

Pedro Auler, Laerte Peotta de Melo, Flávio Elias Gomes de Deus e Rafael Timóteo de Sousa Jr.

***Abstract* — Since the popularization of data encryption techniques, use of virtual machines and cloud computing, the practice of turning computers off and seize them for later dead analysis in laboratory, common until recently, has become quite reckless. Volatile data present on running computers or otherwise data protected through user passwords, may contain essential data to the investigated case elucidation, that will be lost in case of system shutdown. The modern recommendation in cases of computers search and seizure is to extract volatile data and to make a logical acquisition from password protected areas that are visible while the computer is still running, before shutting down the system and performing the traditional seizure.**

***Key-words* — Seizure, forensic, volatile, investigation, capture.**

***Resumo* — A partir da popularização do uso de criptografia, máquinas virtuais e computação em nuvens, a prática de desligar os computadores e apreendê-los para análise posterior, em laboratório, comum até pouco tempo, tornou-se bastante temerária. Dados voláteis presentes no computador ligado, ou dados protegidos de alguma forma através de senhas de usuário, podem conter dados imprescindíveis à elucidação do caso investigado, que serão perdidas em caso de desligamento do sistema. A moderna recomendação em casos de busca e apreensão de computadores é a de realizar uma coleta de dados voláteis e de dados lógicos de áreas protegidas por senha que estiverem visíveis enquanto o computador ainda estiver ligado, antes do desligamento da máquina para apreensão tradicional.**

Palavras-chave—Apreensão; forense; voláteis; investigação; captura.

1. INTRODUÇÃO

Os procedimentos de busca e apreensão de materiais de informática vêm sofrendo drásticas mudanças nos últimos tempos. A abordagem tradicional, que consiste em retirar o cabo de energia da máquina suspeita, com a apreensão de todo o material para análise posterior, em laboratório, pode trazer grave comprometimento da investigação, levando à perda irreversível de dados. Com o uso cada vez mais frequente de criptografia, de máquinas virtuais, e de armazenamento remoto de dados, o desligamento precoce da máquina examinada pode causar a perda imediata e irreversível das informações nela contidas [1].

Desligar o computador através de seu cabo de energia produz menos alterações nas evidências armazenadas no disco rígido, mas, por outro lado, tende a destruir uma quantidade significativa de evidências voláteis.

Coletar dados digitais em um sistema já desligado traz a vantagem de tornar a sobrescrita acidental ou modificação de dados praticamente impossível. Por outro lado, não permite a aquisição de dados voláteis, que são perdidos durante o processo de desligamento do sistema. Além disso, há outras situações em que a recuperação de dados permanentes também é praticamente inviabilizada. É o caso, por exemplo, do uso de criptografia, quando só é possível recuperar as informações com o uso da senha de acesso correta [2].

Um dos princípios mais importantes ligados à informática forense é o Princípio da Troca, de Locard (Locard´s Exchange Principle), segundo o qual a simples passagem do tempo pode provocar mudanças em um sistema de informática ativo. Isto ocorre devido a processos em execução, dados gravados ou apagados da memória, conexões de rede sendo criadas ou finalizadas, e assim por diante [3]. O uso adequado de ferramentas de coleta de dados pelo Perito, embora agravem esta situação, não adicionam nenhuma evidência ao sistema.

Todas essas pequenas alterações não produzem grandes consequências no sistema como um todo e podem ser explicadas posteriormente, através do exame minucioso e detalhado do material coletado. As modificações são produzidas pela interação das ferramentas com o sistema operacional do Windows, interferindo apenas com os arquivos do sistema operacional, não acarretando nenhuma mudança importante no conteúdo dos dados salvos no sistema [4].

Os princípios fundamentais que norteiam a extração de dados em sistemas ligados orientam as seguintes condutas [5]:

- Devem-se coletar todos os dados que serão perdidos ao desligar o sistema;
- Devem-se coletar primeiramente os dados mais voláteis, deixando os menos voláteis para o final;
- Os dados devem ser coletados no menor tempo possível e levando em conta a sua importância;
- Os dados coletados devem permanecer disponíveis para futuras análises, se necessárias, e os exames realizados devem ser tão repetíveis quanto possível;
- Deve-se manter a integridade dos dados coletados;
- As ferramentas de coleta devem capturar os dados de forma fidedigna;
- As ações realizadas em cada caso em particular devem ser relevantes e específicas o caso.

A memória RAM é chamada volátil porque os dados são perdidos quando a máquina é desligada. A grande

importância em se coletar a memória RAM antes de desligar o computador suspeito é que nela podem ser encontradas informações de grande interesse para a condução da análise posterior, ou mesmo no processo investigatório, como por exemplo [4]:

- Processos em execução;
- Lista de comando executados;
- Senhas em texto claro;
- Versões decifradas de dados criptografados;
- Mensagens instantâneas;
- Endereços IP;
- *Malwares*.

2. CADEIA DE CUSTÓDIA

Quando há necessidade de intervir em sistemas ligados, todos os passos devem ser bem documentados, de preferência incluindo fotografias e filmagens dos procedimentos e do estado do material periciado e apreendido. Deve ser garantida a integridade dos arquivos resultantes da coleta, normalmente através de uma função unidirecional de resumo (*hash*), na presença de pelo menos duas testemunhas, incluindo-se os valores resultantes no Auto de Busca e Apreensão.

A cadeia de custódia trata dos procedimentos que buscam garantir a idoneidade das evidências através da descrição e documentação detalhada de como a evidência foi encontrada e de como foi tratada dali por diante. Todo o procedimento deve ser documentado de tal maneira, que fique registrado onde, quando e por quem a evidência foi descoberta, manipulada, coletada e armazenada. Quando a evidência passa para a responsabilidade de outra pessoa, este fato, com todos os detalhes envolvidos, incluindo número de lacres e outros procedimentos de segurança, deve ser também cuidadosamente documentado [6].

As funções de *hash* relacionam um arquivo de entrada de tamanho variável a um valor de saída de tamanho fixo, que serve como autenticador [7]. Alguns exemplos de algoritmos utilizados são MD5, SHA-1, SHA-256, SHA-384 E SHA-512 [8]. Sua característica marcante é que é muito difícil encontrar dois arquivos de entrada que produzam o mesmo resultado na saída, e, a partir da saída, é computacionalmente inviável encontrar a entrada.

3. METODOLOGIA PARA APREENSÃO DE COMPUTADORES

Os procedimentos de coleta devem ser tão detalhados quanto possível, minimizando a necessidade de tomada de decisões durante o procedimento da apreensão. Além disso, os procedimentos da cadeia de custódia devem ser claramente documentados [6].

Após ter o local de apreensão sob controle, o Perito Criminal, na presença de duas testemunhas, deve fazer um reconhecimento do ambiente, a fim de localizar os equipamentos de informática, verificando se está ligado e se está conectado a outros equipamentos.

A sequência de atos recomendada está ilustrada na Figura 1. Se o computador estiver desligado, deve assim permanecer e deve ser apreendido para exames posteriores, em laboratório. Se estiver ligado, deve ser verificado se está bloqueado e se a senha está disponível. Se o acesso ao sistema não for possível, o equipamento deve ser desligado e apreendido para perícia em momento posterior.

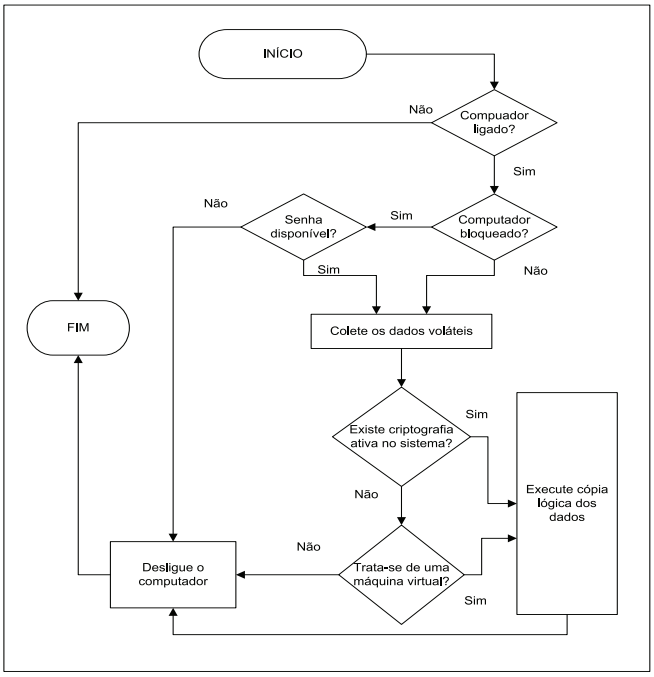

Figura 1. Metodologia proposta para apreensão de computadores.

Se o equipamento estiver ligado e acessível, devem ser realizados procedimentos de coleta de dados voláteis. A seguir, deve ser verificado se existe algum volume criptografado, e, no caso de estar acessível, deve ser efetuada uma cópia lógica dos dados nele contidos. Deve também ser verificado se se trata de uma máquina virtual, caso em que também deve ser realizada a cópia lógica dos arquivos do sistema. A seguir, o equipamento deve ser desligado e apreendido para continuação dos exames em laboratório.

4. COLETA DE DADOS VOLÁTEIS

Dados voláteis podem ser definidos como qualquer dado que deixe de existir quando o computador é desligado, não sendo possível recuperá-lo posteriormente [1].

As ferramentas de captura de dados voláteis devem ser capazes de extrair e preservar de forma sistemática e automática, os dados de um sistema de informática ligado, produzindo o mínimo de alterações possíveis no sistema.

A RFC 3227 [6] traz um exemplo de ordem de coleta, em um sistema de informática típico, partindo dos dados mais voláteis para os menos voláteis:

- Registros e memória *cache*;
- Tabela de roteamento, Tabela de processos e memória física;

- Sistemas de arquivos temporários;
- Conexões remotas;
- Topologia de rede.

As ferramentas preferencialmente utilizadas para a coleta são as de linha de comando, que são mais leves, comprometem menos recursos da máquina alvo, e facilitam a automação através de arquivos batch [9].

Existem diversas ferramentas voltadas para resposta a incidentes e segurança na Tecnologia da Informação (TI). Um dos problemas de se utilizar estas ferramentas isoladamente está no fato de que o usuário tem que lembrar todos os comandos e parâmetros para executar as ferramentas corretamente em linha de comando. Após, o investigador terá que consolidar os resultados de forma a realizar seu relatório. Assim, para utilizar estas ferramentas em todo o seu potencial, é necessário agregá-las em um aplicativo que as execute de forma automática e na ordem correta, atendendo aos princípios forenses relacionados, e salvando os resultados de forma integrada e lógica em um arquivo, para análise posterior.

A solução para este problema está em utilizar um framework que integre e automatize a execução das ferramentas necessárias. Dessa forma, diminui-se o risco de erro por esquecimento de alguma ferramenta específica para coletar determinado dado, ou pelo uso das ferramentas na ordem incorreta, permitindo a coleta mais rápida e correta de todos os dados, na sequência ideal. Algumas soluções existentes incluem o COFEE [10] (Computer Online Forensic Extractor), desenvolvido pela Microsoft, o WFT [11] (Windows Forensics Toolchest), desenvolvido pela Fool Moon Software & Security, e o Live Response, desenvolvido pela E-fense [12].

A maioria das ferramentas de captura de dados voláteis utilizadas pelas soluções de integração existentes é disponibilizada gratuitamente na internet. As principais fontes são a Nirsoft [13] e a Sysinternals [14], que possuem diversos utilitários genéricos. O "MDD" é uma ferramenta específica para captura de memória física, disponibilizada pela Mantech [15].

A Tabela 1 apresenta algumas das ferramentas gratuitas para coleta de dados voláteis, com resumo de suas funcionalidades, desenvolvidas pela Nirsoft [13].

Tabela 1. Exemplos de ferramentas da Nirsoft.

Ferramenta	Funcionalidade
USBDeview	Lista os dispositivos USB conectados
IEHistoryView	Recupera páginas acessadas pelo Internet Explorer
MozillaHistoryView	Recupera páginas acessadas pelo Mozilla Firefox
ChromeHistoryView	Recupera páginas acessadas pelo Google Chrome
MyLastSearch	Recupera últimos termos pesquisados
SkypeLogView	Mostra detalhes de chamadas e mensagens do Skype

A Tabela 2 apresenta algumas das ferramentas gratuitas para coleta de dados voláteis do pacote Sysinternals, com resumo de suas funcionalidades, disponibilizadas pela Microsoft [14].

Tabela 2. Exemplos de ferramentas da Sysinternals.

Ferramenta	Funcionalidade
Handle	Recupera relação de processos com arquivos e pastas abertos
ListDLLs	Recupera DLLs carregadas no sistema
PsFile	Exibe os arquivos abertos remotamente
PsInfo	Recupera informações sobre o sistema
PsList	Exibe os processos em execução
PsLoggedOn	Verifica quais usuários estão ativos

A Jadsoftware [16] desenvolveu o EDD (*Encrypt Disk Detector*), ferramenta de linha de comando, grátis, com capacidade de diagnosticar a presença de volumes criptografados pelos programas TrueCrypt, PGP, Safeboot e Bitlocker. A Figura 2 apresenta uma tela de saída do aplicativo, onde é possível verificar que foi detectada a presença de criptografia no drive "M".

Para detecção de máquinas virtuais VWware, pode ser utilizada a ferramenta ScoopyNG, desenvolvido e disponibilizado pela Trapkit [17]. A Figura 3 apresenta uma tela de saída do aplicativo, confirmando a presença de máquina virtual VWware.

Outra ferramenta bastante útil, apesar de não ser de linha de comando, também disponibilizada para *download* gratuito, é o "FTK Imager Lite" [18], que permite, entre outras diversas funcionalidades, executar cópia lógica do sistema e dos registros, e capturar a memória física.

Assim, o Perito pode criar seu próprio conjunto de ferramentas para captura de dados voláteis, integrando e automatizando a sua execução, através de um arquivo *batch*. Não devem ser utilizados executáveis da máquina suspeita, já que podem ter sido alterados pelo investigado. Além de coletar as informações para análise posterior, pode ser útil fazer uma rápida análise dos arquivos coletados, ainda durante o procedimento de busca e apreensão. A análise pode ser manual, verificando o conteúdo dos arquivos coletados, mas o ideal é que esta análise seja também automatizada. Através de mecanismos relativamente simples, podem ser incluídos pequenos testes no arquivo *batch* de coleta. Com o auxílio das ferramentas *strings* [14] e *grep* [19], pode ser feita uma busca nos arquivos texto coletados a partir da saída das ferramentas edd e ScoopyNG, por exemplo, mostrados nas Figuras 2 e 3, respectivamente, que identifiquem a presença de criptografia ou máquina virtual. Da mesma forma, pode ser feita uma busca no arquivo texto de saída da ferramenta *PsList*, que mostra os arquivos em execução no sistema, onde também podem ser verificados indícios de criptografia ou máquina virtual. Estes testes ainda no local de busca, com a máquina ligada, podem ser muito úteis no auxílio à tomada de decisão, quanto a coletar dados lógicos do sistema ou não, antes de desligá-lo para apreensão.

```
Encrypted Disk Detector v1.1
Copyright (c) 2009 Jad Saliba
http://www.jadsoftware.com
// This program comes with no guarantee or warranty.
   All risk is assumed by the user. //

* Checking physical drives on system... *

PhysicalDrive0, Partition 1 --- OEM ID: NTFS

PhysicalDrive1, Partition 1 --- OEM ID: NTFS

* Completed checking physical drives on system. *

* Now checking logical volumes on system... *

Drive A: appears to be a virtual disk
  - possibly a TrueCrypt or PGP encrypted volume
Drive C: is located on PhysicalDrive0, Partition #1.
Drive D: is a CD-ROM/DVD device (#0).
Drive E: is located on PhysicalDrive1, Partition #1.
Drive M: appears to be a virtual disk
  - possibly a TrueCrypt or PGP encrypted volume

* Completed checking logical volumes on system. *
```

Figura 2. Resultado da execução do aplicativo EDD.

```
::     ScoopyNG - The VMware Detection Tool     ::
   ::            Windows version v1.0            ::

   [+] Test 1: IDT
   IDT base: 0xffc18000
   Result  : VMware detected

   [+] Test 2: LDT
   LDT base: 0xdead4060
   Result  : VMware detected

   [+] Test 3: GDT
   GDT base: 0xffc07000
   Result  : VMware detected

   [+] Test 4: STR
   STR base: 0x00400000
   Result  : VMware detected

   [+] Test 5: VMware "get version" command
   Result  : VMware detected
   Version : Workstation

   [+] Test 6: VMware "get memory size" command
   Result  : VMware detected

   [+] Test 7: VMware emulation mode
   Result  : Native OS or VMware without emulation mode
          (enabled acceleration)

   ::                tk,  2008                ::
   ::             [ www.trapkit.de ]          ::
```

Figura 3. Resultado da execução do aplicativo ScoopyNG.

5. CONCLUSÃO

Devido às limitações da coleta de dados tradicional, em sistemas desligados, a aquisição com o computador ainda ligado parece ser a alternativa salvadora. Esta técnica permite a recuperação de valiosas informações que de outra maneira poderiam ser perdidas.

No cenário atual, a melhor forma de busca e apreensão de itens relacionados a sistemas informatizados deve incluir a coleta dos dados voláteis, cópia lógica do disco rígido, quando necessário, e apreensão física dos equipamentos para análise tradicional em laboratório.

Para a captura de dados voláteis podem ser utilizadas soluções desenvolvidas por terceiros, trazendo as limitações de custo de aquisição e dificuldades de atualização e adaptação às necessidades da perícia. As soluções disponíveis capturam uma grande quantidade de informações, nem sempre necessárias ao caso concreto, trazendo assim uma invasão adicional desnecessária ao sistema analisado.

O perito pode criar seu próprio conjunto de ferramentas de captura de dados voláteis, todas disponíveis gratuitamente na Internet, integrando e automatizando-as através de um arquivo *batch*. As vantagens desta solução são a ausência de custo de aquisição e a oportunidade de coletar somente as informações julgadas necessárias pelo perito para o caso concreto em análise. Além disso, pode incluir alguns testes para detecção de criptografia ou máquina virtual, que irão auxiliá-lo na tomada de decisão durante a apreensão, que deve ser rápida e precisa, com o mínimo possível de alteração do sistema alvo.

AGRADECIMENTOS

O presente trabalho resultou dos estudos realizados durante o mestrado em Engenharia Elétrica, na área de concentração Informática Forense e Segurança da Informação, ainda em curso na Universidade de Brasília, com o apoio do Departamento de Polícia Federal e recursos do Programa Nacional de Segurança Pública com Cidadania – PRONASCI, do Ministério da Justiça.

Referências

[1] I. Sutherland, J. Evans, T. Tryfonas, e A. Blyth. Acquiring volatile operating system data tools and techniques. Disponivel em: <http://doi.acm.org/10.1145/1368506.1368516>. Acesso em: 09 ago. 2010.

[2] M. M. Grobler e S. H. Von Solms. Best practice approach to live forensic acquisition. Disponivel em: <http://hdl.handle.net/10204/3509>. Acesso em: 09 ago. 2010.

[3] H. Carvey. Windows Forensic Analysis. Burlington: 2007.

[4] T. G. Shipley e H. R. Reeve. Collecting evidence from a running computer: A technical and legal primer for the Justice Community. Disponivel em: <http://www.search.org/files/pdf/CollectEvidenceRunComputer.pdf>. Acesso em: 11 abr. 2011.

[5] R. Ieong. Freeware live forensics tools evaluation and operation tips. Disponivel em: <http://scissec.scis.ecu.edu.au/proceedings/2006/forensics/Ieong%20-%20Freeware%20Live%20Forensics%20tools%20evaluation%20and%20operation%20tips.pdf>. Acesso em: 09 abr. 2011.

[6] D. Brezinski e T. Killalea. Guidelines for evidence collection and archiving. RFC 3227, 2002. Disponivel em: <http://www.faqs.org/rfcs/rfc3227.html>. Acesso em: 16 jun. 2011.

[7] W. Stallings. Criptografia e Segurança de Redes - Princípios e Práticas. 4. ed. São Paulo: [s.n.], 2008.

[8] N. Ferguson e B. Schneier. Practical Cryptography. Indianapolis: Willey Publishing, 2003.
[9] C. Steel. Windows Forensics: The Field Guide for Conducting Corporate Computer Investigations. Indianápolis: 2006.
[10] Microsoft. "Computer Online Forensics Evidence Extractor (COFEE)". Disponível em: <http://www.microsoft.com/industry/government/solutions/cofee/default.aspx>. Acesso em 20 jul. 2011.
[11] Fool Moon Software & Security. "Windows Forensic Toolchest (WFT)". Disponível em: < http://www.foolmoon.net/security/wft/>. Acesso em 20 jul. 2011.
[12] E-fense. "Live Response". Disponível em: <http://www.e-fense.com/live-response.php>. Acesso em 20 jul. 2011.
[13] Nirsoft. "Freeware utilities for Windows". Disponível em: <http://www.nirsoft.net/utils/index.html>. Acesso em 20 jul. 2011.
[14] Microsoft. "Windows Sysinternals Suite". Disponível em: <http://technet.microsoft.com/en-us/sysinternals/bb545027>. Acesso em 20 jul. 2011.
[15] Mantech. "ManTech Memory DD". Disponível em: <http://www.mantech.com/capabilities/mdd.asp>. Acesso em 20 jul. 2011.
[16] Jadsoftware. "Encrypted Disk Detector". Disponível em: <http://www.jadsoftware.com/go/?page_id=167>. Acesso em 20 jul. 2011.
[17] Trapkit. ScoopyNG – The WMware detection tool. Disponível em: < http://www.trapkit.de/research/vmm/scoopyng/index.html>. Acesso em 20 jul. 2011.
[18] AccessData. FTK Imager Lite. Disponível em: <http://accessdata.com/support/adownloads#FTKImager>. Acesso em 20 jul. 2011.
[19] Unxutils. GNU utilities for WIN32. Disponível em: <http://unxutils.sourceforge.net/>. Acesso em 20 jul. 2011.

Pedro Auler Possui graduação em Medicina pela Universidade de Caxias do Sul (1985) e em Direito, pelo Centro Universitário de Barra Mansa (2005), especialização em Análise, Projeto e Gerência de Sistemas pela Pontifícia Universidade Católica do Rio de Janeiro (1996) e especialização em Perícia Digital pela Universidade Católica de Brasília (2009). Atualmente é Mestrando (UnB) em Engenharia Elétrica, na área de concentração Informática Forense e Segurança da Informação e atua como Perito Criminal Federal no Departamento de Polícia Federal, na área de perícias de informática, desde janeiro de 2008 - pedroauler.pa@dpf.gov.br, Brasília-DF, Brasil.

Laerte Peotta de Melo Possui graduação em Elétrica com ênfase em Eletrônica pela Universidade Presbiteriana Mackenzie-SP (1996), especialização em segurança de redes de computadores pela Universidade Católica de Brasília (2004), perito forense computacional pela Universidade Federal do Ceará (2007), Mestrado em Engenharia Elétrica pela Universidade de Brasília (2008). Atualmente é Doutorando (UnB) e pesquisador pelo Banco do Brasil, trabalhando na área de fatores de autenticação fortes. Professor em cursos de pós-graduação atuando nos cursos Tratamento de incidentes de segurança, Auditoria e Análise forense e Segurança da Informação.

Flávio Elias Gomes de Deus Possui graduação em Engenharia Elétrica pela Universidade Federal de Goiás (1998), mestrado em Engenharia Elétrica pela Universidade de Brasília (2001) e Doutorado pela Universidade de Brasília (2006) com Doutorado Sandwich na University of Pittsburgh (2005). Atualmente é Professor Adjunto no Departamento de Engenharia Elétrica-UnB. Tem experiência na área de Redes de Comunicação, atuando principalmente nos seguintes temas: Tecnologia da Informação, Wireless Local Area Network (WLAN), Mobile ad-hoc Networks (MANET) entre outros tópicos correlatos.

Rafael Timóteo de Sousa Jr. Possui graduação em Curso de Engenharia Elétrica pela Universidade Federal da Paraíba, Campina Grande (1984), mestrado (DEA) em Telemática e Sistemas de Informação pela Ecole Supérieure d'Electricité - SUPELEC (1985) e doutorado em Processamento de Sinais e Telecomunicações pela Université de Rennes I (França, 1988). Fez pós-doutorado na Ecole Supérieure d'Electricité - SUPELEC (2006-2007). Atualmente é professor adjunto da Universidade de Brasília, curso de Engenharia de Redes de Comunicação. Tem experiência em Engenharia de Software e Engenharia de Redes de Comunicação, atuando principalmente nos seguintes temas: segurança da informação e confiança computacional, gerência de redes, mobile ad-hoc networks (manet), computação distribuída na Internet.