GIULIANO GIOVA

WEBLABS NA INVESTIGAÇÃO FORENSE DE SISTEMAS ELETRÔNICOS DIGITAIS

São Paulo
2011

GIULIANO GIOVA

WEBLABS NA INVESTIGAÇÃO FORENSE DE SISTEMAS ELETRÔNICOS DIGITAIS

Dissertação apresentada ao Departamento de Engenharia de Sistemas Eletrônicos, da Escola Politécnica da Universidade de São Paulo para obtenção do título de Mestre em Engenharia.

São Paulo

2011

GIULIANO GIOVA

WEBLABS NA INVESTIGAÇÃO FORENSE DE SISTEMAS ELETRÔNICOS DIGITAIS

Dissertação apresentada ao Departamento de Engenharia de Sistemas Eletrônicos, da Escola Politécnica da Universidade de São Paulo para obtenção do título de Mestre em Engenharia.

Área de Concentração: Sistemas Eletrônicos

Orientador: Prof. Dr. Pedro Luis Próspero Sanchez

São Paulo

2010

DEDICATÓRIA

À minha esposa Sandra
e às nossas famílias

AGRADECIMENTOS

Ao Professor Doutor Pedro Luis Próspero Sanchez, por me ter acolhido, orientado, doutrinado e mostrado os fundamentos para desenvolvimento deste trabalho.

Reiteradamente ao Professor Doutor Pedro Luis Próspero Sanchez e ao Professor Doutor Volnys Borges Bernal, pela sua produção científica e ensinamentos que impulsionaram meu conhecimento sobre a ciência forense e sua aplicação na Engenharia.

Aos diretores, coordenadores, professores e funcionários da Escola Politécnica e do Departamento de Sistemas Eletrônicos, pelos ensinamentos e pela honra de participar de um dos principais centros de ensino e pesquisa existentes.

À Universidade de São Paulo, por viabilizar tudo isso.

Aos pesquisadores e autores referenciados neste documento, pelos importantes subsídios que proporcionaram.

EPÍGRAFE

“A informação está substituindo a autoridade”

(Peter Druker)

RESUMO

Giova. G, Weblabs na investigação forense de sistemas eletrônicos digitais [dissertação]. São Paulo: Universidade de São Paulo, Escola Politécnica, 2010. 144 f.

Sistemas digitais tornaram-se onipresentes, há cerca de um bilhão de computadores conectados à Internet, e essenciais às atividades humanas. Em consequência, aumentam os casos judiciais cuja solução depende do exame forense de dispositivos eletrônicos. A investigação de ilícitos é quase sempre presencial: oficiais de justiça e peritos coletam computadores suspeitos e os conduzem para laboratórios especializados mantidos pelo Estado (Institutos de Criminalística), por universidades ou pelos próprios peritos judiciais. Funcionários públicos ou especialistas nomeados pelos Juízes e, quando admissíveis, representantes dos autores e réus, conduzem exames técnicos segundo métodos e ferramentas forenses. O resultado é submetido ao Magistrado na forma de um laudo pericial cuja qualidade tem severa repercussão social por ser elemento de convencimento, decisão e julgamento nos processos judiciais. Essa qualidade é ameaçada pela demanda superior aos recursos disponíveis e pela crescente complexidade. Poucos centros de estudo reúnem recursos e competência apropriados ao desafio, além de quase sempre estarem distantes dos seus principais usuários: milhares de fóruns e delegacias espalhados pelo país. Impõe-se, portanto, que os meios acadêmicos lancem mão das mais recentes descobertas científicas para trazer inovações compatíveis com as novas demandas sociais. Uma das mais promissoras tecnologias nesse sentido é o laboratório acessível remotamente via internet, denominado WebLab, no Brasil alvo do projeto KyaTera, coordenado pela Fapesp. A presente dissertação explora e contextualiza esses temas e faz análise preliminar sobre uma alternativa que poderia, dependendo de estudos complementares futuros, proporcionar aos operadores do Direito, como juízes, peritos oficiais e assistentes técnicos das partes, acesso remoto a laboratórios especializados no exame de sistemas eletrônicos digitais e à sociedade uma ferramenta para tornar mais confiáveis os procedimentos periciais forenses.

Palavras-chave: Weblabs. Internet. Perito. Prova. Laboratório. Forense.

ABSTRACT

Giova. G, Weblabs in forensic investigation of electronic digital systems [dissertation]. São Paulo: Universidade de São Paulo, Escola Politécnica, 2010. 144 f.

Digital systems have become ubiquitous, there are nearly a billion computers connected to Internet, and essential for human activities. This leads to the increase of the number of legal cases whose solution depends on the forensic examination of electronic devices. The investigation of unlawful acts is almost always made on site: bailiffs and experts witness collect suspect computers and take them to specialized laboratories maintained by the governments (criminology institutes), universities or even by expert witnesses. Experts appointed by judges and, if eligible, representatives of the defendants and plaintiffs, conducts technical examinations based on forensic methods and tools. The result of this work is submitted to the Judge as an expert witness report whose quality has severe social repercussions as a matter of conviction and decision in the trial proceedings. This quality is under serious threat due to demand greater than available resources and due to growing complexity. Few centers of study have resources and enough technical skill enough to overcome these challenges, and those centers are often distant from users: thousands of courts and police stations throughout Brazil. It is really necessary the academic community engagement to bring solutions to those new social demands by means of latest scientific findings. One of the most promising technologies in this area is an Internet remotely accessible laboratory, using so called WebLab technology, in Brazil developed mainly by the Fapesp project KyaTera. This dissertation explores and contextualizes these themes and makes a preliminary analysis about an alternative which, depending on future complementary studies, may offer to legal professionals and especially to experts and technical assistants remote access to specialized laboratories for the examination of electronic digital systems, providing a tool to society that makes forensic exams more reliable.

Keywords: Weblabs. Internet. Expert Witness. Proof. Laboratory. Forensic.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
AFF	*Advanced Forensic Format*
ANATEL	Agência Nacional de Telecomunicações
CAD	*Computer Aided Design*
CD	*Compact disk*
CETIC.BR	Centro de Estudos sobre as Tecnologias da Informação e da Comunicação – NIC.BR
CGI	Comitê Gestor da Internet no Brasil
ESI	*Electronic Stored Information*
FIB	*Focused Ion Beam*
HD	*Hard disk*
IBGE	Instituto Brasileiro de Geografia e Estatística
ISO	*International Standardization Organization*
JSON	*JavaScript Object Notation*
ITU	*International Telecommunication Union*
MDGs	*Millennium Development Goals*
NIC.BR	Núcleo de Informação e Coordenação do Ponto BR
P2P	*Peer to peer*
RAM	*Random Access Memory*
ROM	*Read Only Memory*
SOAP	*Simple Object Assess Protocol*
TI	Tecnologia da Informação
TIC	Tecnologias da informação e das comunicações
URL	*Uniform Resource Locator*
USP	Universidade de São Paulo
VoIP	*Voice over IP*
XML	*eXtended Markup Language*

SUMÁRIO

1 INTRODUÇÃO

Os sistemas eletrônicos para processamento de dados tornaram-se essenciais e onipresentes em todas as atividades humanas; há mais de um bilhão de computadores pessoais em operação no mundo e por ano são vendidos mais de um bilhão de telefones celulares, dispositivos que também incorporam crescente capacidade de processamento (GARTNER, 2009).

A par dos benefícios fundamentais trazidos pelo intenso uso das tecnologias da informação e das comunicações (TIC), cresce a quantidade de conflitos de interesses onde dispositivos digitais têm papel relevante, seja como objeto direto da disputa, seja como elemento indireto de prova.

O presente trabalho reúne informações sobre a evolução desse ambiente tecnológico e seu impacto na perícia técnica enquanto elemento auxiliar na produção de provas para o convencimento dos juízes, focando a distância existente entre os principais laboratórios periciais e o local onde efetivamente transcorrem os processos judiciais, considerando-a como um fator limitador da qualidade das decisões tomadas pelos magistrados. Em seguida, busca uma possível alternativa para melhorar esse cenário no âmbito forense partindo de modelos que vem sendo experimentados e aperfeiçoados em outras áreas científicas.

Este capítulo contextualiza e justifica o tema e depois detalha objetivo, métodos e organização do trabalho.

1.1 CONTEXTO

Nos processos criminais, o exame forense de dispositivos eletrônicos digitais é realizado nos núcleos de engenharia ou informática dos institutos de criminalística subordinados às polícias científicas dos governos estaduais ou do governo federal, estando o procedimento sob a responsabilidade de policiais ou peritos admitidos por concurso público e treinados nas práticas periciais em academias de polícia.

Em processos de outras naturezas, principalmente cíveis, trabalhistas ou da família, os exames forenses são usualmente realizados por peritos judiciais nomeados pelo juiz, escolhidos *ad hoc* entre os profissionais de nível superior do meio acadêmico ou

que atuam no mercado como funcionários de empresas ou prestadores de serviços. Algumas vezes, juízes ou promotores valem-se dos profissionais de informática que prestam suporte internamente ao próprio tribunal ou órgão do Estado.

O papel das universidades nesse cenário mostra-se heterogêneo e mutável em função das suas normas internas, da matéria a ser analisada, do andamento de cada processo e das práticas individuais de cada comarca e juiz.

Quanto ao método de trabalho, a primeira tarefa pericial usualmente consiste em localizar e coletar evidências, frequentemente no exame do local do crime ou por meio de "vistorias" ou "buscas e apreensões" determinadas por um juiz, muitas vezes sem o conhecimento prévio da parte averiguada, formato cada vez mais adotado diante do receio de que o investigado oculte, modifique ou destrua intencionalmente evidências digitais altamente voláteis. Nessa tarefa o perito acompanha um oficial de justiça ou alguma autoridade policial, mas algumas vezes o trabalho pericial é realizado mais livremente, com o simples agendamento de diligências pelo perito diretamente junto às partes no processo judicial.

Raramente o exame das evidências é feito diretamente no local da diligência, pois podem ser necessárias dezenas ou centenas de horas de trabalho antes que se possa chegar a uma conclusão suficientemente segura para culpar ou inocentar um suspeito.

Há muitas razões que dificultam ou impedem o exame apressado de sistemas eletrônicos digitais. Além de armazenar facilmente bilhões ou trilhões de bytes, os modernos dispositivos digitais utilizam estruturas de armazenamento distintas em função do dispositivo (HD, CD, RAM, *flash memory* etc.), do tipo de dado armazenado (texto alfanumérico, banco de dados, mensagens, áudio, vídeo etc.), dos recursos de proteção (criptografia), entre outras características e propriedades.

Isso faz com que uma busca por palavras-chave como “cocaína” ou “pedofilia” em um computador pessoal, até recentemente procuradas simplesmente no formato texto entre documentos eletrônicos armazenados no disco rígido, atualmente tenham que ser procuradas também segundo o padrão Unicode, que contempla desde nosso idioma até ideogramas orientais, ou como fonemas ocultos dentro de arquivos multimídia ou pacotes VoIP.

Cumpre observar também que esses dados e sistemas cada vez mais ultrapassam os limites geográficos do dispositivo local para integrar-se, distribuir-se e serem processados em redes locais, metropolitanas ou mundiais, tornado mais complexas sua localização, preservação e análise.

A crescente preocupação da sociedade com questões sobre privacidade e segurança leva fabricantes de sistemas eletrônicos digitais e prestadores de serviços a adotar progressivamente mais recursos para criptografar dados armazenados, processados ou transmitidos, protegendo com isso os usuários, mas ao mesmo tempo dificultando exames periciais por ocultar possíveis evidências.

Esse cenário torna temerária qualquer conclusão obtida apressadamente durante uma vistoria, pela limitação do tempo e recursos técnicos disponíveis durante uma diligência pericial realizada em ambiente externo, restando como alternativa segura a preservação dos dados e seu exame pelo tempo que for necessário em laboratórios periciais dotados de recursos técnicos adequados, contudo isso pode levar a autoridade a confiscar os equipamentos e sistemas.

Porém, essa apreensão traz graves prejuízos aos proprietários e usuários, pois impede que prossigam com suas atividades dependentes dos computadores, celulares e outros dispositivos digitais apreendidos. Além disso, ao perderem o acesso físico aos seus equipamentos torna-se mais difícil que eles possam encontrar evidências e contraprovas eventualmente existentes, prejudicando sua defesa no processo.

A alternativa recomendada em substituição ao confisco de equipamentos é a apreensão judicial de cópia forense dos dados. Cabe salientar a distinção entre “apreensão de equipamentos” e “apreensão dos dados digitais contidos nos equipamentos”, deixando-se ou não os dados originais com o suspeito, decisão que usualmente está relacionada à constatação ou não de algum ilícito relacionado aos dados. Uma cópia forense consiste na aquisição dos dados originais mediante cópia bit a bit realizada em conformidade com os princípios forenses, isto é, a geração de uma cópia com conteúdo idêntico ao original, coletada sem que nesse procedimento ocorra qualquer modificação no dispositivo original e assegurando o registro da cadeia de custódia. A proteção do dispositivo original baseia-se em um recurso denominado *hard block* intercalado na conexão com o computador, bloqueando

qualquer tentativa de gravação no dispositivo original e permitindo apenas sua leitura. A cadeia de custódia visa assegurar a possibilidade de que, a qualquer tempo, seja possível verificar a origem e integridade da peça pericial. O elemento principal na cadeia de custódia de um dispositivo digital é o seu código *hash*, um resumo na forma de uma pequena sequência numérica hexadecimal gerada por um algoritmo matemático que lê todos os bits do dispositivo examinado. O código *hash* acompanhará a vida da evidência digital e se posteriormente houver diferença até mesmo em um único bit no dispositivo original, o seu código *hash* será diferente, alertando sobre a existência de uma diferença.

O resultado de um procedimento de cópia bit a bit é usualmente um “clone”, isto é, a cópia forense de um disco rígido resultará em outro disco rígido com a mesma estrutura e conteúdo, de onde provém seu nome. Mais modernamente, peritos preferem coletar dados no formato “imagem”, ou seja, todo o conteúdo de um disco rígido passa a ser representado dentro de um único arquivo, chamado arquivo imagem do disco original. A imagem forense apresenta diversas vantagens em relação à cópia forense, porque possui controles adicionais de integridade e pode mais facilmente ser replicada e analisada. Sua desvantagem é que o perito passa a depender de algum programa forense para visualizar o conteúdo do arquivo imagem, diferentemente do clone, pois este pode ser visualizado como qualquer outro disco, desde que protegido contra gravação.

Nesse novo modelo de atuação, a diligência é finalizada com a apreensão de cópias ou imagens forense, em vez do material original, e com sua condução até um instituto de criminalística ou ao laboratório particular de um perito judicial, onde serão devidamente examinadas. Existe ainda a solução intermediária que consiste na apreensão do material original apenas pelo tempo necessário para se gerar as cópias ou imagens forenses, com sua devolução ao proprietário logo em seguida.

Com os métodos discutidos, deixa de existir nos institutos de criminalística a necessidade de armazenar e vigiar grande quantidade de computadores e discos apreendidos, havendo em seu lugar bibliotecas digitais que armazenam virtualmente as imagens forenses desses dispositivos.

O exame pericial dessas imagens forenses ocorre normalmente no modo passivo, através de programas periciais forenses, como o EnCase, FTK ou Autopsy, entre

outros, isto é, o sistema examinado não “sobe”, pois é apenas examinada passivamente a sua estrutura de dados. Se houver a real necessidade de verificar o funcionamento do computador examinado, a perícia cria máquinas virtuais que podem ser configuradas à semelhança do computador original.

Não foram obtidas estatísticas oficiais sobre a quantidade de computadores originais ou cópias forenses apreendidas em ações policiais ou judiciais. Os relatos informais encontrados, detalhados mais adiante nesta dissertação, sugerem que estão ocorrendo níveis crescentes de apreensões e que existem frequentes reclamações sobre a baixa qualidade e demora excessiva dos trabalhos periciais.

Nos processos criminais, os exames são realizados nos núcleos de criminalística das polícias científicas, em nível estadual ou federal. O Departamento de Polícia Federal conta com o Instituto Nacional de Criminalística e com mais de trinta unidades regionais de perícia, neles um quadro de aproximadamente mil peritos produziu nos últimos anos mais de 200 mil laudos nas diversas áreas de conhecimento (SANTOS JR., 2009). Na esfera estadual, praticamente todos os governos instituíram a sua própria Polícia Científica que opera núcleos especializados de criminalística.

Os peritos federais e estaduais são funcionários públicos subordinados às respectivas estruturas policiais, fato que tem sido criticado por alguns setores da sociedade pelo risco de ingerência política e de outras naturezas na coleta de evidências, no andamento dos trabalhos e no resultado da perícia.

Por esse motivo, membros da OAB chegaram a defender que os institutos de criminalística deveriam passar a subordinar-se às universidades e não mais às Secretarias de Segurança Pública, visando assegurar sua independência e autonomia durante os trabalhos periciais e maior observância dos rigores científicos (LEITÃO, 2008).

De outro lado, os críticos dessa separação alegam que a perícia criminal inclui-se no conceito de Polícia Judiciária, não podendo de ela ser dissociada, cabendo apenas autonomia para o cargo, mas não do órgão.

Nas decisões sobre qualquer modelo hierárquico e funcional que possa ser adotado para custodiar e examinar evidências digitais, é preciso ter presente que essas

evidências são altamente voláteis, podem facilmente ser modificadas ou destruídas e seu exame requer conhecimentos técnicos e metodologia avançados.

Nas esferas cível, trabalhista e da família, os exames são tipicamente realizados por peritos judiciais nomeados *ad hoc* diretamente pelos juízes, geralmente são funcionários de empresas privadas, universidades ou órgãos públicos, outras vezes são prestadores de serviço no mercado.

O Brasil conta com mais de cinco mil municípios, neles havendo aproximadamente 2.500 comarcas judiciais, ou seja, apenas metade dos municípios possui acesso local aos serviços judiciários, o restante precisa recorrer aos serviços prestados em algum município próximo ou por juízes itinerantes (INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA, 2008).

Assumindo-se como premissa que existam pelo menos dois peritos judiciais em tecnologia da informação nas comarcas menores e mais do que isso nas comarcas maiores, resulta a estimativa informal de que devam existir cerca de 5 ou 6 mil peritos judiciais em TI efetivamente ativos no país.

As notícias informais mostram ainda que raramente peritos judiciais têm dedicação exclusiva a essa atividade, pois a maior parte é convocada apenas esporadicamente pelos juízes, caso a caso. Menos frequentemente ainda, esses profissionais mantêm laboratórios permanentes e atualizados com os equipamentos e softwares forenses necessários para produzir exames periciais confiáveis.

Os altos custos dos softwares forenses mais completos e atualizados[1] podem ainda tentar alguns peritos a utilizar ferramentas inadequadas ou até mesmo cópias contrafeitas, tornando venal esse procedimento, o que seria absolutamente inadmissível na produção de provas forenses, fragilizando todo o sistema.

Nas grandes cidades, os peritos judiciais têm a possibilidade de contratar pontualmente serviços de laboratórios privados, como alternativa à aquisição de licenças definitivas dos programas, porém essa solução é praticamente inviável para

[1] Licenças individuais de programas forenses em tecnologia da informação custam geralmente entre 2 e 20 mil reais, licenças corporativas podem alcançar valores na ordem de um milhão de reais ou mais. O cenário agrava-se se for considerado que quase sempre os softwares são especializados, ou seja, o mesmo produto não é eficaz, por exemplo, tanto para discos rígidos de computador como para telefones móveis celulares, implicando na aquisição de licenças para diversos softwares.

os peritos judiciais que atuam em regiões distantes e, ainda mais complexo, os laboratórios precisam ter licenças de software que permitam essa prática.

Juízes e peritos judiciais podem também recorrer às universidades, quando elas existirem nas proximidades da comarca; contudo verificações informais sugerem que na maior parte delas a atenção com as Ciências Forenses ainda é mais uma iniciativa isolada de alguns professores do que um esforço acadêmico organizado.

Não se pode deixar de considerar, também, que a incorporação contínua de novas tecnologias da informação e das comunicações impõe a necessidade de envolvimento de novos tipos de especialistas para o exame pericial de dispositivos utilizados no dia a dia. Com isso, aumenta a quantidade das perícias consideradas complexas, que obrigam a nomeação simultânea de mais de um perito, um para cada especialidade, além da necessidade de alocação de laboratórios multidisciplinares (FEDERAL JUDICIAL CENTER, 2000).

O principal problema não parecer residir na falta de competência técnica ou na inexistência de laboratórios especializados, mas no fato desses recursos não estarem adequadamente organizados para realizar trabalhos forenses e situarem-se preponderantemente locais distantes de onde os serviços precisam ser utilizados, em milhares de municípios distantes dos grandes centros tecnológicos.

Assim, o forte crescimento na demanda forense por exames técnicos altamente especializados e a grande dispersão geográfica dos locais onde ocorrem crimes ou procedimentos indevidos impõem a busca de soluções que tornem disponíveis laboratórios e competências técnicas de alta qualidade diretamente nos locais onde a Justiça deve processar os feitos jurídicos.

Mais ainda, a natureza dos novos sistemas impõe às partes envolvidas nos processos judiciais e à própria sociedade fiscalizar o tratamento dados às evidências digitais e como elas são preservadas, examinadas e consideradas no julgamento das ações judiciais.

1.2 PROBLEMA A RESOLVER

Como será detalhado nesta dissertação, em milhares de comarcas brasileiras está ocorrendo grande aumento na utilização de dispositivos baseados em modernas e

sofisticadas tecnologias da informação e das comunicações. Com isso, há crescente demanda por recursos técnicos locais adequados para a produção de provas periciais, contudo esses recursos são até hoje escassos e presentes apenas nos grandes centros econômicos, onde estão as principais universidades e empresas dedicadas à pesquisa científica e à produção tecnológica.

Esse cenário tende a se agravar, por fatores como:

a) aumento na quantidade, diversidade, complexidade e capacidade dos dispositivos digitais submetidos à perícia forense;

b) aumento dos recursos de segurança e de proteção da privacidade, dificultando muito o exame pericial de sistemas eletrônicos digitais;

c) baixa disponibilidade, nos locais das disputas judiciais, de laboratórios periciais equipados com recursos adequados (peritos competentes, computadores potentes, softwares especializados);

d) dificuldade de acesso em escala nacional aos poucos laboratórios efetivamente equipados, deixando à margem autoridades e peritos dos municípios menores ou mais distantes, os poucos centros governamentais e privados dotados de recursos avançados para perícia forense em dispositivos digitais dificilmente conseguem atender a demanda no resto do país;

e) falta de profissionais preparados e existência de deficiências em sua formação e atualização técnica;

f) falta de padrões de qualidade e uniformidade nos procedimentos periciais, insuficientes para trazer segurança às decisões judiciais.

g) dificuldade ou mesmo impossibilidade de que os operadores do Direito e a própria sociedade exerçam seu papel de fiscalização sobre a produção da prova pericial, questão bastante grave tendo em vista que a prova técnica é considerada uma das mais importantes;

h) severas consequências sociais, pois a sociedade presume que exames e as conclusões periciais são confiáveis e imparciais.

Dessa maneira, o problema a resolver é encontrar soluções pelas quais os operadores do Direito que atuam nos milhares de comarcas de todo o país e que demandam perícias em sistemas eletrônicos digitais poderiam ter acesso aos

serviços e recursos altamente especializados disponíveis nos mais competentes e aparelhados centros periciais governamentais, acadêmicos ou privados existentes no Brasil ou no mundo.

1.3 OBJETIVO DO TRABALHO

O objetivo e a motivação deste trabalho é estudar a bibliografia básica sobre esses temas e, em seguida, apresentar um experimento simples para exame remoto de um dispositivo digital. Mesmo se de forma bastante limitada, visa contribuir com a escolha e desenho de experimentos futuros, mais completos, os quais, por sua vez, possibilitariam propor a criação de uma rede de laboratórios remotos voltados ao exame forense de sistemas eletrônicos digitais.

1.4 DELIMITAÇÃO

A propositura de soluções para o problema apresentado e a verificação de sua viabilidade prática são tarefas complexas devido às múltiplas questões técnicas, jurídicas e sociais envolvidas.

O objeto deste estudo situa-se na região multidisciplinar situada entre áreas distintas e muito abrangentes da Engenharia Eletrônica, da Tecnologia da Informação, do Direito e das Ciências Sociais.

A complexidade é ainda maior porque o objetivo da perícia judicial em dispositivos digitais frequentemente abrange outras áreas científicas além daquelas mencionadas. O exame de um computador pode ter como meta identificar evidências digitais que se situam em áreas tão distintas como Medicina, Aviônica, Construção Civil, Química, Literatura, Ciências Contábeis ou Mercado Financeiro.

Essa complexidade transfere-se também para as próprias ferramentas, requerendo softwares forenses cada vez maiores e mais caros, mais difíceis de serem projetados e lançados pelos seus fabricantes.

Por esses motivos, o presente trabalho não pode abranger o tema com a profundidade e extensão desejados inicialmente, deve limitar-se ao estudo da bibliografia básica e à proposição bastante limitada de uma possível solução,

focando o conceito principal e algumas características da sua implementação prática por meio de um experimento em um único dispositivo digital.

O detalhamento da solução, sua avaliação mais completa e a evolução do assunto são tarefas mais complexas que devem ser remetidas a trabalhos complementares que poderão ser desenvolvidos subsequentemente.

1.5 MÉTODO

Foi realizada uma pesquisa descritiva preliminar sobre o cenário dos dispositivos digitais baseados nas tecnologias da informação e das comunicações, focando tanto sua disseminação na moderna sociedade da informação, em nível mundial e nacional, quanto nos principais problemas de segurança apontados no país.

Tendo em vista a ausência de informações científicas, foi realizada verificação informal sobre as dificuldades da perícia nacional, coletando-se frases de interesse contidas nas notícias divulgadas pela imprensa.

Esse material indica informalmente a existências de problemas severos nas práticas periciais, pois mostra baixa eficácia na resolução de crimes, erros nos procedimentos, falta de estrutura, heterogeneidade nas competências periciais, sobrecarga dos órgãos governamentais, demora excessiva dos trabalhos e falta de fiscalização pela sociedade.

Foram compiladas informações sobre crescimento da base de sistemas eletrônicos digitais e os resultados foram confrontados com as notícias sobre a baixa qualidade pericial, resultando uma indicação informal que sugere o agravamento do cenário no decorrer dos próximos anos.

Em seguida, foram verificadas notícias sobre soluções adotadas para problemas similares em outras áreas científicas, como Química, Medicina e Engenharia, constatando-se estar ocorrendo criação, teste e implantação de laboratórios remotos denominados WebLabs.

Assim, o presente trabalho trouxe subsídios para a definição preliminar do que seria um WebLab Forense voltado ao exame de sistemas eletrônicos digitais. Possibilitou, também, a realização de um experimento restrito a um componente, a título de prova

de conceito, que consistiu no acesso remoto a um laboratório forense para coletar e examinar o conteúdo de um disco rígido de computador pessoal.

Com isso, a possibilidade de adoção do modelo típico de WebLabs para estruturar laboratórios voltados ao exame forense remoto em sistemas eletrônicos digitais foi testada por meio de uma prova de conceito que consistiu em um experimento prático utilizando os recursos disponíveis e sem a necessidade de desenvolvimento de uma solução mais completa ou complexa.

Esse experimento certamente tem severas limitações técnicas que não puderam ser superadas em decorrência da grande amplitude do tema e das fortes limitações de tempo e recursos, conforme dito inicialmente, mas foi considerado apto enquanto uma avaliação preliminar da proposta e para apoiar a definição de possíveis estudos futuros, mais abrangentes e profundos. Os resultados obtidos foram registrados e são apresentados nos próximos capítulos, para subsidiar debates acadêmicos e novos estudos que possam melhor avaliar ou até mesmo estender a solução proposta.

1.6 ESTRUTURA

A dissertação está estruturada em cinco capítulos. O primeiro capítulo contextualizou as periciais digitais forenses e discorreu sobre a piora desses serviços em função do aumento quantitativo e qualitativo dos sistemas eletrônicos digitais na sociedade moderna, levando ao problema a ser resolvido e à motivação deste trabalho, detalhando seus objetivos, metodologia e limitações. O segundo capítulo discorre sobre a crescente presença dos dispositivos digitais na sociedade da informação e sobre a missão do Estado em resolver os conflitos de interesse por meio de perícias técnicas. O terceiro capítulo estuda as dificuldades dos laboratórios periciais nesse cenário e apresenta uma possível solução baseada no modelo de WebLabs. O quarto capítulo detalha uma prova de conceito realizada com o objetivo de obter informações preliminares sobre a viabilidade prática da solução proposta e depois avança no sentido de propor linhas de ação para experimentos futuros mais completos. O quinto capítulo discute as conclusões desse trabalho, as contribuições resultantes e os trabalhos futuros sugeridos.

2 A SOCIEDADE DA INFORMAÇÃO E A PROVA PERICIAL

Este capítulo avalia o impacto das novas tecnologias da informação e das comunicações no modo de vida da sociedade moderna, partindo dos dados publicados recentemente pelos principais centros de pesquisa. Avalia, ainda, a repercussão dessas tecnologias nas tarefas do Estado para a resolução dos conflitos de interesse, focando as implicações sobre o trabalho desenvolvido pelos peritos e suas consequências na formação do convencimento judicial.

2.1 TECNOLOGIAS DA INFORMAÇÃO E DA COMUNICAÇÃO

Os sistemas eletrônicos para processamento de dados tornaram-se essenciais e onipresentes em todas as atividades humanas.

Nos últimos anos, esse movimento ressentiu a recente crise econômica mundial, mas mesmo assim a utilização das tecnologias da informação e das comunicações continuou a crescer intensamente em nível mundial (GARTNER, 2009).

A Figura 1 mostra a expansão mundial da telefonia e da internet de 1998 a 2009, vendo-se que a penetração de telefones móveis celulares no mundo mais que dobrou desde 2005, passando de 23 para 67 assinaturas para cada 100 habitantes ao final de 2009.

A internet continuou crescendo a taxas pouco inferiores, estima-se que em 2009 chegou a cerca de 26% da população mundial, estimada em 1,7 bilhões de pessoas (ITU, 2010, p. 1).

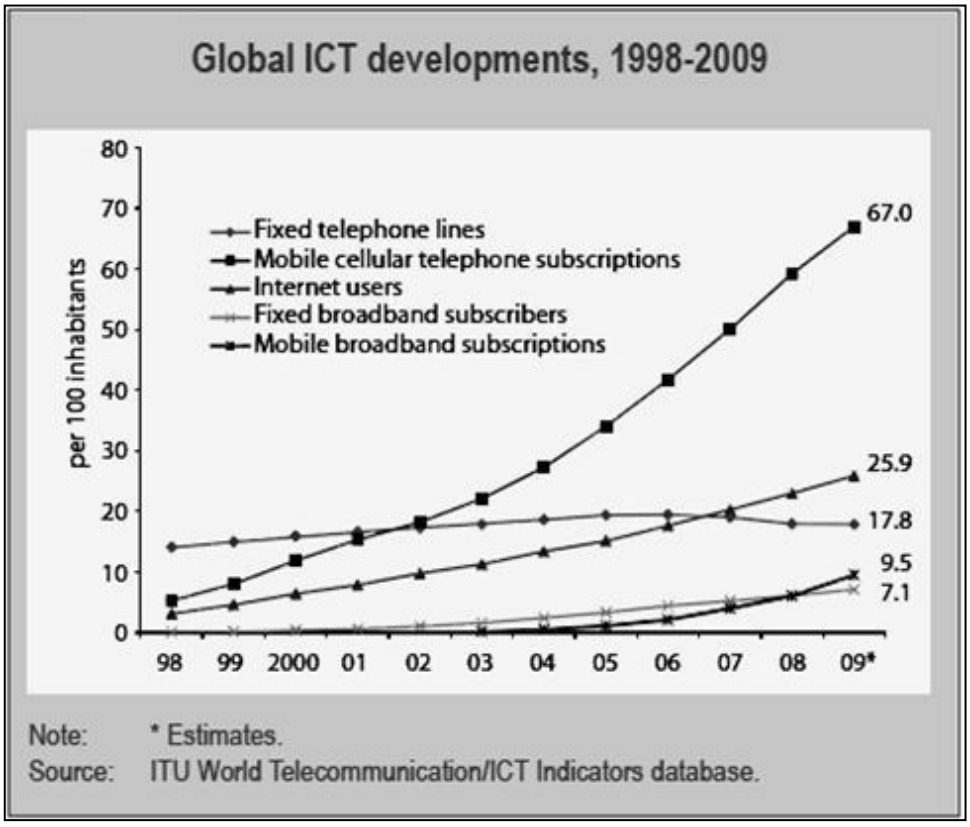

Figura 1. Expansão da telefonia e da internet

A introdução do acesso móvel à internet em alta velocidade acelerou o crescimento mundial de usuários, especialmente nos países em desenvolvimento, ao ponto de em 2008 o número de assinaturas de banda larga móvel ter superado consistentemente a quantidade de assinantes fixos (ITU, 2010, p. 2).

A adesão continuou a crescer intensamente em 2009. Mais relevante ainda é tendência de alta, pois nos levantamentos do início de 2009 a maior parte dos países ainda não havia implantado a tecnologia 3G, portanto ainda não ofereciam acesso móvel de alta velocidade, cenário que muda rapidamente logo depois alavancando a tendência de adesão à internet e às comunicações móveis para os próximos anos (ITU, 2010, p. 2).

A Figura 2 apresenta a variação mundial no preço da telefonia e acesso fixo em banda larga em 2008 e 2009, mostrando franca queda na evolução do preço dos serviços que envolvem tecnologia da informação e telecomunicações, com reduções de 10% a 50% ao ano, muito expressivas se comparadas ao aumento de desempenho técnico dos serviços (ITU, 2010, p. 59).

ICT Price Basket and sub-baskets*

	2008	2009	Average 2008/2009 value decrease	
			Absolute	Percentage
ICT Price Basket	15.0	12.8	2.2	14.8
Fixed telephone sub-basket	7.4	5.9	1.5	20.4
Mobile cellular sub-basket	7.5	5.7	1.9	25.0
Fixed broadband sub-basket	210.8	122	88.8	42.1

Note: * Simple averages. Discrepancies may be due to rounding.
Source: ITU.

Figura 2. Preço da telefonia e acesso fixo em banda larga

Os impactos econômicos e sociais resultantes desses movimentos estão refletidos nas metas definidas por organismos nacionais e supranacionais. O *World Summit on the Information Society* (WSIS) prevê para 2015 que metade dos habitantes deverá ter acesso às tecnologias da informação e telecomunicações, priorizando a conexão de pequenas cidades, escolas, centros de saúde, bibliotecas e órgãos governamentais, e que deverão ser incluídas nos currículos escolares matérias relacionadas à internet e às comunicações.

As Nações Unidas incluíram nos *Millennium Development Goals* metas específicas para serviços móveis de saúde e monitoramento, educação à distância para crianças e tele-trabalho. Com base em levantamentos empíricos, a *International Telecomunication Union* conclui que as tecnologias de informação e tecnologias de telecomunicações efetivamente aumentaram os níveis globais de produtividade, comércio e empregos (ITU, 2010, p. 79).

Os indicadores sociais confirmam a existência de movimento similar também no Brasil. A *Internet World Stats* consolidou dados de outras fontes (ITU, CI Almanac, World Bank, IBGE e CGI) mostrando que o país chegou ao índice de 36,2% de penetração em 2009. Os dados informais consolidados indicam forte crescimento da Internet entre 2000 e 2009, mesmo se houve crescimento menor entre 2008 e 2009 em decorrência da recente crise econômica (INTERNET WORLD STATS, 2009).

Internet Growth and Population Statistics:

YEAR	Population	Internet Users	% Pen.	GNI p.c.	Usage Source
2000	169,544,443	5,000,000	2.9 %	$ 3,570	ITU
2005	184,284,898	25,900,000	14.1 %	$ 3,460	C. I. Almanac
2006	186,771,161	32,130,000	17.2 %	$ 3,460	I. T. U.
2007	186,771,161	42,600,000	22.8 %	$ 4,730	I. T. U.
2008	196,342,587	67,510,400	34.4 %	$ 5,910	I. T. U.
2009	198,739,269	72,027,700	36.2 %	$ 5,910	I. T. U.

Note: GNI is Gross National Income per capita, and corresponds to World Bank data in US dollars.

Figura 3. Índices de penetração da Internet no Brasil.

Artigo divulgado pelo Centro de Estudos sobre as Tecnologias da Informação e da Comunicação (CETIC.BR) informa que o país tem a banda larga mais cara do mundo e ela é ainda considerada insuficiente porque só existe nos grandes centros, caracterizando um fenômeno urbano concentrado nas regiões de alta renda (CGI.BR, 2009, p. 55).

Outro artigo apresentado pelo CETIC mostra elevado nível de concentração das empresas prestadoras de serviços de banda larga nos municípios brasileiros. Os serviços são prestados por mais de uma operadora em 184 municípios brasileiros (83 milhões de pessoas), por uma única operadora em 2.235 municípios (63 milhões de pessoas) e ainda não há efetivo atendimento nos demais 3.145 municípios (CGI.BR, 2009, p. 56).

O Plano Nacional de Banda Larga pretende aumentar o nível de atendimento em todo o Brasil ao fixar como meta reduzir em cerca de 70% o preço médio cobrado pelo serviço e levar o atendimento a 88% da população brasileira até 2014 (CGI.BR, 2009, p. 56).

Esse plano passa a considerar o acesso em banda larga como uma infraestrutura essencial, nos moldes dos outros serviços essenciais como eletricidade, água e esgoto (CGI.BR, 2009, p. 71).

O Plano Geral de Atualização da Regulamentação de Telecomunicações no Brasil, da ANATEL, prevê que a banda larga móvel via Serviço Móvel Pessoal deverá atingir até o ano de 2018 a marca de 125 milhões de acessos mediante tecnologia

que possibilita utilizar a internet mesmo enquanto em movimento, sendo relevante considerar que cerca de 78% dos domicílios brasileiros possuem pelo menos um telefone celular (CGI.BR, 2009, p. 71).

A pesquisa sobre o uso das tecnologias da informação e da comunicação no Brasil mostra intenso crescimento nacional em 2009 na quantidade de domicílios que utilizam equipamentos baseados em tecnologias informação e da comunicação.

A Figura 4 mostra que até mesmo as conexões de telefonia fixa, que vinham em queda, voltaram a crescer em função da oferta de pacotes “combos” que incluem o acesso à internet (CGI.BR, 2009, p. 119).

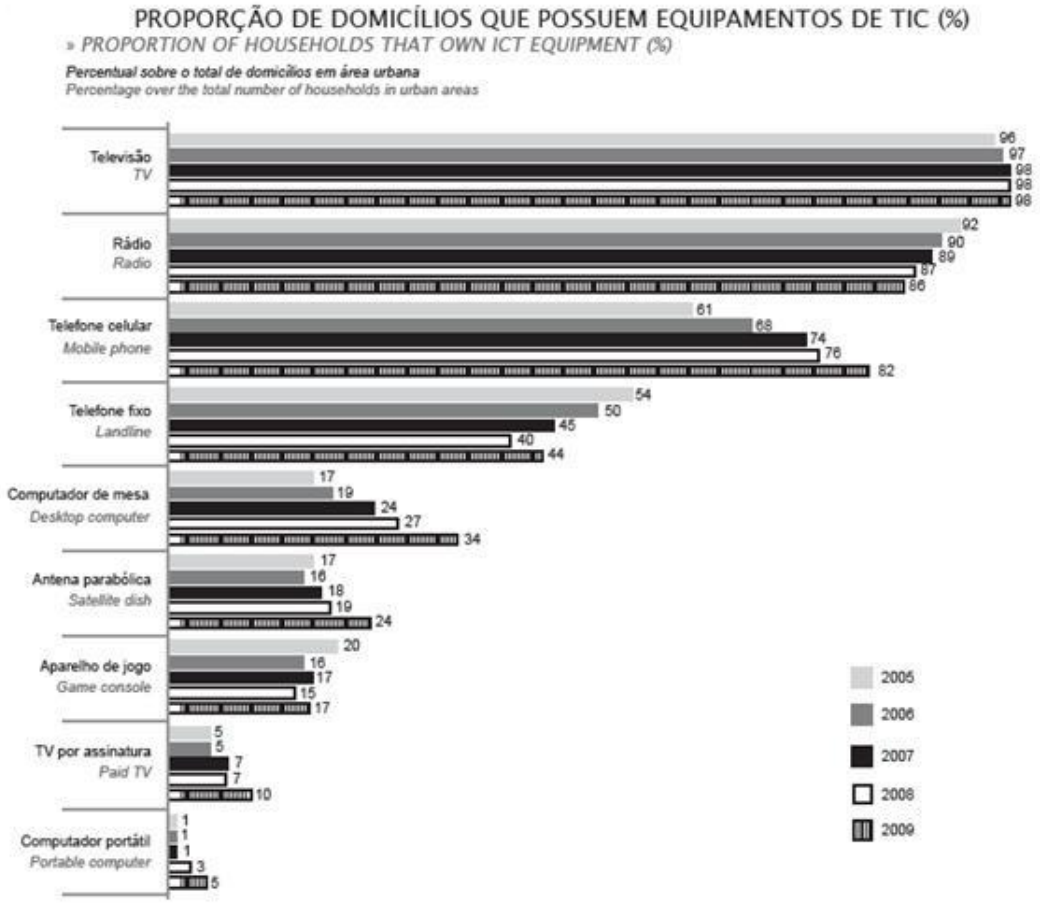

Figura 4. Domicílios com equipamentos de TI e Telecom

A Figura 5 mostra o crescente aumento das tecnologias de informação e comunicação no modo de vida de sociedade atual, mesmo se são visíveis reflexos dos problemas econômicos nos anos de 2008 e 2009 com queda nos serviços financeiros (CGI.BR, 2009, p. 137).

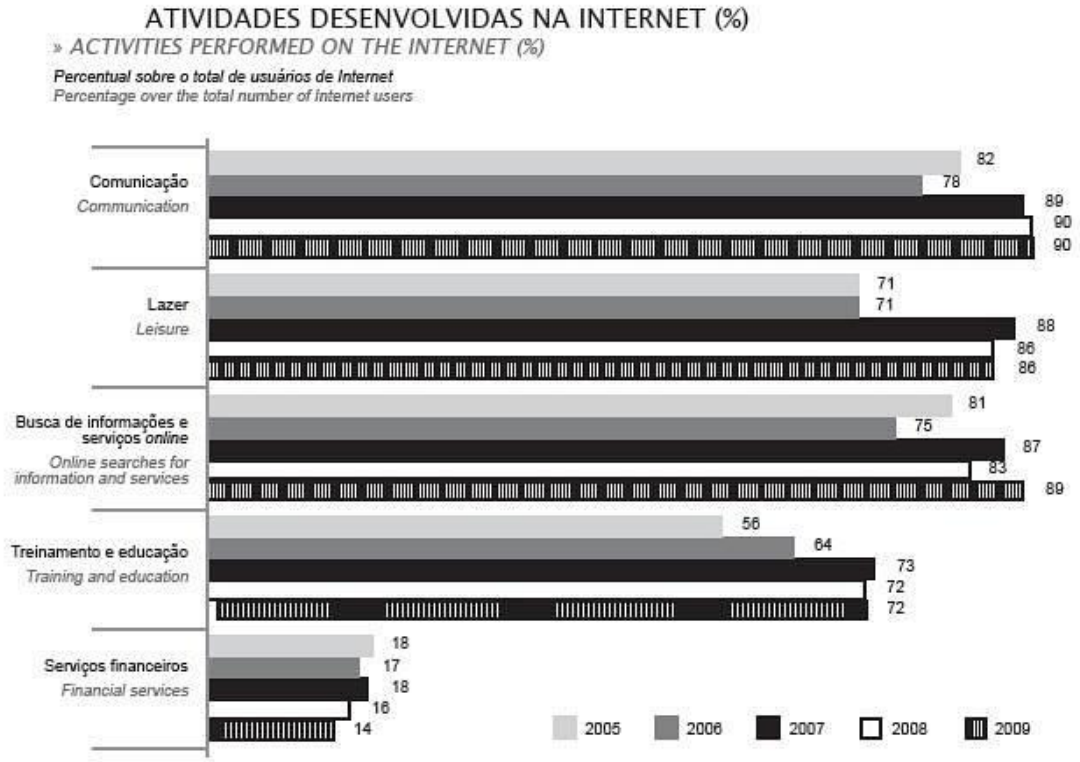

Figura 5. Atividades desenvolvidas na Internet

A Figura 6 mostra a crescente inserção do telefone celular nas atividades das rotineiras das pessoas físicas (CGI.BR, 2009, p. 148).

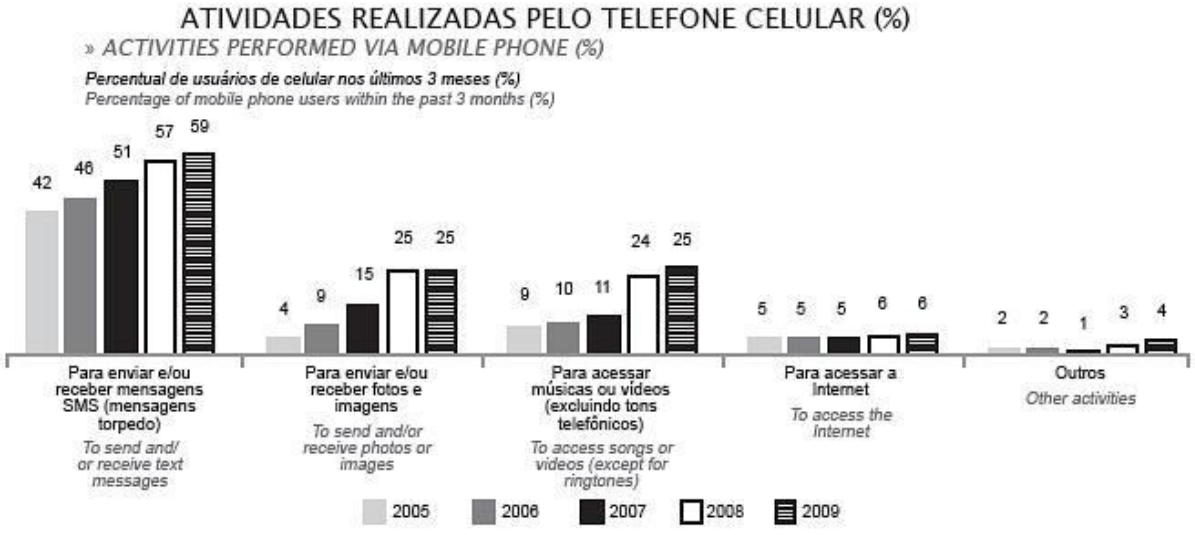

Figura 6. Atividades realizadas com o telefone celular

No mundo empresarial, a pesquisa indica que cerca de 65% das empresas brasileiras adotam telefones celulares corporativos, sendo que 45% utilizam o aparelho para envio e recebimento de SMS e MMS, 25% para acesso à internet e 25% enviam e-mails (CGI.BR, 2009, p. 191).

Cerca de 97% das empresas brasileiras com mais de 10 funcionários utilizam computadores, chegando esse índice a 100% naquelas com mais de 50 funcionários. Nas empresas menores, o índice é de 96% com tendência de crescimento rumo à generalização no uso de computadores (CGI.BR, 2009, p. 193).

Dentro das empresas, o percentual dos funcionários que utilizam computador é pouco inferior à metade, cerca de 45% (CGI.BR, 2009, p. 194).

A conectividade apresentou mudanças relevantes, pois em 2006 cerca de 15% possibilitavam acesso remoto dos funcionários aos seus computadores, tendo havido um crescimento até 25% em 2009. Em 2009, cerca de 41% das empresas já possuíam acesso a rede local sem fio, com redução entre 2008 e 2009, de 83% para 79%, nas empresas com LAN estruturada com fio, porém essa variação não pode ser considerada uma substituição das redes com fio pelas sem fio (CGI.BR, 2009, p. 196).

Os indicadores apresentados neste capítulo, entre outros analisados, demonstram que a sociedade brasileira já está fortemente imersa no dito mundo virtual e que esse processo deve prosseguir nos próximos dez anos com a crescente inclusão de atividades pessoais, empresariais e governamentais ainda não atendidas, fortalecendo o enquadramento da sociedade brasileira como uma efetiva sociedade da informação.

2.2 CONFLITOS DE INTERESSE NO MUNDO VIRTUAL

O estudo do Comitê Gestor procurou também identificar problemas relacionados ao uso de tecnologias da informação e das comunicações, mapeado os problemas de segurança percebidos nos meses antecedentes à pesquisa em assuntos como ataques de vírus, fraudes financeiras e uso indevido de informações pessoais (CGI.BR, 2009, p. 148).

Na Figura 7, as colunas “Total Brasil” mostram que em 2009 cerca de 35% dos usuários da internet declaram ter encontrado problemas de segurança durante o uso da internet, contra 28% em 2008, portanto um crescimento de 7 pontos percentuais em apenas um ano (CGI.BR, 2009, p. 150).

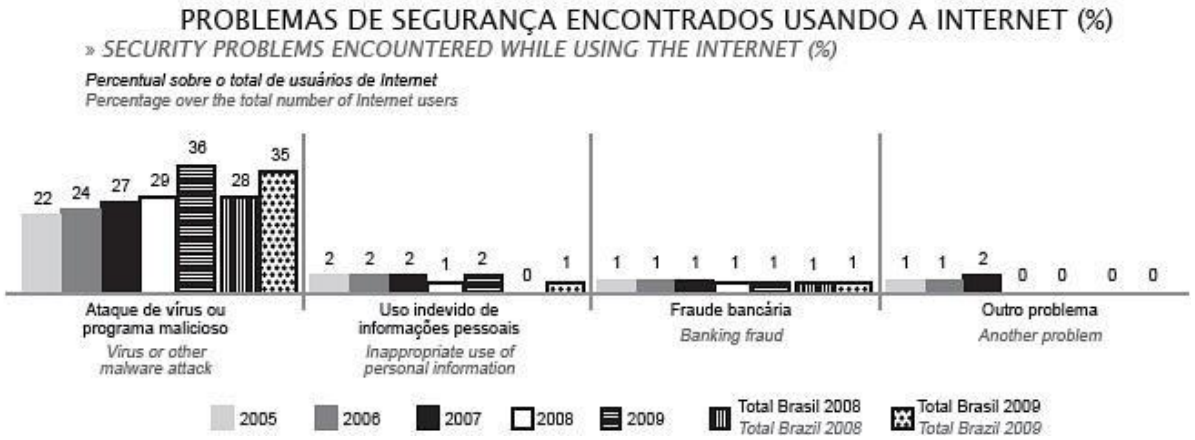

Figura 7. Problemas de segurança das pessoas no uso da Internet

Esses indicadores sobre segurança mostram-se ainda mais graves se considerados dados do Comitê Gestor que indicam ter ocorrido uma redução de dois pontos percentuais na quantidade de empresas que já adotavam políticas de segurança ou de uso aceitável das tecnologias de informação e das comunicações, portanto são empresas que deixaram de adotá-las. Em termos gerais resulta que mais da metade das empresas não utiliza qualquer dessas políticas. (CGI.BR, 2009, p. 212).

Ainda em contradição com o aumento das ocorrências, o levantamento detectou que o uso de tecnologias de proteção de dados apresentou estabilidade. Cerca de 84% das empresas fazem backup interno e 28% backup externo. A criptografia foi utilizada por aproximadamente 24% das empresas em desktops e 17% em dispositivos móveis. Cerca de 75% utilizam senhas, 38% utilizam certificados digitais e 19% utilizam *tokens* ou smartcards (CGI.BR, 2009, p. 212).

Nas relações com o governo, o quadro não é melhor. Ao averiguar o uso de recursos do governo eletrônico entre pessoas que utilizam a internet, o estudo detectou a existência de problemas como preocupação com proteção dos dados (15%) e deficiências de usabilidade (12%), fatores que segundo o estudo levaram 56% dos internautas a preferir fazer consultas e contatos pessoalmente em vez de confiar na via eletrônica (CGI.BR, 2009, p. 159).

Quanto ao comércio eletrônico, 26% dos internautas alegam preocupação com segurança ou privacidade e cerca de 22% afirmam não confiar no produto pretendido. Apenas 7% dos internautas realizam transações online através de Internet Banking (CGI.BR, 2009, p. 161).

No âmbito trabalhista, a pesquisa revela que em 2008 cerca de 66% das empresas brasileiras adotavam medidas que restringiam o acesso dos empregados a determinadas páginas da Internet. As principais restrições registradas são 62% a sites pornográficos, 48% a sites de relacionamento e 30% a e-mails pessoais, indicando a existência de zonas de conflito entre empregados e empregadores (CGI.BR, 2009, p. 207).

A Figura 8 mostra que em 2009, 63% das empresas declararam terem tido problemas com vírus, um aumento de 8 pontos percentuais em relação a 2008, e cerca de 53% das empresas relataram problemas com cavalos de tróia (*trojans*), um aumento de 5 pontos desde 2008 (CGI.BR, 2009, p. 363).

PROBLEMAS DE SEGURANÇA IDENTIFICADOS
IT SECURITY PROBLEMS IDENTIFIED
Percentual sobre o total de empresas com acesso à Internet[1]
Percentage over the total number of enterprises that have Internet access[1]

Percentual (%) *Percentage (%)*	Vírus *Virus*	Cavalos de Tróia (*Trojans*) *Trojans*	*Worms* ou *Bots* *Worms or Bots*	Acesso interno não autorizado *Unauthorized internal access*	Acesso externo não autorizado *Unauthorized external access*	Fraude facilitada pelas tecnologias de informação e comunicação (como furto de identidade, *phishing* etc.) *Fraud facilitated by ICTs (such as ID stealing, phishing etc.)*
TOTAL	63	53	21	9	9	6

PROBLEMAS DE SEGURANÇA IDENTIFICADOS – Continuação
IT SECURITY PROBLEMS IDENTIFIED – Continuation
Percentual sobre o total de empresas com acesso à Internet[1]
Percentage over the total number of enterprises that have Internet access[1]

Percentual (%) *Percentage (%)*	Furto de *notebooks*, PDAs ou outros dispositivos móveis *Stealing of notebooks, PDAs or other mobile devices*	Ataque de negação de serviço (DoS) *Denial of service attack (DoS)*	Ataque ao servidor *Web*/ Desfiguração *Attack to the Web server/ disfiguration*	Declarou não ter identificado problemas de segurança *Did not identify security problems*	Não sabe/ Não respondeu *Does not know/ Did not answer*
TOTAL	6	5	5	26	1

Figura 8. Problemas de segurança nas empresas

Os dados analisados mostram está havendo forte aumento na adoção de sistemas eletrônicos digitais pela população mundial e brasileira. Os levantamentos mostram também que, em correspondência a esse crescimento no uso, aumenta também a quantidade de problemas envolvendo esses dispositivos, como atos indevidos ou ilícitos e deficiências no serviço.

2.3 TUTELA DO ESTADO E O PAPEL DAS PROVAS NO CONVENCIMENTO JUDICIAL

O Estado é a organização funcional do poder político que tem a finalidade de promover o bem comum da população por meio de três funções principais (LEAL, p. 2):

- executiva, que consiste nos atos do governo e atos de administração;
- legislativa, por meio da elaboração de normas do ordenamento jurídico;
- jurisdicional, por meio da qual o Estado substitui a atuação privada na solução de conflitos de interesse com a finalidade de manter a paz social.

No âmbito da função jurisdicional, cabe ao Estado solucionar conflitos por meio de uma relação jurídica triangular na qual as partes lhe submetem suas razões e o conhecimento dos fatos sobre os quais se aplicará a norma jurídica. O sujeito que é titular do direito leva o ponto litigioso ao processo, requerendo ao Estado a tutela jurisdicional (GERALDO).

Na primeira instância, cabe ao juiz conduzir o processo e julgar a causa ao convencer-se sobre o verdadeiro autor e sobre os fatos verdadeiramente praticados, porém a identificação dessas verdades nunca foi uma tarefa simples. Havendo qualquer dúvida sobre a verdade, a sociedade não pode correr o risco de punir um inocente, pode punir apenas o verdadeiro culpado (MALATESTA, p. 16):

> E na verdade, se a sociedade ofendida tem o direito de punir o réu, não tem, contudo, o direito de ver sacrificar no seu altar uma vítima, seja ela qual for, culpada ou inocente; não: o direito da sociedade só se afirma racionalmente como direito de punir o verdadeiro réu; e para o espírito humano só é verdadeiro o que é certo.

O movimento histórico enalteceu progressivamente o papel das provas no convencimento do julgador como forma para fortalecer a averiguação da verdade e do que é certo. O regime das “provas legais” fixou na lei condições rigorosas sobre como deveriam ser avaliadas as provas, com isso reduziram-se os debates judiciais para apreciação dessas provas, mas limitou-se a liberdade do juiz ao decidir.

O Brasil não adota o regime de provas legais, mas sim o princípio da persuasão racional do juiz e da livre motivação das decisões judiciais. O magistrado não está

obrigado a seguir critérios inflexíveis, mas também não tem liberdade absoluta (CINTRA; DINAMARCO; GRINOVER, p. 68).

Nesse modelo, a eficácia da prova será tanto maior, quanto mais clara, ampla e firmemente fizer surgir no espírito do juiz a crença de posse da verdade. Como a certeza do juiz é um estado subjetivo do espírito, que pode não corresponder à verdade objetiva, a busca da verdade judicial objetiva deve sempre valer-se do raciocínio, da reflexão intelectual (MALATESTA, p. 27):

> É sempre a reflexão intelectual que nos conduz do conhecido ao desconhecido; e aí nos conduz por meio do raciocínio. O raciocínio, instrumento universal da reflexão, é a primeira e mais importante fonte da certeza em matéria criminal.

A verdadeira certeza quanto à prova resulta da combinação entre a certeza física e a certeza lógica, a primeira provém da verdade natural e sensível percebida pelos sentidos e a segunda resulta de um trabalho marcantemente intelectual.

Se o convencimento judicial resultou tanto do natural quanto do racional, entendem os autores estudados que as mesmas provas deveriam produzir em qualquer outra pessoa racional uma convicção similar àquela que produziram no juiz.

Daí a possibilidade da sociedade fiscalizar o convencimento judicial e seu reflexo na sentença. Cabe ao magistrado declarar as razões do seu convencimento e à sociedade fiscalizar essa convicção (MALATESTA, p. 66):

> Este princípio da sociabilidade do convencimento judicial, ainda não exposto anteriormente, que eu saiba, por pessoa alguma, é da maior importância... nesta sociabilidade, que é uma espécie de objetivação da certeza, está a melhor determinação do convencimento judicial, determinação que impede que ele se resolva, mais ou menos hipocritamente, em um arbítrio do juiz.

Para que a fiscalização da sociedade seja possível, o convencimento judicial deve ter uma concretização exterior, ou seja, deve ser dada publicidade tanto sobre o que resultou da percepção dos sentidos quanto aos elementos naturais, assim como sobre os debates racionais que avaliaram as provas e originaram a sentença, possibilitando sua fiscalização e aprovação ou reprovação social.

Com o princípio da persuasão racional, o juiz não está atrelado a critérios legais específicos que limitem e conduzam a apreciação das provas, mas também seu livre convencimento não pode estar desvinculado das provas e dos elementos existentes

nos autos, devendo decidir com base nos elementos existentes no processo, avaliados segundo critérios críticos e racionais (CINTRA; DINAMARCO; GRINOVER, p. 68).

Portanto, o juiz não precisa estar adstrito à prova pericial, mas deve ser dada publicidade à produção dessa prova e ao papel que essa prova teve na formação do convencimento judicial, possibilitando à sociedade exercer seu poder de fiscalização.

No contexto da presente dissertação é relevante entender como esses fortes princípios sobre as provas e a busca socializada da verdade em mundo físico, facilmente detectado pelos sentidos e tido há muitos séculos como familiar às pessoas, tornam-se ainda mais importantes em um mundo virtual ainda pouco conhecido, altamente volátil, com tênues limites geográficos e onde tudo se transforma e inova rapidamente.

2.4 PRODUÇÃO DE PROVAS DIGITAIS

Nesta dissertação foram vistos indicadores sobre como a sociedade moderna depende cada vez mais das tecnologias da informação e das comunicações embutidas em computadores, celulares e demais dispositivos digitais. Viu-se, ainda, que crescem proporcionalmente os conflitos de interesses que envolvem direta ou indiretamente sistemas eletrônicos digitais, conflitos esses que, quando mais graves, devem ser resolvidos pelo Estado.

Foi também estudada a importância das provas digitais no convencimento do juiz, pois em uma sociedade eletrônica elas passam a ter progressivamente mais importância para que o juiz conheça a verdade dos fatos e seus autores.

Como a avaliação das provas baseia-se na observação natural e também na certeza lógica, raciocinada, caberá ao juiz inteirar-se cada vez mais sobre as novas tecnologias e sobre os fatos voláteis que ocorrem no mundo virtual. Além disso, cabe ao magistrado coordenar ou deferir as ações pelas quais as provas digitais são produzidas.

A identificação, coleta e exame das evidências digitais são tarefas usualmente atribuídas aos peritos oficiais[2] ou por peritos judiciais[3] e realizadas sob a condução do Poder Judiciário. O trabalho pericial começa em vistorias na cena do crime ou com procura por evidências durante "buscas e apreensões" acompanhadas por oficiais de justiça e autoridades policiais quando for o caso.

Raramente os exames periciais são concluídos no próprio local da diligência pericial, devido à grande quantidade de dados armazenados e processados nos modernos dispositivos digitais. Outro fator agravante é a necessidade de interpretar grupos específicos de dados conforme formatos particulares adotados por cada programa processado em um computador investigado, o que demanda diversas bases de conhecimento, métodos e ferramentas de exame.

Ao final da vistoria seria necessário apreender os equipamentos, tanto para preservar as evidências neles armazenadas, assim como para que possam ser examinados em laboratórios periciais dotados dos recursos adequados.

A apreensão dos equipamentos traz graves prejuízos aos réus porque os impede de prosseguir nas suas atividades normais, pois pessoas e empresas são cada vez mais dependentes dos computadores e das comunicações. Retira-lhes a posse do material prejudica seus proprietários também quando à sua análise para eventual contraprova.

Por isso, a alternativa mais empregada atualmente é a apreensão não dos próprios equipamentos, mas apenas de cópias forenses[4] dos seus dados, deixando-se os

---

[2] Peritos oficiais são funcionários públicos admitidos como peritos na Polícia Federal ou nas Polícias Estaduais, geralmente subordinados à Polícia Científica e atuando em Institutos de Criminalística. Atuam em processos criminais.

[3] Peritos judiciais são profissionais de nível superior nomeados pelo Magistrado em função do seu saber na área e por serem de sua confiança. Atuam tipicamente em processos cíveis ou trabalhistas.

[4] Cópias forenses são idênticas aos originais e essa igualdade pode ser verificada (certificada) a qualquer momento por meio de mecanismos como o cálculo do código *hash*, O código *hash* é um código alfanumérico curto, com dezenas de caracteres, gerado por algum método matemático que mapeia todos os bits armazenados em um dispositivo digital, tendo esse método propriedades como: (i) ser unidirecional, isto é, impossibilitar a descoberta da informação original a partir do código; (ii) assegurar que se um único bit do dispositivo original for alterado, o código *hash* será diferente e (iii) se dois dispositivos digitais apresentarem o mesmo código *hash*, fica demonstrado que seus conteúdos originais também são iguais. Se o método for inadequado, pode ocorrer que dois dispositivos com conteúdo ligeiramente diferente, ou alterado, apresentem o mesmo código *hash*, defeito chamado colisão (GUELFI, 2007, p. 96).

equipamentos e dados originais para que os investigados possam continuar normalmente suas atividades, desde que não haja flagrante prática de ilícito.

Assim, concluída a busca, as cópias forenses são apreendidas e transportadas até um Instituto de Criminalística ou laboratório particular de um perito judicial.

São escassas e incompletas as informações governamentais sobre a quantidade de equipamentos apreendidos e periciados. Buscas informais realizadas na internet indicam haver aumento relevante na quantidade de trabalhos periciais e aumento nos problemas relacionados à sua execução, como baixa qualidade dos trabalhos e demora excessiva na conclusão das perícias.

Em artigo informal intitulado “Sobre as buscas e apreensões determinadas em locais de residência e trabalho”, José Carlos Fragoso afirma (FRAGOSO, p. 1):

> Têm sido frequentes as determinações judiciais de buscas a apreensões a serem realizadas, na fase de inquérito policial, nos locais de residência e de trabalho de cidadãos indiciados.

Apresentação informal divulgada na internet por empresa que comercializa software forense no país informa que os institutos estaduais de criminalística são mal aparelhados e seus peritos não tem acesso a treinamento adequado (THIBAU, 2007, p. 7):

- ✓ Institutos de Criminalística estaduais mal aparelhados
- ✓ Peritos sem acesso a treinamentos de atualização, participação em congressos de mercado e internacionais.
- ✓ Ausência de um projeto nacional, com troca de experiências, melhores práticas e resultados integrando as forças estaduais.
- ✓ Desconexão entre equipes de laboratório, investigação e logística de campo.
- ✓ Limitação à investigação de Crimes Eletrônicos

Em 15 de agosto de 2010, o portal do jornal O Estado de São Paulo publicou artigo informal intitulado “*Perícia criminal no País é extremamente precária*” que divulga levantamento feito em todo o país a respeito da perícia criminal, chegando à conclusão que sua situação é, salvo raríssimas exceções, “*tão precária que beira a indigência*”. Informa que existem pouco mais de 12 mil peritos para atender 32 especialidades de perícia criminal, índice muito inferior ao mínimo necessário. O levantamento indica que dentre os estados brasileiros apenas quatro (BA, DF, RS,

SP) tem equipamentos considerados essenciais para a perícia criminal (AGÊNCIA ESTADO, 2010).

Verificação informal realizada no mecanismo de busca Google, em julho de 2010, trouxe exemplos de links com chamadas para notícias sobre buscas e apreensões de computadores ocorridas em todo o país, algumas delas mostradas parcialmente a seguir, ocultados propositalmente os dados sobre os envolvidos e as URLs:

> [...] a operação realizada pela Polícia Civil apreendeu 2.339 computadores [...]
>
> [...] o Gaeco (Grupo de Atuação Especial de Repressão ao Crime Organizado) devolveu os sete computadores apreendidos do Jornal [...]
>
> [...] depois de mais de 5 meses, os advogados [...] finalmente tiveram seus computadores devolvidos pela Polícia Federal [...]
>
> [...] peritos do Grupo de Atuação Especial Contra o Crime Organizado (Gaeco) realizam [...] a perícia nos computadores apreendidos em residências de pessoas envolvidas, direta ou indiretamente, no concurso [...]
>
> [...] computadores apreendidos na operação [...] já começaram a ser devolvidos a seus respectivos donos. O juiz deu prazo até esta quarta-feira para que equipamentos pertencentes à Câmara e de alguns vereadores fossem restituídos [...]
>
> [...] foram apreendidos documentos da secretaria de Estado [...] e computadores da Secretaria de [...] devido às investigações que apuram o superfaturamento na compra [...]
>
> [...] policiais federais participam da operação [...] para desmantelar quadrilha que corrompia menores [...] foram apreendidos dois computadores [...]
>
> [...] a polícia confirmou que os dois computadores apreendidos serão periciados mesmo em Penápolis e não mais em São Paulo [...]
>
> [...] a Polícia Federal informou que os 6 computadores que foram apreendidos do Sindicato [...] durante uma operação da PF na última quinta-feira, foram devolvidos. A ordem partiu do Juíz [...], o mesmo que assinou o pedido de busca e apreensão para que a operação acontecesse [...]
>
> [...] quinze computadores foram apreendidos hoje em 11 endereços de suspeitos de prática de pedofilia na internet, por ordem de promotores [...]
>
> [...] mentiras do Sr. Delegado [...] disse primeiro de que os micros pegos no caso estavam cheios [...] depois disse que não dava para acessá-los [...]
>
> [...] após a operação [...] para prender policiais, delegados, advogados e outras pessoas [...] uma equipe do setor de inteligência irá [...] periciar os equipamentos de informática apreendidos [...]

> [...] a polícia investiga empresas de venda pela internet [...]
>
> [...] pessoas foram presas e computadores apreendidos na sede [...] por meio da operação realizada pela Polícia Civil em parceria com o Ministério Público [...] acusadas de participarem da organização criminosa comandada pelo empresário [...]
>
> [...] retornando à sede da Polícia Civil, com quilos de documentos e computadores apreendidos em imóveis e empresas de uma quadrilha suspeita de fraudar licitações [...]

São raros documentos oficiais com dados quantitativos ou qualitativos sobre perícias e praticamente inexistentes informações específicas sobre perícias em tecnologias da informação e telecomunicações. Alguns documentos trazem registros genéricos e indiretos sobre o assunto. Em Acórdão do Conselho Superior da Justiça do Trabalho[5], referente à criação do cargo de perito nas áreas de medicina do trabalho, engenharia e contabilidade, o conselheiro Dr. João Orestes Dalazen registra:

> Comprovadamente, portanto, o número absoluto de perícias realizadas nas Varas do Trabalho vem aumentando no decorrer dos anos...no ensejo das correições ordinárias, pude, pessoalmente, inferir da análise de processos, por amostragem, delongas causadas exclusivamente pela falta de peritos habilitados na forma exigida pelo art. 195, da CLT.

Em artigo informal disponível no site da Associação Brasileira de Criminalística[6], o perito Carlos Kleber da Silva Garcia, presidente da associação em Goiás, relata (GARCIA, 2009):

> A situação da Polícia Científica hoje é dramática e caminha para o colapso total de suas atividades. As seções internas do Instituto de Criminalística estão abarrotadas de materiais para serem periciados e estima-se que seriam necessários cinco anos para concluir todas as perícias já solicitadas.
> A quantidade de peritos nas seções internas do Instituto de Criminalística está muito aquém do mínimo necessário. Seções com grande demanda de perícias como as Seções de Balística, Informática, Documentoscopia e Meio Ambiente trabalham com apenas dois ou três peritos para atender todas as ocorrências do Estado...
> A chegada de mais 112 novos delegados prevista no concurso em andamento da Polícia Civil vai sobrecarregar ainda mais o trabalho pericial, com o aumento das investigações e das requisições de perícia. A Polícia Científica está se tornando o gargalo do sistema investigativo-judicial, onde as demandas por perícias não estão

[5] Acórdão do Tribunal Superior do Trabalho, processo número TST-CSJT-360/2007-000-90-.005, de 21 de agosto de 2007.

[6] Disponível em: <http://www.abcperitosoficiais.org.br/ver.asp?id=506>. Acesso em: 30 jul. 2010.

> sendo atendidas em tempo hábil por falta de pessoal, levando morosidade ao sistema e causando prejuízos à população.

Em notícia publicada em 2006 no jornal Folha de São Paulo[7] com o título “Efeito CSI multiplica interesse pela profissão de perito criminal”, as jornalistas Andrea Murta e Marina Tamari registram:

> Em todo o Estado de São Paulo, os 910 peritos ativos tiveram que se desdobrar para cuidar, entre janeiro e abril de 2006, de 195.541 casos, uma média de 53 exames periciais por mês para cada profissional...
> Um estudo realizado por peritos do Instituto de Criminalística do Distrito Federal em todo o país mostra que, para dar conta da demanda em São Paulo, seria preciso um acréscimo de pelo menos 6.400 profissionais no Estado.

O site “NoMinuto”[8] publicou em de 28/07/2009 notícia intitulada “Deficiência em perícias técnicas compromete inquéritos policiais”, onde o autor Fred Carvalho registra:

> O Instituto Técnico-Científico de Polícia (Itep) deixou de concluir quase mil perícias no ano passado. A quantidade de procedimentos não concluídos chamou atenção da Corregedoria Geral da Secretaria de Segurança Pública e Defesa Social (Sesed), que no começo do mês instaurou 15 processos administrativos disciplinares para apurar o que classificou como "desídia" - atitudes negligentes ou atos imprudentes do empregado que causam prejuízo ao serviço.
> Segundo levantamento feito pela direção do Itep e encaminhado à Corregedoria, 15 peritos criminais deixaram de concluir 938 perícias de um total de 1.072 que foram designadas a eles, o que representa quase 90% do montante...
> “É um número muito pequeno [de peritos] para a quantidade de perícias que temos que fazer todos os dias. Vale lembrar que essas perícias são peças científicas muito importantes, que devem ser elaboradas com o maior cuidado possível. Em alguns casos, uma perícia mal feita pode incriminar um inocente ou inocentar um culpado por um crime”, ressaltou.
> Além da falta de pessoal, o presidente da Associação dos Peritos questionou também a estrutura do Itep. “Foram adquiridos alguns equipamentos novos, mas isso ainda é muito pouco quando comparado à nossa demanda. O Itep carece de mais equipamentos e que eles sejam de ponta. Os que temos, na maioria dos casos, já estão sucateados”.

---

[7] Disponível em: <http://www1.folha.uol.com.br/folha/treinamento/novoemfolha41/te21062006042.shtml>. Acesso em: 30 jul. 2010.

[8] Disponível em: <http://www.nominuto.com/nasemana/conteudo-do-jornal/deficiencia-em-pericias-tecnicas-compromete-inqueritos-policiais/35540/print/>. Acesso em: 17 ago. 2010.

Essas notícias e informações indicam que a adoção em grande escala de novas tecnologias na sociedade moderna agravará o cenário que já mostra demora no atendimento e baixa qualidade dos exames periciais em dispositivos eletrônicos digitais.

2.5 SÍNTESE DO CAPÍTULO

Neste capítulo foram analisados indicadores sobre a utilização brasileira e mundial das tecnologias da informação e das comunicações, constatando-se a existência de uma forte expansão que traz como consequência o aumento na quantidade de conflitos de interesse e disputas judiciais que envolvem, direta ou indiretamente, dispositivos eletrônicos digitais.

Essa nova realidade está impondo aos juízes a necessidade de familiarizar-se com os dispositivos baseados em alta tecnologia, de reavaliar continuamente os procedimentos utilizados para a produção de provas no mundo digital e, ainda mais importante, manter-se a par do extenso e dinâmico leque de produtos e serviços típicos da sociedade digital.

Com isso, o juiz estará em condições de compreender e, portanto, sensibilizar-se a respeito dos elementos formadores da sua convicção pessoal e que embasarão suas decisões nos processos judiciais que preside. Porém, como vimos apenas isso não basta para assegurar decisões corretas.

Cabe ao juiz estar preparado para racionar a respeito dos fatos do mundo virtual, para isso a melhor abordagem é aprimorar seu conhecimento sobre sistemas, os mesmos princípios e métodos que suportam seus estudos sobre os sistemas legais aplicam-se igualmente ao estudo de sistemas tecnológicos.

Em outras palavras, a motivação judicial não pode restringir-se à avaliação sistêmica dos fatos digitais, mas dela não se pode prescindir em tribunais que decidem conflitos na sociedade digital.

Esse contexto pressiona ainda mais os peritos oficiais ou judiciais não apenas pelo aumento da demanda de exames, mas também em função do aumento de complexidade tecnológica, requerendo melhores conhecimentos técnicos e ferramentas sofisticadas de análise pericial que devem produzir laudos plenamente

fundamentados, que embasem o exercício do contraditório e, por fim, a motivação judicial.

Contudo, este capítulo mostrou cenários bastante distantes das metas e responsabilidade atribuídas aos peritos. Viu-se que os laboratórios periciais estão sobrecarregados, impondo prazos incompatíveis com a velocidade dos acontecimentos em uma sociedade digital e, portanto, dos anseios da sociedade frente ao Poder Judiciário.

Constatou-se forte desaparelhamento, falta de recursos humanos, ausência de competência e até mesmo falta de infraestrutura básica nos institutos de criminalística, especialmente nos estados e municípios mais distantes dos principais centros acadêmicos e empresariais.

Com isso, há aumento no risco de que os operadores do Direito sejam levados a decisões erradas por omissões ou erros nos trabalhos periciais, pois as principais decisões não mais ocorrem no mundo físico que nos é familiar há milhares de anos e cujos princípios herdamos pelo menos nos arquétipos; ao contrário, tais decisões são tomadas em um mundo virtual novo para todos nós, ainda muito pouco conhecido por vítimas, réus e por quem deve decidir os conflitos.

3 LABORATÓRIOS FORENSES

Este capítulo descreve os principais centros nacionais voltados à elaboração de perícias técnicas e, em seguida, classifica o ambiente onde são realizados os trabalhos periciais quanto à presença das pessoas envolvidas e quanto às possibilidades de virtualização dos exames periciais.

3.1 LABORATÓRIOS ESTATAIS OU PRIVADOS

Nos processos criminais, os exames técnicos são realizados essencialmente por peritos federais ou estaduais. O Instituto Nacional de Criminalística, do Departamento de Polícia Federal, produziu nos últimos anos mais de 200 mil laudos nas diversas áreas de conhecimento, contando para isso com um quadro de aproximadamente mil peritos (SANTOS JR., 2009).

Na esfera estadual, praticamente todos os governos mantém Institutos de Criminalística subordinados à sua Polícia Científica. Reportagem publicada no jornal O Estado de São Paulo informou há cerca de 12 mil peritos para atender 32 especialidades de perícia criminal, o que indica uma média de 375 peritos por especialidade, índice que se mostra inferior ao mínimo necessário (AGÊNCIA ESTADO, 2010).

O governo empreende esforços que visam aparelhar as unidades periciais, especialmente por meio da Secretaria Nacional de Segurança Pública (Senasp), do Ministério de Justiça, que concentra os investimentos no setor e instituiu a Rede Nacional de Altos Estudos em Segurança Pública (Renaesp), um projeto de educação permanente voltado aos profissionais de segurança pública. O Ministério apoia também as atividades periciais dos Institutos de Criminalística editando padrões e manuais de procedimentos (MINISTÉRIO DA JUSTIÇA, 2009).

Peritos federais e estaduais são funcionários públicos subordinados às respectivas unidades policiais, fato criticado por alguns setores da sociedade que veem risco de ingerência política ou de outras naturezas. Entidades como a OAB chegaram a defender que os Institutos de Criminalística devem ser vinculados às Universidades e não mais às Secretarias de Segurança Pública, para que se possa assegurar sua independência e autonomia durante os trabalhos periciais e a observância dos

rigores científicos. Críticos dessa separação alegam que a perícia criminal inclui-se no conceito de Polícia Judiciária, não podendo dela se dissociar, devendo apenas haver autonomia de cargo e não de órgão (LEITÃO, 2008).

Os institutos periciais oficiais são alvo de severas críticas, ficando claro seu desaparelhamento, condições inadequadas de trabalho e consequente baixa qualidade técnica. Por outro lado, o país conta com alguns poucos centros periciais mundialmente reconhecidos pela competência de trabalhos realizados, como o Instituto Nacional de Criminalística do Departamento de Polícia Federal. Parte da demanda oficial é atendida por alguns centros de pesquisa ligados às universidades ou à iniciativa privada, geralmente de elevada qualidade técnica.

Nas esferas cíveis, do trabalho e da família, os peritos judiciais são pessoas físicas sem vínculo estável com o Estado. Geralmente são especialistas em suas respectivas áreas de atuação que atuam na esfera privada, nomeados *ad hoc* pelos Juízes nas diversas comarcas de todo o país.

O Brasil conta com mais de cinco mil municípios e aproximadamente 2.500 comarcas, o que indica que metade dos municípios possui acesso local aos serviços judiciários, enquanto que o restante precisa recorrer aos serviços prestados em algum município próximo ou por Juízes itinerantes (IBGE, 2008). Com base nesses números, estima-se que existem pelo menos dois peritos judiciais nas comarcas menores e centenas deles nas maiores, indicando a ordem de grandeza de pelo menos 6.000 peritos judiciais ativos no país.

Verificações informais feitas durante o desenvolvimento deste trabalho e entrevistas publicadas na imprensa indicam que, por serem profissionais liberais ou funcionários da iniciativa privada, os peritos judiciais raramente têm dedicação exclusiva à atividade pericial. Menos frequentemente ainda possuem laboratórios dotados dos equipamentos e softwares cada vez mais necessários para realizar exames periciais confiáveis. Como programas forenses são dispendiosos e são raros programas gratuitos eficientes, resulta naturalmente que muitos trabalhos sejam feitos sem esses softwares ou utilizem programas contrafeitos, enfraquecendo todo o sistema.

Em síntese, os estudos realizados indicam que:

a) Há baixa disponibilidade de software e equipamento forense compatível com a grande diversidade de novas tecnologias da informação e das

comunicações empregadas em mais recentes computadores, celulares e dispositivos embarcados;

b) A grande velocidade com que são adotadas novas tecnologias aumenta a distância entre elas e os laboratórios existentes, devido ao baixo investimento existente para sua modernização;
c) A demora e o custo para certificação de novos produtos forenses junto aos órgãos acreditadores mundiais e nacionais aumentam o descompasso entre o lançamento de novos dispositivos digitais e a disponibilidade de software forense adequado para sua análise;
d) Verificações informais mostram que não há oferta de software livre forense em quantidade e qualidade compatíveis com o lançamento de novos dispositivos digitais;
e) Verificações informais indicam que os operadores do direito, autoridades policiais, peritos e as próprias partes em processos judiciais manifestam-se rotineiramente sobre as deficiências dos laboratórios periciais, alertando para falta de recursos, erros no trabalho pericial, demora excessiva, baixa qualidade técnica dos peritos e demais problemas dessa natureza.

Como se viu nos demais capítulos desta dissertação, os laboratórios que atuam em outras áreas científicas são alvos de críticas similares àquelas percebidas quanto aos laboratórios das tecnologias da informação e da comunicação. Paradoxalmente, em quase todas essas áreas, como Medicina, Biologia, Química, Engenharia Elétrica e Física, é notória a existência de laboratórios altamente especializados que apresentam elevada produção científica como demonstram os indicadores nacionais em ciência e tecnologia.

Portanto, constata-se que nessas áreas não se pode entender que inexistam laboratórios, mas sim que exista distanciamento ou mesmo falta de acesso a partir dos mais de cinco mil municípios brasileiros. Isso indica que há necessidade de proporcionar a peritos e especialistas que atuam junto a comarcas distantes o acesso aos equipamentos e conhecimentos disponíveis para os pesquisadores situados nos grandes centros, onde geralmente se situam as principais universidades e centros de pesquisas.

O problema que se põe é a distância física entre os laboratórios disponíveis e o local onde ocorrem os fatos, ou seja, a separação entre os laboratórios e a comarca onde

estão situados o tribunal, o perito de confiança do juiz, as partes do processo e as peças a serem examinadas. Trata-se, portanto, de apontar ou adotar alternativas que propiciem acesso e interação remota.

3.2 LABORATÓRIOS QUANTO AO ACESSO E VIRTUALIZAÇÃO

Laboratórios são locais providos de recursos materiais e humanos para realizar análises, experiências, pesquisas, aplicações práticas e ensino dos conhecimentos científicos. Desde a idade média, laboratórios são tipicamente organizados como salas frequentadas por pesquisadores e estudantes, dotadas de equipamentos e materiais destinadas ao estudo e à manipulação de espécimes.

Apenas recentemente, as tecnologias da informação e das telecomunicações começaram a mudar o formato tradicional dos laboratórios. Casini; Prattichizzo e Vicino (2003, p. 252) classificam esses novos laboratórios como virtuais ou remotos, o que leva a adotar para este trabalho um modelo similar, representado pelo *grid* mostrado na Figura 9 para avaliar os laboratórios dentro de um enfoque pericial:

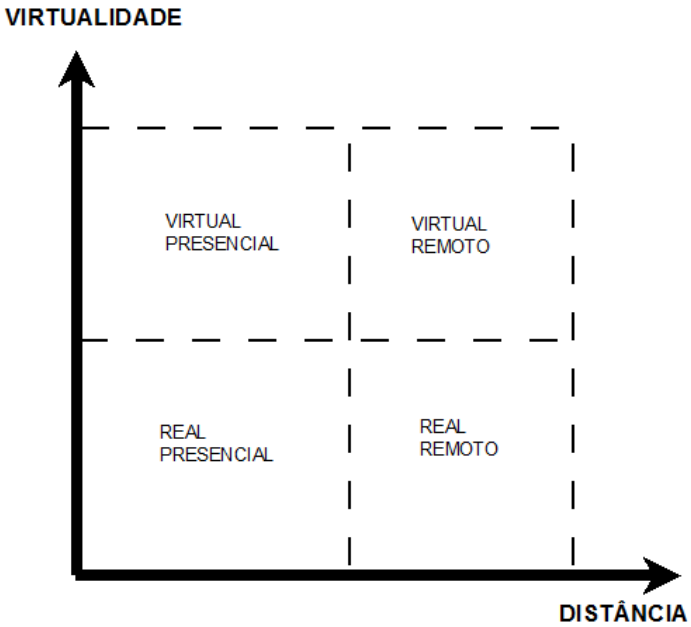

Figura 9. Virtualidade *versus* distância dos laboratórios

Laboratórios virtuais são laboratórios onde equipamentos, materiais e condições reais são substituídos por sistemas informáticos que os simulam, isto é, um laboratório virtual simula um modelo de um processo físico. Portanto, nos laboratórios virtuais não há manuseio de componentes físicos, apenas componentes

e ambientes modelados matematicamente por programas de computador. Por não terem estrutura física, laboratórios virtuais podem facilmente ser utilizados a distância por uma ou mais pessoas simultaneamente, independentemente da sua localização.

Laboratórios remotos são laboratórios com equipamentos, materiais, espécimes e interações reais, mas que podem ser acessados e manipulados remotamente, através de redes de computadores (FERREIRA, 2007, p. 16).

Uma evolução importante nos laboratórios remotos veio da possibilidade de acessá-los através da Web, a partir de qualquer local do mundo, de modo compartilhado e mediante o uso de navegadores comuns (browsers Internet). Essa estrutura vem sendo denominada na literatura científica como WebLab.

A grande complexidade das questões relacionadas a Weblabs, por um lado, e dos procedimentos para exame forense de dispositivos digitais, por outro lado, faz com que o presente estudo tenha que ser limitado, conforme exposto em seus objetivos.

Por isso, será adotado um modelo simplificado baseado apenas em um disco rígido de computador pessoal, deixando-se para trabalhos futuros analisar a grade diversidade de sistemas eletrônicos digitais que um laboratório dessa natureza deverá examinar. Assim sendo, a presente análise considera apenas exame de um disco rígido frente a um hipotético processo judicial com a presença de operadores do direito e das partes.

3.3 LABORATÓRIO PRESENCIAL E REAL

Esse é o cenário mais comum e frequentemente recomendado pelas atuais práticas forenses.

O computador é apreendido pela autoridade e depois conduzido diretamente a um instituto de criminalística ou laboratório forense do perito judicial. Nesse local, o disco rígido é removido do interior do equipamento e conectado a um computador

forense. Um dispositivo de bloqueio (hard block) deve proteger o disco contra gravações, para evitar contaminação da evidência durante seu exame[9].

O disco é examinado pelos peritos e o resultado submetido ao juiz. Subsequentemente, o juiz dá ciência e requer manifestações das partes a respeito do laudo.

Como pode ser visto na Figura 10, nesse modelo o perito interage diretamente com o disco rígido, contudo as demais pessoas ficam completamente apartada dessa realidade, tendo apenas uma visão posterior e limitada dos fatos somente por meio do laudo pericial.

Em alguns procedimentos, principalmente naqueles da esfera cível, é comum que as partes indiquem assistentes técnicos, que figuram como representantes técnicos das partes e que podem ter uma interação um pouco mais intensa durante os exames.

Essa participação é normalmente limitada por questões de tempo e geográficas, o que reduz a possibilidade da presença física junto ao perito, pelo que muito raramente os assistentes técnicos acompanham integralmente os trabalhos periciais.

Quando o exame é realizado em laboratórios oficias, raramente existe atuação direta dos assistentes técnicos, menos ainda quanto à presença do juiz ou advogados das partes durante os atos periciais realizados no laboratório.

Dessa forma, trata-se de um cenário eminente presencial para os peritos e assistentes técnicos, mas isso somente ocorre em “reuniões”, sendo que durante todo o tempo o perito trabalha praticamente sozinho no caso. Por isso mesmo, praticamente inexiste qualquer fiscalização desses operadores do Direito e da sociedade.

[9] Além do *hard block*, as melhores práticas recomendam que, em vez de ser examinado diretamente, o disco original seja copiado, produzindo um disco clone fiel que será utilizado nos exames enquanto que o disco original permanece preservado em local seguro. Porém, muitas vezes essas recomendações não são seguidas por custo dos equipamentos ou porque demandam tempo de cópia e espaço de armazenamento.

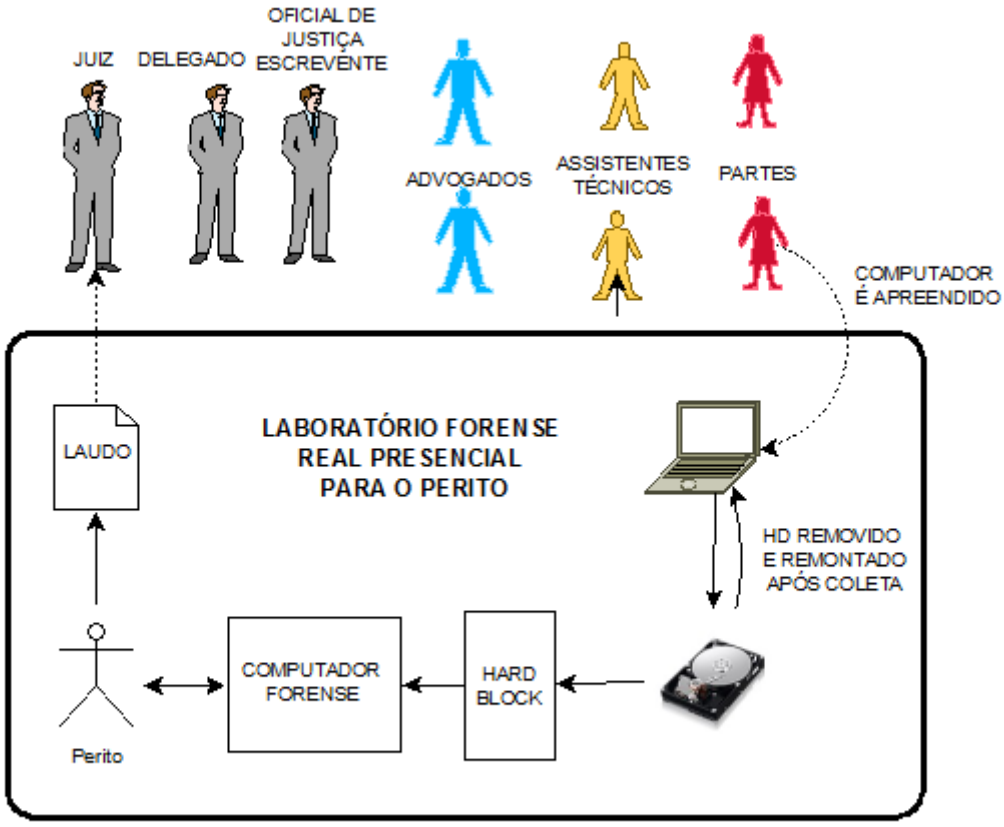

Figura 10. Laboratório presencial e real

3.4 LABORATÓRIO PRESENCIAL COM VIRTUALIZAÇÃO PARCIAL

Uma das mais importantes evoluções nos procedimentos periciais forenses tem sido a substituição, durante os exames, do disco rígido real por uma cópia desse disco. O procedimento mais rudimentar consiste em gerar uma cópia forense bit a bit. Mais modernamente, em lugar da cópia forense gera-se uma imagem forense, isto é, um modelo que representa o disco original, em termos práticos esse modelo é denominado arquivo imagem forense.

O laboratório forense passa então a atuar como um laboratório virtual, pois em vez de examinar o sistema eletrônico digital original, analisa-se um modelo que o representa, contendo algum tipo de representação dos dados originais e metadados que qualificam o dispositivo de origem. Aumentam a transparência e a segurança dos procedimentos, pois há supervisão da autoridade, geração da cadeia de

custódia, certificação por código *hash*[10] e criação de cópias forenses da evidência. Como mostra a Figura 11, neste formato há duas fases distintas e segregadas entre si, a primeira no momento da busca e apreensão, ou vistoria, onde é coletado o material por meio de arquivo imagem, e a segunda fase onde esse clone é examinado pelo perito forense e preservado enquanto evidência.

Mesmo se há melhoras com relação ao formato anterior, o fato é que a maior parte dos operadores do direito tem poucas condições de fiscalizar ou mesmo contribuir com as tarefas periciais e as imagens forenses ainda são bastante incompletas pois são focadas apenas na coleta dos dados, sendo deficientes no controle da cadeia de custodia.

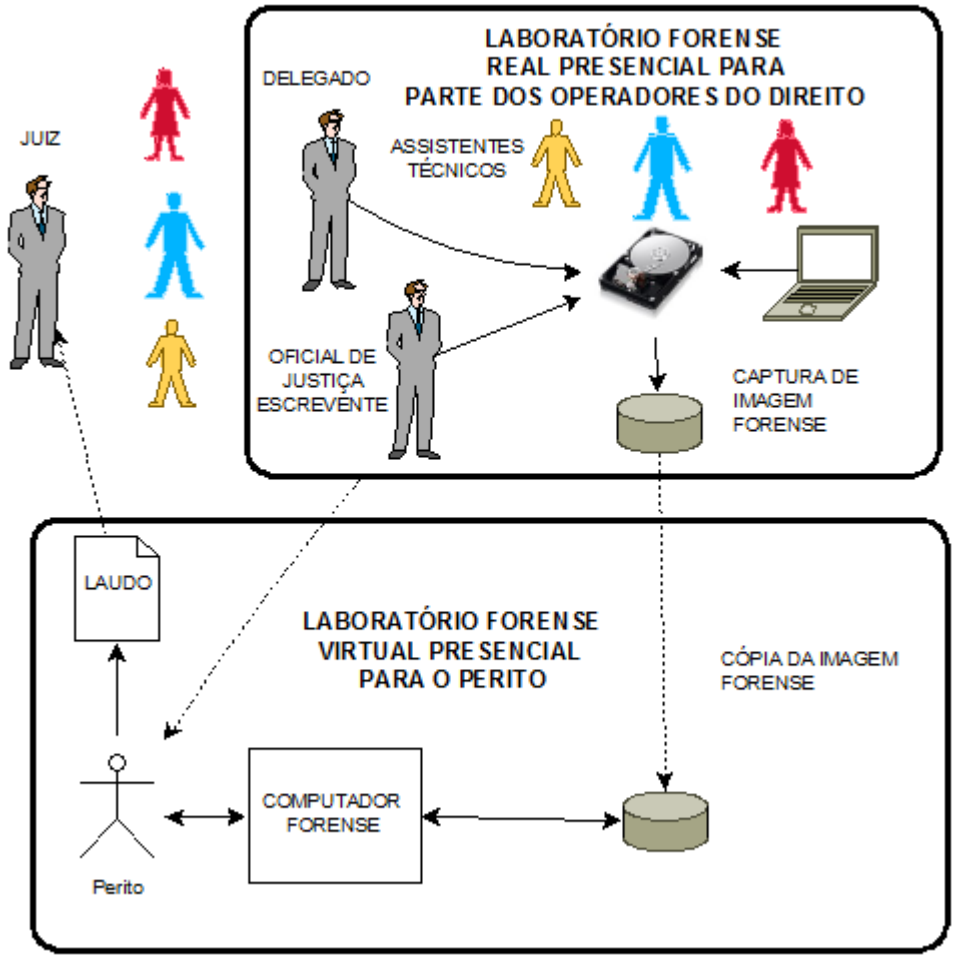

Figura 11. Laboratório presencial com virtualização parcial

[10] As melhores práticas determinam o cálculo do código *hash* como recurso para verificar a integridade de uma evidência digital, contudo esse código não possibilita a verificação do conteúdo para fins de contraprova.

3.5 LABORATÓRIO SEMIPRESENCIAL COM ACESSO REMOTO E VIRTUALIZAÇÃO

A Figura 12 mostra outro modelo, adotado mais recentemente, que consiste na coleta online e em tempo real desde uma estação remota, podendo a parte investigada estar ciente ou não dessa coleta. Nesse modelo, a parte autora e alguns operadores do direito podem acompanhar ou realizar a operação a partir de uma central de controle, portanto nela devem estar fisicamente presentes, mesmo se localizados remotamente em relação ao comutador investigado. A parte investigada pode estar presente junto ao computador examinado, assim como alguma autoridade.

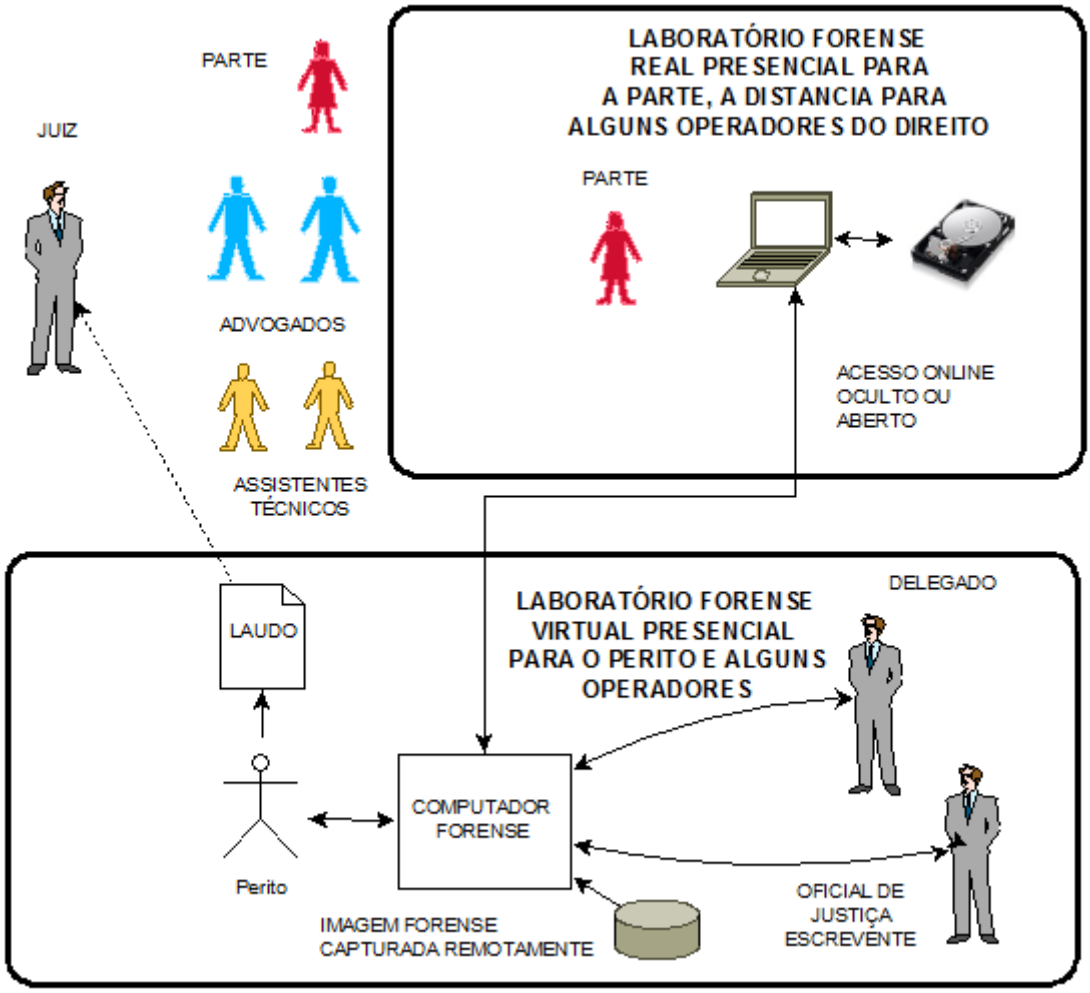

Figura 12. Laboratório semipresencial com acesso remoto e virtualização

Diversos procedimentos desse tipo foram sendo implementados paulatinamente por autoridades, peritos e fabricantes de softwares forenses. Um dos exemplos é o

EspiaMule, software adaptado pelo Departamento de Polícia Federal para buscar arquivos com material ilícito compartilhado em redes P2P. Ao constatar indícios sobre a presença de arquivo suspeito na rede, o EspiaMule solicita ao programa eMule do suspeito que envie cópia do arquivo, momento em que são capturados dados sobre a origem, suposto autor do ilícito.

Outro grupo de soluções está nos pacotes forenses mais completos voltados a exames remotos. Casey e Stanley (2004) avaliaram dois softwares pioneiros nessas funções: o Encase Enterprise Edition (EEE)[11] e o ProDiscovery IR (PDIR)[12]. Em ambas as soluções, é necessário carregar na memória do computador alvo um pequeno programa (*servlet*) que possibilita a comunicação entre ele e o computador forense. Trata-se de tarefa complexa, pela necessidade de descobrir como instalar o *servlet* no computador alvo, o que muitas vezes impõe ao investigador a necessidade de ter privilégios de administrador no computador alvo. Além disso, os autores do estudo alertam para o fato do próprio *servlet* poder ser alterado por usuários que tenham os conhecimentos suficientes para isso, risco mais relevante se não houver autoridades fisicamente presentes no local da coleta. Por isso, até o momento essas soluções são consideradas apenas tipicamente corporativas e não forenses no real sentido da palavra.

Casey e Stanley (2004) prosseguem sua análise demonstrando como esses produtos possibilitam o exame e a coleta remotos de dados voláteis que transitam pela memória RAM do equipamento e os dados armazenados nos dispositivos de armazenamento de massa do equipamento, como discos rígidos, buscando arquivos ativos, arquivos deletados, áreas remanescentes e áreas não alocadas, além de ter recursos para as demais tarefas investigativas. O produto possui também recursos para o estabelecimento de cadeia de custódia mais simples, como o cálculo de códigos *hash*.

Cumpre salientar que um dos maiores desafios técnicos desses softwares está no fato de ser parcialmente processados nos sistemas examinados, o que contrasta e se contrapõe com a obrigação de gerar a menor interferência possível nesses sistemas, para não comprometer a coleta das evidências.

---

[11] EnCase Enterprise Edition 4.19a

[12] ProDiscover IR 3.5 (PDIR)

Outro risco relevante apontado por Casey e Stanley (2004) refere-se à segurança da própria ferramenta forense, alertando para a gravidade de qualquer perda de controle sobre o exame remoto possa levar ao uso malicioso desses recursos poderosos por terceiros mal intencionados. O produto Encase incorpora um módulo específico de segurança, denominado SAFE, que gerencia a segurança do sistema e a comunicação entre o computador forense e os computadores examinados. Utiliza uma combinação de chaves públicas, privadas e de sessão para assegurar que as comunicações com os *servlet* remotos sejam sempre devidamente autorizadas e criptografadas. Cuida, ainda, da segregação das diversas contas de usuários que podem usar o sistema para investigações, havendo controle severo sobre as regras, isto é, sobre o que cada conta pode acessar. Por exemplo, alguns usuários podem realizar investigações remotas, visualizando conteúdo dos arquivos, enquanto que outros podem apenas coletar evidências de forma criptografada e repassá-las a investigadores forenses, sem conhecer seu conteúdo.

Outro ponto analisado por Casey e Stanley (2004) refere-se ao desempenho do acesso forense remoto. Nos exames realizados pelos autores foi praticamente imediata a leitura remota inicial (visualização da configuração e da estrutura principal de um disco) pelo produto Encase, contudo foram necessários diversos minutos para ler o conteúdo do dispositivo, tendo sido detectada a demanda de pelo menos 5MB/s de banda na rede.

Em síntese, Casey e Stanley (2004) consideram como limitações relevantes a necessidade de privilégio de administrador no computador investigado e que firewalls poderem impedir a comunicação com o computador forense. As principais características identificadas por Casey e Stanley (2004) nos sistemas dedicados ao exame forense remoto foram:

a) possuir interface gráfica de usuário;
b) habilidade para processar *servlets* na memória a partir de dispositivos *read-only*;
c) habilidade para instalar *servlets* como serviço;
d) configuração de *servlet* para escuta em portas alternativas;
e) possibilidade de ocultar *servlets* dos usuários nos sistemas remotos examinados;
f) autenticação por senha PKI entre cliente e *servlet;*

g) comunicação criptografada entre cliente e *servlet;*
h) detectar alterações maliciosas no *servlet*. Cliente somente deve conectar em *servlets* aprovados por PKI;
i) capacidade mínima para analisar meios de armazenamento e estruturas de dados FAT/NTFS, EXT2/EXT3, UFS;
j) visualizar informações no file systems no computador remoto sem alterar seus metadados;
k) identificar arquivos conhecidos ou maliciosos a partir de valores hash MD5;
l) copiar arquivos ou pastas preservando seus metadados;
m) identificar no sistema alvo quais arquivos estão abertos para edição;
n) capturar imagem forense de computadores remotos;
o) visualizar informações sobre processos em execução nos computadores remotos via inspeção da memória;
p) obter detalhes dos processos sem alterar o sistema de arquivos remoto, via inspeção da memória;
q) revelar processo ocultos no sistema remoto, via inspeção da memória;
r) prever caminhos executáveis no computador remoto;
s) listar arquivos abertos no computador examinado;
t) adquirir memória dos processos em execução no computador remoto;
u) prover informações sobre conexões de rede existentes em computadores remotos;
v) visualizar discos RAM montados no computador remoto, como discos PGP etc.;
w) ver compartilhamentos de rede montados no computador remoto;
x) combinar e correlacionar dados de múltiplos sistemas remotos;
y) ser integrável com sistemas detectores de intrusão;
z) possuir controles para administrar a carga de processamento nos sistemas remotos.

3.6 LABORATÓRIO MULTIFUNCIONAL: REAL E VIRTUAL, PRESENCIAL E A DISTÂNCIA

Com base no estudo realizado, entende-se que um laboratório forense para dispositivos digitais deve possibilitar simultaneamente:

(i) exames diretos em dispositivos físicos (disco, memória etc.) ou exames em suas cópias virtuais (imagens forenses), obtendo resultados iguais;

(ii) exames presenciais ou exames remotos, obtendo resultados iguais;

(iii) habilidade para interagir remotamente com dispositivos físicos, como acoplar, reconhecer, interagir e desacoplar dispositivos eletrônicos como discos ou aparelhos telefônicos celulares;

(iv) controle e acompanhamento remoto ou presencial por grupos *ad hoc* de usuários (organizados por casos ou processos), estando os grupos e casos isolados entre si;

(v) elevados níveis de fiscalização, focados em controlar a cadeia de custódia forense e na preservação, tanto no ambiente virtual como no físico, abrangendo, por exemplo, a identificação e vigilância visual remota de discos rígidos a partir de câmaras, detecção remota de redes sem fio, identificação de pessoas por biometria etc.

Não foram localizadas na literatura notícias sobre implementações efetivas de laboratórios desse tipo que pudessem ser utilizados pelos operadores do Direito e pelas partes nos processos judiciais envolvendo sistemas eletrônicos digitais. Por outro lado, o presente trabalho encontrou referências científicas e técnicas que trouxeram as bases para o estudo preliminar de uma possível solução desse tipo, conforme descrito no próximo capítulo.

3.7 SÍNTESE DO CAPÍTULO

Neste capítulo foram descritos os principais centros nacionais voltados à elaboração de perícias técnicas e com base nesse estudo foram classificadas as principais formas de atuação quando à presença dos especialistas e demais operadores do direito envolvidos nas questões da prova digital. Conclui-se que um dos modelos possíveis baseia-se na tele-presença ou exame à distância e na virtualização dos dispositivos digitais a serem periciados.

4 WEBLAB FORENSE

Nos capítulos anteriores verificou-se que novos modelos de trabalho poderiam melhorar os serviços nacionais dedicados a exames periciais envolvendo tecnologias da informação e das comunicações, fazendo frente à deficiência crônica de recursos materiais e competências técnicas. Esses novos modelos baseiam-se em dois pontos principais: (i) a substituição parcial ou total das atividades presenciais por acessos remotos; e (ii) a substituição dos exames em corpos de delito físicos pela sua representação virtual, isto é, mediante a virtualização das atividades periciais.

4.1 LABORATÓRIOS REMOTOS ACESSADOS VIA INTERNET

Uma das motivações para o presente trabalho é identificar um modelo de aplicação que possa levar aos milhares de municípios distantes dos grandes centros o acesso a laboratórios periciais eficazes e confiáveis, normalmente disponíveis apenas nos principias centros econômicos ou científicos.

A análise da literatura indicou que outras áreas de científicas já adotam modelos denominados WebLabs, que consistem em laboratórios físicos que podem ser acessados e controlados remotamente através da Internet.

Neles usuários postados remotamente podem controlar os equipamentos e sistemas reais disponíveis nos laboratórios, podem alocar, ativar e configurar seus recursos, comandar execução de experimentos e receber os resultados.

Em todo o mundo, esses sistemas ainda estão em fase experimental, utilizados principalmente para fins educacionais ou em nível experimental para compartilhar equipamentos entre pesquisadores geograficamente dispersos. Há experimentos em andamento em áreas tão diversas como Óptica e Fotônica, Engenharia Química, Bioquímica, Telecomando, Serviços Ambientais, Robótica e Medicina.

A pesquisa bibliográfica realizada até o momento não logrou êxito em encontrar artigos, dissertações ou teses, nacionais ou internacionais, sobre a utilização de WebLabs em aplicações tipicamente forenses para examinar dispositivos digitais como computadores e aparelhos telefônicos celulares.

Laboratórios são essenciais para as atividades científicas, mas incorrem em custos geralmente elevados para sua aquisição, montagem e operação. Além disso, sua utilização é bastante limitada, pois dependem da presença física dos usuários, há restrições de horários durante os quais podem ser utilizados, apresentam custos operacionais elevados pela movimentação de pessoas e são inadequados para a realização de muitos experimentos simultaneamente (FERREIRA, 2007).

A evolução das tecnologias de processamento de dados e das telecomunicações fez surgir, em complemento aos laboratórios ditos reais, programas de computador procuram reproduzir, pelo menos em parte, o comportamento de situações do mundo real. Isso é feito mediante simulações matemáticas que reproduzem em um laboratório dito virtual as características de interesse do mundo real

Essa solução traz importantes vantagens quanto à escalabilidade, flexibilidade, possibilidade de acesso à distância, uso por múltiplos usuários e custo proporcionalmente menor, mas não conseguem atender plenamente os casos que envolvem experimentos complexos pela dificuldade ou impossibilidade de construir modelos matemáticos adequados (FERREIRA, 2007).

Os WebLabs buscam unir as vantagens dos laboratórios reais e dos laboratórios virtuais, pois os experimentos são realizados à distância através de interfaces que possibilitam o controle remoto das variáveis em equipamentos laboratoriais e amostras reais. Agregam condições mais fidedignas a modelos que até então eram apenas simulados em laboratórios virtuais. Com seu desenvolvimento, os laboratórios remotos controlados via Internet passaram gradualmente a chamar-se WebLabs (DEL ALAMO, et al., 2002).

Para o presente estudo é relevante constatar que WebLabs possibilitam a diferentes pesquisadores participar de maneira interativa dos mesmos experimentos e exames. Diversos protótipos tiveram sucesso ao prover interação de equipes heterogêneas e fisicamente distantes em torno de um mesmo experimento (JESUS et al., 2007).

Essa característica mostra-se importante para um ambiente de perícia forense, onde interagem peritos e assistentes técnicos, com formações, experiências e interesses diversos entre si. Além disso, as autoridades e a própria sociedade devem fiscalizar e autenticar as atividades realizadas nesse ambiente pericial.

Dessa maneira, mostra-se adequado considerar os estudos e experimentos realizados com WebLabs em outras áreas para avaliar a possibilidade de aplicar esse modelo em um WebLab Forense dedicado ao exame de sistemas eletrônicos digitais.

Nesta dissertação será discutido o conceito geral de uma possível aplicação de WebLab Forense, ficando para trabalhos posteriores o estudo detalhado dos seus aspectos conceituas e práticos uma vez que essa tarefa extrapola os limites práticos estabelecidos para o presente trabalho.

4.2 PROPOSTA DE UM WEBLAB FORENSE

O estudo dos WebLabs implementados em outras áreas de conhecimento (AGRAWAL; SRIVASTAVA, 2007) e seu confronto com as necessidades identificadas para o ambiente pericial, indicam que um WebLabs Forense deva contemplar as funções principais indicadas no Quadro 1.

Principais Funções	Descrição
Processos/Casos	Gestão de processos judiciais e das tarefas periciais (controles de processo, partes envolvidas, peças submetidas à perícia, prazos, quesitos, etc..)
Usuários	Gestão de usuários (direitos, permissões, responsabilidades, etc.)
Serviços	Gestão dos serviços (cadeia de custódia, coleta, armazenamento, exames, laudos, pareceres, etc.)
Recursos	Gestão de recursos (alocação de recursos, controle de qualidade, etc.)
Administração	Gestão do sistema (políticas, normas, planejamento, autenticações, auditoria, segurança, manutenção etc.)

Quadro 1 - Principais funções em um WebLab Forense

A Figura 13 apresenta uma proposta de estrutura para o WebLab Forense, contendo em essência os quatro grandes blocos funcionais descritos a seguir:

a) WebLab Server - um servidor central que constitui o núcleo central de controle e serviços do sistema.
b) Lab Servers - um ou mais servidores para laboratórios remotos, responsáveis pelo gerenciamento local de cada laboratório forense.

c) Device Controllers - um ou mais controladores de dispositivos, interfaces especializadas que possibilitam a conexão e o exame das peças de interesse pericial. As interfaces podem ter um papel mais passivo, quando apenas fazem a leitura dos dados armazenados nas peças (memória digital, etc.), ou mais ativo ao enviar sequências de comandos às pelas examinadas e tratar suas respostas (celular, robô etc.). Além da interação digital, os *devices controllers* podem coletar evidências visuais (nome do fabricante, modelo da peça, estado geral de conservação, impressões digitais etc.), evidências sonoras (ruídos anormais indicando falha de um disco rígido etc.), dados ambientais (pessoas presentes, biometria, procedimentos realizados pelas pessoas, localização do laboratório, temperatura, vibrações etc.).
d) Usuários – registros e funcionalidades correspondentes às diversas pessoas que podem interagir com o sistema, tais como: (i) administradores do sistema; (ii) peritos que operam o sistema; (iii) pessoas que participam de diligências, como delegados e oficiais de justiça; (iv) pessoas que atuam junto ao processo, como juízes, advogados, autores, réus, assistentes técnicos etc.; (v) especialistas consultados *ad hoc* em função de seu notório conhecimento; (vi) membros da sociedade autorizados a acompanhar ou fiscalizar os procedimentos etc..

A Figura 13 ilustra o modelo geral proposto neste trabalho para um WebLab Forense, adaptado a partir do modelo desenvolvido por Agrawall e Srivastava (2007, p. 305):

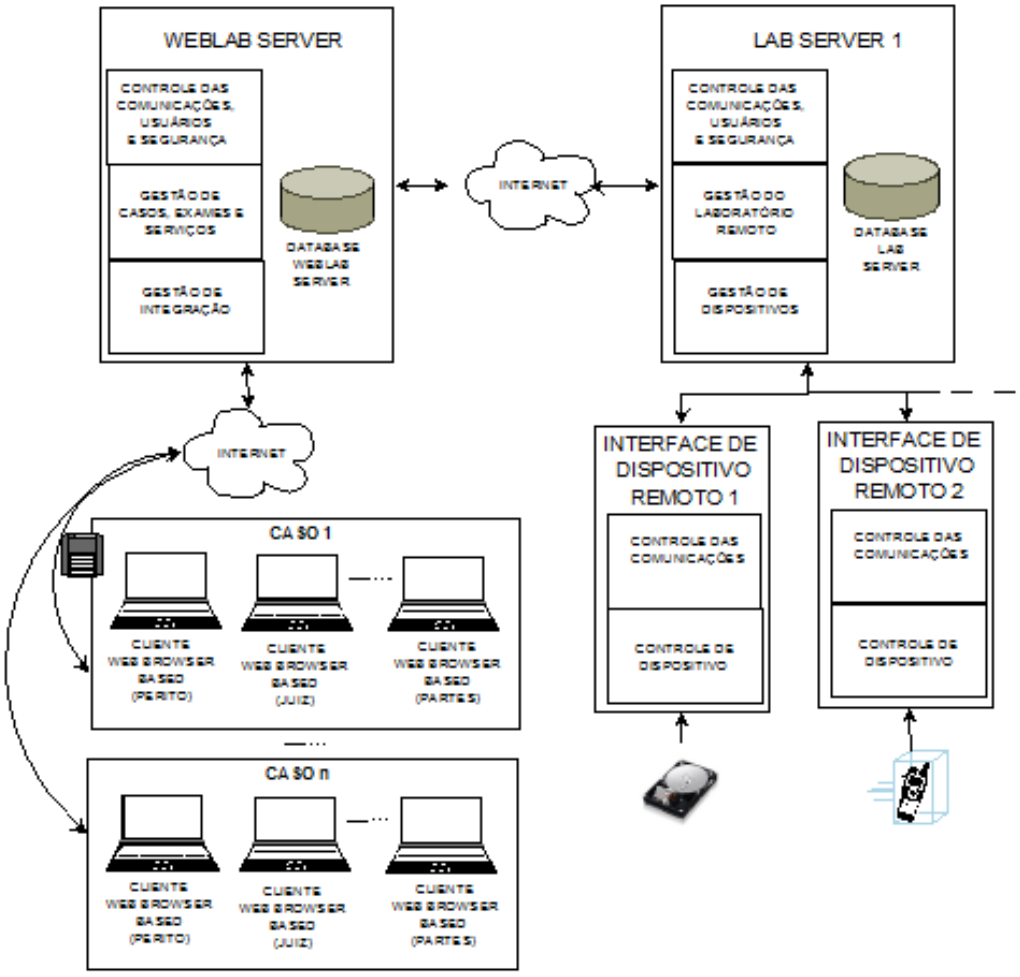

Figura 13. WebLab Forense proposto

Em termos gerais, o WebLab Server atende grupos de usuários organizados em função do papel que cumprem em cada processo judicial (perito, juiz, advogado, assistente técnico etc.,), possibilitando que eles realizem ou fiscalizem remotamente ou presencialmente procedimentos com as peças de interesse pericial, utilizando para isso os Lab Servers e Devices Controllers.

A interação dos usuários com o WebLab Server deve ser a mais natural possível e, preferencialmente, basear-se em simples navegadores Internet, tendo em vista a necessidade de ampla e fácil utilização por qualquer pessoa e em qualquer ponto do país.

Pelo lado dos laboratórios remotos, deve ser possível conectar diversos Lab Servers e cada um deles deve possibilitar a conexão de diversos *Device Controllers* atualizáveis com facilidade na medida em que são lançados no mercado novos dispositivos eletrônicos digitais que pode ser submetidos à perícia técnica.

Dessa maneira, o Weblab Forense sugerido baseia-se em estrutura modular bastante similar àquela adotada por outros WebLabs desenvolvidos no mundo, diferenciando-se basicamente pelo campo de aplicação e por regras de negócio específicas, típicas do ambiente judiciário e dos procedimentos periciais.

Esse modelo foi avaliado a partir de um experimento envolvendo o exame remoto de um disco rígido de computador, apenas com o objetivo de verificar preliminarmente sua validade funcional. Por limitações de recursos e tempo, não é possível e não é escopo deste trabalho detalhar a estrutura e funcionamento do WebLabs Forense, pretende-se apenas verificar a validade geral da ideia, deixando seu detalhamento e implantação para trabalhos futuros.

Os dois próximos itens descrevem a prova de conceito e seus resultados. O item 4.5 - Contribuições e Perspectivas com a Evolução do Experimento, apresenta as contribuições deste trabalho para apoiar estudos futuros.

4.3 PROVA DE CONCEITO: WEBLAB FORENSE PARA DISCOS RÍGIDOS

Partindo-se do modelo básico de WebLab Forense para ambientes digitais foi montada uma estrutura reduzida apenas para testar o conceito de coleta e exame remotos do conteúdo de um disco rígido de computador pessoal, procedimento bastante comum na rotina pericial, tendo sido simuladas no teste a condução dos procedimentos por um perito e sua fiscalização por outros operadores do Direito.

Nesse protótipo experimental e que visa apenas realizar uma prova de conceito[13], foram utilizados tanto produtos tradicionais do mercado forense, assim como produtos mais recentes e modernos, destacando-se:

a) O laboratório forense ImageMASSter Solo 4, da Intelligent Computers, um dos principais e mais recentes produtos mundiais para captura de dados armazenados em dispositivos digitais;

[13] Tendo em vista as condições de licenciamento dos softwares e equipamento forenses, cumpre salientar que o presente experimento foi conduzido apenas em ambiente de laboratório e somente com o objetivo puramente acadêmico de realizar uma prova de conceito sobre o modelo de WebLab Forense. Portanto, não se trata de qualquer aplicação prática comercial e nem mesmo de qualquer engenharia reversa desses produtos. Eventuais aplicações práticas futuras dependerão de autorização e licenciamento pelos detentores dos direitos.

b) O software Autopsy, produto gratuito e que há muitos anos é utilizado no ambiente pericial forense. Foi também avaliada a possibilidade de utilização de softwares forenses de última geração, como o Encase, da Guidance Software, e Forensic Toolkit (FTK), da Access Data, ferramentas utilizadas nos mais modernos órgãos policiais e pericias do mundo.

Esses produtos embutem grande parte das funções necessárias para exames forenses em dispositivos digitais, motivo pelo qual foram selecionados para integrar este experimento. Há no mercado razoável oferta de outros produtos que cumprem funções dessa natureza.

O software Autopsy é um dos mais tradicionais produtos do mercado forense, mas com evolução bastante limitada. O software forense Encase é um dos líderes na área e possui diversas versões com finalidades e escopos distintos, voltados desde a área policial (Law Enforcement), passando pela área pericial propriamente dita (Encase Forensic) e outra voltada para controles corporativos (Encase Enterprise).

Esta última versão possui recursos que possibilitam a uma estação de monitoramento acessar e examinar remotamente os demais computadores da empresa, o que se aproxima bastante do modelo desejável para um WebLab Forense. Esse produto possibilita ainda que escritórios de advocacia tenham acesso a alguns resultados do monitoramento remoto mediante integração de softwares, contudo o ambiente continua predominantemente voltado ao uso corporativo.

Para esta prova de conceito foi adotada a premissa de utilizar apenas componentes prontos disponíveis no mercado, mesmo sabendo-se que a implementação real de um WebLab Forense possivelmente demandará o desenvolvimento de componentes personalizados, possivelmente baseado em software livre, além da aquisição e integração de componentes comerciais, de maneira mais profunda e completa.

Assim sendo, a prova de conceito realizada embasa a análise, mas não se confunde com o modelo completo do WebLab Forense proposto, destacando-se os aspectos apresentados no Quadro 2.

Item	Weblab Proposto	Prova de Conceito
Estrutura	Objeto de trabalhos futuros possivelmente baseados na ampla estrutura dos principais *frameworks* que têm sido adotados em WebLabs para outras áreas científicas	Simples conexão de ferramentas forenses tradicionais com o objetivo limitado de obter uma avaliação preliminar da funcionalidade principal do modelo proposto.
Coleta e exame de evidências	Experimentação prática na coleta e analise remotas de uma grande diversidade de evidências digitais	Teste simples de coleta dos dados de um disco rígido, utilizando recursos muito limitados e sem as funções típicas de um WebLab.
Fiscalização e participação de juízes, promotores, advogados, oficial de justiça, delegado de polícia, autor da ação, réu e assistentes técnicos	Acessos à distância e interativos via WebLab Forense, feitos pelos envolvidos ou interessados no exame pericial a partir de seus locais de trabalho.	Teste simples apenas em rede local e sem usuários reais. Os nomes de usuário como perito, juiz e delegado foram utilizados apenas para ilustrar as diferentes visões no experimento realizado, visando com isso ilustrar as possibilidades futuras em exames mais completos.
Identificação e coleta de evidências	WebLab Forense com recursos para acoplar-se a diversos módulos especializados no acesso e captura de dispositivos digitais (computadores, telefones celulares, câmaras, sistemas embarcados etc.).	Utilizado o moderno e recém-lançado laboratório de coleta forense Solo 4. Como peças a examinar, foram adquiridos, sem qualquer seleção, dois discos rígidos que estavam à venda como sucata em região tradicional de comércio de produtos eletrônicos na cidade de São Paulo.
Laboratório para exames forenses	Ampla infraestrutura com servidores, softwares forenses, sistemas de armazenamento, comunicações, custódia de evidências, segurança, gestão etc.	Um computador equipado com sistema operacional e o software Autopsy, cumprindo o papel de WebLab Server para fins do experimento. Um computador simulando o acesso remoto dos usuários.

Amplitude	Experimento completo via web, disponível em todo o país, com intensos recursos de segurança para proteção do sistema e autenticação de usuários, gestão de atividades, transmissão de dados e análise de evidências. Sistema modular, crescente na medida da demanda.	Rede local com segurança elementar. Ambiente simplificado composto por computadores PC com sistema operacional Windows, máquina virtuais Debian, ferramentas comuns para administração remota (VNC), câmara e microfones.
Demais funções	Funções típicas de WebLabs redefinidas conforme necessidades forenses.	Não implementadas no protótipo.

Quadro 2 - Comparativo WebLab Forense proposto e prova de conceito

A prova de conceito foi realizada em ambiente fechado, com equipamentos interligados em rede local e apenas em nível experimental e acadêmico, sem qualquer utilização para casos reais. Mesmo assim, cuidou-se de ter presentes a quantidade de licenças em número proporcional ao teste.

Decidiu-se ainda que a prova de conceito não avaliaria questões de funcionalidade, segurança e desempenho, tratando-se apenas de prova de conceito em ambiente restrito.

Foram utilizados computadores desktop padrão para simular estações de trabalho dos operadores do Direito e das partes, como o juiz, delegado de polícia, perito, autor, réu e perito judicial. O WebLab Server foi simulado em um computador desktop e como Lab Server foi configurado e utilizado o computador existente no interior do equipamento forense Solo 4, que incorporou também as funções de interface com o dispositivo a analisar, como mostra a Figura 14.

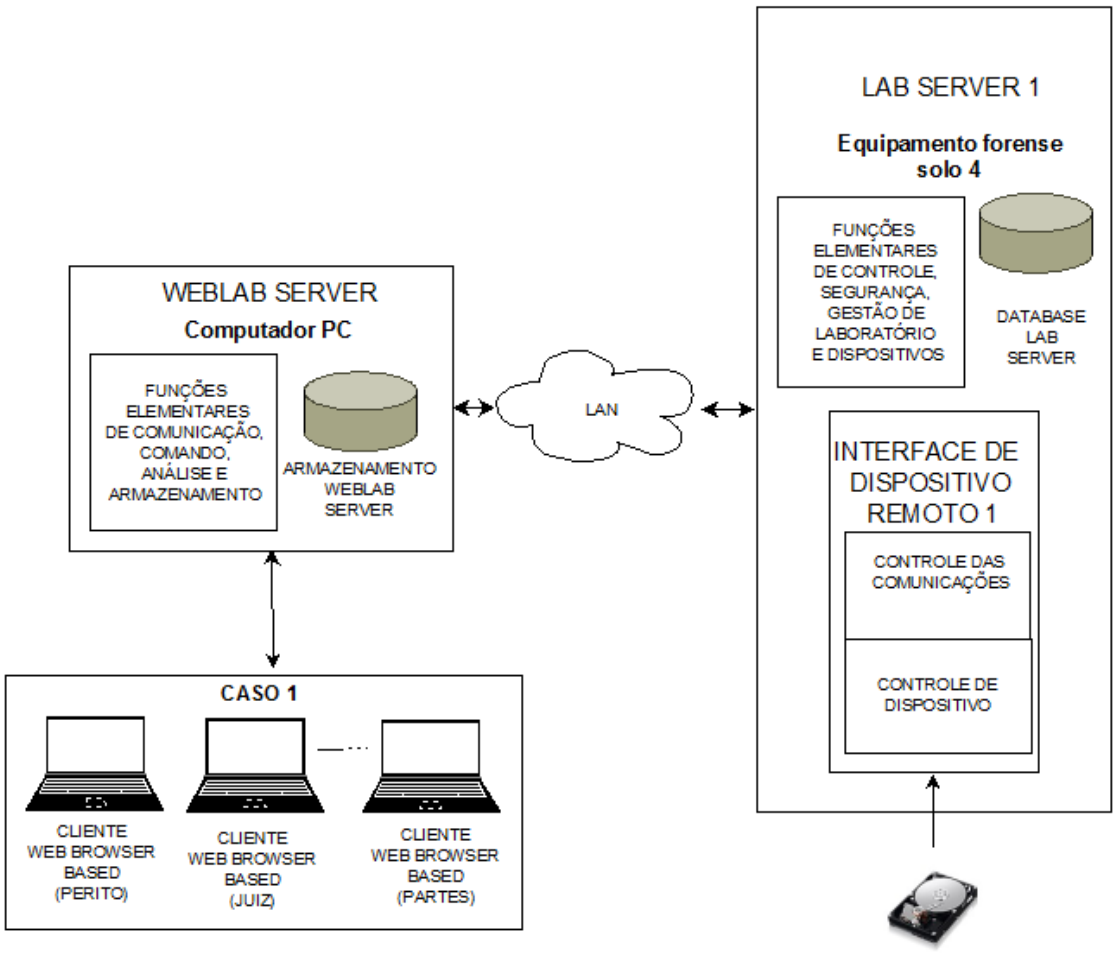

Figura 14. Prova de conceito

Para realizar o teste foram utilizados discos rígidos adquiridos como sucata em lojas de bairro paulistano tradicional no comércio eletroeletrônico. Trata-se, portanto, de discos rígidos antigos e usados, descartados como sucatas, mostrados na Figura 15 e na Figura 16.

Figura 15. Primeiro disco para prova

Figura 16. Segundo disco para prova

Os discos rígidos foram conectados e ativados remotamente em equipamento forense ImageMASSter Solo-4 Forensic, produzido pela Intelligent Computer Solutions, mostrado na Figura 17.

Figura 17. Equipamento forense Solo 4: lab server e interface de dispositivo

O primeiro disco rígido foi conectado ao equipamento Solo 4, na entrada destinada a discos suspeitos, denominada “Suspect 1”, como pode ser visto na Figura 18. A especificação técnica do Solo 4 informa que as portas destinadas a discos “suspeitos” são automaticamente protegidas contra gravação.

Figura 18. Conexão do primeiro disco à porta “Suspect 1” do Solo 4

O segundo disco rígido foi conectado à entrada “Suspect 2” do Solo 4, como mostra a Figura 19.

Figura 19. Conexão do segundo disco à porta “Suspect 2” do Solo 4

Em seguida, um disco rígido novo foi conectado ao Solo 4, à entrada denominada “Evidence 1”, destinada ao armazenamento das evidências digitais coletadas nos

discos suspeitos. O próprio Solo 4 encarrega-se de formatar automaticamente o disco para evidências.

Figura 20. Disco móvel para armazenar evidências.

Figura 21. Conexão do disco de evidências à porta “Evidence 1” do Solo 4.

Neste experimento, o equipamento Solo 4 assume dupla função: (i) como Device Controller, ao atuar como interface com os dispositivos digitais a examinar; e (ii) como Lab Server que interage com os Device Controllers e coleta evidências repassando-as ao WebLab Server, no conjunto mostrado na Figura 22.

Figura 22. Lab server, discos suspeitos e disco para evidencias (centro)

A prova de conceito prevê que o WebLab Forense deve propiciar o acompanhamento e fiscalização remota de todas as atividades por meio de microfones e câmaras de vídeo controladas à distância. As câmaras IP devem poder

ser movimentadas remotamente sob controle dos usuários a partir de um simples navegador Internet, possibilitando a fiscalização à distância e a gravação dos procedimentos periciais realizados, a título de cadeia de custódia. Possibilita, ainda, a conferência remota dos dados físicos das peças examinadas, por exemplo, da marca, modelo e número de série que são impressos na etiqueta posta pelo fabricante sobre o disco, além da obtenção de fotos e vídeos para o laudo pericial, e, com sua evolução, até mesmo medições de temperaturas por infravermelho, busca de marcas decorrentes de uso, etc.. Podem ainda servir no reconhecimento biométrico das pessoas que participam dos procedimentos periciais. As câmaras podem ser movimentadas nas direções horizontal e vertical, sob comando remoto pelo usuário do sistema, e ainda realizar operações de zoom[14], como aquelas mostradas na Figura 23. Possibilitam também a detecção de movimentos e a visão noturna, para cumprir a função de vigilância sobre as peças periciais custodiadas. Idealmente, essas câmaras e microfones devem ser integrados aos Device Controllers.

Figura 23. Câmaras IP
controladas remotamente

A infraestrutura para realizar a prova de conceito foi gerada basicamente com a instalação do software VNC, viabilizando acesso remoto entre o computador Solo 4, o computador que cumpriu o papel de WebLab Server e o computador que simulou a participação dos usuários. Foram utilizados os recursos normais do ambiente PZ para comunicação de dados, processamento, armazenamento, autenticação de

[14] Câmaras marca Cisco e outras marcas comerciais.

usuários e segurança. O código-fonte do software VNC foi utilizado conforme disponível no mercado, mas ele pode ser modificado em experimento futuro para aproximar sua funcionalidade ao modelo previsto para WebLab Forense. Na descrição da prova de conceito são utilizados os termos juiz delegado, perito e outros similares para referir-se a usuários simulados durante o experimento, pois não houve a participação real dessas autoridades. Considera-se que esse ambiente real deve ser objetivo dos próximos experimentos.

Iniciado o experimento, foi possível a partir do computador WebLab Server ou das estações a ele conectadas acompanhar remotamente as operações realizadas pela pessoa que estava junto aos discos rígidos, inclusive a inspeção visual das peças periciais e sua conexão ao Device Controller via Lab Server.

O perito na simulação acionou remotamente[15] o Solo 4 e obteve a identificação digital do disco rígido, para em seguida comparar visualmente esse número de série com a inscrição existente em etiqueta colocada pelo fabricante no corpo do disco rígido.

A operação realizada remotamente no equipamento forense Solo 4 era simultaneamente acompanhada, também remotamente, pelos personagens que representam o juiz, o delegado ou advogados, entre as diversas partes no processo.

Durante parte do experimento utilizou-se conexão remota onde foram abertas diversas sessões de conexão VNC ao equipamento Solo 4. Uma das conexões destina-se a manipular o sistema, cumprindo o papel destinado ao perito, e as outras sessões foram abertas apenas como visualização para os papéis de juiz, autor, réu, delegado, advogados e assistentes técnicos. Nessa mesma linha, caberia tecnicamente ofertar o acompanhamento remoto à sociedade, para socializar a fiscalização sobre os procedimentos periciais, proporcionando, por exemplo, o acesso ao WebLab Server para entidades representativas da sociedade, como OAB, jornalistas etc.

O experimento estabeleceu conexão remota dos diversos componentes do sistema, ou seja, entre o computador que exerce a função de WebLab Server, o

[15] Como visto nesta dissertação, a operação remota foi simulada em rede local.

equipamento que exerce a função de Lab Server (Solo 4) a Interface de Dispositivo Digital (idem Solo 4, neste caso).

A Figura 24 mostra a tela do computador que simula o WebLab Server vendo-se em seu interior a tela da conexão remota com o equipamento Solo 4.

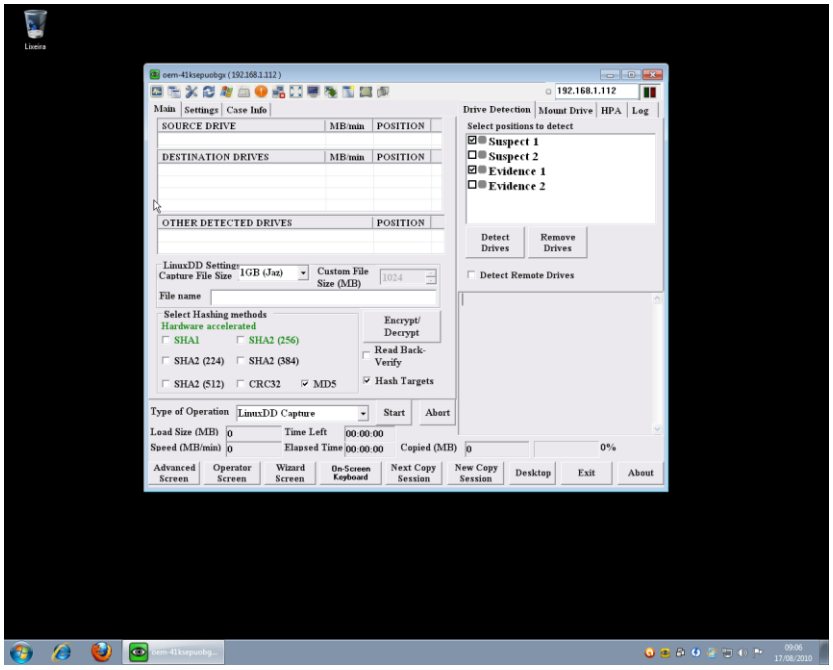

Figura 24. WebLab Server com visualização remota da tela do Solo 4

Em seguida, vê-se na Figura 25 simulação da tela do computador cliente do perito acessando o WebLab Server via software VNC.

Nesse modelo, o perito é o único usuário que pode manipular teclado e mouse e realizar transferência de arquivos.

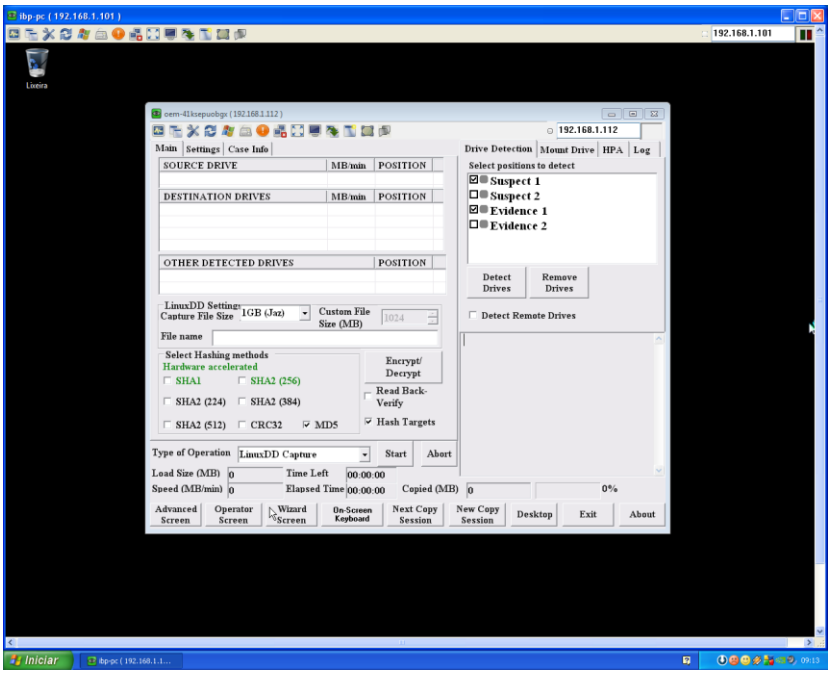

Figura 25. Perito acessa WebLab Server e manipula o Lab Server

A Figura 26 mostra tela onde a autoridade policial visualiza, em tempo real e remotamente, os fatos que ocorrem no WebLab Server, porém sem interação com o equipamento para manipulação de evidências.

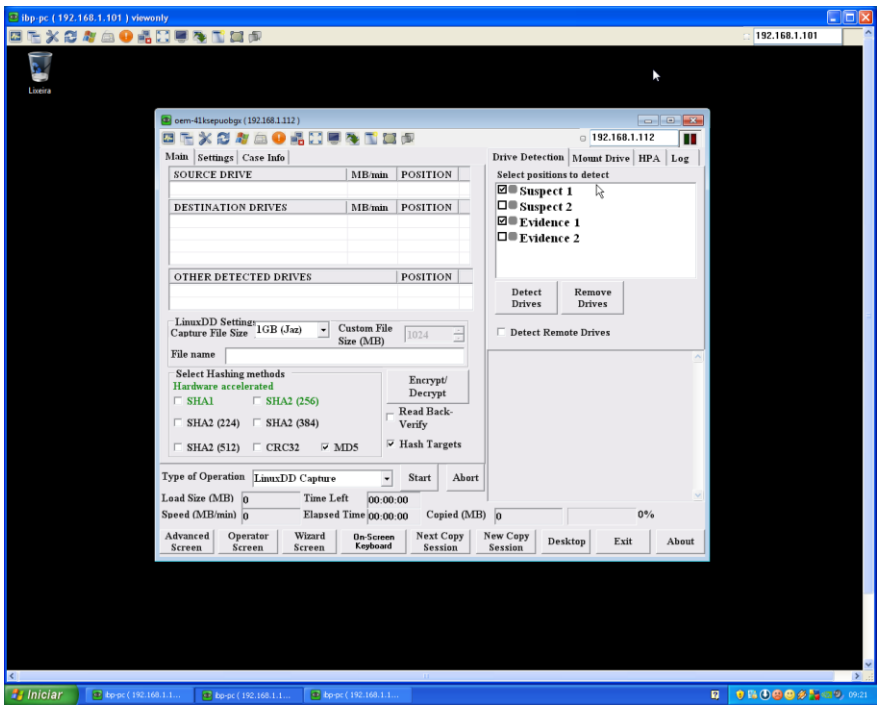

Figura 26. Delegado acessa WebLab Server e fiscaliza o Lab Server

A Figura 27 mostra a tela na qual o juiz visualiza remotamente, através do WebLab Server, a própria tela de captura no Solo 4 posto a distância, porém sem interação com as evidências.

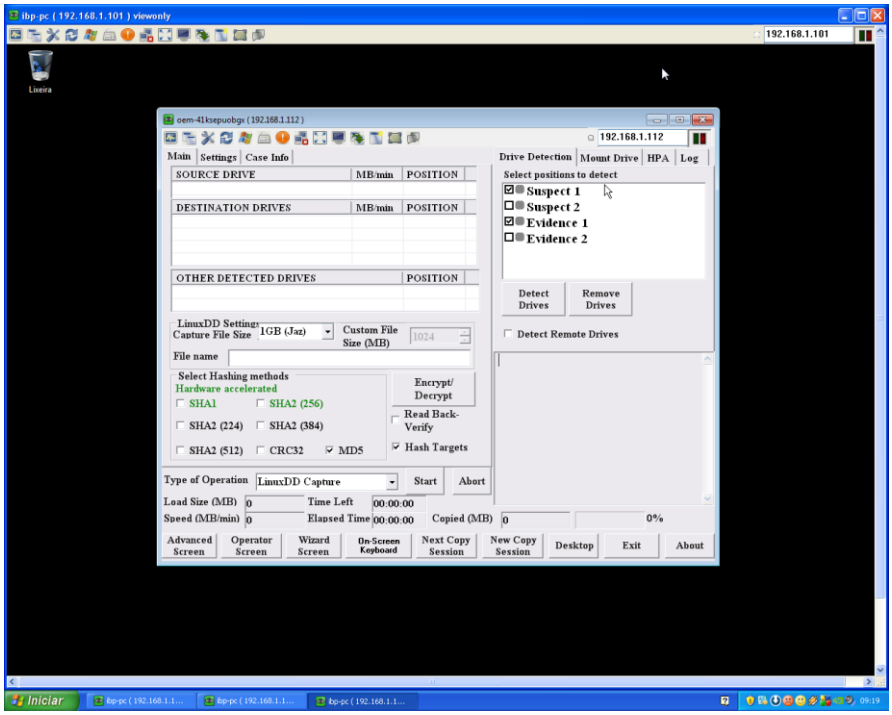

Figura 27. Juiz acessa WebLab Serve e fiscaliza Lab Server

Na Figura 28, o perito, a partir do seu computador, acessa o WebLab Server e a partir dele acessa o equipamento Solo 4 e ali aciona procedimento para identificar os discos rígidos que a ele foram conectados.

As luzes acesas (verdes) no canto direito superior (Suspect 1, Evidence 1) indicam que ambos os disco foram identificados e seus dados são visíveis na parte inferior direita da janela.

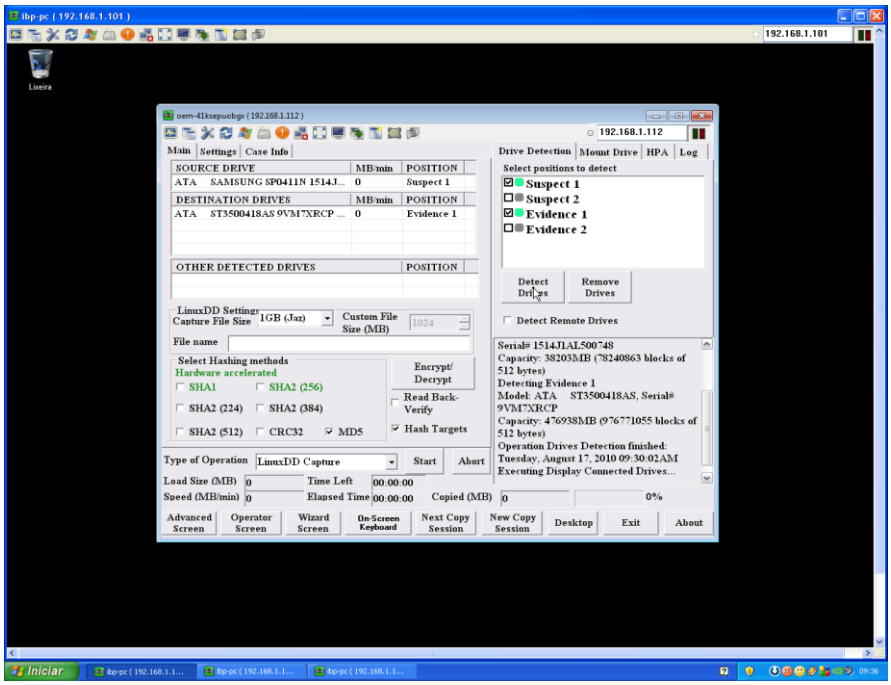

Figura 28. Perito comanda a identificação dos discos no Solo 4

A Figura 29 mostra a imagem vista no computador do perito, vista através do WebLab Server, que mostra a tela no Solo 4, que cumpre o duplo papel de Lab Server e Device Controller, indicada a correspondência com os dispositivos físicos (HDs) cuja conexão e desconexão são comandadas remotamente.

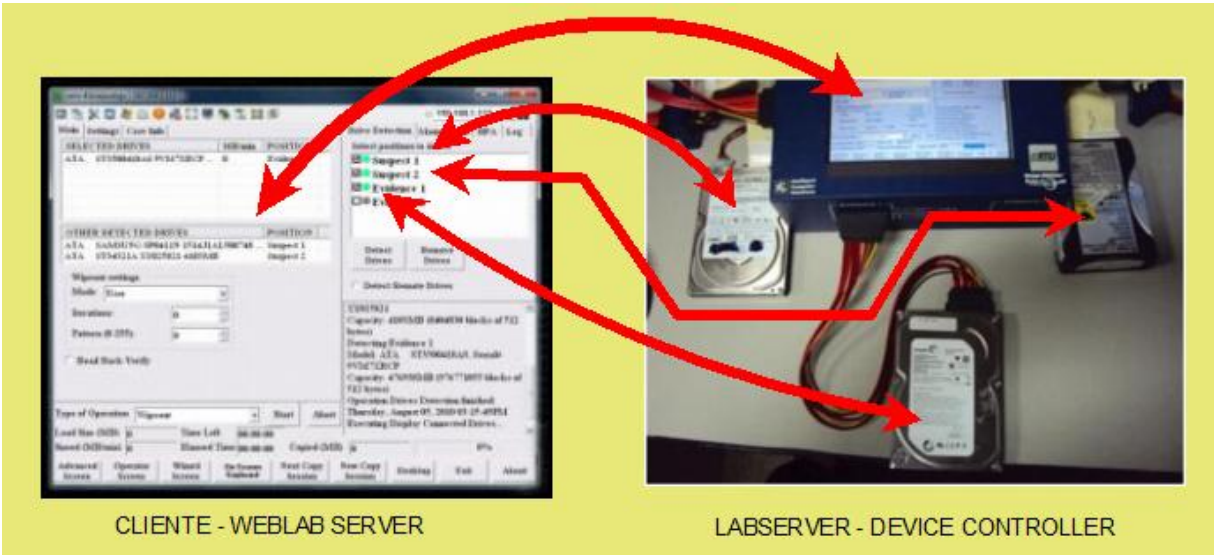

Figura 29. Dispositivos físicos e sua representação no WebLab

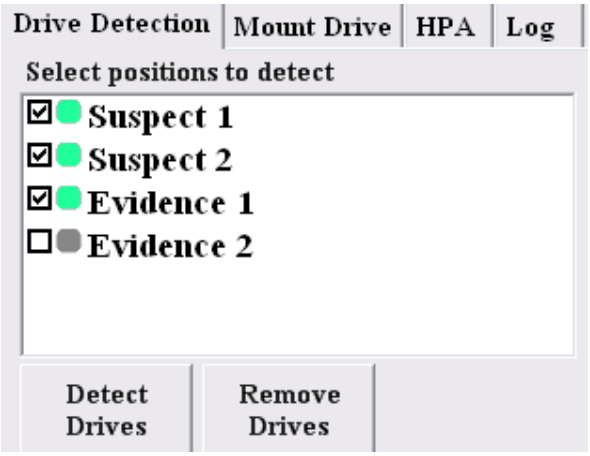

Figura 30. Detalhe da detecção remota de discos conectados

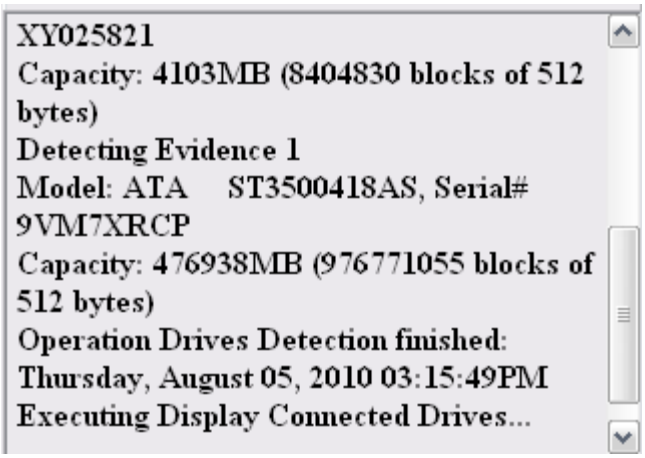

Figura 31. Detalhe dos dados lidos nos discos e fiscalizados remotamente

A Figura 32 mostra o perito comandando remotamente o início da cópia forense do disco Suspeito 1 (01_Evidencia), cujo progresso é visualizado remotamente no canto direito inferior da janela.

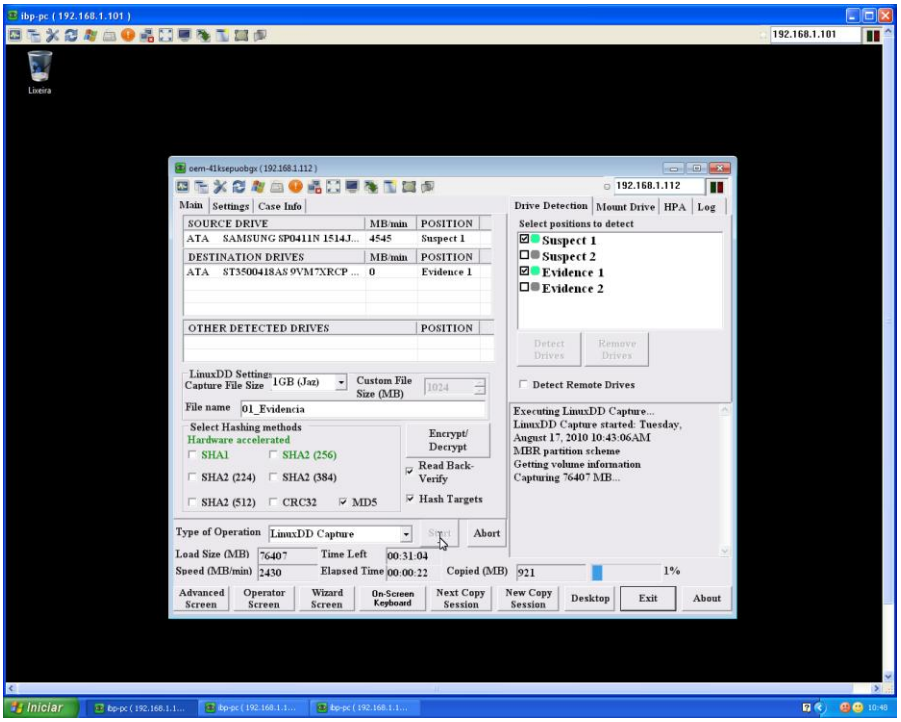

Figura 32. Perito comanda a cópia do disco Suspeito 1 no Solo 4

A Figura 33 mostra o computador do juiz, do delegado, etc. acompanhando as ações do perito, porém sem interação com os dados (decisão administrativa).

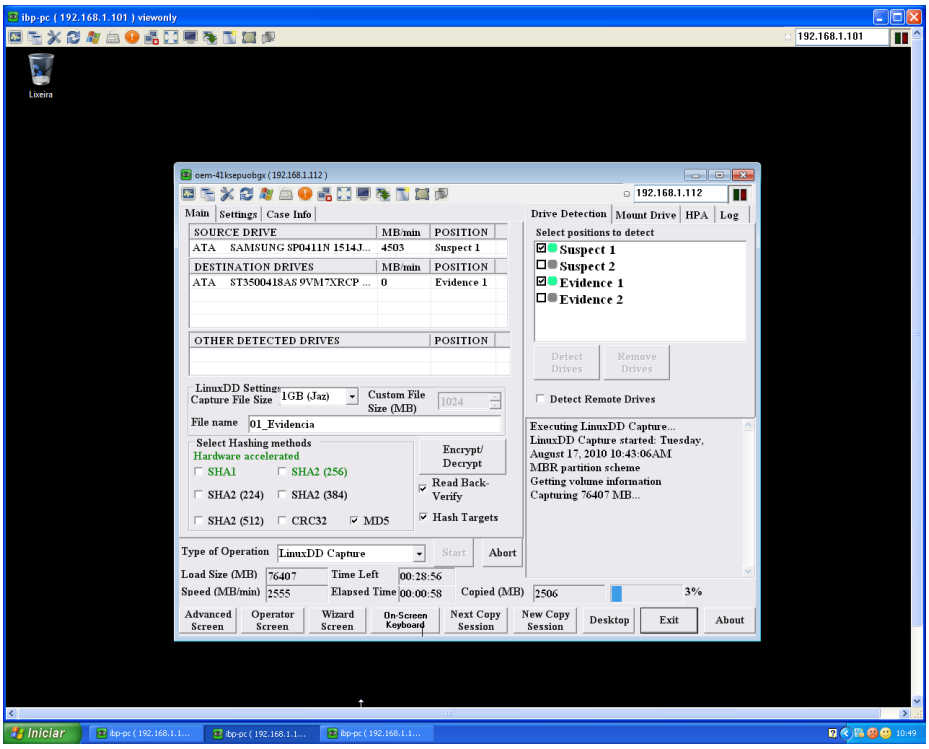

Figura 33. Juiz fiscaliza procedimentos no Solo 4

Na Figura 34, vê-se através da tela do perito que a coleta foi concluída, com a geração de imagem forense e em seguida o perito comanda a verificação do código *hash* da imagem gerada.

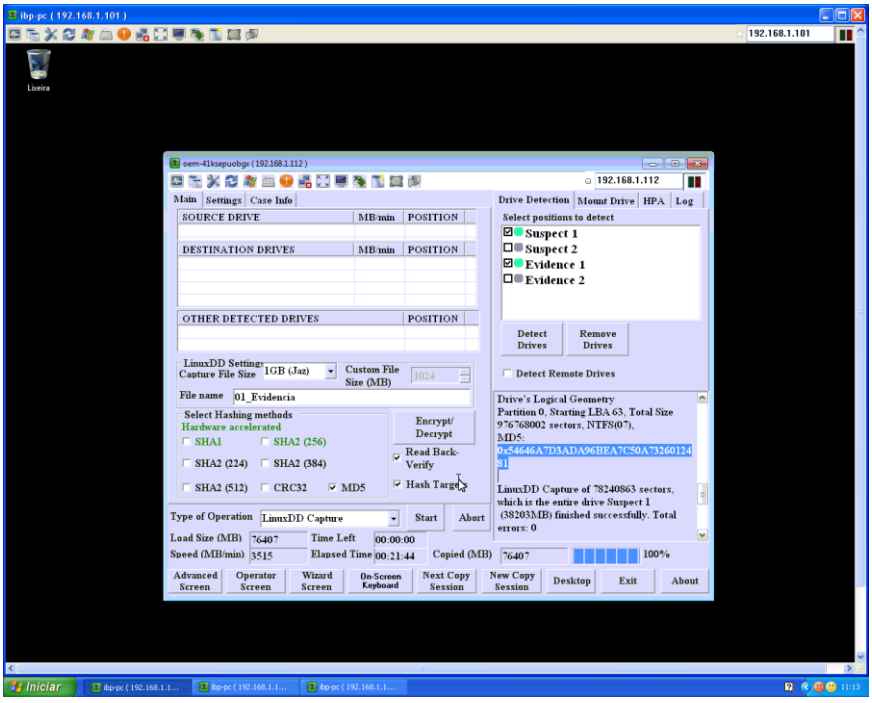

Figura 34. Perito comanda verificação do *hash* da imagem no Solo 4

Na Figura 35, o juiz acompanha remotamente a verificação do hash da imagem gerada anteriormente pelo perito.

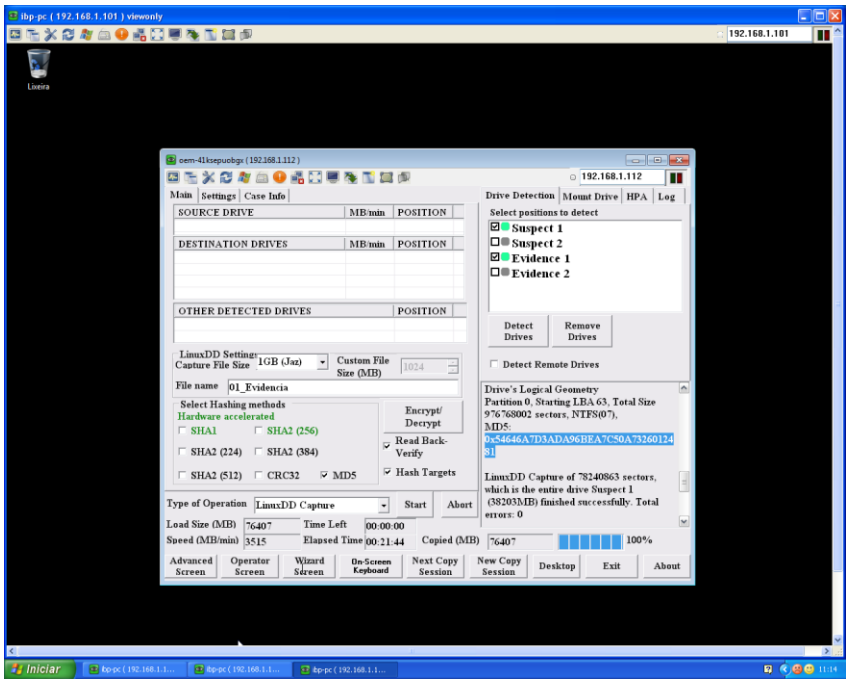

Figura 35. Juiz fiscaliza cálculo do hash no Solo 4

Concluída a captura do primeiro disco, o perito configura novamente e remotamente o Solo para que passe a capturar o segundo disco, nomeando 02_Evidencia, e comanda o processo de clonagem.

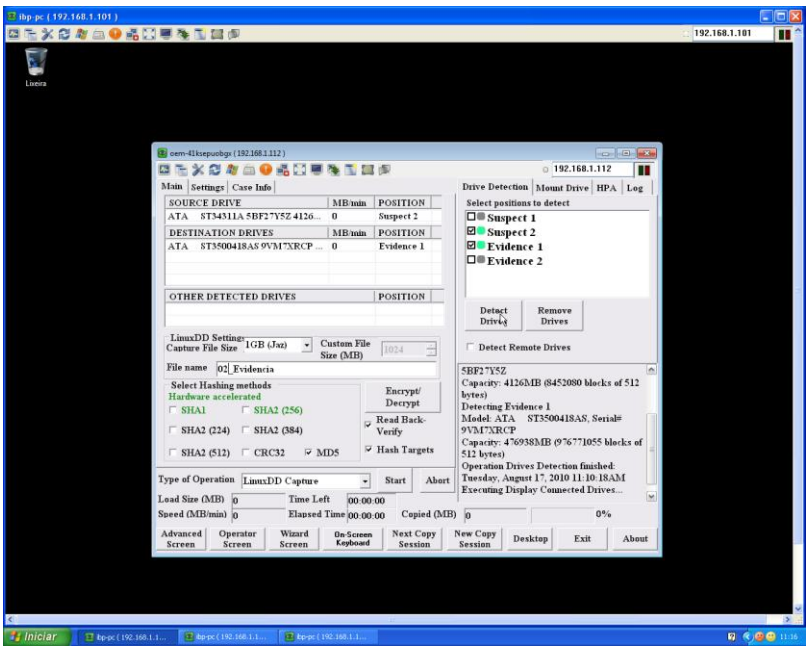

Figura 36. Perito reconfigura Solo 4 para captura do segundo disco

Em seguida tem início a geração da segunda imagem forense, sob comando remoto do perito (Figura 37) e fiscalização remota pelo delegado (Figura 38) e pelo juiz (Figura 39)

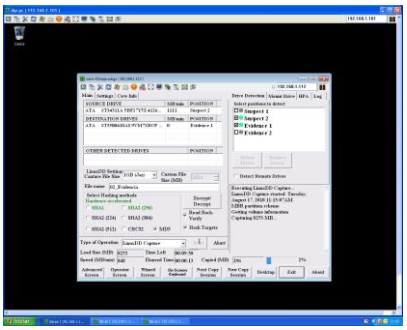

Figura 37. Perito aciona captura do segundo disco

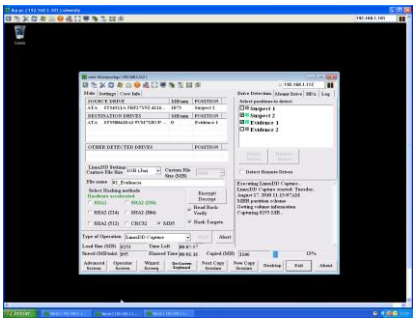

Figura 38. Delegado fiscaliza captura do segundo disco

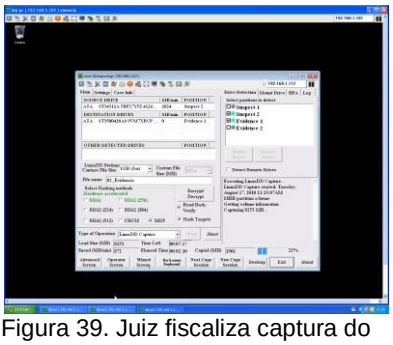

Figura 39. Juiz fiscaliza captura do segundo disco

Na Figura 40, concluída a segunda cópia forense, o perito comanda remotamente a conferência da imagem gerada, sempre sob o controle do delegado e do juiz.

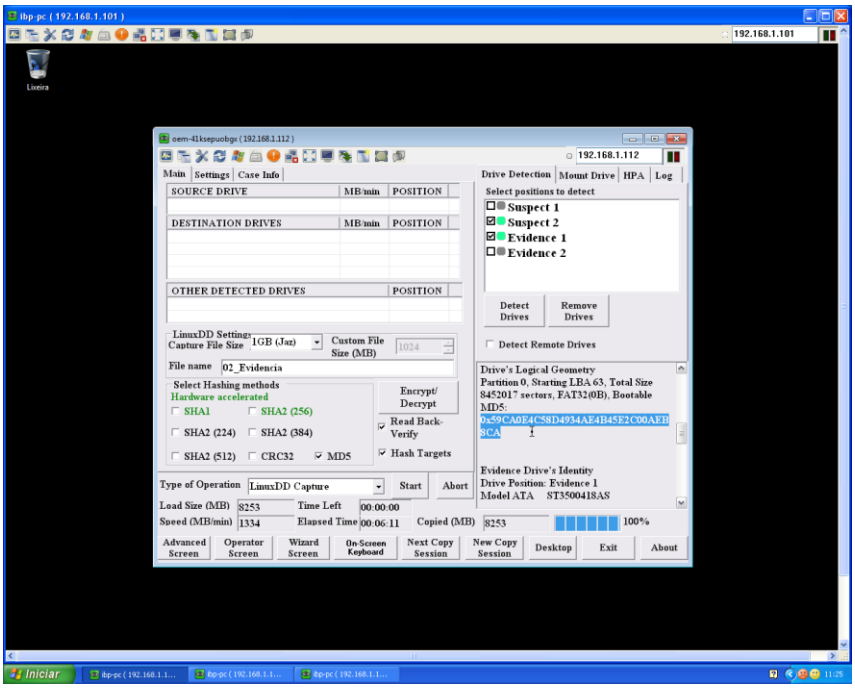

Figura 40. Perito comanda conferência do *hash* da imagem do segundo disco

Tendo concluído a captura remota das imagens forenses dos dois discos suspeitos, o perito aciona remotamente a transferência dos arquivos imagens desde o Solo 4 até o WebLab Server (Figura 41), sob a supervisão remota do delegado (Figura 42).

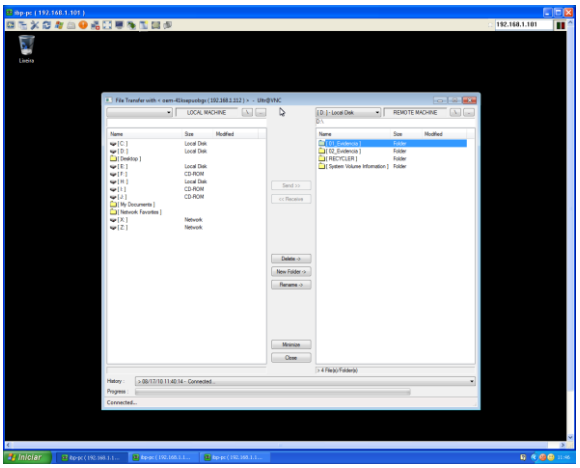

Figura 41. Perito comanda transferência das imagens para WebLab Server

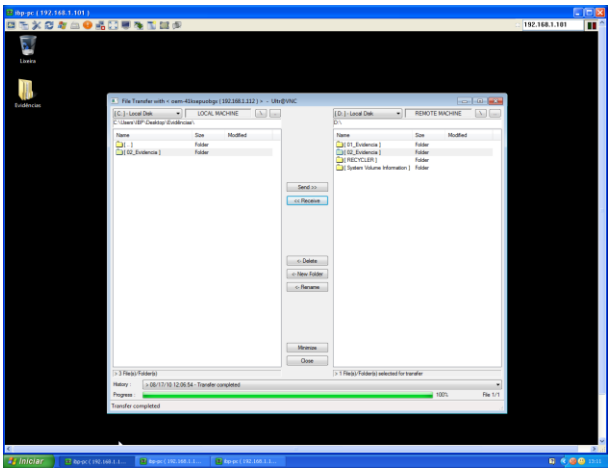

Figura 42. Delegado fiscaliza transferência das imagens para WebLab Server

As transferências demoraram cerca de 2 horas no ambiente onde foi efetuado o experimento.

Concluídas as transferências, o perito confirma o tamanho dos arquivos recebidos (Figura 43), sob a supervisão do juiz (Figura 44).

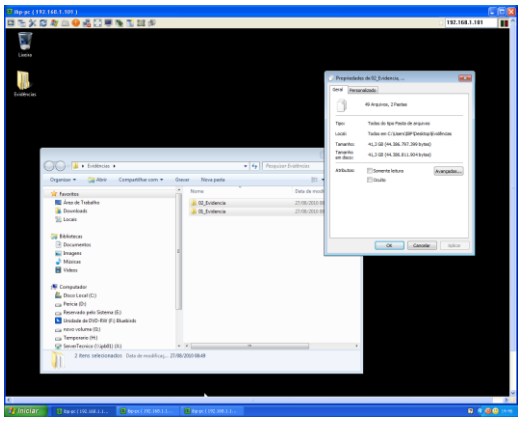

Figura 43. Perito verifica imagem forense recebida no WebLab Server

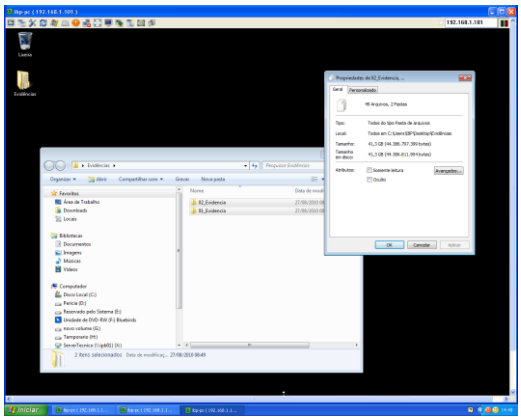

Figura 44. Juiz fiscaliza a verificação da imagem pelo perito

Tendo concluído a transferência das imagens desde o equipamento Solo 4 até o WebLab Server, o perito atuando ainda remotamente cria uma máquina virtual Linux Debian 5 que servirá de recipiente específico e isolado para o caso em perícia (Figura 45), ou seja, para cada processo gera-se uma máquina virtual que acomoda as evidências coletadas e constitui um ambiente de trabalho conjunto e interativo (*groupware*) para o grupo específico, com perito, juiz, delegado, oficial de justiça, escrevente, assistentes técnicos, advogados etc.

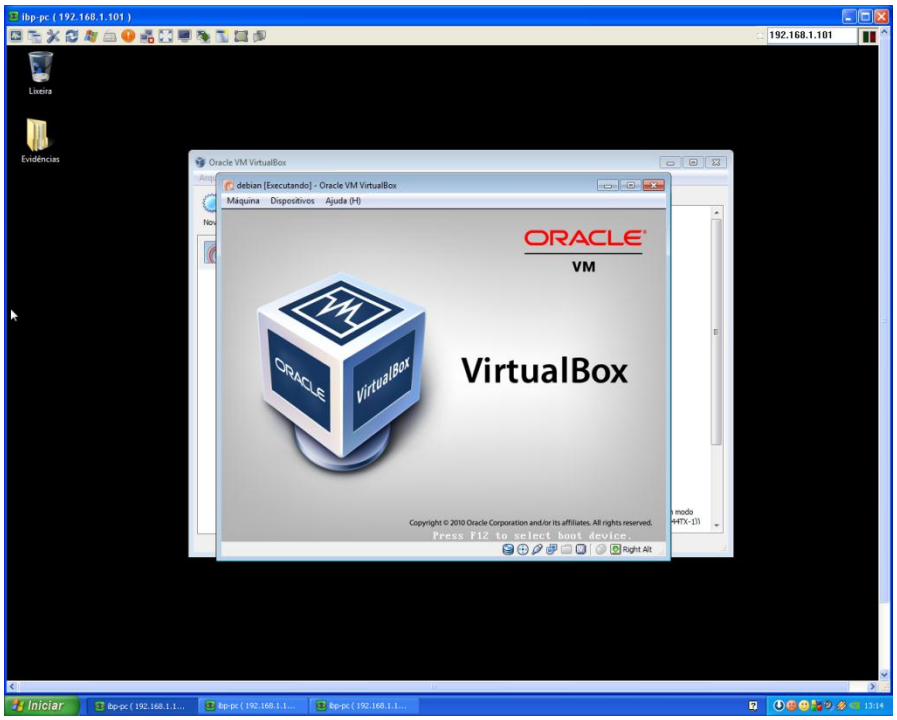

Figura 45. Perito cria máquina virtual no WebLab Server para o processo judicial

O delegado (Figura 46) e o juiz (Figura 47) supervisionam remotamente as ações do perito.

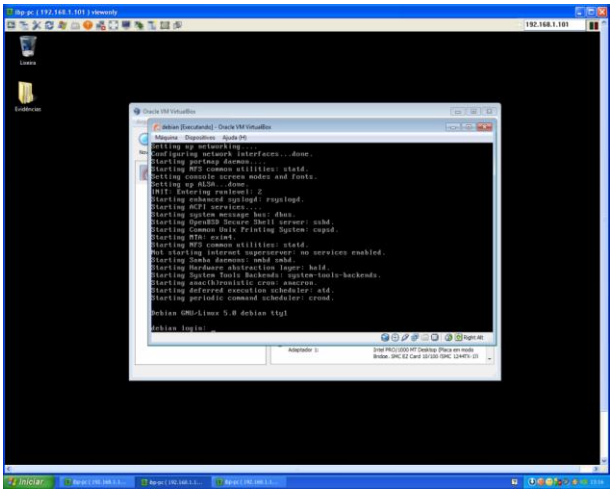

Figura 46. Delegado fiscaliza criação da máquina virtual para o processo

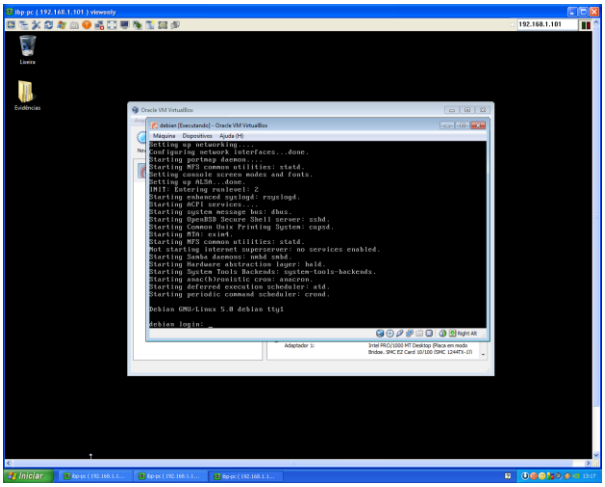

Figura 47. Juiz fiscaliza criação da máquina virtual para o processo

Como pode ser visto na Figura 48, as evidências foram transferidas para a máquina virtual (demora de cerca de 40 minutos, no experimento), criando um ambiente reservado para os exames do caso específico. As atividades ainda são supervisionadas remotamente pelo delegado e pelo juiz.

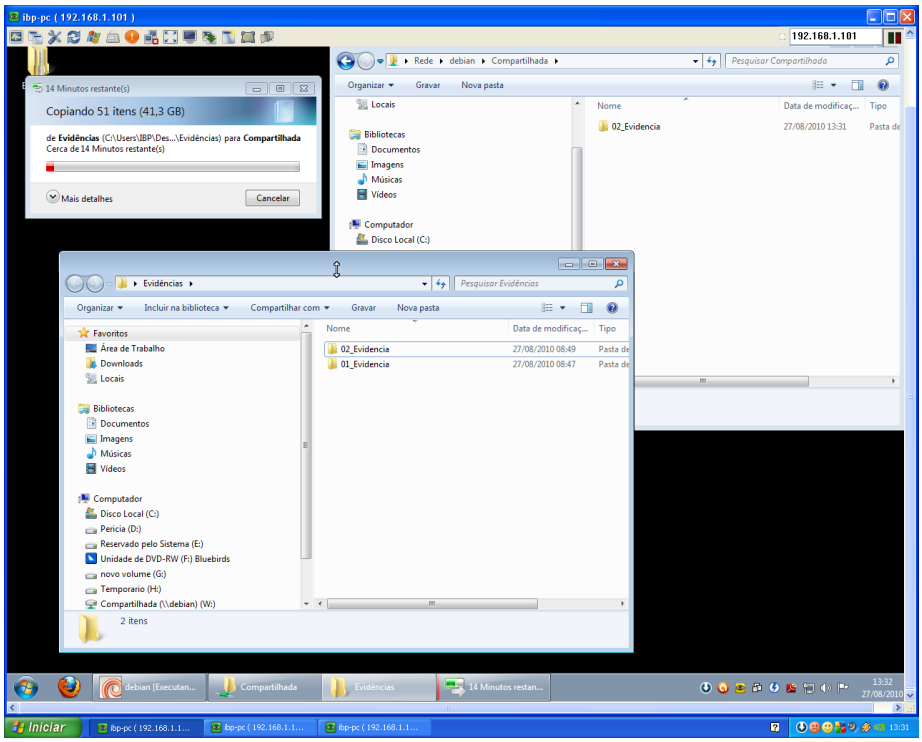

Figura 48. Perito organiza evidências em maquina virtual no WebLab Server

Sob a supervisão remota e contínua do juiz e do delegado, o perito também localizado remotamente inicia o processamento do software de análise forense Autopsy no WebLab Server (Figura 49).

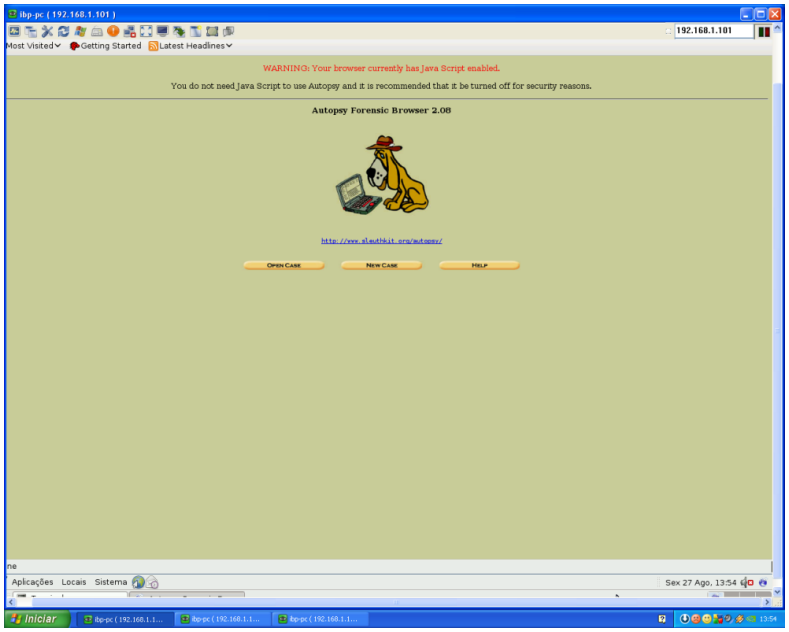

Figura 49. Perito ativa software forense Autopsy no WebLab Server

O perito posicionado remotamente em relação ao WebLab Server, sob a supervisão em tempo real e remota do delegado, do juiz etc., prossegue nos exames realizados na máquina virtual Debian, abrindo as evidências (Figura 50) e examinando seu contéudo (Figura 51).

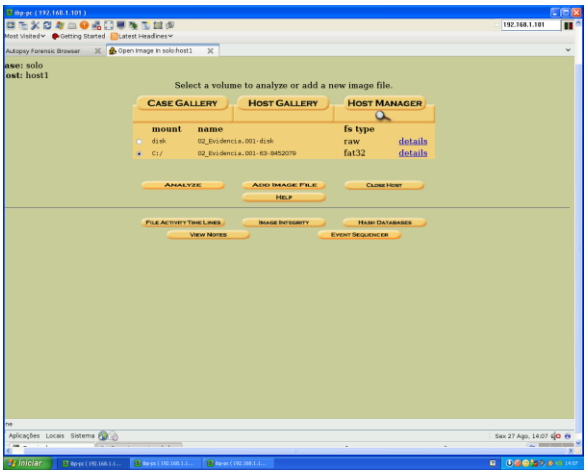

Figura 50. Perito cria o caso e carrega evidências no WebLab Server

Figura 51. Perito examina evidências no WebLab Server

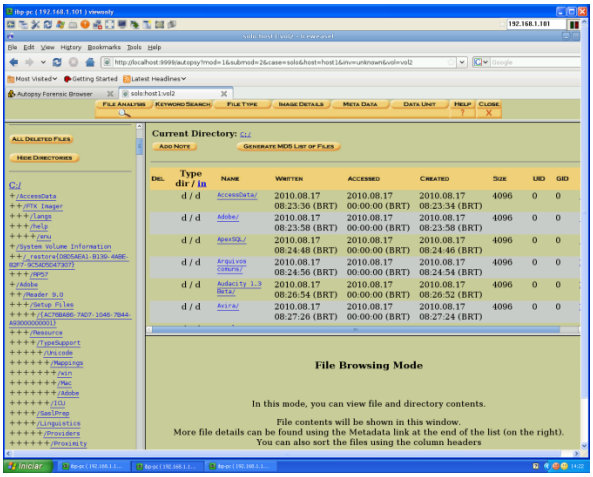

Figura 52. Delegado fiscaliza exame feito pelo perito

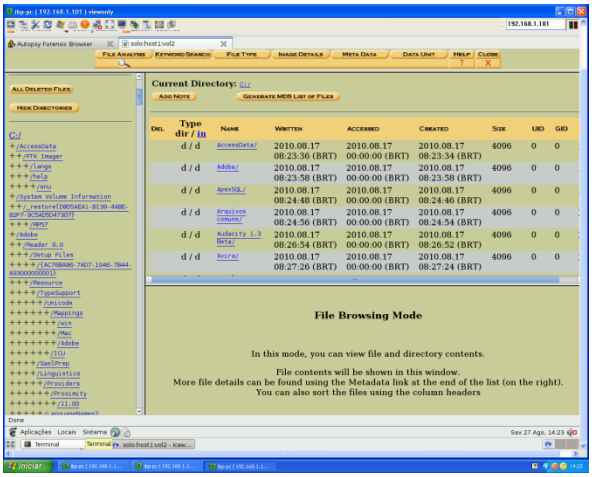

Figura 53. Juiz fiscaliza exame feito pelo perito

O experimento possibilitou verificar na prática a possibilidade e mesmo a flexibilidade da solução. Outras ferramentas forenses mostram-se compatíveis e utilizáveis, como, por exemplo, com as soluções Encase e Forensic Toolkit, que deixam de ser objeto de análise detalhada nesta dissertação pelas questões de licenciamento junto aos fornecedores, ficando a tarefa a ser planejada para experimentos futuros.

Os procedimentos para captura remota via Solo 4, transferência da imagem forense para o WebLab Server e análise via Autopsy mostraram-se muito similares àqueles que seriam realizados presencialmente junto ao disco rígido original, especialmente porque em todos os passos foi utilizada interface gráfica, a qual naturalmente padroniza eventos e ações. A principal diferença está relacionada ao tempo de transmissão de dados, fator que deverá ser mais bem estudado em experimentos

futuros mais completos, considerando por um lado o aumento progressivo das velocidades de transmissão das redes e por outro lado o aumento na capacidade de armazenamento dos sistemas eletrônicos digitais a examinar. De qualquer modo, considera-se a solução em princípio vantajosa se for comparada com o transporte físico de evidências a partir de comarcas distantes dos grandes centros, foco do presente trabalho.

4.4 RESULTADO DA PROVA DE CONCEITO

A prova de conceito mostrou que, em princípio, é viável a integração de ferramentas forenses com o objetivo de montar estruturas evolutivas de WebLabs Forenses a serem acessadas em comarcas distantes dos grandes laboratórios forenses, porém uma avaliação mais profunda depende de experimentos futuros mais completos. Foi possível verificar, ainda, que os laboratórios forenses podem ser operados remotamente a partir de interfaces gráficas acionadas à distância, maximizando seu usufruto e compartilhamento, além de ter-se verificado que os procedimentos podem ser fiscalizados remotamente, pelas diversas pessoas e autoridades interessadas ou envolvidas no processo, independentemente da sua localização geográfica.

Nesse sentido, verificou-se preliminarmente ser possível e válido avançar no estudo de WebLabs Forenses com o objetivo de proporcionar maior transparência e embasamento nas decisões judiciais e suportar um exame mais racional e científico das evidências digitais.

O modelo que foi utilizado na prova de conceito, mesmo sendo elementar e carente de quase todas as funcionalidades afeitas a um WebLab efetivamente operacional, mostrou-se potencialmente útil para permitir a juízes, delegados, advogados e partes acompanharem remotamente os detalhes dos exames realizados.

O experimento indicou, também que os projetos de WebLabs Forenses deverão contemplar tanto o reconhecimento seguro das pessoas que tiverem acesso ao ambiente físico ou virtual, assim como o reconhecimento seguro de todos os dispositivos que forem conectados a esse ambiente, além de cuidar da sua cadeia de custódia física e digital.

Como vimos na prova de conceito, conseguiu-se com grande facilidade a conexão remota do equipamento forense Solo 4 com o ambiente que simulou o WebLab Server. Essa é uma vantagem, mas pode ser também uma severa questão de segurança, se os equipamentos do laboratório puderem ser conectados ou substituídos sem o devido controle dos administradores, peritos e autoridades responsáveis pela produção e fiscalização de provas. Por esse motivo, os exames realizados indicam fortemente que todos os recursos utilizados em WebLabs Forenses devem ser continuamente identificados e autenticados por meio de certificados digitais.

Nesse mesmo sentido, verificou-se que deve caber aos WebLabs Forenses o papel de garantidores centrais da cadeia de custódia, isto é, deve haver grande segurança na geração, preservação e análise de *logs* e demais registros gerados automaticamente sobre a conexão, captura, armazenamento, cópia, modificação, distribuição e destruição de qualquer componente. Esses registros demonstraram-se essenciais para a validade da adoção de laboratórios remotos. No experimento realizado constatou-se que tanto o software forense Autopsy, quanto o laboratório forense Solo 4, geram e mantêm *logs* suas próprias atividades. Porém, ambas não podem ser consideradas suficientes diante do ambiente mais amplo proporcionado pelos WebLabs. Além disso, a interoperação entre diversos componentes proporcionada pelos WebLabs demanda um nível ainda maior de *logs* como resultado da própria integração e interação de ambientes remotos, necessidade a ser detalhada em futuros estudos e projetos práticos sobre WebLabs Forenses.

Finalmente, durante a realização da prova de conceito surgiram comparações entre o presente experimento e os debates que ocorrem no Poder Judiciário e na imprensa sobre a utilização da teleconferência em interrogatórios remotos de pessoas encarceradas.

No debate entre as partes favoráveis e as partes contrárias ao uso de teleconferência nos interrogatórios, houve alegações sobre de inconstitucionalidade do método porque violaria o direito à audiência pessoal, o direito à presença do réu, o direito do acusado de comparecer aos atos processuais mesmo quando eles ocorrerem em local diverso e, finalmente, a natureza dialógica do processo acusatório.

Interrogatórios e produção de provas pericias são situações distintas, mas não se pode deixar de considerar que há semelhanças entre ambas quanto à distância geográfica das provas, dos operadores do Direito e das partes no processo.

Se por um lado, o WebLab Forense aumenta a participação e transparência durante os procedimentos periciais, pois traz a tele-presença onde até hoje há apenas a ausência de autoridades ou partes, por outro lado esse mesmo WebLab tende a vulgarizar a tele-presença em detrimento da presença física. Nesse contexto, a prova de conceito indicou que esse tema precisará ser avaliado com profundidade nos próximos trabalhos, inclusive quanto à possibilidade de que o uso de WebLabs Forenses tenha que ser avaliado e até mesmo normatizado pelo Poder Judiciário.

4.5 CONTRIBUIÇÕES E PERSPECTIVAS COM A EVOLUÇÃO DO EXPERIMENTO

O estudo da literatura e o experimento realizado trouxeram diversas contribuições que podem ser aproveitadas em esforços futuros para criação de um WebLab Forense. Mesmo se essa evolução está além deste trabalho, a extensão das contribuições obtidas recomenda que elas sejam descritas em detalhe a seguir e sumarizadas ao final da dissertação.

4.5.1 DA PROVA DE CONCEITO AO WEBLAB FORENSE

Na revisão da literatura realizada neste trabalho, verificou-se a necessidade de identificar novas soluções para tornar possível o atendimento de milhares de comarcas distribuídas por todo o país. Verificou-se, também, que universidades e empresas estão empenhadas em estudar e desenvolver WebLabs em diversas áreas do conhecimento, provendo:

a) laboratórios remotos experimentais;
b) laboratórios remotos para fins educacionais;
c) laboratórios remotos para pesquisa científica;
d) laboratórios remotos para finalidades empresariais ou profissionais.

Conceitos e modelos derivados desses trabalhos foram utilizados na presente dissertação com o objetivo de propor uma possível solução ao problema inicial, na

forma de um modelo muito simples de WebLab Forense voltado ao exame de sistemas eletrônicos digitais. Esse modelo foi avaliado por meio de uma prova de conceito que consistiu na coleta e análise remota do conteúdo de um disco rígido de computador.

Nesse experimento foram cumpridos os objetivos centrais do presente trabalho, mostrando, em síntese, que é possível e adequado utilizar conceitos derivados de WebLabs para apoiar a coleta e análise pericial forense remota e o acompanhamento remoto desses procedimentos com o objetivo de melhorar qualidade, velocidade e fiscalização dos trabalhos periciais, especialmente para atender comarcas mais distantes dos grandes centros econômicos e tecnológicos.

Os resultados positivos obtidos sugerem que devem ser realizados trabalhos futuros para aprofundar essa matéria e implementar um WebLab Forense efetivo, contudo esse esforço se situa além do presente trabalho, pelo tempo requerido, complexidade envolvida e recursos necessários.

O WebLabs Forense proposto poderia atender, ainda em nível experimental, alguma comarca distante proporcionando-lhe acesso remoto a laboratório forense moderno situado em uma universidade ou centro de pesquisa.

Dependendo dos resultados, o experimento poderia ir sendo ampliado progressivamente, estendendo o uso do WebLab Forense a outros municípios brasileiros e integrando outros laboratórios e novos tipos de exames periciais.

Os itens a seguir detalham a aplicação dos resultados do estudo de caso com o objetivo de contribuir com experimentos futuros para a montagem um WebLab Forense.

4.5.2 CADEIA DE CUSTÓDIA

Os estudos realizados mostraram que WebLabs Forenses para a investigação de sistemas eletrônicos digitais exigem o estabelecimento de cadeias de custódia abrangentes, detalhadas e confiáveis, destacando-se dois requerimentos principais:

a) O primeiro requerimento é que WebLabs Forenses somente podem operar se dotados de funções eficazes para controle detalhado e automático da cadeia de custódia das provas digitais. Esse objetivo é aderente à meta de melhorar

a qualidade e os resultados dos procedimentos periciais em todo o país. Os vestígios digitais examinados nos WebLabs Forenses devem ser certificados quanto à sua origem, dando-lhe a credibilidade necessária para fundamentar laudos periciais e as decisões da Justiça. Essa certificação deve começar no local do crime ou em qualquer outro lugar onde os vestígios são coletados, e prosseguir controlando toda e qualquer movimentação que possa ocorrer com o material coletado até o seu descarte final pela Justiça. A cadeia de custódia deve, ainda, incorporar indicadores seguros sobre os acessos e movimentos realizados e sobre a confiabilidade e qualidade dos exames realizados, possibilitando a validação em tempo real ou posterior dos procedimentos realizados e a confirmação dos resultados obtidos. Em síntese, a cadeia de custódia digital deve registrar e manter automaticamente um leque de indicadores de qualidade sobre todo o ciclo de vida das evidências.

b) O segundo requerimento refere-se à segurança e integridade do próprio WebLab Forense. Assim, a cadeia de custódia das múltiplas evidências digitais deve integrar-se ao controle de segurança do próprio WebLab Forenses e dos demais laboratórios a ele conectados, diante do risco de que os próprios recursos dos WebLabs Forenses possam ser utilizados para fins ilícitos. O objetivo, em termos simples, é ter-se trilha de auditoria dos recursos técnicos e humanos que os WebLabs Forenses colocarão à disposição de milhares de comarcas de todo o país, especialmente frente ao risco de que os próprios laboratórios possam ser utilizados para explorar vulnerabilidades de produtos, violar sigilos, realizar ataques, criar falsas evidências ou destruir ou adulterar evidências verdadeiras. Essa estrutura laboratorial sofisticada e acessível remotamente poderia em tese ser indevidamente utilizada diretamente na prática de ilícitos, como ocorreria se um microscópio eletrônico ou um supercomputador do WebLab Forense fosse utilizado para adulterar ou violar um cartão inteligente com fins criminosos. Há ainda situações nas quais a estrutura de um WebLab Forense poderia ser utilizada para ações indevidas de engenharia reversa, violação de direitos autorais ou furto de segredos industriais.

O princípio da igualdade processual entre as partes é um dever do Juiz. No âmbito deste trabalho, o dever da igualdade processual impõe preservar evidências digitais

contra quaisquer possíveis adulterações ou violações e, ainda, proporcionar aos operadores do Direito e às partes o acesso simétrico às evidências, garantindo-lhes equilíbrio no exercício do contraditório, mantendo-se assim o equilíbrio na análise das evidências digitais e seu uso como fundamento para convencimento do Magistrado.

Nesse contexto, a cadeia de custódia assume papel fundamental como elemento de mensuração da integridade das evidências digitais e de avaliação do equilíbrio no acesso às evidências e aos exames pelas diversas partes no processo.

Em termos gerais, pode-se dizer que a cadeia de custódia deve ser aplicada tanto nos locais externos como naqueles internos ao laboratório pericial. O principal local externo é a cena do crime, onde a cadeia de custódia visa à identificação do próprio local, dos vestígios ali encontrados, dos eventos ocorridos e das pessoas que interagiram com esse material, culminando com sua coleta e transporte ao laboratório pericial.

Nos locais internos do laboratório forense, a cadeia de custódia registra a chegada dos vestígios e todo seu manuseio e armazenamento até a disposição final a critério da Justiça.

Esse é um modelo simplificado e absolutamente genérico mais voltado à esfera criminal. Nos processos reais há inúmeras variantes, por exemplo, nos âmbitos cível, da família e trabalhista é comum a nomeação de peritos judiciais em vez de peritos oficiais lotados nos institutos de criminalística. Uma grande alteração do fluxo está no fato de peritos judiciais geralmente examinarem as peças coletadas não em institutos de criminalística, ambiente pelo menos em tese controlado, mas em suas próprias residências. As residências ou escritórios dos peritos judiciais não podem ser considerados ambientes controlados e seguros à luz das normas e melhores práticas da segurança da informação, motivo pelo qual entende-se que a cadeia de custódia do WebLab Forense deve alcançar as evidências mesmo enquanto elas estiverem na residência ou escritório do perito judicial. Melhor ainda, se tais evidências estiverem custodiadas dentro do WebLab Forense e o perito utilizar as ferramentas forenses remotamente, a partir da residência ou escritório.

Outro risco nos procedimentos atuais está em que as peças digitais coletadas no local dos fatos são transportadas fisicamente até a delegacia de polícia, até a polícia

científica, aos tribunais ou ao escritório do perito. Essa movimentação física, algumas vezes por longas distâncias, por longo tempo e sem os devidos cuidados, traz vulnerabilidades e riscos, como quedas de HDs, desaparecimento de computadores ou memórias, adulterações, cópias não autorizadas etc.

Outra questão refere-se aos chamados depósitos judiciais, onde muitas vezes as evidências digitais ficam por meses ou anos, sendo sabido que quase sempre essas unidades são carentes de recursos mínimos até mesmo para o transporte e armazenamento adequados de um simples microcomputador, em alguns casos ficam empilhados, sujeitos a humidade e sem vigilância efetiva.

Mais recentemente, a Polícia Federal e algumas Polícias Estaduais adotaram as Centrais de Custódia de Provas (CCP), depósitos mais modernos projetados para armazenar com segurança os vestígios, contraprovas e demais objetos apreendidos, restringido seu acesso apenas às autoridades e às partes interessadas e autorizadas, com o objetivo de garantir sua clara identificação e a proteção da integridade, além da manutenção de um histórico detalhado sobre sua movimentação.

Além disso, os organismos policiais adotam cada vez mais métodos periciais forenses com o objetivo de evitar manipulação inadvertida das evidências e aprimorar o registro da cadeira de custódia como meio de reduzir a impugnação das evidências pelas partes e pela sociedade.

Mesmo se a criação das Centrais de Custódia de Provas e a adoção de melhores métodos periciais têm contribuído para reduzir a perda ou contestação das evidências, ocorre que os atuais procedimentos ainda mantêm as partes e os próprios operadores do Direito muito alijados da produção e da custódia das provas digitais, não havendo certeza efetiva da sua integridade e do pelo e efetivo exercício do princípio do contraditório. Verifica-se que a cadeia de custódia acaba sendo preterida e substituída por algum grau de confiança na figura do perito e nos métodos periciais, a que nem sempre deve ser aceito como isento de riscos.

O presente trabalho concluiu que a criação de WebLabs Forenses contribui com os esforços para reduzir esse problema, ao melhorar a interação das partes e dos operadores do direito com as evidências digitais e fortalecer a cadeia de custódia.

Os diagramas a seguir confrontam a realidade atual e o modelo proposto, demonstrando alguns dos benefícios do segundo modelo.

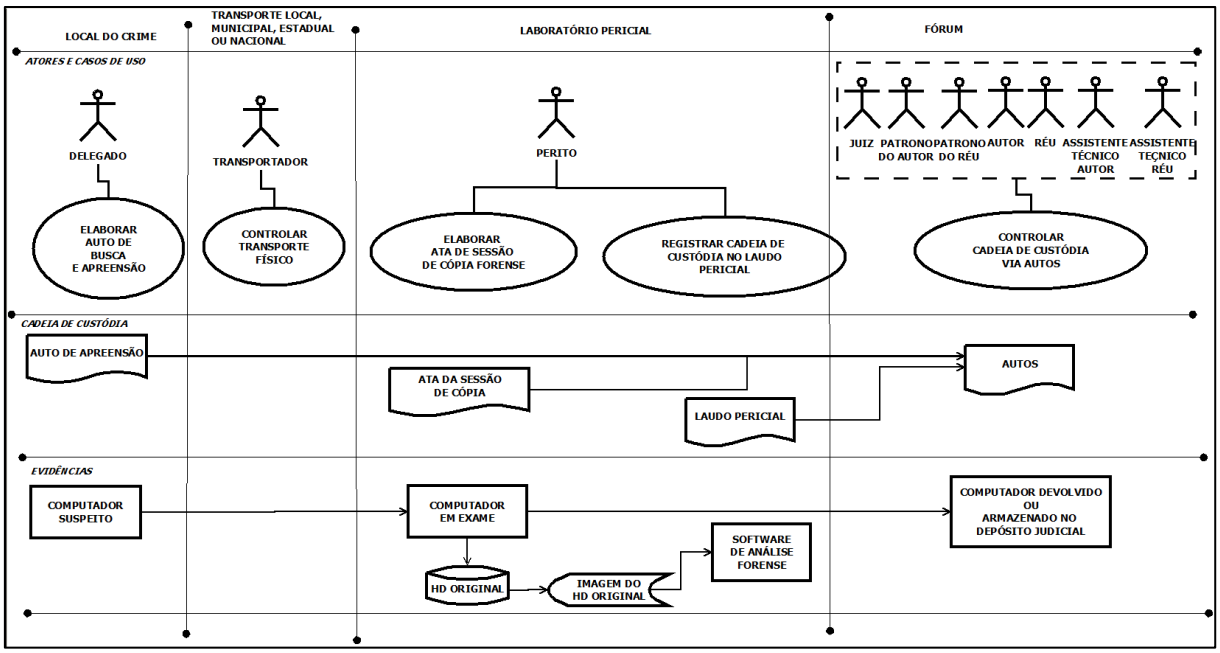

Figura 54. Cadeia de custódia atual[16]

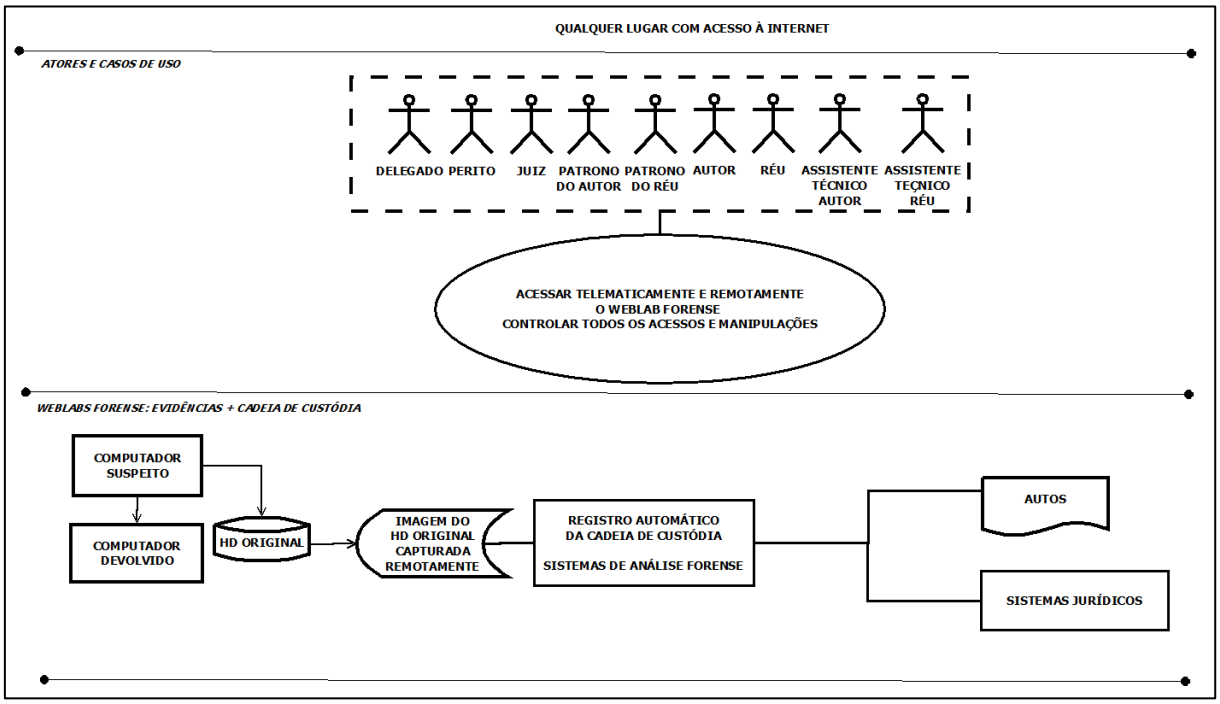

Figura 55. Cadeia de custódia com WebLab Forense

[16] Diagramas simplificados, em formato livre adaptado pelo autor.

Os diagramas ilustram a substituição do transporte físico de evidências digitais desde o local dos fatos até o laboratório pericial, adotando-se em seu lugar a captura remota de evidências digitais. Com isso, o material digital deixa de ser transportado e armazenado fisicamente em locais nem sempre adequadamente controlados e passiveis de ações inadvertidas ou indevidas, em seu lugar passa a haver a coleta eletrônica segura e a transmissão telemática por canais cifrados e com acesso autenticado.

As mídias encontradas no próprio local do crime ou em lugares a ele relacionados, como CD/DVDs, memórias flash, HD ou celulares, são atualmente considerados material físico objeto de apreensão, pois esse material é considerado a origem das provas a serem produzidas. No modelo proposto, o objeto da apreensão passa a ser não mais o equipamento, o hardware em si, mas apenas os dados nele contidos. Com isso, a produção da prova digital passa a envolver a desmaterialização da peça pericial original no sentido de que apenas os dados armazenados são capturados e transformados em fluxo de dados conduzido até seu novo armazenamento em uma central de custódia gerida dentro do WebLab Forense. Em certo sentido também o hardware é desmaterializado e capturado mediante fotografias e programas de inventário que auditam o hardware e incorporam os dados sobre sua especificação e configuração aos resultados na coleta.

Outra mudança relevante é que com o WebLab Forense os operadores do Direito passam a interagir diretamente e remotamente com as evidências, podendo controlar em qualquer momento os procedimentos realizados por autoridades ou peritos. Isso significa que o modelo proposto aperfeiçoa a cadeia de custódia por agregar novos pontos de controle que vão bem além da simples escrita de uma ata de apreensão e cálculo de código *hash*. Mesmo se o cálculo do código *hash* é seguro sob o ponto de vista da matemática, o mesmo não se pode afirmar quanto aos procedimentos que lhe são periféricos, como a seleção das mídias que serão ou não apreendidos, a escolha dos procedimentos e objetos envolvidos no cálculo do *hash*, a forma como é feito o registro do seu resultado do cálculo e o posterior ciclo de vida das evidências, apenas para mencionar alguns exemplos.

Além dos benefícios decorrentes da maior disponibilidade de laboratórios forenses, mais eficientes e com maior disponibilidade geográfica, os operadores do direito passam a poder interagir e fiscalizar todos os procedimentos relacionados à

produção da prova desde o primeiro momento em que é determinada a vistoria policial ou pericial. Esse registro automático da cadeia de custódia prossegue com o objetivo de assegurar que todos os acesso e modificações nas peças sejam devidamente registrados e controlados.

O novo modelo sugerido é apropriado para a adoção de Centrais de Custódia de Provas Digitais, uma vez que o material coletado eletronicamente a partir da cena do crime passa a integrar automaticamente alguma Central Custódia Digital.

Diante dessas questões, considera-se que a definição e implantação de sistemas eficazes para controle da cadeia de custódia digital é uma das tarefas mais relevantes a ser planejada para os trabalhos futuros, proporcionando uma segura trilha de auditoria sobre os WebLabs Forenses e as evidências digitais.

Sugere-se ainda que um dos próximos estudos priorize a definição de uma taxonomia comum e normas nacionais para desenvolvimento e certificação dos WebLabs Forenses com foco especial na qualidade da cadeia de custódia digital distribuída geograficamente.

Nesse estudo deve ser prevista a verificação da aderência de cada laboratório às normas mediante auditorias e monitoramentos sobre os controles da cadeia de custódia individual de cada dispositivo interligado e da rede de WebLabs Forenses.

Sugere-se ainda que os estudos futuros abordem a revisão das normas sobre as responsabilidades de autoridades, peritos, partes e população em geral que interagem com provas digitais em todas as fases dos processos, desde o primeiro atendimento em cenas de crime até o descarte final da evidências pela Justiça.

4.5.3 CENTRAIS DE COLETA

O WebLab Forense proposto prevê a coleta remota dos vestígios digitais a partir do local dos fatos, dados esse que serão em seguida transmitidos para a central de custódia do WebLab.

Contudo, considera-se que especialmente durante o primeiro ou primeiros anos de operação os peritos prefiram deslocar-se fisicamente até o WebLab Forense para ali realizar a coleta local das evidências digitais, em detrimento da coleta remota.

Nesse sentido, entende-se que os próximos estudos devem avaliar a possibilidade e conveniência de instituir postos remotos de coleta, constituindo uma abordagem intermediária entre a coleta a partir do local do crime e, no outro extremo, a manutenção do equipamento sob a responsabilidade do perito.

Outra variante a ser avaliada é considerar que os próprios peritos criminais ou judiciais podem assumir o papel de pontos remotos de coleta, fazendo uso dos seus próprios equipamentos.

4.5.4 CENTRAIS DE CUSTÓDIA

Atualmente, os dispositivos eletrônicos envolvidos em ilícitos são apreendidos ou submetidos voluntariamente pelos seus proprietários e em seguida encaminhados ao laboratório pericial para os exames técnicos. Posteriormente, são encaminhados a depósitos judiciais ou devolvidos aos proprietários. Nesse trajeto, frequentemente os equipamentos são transportados e armazenados em condições impróprias, pondo em risco a preservação dos dados contidos frente às condições ambientais a possíveis procedimentos inadvertidos ou indevidos.

Devido a esses riscos, a Polícia Federal e algumas Polícias Estaduais têm instituído Centrais de Custódia de Provas (CPP), órgãos especializados em recepcionar, controlar e proteger os corpos de delito e demais peças relevantes como provas em processos judiciais.

Com o WebLab Forense proposto, deixa-se de apreender fisicamente os equipamentos para, em seu lugar, apreender-se uma cópia dos dados contidos nesses dispositivos. No modelo proposto perde relevância a custódia física dos equipamentos físico, privilegiando-se em seu lugar a custódia das evidências digitais.

Assim, cabe aos WebLabs Forenses manter Centros de Custódia de Provas Digitais, constituídos na forma de repositórios digitais que alimentam as operações dos WebLabs, possibilitando seu acesso controlado pelos operadores do Direito e pelas partes. Considerando a existência de um período de migração, entende-se que essa central de custódia digital poderá e provavelmente deverá conviver com a custódia

de dispositivos físicos e até mesmo eventualmente funcionar como centro de captura, isto é, prover a conversão de mídias físicas em clones ou imagens digitais.

4.5.5 SEGURANÇA DO SISTEMA

Um dos grandes desafios para qualquer WebLab Forense é o quesito segurança, tendo em vista que os dados armazenados e processados nesse sistema são críticos nas decisões judiciais. A preocupação com a segurança agrava-se pelo fato do sistema ser geograficamente disperso e os usuários não necessariamente se conhecerem ou conviverem.

Diante de fatores como esses, os estudos realizados sugerem que o projeto de um WebLabs Forense tenha como uma de suas prioridades a definição de infraestrutura que incorpore as funcionalidades típicas em instalações de alto risco, à semelhança dos recursos de segurança que estão sendo adotados atualmente em projetos de *cloud computing*[17].

Nesse sentido, o estudo realizado indica que a análise de segurança dos WebLabs forenses tende a apresentar semelhanças com a análise de risco em um ambiente *cloud*, sugerindo-se que essa linha seja melhor avaliada em trabalhos futuros. As semelhanças de ambos os modelos estão associadas à existência de áreas e funções públicas, privadas, de comunidade e mistas, de forma que se assemelha ao modelo de risco previsto pelo NIST para *cloud computing*, considerando como críticas nas implementações práticas as questões de governança, gestão de riscos, *compliance*, auditoria, garantia de continuidade, respostas a incidentes, criptografia, gestão de senhas, identificação de usuários, controle de acesso, segurança da aplicação e dados, segurança na comunicação, interoperabilidade, além dos aspectos sobre segurança presentes na Tecnologia da Informação tradicional.

Recomenda-se que os trabalhos futuros busquem definir essa arquitetura tendo presente que os WebLabs Forenses constituem uma interface entre os principais centros de pesquisa, tipicamente universidades e institutos de criminalística, e os operadores do Direito, tornando recomendável a compatibilidade com políticas de

[17] Cloud Security Alliance (https://www.cloudsecurityalliance.org)

segurança e gestão de usuários e chaves criptográficas próprias dessas distintas comunidades.

4.5.6 GESTÃO DO CONHECIMENTO SOBRE MÉTODOS E FERRAMENTAS PERICIAIS

Os estudos realizados indicam que uma rede nacional de WebLabs Forenses poderia e deveria assumir naturalmente papel relevante na gestão do conhecimento sobre métodos e ferramentas periciais. Cada WebLab poderia participar na coleta, organização e compartilhamento de um acervo integrado de conhecimento sobre métodos e melhores práticas para procedimentos periciais. Acoplado a esse serviço, poderia haver um índice nacional de recursos técnicos que indicasse aos interessados, por exemplo, onde estaria disponível um leitor raro para mídias fora de uso, viabilizando assim seu uso pelo laboratório demandante.

4.5.7 TAXONOMIA E PADRÕES PARA WEBLABS FORENSES

Sugere-se que os trabalhos futuros compilem e ofereçam à comunidade acadêmica um esquema taxonômico específico para WebLabs Forenses. Essa taxonomia deve ser base para a propositura de padrões e normas nacionais e internacionais voltadas à construção, integração e operação de WebLabs Forenses.

Sugere-se que essa análise considere um ambiente internacional, por estarem cada vez mais próximos os debates sobre tecnologia realizados nos tribunais brasileiros e aqueles que ocorrem em fóruns de outros países ou mundiais. As questões tecnológicas descolam-se continuamente das fronteiras físicas e jurídicas das nações, pois os limites geopolíticos são continuamente ultrapassados por redes de telecomunicações, sistemas operacionais, estruturas de bancos de dados, software aplicativo e pela internet e seus serviços.

Há exames periciais conduzidos em nível internacional a partir de acordos bilaterais entre organismos polícias dos diversos países. Quando os crimes envolvem vários

países ou são crimes políticos, pode haver cooperação da Interpol, a maior organização policial internacional, com 188 países membros[18].

Existem ainda entidades civis que promovem em nível mundial a proteção de direitos relacionados aos sistemas eletrônicos digitais. A World Intellectual Property Organization (WIPO) atua nas questões envolvendo patentes e, mais recentemente, sobre a resolução mundial de conflitos com nomes de domínios de internet, ambos envolvendo avaliações em contextos arbitral ou judicial[19].

A Business Software Aliance (BSA) é uma entidade que representa os interesses da indústria de Tecnologia da Informação em mais de 80 países mediante o desenvolvimento de políticas e programas nas áreas jurídica e da educação para proteção da propriedade intelectual e apoio ao combate do crime virtual[20].

Com o aumento na demanda de perícias envolvendo alta tecnologia e das questões internacionais tratadas por essas e outras organizações, entende-se que os trabalhos futuros devem ter entre suas metas a criação de esquema taxonômico, normas e padrões para WebLabs Forenses nacionais e internacionais, abrangendo tanto laboratórios específicos para exames em sistemas eletrônicos digitais, quanto aqueles voltados para outras áreas científicas, mas cujos laboratórios utilizem recursos digitais com enfoque e métodos forenses.

Essa postura é vista nos laboratórios que realizam exames de DNA[21], pois aliam às análises médicas os procedimentos tipicamente forenses, como a manutenção de rigorosa cadeia de custódia sobre as peças analisadas e padrões de testes.

O exame forense sobre colapsos em prédios envolve estudos em Engenharia Civil, como simulações e a avaliação de amostras de concreto e ferro, mas incorpora também avaliações digitais em registros remanescentes de sistemas de supervisão predial ou busca de erros em programas CAD, configurando zonas comuns entre os exames típicos de Engenharia Civil e os exames específicos em sistemas eletrônicos digitais.

---

[18] Interpol. Disponivel em: <http://www.interpol.int>. Acesso em: 04 set. 2010.

[19] World Intellectual Property Organization. Disponível em: <http://www.wipo.int>. Acesso em: 04 set. 2010.

[20] Business Software Aliance. Disponível em: <http://www.bsa.org>. Acesso em: 04 set. 2010.

[21] Federal Bureau of Investigations (FBI) – Standards for Forensic DNA Testing Labs. Disponível em: <http://www.fbi.gov/hq/lab/codis/forensic.htm>. Acesso em: 04 set. 2010.

Outra aplicação multidisciplinar está no exame forense de disco rígido criptografado contendo registros de conversa mantida por meio de sistema VoIP, implicando que esse material precisa primeiro ser submetido a laboratório com recursos para a quebra de proteção criptográfica, segundo a um laboratório de engenharia eletrônica para extração da carga útil dos pacotes VoIP e terceiro precisa ser submetido a laboratório especializado em fonética forense para reconhecimento de locutores na carga útil sonora consolidada. Há claro intercâmbio de informações sobre evidências digitais e procedimentos periciais entre os laboratórios.

Os formatos utilizados até hoje para armazenar evidências digitais mostram um nível baixo de padronização, insuficiente diante dos objetivos e potencialidade dos WebLabs Forenses. Em termos gerais, os formatos adotados na prática são conhecidos genericamente como *Electronic Stored Information* (ESI), termo utilizado especialmente nos Estados Unidos (US DISTRICT COURT - MARYLAND, 2006).

O formato aberto mais divulgado contendo metadados é o Advanced Forensic Format (AFF), enquanto que o formato proprietário mais utilizado é aquele do Encase[22], este proveniente do formato Expert Witness Compression Format, desenvolvido pela empresa ASR Data.

O software Forensic Toolkit (FTK)[23] utiliza os formatos tradicionais do Encase, SMART ou Saferback, já a família de produtos ProDiscover[24] utiliza um formato próprio. O software PyFlag utiliza variante do *gzip* ou formato EWF, o software SMART utiliza *bitstreams* puros ou o formato EWF.

Em síntese, há uma importante diversidade de formatos[25] utilizados pelos softwares forenses, dificultando o exame das evidências em laboratórios distintos e seu acesso remoto e integrado (GARFINKEL et al., 2006, p. 17).

---

[22] Guidance Software. Disponível em: <http://www.guidancesofttware.com>. Acesso em: 03 jun. 2010

[23] Access Data. Disponível em: <http://www.accessdata.com>. Acesso em: 03 jun. 2010

[24] Technology Pathways. Disponível em: <http://www.techpathways.com>. Acesso em: 29 jul. 2010

[25] São distintos os “clones forenses”, criados pela cópia de dispositivo digital em outro idêntico ou similar, e as “imagens forenses” que constituem a coleta do conteúdo de um dispositivo digital gerando um arquivo denominado “imagem”, o qual portanto representa todo o conteúdo do dispositivo digital original. Estes parágrafos referem-se aos formatos de imagens forenses, não aos clones forenses.

Os formatos mais abrangentes de imagem forense são próximos ao modelo genérico mostrado na Figura 56, adaptado de Garfinkel et al. (2006, p, 19).

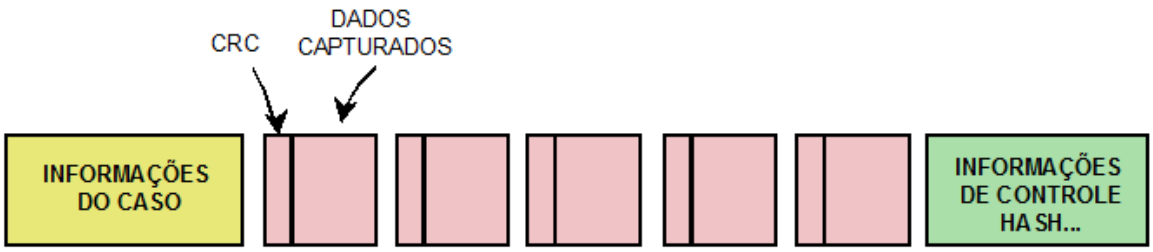

Figura 56. Formato genérico de imagem forense

Nesse formato constam tanto os dados que constituem as evidências digitais, quantos os dados sobre esses dados, portanto os metadados que descrevem e classificam as evidências digitais. As principais funcionalidades dos softwares que utilizam esse tipo de formato são, em síntese (GARFINKEL et al., 2006, p. 22):

a) coleta e armazenamento, com ou sem compreensão, das imagens de dispositivos digitais;
b) armazenamento de imagens com qualquer dimensão, desde imagens de memórias ou assinaturas digitais com apenas poucos bytes, até sistemas distribuídos na ordem de terabytes ou petabytes;
c) armazenamento de metadados, dentro ou separadamente das imagens
d) possibilidade de criação de metadados de interesse do usuário ou específicos do caso;
e) serem extensíveis e multi-plataforma;
f) dotados de recursos internos para verificação de consistência;
g) previsão para certificação de autenticidade mediante códigos *hash* e assinatura digital com base em certificados X.509

Garfinkel *et al.*(2006) analisam a evolução dos formatos forenses, partindo do modelo utilizado pelo programa DD, do sistema operacional Unix, largamente utilizado desde os primórdios dos exames forenses em computadores. Esse programa grava tipicamente um *bitstream*[26] com os dados do dispositivo original, mas não captura dados e metadados descritores do próprio dispositivo capturado e

[26] Literamente, fluxo de bits.

dos procedimentos realizados. Por exemplo, faltam dados como o número de série do disco rígido copiado.

Os autores supramencionados reconhecem que o modelo DD é de largo uso no mundo, mas possui graves limitações por apenas capturar dados e não metadados. Por isso propuseram a criação de um novo programa[27] similar ao DD, mas que colete automaticamente alguns metados, por exemplo sobre o disco rígido.

Adotando uma abordagem similar e partindo dos estudos desta dissertação, sugere-se que estudos futuros avaliem se os formatos atualmente mais utilizados poderiam agregar metadados específicos e comuns entre si e, além disso, adotar recuros para registro e fiscalização de eventos em tempo real e remoto, para que possam ser tratados mais eficazmente em uma rede de WebLabs Forenses.

Nesta dissertação utiliza-se de forma livre os termos metadados ou dados descritores do dispositivo analisado apenas no sentido disntiguí-los dos dados contidos no dispositivo. Assim a lista de clientes contida em um disco é referido como dado, enquanto que o número de série do disco rígido é referido como metadado ou descritor do dispositivo. A melhor conceituação desse elementos não é objeto deste estudo, ficando para trabalhos futuros.

Assim, sugere-se que os próximos trabalhos definam uma estrutura de dados para constituir a cadeia de custódia sobre o que foi coletado pela perícia, se houveram transformações nas evidências digitais e quais pessoas entraram em contato com elas. Sugere-se, ainda, que sejam adotados metados mais abrangentes que constituam, por exemplo, uma trilha de auditoria a qualidade dos dados forenses coletados, registrando eventuais erros na coleta, e dados para classificar o nível de proteção de evidências digitais, como tentativas de acesso indevido.

Alguns produtos de mercado, como o Encase Entreprise, já adotam recursos voltados a esse objetivo, como o módulo SAFE e a adoçaõ de criptografia para proteção das imagens forenses.

O modelo a ser analisado em trabalhos futuros poderia considerar, entre outros elementos, a ordenação sugerida na Figura 57.

---

[27] Os autores denominaram o programa como Advanced Disk Imager.

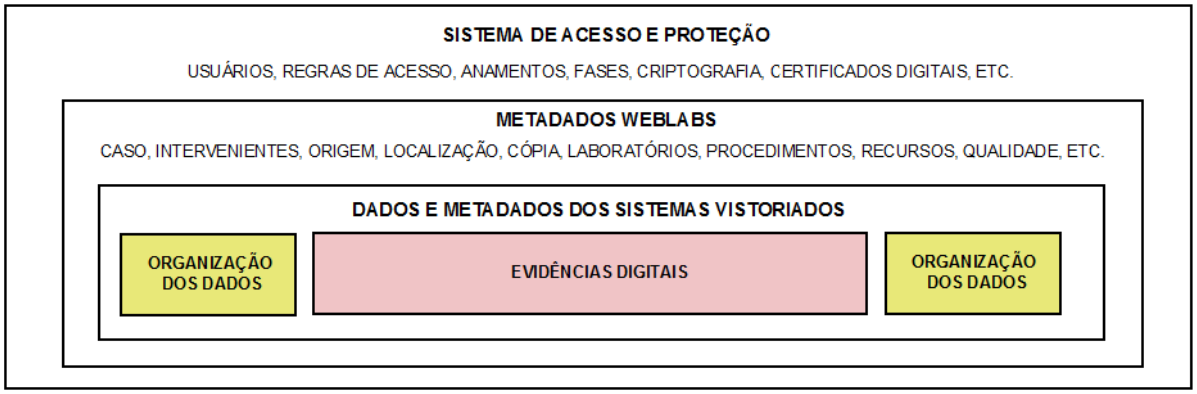

Figura 57. Estrutura de metadados sugerida para WebLab Forense

A adoção de padrões abertos de metadados é ainda mais relevante em aplicações onde há grande heterogeneidade nos dados tratados, com origens diversas e armazenados em formatos diferentes (FERREIRA, 2007, p. 30). Tendo em vista os objetivos dos WebLabs Forenses, os estudos futuros deveriam contemplar a criação ou adoção de um padrão aberto de metadados com elementos comuns aos diversos tipos de laboratórios remotos forenses, preferencilamente baseado em XML, visando sua fácil e rápida integração em redes de WebLabs Forenses. Visando a interoperabilidade dessas redes, o modelo a ser estudado deveria ser independente do esquema e orientado a serviços, possivelmente baseado na tecnologia de *web services*[28], porém tendo a cautela de minimizar a dependência de programas clientes mais complexos, levando ao indesejável afastamento da utilização de um simples navegador para acesso aos Weblabs (FERREIRA, 2007, p. 37). Sugere-se para os trabalhos futuros o estudo de metadados para as funções indicadas no Quadro 3.

Funções	**Estrutura de Dados e Metadados a avaliar em estudos futuros**
Evidências	Sistemas eletrônicos digitais periciados
Procedimentos	Procedimentos periciais realizados.
Intervenientes	Pessoas e usuários que entram em contato, acompanham ou fiscalizam o manuseio de evidências.
Qualidade	Qualidade da imagem forense, indicando existência de

[28] *Web services* ou serviços web são soluções para integração de sistemas cujos recursos são identificados por meio de Uniform Resource Identifier (URI) e definidos com base em documento de descrição XML, utilizados conforme normas organizadas pelo World Wide Web Consortium (W3C), disponível em: <http://www.w3.org/>, e pela Organization for the Advancement of Structured Information Standards (OASIS), disponível em: <http://www.oasis-open.org/>. Acesso em: 18 ago. 2010.

	erros na coleta, diferença de tempo entre os fatos averiguados e a coleta das imagens, falta de dados ou estrutura em relação às evidências originais, contaminação das evidências etc.
Laboratórios	Identificação de WebLabs e Laboratórios.
Localização	Controle de cópias e localização das imagens forenses, incluindo subconjuntos das imagens ou conjuntos de imagens distintas agregadas.
Controle técnico	Controle técnico das imagens, como formato, compactação etc.
Andamento	Controle de prazos, andamentos e objetivos dentro dos processos.
Usuários	Descritores adicionais escolhidos livremente pelos usuários.
Proteção	Recursos técnicos para proteção das evidências e acesso, incluindo criptografia dos dados identificação das evidências, dos laboratórios e das pessoas mediante certificados digitais. Proteção contra ataques e incidentes.
Recursos do sistema	Planejamento de alocação de recursos e uso de evidências, alocação e balanceamento no uso de recursos. Controle de atualizações técnicas e compatibilidade reversa. Controle de pacotes.
Resultados	Controle dos resultados obtidos.

Quadro 3 - Naturezas de metadados a avaliar em estudos futuros

4.5.8 INFRAESTRUTURA PARA WEBLABS FORENSES

A prova de conceito mostrou a utilização de um laboratório forense comercial, o Solo 4, cumprindo funções de laboratório remoto e interagindo com uma estrutura reduzida para compartilhamento de seu acesso.

Nesse contexto, considera-se que devem ser mais profundamente avaliadas as possibilidades tanto de desenvolvimento específico de estruturas para WebLabs Forenses, quanto de aproveitamento de estruturas existentes ou de incorporação de produtos comerciais.

Algumas das soluções disponíveis na literatura científica e técnica são discutidas a seguir no contexto de contribuição para estudos futuros que visem detalhar uma infraestrutura para a construção de WebLabs Forenses.

Em linha de princípio, considera-se que deve ser avaliada a possibilidade de adotar-se uma arquitetura orientada a serviços (SOA), fornecendo padrões para implantação de uma estrutura de aplicações diferentes pouco acopladas entre si.

Deve contemplar os serviços básicos no sentido de prover flexibilidade e escalabilidade, sendo o acesso provido pela tecnologia de *web services*, isto é, baseada em funcionalidades XML que fornecem unidades de trabalho a outros programas via Internet.

Possivelmente, será necessário adotar recursos adicionais que possibilitem a interação com *web services* via navegadores Internet (FERREIRA, 2007, p. 37).

Nesse mesmo sentido, sugere-se que seja projetado para o WebLab Forense um sistema de segurança *web based* que contemple basicamente as funções de autenticação e autorização, a primeira consistindo da identificação do usuário e a segunda na verificação e autorização para tarefas específicas (GUIMARAES et al., 2010, p. 3).

4.5.9 WEBLABS NA UNIVERSIDADE DE SÃO PAULO E A FAPESP

Há diversos estudos e experimentos pioneiros na Universidade de São Paulo (USP) que devem ser utilizados como base para experimentos futuros. Pela grande extensão e profundidade dos trabalhos realizados na USP, não é possível e não é objetivo seu estudo detalhado no presente trabalho.

Deve ser considerado que já em 1996, a Escola Politécnica inovou seu curso de controle de processos utilizando uma malha de ajuste de temperatura para uma planta-piloto multi-propósito com placas de aquisição e sistema supervisório, onde os alunos realizavam distúrbios e efetuavam ajustes em tempo real.

Posteriormente, a escola implantou o WebLab de Controle de Nível, destinado ao estudo de processos da indústria química (GE, 2005).

Figura 58. Esquema da arquitetura do sistema

Figura 59. Planta-piloto do projeto WebLab na USP

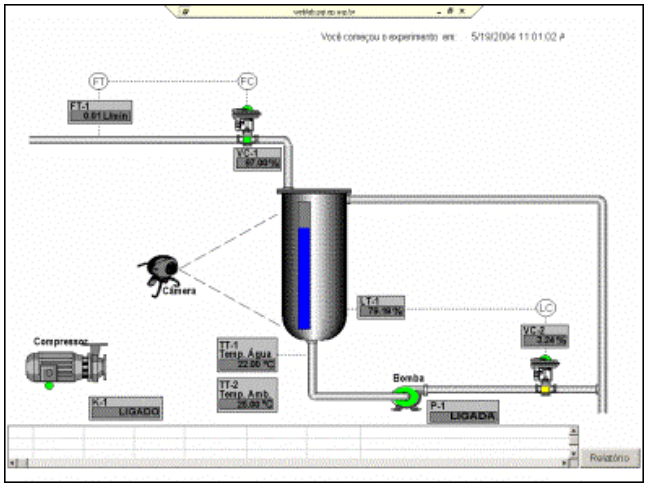

Figura 60. Interface gráfica do processo implementada no sistema supervisório.

Esse experimento pode ser monitorado por câmara digital e os resultados são acompanhados através da internet.

Figura 61. Monitoramento por câmera digital

Figura 62. Tela apresentada ao final do experimento

Posteriormente, o WebLab de Química da Escola Politécnica evoluiu para o Continuous Stirred Tank Reactor (CSTR), dedicado a fins educacionais. Utiliza

tipicamente protocolos TCP/IP e servidores Web (EPUSP QUIMICA, 2008). Esse esforço baseou-se no projeto do MIT, já mencionado, e no Open Course Ware (OCW).

Com a inclusão nos programas da Fapesp, o projeto evoluiu para a montagem de um cluster de WebLabs abrangendo Engenharia Química e Bioquímica da USP e Unicamp, entre outras instituições.

Dentre os programas da FAPESP é de interesse principal para os trabalhos futuros sobre WebLabs Forenses o Programa de Tecnologia da Informação no Desenvolvimento da Internet Avançada (TIDIA), que reúne centenas de pesquisadores dos institutos de pesquisa do Estado de São Paulo. Dentre suas vertentes, destaca-se a KyaTera, uma rede de fibras ópticas que suporta experimentos variados com acessos nos laboratórios a velocidades da ordem de 10 gigabits e superiores. No contexto do programa Tidia e do projeto KyaTera, a Fapesp passou a apoiar grupos de pesquisa experimental em todas as áreas de conhecimento para disponibilizar acesso remoto a WebLabs.

O projeto evoluiu com a inclusão de dezenas de WebLabs cujos laboratórios reais são controlados através da Internet, conforme elencado no site da entidade (FAPESP, 2009):

> WebLabs de Óptica e Fotônica para colaboração eletrônica.
>
> - Mistura de quatro ondas e instabilidade modulacional. Laboratório de Comunicações Ópticas.
> - Análise de Dispersão em Fibras Monomodo e Multimodo. Laboratório de Comunicações Ópticas.
> - Optical testbed to verify effects of filtering and lambda-conversion in MetroNet signals. Lapcom
> - Medida do coeficiente de atenuação de fibras ópticas. Laboratório de Fotônica do Mackenzie
>
> Experimentos de WebLab para ensino de Engenharia Química e Bioquímica.
>
> - Determinação do coeficiente volumétrico de transferência de oxigênio (kLa) em biorreator convencional. LaDABio.
> - Controle de nível num tanque. WebLab de processos químicos e bioquímicos.
> - Processo de transferência de calor em uma barra metálica. Departamento de Química
> - Acesso remoto a métodos cromatográficos para o estudo da catálise. Lepac
> - Processos químicos em alta e baixa pressão. Lepac

WebLabs de serviços ambientais.

- BBB (Big Brother Bee): monitoramento de colmeias de abelhas nativas. ViNCES.
- Estufa: monitoração remota de variáveis ambientais. ViNCES.
- Câmaras de topo aberto: WebLab sobre fotossíntese e absorção de CO2 por plantas. ViNCES.

WebLidar.

- WebLidar. Laboratório de aplicações ambientais a laser.

WebLabs de Robótica.

- Ambiente educativo para a operação remota de um robô manipulador. OPF.
- Remanufatura flexível telecomandada baseada em processamento de imagens. OPF

WebLabs de Medicina.

- WebLab para um banco abrangente de imagens médicas. Incor

4.5.10 MASSACHUSETTS INSTITUTE OF TECHNOLOGY: ILAB REMOTE ONLINE LABORATORIES

A partir dos estudos realizados, considera-se que os futuros trabalhos sobre WebLabs Forenses devem considerar as pesquisas e recursos ofertados pelo MIT, incluindo a estrutura e do código-fonte do projeto “iLab: Remote Online Laboratories”, desenvolvido a partir do ano de 2000 no contexto do projeto iCampus.

Os principais investigadores, o Prof. Steve Lerman e o Prof. Jesús del Alamo tiveram por objetivo desenvolver laboratórios online que pudessem ser utilizados remotamente por estudantes, educadores em ciências e engenheiros para realizar experimentos a qualquer hora e a partir de qualquer lugar, utilizando apenas seus navegadores internet. Em 2005, o iLab já havia sido utilizado em milhares de estudos ao redor do mundo.

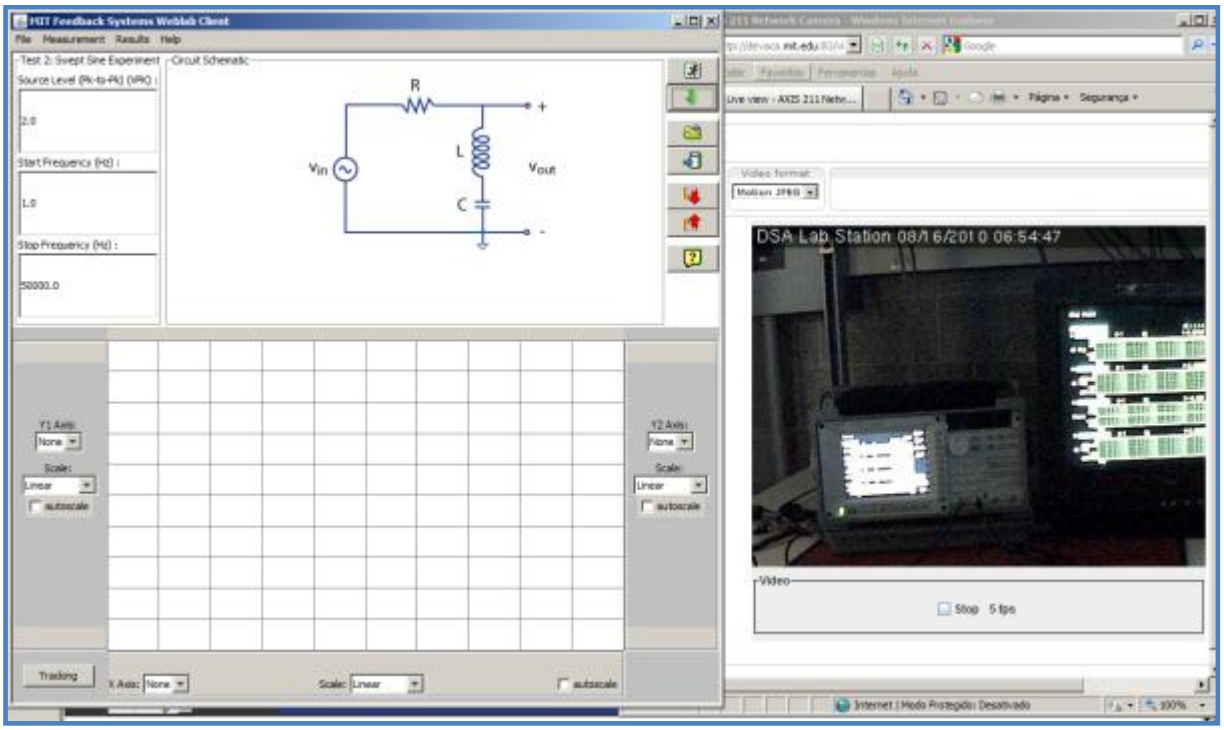

Figura 63. WebLab do MIT visualizado e comandado pelo autor a partir do Brasil.

O grupo do ILabs Project desenvolveu uma suíte de ferramentas de software que possibilita a criação de laboratórios complexos e provê a infraestrutura para seu gerenciamento. Dentre seus objetivos, destacam-se:

- prover laboratórios remotos, minimizando o esforço de desenvolvimento e gestão;
- prover um conjunto comum de serviços e ferramentas de desenvolvimento;
- atender grande quantidade de usuários em escala mundial;
- possibilitar a múltiplas universidades compartilharem seus laboratórios remotos, mesmo que tenham infraestruturas distintas de rede.

A estrutura do iLab baseia-se em um mediador denominado Interactive Service Broker (ISB) que conecta clientes e laboratórios, cuidando também da autenticação e autorização. O módulo é responsável também por administrar protocolos para passar controles e resultados na comunicação entre clientes e laboratórios, proporcionando flexibilidade na escolha de protocolos próprios de comunicação e, com isso, o uso de pacotes próprios de terceiros, como o LabView ou o MatLab, durante o desenvolvimento de WebLabs. Mesmo se esse critério trouxe maior complexidade para o desenvolvimento do iLab, a equipe adotou o recurso para

maximizar os benefícios proporcionados pelo projeto à comunidade científica (HARWARD; JABBOUR; MAO, 2009).

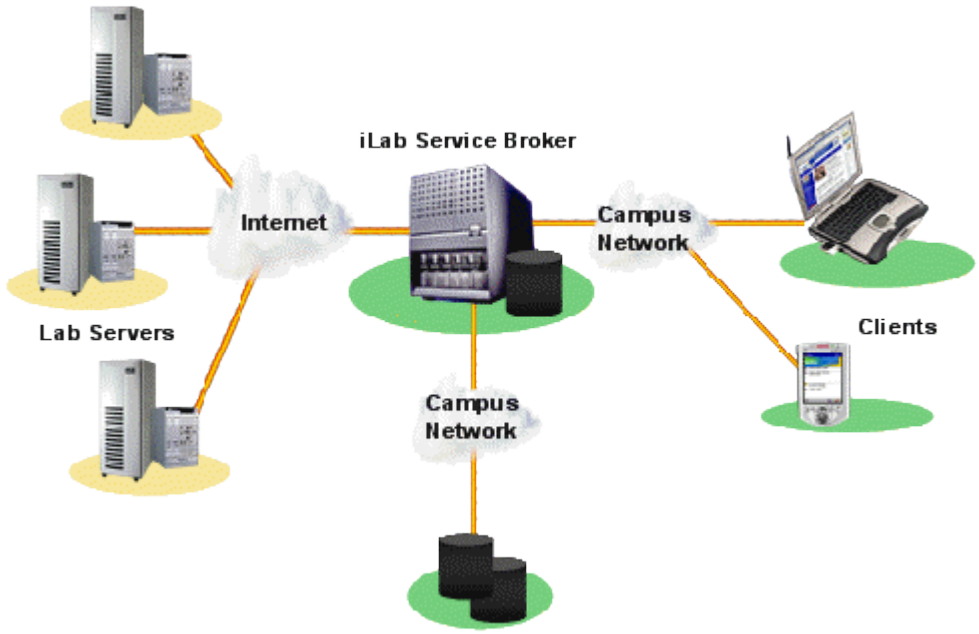

Figura 64. Estrutura do iLab do MIT

Como mostra a Figura 64, o iLab prevê basicamente os seguintes servidores:

- Service Broker (SB)
- Experiment Storage Server (ESS)
- Userside Scheduling Server (USS)
- Labside Scheduling Server (LSS)
- Lab Server (LS)

Durante o presente trabalho, foram feitas verificações preliminares sobre a estrutura e o código-fonte do iLab, contudo sua avaliação no sentido de buscar utilizá-los como base para um experimento relativo ao WebLab Forense deve ser objeto de trabalhos futuros, pois essa atividade demanda tempo e recursos superiores aos disponíveis neste trabalho. Considera-se que o estudo futuro poderá realizar as seguintes atividades preliminares para implantação experimental de um WebLab baseado no recurso do MIT com o objetivo de testar sua aplicabilidade ao tema em análise (DELONG, 2007):

- Interactive Service Broker (Create Virtual Web Site, Create Database, Database Permissions, Database Process Agent scripts, Database Ticketing scripts, Database Interactive Service Broker scripts, Edit Web.Config file, Test service)

- Experiment Storage Server (Create Virtual Web Site, Create Database, Database Permissions, Database Process Agent scripts, Database ESS scripts, Edit Web.Config file, ESS self registration, Test service)
- User-Side Scheduling Service (Create Virtual Web Site, Create Database, Database Permissions, Database Process Agent scripts, Database USS scripts, Edit Web.Config file, USS self registration, Test service)
- Lab-Side Scheduling Service (Create Virtual Web Site, Create Database, Database Permissions, Database Process Agent scripts, Database LSS scripts, Edit Web.Config file, LSS self registration, Test service)
- Laboratories – Iniciar testando o Interactive Time Of Day Server e depois desenvolver e testar aplicação experimental para um WebLab Forense (Create Virtual Web Site, Create Database, Database Permissions, Database Process Agent scripts, Edit Web.Config file, ToD self registration, Test service)

Essa estrutura do MIT foi concebida para ambientes Microsoft Windows, envolvendo instalação e ajuste, como mínimo, de um sistema operacional Windows Server Enterprise, do gerenciador de banco de dados SQL Server e dos ambientes *dot Net* e Visual Studio, conforme indica a documentação do MIT sobre o código-fonte do iLab (DELONG; FELKNOR, 2006).

4.5.11 UNIVERSIDADE DE DEUSTO: WEBLAB DEUSTO

A Universidade de Deusto iniciou em 2001 o projeto de um WebLab com o objetivo de oferecer aos usuários acesso a experimentos remotos obtendo o mesmo nível de experiência proporcionada pelos laboratórios tradicionais. O código-fonte do seu sistema, denominado WebLab-Deusto, é distribuído na modalidade open-source e tem por objetivo prover uma infraestrutura independente do tipo de experimento realizado nos diversos laboratórios interligados. Por esses motivos, ainda que voltado ao ensino, considera-se que esse projeto deve ser avaliado e eventualmente utilizado no desenho de um experimento mais detalhado de WebLab Forense.

O software apoia funções como gestão de usuários e grupos, suas permissões, os experimentos e a interligação entre servidores. Sua arquitetura procura facilitar a integração de experimentos no sentido de deixar essa tarefa o mais transparente possível.

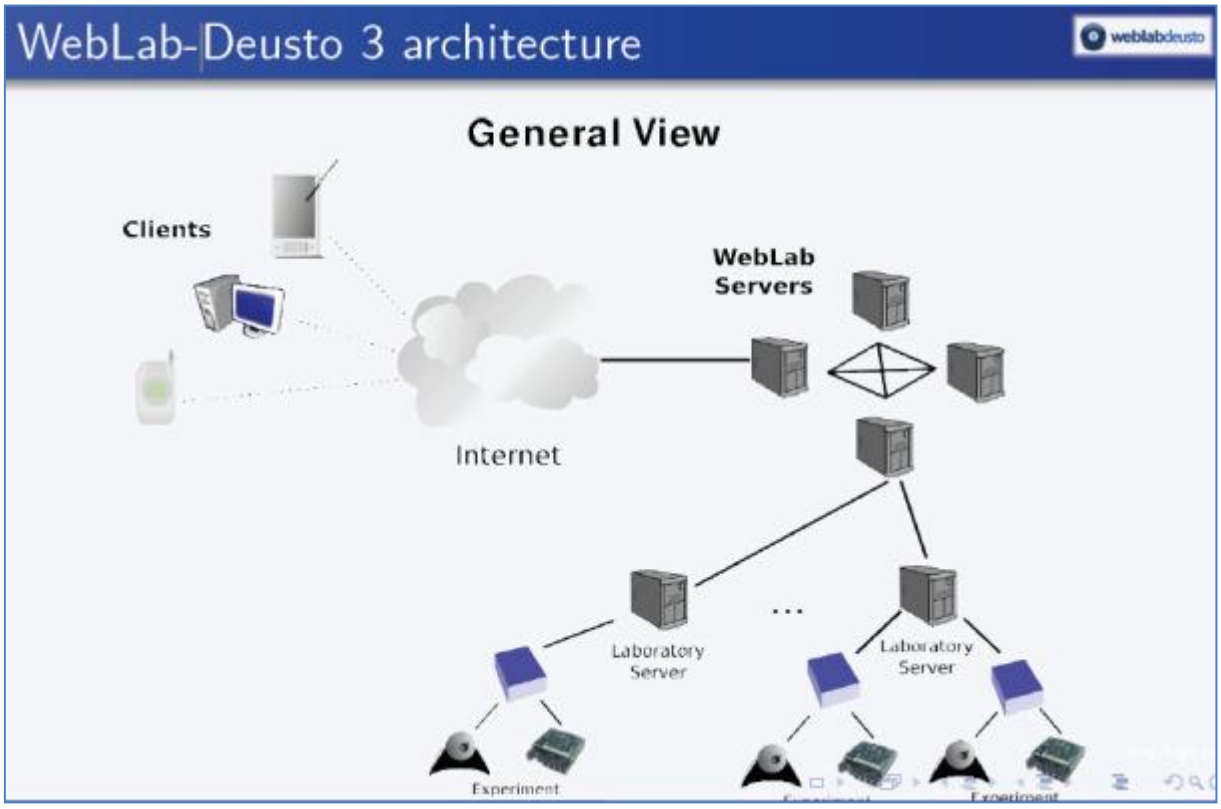

Figura 65. Arquitetura do WebLab-Deusto

No estudo divulgado pela Universidade à comunidade científica constam os protocolos a serem adotados na conexão entre os dispositivos digitais, os servidores de experimentos e a estrutura de WebLabs, orientada a serviços, conforme modelo na Figura 66.

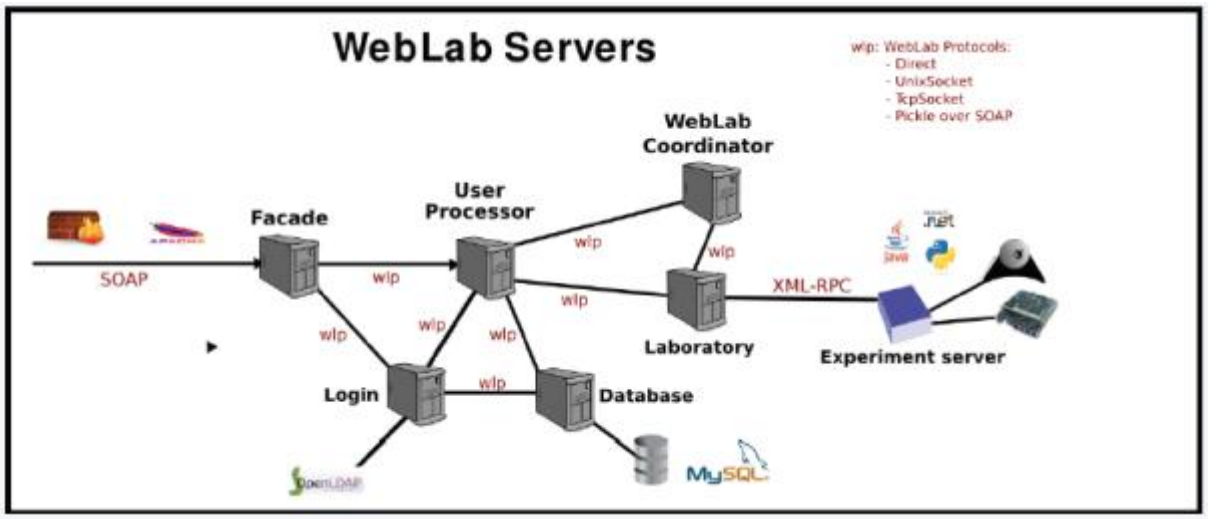

Figura 66. Protocolos e serviços no WebLab Deusto

A Figura 67 detalha a estrutura de protocolos, focada nas transações inter-servidores.

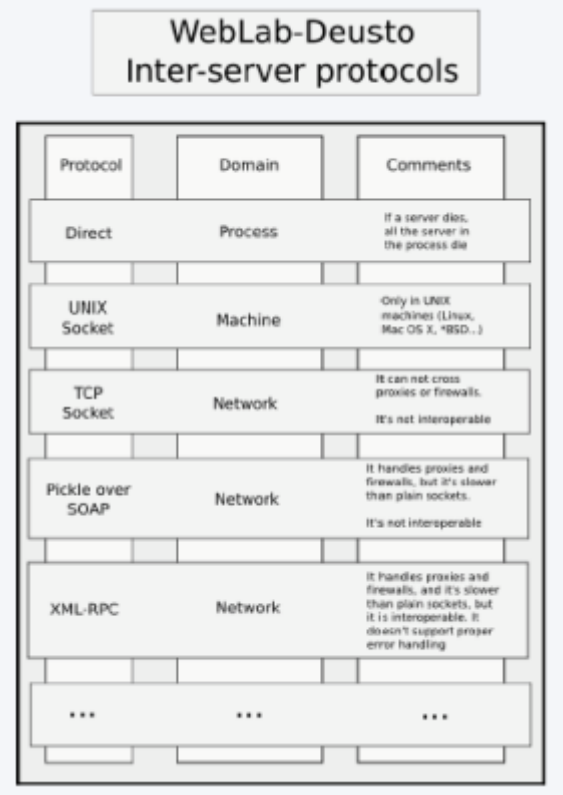

Figura 67. Protocolos inter-servidores no WebLab Deusto

Os pesquisadores esclarecem que a integração de novos experimentos na rede do WebLab Deusto requer somente a escrita de código específico do novo experimento que será introduzido, tendo ampla flexibilidade tanto do lado do cliente quanto do laboratório por utilizar tecnologias como XML-RPC, Java e LabView na estrutura de serviços esquematizada na Figura 68.

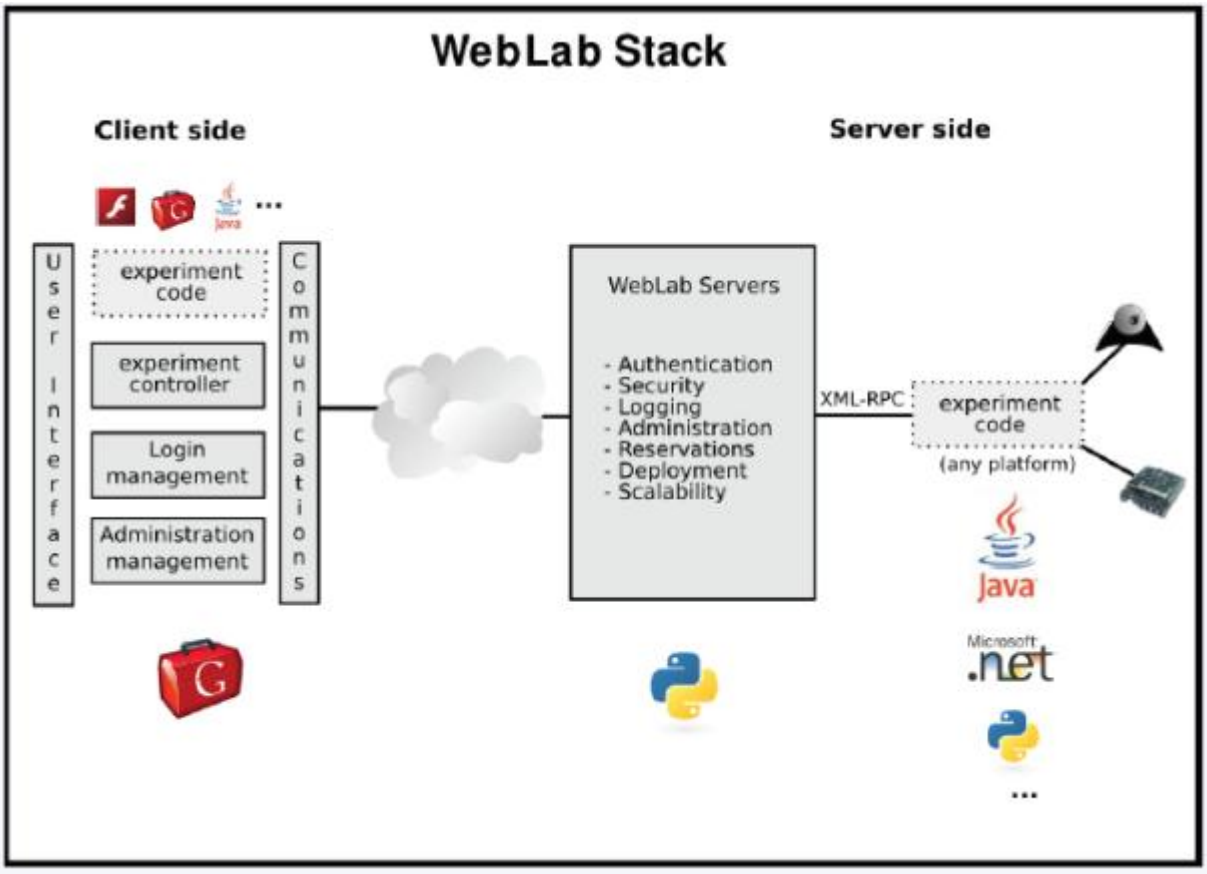

Figura 68. Estrutura de serviços do WebLab Deusto

A estrutura de serviços prevê interações bastante simples nos laboratórios, com comandos como "*Start*", "*Dispose*", "*sendCommand*" e "*sendFile*", entre outros, em um ambiente que utiliza SOAP, XML-RPC e JSON (ORDUÑA, 2009). Esse ambiente se mostra útil para evolução de um WebLab Forense, mas esse conjunto de comandos parece ser insuficiente diante testes realizados durante a prova de conceito.

Dessa maneira, uma das linhas experimentais que pode vir a ser selecionada para os próximos trabalhos consiste na avaliação de uma integração multimídia entre, por exemplo, um equipamento Solo 4 e uma solução experimental derivada do WebLab Deusto e voltada a um ambiente forense.

Os testes iniciais devem considerar a disponibilidade open source do código fonte do WebLab Deusto e podem partir da versão cliente desenvolvida em AJAX com o Google Web Toolkit (GWT). Sugere-se proceder com a customização do código Java, mediante kits específicos de desenvolvimento, e compilação com o GWT para os diferentes navegadores, gerando arquivos ".html" e ".js". Para o servidor escrito em linguagem de programação Python, podem ser analisadas e revistas as funções

de *login* (credenciais dos usuários), núcleo dos servidores (uso, acesso), servidores dos laboratórios (localizados nos laboratórios físicos e interligados aos servidores dos experimentos) e servidores dos experimentos (contém a lógica específica de cada experimento).

4.5.12 LABVIEW

LabView é um produto comercial da National Instruments, integra um amplo conjunto de dispositivos para laboratórios científicos e técnicos. Trata-se de um ambiente de programação gráfica utilizado mundialmente no desenvolvimento de sistemas de mensuração, teste e controle. Como indica a Figura 69, essa solução oferece grande diversidade de funções e ambientes operacionais, o que proporciona a integração da sua interface gráfica de programação com centenas de dispositivos de hardware e bibliotecas de software para criar instrumentação virtual. É a plataforma comercial líder mundial na criação de laboratórios virtuais com recursos de compartilhamento e colaboração remota, inclusive para ambientes acadêmicos e de pesquisa (NATIONAL INSTRUMENTS, 2010).

Operating System	Windows only	Windows, Linux, Mac	Windows, Linux, Mac	Windows only
Programming Environment	●○○	●●○	●●●	●●●
Customize User Interfaces	●●●	●●●	●●●	●●●
Hardware I/O Integration	●●●	●●●	●●●	●●●
Math and Signal Processing	●○○	●●○	●●○	●●●
Read, Write, and Share Data	●○○	●●○	●●○	●●●
Executables and Distribution	●○○	●●○	●●●	●●●
Software and Code Integration	●○○	●●○	●●○	●●●
Compatibility with Add-On Software	●●○	●●●	●●●	●●●
Standard Service Program (SSP)	●●●	●●●	●●●	●●●

Figura 69. Principais facilidades do LabView, da National Instruments

A análise da literatura indica que os grupos desenvolvedores de WebLabs preferem código abertos para seus projetos, o que tende a afastar o LabView. Mesmo assim,

a literatura mostra que usualmente o LabView é considerado como uma das possíveis plataformas a serem integradas.

Dessa maneira, sugere-se que o futuro experimento sobre WebLabs Forenses leve em consideração a possibilidade de integração com essa plataforma.

4.5.13 ELECTRONIC DISCOVERY (E-DISCOVERY)

Utiliza-se essa expressão para referenciar um extenso leque de softwares destinados ao exame de computadores e serviços eletrônicos geralmente com objetivos corporativos, na linha das auditorias internas.

Os produtos para e-Discovery possuem procedimentos semiautomáticos para armazenamento, busca, coleta e análise de evidências digitais, apresentando os resultados para a administração da empresa de maneira interativa e amigável. Os sistemas inspecionam estações de trabalho, laptops, servidores de arquivos e mensagens, repositórios diversos e mídias removíveis. Nessa tarefa colecionam automaticamente pontos potencialmente mais relevantes, fazem buscas por combinações de metadados, palavras-chave e assinaturas, mantendo a cadeia de custódia, e gerando relatórios. Contêm recursos para armazenamento e reuso de consultas e possuem ferramentas específicas para tratamento e exame de dados suspeitos. Podem integram-se com softwares utilizados por escritórios de advocacia na gestão de documentos dos processos judiciais.

Está aumentando a disponibilidade de softwares e serviços de Electronic Discovery (e-Discovery), abrangendo produtos como o Encase Enterprise Edition e o ProDiscovery IR, já descritos nesta dissertação.

O principal impulso na direção do e-Discovery está geograficamente localizado nos Estados Unidos em função de lei específica promulgada em 2006[29], o que não se aplica diretamente no Brasil, mas tem reflexos específicos tanto nas filiais brasileiras de empresas americanas ou nas brasileiras que atuam naquele país, assim como naquelas empresas que adotam padrões internacionais de governança. O e-Discovery ainda não é ponto pacífico em função das questões jurídicas sobre

[29] *Amendments to the Federal Rules of Civil Procedure concerning the discovery of "electronically stored information"*

proteção de privacidade, contudo considera-se que essas soluções e serviços devem ser estudados nos trabalhos futuros sobre Weblabs Forenses, por serem uma realidade de mercado.

4.5.14 LABORATÓRIOS PARA CAPTURA E ANÁLISE DE EVIDÊNCIAS DIGITAIS

No modelo de WebLab Forense proposto, a interligação entre a peça periciada e o WebLab Server está a cargo de dois componentes principais denominados nesta dissertação como Device Controller e Lab Server

O Device Controller é um componente especializado em cada tipo de dispositivo, por exemplo, um telefone celular ou um disco rígido de computador. Diversos Devices Controllers podem ser administrados por um Lab Server, organizados segundo alguma arquitetura mais conveniente, como por tipo de dispositivo, localização geográfica, comarca ou instituição de pesquisa.

Usualmente, Lab Servers e Devices Controllers serão equipamentos distintos, mas pode haver equipamentos que reúnam ambas as funções no mesmo gabinete, como o Solo 4 utilizado na prova de conceito deste trabalho[30].

Lab Servers ou Devices Controllers podem ser agregados ao WebLab tanto de forma permanentemente, atendendo continuamente as necessidades dos processos judiciais, quanto de modo *ad hoc*, apenas para um processo judicial ou análise específica.

Sugere-se que os estudos e experimentos futuros verifiquem viabilidade de se projetar e construir Device Controllers e Lab Servers específicos para serem integrados com o WebLab Forense proposto. Tendo em vista os objetivos mais amplos, no sentido de que WebLabs Forenses devem apoiar tarefas periciais nas comarcas distantes, torna-se recomendável que o sistema também possibilite o acoplamento de maior variedade possível de dispositivos comerciais utilizados pelos peritos e laboratórios periciais.

---

[30] O Solo 4 cumpriu tanto as funções de conexão e captura dos discos rígidos, típicas do Device Controller, assim como as funções de gestão das evidências capturadas e interação com o WebLab Server, típicas de um Lab Server. O Solo 4 pode capturar dois discos rígidos ao mesmo tempo e de forma independente, atuando como dois Devices Controllers.

Figura 70. Computador forense portátil

Uma das principais categorias de dispositivos que devem integrar em um WebLab Forense para sistemas eletrônicos digitais corresponde aos laboratórios móveis ou portáteis para coleta e análise de evidências, como o exemplo mostrado na Figura 70. Na prática, são computadores portáteis[31] equipados com recursos para coletar, proteger e analisar evidências acessadas por meio de conexões diversas como Fireware, USB, IDE, SATA, SAS e SCSI. Essas maletas são utilizadas principalmente por forças policiais ou por órgãos corporativas de segurança.

Outra categoria de equipamento de interesse como Device Controller corresponde aos duplicadores automáticos de discos, como o exemplo mostrado na Figura 71.

Figura 71. Duplicador de discos

São dispositivos que proporcionam maior velocidade na clonagem[32], requisito relevante nas operações de busca e apreensão onde há muitos computadores alvo ou então como equipamento padrão em institutos de criminalística e outros laboratórios periciais que atendem grande quantidade de casos. Podem ser utilizados também em corporações que mantém programas regulares de auditoria dos seus equipamentos. Possibilitam a coleta simultânea de 10 ou mais discos suspeitos por conexões SAS, SATA ou IDE, podem ser controlados remotamente por interfaces amigáveis, geram arquivos formato DD e fazem a transmissão dos dados por meio de conexões seguras.

[31] Equipamento forense portátil da ICS. Disponível em: <http://www.icsforensic.com>. Acesso em 21 ago. 2010

[32] Duplicadores de disco ICS. Disponível em: <http://www.ics-iq.com>. Acesso em 21 ago. 2010.

Ainda tendo em vista as situações onde há grande quantidade de dados a serem vistoriados, entende-se que pode haver a necessidade de Devices Controllers que possam ser conectados a grandes centros de processamentos de dados ou aos seus componentes igualmente de grande porte como, por exemplo, robôs[33] similares ao mostrado na Figura 73. A adoção generalizada de recursos para transmissão de sons e imagens, como os sistemas de telefonia VoIP e IoIP, e as facilidades para gravações de áudio e vídeo em simples celulares, tornam cada vez mais comum ser necessário exame forense desse material sob os aspectos da engenharia legal e da fonética forense visando o reconhecimento de locutores, a melhoria na audibilidade e inteligibilidade da fala em gravações de má qualidade e o exame de originalidade e integridade de material digital, buscando vestígios de adulteração. Esses procedimentos periciais requerem a disponibilidade e compartilhamento de laboratórios de áudio para a realização de exames, como aquele mostrado na Figura 72[34]. Outro grupo de estudos forenses refere-se à mensuração de níveis de ruído ambiental, que requer equipamento laboratorial adequado.

Figura 73. Robô para biblioteca de dados

Figura 72. Laboratório forense de áudio

Para o exame de imagens capturadas por câmaras de vigilância e dispositivos similares são requeridos laboratórios com alto poder computacional. Realizam procedimentos de super-resolução de imagens, visando melhorar sua qualidade e o reconhecimento automático de padrões, para, por

[33] Storage Teck Tape Robot. Disponível em: <http://www.sun.com/storage/products.xml>

[34] Speech Technology Center, dados disponíveis em http://www.speechpro.com

exemplo, o reconhecimento de faces em tempo real dos transeuntes ou busca automática por pessoas em gravações de segurança, sistema cada vez mais utilizado pelas autoridades policiais nacionais e internacionais.

Figura 74. Sistema portátil para coleta de dados em telefones celulares

A grande expansão nos serviços móveis de telecomunicações, leva à necessidade de adoção de Devices Controller especializados no exame forense de telefones celulares e outros dispositivos digitais móveis, como a maleta forense[35] mostrada na Figura 74.

Cumpre considerar que a partir do ano de 2011 passará a ser adotado mais efetivamente o padrão IPv6[36], que gradativamente substituirá IPv4 porque este suporta apenas pouco mais de 4 bilhões de endereços, quantidade que logo se tornará insuficiente diante da expansão no uso da comunicação de dados em um ambiente de computação ubíqua, com muitos bilhões de dispositivos digitais interligados em redes mundiais (WAN), metropolitanas (MAN), locais (LAN) e pessoais (PAN).

Essa grande quantidade de dispositivos de pequenas dimensões e dotados de potentes recursos de telecomunicações tende a tornar o exame pericial em qualquer ambiente tende cada vez mais complexo, especialmente nas buscas e apreensões determinadas pela Justiça que envolvem a busca de pequenos dispositivos eletrônicos sem que exista real colaboração por parte dos investigados.

Por isso, é necessário que o perito e as autoridades responsáveis pela vistoria tenham acesso a recursos tecnológicos eficazes para localizar rapidamente sinais eletromagnéticos que indicam a presença de sistemas eletrônicos digitais no ambiente investigado, antes que eventuais evidências sejam destruídas.

A Figura 75 ilustra possíveis pontos de interesse pericial durante hipotética vistoria em ambiente típico de escritório, onde estão indicados exemplos fictícios de dispositivos procurados pela perícia, sendo que muitos deles podem estar ocultos

[35] Equipamento XRY, da Micro Systemation, dados disponíveis em http://www.msab.com.

[36] Internet Protocol Version 6, definido na RFC 2460, disponível em http://tools.ietf.org/html/rfc2460.

dentro de móveis, bolsos e bolsas, portanto dificilmente poderão ser localizados sem o apoio de meios eletrônicos de busca, diante da sua crescente miniaturização.

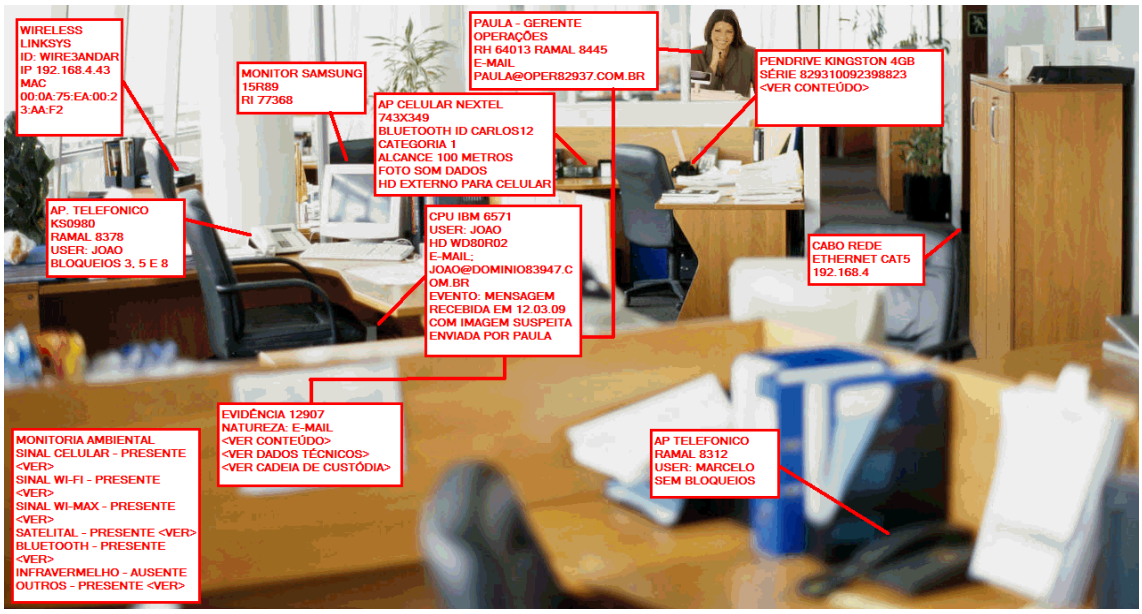

Figura 75. Localização de evidências em um ambiente vistoriado

Esses equipamentos apresentam alguma emissão eletromagnética, quando em uso, radiação que pode, em tese, ser detectada por sensores apropriados portados pela perícia. Como os dispositivos procurados pela perícia cada vez mais adotam recursos de comunicação por rádio, com tecnologias como GSM (celulares), família IEEE 802.11 (Wi-Fi), Bluetooth (SIG), podem ser detectados e até mesmo identificados por meio de *scanners* de radiofrequência.

Figura 76. Receptor móvel para monitoramento de espectro de radiofrequência

Por esse motivo, sugere-se que o modelo de WebLab Forense a ser avaliado em trabalhos futuros considere a integração com monitores de radiofrequência ou analisadores de espectro capazes de detectar e indicar intensidade e direção de fontes de rádio presentes no recinto examinado.

A Figura 76 mostra exemplo de um equipamento profissional para monitoramento de rádio em campo, faz buscas por transmissores miniatura que operam na extensa faixa de 9KHz a 7.5GHz, equipado com antena direcional e interface para comunicação de dados que poderia ser utilizada inclusive para integração remota com o WebLab Forense[37].

Sugere-se, ainda, que os estudos futuros sobre a integração de laboratórios móveis de radiofrequência considerem:

a) Adotar no WebLab Forense funções que possibilitem relacionar os dados sobre equipamentos coletados pelos scanners com os dados mantidos pelos fabricantes (bancos de dados), obtendo automaticamente a especificação técnicas dos produtos monitorados para fins forenses.
b) Adotar funções de inventário, com o cruzamento dos dados de identificação do equipamento coletados pelos scanners (*mac address*, etc.) com os dados dos fabricantes ou da própria empresa fiscalizada, obtendo informações adicionais como proprietários, número de patrimônio, departamento, usuário, etc.
c) Adotar funções para coletar dados públicos transmitidos pelos objetos investigados, como ID do equipamento, sistema operacional etc..
d) Adotar recursos pelos quais o equipamento móvel portado por agentes possa ser operado remotamente por especialistas enquanto interagem com os resultados obtidos. Além disso, sugere-se avaliar a possibilidade de que as imagens e os dados coletados sejam postos à disposição em tempo real aos interessados na vistoria, como o juiz, o delegado e os outros operadores do direito.
e) Avaliar a possibilidade de utilizar recursos de realidade aumentada. Poderia ser desenvolvido em projeto futuro um dispositivo para mostrar o ambiente real visto através de câmara ou visor *see through* operado pela perícia e a essa visão seriam sobrepostas informações sobre fontes de radiofrequência. As informações podem provir da radiogoniometria das fontes eletromagnética (dois scanners móveis), dados de GPS e informações cruzadas em tempo

[37] Equipamento Rohde 7 Schwarz, especificação disponível em http://www2.rohde-schwarz.com/en/

real com os bancos de dados dos fabricantes, da empresa ou de terceiros que lhe prestam serviços.

Dessa maneira, sugere-se avaliar a possibilidade de projetar uma interface para coleta de dados forense operada localmente, mas que simultaneamente possibilite interação remota com sistemas ou pessoas. A análise do diagrama das artificialidades e espaços da Figura 77, apresentado por Kirner e Tori (2006, p. 34), indica que sugestão apresentada traria benefícios pela adição à interação visual do mundo real dos dados provenientes de *scanners* de RF e sistemas administrativos remotos. Essa solução contemplaria, ao mesmo tempo, a tele-presença para fiscalização remota das atividades pelo juiz e demais operadores do Direito.

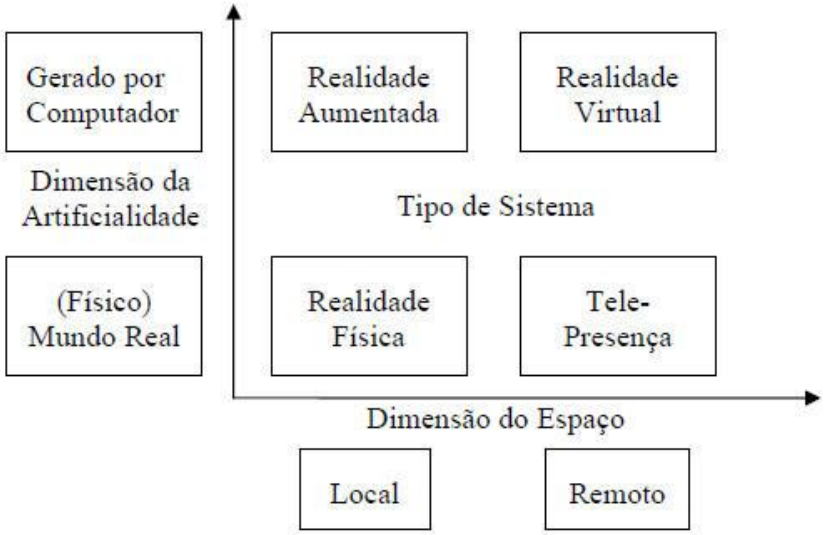

Figura 77. Diagrama da artificialidade e espaços

Ainda no contexto dos estudos futuros, sugere-se avaliar os recursos necessários para os WebLab Forense quanto a recursos com grande capacidade de armazenamento e processamento de dados.

O crescimento na capacidade dos dispositivos digitais torna necessário que os laboratórios forenses utilizem estruturas mais amplas, fornecidos por *data centers*

montados e configurados especificamente para análise forense[38], como o exemplo mostrado na Figura 78.

Utilizam sistemas operacionais para servidores especialmente configurados para o máximo desempenho nas tarefas forenses[39]. São soluções montadas em *rack* com diversos computadores servidores, sistemas de *storage* de alta capacidade e velocidade e recursos eficientes para comunicação de dados. Possuem ainda funções para gestão centralizada e intensiva de segurança lógica, controle de usuários locais ou remotos e os serviços de backup e salvaguarda.

Figura 78. Data center forense

Os maiores centros forenses integram diversos conjuntos desse tipo, provendo inclusive soluções de contingência, salas cofres, proteção contra incêndio e ampla segurança física para preservar as evidências digitais.

Nesse contexto, sugere-se ainda que, além de computadores servidores potentes, seja prevista ainda o uso de estações de trabalho forense de alto desempenho, como o exemplo mostrado na Figura 79.

Figura 79. Estação forense

Essas estações são de fato computadores potentes[40] montados em pequenos *racks* contendo *arrays* de discos com diversos terabytes de espaço para armazenamento de evidências, usualmente configurados em RAID para melhor desempenho e com facilidade de *hotswap*. Possuem recursos flexíveis para coletar diversos dispositivos IDE, EIDE, ATA, ATAPI e SATA, protegendo-os contra gravação (*write-block*). Usualmente são dotados de processadores potentes e extensa memória RAM para que possam cumprir mais rapidamente tarefas computacionais intensivas, como a busca simultânea por muitas

[38] Equipamento FREDC. Disponível em: <http://www.digitalintelligence.com/products/fredc/>. Acesso em 29 ago. 2010.

[39] FREDC, informação disponível em http://www.digitalintelligence.com/products/fredc/

[40] Digital Intelligence, informação disponível em http://www.digitalintelligence.com

palavras-chave, indexação, filtragem por imagens ou sons e quebra ética de senhas e criptografia. Possuem ainda recursos variados para leitura de cartões de memória ou leitura de fitas de backup.

Nos futuros estudos sobre WebLabs Forenses, sugere-se ainda avaliar a integração com laboratórios para a quebra ética de senhas e criptografia. Recomenda-se considerar na análise desde dispositivos discretos para acelerar o desempenho do hardware[41], como o dispositivo mostrado na Figura 80 que pode ser acoplado a computadores, até soluções de maior porte baseadas em redes de processamento colaborativo para quebra legal de senhas.

Figura 80. Acelerador de hardware para quebra de senha

Os estudos indicam que este é um dos principais serviços que o WebLab Forense poderá prestar às autoridades e aos peritos em todo o país, uma vez que dificilmente haverá nas comarcas mais distantes recursos locais computacionalmente suficientes para essas tarefas. A adoção generalizada de recursos de criptografia para assegurar privacidade e segurança, tendência que se mostra adequada na proteção da sociedade e do indivíduo, traz severas dificuldades para exames forenses e produção das provas determinadas pela Justiça.

Os recursos de criptografia transformam-se em itens regulares de fábrica para computadores domésticos ou empresariais e também para telefones celulares e outros dispositivos eletrônicos digitais. Esse movimento tende a tornar praticamente inúteis os procedimentos atuais da perícia forense digital, pois impede o reconhecimento dos dados armazenados em discos rígidos e memórias.

Nos últimos dez anos aumentou o uso de softwares para criptografia como o PGP[42] e o TrueCrypt[43]. Inicialmente esses programas eram utilizados para criptografar apenas alguns arquivos considerados sigilosos pelos usuários. Essa prática protegia o arquivo, mas seu conteúdo ainda podia ser visto mediante acesso forense às áreas de trabalho utilizadas enquanto os textos eram redigidos ou lidos pelo usuário.

---

[41] Acelerador Tableau. Disponível em: <http://www.tableau.com>.

[42] O software PGP é fabricado pela PGP Corporation, empresa especializada pioneira em soluções de proteção baseadas em criptografia, recentemente adquirida pela Symantec. Disponível em: <http://www.pgp.com>.

[43] TrueCrypt, software open-source. Disponível em: <www.truecrypt.org>.

Esses dados também podiam ser recuperados em áreas do próprio sistema operacional, como no arquivo *pagefile.sys* de paginação do Windows. Portanto, mesmo quando era adotada criptografia de arquivos, os peritos forenses conseguiam encontrar cópias do conteúdo armazenado no disco rígido que eram legíveis sem a necessidade de quebrar a senha secreta.

Entretanto, os softwares atuais possibilitam criptografar todo o disco, impedindo a visualização direta das áreas de trabalho do software aplicativo ou do próprio sistema operacional. Resta a possibilidade de capturar a imagem forense do disco rígido e levá-la a computadores de alto desempenho para tentar a quebra ética de senhas ou a busca de vulnerabilidade ou fragilidades dos sistemas de segurança.

Contudo, os sistemas mais modernos de proteção vinculam os dados armazenados a um hardware específico, na direção de impedir sua leitura se o acesso aos dados não tiver sido autenticado no próprio hardware e software de origem. Assim, passa a haver tripla segurança, baseada na autenticação do usuário, autenticação do software e autenticação do hardware.

Dessa maneira, os atuais softwares e computadores forenses tendem a tornar-se inúteis na tarefa de capturar e analisar provas a partir de dispositivos eletrônicos digitais criptografados.

O principal componente comercial nessa evolução é um padrão implementado por um chip denominado Trusted Platform Module (TPM), como o exemplo mostrado na Figura 81[44].

Figura 81. Trusted Platform Module

No estudo da literatura verificou-se que a tecnologia TPM é utilizada segundo diversas arquiteturas prevenir o uso não autorizado de dados perdidos ou furtados. A documentação técnica divulgada pelos fabricantes de soluções indicam as tendências de mercado. Será detalhada a seguir a documentação técnica divulgada pela Intel em seu portal na Internet (SMITH, 2008), por ser uma documentação geral, considera-se que o modelo é válido para indicar tendências do mercado.

[44] Exemplo de produto TPM, fabricado por Infeon Technologies - foto Infineon/CNET

O modelo mais simples, mostrado na Figura 82, prevê que as operações de criptografia são realizadas apenas na principal camada de software.

Para isso, o módulo de segurança deve atuar na rota do armazenamento de dados, ou seja, acima da estrutura de arquivos, operando mediante o *hooking* das leituras e gravações do file system. Assim, intercepta leituras e gravações no nível de drivers, como faz a Advanced Host Controller Interface (AHCI).

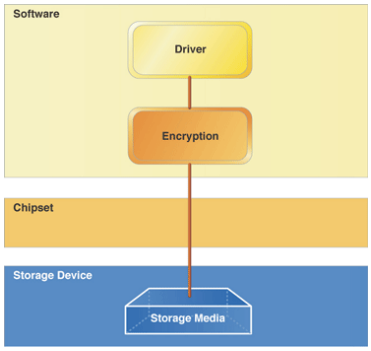

Figura 82. Criptografia baseada somente em software

No exame forense de computadores que utilizam esse modelo de proteção, os laboratórios periciais que sejam dotados da tecnologia adequada poderiam ter acesso aos dados originais mediante o *bypass* das funções de criptografia.

A Figura 83 mostra método distinto de proteção, onde há um microcontrolador dedicado para a tarefa de criptografia instalado diretamente no disco rígido.

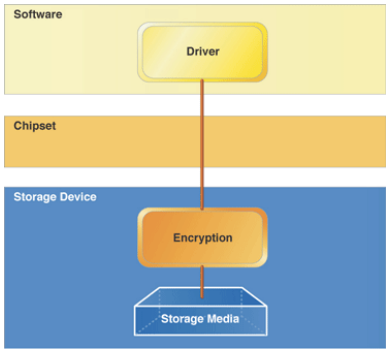

Figura 83. Criptografia baseada em dispositivos de armazenamento

Mesmo havendo um avanço em termos de proteção, essa criptografia do disco ainda depende de software externo para autenticação do usuário, gestão de chaves e serviços de suporte, situação onde dados podem ser analisados por laboratório forenses adequadamente equipados.

A Figura 84 mostra solução de criptografia baseada no *chipset* do controlador de armazenamento que utiliza o hardware do controlador de armazenamento e hardware dedicado para criptografia.

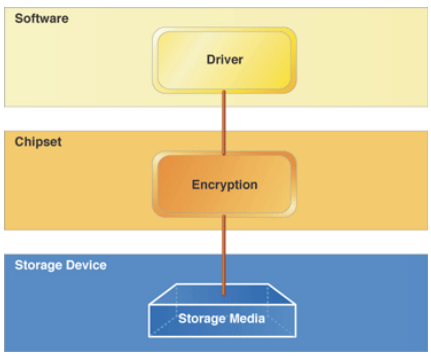

Figura 84. Criptografia baseada no controlador de armazenamento

O controlador decodifica os comandos no fluxo de dados e localiza pacotes de dados que são então criptografados e remontados antes de ser enviados ao dispositivo de armazenamento. O método baseia-se em firmware para autenticação de usuários,

gestão das chaves e serviços de suporte, tornando o acesso aos dados em exame forense muito mais complexo.

A Figura 85 apresenta modelo com criptografia do armazenamento remoto baseado no redirecionamento dos protocolos através de interfaces de rede, implementado por tecnologias como *Intelligent Drive Electronics Redirection* (IDE-R) ou *Internet Small Computer System Interface* (iSCSI). Dados são protegidos através de políticas e autorizações que pertencem ao cliente, configurando a utilização de recursos poderosos de criptografia não apenas nos computadores equipados com chips TPM, mas também ao longo das redes de comunicação de dados e armazenamento remoto, tornando os exames forenses ainda mais complexos.

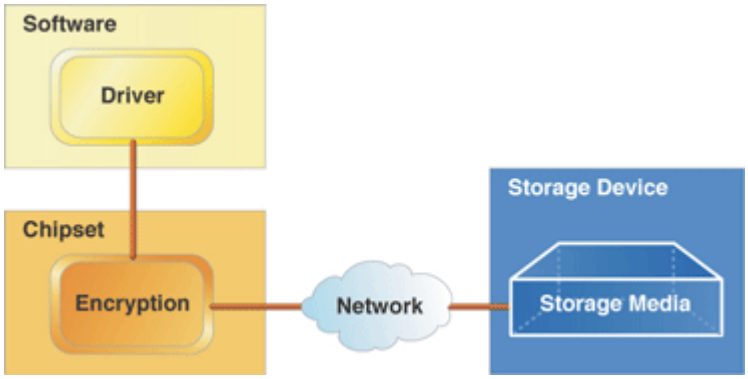

Figura 85. Encriptação de armazenamento remoto

A documentação da Intel mostra ainda tecnologia similar utilizada para expandir a proteção dos ativos em nível mais amplo ao longo da empresa, inclusive com o armazenamento local de chaves, autenticação de usuários e auditoria, porém estendendo a proteção a pontos remotos de armazenamento e até mesmo a recursos móveis conectados via rede, como o modelo da Intel mostrado na Figura 86

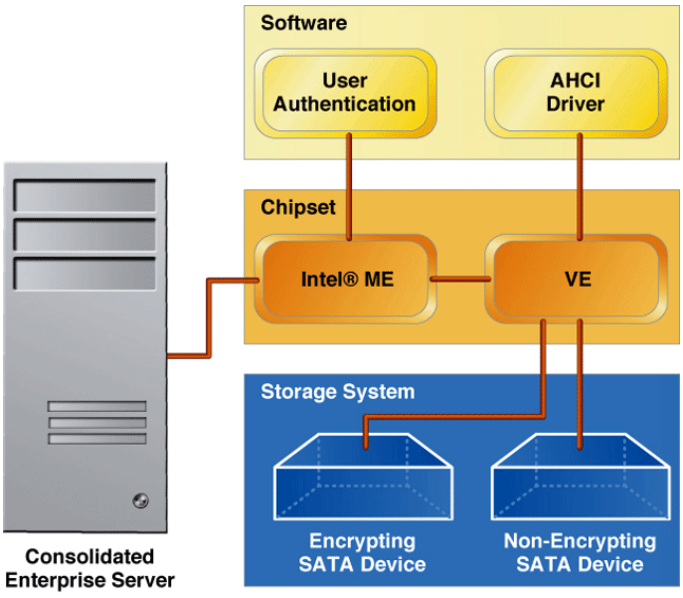

Figura 86. Servidor corporativo de criptografia TPM

Nesse contexto, resulta que os sistemas de proteção tendem a impossibilitar a realização de exames periciais, mesmo em dispositivos remotos, sempre que não se disponha das chaves de criptografia, impedindo as autoridades de acessar evidências. A quebra judicial de proteções

demandaria o auxílio dos próprios fabricantes ou, em sua ausência, a atuação de laboratórios independentes dos fabricantes dotados de tecnologia adequada para a leitura dos dados.

Como os estudos realizados mostraram que a criptografia é uma tendência de mercado, sugere-se que nos trabalhos futuros sobre WebLabs Forenses seja avaliada a possibilidade de integração dos laboratórios dos próprios fabricantes com o objetivo de que eles apoiem ou mesmo executem as tarefas necessárias para a abertura judicial dos recursos de proteção. Nessa possível solução, será necessário definir formas pelas quais os fabricantes poderiam quebrar a criptografia em procedimentos fiscalizados pelo Poder Judiciário, gerando a cadeia de custódia, mas em um ambiente onde o próprio WebLab pudesse assegurar a preservação dos segredos técnicos e comerciais do próprio fabricante.

Pode-se considerar que há certa similaridade funcional com o modelo atualmente utilizado na interceptação legal de comunicações telefônicas, onde há integração entre a planta operacional da operadora de telecomunicações e o sistema de gestão das interceptações instalado nas unidades policiais, mas em ambientes mutuamente protegidos e controlados.

Nas situações em que não houver participação dos laboratórios dos fabricantes, por qualquer razão, resta às autoridades determinar a participação de laboratórios independentes, imprescindíveis porque os sistemas de proteção são cada vez mais complexos e baseados em recursos de hardware, não mais apenas em software.

Figura 87. Laser scanning microscope

Por isso, quando não houver apoio dos fabricantes, o cumprimento das determinações judiciais pode implicar na necessidade de adotar recursos de engenharia reversa de hardware, em nível microscópico, com o objetivo de extrair códigos, algoritmos, chaves e dados em geral. Em outro tipo de demanda judicial pode ser necessário examinar os dispositivos eletrônicos em

nível microscópico para apurar se seus componentes eletrônicos foram modificados com intenção de fraude.

Os laboratórios forenses para essas tarefas devem lidar com questões eletrônicas, como mudanças rápidas na frequência de operação de circuitos para gerar saltos na execução de programas, alterações ríspidas na tensão de alimentação para provocar decodificações incorretas e uso de tecnologia de microscopia eletrônica para obter o *bypass* dos recursos de segurança.

Figura 88. Focused Ion Beam (FIB)

Nos exames realizados pelos próprios fabricantes ou por laboratórios independentes são necessários equipamentos específicos para micro e nanotecnologias, como microscópios ópticos de alta potência, conforme exemplo mostrado na Figura 87[45], microscópios eletrônicos, além de sistemas baseados em Focused Ion Beam (FIB), como o equipamento da Figura 88[46]. Possibilitam a obtenção de imagens, a análise detalhada dos dispositivos semicondutores e até mesmo modificar seu comportamento elétrico com o objetivo de ultrapassar proteções e conseguir a leitura de dados.

Em termos gerais, as principais atividades são a captura do layout, a localização de nós, o *bypass* de camadas protetoras por meio de ácidos e Reactive Ion Etching (RIE), a definição de sistemas de coordenadas, a análise detalhada do layout e interruptores de segurança e defesas, o estabelecimento de contatos, a injeção de sinais e a extração de dados.

Esses recursos de micro e nanotecnologias podem ser necessários em diversos contextos, como na verificação e comprovação de falhas ou vulnerabilidades, na

[45] Zeiss Axiotron

[46] Hitachi FB-2200

constatação de fraudes com cartões, na constatação de plágio ou falha no circuito, entre outros exames previsíveis.

Um conhecido especialista em segurança[47] apresentou, na conferência Black Hat realizada em fevereiro de 2010, em Washington, uma longa e detalhada palestra intitulada “Desconstructing a Secure Processor”, onde descreveu todas as para quebrar a criptografia do chip TPM, até então considerado o chip mais seguro da atualidade. Esse material encontra-se atualmente divulgado no YouTube e nele constata-se a utilização de uma estação Focused Ion Bem para análise e quebra de segurança, como indica a

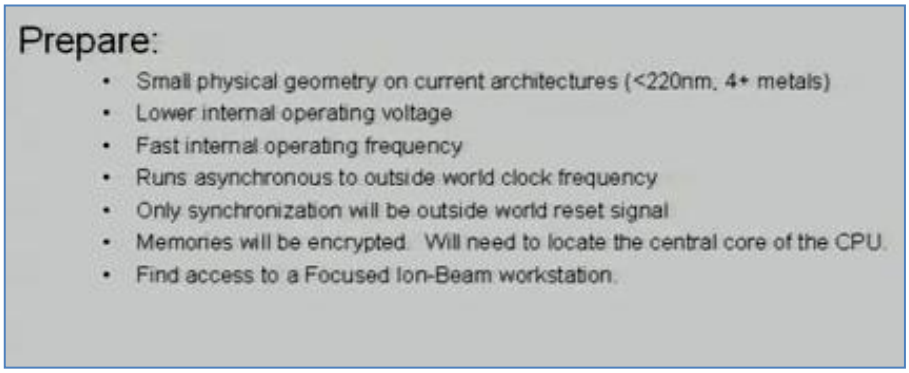

Figura 89. Palestra Black Hack sobre uso de Focused Ion Beam para quebra da segurança

O material divulgado na Black Hat e na Internet mostra em detalhes como utilizar equipamento de micro e nanotecnologia para realizar a engenharia reversa e prover a quebra da criptografia, como mostram algumas das imagens da gravação de vídeo que foi divulgada. As imagens mostradas a seguir foram extraídas do material divulgado na Internet[48] e são apresentadas parcialmente sobrepostas por questão de segurança e direitos autorais.

[47] Nome real omitido, para evitar a divulgação de práticas indevidas.

[48] Omitem-se propositalmente origem e autoria do material apresentado por questões de preservar a segurança e evitar a divulgação de material que pode ser considerado de segurança. As imagens foram propositalmente sobrepostas pelo mesmo motivo.

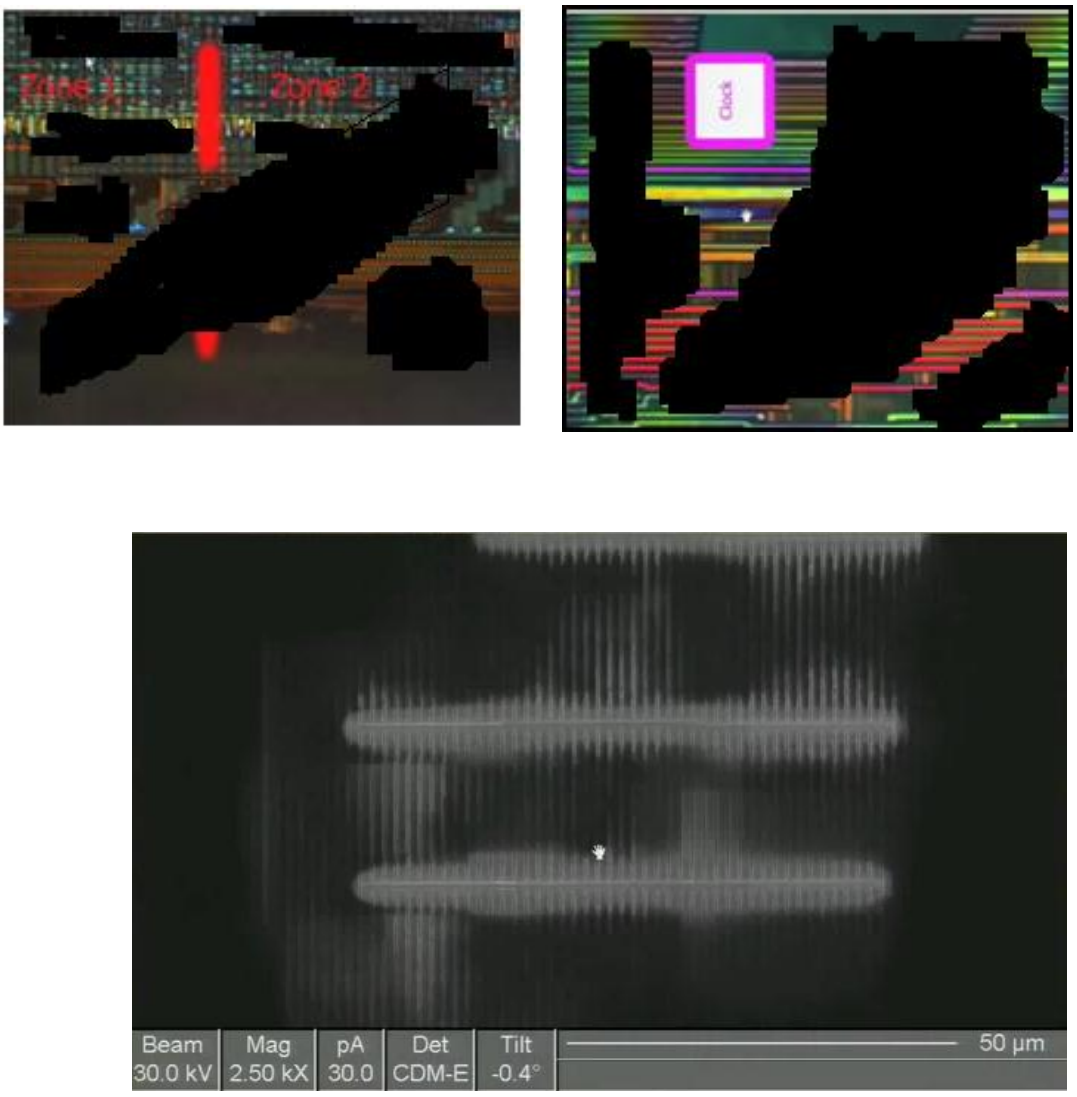

Figura 90. Imagens sobre uso de alta tecnologia para quebra de segurança

Dessa maneira, sugere-se que os estudos e experimentos futuros sobre WebLabs Forenses incluam o acesso a laboratórios de alta tecnologia com objetivos diversos como a verificação de fraudes realizadas mediante micro ou nanotecnologias, avaliação de violação de direitos autorais nessa área e análise forense de riscos e vulnerabilidades de sistemas e dispositivos.

4.5.15 LICENCIAMENTO DE SOFTWARES FORENSES

Ainda com relação aos trabalhos futuros, será necessária a avaliação das questões pertinentes tanto ao licenciamento de software dos diversos laboratórios remotos que podem vir a ser acessados a partir do WebLab Forense, quanto ao

licenciamento do software que comporá a própria infraestrutura do WebLab. Além disso, será necessário avaliar as questões legais pertinentes à própria integração dos equipamentos em rede e a sua operação.

Em princípio, entende-se que o estudo sobre licenciamento em WebLabs pode partir das questões que já estão sendo avaliadas nas comunidades técnicas e jurídicas sobre o uso de software na computação em nuvem e no uso do software em computadores com múltiplos processadores ou múltiplos núcleos.

4.5.16 SINTESE DO CAPÍTULO

Neste capítulo, foi avaliada a implementação de laboratórios forenses operados remotamente por meio da Internet, propondo-se a adoções do modelo de WebLabs para a criação de WebLabs Forenses. Para avaliar essa proposta, foi realizada prova de conceito que consistiu na coleta remota dos dados de um HD e subsequente transferência a um laboratório igualmente remoto para exame e custódia das evidências encontradas. O resultado positivo da prova de conceito permitiu endereçar diversos pontos relevantes que devem ser previstos nos próximos experimentos a serem realizados com o objetivo de criar e testar um WebLabs Forense realmente operacional dedicado a apoiar exames em sistemas eletrônicos digitais.

5 CONCLUSÕES E TRABALHOS FUTUROS

Os capítulos anteriores desta dissertação detalharam os estudos realizados e as conclusões e contribuições obtidas, motivo pelo qual neste capitulo os principais resultados do trabalho são apresentados de maneira objetiva e sintética.

Inicialmente, cabe destacar que a revisão da bibliografia mostrou que a sociedade brasileira está adotando e rapidamente assimilando em seu dia-a-dia os mais recentes dispositivos eletrônicos digitais baseados em tecnologias da informação e das telecomunicações. Com isso, ficou claro que estamos construindo em ritmo acelerado a nossa sociedade da informação.

Os estudos mostraram ainda que esse movimento está se interiorizando rapidamente, ou seja, atingindo milhares de municípios e aldeias por todo o país, tendo como pontas de lança a telefonia celular móvel e a universalização do acesso à internet. Alguns indicadores mostram que nos próximos anos a convergência tecnológica colocará em foco também a TV interativa. De modo geral, a análise dos dados indica que as pessoas e as empresas estão cada vez mais dependentes dos equipamentos eletrônicos digitais.

O confronto das características dessa evolução tecnológica com o perfil dos conflitos de interesses usuais na sociedade contemporânea reforçou a visão de que a adoção generalizada de dispositivos eletrônicos pela sociedade brasileira está impondo cada vez mais ao Poder Judiciário a obrigação de decidir os processos judiciais com base em provas digitais, as quais pela sua própria natureza são voláteis, dispersas, difíceis de coletar, facilmente adulteráveis, pouco compreendidas e difíceis de interpretar.

Além disso, o estudo mostrou que mais ainda nesse ambiente é importante que a decisão do Juiz se baseie em processos racionais de análise das evidências, o que quase sempre depende da opinião de peritos e do exercício verdadeiro do contraditório.

A prova pericial deve basear-se em fatos reais submetidos ao crivo do raciocínio lógico do julgador; contudo, a escassez de laboratórios capazes de realizar análises técnicas são fatores que prejudicam a capacidade do Poder Judiciário em prover

decisões corretas e transparentes à sociedade, cenário agravado pela crescente presença de evidências digitais nos processos judiciais.

A verificação informal de noticias mostrou que autores, réus, advogados, peritos e autoridade policiais reclamam de falta de estrutura adequadas para a realização de perícias técnicas, da ocorrência de erros nos exames técnicos e da demora excessiva nos procedimentos. Essa verificação indicou a existência de dificuldades dos operadores do Direito e da sociedade para lidar com os resultados do trabalho pericial, ao mesmo tempo em que foram detectadas manifestações dos peritos sobre a falta de recursos mínimos para o desempenho das suas funções, provocando erros e demora excessivas nos procedimentos periciais. Esse cenário salientou a falta de confiabilidade e as deficiências no trabalho realizado pelos laboratórios forenses, agravando o risco da condenação indevida de inocentes ou da absolvição indevida de culpados.

Os estudos realizados mostraram que os exames periciais são essencialmente realizados por peritos oficiais, que atuam no interior dos Institutos de Criminalística das Polícias Federal ou Estaduais, ou pelos peritos judiciais que atuam em suas residências ou escritórios. Viu-se que seus laboratórios periciais localizados nos grandes centros estão sendo paulatinamente modernizados graças a investimentos governamentais, mas continuam sobrecarregados, com filas de espera de dois anos ou mais pelo resultado do exame de um simples HD. Nos núcleos descentralizados da Polícia Científica há carência de recursos técnicos e humanos.

Esse cenário permitiu considerar que os milhares de comarcas existentes no país estão distantes e carentes das melhores práticas periciais, problema que tende a se agravar rapidamente em função da crescente complexidade e rápida adoção de dispositivos digitais pela população dessas regiões.

A análise configurou o problema a ser resolvido como a necessidade de levar até essas comarcas brasileiras serviços periciais eficazes e sólidos frente à rápida disseminação da tecnologia. O trabalho concluiu que a solução está na criação de WebLabs Forenses, partindo da constatação de que esse conceito é adequado aos objetivos e de que os modelos dos WebLabs que estão sendo adotados em outras áreas científicas podem ser adotados para construir também WebLabs Forenses.

A principal diferença entre os WebLabs das demais áreas e o WebLab Forense está na interação com o ambiente judicial, ou seja, nos requisitos da prova judicial como elemento confiável de motivação do juiz e em seu debate para se chegar à verdade dos fatos segundo cerimonial próprio de cada ramo do Direito.

A prova de conceito realizada com um WebLab Forense muito simples demonstrou a validade do modelo proposto, tendo havido em ambiente simulado o comando remoto para acesso e captura à distância dos dados contidos em um HD e a remessa telemática e exame da imagem forense em um laboratório central igualmente remoto, sendo todas as etapas fiscalizadas à distância pelos demais participantes interessados no processo.

Concluiu-se que adoção de WebLabs Forenses é tarefa viável e trará benefícios quanto ao problema identificado no início deste trabalho e que constitui seu objetivo principal, provendo maior disponibilidade e presença dos recursos periciais para milhares de comarcas do país. Mais ainda, os estudos indicaram ser recomendável a criação e integração de uma rede de WebLabs Forenses para coleta e exame remoto de dispositivos digitais.

Conforme detalhado nesta dissertação, a adoção de WebLabs Forenses traz relevantes benefícios desde a fase inicial de vistoria do local do crime, atividade que passa a ser monitorada através do laboratório remoto, registrando em tempo real todos os eventos, e pondo esse material ao alcance da autoridade que preside o ato e das partes, gerando sólida e confiável cadeia de custódia e viabilizando o exercício do eficaz do contraditório, que é um princípio fundamental do Direito na nação brasileira.

O modelo proposto traz ainda o grande benefício de possibilitar a coleta remota e controlada das evidências digitais, substituindo um esquema inseguro de sequestro físico do computador suspeito e seu transporte possivelmente no porta-malas de um veículo até um laboratório pericial, figura distante e incompatível com o estado da tecnologia e os desafios da sociedade moderna.

Como foi discutido no presente trabalho, há muitos riscos de perda ou contaminação dessa evidência durante o manuseio físico do dispositivo original. Assim, em vez da apreensão física da caixa do computador, o modelo proposto demonstrou ser possível e muito melhor fazer a coleta lógica dos dados contidos no computador,

gerando-se a parte daí uma sólida e confiável cadeia de custódia, pois o material digital é coletado e transferido ao núcleo do WebLab por meios corretos de coleta e por canais de comunicação criptografados e confiáveis, passando a incorporar a central de custódia digital do WebLab. Pode-se avaliar ainda a existência de centrais descentralizadas de custódia. Assim, passa-se de um sistema antigo calcado na força física para um procedimento moderno de computação forense remota.

Outra conclusão do presente trabalho, suportada também pela prova de conceito realizada, é que a adoção de WebLabs Forenses proporciona ganhos de escala e aumento na confiabilidade do processo, pois as atividades realizadas passam a ser passíveis de monitoramento remoto em tempo real pelos operadores do direito e das partes.

O estudo mostrou ainda que a adoção de conceitos de WebLab Forense beneficia o atendimento a comarcas distantes dos grandes centros, levando-lhes o que há de melhor em métodos e ferramentas periciais disponíveis hoje apenas nos grandes centros de referência pericial. Ao mesmo tempo, o WebLabs Forense passa a constituir sistema de gestão do conhecimento e um acervo de referências técnicas na área, beneficiando todos os peritos e os demais operadores do Direito.

A adoção de sistemas seguros, baseados em certificados digitais e recursos cifrados de comunicação telemática para transporte e acesso às provas, além da transparência dos procedimentos, são elementos que farão com que aumente a confiança nas atividades judiciais, policiais e periciais, uma vez que todo o contato ou manipulação de evidências digitais poderá ser realizado através de “túneis” seguros e seu armazenamento ocorrerá em recipientes protegidos contra acessos inadvertidos ou indevidos.

Esse grau de confiança tornar-se-á maior na medida em que for construída uma rede de WebLabs Forenses, integrando os laboratórios forenses das principais universidades e das polícias científicas. O conceito de rede de WebLabs Forenses possibilitará também a criação de um índice consolidado de recursos técnicos disponíveis, assim se algum laboratório necessitar de um recurso específico, de rara disponibilidade, a rede possibilitará localizar esse recurso em outros centros de referência e, a depender da sua configuração, poderá até mesmo prover sua utilização remota por peritos do laboratório solicitante.

Nesse contexto, os estudos realizados sugerem também que os WebLabs Forenses virão a constituir-se em importantes ferramentas para formação e treinamento de peritos, proporcionando aos milhares de profissionais brasileiros o acesso remoto e prático às melhores ferramentas e metodologias forenses.

Outras conclusões parciais e sugestões de evolução foram apontadas nos capítulos precedentes, sendo certo que a principal conclusão refere-se à conveniência de que seja construído um WebLab Forense efetivamente operacional para a análise de sistemas eletrônicos digitais. Para isso, será necessário definir um projeto técnico detalhado e a avaliação mais profunda dos aspectos legais relacionados ao uso de WebLabs Forenses.

Ainda com relação aos principais trabalhos futuros, sugere-se:

a) Especificação e realização de avaliações mais completas de WebLabs Forenses voltados a sistemas eletrônicos digitais.
b) Definição de estruturas e funcionalidades para WebLabs Forenses, evoluindo com o estudo de arquiteturas e metadados específicos para cadeia de custódia, gestão de evidências, gestão de processos, controles de qualidade e demais funcionalidades indicadas nesta dissertação.
c) Definição de padrões para construção, operação e certificação de WebLabs Forenses.
d) Definição de padrões para interoperabilidade de WebLabs Forenses
e) Interação com as universidades e a indústria para ampliação do leque de ofertas de interfaces forenses com dispositivos digitais que possam ser comandadas remotamente, além da especificação de unidades robóticas especializadas no manuseio de dispositivos digitais vistos como evidências em processos forenses.
f) Apoio à implantação de WebLabs Forenses em nível nacional
g) Apoio ao estabelecimento de uma rede de WebLabs Forenses.

Espera-se que o resultado final deste projeto mais amplo traga elementos concretos para a especificação e construção de WebLabs efetivamente úteis e que possam melhorar a qualidade e a produtividade dos trabalhos periciais realizados em todo o Brasil.

6 CONSIDERAÇOES FINAIS

O tema WebLabs no mundo científico está vivendo apenas a sua fase inicial, considera-se que essa será uma das tecnologias que mais se desenvolverá nos próximos anos no meio pericial forense.

O presente estudo trouxe contribuições iniciais para o projeto de laboratórios forenses controláveis remotamente e espera-se que essas contribuições possam apoiar a subsequente construção de um WebLab Forense plenamente operacional.

REFERÊNCIAS

AGÊNCIA ESTADO. **Perícia criminal no País é extremamente precária**. Jornal O Estado de São Paulo, São Paulo, 15 ago. 2010. Disponível em: <http://www.estadao.com.br/noticias/geral,pericia-criminal-no-pais-e-extremamente-precaria,595345,0.htm>. Acesso em: 17 ago. 2010.

AGRAWAL, A., SRIVASTAVA, S. **WebLab: A Generic Architecture for Remote Laboratories**. In: 15TH INTERNATIONAL CONFERENCE ON ADVANCED COMPUTING AND COMMUNICATIONS, Dec. 2007, Guwahati (India). **Anais**. Guwahati, 2007. p. 301-306.

CASEY, E., STANLEY, A. **Tool review - remote forensic preservation and examination tools**. Digital Investigation, n. 2004/1, p. 284-297, 2004.

CASINI, M., PRATTICHIZZO, D., VICINO, A. **The automatic control telelab: a user-friendly interface for distance learning**. IEEE Transactions on Education, v. 46, n. 2, p. 252-257, maio 2003. Disponível em: <http://act.dii.unisi.it/reports/act_j1.pdf>. Acesso em: 09 set. 2010.

CGI.BR. **Pesquisa sobre o Uso das Tecnologias da Informação e da Comunicação no Brasil TIC Domicílios e TIC Empresas 2009**. São Paulo. Disponível em: < http://www.cetic.br>. Acesso em 17 nov. 2010.

CINTRA, A. C. A., DINAMARCO, C. R., GRINOVER, A. P. **Teoria Geral do Processo**. 22a. ed. São Paulo: Malheiros, 2006.

DEL ALAMO, J. A. et al. **The MIT Microelectronics WebLab: a Web-Enabled Remote Laboratory for Microelectronic Device Characterization**. In: WORLD CONGRESS ON NETWORKED LEARNING IN A GLOBAL ENVIRONMENT, Berlin (Germany), 2002. Anais. 2002. Disponível em: <http://www-mtl.mit.edu/~alamo/pdf/2002/RC-88 del Alamo NL 2002.pd>. Acesso em: 20 ago. 2010.

DELONG, K. **Interactive iLab Bootstrapping and Time of Day Test Lab Configuration**. Massachusetts Institute of Technology: 2007. Disponível em: <http://ilab.mit.edu/iLabServiceBroker>. Acesso em: 16 ago. 2010.

DELONG, K., FELKNOR, C. (2006). **iLabs Service Broker Machine Build Operating System and Database Install Guide**. Massachusetts Institute of Technology: 2006. Disponível em: <http://ilab.mit.edu/iLabServiceBroker>. Acesso em: 16 ago. 2010.

EPUSP QUIMICA. **Heat transfer and chemical reaction kinetics experiments**. Universidade de Sâo Paulo EPUSP QUIMICA, 2008. Disponível em: <http://weblab.pqi.ep.usp.br/features.html>. Acesso em 10 ago. 2010.

FAPESP. **Acesso aos WebLabs**. São Paulo. 2009. Disponível em: <http://kyatera.ifi.unicamp.br/index.php/BR>. Acesso em 23 ago. 2010.

FEDERAL JUDICIAL CENTER. **Reference Manual on Scientific Evidence. Federal Judicial Center**. 2ª. Ed. 2000. Disponível em: < http://www.fjc.gov/public/pdf.nsf/lookup/sciman00.pdf/$file/sciman00.pdf>. Acesso em: 10 set. 2010.

FERREIRA, M. S. J., **Uma arquitetura de sistemas distribuídos para weblabs de serviços ambientais**. 2007. 83 p. Dissertação (Mestrado) - Escola Politécnica, Universidade de São Paulo, São Paulo, 2007.

FRAGOSO, J. C. **Sobre as buscas e apreensões determinadas em locais de residência e trabalho**. Universidade de Santa Catarina. Disponível em: <http://www.buscalegis.ufsc.br/revistas/index.php/buscalegis/article/viewFile/11347/10912>. Acesso em 08 ago. 2010.

GARCIA, C. K. **A Polícia Científica pede Socorro!** Associação Brasileira de Criminalística: Goiás, 2009. Disponível em: <http://www.abcperitosoficiais.org.br/ver.asp?id=506>. Acesso em: 01 ago. 2010.

GARFINKEL, S., MALAN, D., DUBEC, K., STEVENS, C., & PHAM, C. **Advanced Forensic Format: An Open, Extensible Format for Disk Imaging**. In: SECOND ANNUAL IFIP WG 11.9 INTERNATIONAL CONFERENCE ON DIGITAL FORENSIC, 2006, Orlando (Florida). **Anais**. Orlando, 2006. p. 17-31. Disponível em: <http://www.cs.harvard.edu/malan/publications/aff.pdf>. Acesso em 16 ago. 2010.

GARTNER. **Forecast: PC Installed Base, Worldwide, 2004-2012.** Update. 2009. Disponível em: <http://www.gartner.com/DisplayDocument?ref=g_search&id=925027>. Acesso em: 18 Jun. 2009.

GE. **USP implementa Projeto WebLab**. GE, v. 1, n. 41, 2005. Disponível em: <http://www.imakenews.com/gefanucbrazil/e_article000457847.cfm?x=b11,0,w#_ftn2>. Acesso em: ago. 2010.

GERALDO, J. **Apostila de Direito Processual do Trabalho**. (s.d.). Disponível em: <http://www.ebah.com.br/trab-apostila-de-direito-processo-do-trabalho-doc-doc-a1788.html>. Acesso em: 27 ago. 2010.

GUELFI, A. R. **Análise de elementos jurídicos-tecnológicos que compõem a assinatura digital certificada digitalmente pela infraestrutura de chaves públicas do Brasil ICP Brasil**. 2007. 135 p. Dissertação (Mestrado) - Escola Politécnica, Universidade de São Paulo, São Paulo, 2007.

GUIMARAES, E. CARDOZO, E. MORAES, D. COELHO, P. **Design and implementation issues for modern remote laboratories**. IEEE Transactions on Learning Technologies, v. PP, n. 99, p. 1-1, 19 ago. 2010.

HARWARD, J., JABBOUR, I., & MAO, T. T. **iLab Interactive Services — Overview**. Massachusetts Institute of Technology: 2009. Disponível em: <http://ilab.mit.edu/iLabServiceBroker>. Acesso em: 16 ago. 2010.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. **Pesquisa de Informações Básicas Municipais – Perfil dos Municípios Brasileiros**. 2008. Disponível em: <www.ibge.gov.br>. Acesso em: 05 Jun. 2009.

ITU. **Measuring the Internet Society. International Telecommunication Union**. 2010. Disponível em: <http://www.itu.int/ITU-D/ict/publications/idi/2010>. Acesso em 15 ago. 2010.

JESUS, C. D. F., GIORDANO, R. C., CRUZ, A. J., ALIET-GAUBERT, M., JOULIA, X., ROUZINEAU, D., ALBET, J., COUFORT, C., ROUX, G. C. **Weblab in Chemical Engineering between France and Brazil: validation of methodology**. In: INTERNATIONAL CONFERENCE ON ENGINEERING EDUCATION – ICEE 2007, 2007, Coimbra (Portugal). Resumo dos trabalhos. Coimbra: 2007. Disponível em: <http://www.ineer.org/Events/ICEE2007/papers/351.pdf>. Acesso em 04 jul. 2010.

INTERNET WORLD STATS. **Internet Stats and Telecom Market Report**. Miniwatts Marketing Group: 2009. Disponível em: <http://www.internetworldstats.com>. Acesso em: 28 jun. 2010.

KIRNER, C., TORI, R. **Fundamentos de Realidade Aumentada**. In: VIII SYMPOSIUM ON VIRTUAL REALITY, 2006. Livro do Pré-Simpósio. p. 22-34. Belém. Disponível em <http://www.pcs.usp.br/~interlab/>. Acesso em 10 set. 2010.

LEAL, L. d. (s.d.). **O Acesso à Justiça e a Celeridade na Tutela Jurisdicional**. Revista do Direito: TJ-RJ, n. 65, p. 40-55, outubro 2005.

LEITÃO, H. A. **Criminalística deve ser agregada à universidade?** Jornal O Povo Online: Ceará, 2008. Disponível em: <http://www.opovo.com.br/opovo/opiniao/761842.html>. Acesso 10 jun. 2009,

MALATESTA, N. F. **A Lógica das Provas em Matéria Criminal**. 2ª. Ed. 1927. BDJur Brasília, DF, 26 jan. 2010 Disponível em: <http://bdjur.stj.jus.br/dspace/handle/2011/26788>.Acesso em: 10 ago. 2010.

MINISTÉRIO DA JUSTIÇA. **Portal do Ministério da Justiça sobre Segurança Pública**. 2009. Disponível em: <http://portal.mj.gov.br/senasp>. Acesso em: 08 ago. 2010.

NATIONAL INSTRUMENTS. **What is NI LabVIEW?** 2009. Disponível em: <http://www.ni.com/labview/whatis/>. Acesso em 29 ago. 2010.

ORDUÑA, P. **WebLab Deusto**. Villach (Austria), 2009. 81 p. Taret 2009 Training in Advance Remote Technologies – Remote Enginnering Applications – Summer 2009. Disponível em: <http://www.slideshare.net/nctrun/weblabdeusto-taret3>. Acesso em: 16 jul. 2009.

SANTOS JR., A. C. (2009). **Sistema Nacional de Gestão de Atividades de Criminalística do Departamento de Polícia Federal**. Ministério do Planejamento, Orçamento e Gestão - Inovação da Gestão Pública: Belo Horizonte, 2009. Disponível em: <http://inovacao.enap.gov.br/index.php?option=com_docman&task=doc_view&gid=283>. Acesso em: 17 agp. 2010.

SMITH, N. **Intel vPro Technology**. Intel Technology Journal, USA, v. 12, n. 04. Dezembro 2008. Disponível em: <http://www.intel.com/technology/itj/2008/v12i4/7-paper/1-abstract.htm>. Acesso em: 30 ago. 2010.

THIBAU, G. **Ferramentas para computação forense**. TechBiz Forense Digital. 2007. Disponível em: <http://www.forensedigital.com.br>. Acesso em: 08 ago. 2010.

US DISTRICT COURT MARYLAND. **Suggested Protocol for Discovery of Electronically Stored Information**. Maryland (USA), 2006. Disponível em: <http://www.mdd.uscourts.gov/news/news/ESIProtocol.pdf>. Acesso em 28 dez. 2009.