DOI: http://dx.doi.org/10.5769/C2011010

Ensino da Forense Digital Baseado em Ferramentas Open Source

Leonardo L. Fagundes[1], Paulo A. Neukamp[2], and Pamela C. da Silva[3]
(1) Mestre em Computação Aplicada, Universidade do Vale do Rio dos Sinos (UNISINOS), São Leopoldo, Brasil, leonardo.lemes@defenda.com.br
(2) Professor Especialista, Universidade do Vale do Rio dos Sinos (UNISINOS), São Leopoldo, Brasil, pneukamp@unisinos.br
(3) Analista de Fraudes Eletrônicas, Defenda Consultoria em Segurança da Informação, São Leopoldo, Brasil, pamela.silva@defenda.com.br

***Abstract* — Developing competence in Digital Forensics is a critical function in courses on Information Security or that approach this theme. The high cost involved to equip laboratories and acquire the necessary tools may preclude the offering of this discipline. In this scenario, the adoption of Open Source tools may facilitate the learning process and provide students their first contact with the tools used by experts, as well as familiarity with the steps composing digital forensics. This article, therefore, presents a proposal on the teaching of this discipline.**

Keywords* — *Forense Open Source, FDTK, Digital Forensic Education,

***Resumo* — Desenvolver competência em Forense Digital é uma função crítica em cursos de Segurança da Informação ou que abordem este tema. O alto custo envolvido para equipar laboratórios e adquirir as ferramentas necessárias pode inviabilizar a oferta desta disciplina. Neste cenário, a adoção de ferramentas Open Source pode viabilizar o processo e proporcionar aos alunos, seu primeiro contato com as ferramentas utilizadas por peritos, além da familiarização com as etapas que compõem uma perícia, desta forma este artigo apresenta uma proposta para o ensino da disciplina.**

Palavras chaves* — *Forensic Open Source, FDTK, Ensino Forense Digital.

1. Introdução

De acordo com pesquisadores *"um passo fundamental na melhoria das técnicas forense reside na criação de uma abordagem abrangente à educação forense"* [1]. Porém a forense digital apresenta peculiaridades com relação a outras disciplinas forense, pois tratando-se de uma competência de âmbito tecnológico, requer habilidade e disponibilidade para acompanhar os avanços das tecnologias digitais.

No ensino da forense digital, ainda existe uma dificuldade em gerar um *"modelo utilizável pedagogicamente"* [1], capaz de compartilhar o conhecimento de forma ativa, despertando a dimensão cognitiva do acadêmico e oportunizando um aprender crítico-reflexivo que garante um aprendizado integrado e qualitativo por compreender o acadêmico como um indivíduo crítico, incompleto e dotado de autonomia intelectual. Assim esta é a apresentação de uma proposta implementada na Universidade do Vale do Rio dos Sinos – Unisinos [2], que através do uso de ferramentas *Open Source,* tem o objetivo de proporcionar aos alunos, em especifico do curso de Segurança da Informação, acesso às técnicas de investigação e coleta de evidências, e a partir disto a possibilidade de aperfeiçoá-las através de pesquisas a serem desenvolvidas.

Atrelado a esta nova demanda, o ensino da Forense Digital exige das instituições, além de novas formas de ensinar, altos investimentos na estruturação de seus laboratórios e na aquisição das ferramentas necessárias para desenvolver tal conhecimento.

Esta abordagem pretende garantir a qualidade do conhecimento, bem como demonstrar que é possível reduzir de forma significante os investimentos sem penalizar o ensino, por meio da adoção de ferramentas *Open Source* para a realização destas atividades no meio acadêmico.

A Distribuição Linux FDTK – Forense Digital ToolKit [3], foi criada por um aluno do Curso de Segurança da Informação da Unisinos como uma das contribuições acadêmicas de seu trabalho de conclusão de curso realizado no ano de 2007. Em 2008 a FDTK foi adotada pela Unisinos para ser utilizada na disciplina de Forense Computacional.

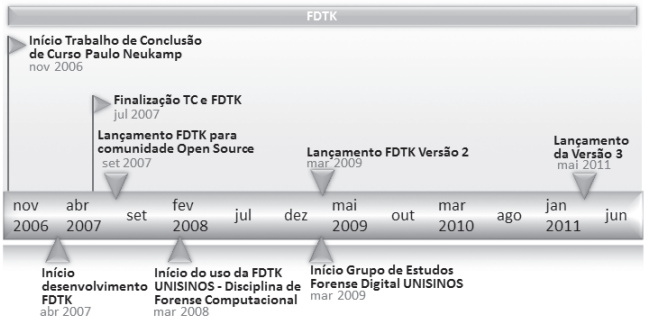

Figura 1.Linha do tempo Projeto FDTK.

A FDTK foi disponibilizada para a comunidade no mesmo período de sua criação, desde então vem sendo utilizada em

diversos cursos específicos e por profissionais da área como uma alternativa aos altos custos e pelo seu potencial didático, apto a auxiliar em práticas Forense aproximando o individuo das técnicas e procedimentos.

A Figura 1 demonstra uma linha do tempo onde podem ser visualizados os principais momentos da FDTK desde seu planejamento até a os dias atuais.

Em âmbitos educacionais que requerem experimentos práticos é essencial observar que os recursos utilizados devem ser apropriados para educação e devem contribuir diretamente para os objetivos de aprendizagem, o que é fundamental para o sucesso na estruturação de uma disciplina educacional [7].

Dados recentes reforçam sua aceitação pela comunidade, somente nos primeiros quinze dias de lançamento da Versão 3 foram registrados mais de 14.000 downloads, já os dados obtidos junto à coordenação do curso de Segurança da Informação da Unisinos demonstram, conforme Gráfico 1, que desde a adoção da FDTK como ferramenta de auxilio ao ensino na disciplina de Forense Computacional, que ocorreu no primeiro semestre do ano de 2008, 155 alunos já foram beneficiados diretamente. Estes alunos atualmente são capazes de aplicar tais conhecimentos em incidentes de segurança que possam vir a ocorrer nas empresas nas quais trabalham, ajudando assim, a preservar provas e evitar a contaminação das mesmas, além de conduzir investigações internas.

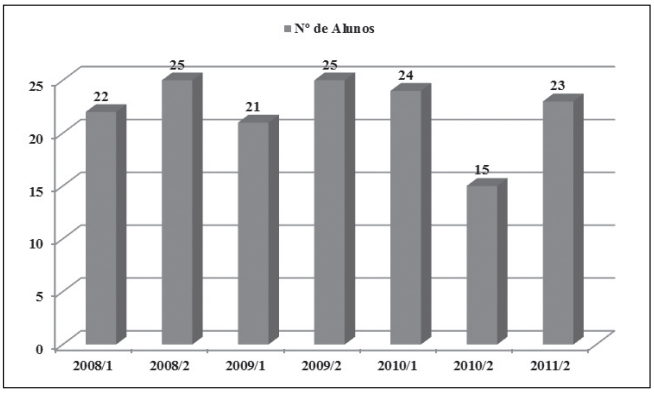

Gráfico 1. Número de alunos que cursaram a disciplina de Forense Digital

A FDTK também vem sendo utilizada em diversos cursos específicos ministrados por consultorias, empresas que oferecem treinamento e instrutores independentes em treinamentos direcionados a profissionais que atuam ou pretendem atuar no combate a incidentes de segurança. Em 2009 ocorreram dois treinamentos para a equipe de guerra cibernética do Ministério do Exército brasileiro e estes foram inteiramente baseados na utilização da FDTK como distribuição Linux específica para a condução de investigações de crimes digitais.

2. Dividir para Conquistar

A realização de uma perícia digital não difere de outras perícias como, por exemplo, a realização de uma balística no que diz respeito à complexidade dos conhecimentos necessários para a condução desta. Tal complexidade pode ser minimizada utilizando uma metodologia adotada inicialmente pelos romanos e que tornou-se bastante popular com o livro "A Arte da Guerra" de *Sun Tzu* [4], que pode ser simplificada na frase "Dividir para Conquistar".

Utilizando os ensinamentos de *Sun Tzu*, diversos departamentos de justiça de vários países possuem equipes divididas em especialidades, ou seja, possuem especialistas em cena do crime, tratamento de evidências, reconstrução dos fatos ocorridos e laudos periciais. Este fato se deve a quantidade de conhecimento e expertise que os peritos necessitam, a fim de não perder nenhum detalhe por falta de conhecimento, o que poderia ocasionar uma decisão equivocada por parte do juiz a frente do caso.

Seguindo esta orientação, a distribuição FDTK foi construída após um profundo estudo de todas as etapas e processos envolvidos em uma pericia digital. Os estudos demonstraram claramente que as ferramentas *open source* disponíveis quando da realização da pesquisa, exigiam diversos conhecimentos por parte dos estudantes. Conhecimentos estes que podem levar muito tempo para serem adquiridos.

3. Open Source e suas vantagens no ensino de Forense Digital

O software *open source* é um modelo didático, pois fomenta o pensamento critico, conta com uma capacidade de adaptação independente, visto que pode ser ajustado de acordo com as necessidades do ambiente acadêmico, através das comunidades há grande compartilhamento de conhecimento e criação, o que oferece uma opção para desenvolver novas competências, e possibilita ao aluno acesso mesmo fora do ambiente universitário às ferramentas de forma legal.

Em uma disciplina forense pode-se enumerar ainda outras características que tornam o uso de ferramentas *open source* recomendado, tais como a disponibilidade do código fonte e de documentação ou especificações dos algoritmos o que permite, caso ainda não existam, que sejam realizados estudos para verificar o impacto das ferramentas no sistema periciado, incluindo o sistema de arquivos [6] além da verificação dos processos envolvidos, já o software proprietário disponibiliza o mínimo de informações, como forma de garantir sua sustentabilidade comercial. Através das comunidades as publicações de falhas tornam-se abrangentes, o que garante que possíveis correções sejam geradas com maior agilidade, isso reduz custos e garante a confiabilidade das ferramentas.

"O uso de software *open source* desempenha um papel de destaque na formação de futuros analistas forense" [6], esta afirmação baseia-se na permissividade que estes oferecem para uma ampla compreensão e avaliação das técnicas utilizadas na execução dos processos em forense digital, tal faculdade é fundamental para especialistas nesta área,

o conhecimento não deve restringir-se ao de usuários, é necessário um entendimento perficiente, "um profissional de forense digital deve ter confiança no software utilizado" [6], seja para obter as evidências, seja para realização da análise.

Como mencionado anteriormente o modelo *open source* incentiva a criticidade do individuo, e com relação a uma disciplina de caráter investigativo espera-se que as metodologias adotadas sejam capazes de desenvolver atitudes de questionamento, deve-se ressaltar que através da análise de códigos fontes é possível criar o interesse para o aperfeiçoamento ou desenvolvimento de novas ferramentas forense.

4. Projeto FDTK

Nenhuma investigação na área da forense digital pode ser conduzida sem um kit de ferramentas [5], assim o projeto FDTK, foi criado, inicialmente, com o objetivo de possibilitar as pessoas com interesse em forense digital o acesso ao conhecimento fundamental sobre o tema de forma facilitada, visando romper algumas barreiras existentes em relação à utilização de ferramentas *open source* em pericias digitais.

A forma como as ferramentas são utilizadas, bem como a aceitação de uma ferramenta de forma legal é indispensável para o progresso de uma pericia [5], assim o projeto reuniu as ferramentas *open source* mais utilizadas por profissionais permitindo ao aluno uma proximidade com a realidade da área, além da aquisição de conhecimentos eminentemente práticos com relação aos processos envolvidos.

A distribuição é fruto do estudo de 10 distribuições Linux existentes na época do estudo (DEFT [8], BackTrack [9], INSERT [10], FCCU [11], Helix [12], Operator [13], PHLAK [14], L.A.S. Linux [15], nUbuntu [16] e Knoppix-STD [17]) que se autodenominavam Distribuições para Forense Computacional ou Digital.

Associando as qualidades de cada uma das distribuições estudadas, foi composta a FDTK, constituída por mais de cem ferramentas, divididas em três etapas, que mantém a estrutura encontrada na grande parte das metodologias utilizadas na área, coleta, exame e análise das evidências, e um grupo denominado Toolkits, formado por frameworks que utilizam diversas ferramentas de forma centralizada para tratar as evidências coletadas na primeira etapa da perícia.

Argumenta-se que abordagens como estas "preparam os alunos para desempenharem um melhor trabalho no campo da forense digital, à medida que adquirem confiança para usar diversas ferramentas e não apenas um único produto".

O modelo de etapas foi baseado em estudos e orientações realizadas pelo NIST - National Institute of Standards and Technology publicado em 2006 no documento intitulado "Guide to Integrating Forensic Techniques into Incident Response" [18]. A partir da interpretação das recomendações feitas pelo NIST, inicialmente foi criado o modelo apresentado na Figura 2.

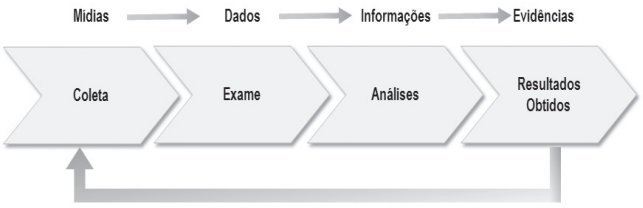

Figura 2. Processo Forense Digital.

Este modelo foi redesenhado recentemente e ao mesmo foram adicionadas as principais tarefas que devem ser executadas a cada etapa, conforme Figura 3.

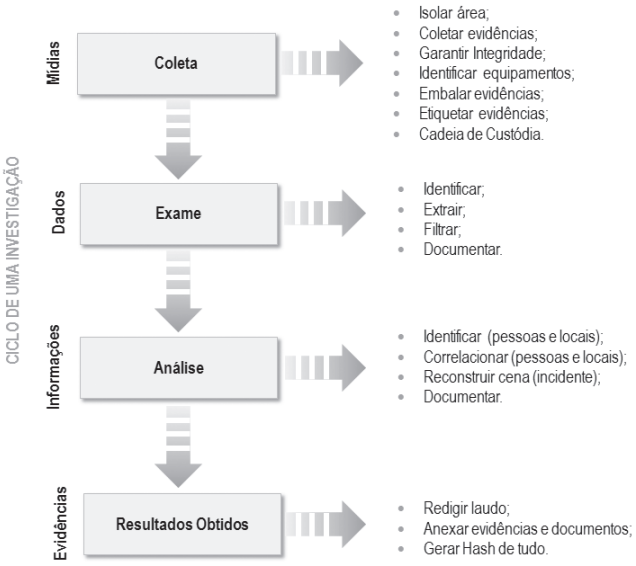

Figura 3. Processo Forense Digital Atualizado.

A divisão dos processos, envolvidos em uma pericia digital, em etapas, possibilitou evidenciar que nenhuma das distribuições estudadas haviam se preocupado em facilitar o acesso às ferramentas disponíveis, esta estruturação inserida no âmbito educacional permite ao aluno a visualização de toda a teoria apresentada, bem como a sua integração com a prática.

Figura 4. Menu Forense Digital demonstrando as etapas de uma pericia.

A Figura 4 ilustra o menu Forense Digital criado na distribuição FDTK, as etapas e os grupos de ferramentas disponíveis em cada uma delas.

Tomando como exemplo a etapa de Coleta dos Dados, a distribuição FDTK oferece diversas ferramentas apropriadas ao processo de criação de imagem dos dados conforme Figura 3.

A Figura 5 demonstra a execução da ferramenta dcfldd [18], a partir do menu, que possui interface gráfica. Para os iniciantes em seus primeiros contatos com as ferramentas foram criados scripts complementares com *Shell Script* e *Zenity* que informam ao perito ou estudante, os parâmetros disponíveis de cada ferramenta e suas respectivas páginas do manual.

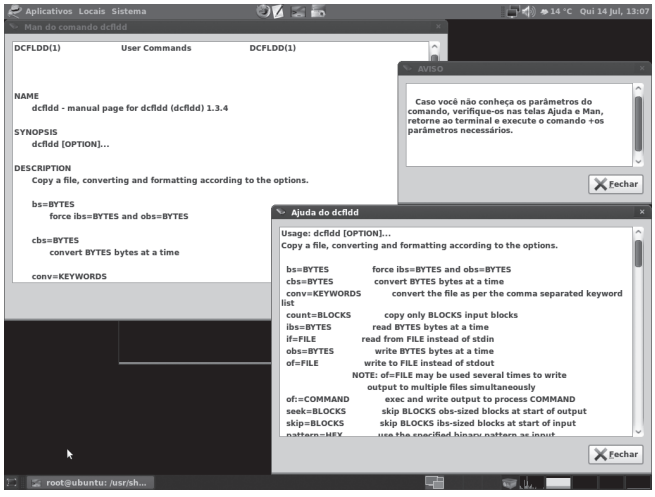

Figura 5. Mensagens sobre parâmetros e manual da ferramenta dcfldd.

5. Ferramentas

Conforme mencionado anteriormente à distribuição FDTK reúne mais de cem ferramentas que podem ser utilizadas na execução de pericias digitais, as imagens a seguir (Figuras 6, 7 e 8) listam as ferramentas de acordo com a etapa da investigação para a qual se aplicam.

Coleta

FERRAMENTAS	
Formulário	Formulário de Cadeia de Custódia
gnome-screenshot	Salvar imagens da área de trabalho ou de janelas individuais
aimage	Geração de imagem dos dados das mídias no padrão aff
air	Interface gráfica para dd/dcfldd, para criação imagem dos dados
dc3ddgui	Interface gráfica para O DC3DD, para criação imagens dos dados
dcfldd	Versão aprimorada pelo DOD-Departament of Defense do dd
dd	Ferramenta para geração de imagem dos dados
ddrescue	Recuperar dados de hds com setores defeituosos (bad blocks)
mondoarquive	Copiar dados de fitas, cd's, nsf ou hd's
mondorestore	Restaurar dados de fitas, cd's, nsf ou hd's
rdd	Versão mais robusta do dd
rddi	Prompt interativo do rdd
sdd	Versão da ferramenta dd para Fitas (DAT, DLT...)
mamdump	Dumper de memória para sistemas UNIX-like
md5sum	Geração hash md5
sha1sum	Geração hash sha 160bits
discover	Obtenção de informações sobre Hardware
hardinfo	Informações e Testes do Sistema
lshw-grafico	Listar os dispositivos de hardware em formato HTML
sysinfo	Exibir informações do computador e do sistema
wipe	Remoção total dos dados das Mídias

Figura 6. Ferramentas para etapa de Coleta - FDTK.

Exame

FERRAMENTAS	
cabextract	Acesso conteúdo de arquivos extensão .cab
orange	Ferramenta para manipulação de arquivos extensão .cab
p7zxip	Acessar arquivos zip
unance	Ferramenta para descompactação de arquivos com extensões .ace
unrar-free	Ferramenta para descompactação de arquivos com extensão .rar
unshield	Ferramenta para descompactação de arquivos com extensão .cab da MS
xarchiver	Criação, modificação e visualização de arquivos compactados
zoo	Acessar de arquivos compactados extensão .zoo
dcraw	Acessar imagens cruas de câmeras digitais
exif	Ler informações EXIF de arquivos com extensão .jpeg
exifprobe	Exame do conteúdo e da estrutura dos arquivos de imagens com extensão .JPEG e .TIFF
exiftrn	Transformação de imagens raw de câmeras digitais
exiftags	Adquirir informações sobre a câmera e as imagens por ela produzidas
exiv2	Manipulação de metadados de imagens
jhead	Visualização e manipulção dos dados de cabeçalhos de imagens extensão .jpeg
jpeginfo	Ferramenta para coletar informações sobre imagens extensão .jpeg
antiword	Ferramenta para leitura arquivos do MS-Word
dumpster	Acessar os arquivos da lixeira do Windows
fccu-docprob	Ferramenta para visualização de propriedades de arquivos OLE
mdp-hexdump	Ferramenta para manipulação de arquivos MDB
readpst	Ferramenta para leitura de arquivos do MS-Outlook
reglookup	Utilitário para leitura e resgate de dados do registro do Windows
regp	Acessar conteúdo de arquivos .dat
tnef	Acessar anexos de email's MS
bcrypt	Encriptar e decriptar arquivos usando o algoritmo blowfish
ccrupt	Encriptar e decriptar arquivos e streams
outguess	Detecção dados ocultos em imagens JPG
stegcompare	Comparação de imagens jpeg e detectar a existência de steganografia
stegimage	Detecção de existência de steganografia em imagens jpeg
stegdetect	Detecção de existência de steganografia em imagens jpeg
xsteg	Ferramenta gráfica para detecção de steganografia em imagens jpeg
ghex2	Visualização de arquivos em formato HEX
hexcat	Visualização arquivos em formato HEX
ghexdump	Visualização arquivos em formato HEX
affcat	Verificação conteúdo de arquivos .aff sem montar
afcompare	Comparação de dois arquivos .aff
afconvert	Converção aff -> raw, raw -> aff, aff -> aff recompactação
afinfo	Visualização estatísticas sobre um ou mais arquivos aff
afstats	Visualização estatísticas sobre um ou mais arquivos aff
afxml	Exportar metadados de arquivos aff para um arquivo xml
dcat	Localização de dados dentro de arquivos dd, aff, ewf
glark	Ferramenta para localização de dados
gnome-serach-tool	Ferramenta gráfica de localização de arquivos
slocate	Localização de arquivos e indexação dos disco
mac-robber	Coletar dados de arquivos para criação de linha de tempo (timeline)
mactime	Criação de uma linha do tempo ASCII das atividades dos arquivos
ntfscat	Concatenação de arquivos e visualização sem montar a partição NTFS
ntfsclone	Clonar um sistema de arquivos NTFS ou somente parte dele
ntfscluester	Localizar arquivo dentro de cluster ou de v rios clusters NTFS
ntfsinfo	Obter informações sobre partições NTFS
ntfslabel	Verificação ou alterar a descrição de partições NTFS
ntfsls	Lista o conteúdo de diretórios em partições NTFS sem montá-los
fcrackzip	Ferramenta para quebrar as senhas de arquivos compactados em ZIP
john the ripper	Ferramenta para localização de senhas de usuários
medussa	Crack de senhas
ophcrack	Crack de senhas do Windows
e2undel	Ferramenta para recuperação de arquivos em partições ext2
fatback	Ferramenta para recuperação de dados de sistemas de arquivos FAT
foremost	Ferramenta para recuperação de imagens a partir dos cabeçalhos
gzrecover	Ferramenta para extração dados de arquivos gzip corrompidos
magicrescue	Recuperação de imagens RAW, baseando-se nos cabeçalhos
ntfsundelete	Recuperação de arquivos deletados em partições NTFS
recover	Ferramenta para recuperação todos inodes deletados de um disco
recoverjpg	Ferramenta para recuperação de imagens jpg
scrounge-ntfs	Ferramenta pararecuperação de dados de partições NTFS
chkrookit	Ferramenta para identificar presença de rootkits no sistema
rkhunter	Ferramenta para identificar a presença de rootkits no sistema
fspot	Organizador de imagens fotos
ghtumb	Visualizar e organizar imagens
imageindex	Geração de galeria de imagens em html

Figura 7. Ferramentas para etapa de Exame - FDTK

Análise

FERRAMENTAS	
coockie_cruncher	Análise de coockies
eindeuting	Análise de arquivos .dbx
fccu-evtreader	Script perl para visualização de arquivos de eventos da MS (EVT)
galleta	Análise de coockies do Windows
GrocEVT	Coleção de scripts construídos para leitura de arquivos de eventos do Windows
mork	Script perl para visualização de arquivos history.dat do firefox
pasco	Análise de cache do IExplorer
rifiuti	Análise de arquivos INF2 da MS
xtraceroute	Tracerouter gráfico

Figura 8. Ferramentas para etapa de Análise – FDTK

4. Conclusão

Os desafios para construir uma proposta de aprendizado que atenda as necessidades educacionais da área são diversos, é preciso um posicionamento que não concentre-se inteiramente na técnica, pois disciplinas forenses englobam campos como direito, requerem capacidade de comunicação e argumentação [7].

Desenvolver um modelo que realize uma abordagem unificada, baseado no domínio cognitivo de Bloom [19], pode ser uma alternativa para geração de um modelo pedagógico. Para tanto, é necessário que este contemple conhecimento,

compreensão, aplicação, análise, síntese e avaliação [7], dos processos descritos no domínio cognitivo [19].

Os processos de análise, síntese e avaliação desempenharão papel diferencial para os acadêmicos, pois é neles que habilidades essenciais no campo da ciência forense são desenvolvidas, além disso, o ensino da forense digital exige grande capacidade de adaptação, tal disciplina, bem como outras disciplinas de caráter tecnológico, precisam acompanhar os recorrentes avanços, nos aspectos mercadológicos e tecnológicos, compõem ainda o desafio de estruturação de uma disciplina forense as constantes atualizações de técnicas, ferramentas, metodologias e conceitos jurídicos.

Uma proposta que faz uso de ferramentas *Open Source* surge como alternativa para manter a qualidade do conhecimento exigido dos profissionais desta área, igualmente permite a ampliação do desenvolvimento das pesquisas propiciando aos alunos a colaboração em muitos projetos de pesquisa, saindo da esfera de mero sujeito aprendente passivo a um sujeito cognoscente. Tal movimento se torna possível, através de sugestões e ações que aprimoram ferramentas atualmente utilizadas.

Assim como outros projetos *Open Source*, a FDTK está em constante mudança, buscando sempre manter-se atualizada. A partir do grupo de estudos e do interesse desperto nos acadêmicos outras pesquisas, visando o aperfeiçoamento da FDTK, bem como a melhoria da disciplina de Forense Computacional, devem ser iniciadas.

Trabalhos Futuros

Este projeto mantém-se em desenvolvimento, atualmente existe um grupo de estudos voltado para área, no qual a FDTK desempenha papel primordial na tentativa de desenvolver capital intelectual para área, pesquisas nas mais diversas linhas vêm sendo realizadas: ferramentas para tratamento de dados voláteis objetivando o desenvolvimento de uma ferramenta direcionada a sistemas Microsoft, testes de ferramentas de rede para sua possível inserção em outras versões da distribuição, elaboração de documentação técnica e criação de manuais de utilização das ferramentas que compõem a FDTK. A documentação produzida está sendo disponibilizada em uma página WIKI da distribuição, com intuito de facilitar o acesso ao conhecimento e apresentar este de forma didática aos interessados pela área, bem como aos estudantes do curso.

Referências

[1] Erboncher, Robert F., Marks, Donald G., Pollitt, Mark M., Sommer, Peter M., Yasinsac, Alec, Computer Forensics Education ,2003.

[2] Site oficial do Curso de Segurança da Informação da Universidade do Vale do Rio dos Sinos – Unisinos. Disponível em < http://www.unisinos.br/graduacao/seguranca-da-informacao/apresentacao > Acesso em: Jul de 2011.

[3] FDTK. Site official da Distribuição FDTK – Forense Digital ToolKit. Disponível em < http://fdtk.com.br/ > Acesso em: Jul de 2011.

[4] Tzu, Sun , A Arte da Guerra Os Treze Capítulos Originais, –Jardim dos Livros, 2006.

[5] CP Grobler, Prof B Louwrens , Digital Forensics: A Multi-Dimensional Discipline, University of Johannesburg, Department of Business IT, 2006.

[6] Hauebner, Ewa and Znero, Stefano - Open Source Software for Digital Forensics , 2010.

[7] Nance, Kara., Armstrong, Helen and Armstrong, Colin. Digital Forensics: Defining an Education Agenda, 2010.

[8] DEFT- Digital Evidence & Forensic Toolkit. Página oficial da distribuição. Disponível em <http://www.stevelab.net/deft/>. Acesso em: Jul de 2011.

[9] BACKTRACK. Página oficial da distribuição Backtrack. Disponível em: <http://www.remote-exploit.org/backtrack.html>. Acesso em: Jul de 2011.

[10] INSIDE Security Rescue Toolkit. Página oficial da distribuição insert. Disponível em: <http://www.inside-security.de/insert_en.html>. Acesso em: mai. de 2007.

[11] FCCU. Página oficial da distribuição FCCU. Disponível em <http://www.lnx4n6.be/>. Acesso em: Jul de 2011.

[12] HELIX. Página oficial da distribuição Helix. Disponível em <http://www.e-fense.com/index.php > Acesso em: Jul de 2011.

[13] OPERATOR. Página oficial da distribuição Operator. Disponível em: <http://www.ussysadmin.com/operator/ > Acesso em: Jul de 2011.

[14] PHLAK. Página oficial da distribuição PHALK. Disponível em <http://sourceforge.net/projects/phlakproject/ > Acesso em: Jul de 2011.

[15] L.A.S Linux. Página oficial da distribuição PHALK. Disponível em < http://localareasecurity.com/tag/l-a-s-linux/ > Acesso em: Jul de 2011.

[16] NETWORK UBUNTU. Página oficial da distribuição nubuntu. Disponível em: <http://www.nubuntu.org/ > Acesso em: Jul de 2011.

[17] KNOPPIX. Página oficial da distribuição Knoppix. Disponível em: <http://www.knoppix.org/ > Acesso em: Jul de 2011.

[18] CSRC-NIST. Página oficial do CSRC-NIST - Computer Security Resource Center of National Institute of Standards and Tecnology. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf>. Acesso em: Jul. de 2011.

[19] Bloom, Benjamin S.,Taxonomy of Educational Objectives: The Classification of Educational Goals, 1956.

Leonardo Lemes Fagundes. Doutorando em Computação pela Universidade Federal do Rio Grande do Sul (UFRGS), Mestre em Computação Aplicada e Bacharel em Análise de Sistemas, ambos pela Universidade do Vale do Rio dos Sinos (UNISINOS). Professor e Coodenador da Graduação Tecnológica de Segurança da Infotmação na UNISINOS e Sócio e Diretor da área de Consultoria da Defenda.

Paulo Alberto Neukamp. Especialista em Administração da Técnologia da Informação, Graduado em Segurança da Tecnologia da Informação ambos pela Universidade do Vale do Rio dos Sinos (UNISINOS). Professor da Graduação Tecnológica de Segurança da Infotmação na UNISINOS, Perito em Forense Digital da Defenda e criador e mantenedor da FDTK.

Pamela Carvalho da Silva. Estudande da Graduação Tecnológica de Segurança da Informação da Universidade do Vale do Rio dos Sinos (UNISINOS), Técnica em Sistemas de Informação pelo Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul - Campus Porto Alegre e Analista de Fraude da Defenda, na qual desempenha atividades relacionadas com forense digital e gestão de incidentes.