DOI: http://dx.doi.org/10.5769/C2011003

Ferramentas e Metodologia para Simplificar Investigações Criminais Utilizando Interceptação Telemática

André Peron[1], Flávio Elias Gomes de Deus[2], and Rafael Timóteo de Sousa Júnior[3]
(1) Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília-DF, Brasil, andre.peron@yahoo.com
(2) Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília-DF, Brasil, flavioelias@unb.br
(3) Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília-DF, Brasil, desousa@unb.br

***Abstract* — This paper presents the legal and technical aspects and the difficulties involved in the interception of Internet connections for the purpose of criminal investigation in Brazil. We propose a central infrastructure for receiving the intercepted traffic and a tool for obtaining, processing, importing and analyzing the traffic, in order to automate the entire process, simplifying and increasing the use of these interceptions in investigations.**

Key-words — Internet traffic interception, lawful interception, NFAT, network traffic, sniffer.

***Resumo* — Este artigo apresenta os aspectos jurídicos e técnicos e as dificuldades envolvidas nas interceptações de conexões de internet para fins de investigação criminal no Brasil. Propõe uma infraestrutura central para recebimento do tráfego interceptado e ferramenta para obtenção, tratamento, importação e análise do mesmo a fim de automatizar todo o processo, simplificando e aumentado o uso da interceptação de internet nas investigações.**

Palavras Chave — interceptação de internet, interceptação legal, NFAT, tráfego de rede, sniffer.

1. Introdução

A interceptação de comunicação de dados para fins de prova em investigação criminal e em instrução processual é prevista pela legislação brasileira. Para se utilizar deste artifício essencial para o sucesso de muitas investigações nos dias de hoje, os Órgãos de Investigação Criminais Brasileiros (OICB) necessitam, além de infraestrutura de *software* e *hardware*, metodologia adequada para a produção de provas para que não venham a ser questionadas na esfera judicial.

Diferentemente da interceptação de comunicações telefônicas, que é regida pela mesma lei e já se encontra bem sedimentada nos OICBs, tem se encontrado dificuldade para obter soluções informatizadas para a análise de interceptação telemática, mais especificamente a interceptação de conexão à internet, considerando os aspectos legais e técnicos da casuística brasileira.

A falta de normatização para a disponibilização dos dados trafegados e a incompatibilidade das ferramentas de análise com os dados recebidos tornam complexos os procedimentos de investigação, inibindo seu uso em larga escala nos OICBs.

O presente trabalho visa apresentar os aspectos jurídicos envolvidos, os aspectos técnicas considerando as formas de disponibilização do tráfego dos principais provedores de serviço de conexão à internet brasileiros (operadoras), os métodos de investigação utilizados e propor soluções para simplificar o uso da interceptação telemática e aumentar seu uso nas investigações criminais.

Este trabalho está organizado como segue: nas seções II, III e IV é apresentada a situação atual, com seus aspectos jurídicos, aspectos técnicos e metodologia de investigação em uso com as ferramentas disponíveis, respectivamente. Nas seções V, VI e VII são apresentadas as contribuições deste artigo: as duas ferramentas propostas (Servidor e Cliente de Interceptação Telemática) e a nova metodologia de investigação com o uso das mesmas. A conclusão e trabalhos futuros estão na seção VIII.

2. ASPECTOS JURÍDICOS

A interceptação telefônica e de dados (telemática) é prevista pela legislação brasileira como meio legal de prova em processos criminais. Era inicialmente regida pelo Código Brasileiro de Comunicações (Lei nº 4.117/1962 [1]), depois pela Constituição de 1988 [2] e pela Lei da Interceptação (Lei nº 9.296/1996 [3]). Em 2008, o CNJ publicou a Resolução Nº 59/2008 [4] a fim de disciplinar e uniformizar procedimentos. No momento tramitam no Congresso Nacional projetos modificando a Lei nº 9.296/1996.

A. Constituição de 1988

No seu artigo 5º (trata dos direitos e garantias fundamentais e direitos e deveres individuais e coletivos) inciso XII, a Constituição da República Federativa do Brasil de 1988 estabelece:

* Este trabalho foi financiado pelo Ministério da Justiça - Departamento de Polícia Federal - Diretoria Técnico-Científica sob o contrato n° 17/2008 com a Universidade de Brasília

"É inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal." [1]

Este inciso concede ao cidadão o direito ao sigilo de suas comunicações telefônicas e de dados, dentre outras, relativisando-o quando seu uso for para fins criminais. O inciso indica ainda que uma lei deve ser editada regulamentando em quais situações esse direito pode ser "quebrado" mediante ordem judicial.

O artigo 5º é uma cláusula pétrea, ou seja, só pode ser modificado com a convocação de uma Assembléia Constituinte.

B. Lei da Interceptação (Lei nº 9.296, de 1996)

Somente após oito anos da promulgação da Constituição de 1988 foi regulamentado o seu inciso XII do artigo 5º através da sanção da Lei da Interceptação (lei nº 9296/1996).

A Lei da Interceptação trata da interceptação telefônica e telemática e estabelece, dentre outras providências, que:

- Dependerá de ordem de juiz competente (art. 1º);
- Apenas para crimes com pena superior a detenção (art. 2º inciso III);
- Pode ser requerida por autoridade policial ou ministério público (art. 3º incisos I e II);
- Decisão judicial deve ser fundamentada, de no máximo 15 dias, renovável uma vez (art. 5º);
- Resultado relatado ao juiz em auto circunstanciado (art. 6º §2º);
- Autoridade policial poderá requisitar serviços técnicos especializados às concessionárias de serviço público (art. 7º);
- Constitui crime realizar interceptações sem autorização judicial com pena de reclusão de dois a quatro anos e multa (art. 10º).

C. Resolução nº 59/2008-CNJ

Em 2008, o Conselho Nacional de Justiça (CNJ), "órgão voltado à reformulação de quadros e meios no Judiciário, sobretudo no que diz respeito ao controle e à transparência administrativa e processual" [5], publicou a Resolução nº 59/2008 que "Disciplina e uniformiza as rotinas visando ao aperfeiçoamento do procedimento de interceptação de comunicações telefônicas e de sistemas de informática e telemática nos órgãos jurisdicionais do Poder Judiciário, a que se refere a Lei nº 9.296, de 24 de julho de 1996" [4].

A Resolução nº 59/2008 trata de aspectos da movimentação de documentos para garantir o sigilo das medidas judiciais e estabelecimento de controles a fim de coibir abusos no uso desse meio de prova.

D. Limitações

Tendo em vista as diversas tecnologias de acesso à internet utilizadas pelas operadoras (ADSL - *Asymmetric Digital Subscriber Line*, VDSL - *Very-high-bit-rate Digital Subscriber Line*, Cabo, GPRS - *General Packet Radio Service*, WCDMA - *Wideband Code Division Multiple Access*, HDSPA - *High-Speed Downlink Packet Access*, EDGE - *Enhanced Data Rates for GSM Evolution*, WiMax - *Worldwide Interoperability for Microwave Access*, etc.), os OICBs normalmente requerem às operadoras que capturem o tráfego da conexão investigada e disponibilizem-no de forma automatizada, já que elas possuem domínio da tecnologia utilizada e da complexidade de sua rede. Infelizmente não há qualquer norma brasileira que estabeleça como deve ser entregue esse tráfego. Com isso, as operadoras disponibilizam os dados interceptados da forma mais simples considerando sua tecnologia e seus técnicos sem qualquer padronização, ficando os OICBs com a obrigação de se adequar as especificidades de cada operadora.

3. Aspectos Técnicos

No Brasil existe uma concentração de clientes de acesso à internet em grandes operadoras (99% em 3G [6] e 88% em banda larga [7]), que já possuem pessoal especializado e método definido de disponibilização do tráfego interceptado de uma conexão de internet investigada para os OICBs. Neste item são apresentadas as formas de entrega do tráfego, formatos de arquivos e de pacotes adotados pelas principais operadoras e ferramentas utilizadas pelos OCIBs para análise do tráfego.

E. Formas de entrega do tráfego

As principais operadoras brasileiras entregam o tráfego capturado em três formas, aqui categorizados como SFTP-Server, SFTPClient e espelhamento de tráfego.

1) SFTPServer

Na forma SFTPServer (Fig. 1), a operadora fornece em seu servidor de interceptação uma conta de um servidor SFTP (*Secure File Trasnfer Protocol*) ou SCP (*Secure CoPy*) por conexão interceptada, onde ficam disponíveis para *download* arquivos de captura (arquivos contendo o pacotes de rede coletados) referentes ao tráfego de rede da conexão alvo. Os arquivos de captura são limitados a determinado tamanho (ex: 20MB) e possuem nomenclatura sequencial.

O servidor SFTP é configurado para que o arquivo ativo (arquivo que ainda encontra-se aberto para gravação de novos pacotes coletados e que não alcançou o tamanho limite) possa ser baixado e com função de continuação de *download* ativo, o que permite que a qualquer tempo o investigador possa acompanhar os últimos passos do investigado.

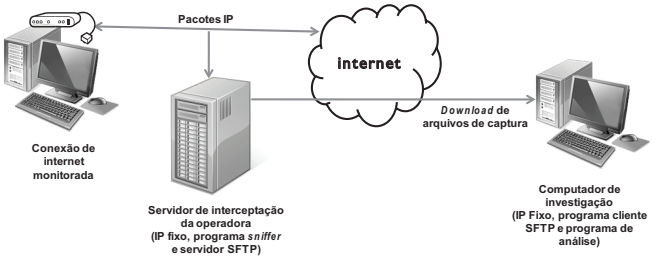

Figura 1. Entrega SFTPServer

Como os pacotes são capturados e armazenados dentro da rede da operadora e os arquivos de captura são apagados pelo investigador apenas depois de copiados, essa é forma mais confiável de entrega (menor perda de pacotes trafegados).

2) SFTPClient

Na forma SFTPClient (Fig. 2), a operadora coleta em seu servidor de interceptação os pacotes de rede da conexão alvo em pequenos arquivos de captura (normalmente 50KB ou 500KB e ainda por tempo limite de 30 segundos) e os envia (*upload*) para uma conta em servidor SFTP disponibilizado pelo OICB.

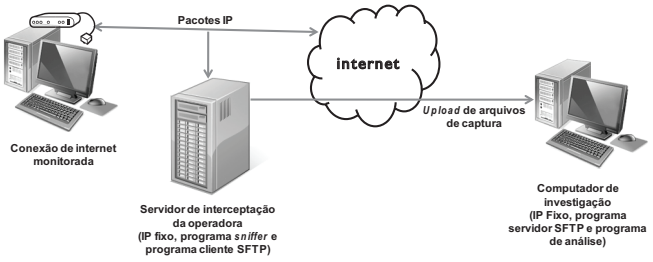

Figura 2. Entrega SFTPClient

Arquivos de captura que não puderem ser entregues após determinado número de tentativas são desprezados pela operadora, devendo o OICB utilizar equipamentos e conexões de internet confiáveis sob risco de perda de informações.

3) Espelhamento de tráfego

Na forma espelhamento de tráfego (Fig. 3), a operadora configura seu servidor de interceptação para gerar cópia de todos os pacotes de rede que trafegam pela conexão alvo e enviá-los para o OICB. O pacote de rede original é encapsulado em um novo pacote de rede que tem como endereço de origem o IP do equipamento da operadora e como endereço de destino o IP do servidor do OICB.

Nesta forma não há buferização no envio nem confirmação de entrega dos pacotes. Então a premissa básica é que a conexão de internet do OICB tenha banda superior à soma das bandas de subida e descida da conexão interceptada, o que mesmo assim não garante o recebimento de todos os pacotes, já que na rota entre o servidor da operadora e o do OICB pode haver congestionamento.

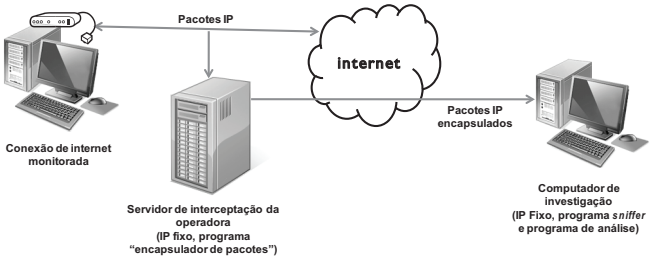

Figura 3. Entrega Espelhamento de Tráfego

F. Formatos de arquivo de captura

As operadoras que entregam o tráfego interceptado em forma de arquivo utilizam os formatos de arquivo de captura pcap [8], Snoop [9] e ETSI [11].

4) Pcap

Pcap é um formato de arquivo para salvar pacotes de rede capturados que se tornou padrão de fato. O arquivo possui um cabeçalho global seguindo por zero ou mais registros de pacotes. Cada registro de pacote possui um cabeçalho e o pacote de rede capturado.

5) Snoop

Snoop é um formato de arquivo de captura utilizado pelo programa de mesmo nome da Sun. O formato está documentado na RFC 1761 [9].

Assim como o formato pcap, o Snoop possui um cabeçalho global seguindo por zero ou mais registros de pacotes. Cada registro de pacote possui um cabeçalho e o pacote de rede capturado.

6) ASN.1 – ETSI

O formato de arquivo de captura padronizado pelo *European Telecommunication Standards Institute* (ETSI) é uma estrutura de dados ASN.1 (*Abstract Syntax Notation One*) [10] descrita no documento ETSI TS 102 232-3 [11].

G. Formatos dos pacotes

Os pacotes contidos em arquivos de captura entregues pelas operadoras, ou mesmo capturados pelo OICB quando são entregues na forma "espelhamento de tráfego", possuem geralmente um ou mais cabeçalhos de enlace. Os cabeçalhos de enlace Ethernet, LCC, PPPoE e VLAN, bem como uma combinação entre eles, são os normalmente encontrados.

Além do cabeçalho de enlace, algumas operadoras entregam os pacotes IPs interceptados encapsulados dentro de outro pacote IP (exemplo Fig. 4 [12]). Os encapsulamentos IP/UDP, Juniper [12], PCLI [13] e TZSP [14] e IP/GRE [15] são os utilizados pelas operadoras brasileiras.

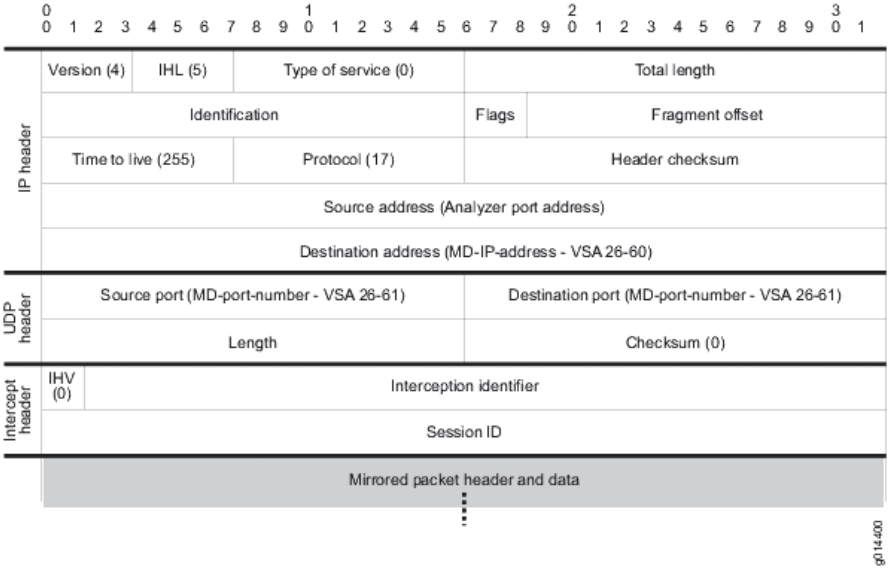

Figura 4. Encapsulamento IP Juniper

H. Programas de Análise de Tráfego

As ferramentas de análise forense de tráfego de rede (NFAT - *Network Forensics Analisys Tool*) são programas que permitem uma visualização de alto nível de dados coletados, focando na análise da camada de aplicação (*e-mails*, páginas *web*, VOIP (*Voice Over IP*), comunicadores instantâneos, etc.) [16]. São diferentes de ferramentas de segurança e monitoramento de rede (NSM - *Network Security and Monitoring*) tais como Wireshark [17] e Tcpdump [18], que embora possam ajudar na análise forense, são desenvolvidas para serem usadas por especialistas de segurança de rede [19].

Nas investigações são comumente utilizado um conjunto de NFATs, tais como os programas Netresec NetworkMiner [20] e NetWitness Investigator [21], destacando-se o Tamos NetResident [22] pela sua facilidade de uso por usuários leigos e a decodificação de diversos de protocolos.

I. Limitações

A entrega dos dados é a etapa mais crítica do processo, que dependendo da forma implementada pode levar a perda de informações. Embora a solução SFTPServer seja a mais segura no ponto de vista da entrega garantida, ela esbarra em questionamentos jurídicos de muitas operadoras, que alegam que sua obrigação legal é de apenas entregar o dado, não devendo armazená-lo, fazendo analogia com a interceptação telefônica. Na solução SFTPClient o armazenamento da informação é por um tempo mínimo, ou seja, apenas uma buferização para evitar a perda dos dados até que ele seja enviado para o OICB, apresentando como desvantagem a geração de uma quantidade imensa de pequenos arquivos de captura, tornando seu gerenciamento complexo. A solução espelhamento de tráfego é a menos recomendada, pois é a mais suscetível em perda de pacotes. O ideal neste caso é o OICB instalar equipamento para capturar os pacotes dentro da rede da operadora e disponibilizá-los remotamente através de um servidor SFTP.

A diversidade de formatos de captura é um complicador, pois nem todas as NFATs suportam os formatos Snoop e ETSI, enquanto o formato pcap é praticamente universal. Para conversão de formatos, pode ser utilizado o programa editcap, que faz parte do pacote Wireshark.

Os diversos formatos de pacotes também adicionam complexidade ao processo, já que as NFATs suportam normalmente apenas pacotes IP com enlace Ethernet e sem encapsulamento IP, que deveria ser o padrão de entrega pelas operadoras. Ferramentas como a Bittwiste [23] podem ser usadas para retirar ou modificar a camada de enlace e para remover encapsulamentos IP quando estes não gerarem fragmentação dos pacotes IP.

As NFATs utilizadas não tem se mostrado muito eficientes para uso nas investigações nos OICBs, pois:

- Não suportam os formatos de arquivo e de pacotes enviados pelas operadoras brasileiras.
- A importação de arquivos de captura deve ser gerenciada pelo investigador, trabalho que seria facilitado caso fosse possível indicar uma pasta local a ser varrida pela ferramenta, importando os arquivos novos de tempos em tempos de forma automática.
- A não decodificação de diversos protocolos importantes para determinadas investigações, tais como *chats* via web e *webmails* brasileiros.
- Demoram receber atualização, deixando de decodificar comunicações quando aplicações proprietárias sofrem alteração de protocolo.
- Não permitem o desenvolvimento de novos filtros (decodificadores de protocolos) nem integração com outras ferramentas, por se tratarem de tecnologia proprietária.
- Ausência de comandos simples para classificação de itens quanto sua importância e geração de relatórios.

4. Metodologia de invetigação

A metodologia de investigação utilizando interceptação de internet observado em um OICB pode ser dividida basicamente em três fases (Fig. 5):

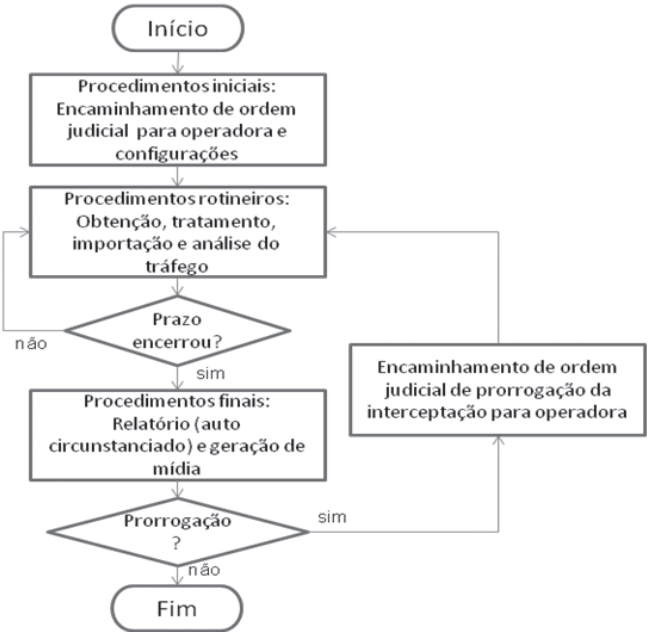

Figura 5. Metodologia de Investigação

1) Procedimentos Iniciais: o processo inicia-se com a emissão por juiz competente de mandado judicial de autorização de afastamento de sigilo telemático com validade de quinze dias. Este mandado deve ser encaminhado à operadora fornecedora da conexão de internet do investigado juntamente com informações para estabelecimento da comunicação para obtenção do tráfego. Com as informações repassadas pela operadora, são realizadas as configurações dos programas e equipamentos na estação de trabalho de análise.
2) Procedimentos Rotineiros: são iniciados tão logo os dados interceptados comecem a ser entregues pela operadora e são realizados em intervalos de tempos regulares. Conforme análise de risco do investigado, esses procedimentos necessitam serem feitos continuamente, pois o acompanhamento dos passos do investigado quase em tempo real pode ser crucial para a investigação. Nesta fase são realizadas a obtenção, tratamento, importação e análise do tráfego.
3) Procedimentos Finais: uma vez vencido ou por vencer o mandado judicial, deve-se confeccionar relatório chamado de auto circunstanciado contendo análise das informações obtidas. No relatório deve-se sugerir pela prorrogação ou não do mandado, que será analisada pelo juiz. Juntamente com o relatório, deve-se encaminhar todo o tráfego obtido com o devido tratamento para sua preservação.

Os Procedimentos Iniciais e os Procedimentos Rotineiros variam dependendo da forma de entrega do tráfego adotado pela operadora, sendo que os Procedimentos Finais são uniformes.

A. Metodologia de Investigação com Entrega "SFTPServer"

Para uma interceptação de uma conexão de uma operadora que fornece os arquivos na forma "SFTPServer" temos os seguintes Procedimentos Iniciais:

1) Envio de mandado: investigador encaminha para a operadora pedido de interceptação telemática da conexão de internet vinculada ao investigado, acompanhado de mandado judicial.
2) Configuração remota: operadora cria conta SFTP em seu servidor de interceptação; configura programa de captura para armazenar os pacotes que trafegam na conexão solicitada em arquivos de captura de determinado tamanho (20MB normalmente) na pasta *home* da conta SFTP criada; informa dados de acesso aos arquivos (IP/porta/usuário/senha).
3) Configuração local: investigador configura programa cliente SFTP e cria pastas "não importados" e "já importados" para armazenamento de arquivos de captura.

Uma vez iniciada a interceptação, os seguintes Procedimentos Rotineiros são realizados:

1) Obtenção: investigador, utilizando o programa cliente SFTP, faz download dos arquivos ainda não baixados do servidor da operadora (para saber qual foi o último arquivo baixado, investigador verifica a pasta "já importados"), exceto o arquivo de captura ainda não finalizado (arquivo de captura não finalizado é o arquivo ainda aberto pelo programa de captura que não alçou o tamanho limite configurado), para a pasta local "não importados".
2) Tratamento: caso os arquivos de captura ou os pacotes nele contidos sejam incompatíveis com o programa de análise, o investigador executa programa de conversão de formato ou de extração de cabeçalhos, gerando novos arquivos de captura. Nessa situação o investigador utiliza uma pasta "tratados" para armazenar os novos arquivos gerados. Os arquivos originais devem ser preservados para encaminhamento junto com o relatório de análise.
3) Importação: investigador, através de comando de importação de arquivos de captura do NFAT, carrega todos os arquivos da pasta "não importados" (ou "tratados", caso tenha sido necessário o procedimento anterior) em ordem cronológica de criação. Após carregados, os arquivos são movidos manualmente para a pasta "já importados".
4) Análise: investigador visualiza, em ordem cronológica, as informações interpretadas pelo programa de análise (páginas *web* acessadas, *e-mails*, conversas realizadas em comunicadores instantâneos, etc.), e os itens que julgar relevantes para a investigação são copiados para relatório de análise, através da área de transferência do sistema operacional; investigador anota a data/hora do último item analisado para retomar o trabalho quando mais arquivos estiverem disponíveis.

Ao fim do prazo de interceptação, os seguintes Procedimentos Finais são realizados:

1) Relatório: investigador revisa seu relatório, que é montado durante os dias de validade do mandado, fazendo buscas na ferramenta de análise pelos itens anteriormente analisados a fim de complementar informações nele contidas. No relatório, o investigador também conclui pelo pedido de renovação ou interrupção da interceptação.
2) Preservação: investigador gera mídia não regravável com os arquivos de captura originais e calcula os seus *hashs*, que são listados no relatório. A mídia passa a ser anexo do relatório durante todo o processo legal.

B. Metodologia de Investigação com Entrega "SFTPClient"

Para uma interceptação de uma conexão de uma operadora que fornece os arquivos na forma "SFTPClient" temos os seguintes Procedimentos Iniciais:

1) Configuração local: investigador cria pastas "não importados" e "já importados" para armazenamento de arquivos de captura; cria conta de usuário no programa servidor SFTP instalado no computador de análise, vinculando a pasta *home* dessa conta à pasta "não importados".
2) Envio de mandado: investigador encaminha para a operadora pedido de interceptação telemática da conexão de internet vinculada ao investigado, acompanhado de mandado judicial, informando dados de acesso (IP/porta/usuário/senha) para envio dos arquivos de captura.
3) Configuração remota: operadora, em seu servidor de interceptação, configura programa de captura para armazenar os pacotes que trafegam na conexão solicitada em arquivos de captura de tamanho pequeno (50KB ou 500KB normalmente) em determinada pasta; configura programa que varre esta pasta a cada intervalo de tempo e os envia para a pasta *home* do usuário do servidor SFTP informado pelo investigador. Após enviados, os arquivos são imediatamente apagados do servidor da operadora. O mesmo ocorre com arquivos que não puderam ser enviados após determinadas tentativas sem sucesso por problemas no servidor SFTP informado.

Uma vez iniciada a interceptação, os seguintes procedimentos são feitos em intervalos regulares:

1) Obtenção: arquivos de captura já são disponibilizados na pasta "não importados" ao serem enviados pela operadora.
2) Tratamento: mesmas considerações da metodologia em IV-A.
3) Importação: além das considerações da metodologia em IV-A, o investigador deve ter especial atenção, pois no período entre o comando de importação e o processo de movimentação, novos arquivos podem ter sido enviados pela operadora e, portanto, não devem ser movidos para a pasta "já importados".
4) Análise: mesmas considerações da metodologia em IV-A.

Os Procedimentos Finais são os mesmos da metodologia em IV-A.

C. Metodologia de Investigação com Entrega "Espelhamento de Tráfego"

Para uma interceptação de uma conexão de uma operadora que fornece os arquivos na forma "espelhamento de tráfego" temos os seguintes Procedimentos Iniciais:

1) Envio de mandado: investigador encaminha para a operadora pedido de interceptação telemática da conexão de internet vinculada ao investigado, acompanhado de mandado judicial, informando o IP para envio dos pacotes espelhados.
2) Configuração remota: operadora, em seu servidor de interceptação, configura programa para copiar os pacotes que trafegam na conexão solicitada para envio para o IP informado (o pacote IP copiado é enviado na área de dados de um pacote IP/GRE ou outro encapsulamento onde o endereço de origem é o IP do equipamento da operadora e o endereço de destino é o IP informado pelo investigador); operadora informa ao investigador o IP de origem dos pacotes;
3) Configuração local: investigador cria pastas "não importados", "desencapsulados" e "já importados" para armazenamento de arquivos de captura; configura programa de captura para armazenar os pacotes que tem como IP de origem o IP informado pela operadora em arquivos de captura de determinado tamanho (10MB normalmente) na pasta "não importados".

Uma vez iniciada a interceptação, os seguintes procedimentos são feitos em intervalos regulares:

1) Obtenção: arquivos de captura já são disponibilizados na pasta "não importados" ao serem gravados pelo programa de captura.
2) Tratamento: investigador executa programa de desencapsulamento para retirar os cabeçalhos IP/GRE ou outro encapsulamento. O programa lê os arquivos de captura da pasta "não importados" (exceto o arquivo de captura ainda não finalizado) e gera novos arquivos na pasta "tratados".
3) Importação: investigador, através de comando de importação de arquivos de captura no programa de análise, carrega todos os arquivos da pasta "tratados" em ordem cronológica de criação dos arquivos originais. Os arquivos originais correspondentes aos desencapsulados são movidos manualmente para a pasta "já importados" e os arquivos da pasta "tratados" são removidos.
4) Análise: mesmas considerações da metodologia em IV-A.

Os Procedimentos Finais são os mesmos da metodologia em IV-A.

D. Discussão

Os Procedimentos Iniciais são os mais complexos e são comumente assistidos por técnico em Tecnologia da Informação (TI), sendo os demais realizados por investigadores especializados no crime sendo investigado (corrupção, desvio de verbas públicas, tráfico de drogas, roubo a bancos, homicídio, etc.), que nem sempre possuem conhecimentos sólidos dessa área.

Alguns Procedimentos Rotineiros (*download* de arquivos de captura, conversão de formatos e desencapsulamento) podem ser automatizados por programas ou *scripts*, mas como as NFATs são programas comerciais fechados e nem sempre permitem execução de comandos através de programas externos, procedimentos manuais são exigidos, e por conseqüência, sujeitos a falhas humanas.

A falta de uma padronização na disponibilização dos dados interceptados pelas operadoras é o principal fator de complexidade, pois são exigidas metodologias de investigação diferentes para cada operadora, inibindo seu uso em uma escala perecida com a usada na interceptação telefônica.

5. Infraestrutura para recebimento de dados

Conforme discutido no item III - Aspectos Técnicos e no item IV - Metodologia da Investigação, o recebimento do tráfego interceptado pelas operadoras trata-se de etapa complexa e sujeita a perda de dados.

Cabe observar que os OICBs possuem órgãos centrais localizados nas capitais estaduais ou federal com funções de gestão e normatização, sendo que as investigações são realizadas pelas suas unidades descentralizadas responsáveis pela circunscrição de local onde o crime é cometido.

Neste item é proposto uma infraestrutura centralizada para recebimento dos dados interceptados, aqui chamada de Servidor de Interceptação Telemática (SIT), que objetiva a padronização na entrega dos dados para a equipe de investigação na forma SFTPServer, e como conseqüência unificando a metodologia de investigação.

A. Servidor de Interceptação Telemática (SIT)

O SIT é composto basicamente por servidor com armazenamento, conexão a internet, faixa de IPs fixos, sistema operacional, *software* servidor SFTP e programa de captura de pacotes (*sniffer*) (Fig. 6).

O SIT deve ser instalado no *datacenter* do OICB, sendo visível através da internet para recebimento do tráfego e da intranet do órgão para entrega do tráfego às unidades descentralizadas.

A fim de minimizar a perda de pacotes pelo programa de captura, é indicado o uso de, pelo menos, três interfaces de rede (NICs – *Network Interface Cards*): a primeira configurada com um IP público respondendo a conexões das operadoras através da internet ao servidor SFTP, a segunda configurada com um IP privado da intranet respondendo a conexões da intranet ao servidor SFTP e a terceira respondendo por uma faixa de IPs púbicos que terão como destino pacotes "espelhados" de uma conexão alvo enviados pelas operadoras.

Como o SIT envolve o uso de programas de uso geral (Sistema Operacional - SO, servidor SFTP e programa de captura), ele pode ser implementado na plataforma de SO escolhida pelo OICB .

B. Administração do SIT

O SIT deve ser administrado por equipe gestora designada e formada por técnicos em TI, que atende pedidos dos responsáveis pelas investigações das unidades descentralizadas. O pedido inclui identificação da operadora e cópia do mandado judicial de afastamento de sigilo de comunicação de dados.

Caso a operadora indicada entregue os dados na forma "SFTPClient", a equipe gestora cria uma conta SFTP no SIT e responde o pedido com as seguintes informações: IP e porta do servidor SFTP, usuário e senha da conta criada. O responsável pela investigação comunica a operadora da autorização e os dados da conta SFTP para envio dos dados. A

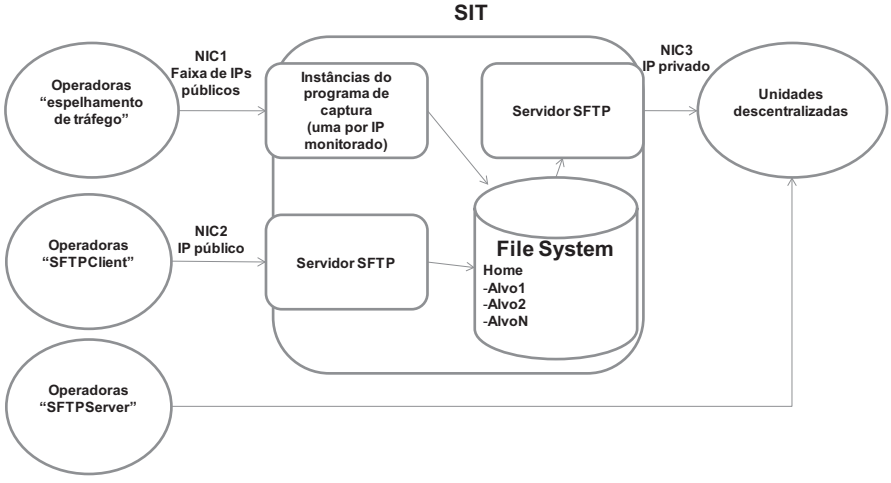

Figura 6. Servidor de Interceptação Telemática

mesma conta SFTP será utilizada para obtenção dos arquivos de captura pelos investigadores.

Caso a operadora indicada entregue os dados na forma "espelhamento de tráfego", a equipe gestora cria uma conta SFTP no SIT, reserva um endereço IP da faixa de IPs públicos e ativa um processo *sniffer* que captura todo o tráfego que tem como IP destino o IP reservado gravando-o em arquivos de captura na pasta *home* da conta SFTP criada. A equipe gestora responde o pedido com as seguintes informações: IP destino da interceptação e os dados da conta SFTP criada (IP e porta do servidor SFTP, usuário e senha). O responsável pela investigação comunica a operadora do mandado e o IP para envio dos dados. A conta SFTP será utilizada para obtenção dos arquivos de captura pelos investigadores.

No caso das operadoras que entregam os dados na forma "SFTPServer" não há a necessidade do uso do SIT, já que a obtenção dos arquivos de caputra pode ser realizada diretamente no servidor da operadora.

C. Benefícios

Além de cumprir seu objetivo de unificar a entrega de dados interceptados para a equipe de investigação nas unidades descentralizadas simplificando o processo, uma infraestrutura centralizada como esta proposta apresenta como benefícios:

- Aproveitamento da infraestrutura centralizada (*datacenter* com refrigeração, energia, segurança, equipe especializada, etc.) e descentralizada (estações de trabalho) e sua interligação (intranet), necessitando apenas de investimento em servidor e conexão de internet no *datacenter*, evitando investimentos em diversas unidades descentralizadas.
- Menores custos no investimento com conexão de internet, já que o preço tende a ser mais baixo nas capitais, além de disponibilidade de bandas maiores.
- Parte mais complexa da interceptação (instalação e configuração de programa servidor SFTP e de captura de pacotes, configurações de rede e validação da comunicação com as operadoras) passa a ser executada por técnicos em TI qualificados.

6. Ferramenta para Obtenção, Tratamento, Importação e Análise

Conforme discutido no item III - Aspectos Técnicos, as NFATs disponíveis não têm atendido as necessidades dos OICBs. No item IV – Metodologia da Investigação foi apresentado que os Procedimentos Rotineiros, que deveriam ser apenas a análise dos novos dados entregues, acaba tendo que ser divido nas fases obtenção, tratamento, importação e análise, devido a falta de compatibilidade com a forma de disponibilização dos dados pelas operadoras brasileiras.

Neste item é proposta uma nova NFAT, desenvolvida com base em requisitos levantados, de forma a simplificar as investigações envolvendo interceptações telemáticas, melhorar seus resultados e aumentar seu uso.

A. Requisitos da NFAT

A partir da análise dos aspectos jurídicos e técnicos e da metodologia empregada nas investigações, os seguintes requisitos foram levantados para uma NFAT:

- Permitir a análise separada de várias conexões de internet interceptadas em um mesmo computador.
- Ter um módulo cliente SFTP integrado, que configurado adequadamente, deve baixar os arquivos de captura do servidor da operadora ou do SIT ainda não baixados, e com função de continuação de download de arquivos parcialmente baixados.
- Ter como entrada uma pasta de arquivos de captura, devendo processar todos os arquivos nela existentes de tempos em tempos em ordem cronológica, mantendo registro dos arquivos já processados e arquivos processados parcialmente.
- Ser independente do SIT, permitindo seu uso integrado com um programa de captura gravando os pacotes de rede em arquivos de captura, com um servidor SFTP que recebe os arquivos de captura da operadora ou ainda alimentado manualmente com arquivos de captura na sua pasta de leitura.
- Reconhecer os formatos de arquivo de captura pcap, Snoop e ASN.1 – ETSI.
- Reconhecer os pacotes IPs encapsulados com enlaces Ethernet, LCC, PPPoE e VLAN e combinações entre eles.
- Reconhecer os pacotes IPs encapsulados em pacotes de rede IP/UDP, Juniper, PCLI e TZSP e IP/GRE tratando adequadamente a fragmentação gerada.
- Permitir a análise do tráfego interceptado quase que em tempo real.
- Reconhecer fluxos TCP e UDP fragmentados em diversos arquivos de captura.
- Possuir tanto interface gráfica quanto por linha de comando, permitindo automatização de tarefas através de *scritps*.
- Permitir a integração com módulos externos de reconhecimento de protocolos de aplicação (filtros) provendo uma interface de fácil leitura dos fluxos TCP e UDP.
- Reconhecer, através de módulos Filtros, pelo menos os protocolos abertos HTTP, POP, SMTP e RTP, mensagens enviadas ou lidas e seus anexos através dos principais serviços de *webmail* utilizados no Brasil, conversas realizadas pelos principais aplicativos de mensagens instantâneas e suas versões *web* e nas redes sociais mais utilizadas.

Os requisitos definidos para os módulos Filtros são:

- Gerar um ou mais objetos (registros no banco de dados de informação interceptada reconhecida) apontando para arquivos a serem gerados no sistema de arquivos,

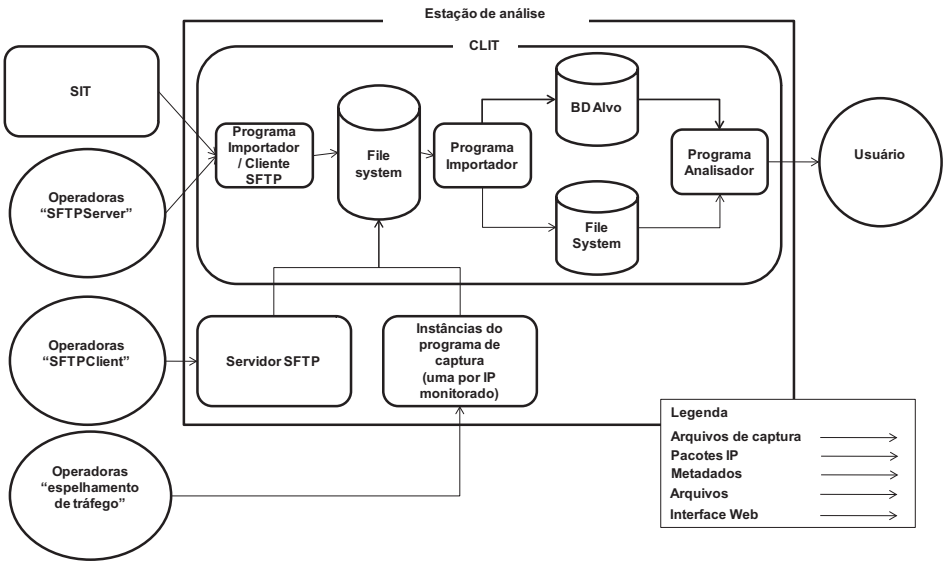

Figura 7. Cliente de Interceptação Telemática (CLIT)

prevendo sua exibição em navegador *web*, quando reconhecer o seu protocolo a partir de um fluxo.

- Incorporar, quando possível, parametrização para classificação automática de relevância para análise dos objetos.

Os requisitos definidos para a interface de análise:

- Ter interface gráfica simples, nos moldes das ferramentas de interceptação telefônica, que exiba tabela com os metadados dos objetos reconhecidos, exiba o conteúdo do objeto selecionado em uma interface web,
- Possibilitar classificação quanto à relevância para a investigação e de inserção de comentário ao objeto selecionado;
- Possibilitar análise em ordem cronológica com fácil identificação do ponto em que foi interrompida a análise anterior;
- Ter, pelo menos, possibilidade de filtro pelos metadados dos objetos;
- Ter formas de exportação de um ou mais objetos selecionados para elaboração de relatório de análise.

B. Cliente de Interceptação Telemática (CLIT)

A ferramenta desenvolvida para obtenção, tratamento, importação e análise, aqui chamada de CLIT (Fig. 7), é composta por dois programas: o Importador e o Analisador.

1) Programa Importador

O programa Importador é o responsável pela obtenção, tratamento e importação dos arquivos de captura, alimentando um banco de dados da conexão interceptada (alvo). Uma vez configurado para determinada interceptação, funciona de forma totalmente automática. Uma instância do programa Importador deve ser executada por alvo, recebendo como parâmetros os dados da conta SFTP onde estão os arquivos de captura (opcional), a pasta local dos arquivos de captura e o banco de dados a ser alimentado.

Possui os seguintes módulos (Fig. 8):

- Coletor: obtêm os arquivos de captura de um servidor SFTP, armazenando-os em uma pasta local. Seu uso é opcional, já que os arquivos de captura podem já estar disponíveis localmente através de um servidor SFTP ou por um programa de captura.
- Gerenciador de Arquivos: mantêm informações de quais arquivos de captura da pasta local já foram processados, parcialmente processados ou não processados. Garante que os arquivos de captura serão processados em ordem cronológica.
- Extrator de Streams: lê os pacotes IP contidos nos arquivos de captura e extrai os fluxos TCP e UDP dos arquivos de captura gerando estruturas mais simples de serem processadas, chamadas de "arquivos de fluxo". Reconhece os formatos de arquivo Pcap, Snoop e ETSI, os enlaces Ethernet, LCC, PPPoE e VLAN e os encapsulamentos IP/UDP, Juniper, PCLI e TZSP e IP/GRE.
- Gerenciador de Filtros: entrega os arquivos de fluxo para os módulos filtros configurados.
- Filtro: módulo que identifica determinado tipo de protocolo de aplicação a partir de um arquivo de fluxo, gerando como saída uma visualização de alto nível para o usuário. Foram implementados filtros para os protocolos abertos HTTP, POP, SMTP e RTP, para protocolos proprietários de *chat* do Windows Live Messenger [24]e Yahoo!Messenger [25], de *e-mails* e seus anexos dos serviços de *webmail* Hotmail [26] e Yahoo!Mail [27] e de *chats* através das redes sociais Orkut [28] e Facebook [29]. Os Filtros ainda classificam os objetos identificados como "Alerta", "Normal", "Sem importância" através de políticas internas do módulo ou configurações.

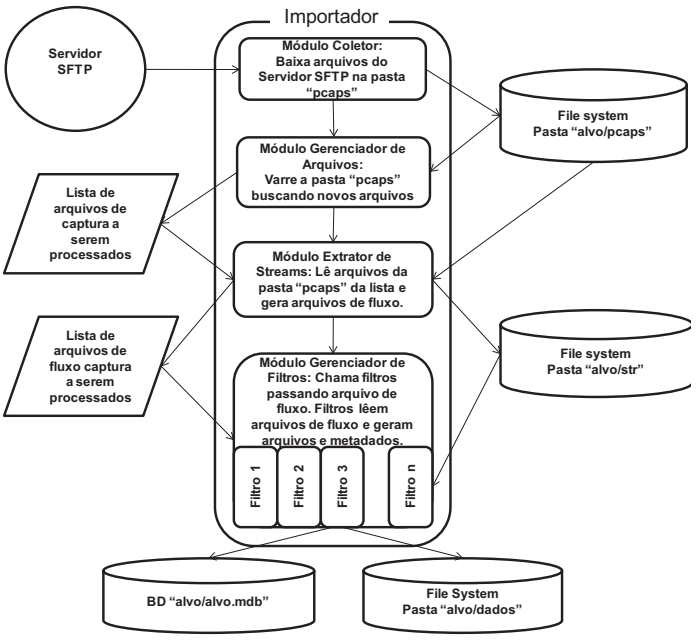

Figura 8. Módulos do Programa Importador

2) Programa Analisador

O programa Analisador é o programa que permite ao investigador abrir o banco de dados gerado pelo programa Importador, a visualização e classificação das informações interpretadas e a exportação para relatório.

Sua interface (Fig. 9) é composta basicamente por uma tabela que exibe os metadados dos objetos extraídos (um por linha) e um navegador de internet que exibe o conteúdo do objeto, além de opções de filtragem de objetos a serem exibidos na tabela.

Permite, através de menu de contexto ou teclas de atalho, que o usuário classifique os objetos como "Importantes" ou "Não Importantes", além de anotações que podem ser posteriormente buscadas. A exportação para relatório é realizadas através de comando que gera uma imagem de cada item selecionado para ser "colada" em um editor de textos.

C. Benefícios

Apesar de não decodificar uma grande quantidade de protocolos e aplicações, o CLIT desenvolvido já pode ser utilizado em na grande maioria das investigações, pois estas objetivam normalmente a captura de comunicações entre as pessoas investigadas (*chats* e *e-mails*), função essa já bem desempenhada pela ferramenta.

O CLIT cumpre o seu objetivo maior, que é a simplificação nas investigações, com a automatização dos processos e, em conseqüência, redução nos erros humanos, já que:

- Arquivos de captura não precisam ser baixados manualmente, já que o CLIT possui um cliente SFTP integrado que baixa apenas arquivos ainda não baixados e reassume *downloads* de arquivos baixados parcialmente.
- É compatível com todos os formatos de arquivos de captura e formatos de pacotes IPs encaminhados pelas operadoras brasileiras.
- Faz importação automática dos novos arquivos de captura que forem gravados na sua pasta
- Permite o acompanhamento quase que em tempo real do investigado, já que processa arquivos de captura abertos pelos programas de captura, guardando em qual pacote parou de processar e reassumindo do ponto de parada.
- Permite o acompanhamento de várias interceptações em uma mesma estação de trabalho, sem riscos de importações de arquivos de captura de outra interceptação.
- Pré-classificação de objetos interpretados quanto a sua relevância.
- Ferramenta de análise com funções de visualização, classificação e exportação de objetos interpretados.

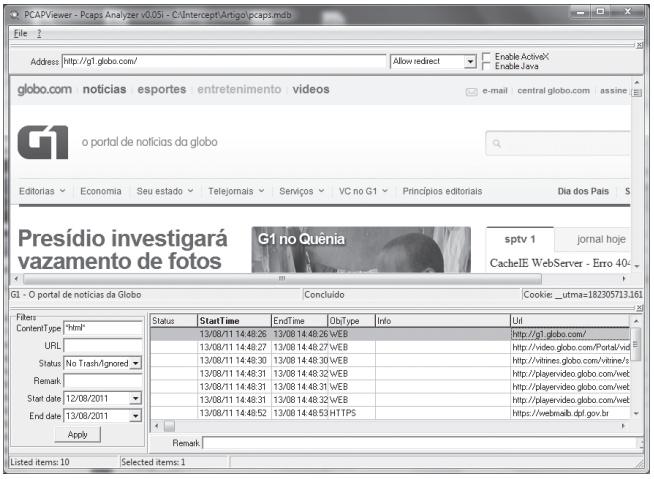

Figura 9. Interface do Programa Analisador

Os módulos Filtros do CLIT precisam de manutenção periódica, pois serviços de *webmail* e aplicativos de comunicação em geral recebem inovações cada vez mais freqüentes.

7. Metodologia de Investigação com SIT e CLIT

Com a utilização do SIT e o CLIT em um OICB, uma metodologia de investigação mais simples passa a ser aplicada dentro das fases de Procedimentos Iniciais, Rotineiros e Finais.

A. Procedimentos Iniciais

Os Procedimentos Iniciais variam dependendo da forma de entrega de dados pela operadora. Para operadoras que entregam na forma SFTPServer, as etapas são:

1) Envio de Mandado: investigador encaminha para a operadora pedido de interceptação telemática da conexão de internet vinculada ao investigado, acompanhado de mandado judicial.

2) Configuração Remota: operadora cria conta SFTP em seu servidor de interceptação; configura programa de captura para armazenar os pacotes que trafegam na conexão solicitada em arquivos de captura de determinado tamanho (20MB normalmente) na pasta *home* da conta SFTP criada; informa dados de acesso aos arquivos (IP/porta/usuário/senha).
3) Configuração Local: investigador cria pasta para a nova interceptação e configura programa o CLIT com as informações da conta SFTP e pasta criada.

Para operadoras que entregam na forma SFTPClient, as etapas são:

1) Pedido Conta SIT: investigador envia pedido de criação de SFTP para interceptação identificando a operadora.
2) Configuração SIT: equipe gestora do SIT cria conta SFTP e informa dados de acesso (IP/porta/usuário/senha).
4) Envio de mandado: investigador encaminha para a operadora pedido de interceptação telemática da conexão de internet vinculada ao investigado, acompanhado de mandado judicial, informando dados de acesso (IP/porta/usuário/senha) para envio dos arquivos de captura.
5) Configuração remota: operadora, em seu servidor de interceptação, configura programa de captura para armazenar os pacotes que trafegam na conexão solicitada em arquivos de captura de tamanho pequeno (50KB ou 500KB normalmente) em determinada pasta; configura programa que varre esta pasta a cada intervalo de tempo e os envia para a pasta home do usuário do servidor SFTP informado pelo investigador. Após enviados, os arquivos são imediatamente apagados do servidor da operadora. O mesmo ocorre com arquivos que não puderam ser enviados após determinadas tentativas sem sucesso por problemas no servidor SFTP informado.
6) Configuração Local: investigador cria pasta para a nova interceptação e configura programa o CLIT com as informações da conta SFTP e pasta criada.

Para operadoras que entregam na forma espelhamento de tráfego, as etapas são:

1) Pedido Conta SIT: investigador envia pedido de criação de SFTP para interceptação identificando a operadora.
2) Configuração SIT: equipe gestora do SIT cria conta SFTP, reserva um IP da faixa disponível e ativa programa de captura para gravar os pacotes destinados ao IP reservado na pasta *home* da conta SFTP criada. Informa dados de acesso (IP/porta/usuário/senha) e IP para envio dos pacotes espelhados.
3) Envio de mandado: investigador encaminha para a operadora pedido de interceptação telemática da conexão de internet vinculada ao investigado, acompanhado de mandado judicial, informando o IP para envio dos pacotes espelhados.
4) Configuração remota: operadora, em seu servidor de interceptação, configura programa para copiar os pacotes que trafegam na conexão solicitada para envio para o IP informado (o pacote IP copiado é enviado na área de dados de um pacote IP/GRE ou outro encapsulamento onde o endereço de origem é o IP do equipamento da operadora e o endereço de destino é o IP informado pelo investigador);
5) Configuração Local: investigador cria pasta para a nova interceptação e configura programa o CLIT com as informações da conta SFTP e pasta criada.

B. Procedimentos Rotineiros

Os Procedimentos Rotineiros passam a ser compostos por apenas uma etapa, já que as etapas de Obtenção, Tratamento e Importação são realizadas de forma automática pelo programa Importador do CLIT:

1) Análise: investigador filtra os objetos ainda não classificados, visualiza em ordem cronológica as informações interpretadas pelo programa de análise (páginas *web* acessadas, *e-mails*, conversas realizadas em comunicadores instantâneos, etc.), classifica os itens analisados como "Importantes" ou "Não Importantes" para a investigação e registra anotações pertinentes.

C. Procedimentos Finais

Os Procedimentos Finais, realizados no final do prazo de interceptação, continua a apresentar as etapas de Relatório e Preservação, sendo que a última permanece como era:

1) Relatório: investigador, através de comando no CLIT, seleciona todos os objetos marcados como "Importantes", exportá-os como imagens e colá-las no editor de textos, registra seus comentário, podendo realizar novas buscas nos metadados dos objetos no CLIT afim de localizar novas informações relevantes. No relatório, o investigador também conclui pelo pedido de renovação ou interrupção da interceptação.
2) Preservação: investigador gera mídia não regravável com os arquivos de captura originais e calcula os seus *hashs*, que são listados no relatório. A mídia passa a ser anexo do relatório durante todo o processo legal.

D. Discussão

Os Procedimentos Iniciais continuam variando dependendo da forma de entrega de dados pela operadora apenas nas suas etapas burocráticas (envio e recebimento de pedidos e mandados), já que a etapa de Configuração Local (etapa técnica) passa a ser única, podendo ser facilmente realizada por investigador sem conhecimentos sólidos de TI.

Nos Procedimentos Rotineiros, que é a fase repetitiva do processo e, portanto, mais desgastante para o usuário, não existem mais as etapas de Obtenção, Tratamento e Importação, já que o CLIT faz *download* dos arquivos de captura, é compatível com os formatos de arquivos e pacotes

enviados pelas operadoras brasileiras e faz o gerenciamento de arquivos importados/não importados de forma automática. A etapa de Análise também é simplificada, já que o CLIT permite que o investigador selecione todos os objetos ainda não classificados, ou seja, o ponto em parou sua análise, evitando que o investigador necessite anotar o seu ponto de parada. Na Análise também não há mais a necessidade de ficar montando o relatório, já que o CLIT permite a classificação dos objetos e a anotação de informações pertinentes, que poderão ser recuperadas na etapa de Relatório dos Procedimentos Finais.

Nos Procedimentos finais a etapa de relatório é simplificada, pois o investigador pode, através de comando no CLIT, selecionar todos os objetos marcados como "Importantes", exportá-los como imagens e colá-las no editor de textos.

Portanto, uma análise comparativa da metodologia de investigação anterior utilizando as ferramentas antes disponíveis e a metodologia utilizando o SIT e o CLIT propostos é que melhor demonstra o poder dessas duas novas ferramentas. As dificuldades técnicas passam a ser assumidas por técnicos em TI e as ferramentas disponibilizadas e o investigador passa a executar apenas suas atribuições originais que são de solicitar quebra de sigilo, analisar os dados recebidos e relatar o encontrado.

8. Conclusão e Trabalhos Futuros

O uso mais freqüente de interceptações de conexão de internet nas investigações criminais passa por dois desafios: a padronização da disponibilização dos dados interceptados pelas operadoras e o desenvolvimento ou adequação de ferramentas considerando a realidade brasileira.

A padronização na disponibilização dos dados pelas operadoras com forma de entrega SFTPServer, arquivos em formato pcap contendo pacotes IP não encapsulados apenas com enlace Ethernet é a solução ideal sob o ponto de vista das OICBs, pois apresenta a melhor confiabilidade na entrega do tráfego, maior compatibilidade com as NFATs disponíveis no mercado e menor complexidade na metodologia de investigação. Sensibilizar a Agência Nacional de Telecomunicações (ANATEL) para editar uma norma com prazo para que as operadoras possam se adequar seria o caminho mais curto para obter para obter essa padronização desejada, ou outra que a unifique.

Neste artigo foi apresentada ainda uma infraestrutura central para recebimento de tráfego (SIT) que simplifica a metodologia de investigação (Procedimentos Iniciais e etapa Obtenção dos Procedimentos Finais), pois unifica a forma de obtenção dos dados SFTPServer para unidades descentralizadas, tirando do investigador a etapa técnica mais complexa, que é a configuração de programas servidor SFTP e de captura de tráfego.

Também foi apresentada uma ferramenta para obtenção, tratamento, importação e análise de dados interceptados (CLIT) adequada aos aspectos técnicos envolvidos na disponibilização do tráfego pelas operadoras brasileiras (forma de entrega e formato de arquivos e pacotes) simplificando ainda mais a metodologia de investigação (Procedimentos Rotineiros e etapa Relatório dos Procedimentos Finais), pois elimina diversas etapas complexas e possui funções de análise (pré-classificação, marcação de itens examinados quanto à relevância e exportação para relatório) inexistentes nas NFATs até então utilizadas.

Embora as ferramentas apresentadas sejam independentes, seu uso combinado exige pequeno investimento e potencializa o uso mais frequente da interceptação de internet nas investigações.

Como trabalho futuro sugere-se o desenvolvimento de filtros para o CLIT que decodifiquem protocolos FTP, IRC, IMAP, comunicações realizadas em outros aplicativos de comunicação instantânea, redes sociais, *webmails*, *chats* via web e aplicativos para dispositivos móveis.

Referências

[1] Brasil. Lei nº 4.117, de 27 de agosto de 1962.
[2] Brasil, Constituição, 1998.
[3] Brasil, Lei nº 9.296, de 24 de julho de 1996.
[4] Brasil, CNJ, Resolução nº 59 de 9 de agosto de 2008.
[5] CNJ, Portal CNJ – Sobre o CNJ, disponível em http://www.cnj.jus.br/sobre-o-cnj, acessado em 31/07/2011.
[6] Teleco, teleco.com.br, disponível em http://www.teleco.com.br/mshare_wcdma.asp, acessado em 31/07/2011.
[7] Teleco, teleco.com.br, disponível em http://www.teleco.com.br/blarga.asp, acessado em 31/07/2011.
[8] Wireshark, "Development-LibpcapFileFormat - The Wireshark Wiki". http://wiki.wireshark.org/Development/LibpcapFileFormat, acessado em 31/07/2011.
[9] B. Callaghan, R. Gilligan. RFC 1761: Snoop Version 2 Packet Capture File Format, 2005.
[10] ISO/IEC FDIS 8824, Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation, 2002.
[11] ETSI, ETSI TS 102 232-3 v2.1.1 - Lawfull Interception (LI); Handeover Interface and Servide-Specific Details (SSD) for IP delivery; Part 3: Service-specific details for internet access services, 12/2006.
[12] Juniper, RADIUS - Based Mirroring, http://www.juniper.net/techpubs/software/erx/junose60/swconfig-system-basics/html/lawful-intercept-config6.html, acessado em 31/07/2011.
[13] Cable Television Laboratories, PacketCable Electronic Surveillance Specification PKT-SP-ESP-I03-040113, 2004.
[14] Wikipedia, TZSP, http://en.wikipedia.org/wiki/TZSP, acessado em 31/07/2011.
[15] T. Li, S. Hanks, D. Meyer e P. Traina, RFC 2784: Generic Routing Encapsulation (GRE), 2000.
[16] V. Corey, C. Peterman, S. Shearin, M. S. Greenberg e J. Van Bokkelen, Network Forensics Analysis, em IEEE Internet Computing, novembro/dezembro-2002, pp. 60-66.
[17] Wireshark, disponível em http://www.wireshark.org/, acessado em 31/07/2011.
[18] Tcpdump, disponível em http://www.tcpdump.org/, acessado em 31/07/2011.
[19] E. S. Pilli, R.C. Joshi, R. Niyogi, Network Forensic Frameworks: Survey and Research Challenges, em Digital Intestigation 7, 2010, pp.14-27.
[20] Netresec NetworkMiner, , disponível em http://www.netresec.com/?page=NetworkMiner, acessado em 31/07/2011.
[21] Netwitness Investigator, disponível em http://www.netwitness.com/products-services/investigator-freeware, acessado em 31/07/2011.
[22] Tamos NetResident, disponível em http://www.tamos.com/products/netresident/, acessado em 31/07/2011

[23] Bittwiste, disponível em http://bittwist.sourceforge.net/, acessado em 31/07/2011.
[24] Windows Live Messenger, disponível em http://messenger.msn.com/, acessado em 31/07/2011.
[25] Yahoo!Messenger, disponível em http://messenger.yahoo.com/, acessado em 31/07/2011.
[26] Microsoft Hotmail, disponível em http://hotmail.com/, acessado em 31/07/2011.
[27] Yahoo!Mail, disponível em http://mail.yahoo.com/, acessado em 31/07/2011.
[28] Orkut, disponível em http://orkut.com/, acessado em 31/07/2011.
[29] Facebook, disponível em http://facebook.com/, acessado em 31/07/2011.