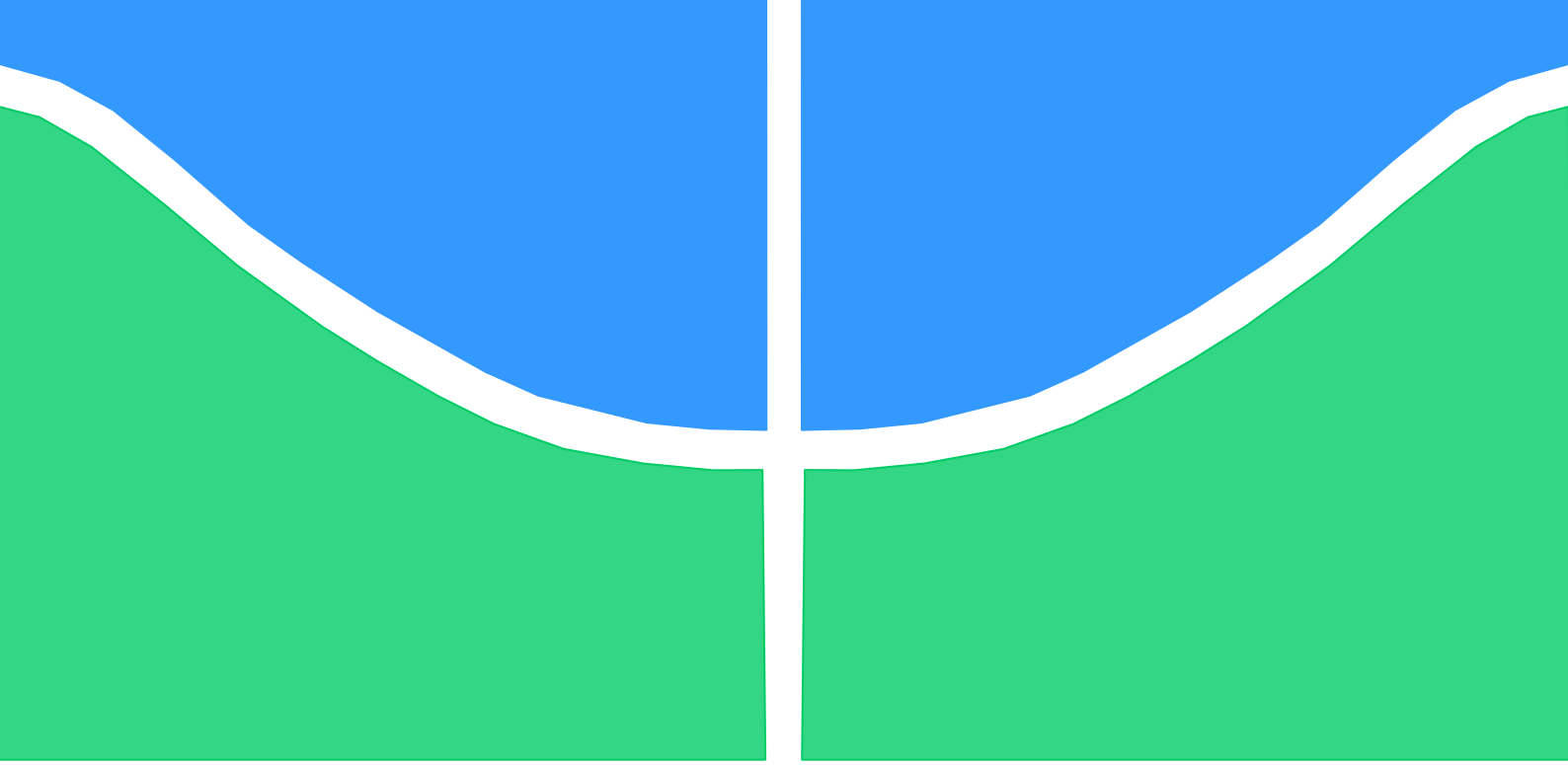


TRABALHO DE GRADUAÇÃO

MOBILE BANKING: METODOLOGIA PARA ANÁLISE DE PACOTES

Yuri Aranha Kawagoe
Orientador: Laerte Peotta de Melo

Brasília, Setembro de 2012

Faculdade de Tecnologia

Universidade de Brasília

TRABALHO DE GRADUAÇÃO

MOBILE BANKING: METODOLOGIA PARA ANÁLISE DE PACOTES

Yuri Aranha Kawagoe

Relatório submetido como requisito parcial para obtenção
do grau de Engenheiro de Redes de Comunicação.

Banca Examinadora

Prof. Dr. Laerte Peotta de Melo, UnB/ ENE
(Orientador) _____

Prof.ª Dra. Edna Dias Canedo, UnB/ ENE _____

Prof. Me. Dino Macedo Amaral, UnB/ ENE _____

Brasília, Setembro de 2012

FICHA CATALOGRÁFICA

YURI, KAWAGOE
Mobile Banking: Metodologia para Análise de Pacotes,
[Distrito Federal] 2012.
xvii, 45 p., 297 mm (FT/UnB, Engenheiro, Redes de Comunicação, 2012).
Trabalho de Graduação – Universidade de Brasília. Faculdade de Tecnologia.

1. *Mobile Banking* 2. Segurança da Informação
3. Pacotes de dados 4. Dispositivos Móveis

I. Redes de Comunicação/FT/UnB II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

KAWAGOE, YURI A., (2012). *Mobile Banking*: Metodologia para Análise de Pacotes. Trabalho de Graduação em Engenharia de Redes de Comunicação, Publicação FT.TG-nº -, Faculdade de Tecnologia, Universidade de Brasília, Brasília, DF, 59p.

CESSÃO DE DIREITOS

AUTOR: Yuri Aranha Kawagoe.

TÍTULO DO TRABALHO DE GRADUAÇÃO: *Mobile Banking*: Metodologia para Análise de Pacotes.

GRAU: Engenheiro ANO: 2012

_____

Yuri Aranha Kawagoe
SRES Quadra 03, Bloco J, casa 57 – Cruzeiro Velho.
70640-105 Brasília – DF – Brasil.

DEDICATÓRIA

Dedico este trabalho a Oswaldo Hideo Kawagoe, Engenheiro Eletricista e Bacharel em Matemática pela Universidade de Brasília, grande pai e amigo de quem sinto a falta todos os dias. Dedico também a Verônica Aranha Kawagoe, mãe que, apesar de nunca ter cursado uma universidade é dotada de uma sabedoria incontestável e é presença constante na minha vida.

AGRADECIMENTOS

Ao meu orientador Prof. Dr. Laerte Peotta de Melo: Pelo constante apoio, incentivo, paciência, dedicação e amizade, essenciais para o desenvolvimento deste trabalho e para o meu desenvolvimento como engenheiro.

Ao Prof. Dr. Anderson Clayton Nascimento, do Curso de Engenharia de Redes de Comunicação - Departamento de Engenharia Elétrica: Pela inspiração profissional, ensinamentos e conselhos.

Aos meus colegas da Universidade de Brasília: Pelas conversas enriquecedoras, ajuda em diversos momentos, colaboração e amizade.

Aos meus colegas de trabalho: Pela colaboração, amizade, ensinamentos e troca de experiências que propiciaram um grande crescimento pessoal e profissional.

A minha família: pelo apoio, amor e compreensão constantes em todas as etapas da minha vida.

A Júlia Mezzomo de Souza que me motivou em alguns momentos nos quais duvidei do meu potencial, e também por estar comigo durante grande parte da minha vida universitária.

A todos, os meus sinceros agradecimentos.

Yuri Aranha Kawagoe.

RESUMO

MOBILE BANKING: METODOLOGIA PARA ANÁLISE DE PACOTES

Autor: Yuri Aranha Kawagoe

Orientador: Laerte Peotta de Melo

Projeto Final de Graduação

Brasília, mês de Setembro (2012)

O trabalho descrito nesta dissertação objetiva definir uma metodologia de análise de dados relacionados a operações bancárias feitas a partir de dispositivos móveis para obter resultados relacionados à segurança da informação, bem como instrumentalizar essa metodologia com o objetivo de reconhecer possíveis vulnerabilidades e descrever qualitativamente a consistência dos dados dessas operações, utilizando um conjunto de softwares que permitirão a interceptação de pacotes trafegando em uma rede sem fio, uma análise mais acurada da informação e um estudo mais detalhado dos dados obtidos.

Palavras Chave: Segurança da Informação, Mobile Banking, Pacotes, Dispositivos Móveis, Telefones Inteligentes.

ABSTRACT

MOBILE BANKING: METHODOLOGY FOR DATA PACKAGE ANALYSIS

Author: Yuri Aranha Kawagoe

Supervisor: Laerte Peotta de Melo

Graduation Thesis

Brasília, mês de Setembro (2012)

The work described in this thesis aims at defining a method for data analysis of banking transactions made through mobile devices to achieve results related to the area of information security, as well as providing a methodology with guidelines to recognize any vulnerability and qualitatively describe the consistency of data from those transactions. Using software set that will allow the interception of wireless network data flow, an accurate information analysis and a deeper study of the obtained data.

Keywords: Information Security, Mobile Banking, Data Frames, Mobile Devices, Smartphones.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE SÍMBOLOS, NOMENCLATURAS E ABREVIAÇÕES

ABA – *American Bankers Association*

CBC – *Cipher Block Chaining*

DNS – *Domain Name System*

DOC – Documento de Crédito

ETH – *Ethernet*

ETSI – *European Telecommunications Standards Institute*

FEBRABAN – Federação Brasileira de Bancos

GPS – *Global Positioning System*

HTTP – *Hyper Text Transfer Protocol*

IDC – *International Data Corporation*

IEEE – *Institute of Electrical and Electronics Engineers*

IP – *Internet Protocol*

LAN – *Local Area Network*

MD4 – *Message Digest 4*

MD5 – *Message Digest 5*

MITM – *Man-in-the-middle*

MFS – *Mobile Financial Services*

NAT – *Network Address Translation*

NFC – *Near Field Communication*

NIST – *National Institute of Standards and Technology*

PC – *Pocket Computer*

PDA – *Personal Digital Assistant*

RC4 – *Rivest Cipher 4*

RSA – *Rivest-Shamir-Adleman*

SHA – *Secure Hash Algorithm*

SIP - *Session Initiation Protocol*

SSL – *Secure Sockets Layer*

TCP – *Transmission Control Protocol*

TED – Transferência Eletrônica Disponível

UDP – *User Datagram Protocol*

USB – *Universal Serial Bus*

VoIP – *Voice over Internet Protocol*

WLAN – *Wireless Local Area Network*

WECA – *Wireless Ethernet Compatibility Alliance*

WEP – *Wired Equivalent Privacy*

WPA – *Wi-Fi Protected Access*

WPA2 – *Wi-Fi Protected Access II*

1. INTRODUÇÃO

O *Mobile Banking*, serviço financeiro voltado para dispositivos móveis, se popularizou em paralelo ao aumento do número de telefones celulares. A difusão desses aparelhos elevou o número de usuários do serviço. Com o aumento das vendas globalmente, as grandes empresas do setor de telefonia móvel investiram em novas tecnologias, desenvolveram aparelhos mais complexos, apresentando dispositivos com interfaces mais amigáveis aos usuários, capazes de conexões mais rápidas com a rede mundial de computadores e com níveis de processamento cada vez mais elevados. Tais avanços permitiram que novos serviços bancários fossem agregados ao *Mobile Banking*, facilitando muitas operações bancárias feitas a partir desses dispositivos.

A popularidade dos serviços bancários via dispositivos móveis e a possibilidade de realizar transações bancárias complexas atraíram os chamados - cyber criminosos - ou criminosos cibernéticos, nomenclatura referente ao termo *computer crime* (Crime de computador) que remete a qualquer tipo de crime que envolva um computador e uma rede. Dessa forma, o *Mobile Banking* se torna um objeto de preocupação a todos os profissionais de segurança da informação, que buscam novos meios de impedir que agentes maliciosos causem danos a organizações, empresas e usuários.

A fim de reconhecer possíveis vulnerabilidades na comunicação do dispositivo móvel com a *internet*, desenvolveu-se neste trabalho uma metodologia para captura de pacotes referentes à troca de dados entre usuário e instituição financeira através de um *smartphone* (telefone inteligente), que consiste em um telefone móvel com certas funcionalidades de um computador, capaz de rodar programas aplicativos e acessar diretamente uma conexão com o banco sem a necessidade de utilizar o navegador do dispositivo.

1.1. OBJETIVOS

Este trabalho visa estabelecer uma metodologia para a captura de pacotes de dados provenientes da comunicação entre um dispositivo móvel do tipo “smartphone” rodando o sistema operacional “*Android”*, na versão 2.1 (“*Eclair*”) com a rede mundial de computadores. Tais pacotes referem-se às tentativas de acesso em contas bancárias com contas e senhas fictícias através de aplicativos bancários, previamente instalados, pertencentes

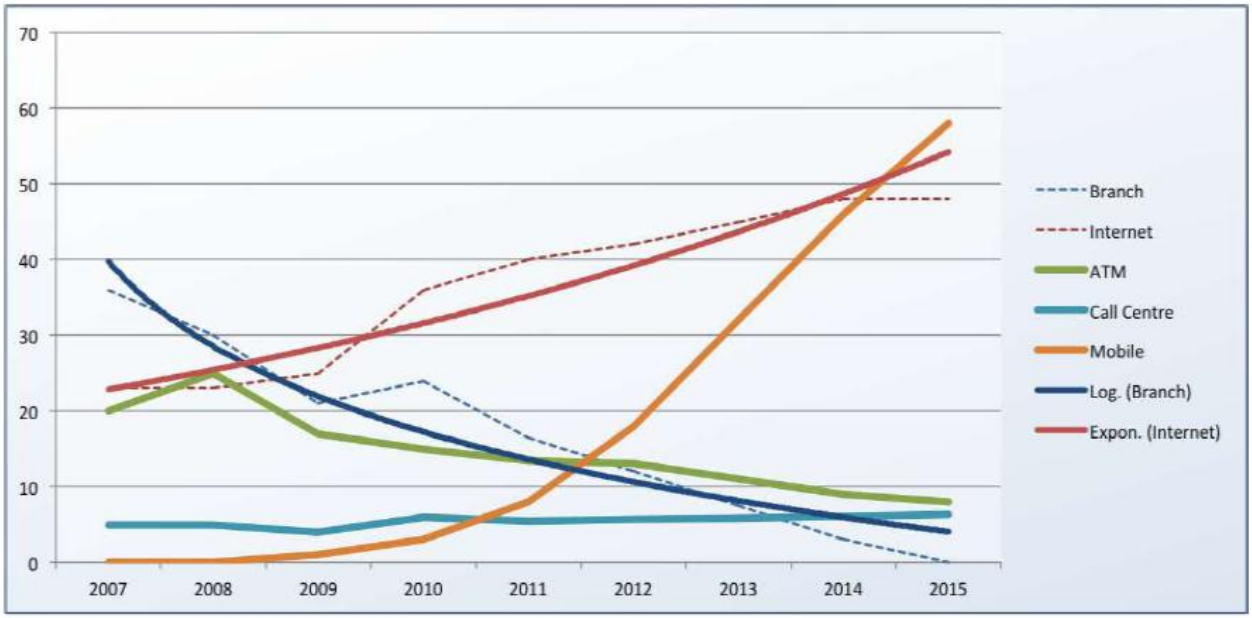
a três dentre as maiores instituições bancárias brasileiras; e disponibilizados gratuitamente na loja de aplicativos própria do sistema operacional móvel: "*Android Market*".

Por fim, o trabalho apresentará uma análise comparativa entre os dados obtidos e espera-se que futuros trabalhos façam uso da metodologia apresentada, a partir de um estudo aprofundado dos dados para apontar diferenças e propor soluções para uma comunicação mais segura no *mobile banking*, com base na em conceitos de segurança da informação.

1.2. JUSTIFICATIVAS

O aumento da demanda pelo "*Mobile Banking*" tem alertado bancos e fornecedores de tecnologia com interesse em, não somente oportunidades de negócios no desenvolvimento e oferta de serviços aos seus respectivos consumidores, mas também no receio do risco de serem ultrapassados neste segmento. A expansão da internet e tecnologias correlatas trouxeram novas oportunidades para os negócios, um novo tipo de serviço de comunicação, utilizando a internet em um dispositivo móvel, com novas oportunidades e trazendo diferentes conteúdos digitais e serviços (Tiwari, Buse, Herstatt, 2007).

Segundo pesquisas do Yankee Group, existirão 500 milhões de usuários de mobile banking até 2015 no mundo. De acordo com a Berg Insight, o número de usuários alcançará 894 milhões. Já a Global Industry Analysts (PRWeb, 2010) prevê 1,1 bilhões de usuários de *mobile banking* até 2015. No Brasil, o *mobile banking* tem crescido a taxas de 50 a 70% ao ano. Esse crescimento está diretamente relacionado ao aumento da utilização de *smartphones* e *tablets* no país. Hoje, mais de três milhões de correntistas já fazem uso deste meio para transações. Se o crescimento do "mobile banking" persistir neste ritmo, em cinco ou sete anos o m-banking terá a mesma relevância do internet banking, que também vem avançando de forma vertiginosa e responde, no Brasil, por mais de um terço de todas as transações eletrônicas ou automáticas do setor bancário (FEBRABAN, 2012). De acordo com a pesquisa anual Ciab Febraban, entre 2010 e 2011 o número de contas correntes com mobile banking cresceu 49%, passando de 2,2 milhões para 3,3 milhões. Em um panorama global segundo projeções do Nielsen Research e da ABA (American Bankers Association), conforme mostrado na Figura 1.1, existe uma tendência migratória relacionada ao crescimento de dispositivos móveis que impulsiona o crescimento exponencial do *mobile banking*, e por consequência o *Internet Banking* em detrimento de caixas eletrônicos e *call centers*.



Fonte: Banking 2020 Survey, 2011

Figura 1.1 – Projeção de crescimento do Mobile Banking

O aspecto mais importante quando se trata de *mobile banking* é a segurança e como torná-lo mais seguro, de forma que os consumidores se sintam mais confortáveis ao utilizar um dispositivo móvel. Levando em conta o rápido crescimento do serviço, do número de usuários e dos *smartphones*, além da capacidade dos bancos de oferecerem serviços móveis mais complexos, a segurança em dispositivos móveis se torna um aspecto fundamental para garantir o bom funcionamento do setor bancário. Com o objetivo de atrair mais consumidores é preciso também assegurar a qualidade e o nível de serviço oferecido, entretanto, é absolutamente necessário garantir que todos os tipos de transações sejam íntegras, disponíveis e confiáveis, principalmente quando se tratam de transações financeiras.

1.3. METODOLOGIA

Para a proposição do método descrito nesse trabalho, optou-se pela plataforma Android por apresentar uma grande popularidade perante os usuários de dispositivos móveis, além de possuir em sua loja virtual uma grande quantidade de aplicativos bancários devido a seu potencial crescimento nos próximos anos.

A partir da escolha do sistema operacional, prosseguiu-se para a escolha do dispositivo móvel que, na prática, poderia ser qualquer dispositivo do tipo smartphone ou similar para a metodologia proposta.

A captura de pacotes consiste na interceptação dos dados a partir de três aplicativos bancários distintos, pertencentes a três instituições financeiras, interceptados por uma rede sem fio conectada a rede mundial de computadores de forma indireta, que permitiu a alteração da rota dos dados através de interfaces de rede o que possibilitou a interceptação.

De forma geral, primeiramente configurou-se toda parte de hardware e *software,* usados no processo de captura e, em seguida, utilizou-se alguns *softwares* que permitiram uma seleção e análise dos dados obtidos.

1.4. ORGANIZAÇÃO DO TRABALHO

Ante o exposto este trabalho foi dividido em quatro capítulos. Neste capítulo foi realizada uma introdução ao tema desta pesquisa, onde foram definidos os objetivos, justificativas e a metodologia do trabalho. O capítulo 2 fornece uma base conceitual e um referencial teórico para que todos os aspectos do experimento tenham fundamentos científicos, desde tópicos de redes de comunicação a forense em dispositivos móveis e *mobile banking*.

O capítulo 3 apresenta a descrição de todas as ferramentas computacionais utilizadas, bem como expõe de forma clara, objetiva e diagramada o método proposto para a captura e análise dos dados bancários.

Finalmente, o capítulo 4 conclui, apresentando uma síntese dos dados obtidos a partir do método proposto, descrevendo sua relevância. Também são apresentadas expectativas para trabalhos futuros, dificuldades encontradas e também propõe formas de se dar continuidade ao trabalho desenvolvido.

2. CONCEITOS E REFERENCIAL TEÓRICO

Segundo o ETSI (European Telecommunications Standards Institute), interceptação é uma ação baseada na lei, realizada por um operador de rede, provedor de acesso ou provedor de serviço, com o intuito de tornar certa informação acessível e remetê-la a uma instituição legal. A interceptação de dados muitas vezes se torna inútil sem a utilização de ferramentas adequadas para a extração de informações relevantes. A análise da informação requer, além de um conhecimento sobre os dados obtidos, um embasamento conceitual para propor soluções, verificar possíveis falhas e fornecer um relatório adequado.

Os telefones celulares estão em um momento tecnológico de grande evolução, possuindo características diferentes a depender do fabricante, do modelo e do sistema operacional como: diferentes memórias para armazenamento do sistema e dos dados; diferentes tipos de hardware; diferentes formas de conexão (microUSB, miniUSB, bluetooth, infra vermelho e em padrões proprietários) e; diferentes sistemas operacionais, a exemplo de aparelhos com customizações do sistema operacional Linux (SIMÃO, 2011). Além dos telefones celulares, um novo dispositivo móvel vem ganhando cada vez mais espaço: o *tablet*, que não se enquadra nem no conceito de *smartphone*, nem no de computador. É um dispositivo em formato de prancheta *touch screen*, tela sensível ao toque, é um tipo de tela sensível à pressão, dispensando assim a necessidade de outro periférico de entrada de dados, como o teclado, ou o *mouse*, capaz de acessar a internet, reproduzir músicas, vídeos e ainda funcionar como leitor de revistas, livros, jornais, entre outros; e da mesma forma que os smartphones, possui características diferentes a depender do fabricante.

Nesse capítulo são apresentados conceitos relevantes para o método que será apresentado no capítulo 3, dessa forma, uma abordagem teórica sobre conceitos de interceptação de comunicação, forense em dispositivos móveis, telefones inteligentes e *mobile banking* fornecerão bases para um melhor entendimento da metodologia apresentada.

2.1. CONCEITOS DE INTERCEPTAÇÃO DE COMUNICAÇÃO

O IEEE 802 é o comitê pertencente ao IEEE (Institute of Electrical and ElectronicsEngineers) que desenvolveu padrões para, LANs (Local Area Networks). Em 1990, o comitê IEEE 802 formou um novo grupo de trabalho, conhecido como IEEE 802.11, com a finalidade de

desenvolver especificações de protocolo e transmissão para redes sem fio, as chamadas WLANs (Wirelles Local Area Networks). A partir desse momento, a procura por este tipo de rede que atua em diferentes freqüências e taxas de dados teve um grande crescimento, segundo o ABI research. Acompanhando essa demanda, o grupo de trabalho IEEE 802.11 elaborou uma lista cada vez maior de padrões.

O primeiro padrão 802.11 aceito pela indústria foi o padrão 802.11b. Embora os produtos que trabalhavam com o 802.11b fossem todos baseados no mesmo padrão, sempre houve uma preocupação com relação à interoperabilidade entre produtos de diferentes fornecedores. A fim de sanar essa preocupação, o *Wireless Ethernet Compatibility Alliance* (WECA), um consórcio da indústria, foi formado em 1999. Esta organização, posteriormente rebatizada de Wi-Fi (*Wireless Fidelity*) *Alliance*, criou um conjunto de testes para certificar a interoperabilidade dos produtos. O 802.11b, usado em produtos certificados é o 802.11b com certificação Wi-Fi, que foi também estendida para certificar os produtos 802.11g. A Aliança Wi-Fi desenvolveu também um processo de certificação para produtos 802.11a, chamado de Wi-Fi5. Atualmente, ela se preocupa com várias áreas de mercado das WLANs, incluindo empresas, usuários domésticos e outros eventuais nichos. Mais recentemente, a Aliança Wi-Fi veio a desenvolver procedimentos de certificação para os padrões de segurança IEEE 802.11, referidos como a Wi-Fi Protected Access (WPA), sendo que a versão mais recente do WPA, conhecido como WPA2, incorpora todas as características do IEEE 802.11i com especificações de segurança para redes sem fio.

Na comparação entre redes cabeadas e redes sem fio:

1. A fim de transmitir através de uma rede cabeada, uma estação deve estar fisicamente ligada à rede. Por outro lado, em uma rede sem fio, qualquer estação de rádio dentro do conjunto de dispositivos da rede pode transmitir.
2. Do mesmo modo, a fim de receber uma transmissão de uma estação que faz parte de uma rede com fio, a estação receptora também deve ser anexada à rede. Por outro lado, em uma rede sem fio, qualquer estação dentro da faixa de rádio pode receber.

Essas diferenças entre redes sem fio e cabeadas sugerem o aumento da necessidade de mecanismos e serviços de segurança robustos em redes sem fio. A especificação original 802.11 incluia um conjunto de funcionalidades de segurança para autenticação e privacidade que eram muito fracas. Para privacidade, o padrão 802.11 definiu o

algoritmo Wired Equivalent Privacy (WEP). Subsequente ao desenvolvimento do WEP, o grupo de trabalho 802.11i desenvolveu um conjunto de ferramentas para resolver os problemas de segurança em WLANs. A fim de acelerar a introdução de uma forte segurança para WLANs, a aliança Wi-Fi promulgou o Wi-Fi Protected Access (WPA) como um padrão Wi-Fi. O WPA Wi-Fi consiste em um conjunto de mecanismos de segurança que elimina a maioria das questões de segurança do 802.11, e é baseado no estado atual do padrão 802.11i. O formato final do padrão 802.11i é referido como Robust Security Network (RSN). A Aliança Wi-Fi, atualmente, certifica fornecedores em conformidade com a especificação 802.11i, desde que de acordo com as referências no âmbito do programa WPA2.

Em redes cabeadas locais, dependendo da estrutura de rede (concentrador ou comutador), é possível capturar o tráfego de toda a rede ou apenas de partes dela a partir de uma única máquina pertencente à rede. Para fins de monitoramento de rede, também pode ser desejável analizar todos os pacotes de dados em uma LAN (Local Area Network) usando um *switch,* dispositivo de rede que conecta segmentos ou dispositivos de rede processando e roteando dados, com uma porta de monitoramento chamado "*monitoring port"* (porta de monitoramento), cujo objetivo é espelhar todos os pacotes que passam por todas as portas do switch quando os sistemas (computadores) estão ligados a uma porta do *switch*. Ou utilizar um "networking tap", dispositivo de hardware capaz de prover meios para acessar o fluxo de dados através de uma rede de computadores, que consiste em uma solução ainda mais confiável do que usar uma porta de monitoramento, uma vez que essas "torneiras" são menos propensas a perder pacotes durante altas taxas de tráfego. Em redes sem fio, é possível capturar o tráfego em um canal particular ou em vários canais, utilizando múltiplos adaptadores.

Na transmissão por cabo e redes sem fio, para capturar o tráfego que não seja o tráfego *unicast* enviado para a máquina executando o *software sniffer (analisador de pacotes)*, ou seja, o tráfego *multicast* enviado a um grupo *multicast* ao qual a máquina esteja ouvindo, ou até mesmo o tráfego de *broadcast*, o adaptador de rede usado para capturar o tráfego deve ser colocado em modo promíscuo; alguns *sniffers* suportam esse modo, outros não. Em redes sem fio, mesmo que o adaptador esteja no modo promíscuo, os pacotes não relacionados ao conjunto de serviços para os quais o adaptador está configurado, por padrão será ignorado. Para visualizar tais pacotes, o adaptador deve estar em modo de monitoramento.

Assim, a informação capturada é decodificada do formato digital para um formato legível, que permite aos usuários do analisador de protocolo visualizar de forma mais amigável as informações obtidas. Analisadores de protocolos variam em suas habilidades para exibir dados em múltiplas visões, detectar erros automaticamente, determinar as causas dos erros, gerar diagramas de tempo, reconstruir fluxo de dados UDP (User Datagram Protocol) ou TCP (Transmission Control Protocol).

Os analisadores de protocolo podem também ser baseados em hardware, o que é cada vez mais comum, sendo combinados com parte do disco do computador. Esses dispositivos gravam pacotes (ou partes de pacotes) em um local do disco. Isto permite a análise forense do histórico de pacotes sem que os usuários causem qualquer interferência.

Naturalmente, outros conceitos relacionados à interceptação de pacotes são os ataques a redes sem fio. Dentre os ataques mais conhecidos podem-se citar dois que abrangem diretamente a interceptação da comunicação: Man-in-the-middle e Browser-in-the-middle.

Ataques Man-in-the-Middle (MITM) são frequentemente referidos como ataques de seqüestro de sessão, sugerindo que o intruso tem como objetivo obter acesso a uma sessão de usuário legítimo e adulterá-la. O ataque geralmente começa com visualizações e escutas em uma conexão de rede, e termina com a tentativa de alterar, fraudar ou redirecionar os dados interceptados. Os ataques Man-in-the-middle são geralmente selecionados por atacantes contra sistemas criptográficos de chave pública. Em um cenário de chave pública, os atacantes podem substituir a chave pública interceptada por suas chaves públicas falsas. Muitas vezes, nesses casos, a vítima é levada a acreditar que elas permanecem seguras na comunicação com outros.

Um cenário comum de ataque MITM pode envolver o atacante ter interceptado a comunicação entre um cliente e um servidor. Em tais cenários, o atacante muitas vezes transmite mensagens enganosas entre o cliente e o servidor para que eles se sintam seguros em se comunicar uns com os outros. Tecnicamente, o invasor pode usar um programa que aparece como um servidor para o cliente e vice-versa. A Figura 2.1 ilustra esse cenário.

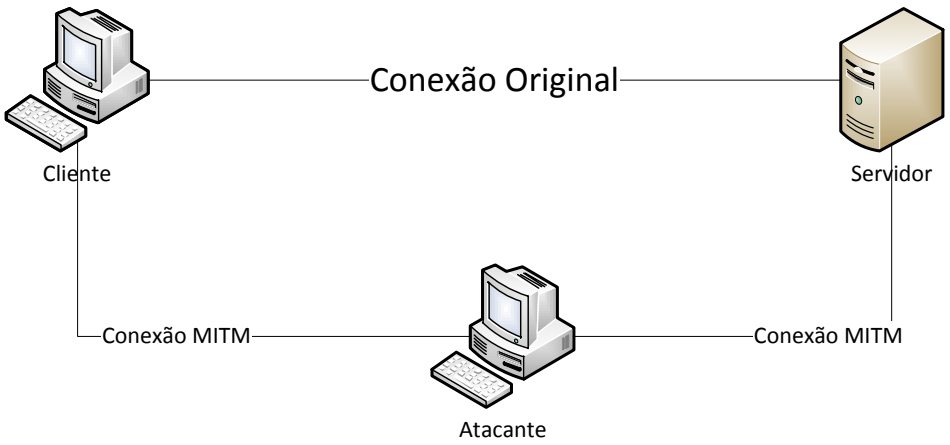


Figura 1.1 – Cenário comum de "man-in-the-middle"

Em ataques MITM, o atacante tenta conseguir um entre dois pontos de rede de destino, e utiliza servidores *proxy,* servidor intermediário que atende a requisições repassando os dados do cliente à frente: um usuário (cliente) conecta-se a um servidor *proxy*, requisitando algum serviço, como um arquivo, conexão, página *web*, ou outro recurso disponível no outro servidor para mascarar toda a comunicação entre eles. Uma vez que o atacante obtenha sucesso, novos ataques podem ser lançados incluindo espionar os pacotes que trafegam e seqüestrar de sessões já autenticadas, injetar pacotes ou comandos no servidor ou enviar respostas forjadas para o cliente.

Ataques MITM visam principalmente informações confidenciais e valiosas. São frequentemente escolhidos para interceptar comunicações HTTP e HTTPS. O Hypertext Transfer Protocol Secure (HTTPS) é um protocolo de comunicação amplamente utilizado para comunicação segura através de uma rede de computadores, especialmente na Internet. Tecnicamente, não é um protocolo por si só, mas sim, o resultado de simplesmente utilizar o Hypertext Transfer Protocol (HTTP) em cima do protocolo SSL/ TLS, aumentando assim os recursos de segurança SSL/TLS (Security Sockets Layer/Transport Layer Security) para o protocolo HTTP.

O ataque Browser-in-the-midde funciona semelhante a uma tentativa de *phishing*, fraude eletrônica, caracterizada por tentativas de adquirir dados pessoais de diversos tipos; senhas, dados financeiros como número de cartões de crédito e outros dados pessoais. O ato consiste em um fraudador se fazer passar por uma pessoa ou empresa confiável enviando uma comunicação eletrônica oficial. Isto ocorre de várias maneiras, principalmente por e-mail, mensagem instantânea, SMS, dentre outros, onde o navegador é infectado por um código malicioso a partir de vulnerabilidades na segurança do navegador visando modificar páginas

da web, modificar o conteúdo de transações ou inserir transações adicionais, tudo sob uma forma completamente encoberta, ou seja, invisível para o usuário, levando o usuário a fornecer informações pessoais, que são colhidas pelo código malicioso e enviadas ao atacante. O código malicioso também pode realizar uma transação sem o conhecimento do usuário, roubando dinheiro de contas bancárias enquanto encobre seus rastros.

Ataques desse tipo são muitas vezes gerados por um pequeno pedaço de código malicioso baixado, muitas vezes, sem intenção. Uma vez que nem todos os programas antivírus detectam esse código. Isso permite que o código de *malware* resida no *cache* do navegador ou em outro lugar do disco rígido, esperando uma oportunidade para ser ativado e detectar, por exemplo, um acesso ao provedor de serviços bancários on-line. Um ataque browser-in-the-middle será bem sucedido, independentemente de mecanismos de segurança como SSL (Secure Sockets Layer).

De acordo com a pesquisa "2010 Online Banking Survey", patrocinada pela PHONEFACTOR, empresa líder em soluções de autenticação para telefones, a maioria dos profissionais de serviços financeiros considera esse tipo de ataque como a maior ameaça ao *internet banking*.

2.2. FORENSE EM DISPOSITIVOS MÓVEIS

Forense em telefones móveis é a ciência responsável por recuperar provas digitais ou evidências, a partir de um telefone móvel sob condições forenses, usando métodos aceitos. Os telefones móveis, especialmente aqueles com recursos avançados, são um fenômeno relativamente recente, geralmente não cobertos em computação forense clássica (Jansen e Ayers, 2007).

O modelo que utiliza ferramentas de software forense para telefones celulares é consideravelmente diferente do modelo dos computadores pessoais. Embora os computadores pessoais sejam concebidos com sistemas de propósito gerais, os telefones celulares são projetados com propósitos especificos, ou seja, são aparelhos que executam um conjunto de tarefas predefinidas. Os fabricantes de telefones celulares também tendem a confiar em diversos sistemas operacionais proprietários, em vez de uma abordagem mais padronizada como aquela encontrada nos computadores pessoais. Devido a esse fato, a variedade de conjuntos de ferramentas para dispositivos móveis é diversificada e a vasta gama de

dispositivos sobre os quais elas operam, normalmente é reduzida para plataformas distintas, para uma linha de produto do fabricante, uma família de sistema operacional ou um tipo de arquitetura de hardware. Os telefones celulares possuem ciclos de lançamento de produtos mais curtos, obrigando os fabricantes dessas ferramentas a atualizá-las continuamente para manter a cobertura atualizada. A tarefa é enorme, e o suporte dos fabricantes das ferramentas com os modelos mais novos, muitas vezes fica significativamente obsoleto.

É possível adquirir dados utilizando ferramentas forenses a partir de um dispositivo de duas maneiras: aquisição física ou aquisição lógica. A aquisição física implica uma cópia bit-a-bit de toda uma parte física (por exemplo, um chip de memória), enquanto que a aquisição lógica implica uma cópia bit-a-bit de objetos lógicos de armazenamento (por exemplo, diretórios e arquivos) que residem em um espaço lógico (por exemplo, uma partição de um sistema de arquivos). A diferença reside na distinção da memória, ora vista como um processo através das instalações do sistema operacional (isto é, de um ponto de vista lógico), ora vista em sua forma bruta pelo processador e outros componentes de hardware relacionados (isto é, de um ponto de vista físico).

A aquisição física tem vantagens em relação à aquisição lógica, uma vez que permite que os arquivos apagados e os remanescentes de dados presentes (por exemplo, na memória ou no espaço não alocado do sistema de arquivos) sejam examinados, que de outra forma seriam perdidos. Imagens físicas extraídas do dispositivo precisam ser analisadas, decodificadas, e traduzidas para descobrir a presença de dados. O trabalho é tedioso e pode ser demorado para se executar manualmente. Imagens dos dados de dispositivos físicos podem ser importadas para uma ferramenta de modo a automatizar o exame e a elaboração de relatórios, no entanto, existem apenas algumas ferramentas espeficicas para a obtenção de imagens de telefones celulares disponíveis atualmente. Uma aquisição lógica, embora mais limitada do que uma aquisição física, tem a vantagem de que as estruturas de dados do sistema são normalmente mais fáceis de extrair com uma ferramenta forense e fornecem uma organização mais natural, facilitando a compreensão e o uso durante a perícia. Se possível, é preferível realizar os dois tipos de aquisição - uma aquisição física antes de uma aquisição lógica.

O analista forense de modo a documentar, resguardar e processar os dados (evidências) de forma mais segura e menos intrusiva possível, deve seguir uma série de passos dependendo do estado do dispositivo.

Inicialmente devem ser preservados os dados do smartphone. Ao receber o smartphone, o analista pericial deve seguir os procedimentos a fim de preservar os dados armazenados no equipamento apreendido. Assim, deve verificar se o telefone encontra-se ligado ou não. Com o telefone desligado, deve-se avaliar a possibilidade de extrair os dados do cartão de memória. No caso em que é possível retirar o cartão de memória, basta removê-lo e duplicar integralmente os dados para um cartão de memória do analista pericial, a fim de garantir sua preservação. Para copiar os dados do cartão de memória, pode-se utilizar a mesma abordagem utilizada em pendrives. Devem-se utilizar ferramentas forenses para a cópia ou até mesmo executar um *disk dump*, operação que consiste em recuperar a imagem do conteúdo do disco byte a byte e gerar o hash dos dados duplicados. Ao término do processo, o cartão de memória com a cópia deve ser reinserido no aparelho. A próxima etapa é isolar o telefone das redes de telefonia e de dados. A situação ideal é utilizar uma sala com isolamento físico de sinais eletromagnéticos. Entretanto, quando não se dispõe de tal infraestrutura, o analista deve colocar o smartphone em modo de vôo, avião ou offline. A partir do momento em que o aparelho está ligado, deve-se imediatamente configurá-lo para esses modos sem conexão, evitando assim a transmissão de dados ou recebimento de chamadas ou mensagens SMS (Short Message Service) após o momento da apreensão do equipamento. Se, porventura, até o momento de isolá-lo da rede, o telefone receber uma chamada, mensagem, e-mail ou qualquer outra informação, o analista deverá documentar e relatar o ocorrido em seu relatório final, que será redigido após o processo de exames e análise dos dados extraídos. Com o smartphone isolado das redes de telecomunicação, o analista pericial verificará se o dispositivo foi configurado para prover algum mecanismo de autenticação, seja uma senha ou um padrao táctil (Simão, 2011). A partir desse ponto, prossegue-se para verificação de controle de acesso, caso não tenha, essa se caracteriza como uma situação menos complexa na qual um examinador pode se deparar e àquela em que o celular não possui bloqueio e está prontamente apto a ter seus dados extraídos. Caso tenha, seja por padrão táctil ou senha, ainda assim e possível ao analista aplicar técnicas para obter acesso ao dispositivo. Tais técnicas são descritas pelo NIST (National Institute of Standards and Technology) como método investigativo ou entrevista com o proprietário, acesso por hardware ou método de acesso por software. Por fim, Recomenda-se que em todas as técnicas e procedimentos utilizados o analista documente o processo, a fim de subsidiar a etapa de exame e análise dos dados extraídos.

2.3. TELEFONES INTELIGENTES

Em 1993, a *BellSouth* lançou o IBM Simon, com sua tela sensível ao toque rudimentar, mas a era do telefone inteligente na América só começou realmente em 2002, quando os PDAs existentes na época eram capazes de fazer chamadas telefônicas. Naquele ano, a empresa RIM lançou o primeiro modelo *BlackBerry*. Com recursos de telefone, a *Handspring* lançou o Palm-OS-powered linha Treo, a *Microsoft* lançou seu Pocket PC Phone Edition e assim a tecnologia de dados móveis como GPRS (General Packet Radio System) tornou-se cada vez mais difundida.

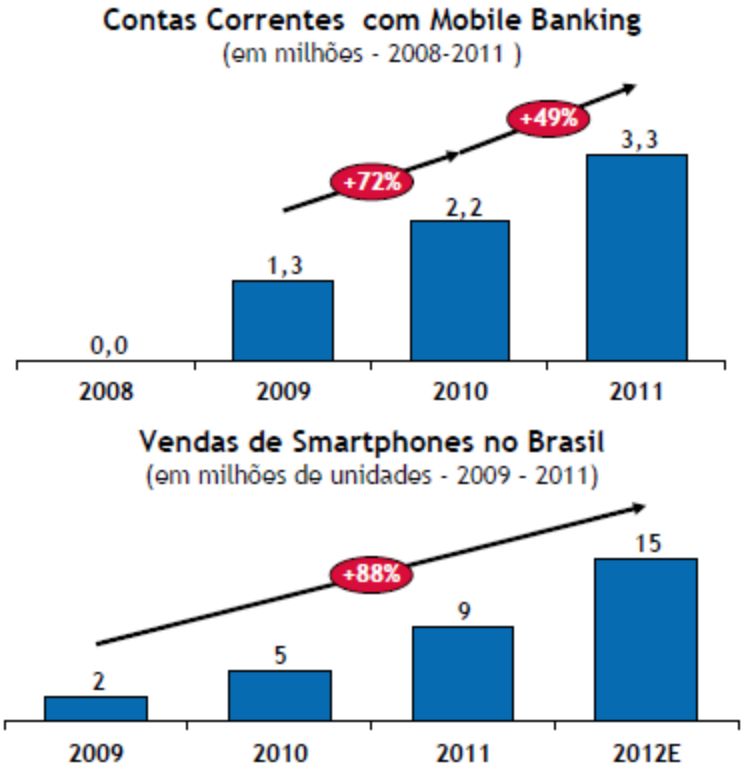
Quatro anos e meio depois, no final de 2006, um trimestre antes de a Apple anunciar o Iphone, agora icônico, apenas 715.000 *smartphones* haviam sido vendidos até o momento, o que representava apenas seis por cento do volume de vendas de telefonia móvel norte-americano. Até aquele ponto, o telefone inteligente não se espalhava muito mais rápido do que os computadores pessoais anos antes, e mais lentamente do que o rádio nas décadas anteriores.

Isso mudou quando o iphone da Apple vendeu 1,12 milhões de unidades em seu primeiro trimestre disponível, apesar dos valores relativamente altos. Ano após ano, a cota de mercado de telefones inteligentes quase dobrou. Foi de seis para onze por cento do volume de vendas de telefonia móvel norte-americana. O Nielsen (Líder global em pesquisa de mercado, informações e ferramentas de análise) relata que os telefones inteligentes representam mais de dois terços de todos os telefones móveis norte-americanos. O Nielsen também relata que 50 por cento de todos os americanos possuem telefone celular, os usuários, que equivalem a cerca de 40 por cento da população dos Estados Unidos, agora usam telefones inteligentes.

Estes números mostram que os telefones inteligentes, depois de um início relativamente rápido, também ultrapassaram quase qualquer tecnologia comparável para uso geral. O telefone fixo demorou cerca de quarenta e cinco anos para ir de cinco por cento a cinquenta por cento de penetração entre as famílias norte-americanas, já os telefones móveis levaram aproximadamente sete anos para atingir uma proporção semelhante entre os consumidores. Os *Smartphones* passaram de cinco por cento a quarenta por cento em cerca de quatro anos, apesar da recessão (Technology Review – MIT, 2012).

No Brasil, as vendas de *smartphones* devem crescer 73% em 2012, após o patamar recorde de 8,9 milhões de unidades comercializadas em 2011. Segundo projeções da consultoria IDC (CIAB FEBRABAN, 2012), especializada no mercado de tecnologia e telecomunicações, serão vendidos no Brasil perto de 15,4 milhões de unidades de smartphones em 2012.

Atualmente, existem aparelhos com preços mais acessíveis, oferta de pacotes de dados até para celulares pré-pagos e uma demanda muito grande ligada às redes sociais e à mobilidade. Isso impulsiona as vendas e a migração de celulares convencionais para os modelos smartphones. Conforme apresentado na Figura 2.2, é possível ver o crescimento do Mobile Banking diretamente relacionado ao crescimento das vendas de *smartphones*. Os números puxaram o Brasil da 16ª para a 10ª posição entre os maiores mercados de *smartphones* do mundo.



Fonte: FEBRABAN

Figura 2.2 – Vendas de Smartphones e Contas correntes em Mobile Banking

Os *smartphones* são a combinação de duas classes de dispositivos: os celulares e os assistentes pessoais (como os Palmtops e os PDAs). Diferente dos antecessores, os *smartphones* podem se conectar a web através de conexões de dados através de tecnologias como 3G, 4G ou Wi-Fi, o que permite que eles ofereçam uma enorme variedade de recursos.

Hoje em dia, mesmo aparelhos relativamente simples e baratos são capazes de navegar na web, rodar clientes de e-mail e permitir mensagens instantâneas, fazer chamadas VoIP (Voice Over IP) via SIP (Session Initiation Protocol), que consiste em um protocolo de sinalização definido pelo IETF largamente usado para controlar sessões de comunicação como chamadas de voz e vídeo sobre o protocolo IP ou Skype, servir como tocados de música, tirar fotos, exibir e gravar vídeos e servir como navegador GPS (Global Positioning System), além da possibilidade de servir como modem 3G para os notebooks, PCs e outros dispositivos.

O grande trunfo, entretanto, está na possibilidade de instalar aplicativos adicionais, o que permite que eles executem inúmeras outras funções. Usando um smartphone, é possível concentrar um volume surpreendente de funções em um aparelho de poucos gramas, que se pode carregar no bolso, com acesso contínuo à web. Essa combinação de fatores tem feito com que eles se tornem cada vez mais indispensável na atualidade.

2.4. MOBILE BANKING

No setor financeiro, os serviços de comércio móvel (*Mobile Commerce Services*) são geralmente conhecidos como Serviços Financeiros Móveis (*Mobile Finance Services* - MFS). Eles compreendem duas aplicações: O "*Mobile Payment*" e o "*Mobile Banking*". Este último, também conhecido como m-banking, mbanking ou SMS Banking é um termo usado para executar verificações de saldo, transações de contas, pagamentos, etc. através de um dispositivo móvel, como um telefone celular (Tiwari e Buse, 2007). O *mobile banking* é o serviço bancário que possibilita aos clientes realizarem pelo celular quase todas as operações disponíveis em caixas de autoatendimento e *internet banking.* Correntistas podem consultar extratos e saldos, fazer transferências entre contas do banco, pagamentos de títulos e convênios, DOC/TED, recarga de celular pré-pago e empréstimos. A principal diferença entre *internet banking* e *mobile banking* é que na internet tem-se um modelo centrado no computador - ou seja, o usuário vai onde o computador está e ainda depende do acesso à rede. No caso do telefone celular, é o serviço que está onde quer que o usuário vá - ou seja, é um modelo centrado no usuário.

2.4.1. Modelo conceitual de *mobile banking*

Segundo Tiwari e Buse, em um modelo acadêmico, o mobile banking é definido como:

"*Mobile Banking* refere-se ao beneficio e disposinibilidade dos serviços bancários e financeiros com a ajuda de aparelhos de telecomunicações móveis. O escopo dos serviços

oferecidos pode incluir a realização de transações bancárias e do mercado de ações, administração de contas e acesso a informações personalizadas".

De acordo com este modelo bancário móvel, três conceitos interrelacionados podem ser descritos:

- Contas móveis;
- Corretagem móvel;
- Serviços de informações financeiras móveis.

A maioria dos serviços, nas categorias de contas e corretagem, é baseada em transações. Os serviços não baseados em transações, de natureza informativa, no entanto, são essenciais para a realização de transações, por exemplo, a consulta de saldos pode ser necessária antes da autorização uma transferência de fundos. Os serviços de contas e de corretagem são, portanto, invariavelmente oferecidos em combinação com serviços de informação. Serviços de informação, por outro lado, podem ser oferecidos como um módulo independente.

O *Mobile Banking* tem crescido entre vários setores da sociedade nos últimos anos. Essa condição se deve aos seguintes fatores:

1) A altíssima penetração de dispositivos móveis;

2) A integração das economias mundiais está sendo direcionada a uma maior mobilidade, fazendo com que os serviços móveis deixem de ser um luxo, mas sim uma necessidade;

3) As novas gerações são fascinadas pela modernidade e serviços de telecomunicações;

4) Os dispositivos móveis têm se tornado mais poderosos e a transmissão de dados tem se tornado mais rápida com os novos padrões de telecomunicações.

Esse crescimento tem se mostrado cada vez mais acentuado e juntamente com novas tecnologias como o NFC (Near Field Communication), que permite transações simplificadas,

troca de dados e conexões sem fio entre dois dispositivos, próximos um ao outro, geralmente por não mais do que alguns centímetros, remete a novos conceitos de pagamento como o *mobile payment*, que está diretamente relacionado ao *mobile banking.* Dessa forma, é coerente afirmar que para as próximas décadas espera-se elevados investimentos no setor bancário visando especificamente o setor de mobilidade.

Segundo (FEBRABAN, 2011), houve uma expansão do mobile banking, impulsionado pela venda de *smartphones* no País. Em 2011 foram 3,3 milhões de contas correntes acessadas por meio de mobile banking, o que representa um salto de 49% em comparação com o ano anterior, esse crescimento está diretamente relacionado ao crescimento das vendas de smartphones. Um dos motivos para a alta, de acordo com a entidade, é o acesso à banda larga móvel, associado ao investimento em segurança. Esse cenário mostra que os bancos estão se preparando para os desafios do futuro, que incluem a aceleração do uso do *mobile banking* e do *mobile payment*. As projeções da pesquisa Ciab Febraban 2012 apontam que, em um prazo de 5 a 7 anos mobile banking terá a mesma relevância do internet banking.

3. DESENVOLVIMENTO

O procedimento experimental e coleta de dados foram realizados no período que compreende os meses de setembro a novembro de 2011 no laboratório de segurança da informação pertencente ao departamento de Engenharia Elétrica da Universidade de Brasília.

Os dados coletados são conjuntos de *bytes* relacionados à comunicação, via rede mundial de computadores exclusivamente através de uma rede sem fio, entre usuário e instituição financeira, por meio do uso de aplicativos bancários instalados em um dispositivo móvel do tipo *smartphone*. O trabalho apresenta três diferentes conjuntos de dados, cada um é relacionado a uma instituição bancária Brasileira distinta, que compõe o conjunto das maiores instituições do setor.

3.1. DESCRIÇÃO DO TRABALHO

Como pré-requisito para a realização do experimento, fez-se uso de alguns equipamentos e ferramentas computacionais.

3.1.1 *Hardware*

1. Dispositivo móvel da marca Samsung, modelo Galaxy S I9000b;
2. Roteador com tecnologia “wireless” da marca Cisco Linksys, modelo WRT54g;
3. Roteador com tecnologia “wireless” da marca Cisco Linksys, modelo WAG54gp2;
4. Computador do tipo “desktop” da marca Semp Toshiba;
5. Dispositivo com interface de rede com entrada USB.

O dispositivo móvel utilizado no experimento foi escolhido por rodar o sistema operacional Android, que foi selecionado como padrão para o experimento, além disso, apresenta como vantagem a conexão Wi-Fi, necessária para o acesso à internet. Ambos os roteadores possuem conexões *wireless*, contudo apenas o roteador que funciona como ponto de acesso para o dispositivo móvel deve necessariamente apresentar esse tipo de conexão. O dispositivo com interface de rede com entrada USB é necessário porque o computador utilizado apresenta

apenas uma interface de rede, sendo assim para adicionar outra, optou-se por uma interface externa, devido à facilidade de uso e mobilidade.

3.1.2 *Software*

Escolheu-se como sistema operacional para o computador utilizado no experimento, o *Backtrack 5*, por ser uma distribuição Linux voltada para testes de penetração, segurança de redes e monitoramento. Dessa forma, o sistema operacional já contém naturalmente a maioria dos softwares utilizados para efetuar a interceptação e manipular os dados, com exceção do *Netwitness Investigator*, que foi escolhido por se tratar de uma poderosa ferramenta forense para análise e monitoramento de redes. Foram utilizados os *softwares*:

1. Sistema operacional móvel *Android 2.1*, codinome "*Eclair*" com compatibilidade com o dispositivo móvel *Samsung Galaxy S I9000b*;
2. Sistema operacional BackTrack (http://www.backtrack-linux.org/);
3. Programa Iptables (http://www.netfilter.org/);
4. Programa *Tcpdump* (http://www.tcpdump.org/);
5. Programa Wireshark (http://www.wireshark.org/);
6. Programa Netwitness Investigator 9.6;

3.1.3 Descrição dos *Softwares*

I. A plataforma *Android* é um sistema operacional móvel que roda sobre o núcleo "Linux". Foi inicialmente desenvolvido pelo *Google* e posteriormente pela *Open Handset Alliance*. Atualmente é a plataforma móvel mais popular, contando com mais de 600.000 aplicativos e jogos.

II. O "*BackTrack*" é uma plataforma avançada de testes de penetração e auditoria de segurança com ferramentas complexas para identificar, detectar e explorar qualquer vulnerabilidade aparente no ambiente da rede alvo. Aplicando-se uma metodologia de testes apropriada com objetivos de negócios definidos e um plano de testes agendado resultará em um teste de penetração robusto em qualquer rede.

Sua versão atual é a versão (5.0). A evolução do "*BackTrack*" se deve a muitos anos de desenvolvimento, testes de penetração e um auxílio sem precedentes da comunidade de segurança da informação. O "*BackTrack*" originalmente começou com versões de distribuições Linux chamadas "*Whoopix*", IWHAX e *Auditor*. Quando foi desenvolvido, o "*BackTrack*" foi desenhado para ser um "*live cd – all in one*" utilizado em auditorias de segurança e foi especificamente construído para não deixar qualquer vestígio em um computador. Ele tem se expandido por ser o mais amplamente adotado "*framework*" de teste de penetrações existente e é utilizado pela comunidade de segurança da informação em todo o mundo.

III. O "*Iptables*" é o nome da ferramenta do espaço do usuário que permite a criação de regras de *firewall* e NAT (*Network Address Translation*). Apesar de, tecnicamente, o "*Iptables*" ser apenas uma ferramenta que controla o módulo "*Netfilter*", o nome "*Iptables*" é frequentemente utilizado como referência ao conjunto completo de funcionalidades do "*Netfilter*". O "*Iptables*" é parte de todas as distribuições modernas do "*Linux*". O "*Netfilter*" citado anteriormente é um módulo que fornece ao sistema operacional "*Linux*" as funções de *firewall*, NAT e *log* dos dados que trafegam por rede de computadores.

IV. O "*Tcpdump*" é uma ferramenta que permite mostrar uma descrição do conteúdo de pacotes em uma interface de rede que combine com a expressão booleana configurada em linha de comando. Ele pode ser rodado com o comando "-w", que permite salvar o pacote de dados em um arquivo para uma futura análise, e/ou com o comando "–r", que permite o programa ler um pacote de dados já salvo ao invés de ler pacotes provenientes da interface de rede. Em todos os casos, apenas pacotes que estão de acordo com a expressão podem ser processados pelo "*Tcpdump*".

V. O "*Wireshark*" (anteriormente conhecido como *"Ethereal"*) é um programa que analisa o tráfego de rede, e o organiza por protocolos. As funcionalidades do "*Wireshark*" são parecidas com as do "*Tcpdump*", mas apresenta uma interface GUI (*Graphical User Interface*), com mais informação e com a possibilidade da utilização de filtros.

VI. O "*NetWitness Investigator*" é uma plataforma de monitoração de rede que fornece uma compreensão precisa de tudo o que acontece na rede. Soluções "*NetWitness*" são implantadas em ambientes de clientes para resolver uma ampla gama de problemas de segurança da informação, incluindo: ameaças internas,

malwares, ameaças avançadas persistentes, fraudes, espionagens, vazamento de dados, além de monitoramento contínuo de controles de segurança.

3.1.4 Topologia utilizada no experimento

Na metodologia proposta não foi prevista a captura de pacotes em dispositivos móveis de modo direto, isto é, não é possível utilizar softwares de captura interceptando diretamente a comunicação do dispositivo móvel com os aplicativos bancários via internet. Dessa forma, como proposta, desviou-se o tráfego por um computador de forma que o tráfego entre as partes comunicantes fosse capturado através de ferramentas instaladas no computador. A Figura 3.1 mostra a topologia do projeto a ser executado no método proposto.

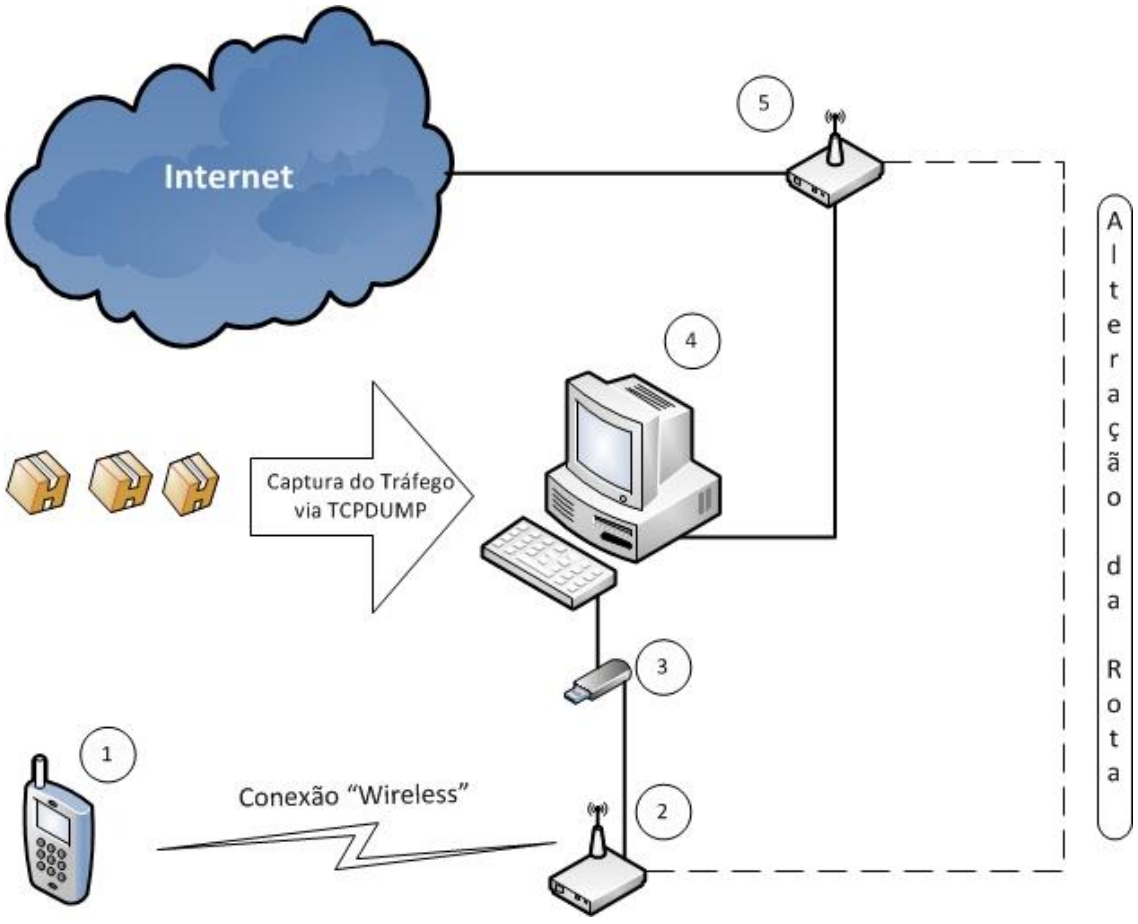


Figura 2.1 - Topologia do experimento

3.2. PROCEDIMENTO EXPERIMENTAL

A metodologia apresentada pode ser divida em quatro diferentes fases como apresentado na Figura 3.2. A fase de configuração, a fase de captura, a fase de seleção dos dados e por fim a fase de análise. A fase de configuração consiste na montagem e configuração de hardwares e softwares a fim de fornecer bases para a interceptação dos dados. A fase de captura implica efetivamente na interceptação dos dados, capturando todos os pacotes que trafegam na rede durante a realização de determinada transação. A terceira fase corresponde à fase de seleção dos dados, na qual todas as informações não relacionadas à transação efetiva são descartadas. Por fim, tem-se a fase de análise, na qual os dados previamente selecionados serão carregados em um software para extração de informações relevantes.

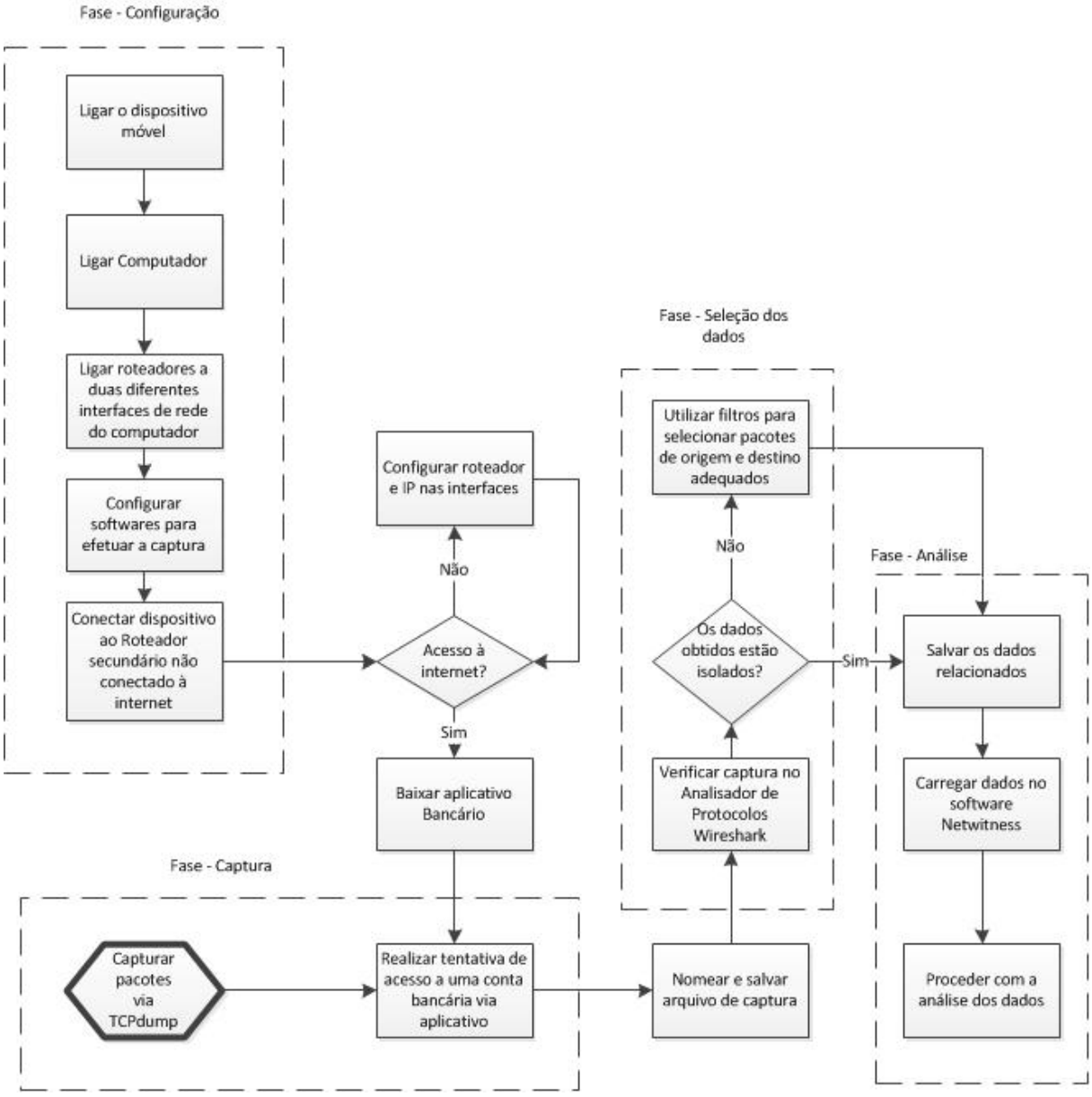


Figura 3.2 - Fluxograma do método

3.2.1. Configuração

O roteador WAG54gp2 (Figura 3.3), indicado por 5 na topologia da Figura 3.1, foi conectado à entrada RJ-45 da placa de rede do computador, a seguir, conectou-se o roteador WRT54g (Figura 3.4), indicado por 2 na topologia, à entrada do conector RJ-45 pertencente ao dispositivo de rede USB, indicado por 3 na topologia. O primeiro fez a conexão com a rede externa enquanto o segundo fez a conexão com o dispositivo móvel via rede Wi-Fi 802.11.

Fonte: Cisco Systems

Figura 3.3 - Roteador WRT54g

Fonte: Cisco Systems

Figura 3.4 – Roteador WAG54gp2

Após a ligação de todos os aparelhos iniciou-se o computador, indicado por 3 na Figura 3.1, com sistema operacional "Backtrack" no modo de interface gráfica. Posteriormente, abriu-se o terminal e digitou-se o comando "*ifconfig*" de modo a permitir o reconhecimento e visualização dos parâmetros TCP/IP em uma rede UNIX. Assim, o sistema operacional reconheceu imediatamente as duas interfaces: ETH0 e ETH1 referentes às interfaces de rede conectadas ao computador.

O próximo passo foi ligar o dispositivo móvel, indicado por 1 na Figura 3.1, conectando-o a rede sem fio fornecida pelo roteador 2. Contudo, foi necessário configurar um IP estático para cada uma das interfaces para, posteriormente, alterar a rota. Através do comando "*ifconfig*", pôde-se realizar essa configuração que é apresentada no Quadro 3.1.

Quadro 3.1: Configurando um IP estático

```
1) ifconfig eth0 192.168.15.112
2) ifconfig eth1 192.168.16.1
3) route add default gateway 192.168.15.1 eth0
```

Além de configurar um IP para as interfaces, foi necessário, na página de configuração do roteador WRT54g, configurar o acesso para um endereço de IP estático. Dessa forma, através do endereço 192.168.1.1, acessou-se a página de configuração do roteador, o que permitiu alterar os parâmetros de rede, adequando-os ao experimento. Colocou-se como IP do ponto de acesso o endereço 192.168.16.2, assim os dispositivos que não pertencem à rede wireless enxergariam o ponto de acesso fazendo parte da rede 192.168.16.0; e os aparelhos que fazem parte da rede wireless enxergariam o ponto de acesso com endereço 192.168.1.1, funcionando como NAT (Network Address Translation) do ponto de acesso, ou seja, reescreveu-se o endereço IP para que os pacotes que passam pela rede interna tenham acesso à rede externa, rede mundial de computadores. A Figura 3.4 mostra a configuração para o IP estático no roteador.

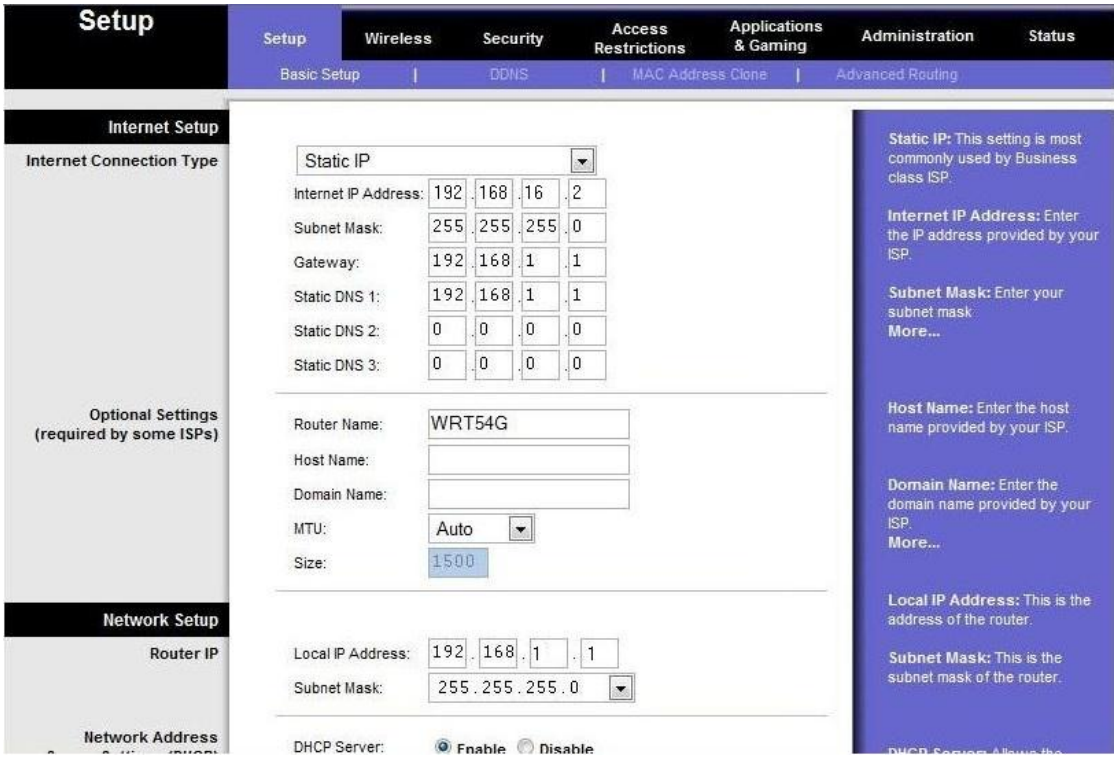


Figura 3.4 - Configuração de Roteador

Para solucionar o direcionamento do tráfego da interface ETH0 para ETH1 alcançando o dispositivo móvel, foram utilizadas regras de tráfego no software "*Iptables*", a fim de viabilizar a comunicação nos dois sentidos. Assim, através de linha de comando no terminal do "*BackTrack*" foram estabelecidas as seguintes regras mostradas no quadro 3.2.

Quadro 3.2 – Regras de tráfego no Iptables

```
1)iptables -t nat -A POSTROUTING -o eth1 -s 192.168.16.2 -j SNAT --to 192.168.15.112
2)iptables -t nat -A PREROUTING -i eth1 -d 192.168.15.112 -j DNAT --to 192.168.16.2
```

Onde:

Tabela 3.1 - Lista de comandos do Iptables

Comandos/Opções	Significado
-t	"table" | -t | Tabela para manipular (padrão: "filtrar")
-A	"append" | -A | Anexar à cadeia
-o	"out-interface" | -o | Nome da saída
-i	"in-interface" | -i | Nome da entrada
-s	"source" | -s | Endereço [/máscara]. Especificação da Fonte
-d	"destination" | -d | Endereço [/máscara] Especificação do Destino
-j	"jump" | -j | Alvo para a regra

Além disso, para ativar o roteamento adicionou-se o comando "*ip_forward*" nos scripts de inicialização, como descrito no quadro 3.3.

Quadro 3.3 - Ativando o roteamento

```
1) echo 1 > /proc/sys/net/ipv4/ip_forward
```

Finalmente, como ultimo passo para redirecionar o tráfego reiniciou-se o serviço de rede do *Linux* com o comando descrito no quadro 3.4.

Quadro 3.4 - Reinicio do serviço de rede Linux

```
1) /etc/initd/networking restart
```

3.2.2. Captura

Definido o objeto de captura como: "Captura de um pacote referente à tentativa de acesso a conta em um aplicativo bancário móvel, utilizando conta e senha (fictícios) de tamanho dos campos pré-estabelecidos por cada um dos três bancos em seus respectivos aplicativos". A captura dos pacotes foi realizada de modo que o momento inicial correspondesse ao momento de entrada no aplicativo pelo usuário do dispositivo móvel; e o momento final correspondesse ao momento no qual o aplicativo detectou a falha na autenticação do usuário devido à falsidade das informações fornecidas na tentativa de acesso.

Na prática, utilizou-se o software "*Tcpdump*" através do terminal, que capturou todo o tráfego proveniente do dispositivo móvel tendo como referência o momento inicial e final definidos previamente. O comando para realizar a captura é descrito no quadro 3.5.

Quadro 3.5 - Captura com o TCPDump

```
1) Tcpdump –i eth1 –s 1500 –w nomedoarquivo.pcap
```

Onde:

Tabela 3.2 - Lista de comandos do TCPdump

Parâmetro	Significado
-i	"interface" | -i | interface a ser monitorada
-s	"size" | -t | tamanho do pacote
-w	"write" | -w | escrever arquivo no disco

Para a primeira captura foi atribuída a nomenclatura "*captura1.pcap*", para a segunda "*captura2.pcap*" e para a terceira "*captura3.pcap*", segundo a Tabela 3.3.

Tabela 3.3 - Pacotes e duração da captura

Banco	Nome do arquivo	Duração da captura
Banco 1	"captura1.pcap"	65.457098 segundos
Banco 2	"captura2.pcap"	27.846014 segundos
Banco 3	"captura3.pcap"	44.651021 segundos

Antes de analisar o pacote no software "*Netwitness*", foi necessário verificar se todos os dados capturados eram estritamente relacionados aos aplicativos bancários. Para isso utilizou-se um "*sniffer*" tal como o *software* "*Wireshark*", uma vez que este programa é capaz de carregar arquivos oriundos do "*Tcpdump*", no formato "*pcap*". Assim, prosseguiu-se carregando cada um dos pacotes no "*Wireshark*" e aplicando filtros de forma que a comunicação *smartphone* - banco fosse completamente isolada de dados não relacionados, a partir da verificação dos endereços IP de fonte e destino, conforme as Figuras 3.5, 3.6 e 3.7.

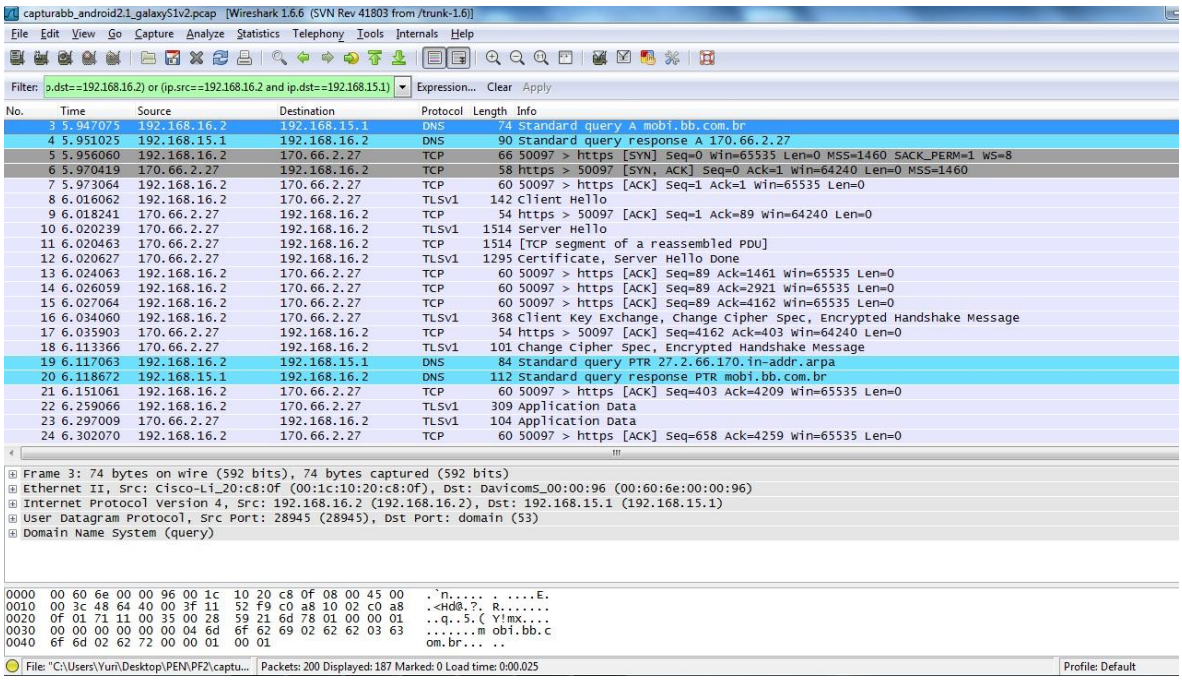


Figura 3.5 - Banco 1 no Wireshark

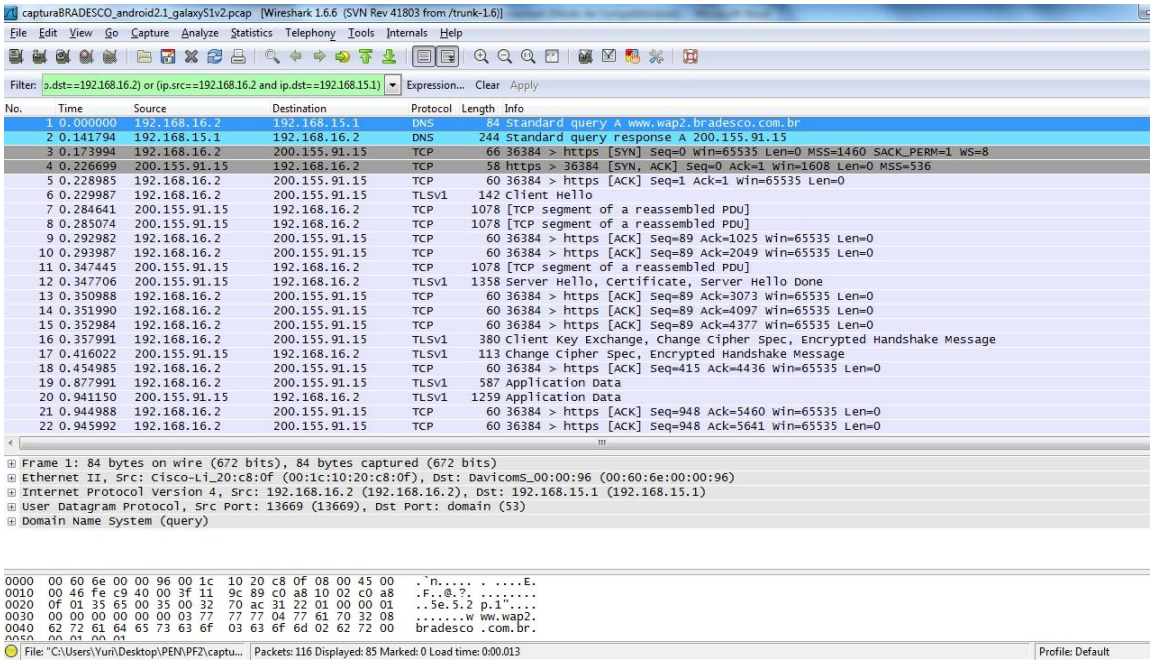


Figura 3.6 - Banco 2 no Wireshark

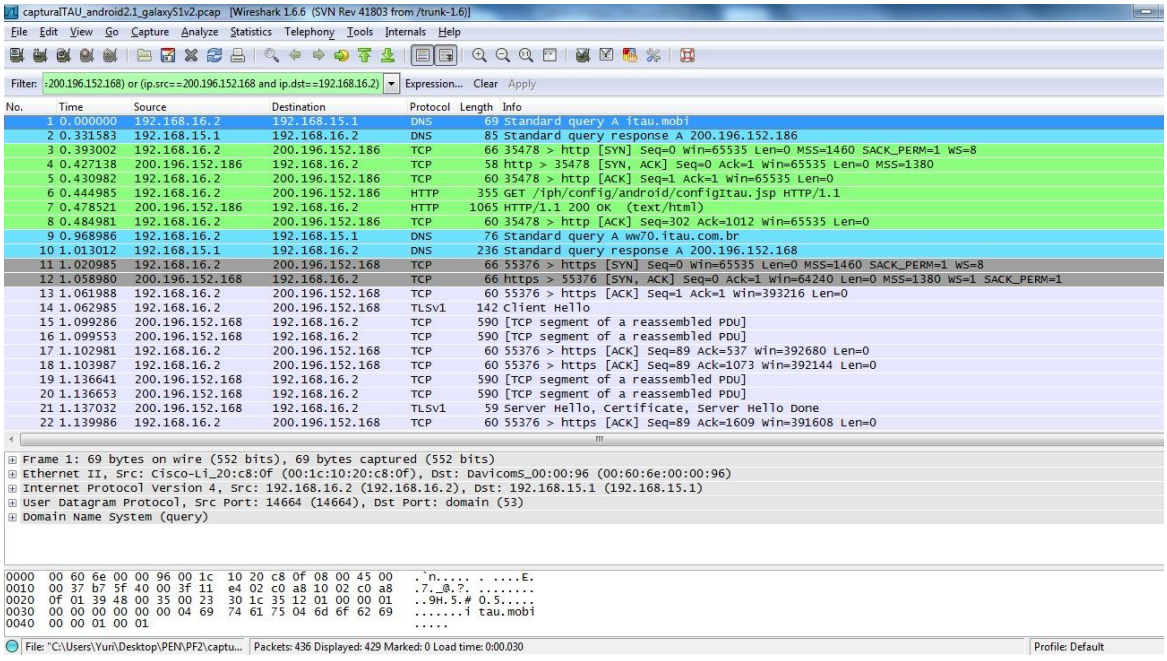


Figura 3.7 - Banco 3 no Wireshark

3.2.3. Seleção dos dados

Para selecionar as informações no "*Wireshark*" utilizaram-se alguns filtros, contudo é imprescindível reconhecer, em primeiro lugar, os endereços de origem e destino das instituições bancárias de forma a não trazer informações inadequadas à análise dos dados obtidos. Dessa forma, o quadro 3.6 mostra os filtros utilizados respectivamente, para os bancos 1, 2 e 3. Utilizou-se lógica Booleana na barra de filtragem para selecionar os endereços de origem e destino, a fim de cobrir todas as possibilidades do tráfego de origem ou de destino pertencerem aos bancos ou à rede do laboratório.

Quadro 3.6 - Filtros do wireshark

```
1) (ip.src==192.168.16.2 and ip.dst==170.66.2.27) or
   (ip.src==170.66.2.27 and ip.dst==192.168.16.2) or
   (ip.src==192.168.15.1 and ip.dst==192.168.16.2) or
   (ip.src==192.168.16.2 and ip.dst==192.168.15.1)

2) (ip.src==192.168.16.2 and ip.dst==200.155.91.15) or
   (ip.src==200.155.91.15 and ip.dst==192.168.16.2) or
   (ip.src==192.168.15.1 and ip.dst==192.168.16.2) or
   (ip.src==192.168.16.2 and ip.dst==192.168.15.1)

3) (ip.src==192.168.16.2 and ip.dst==200.196.152.186) or
   (ip.src==200.196.152.186 and ip.dst==192.168.16.2) or
   (ip.src==192.168.15.1 and ip.dst==192.168.16.2) or
   (ip.src==192.168.16.2 and ip.dst==192.168.15.1) or
   (ip.src==192.168.16.2 and ip.dst==200.192.152.168) or
   (ip.src==200.192.152.168 and ip.dst==192.168.16.2)
```

No quadro acima, o endereço 170.66.2.27 refere-se ao endereço IP do Banco 1, o endereço 200.155.91.15 refere-se ao banco 2 e por fim os endereços 200.196.152.186 e 200.192.152.168 referem-se ao banco 3.

Posteriormente a análise feita no "*Wireshark*", salvou-se os pacotes de modo a suprimir os dados não desejados. A opção "salvar como" no *menu* "*File*" permite salvar apenas os dados apresentados na tela do programa, excluindo os não filtrados. A Figura 3.8 exemplifica um dos casos.

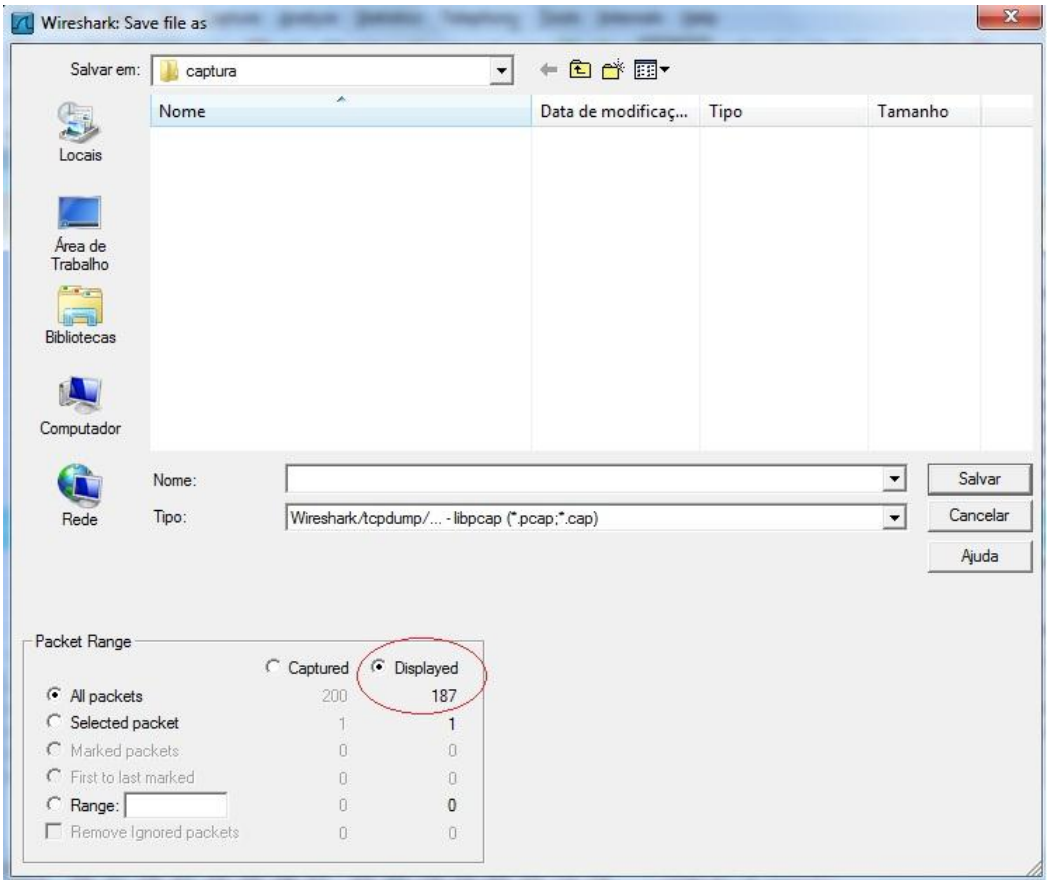


Figura 3.8 - Salvar o pacote filtrado

3.2.4. Análise

Para fins comparativos e de análise dos dados, procedeu-se de forma a replicar o mesmo procedimento apresentado anteriormente, para os três dados de captura, dessa forma obtiveram-se condições de carregar os pacotes no programa "*Netwitness*" e assim observar os relatórios gerados pelo *software*. Para isso, executou-se o programa, em seguida clicando no ícone "*New Local Collection*" dentro da janela "*Collection*", como apontado na figura 3.9:

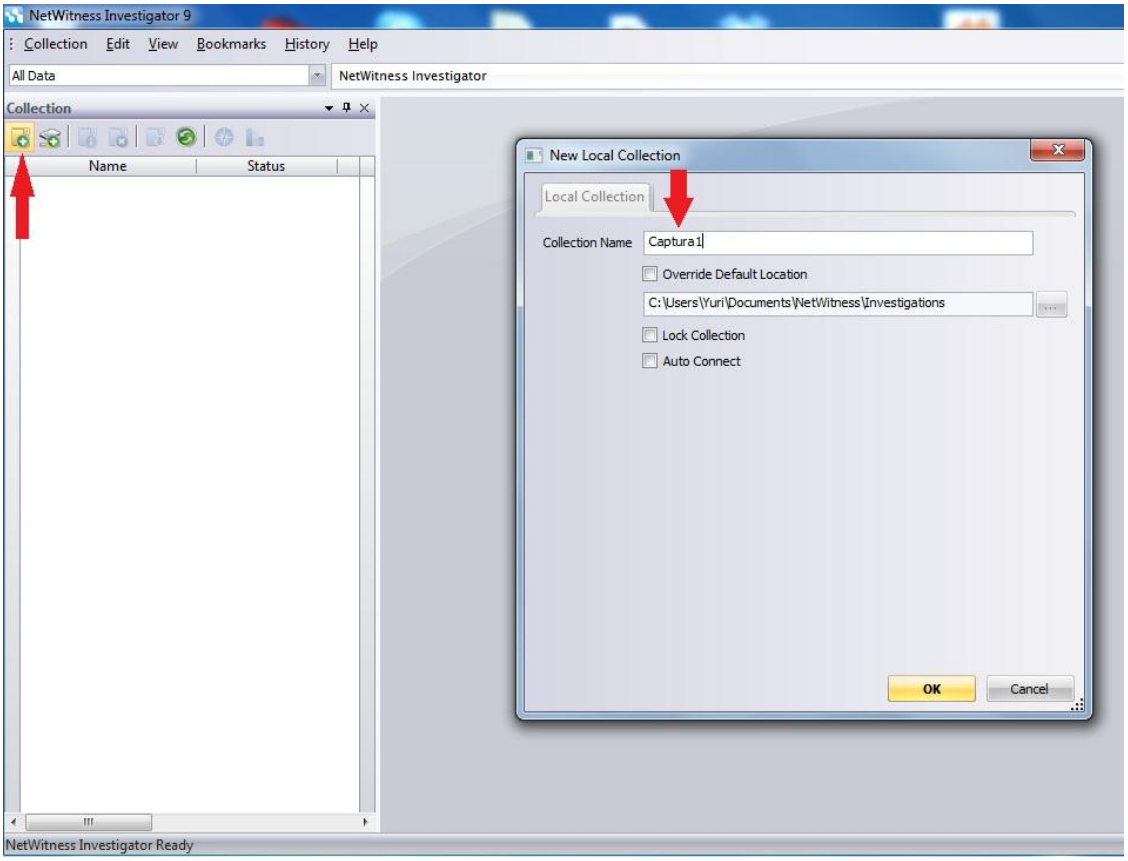


Figura 3.9 - Adicionar coleção ao Netwitness

Nomeou-se a coleção arbitrariamente, e em seguida, a coleção foi criada anteriormente ao estabelecimento da conexão, clicando com o botão direito sobre a coleção criada para, enfim, importar o pacote, como mostrado nas figuras 3.10 e 3.11.

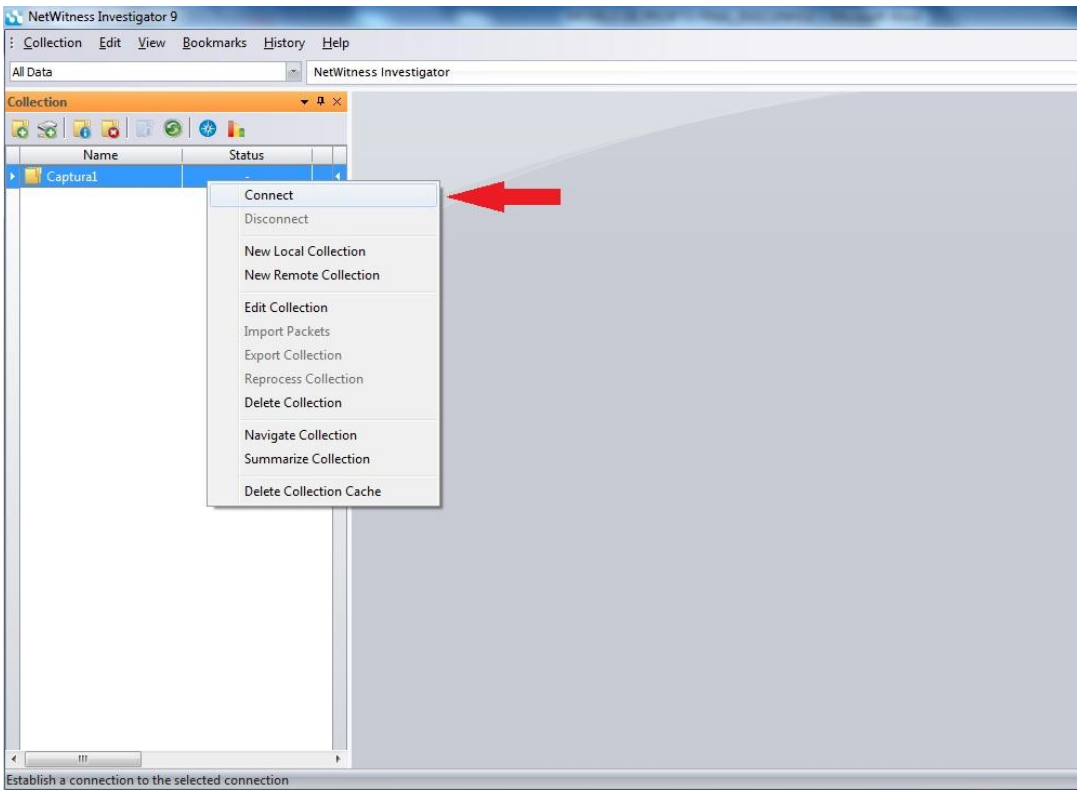


Figura 3.10 – Conectar coleção

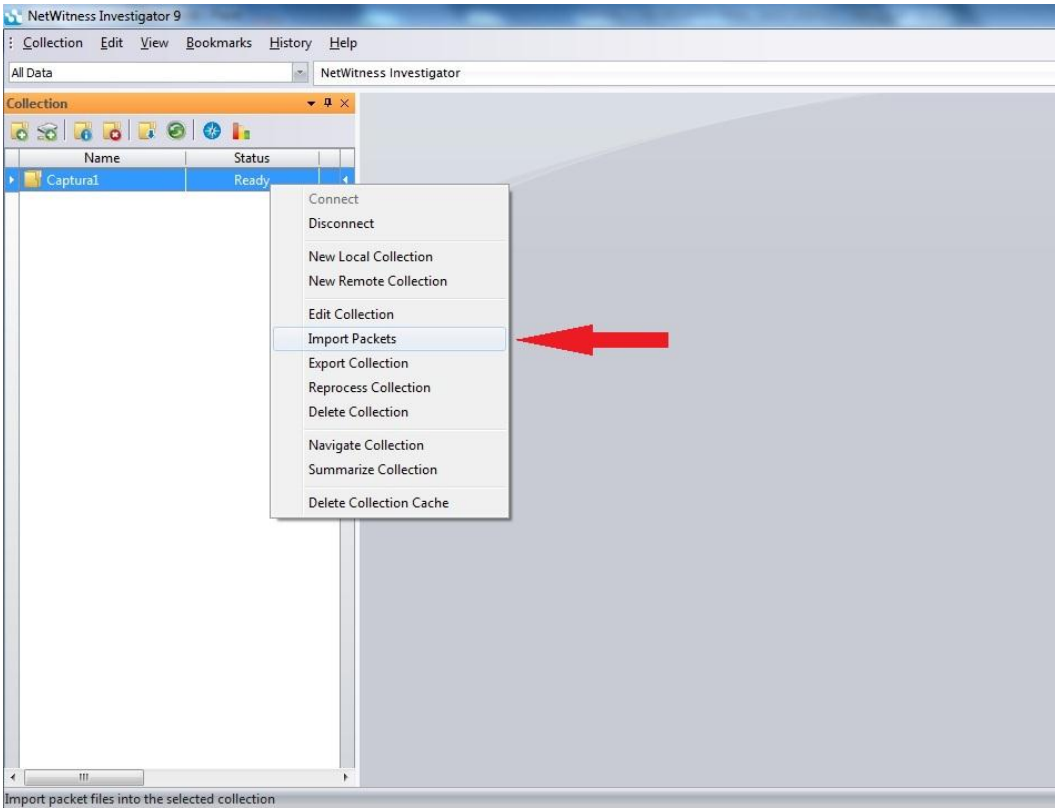


Figura 3.11 - Importar pacotes

Por fim, aguardou-se o status apresentar a palavra "*Ready*", o que significa que já é possível analisar a coleção e ter acesso à meta dados gerados no relatório do programa. Para isso clicou-se no ícone "*Navigate the selected collection*" na janela "*Collection*". As figuras 3.12 e 3.13 mostram esse passo e o resultado.

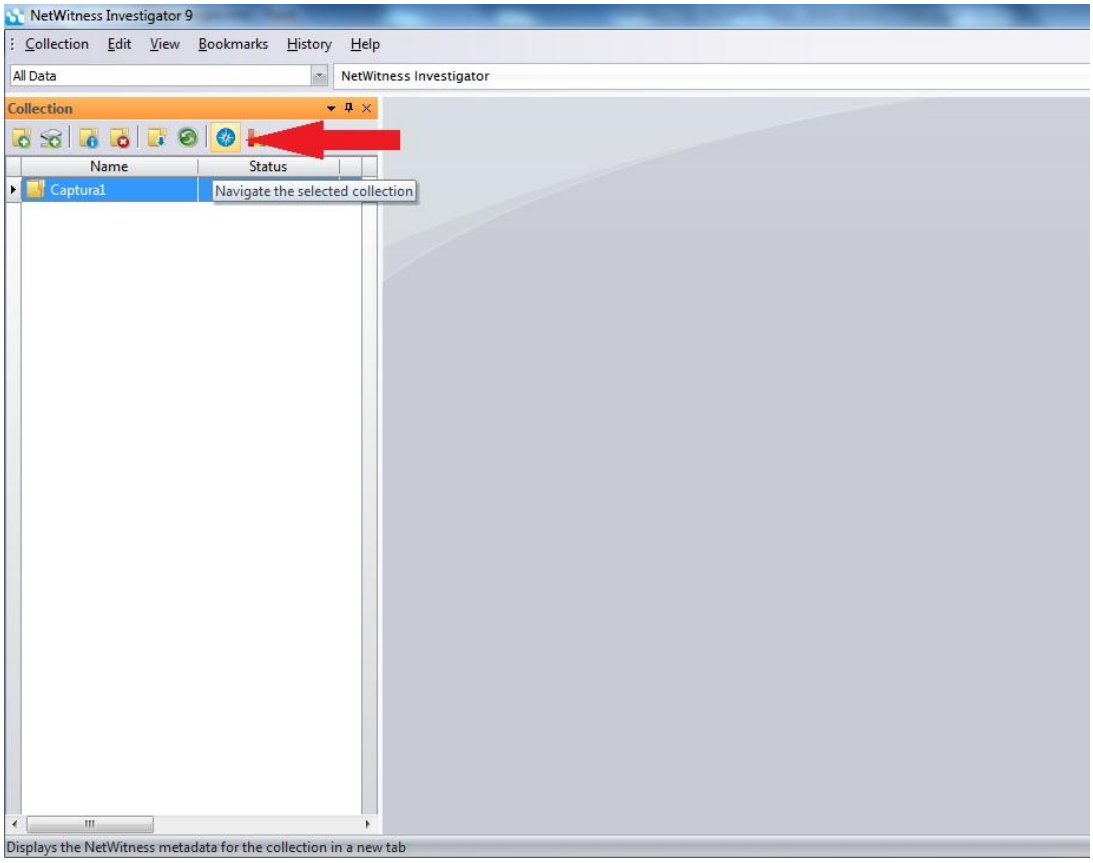


Figura 3.12 - Navegar coleção

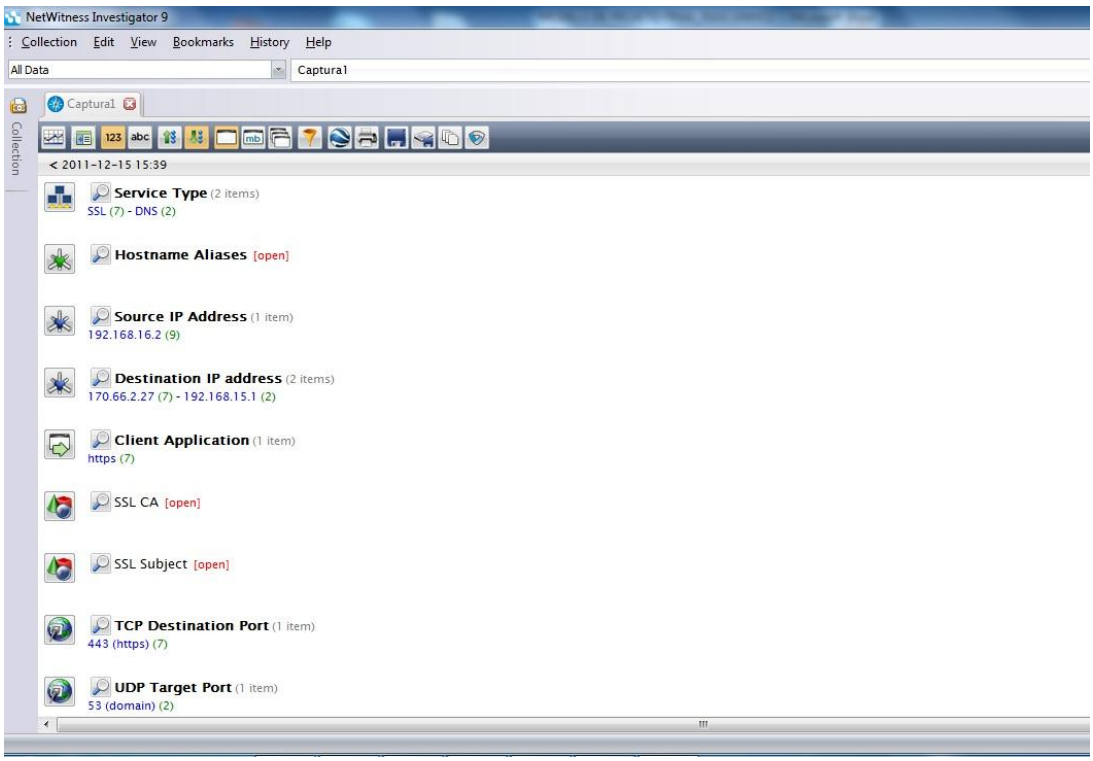


Figura 3.13 - Relatório Netwitness

Para os fins deste trabalho foram suprimidos alguns dados do relatório, com o objetivo de manter o anonimato dos Bancos em questão. Por isso, alguns campos como "*Hostname Aliases*", "*SSL CA*" e "*SSL Subject*" foram fechados. A seguir, voltou-se para a janela "*Collection*" e pôde-se acessar o sumário dos pacotes importados no programa – Nessa opção, é possível obter uma visão gráfica da quantidade de pacotes, de bytes e de sessões relacionadas aos dados coletados. As figuras 3.14 e 3.15 mostram esse resultado.

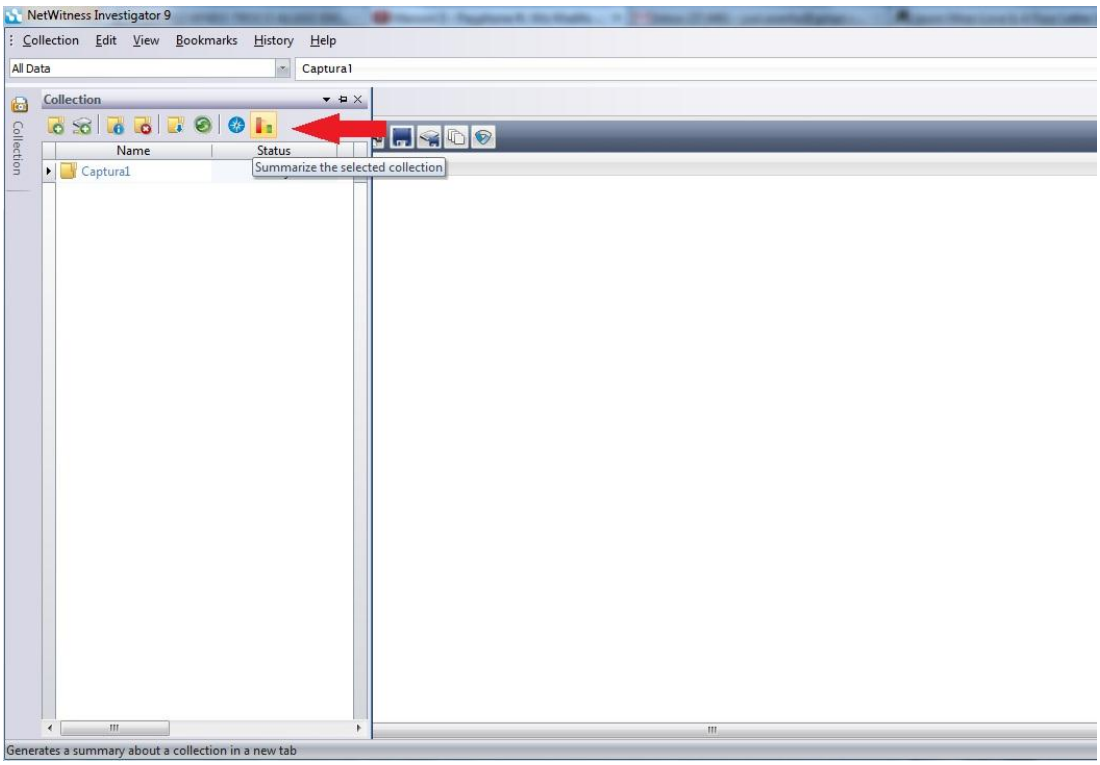


Figura 3.14 - Sumário da coleção

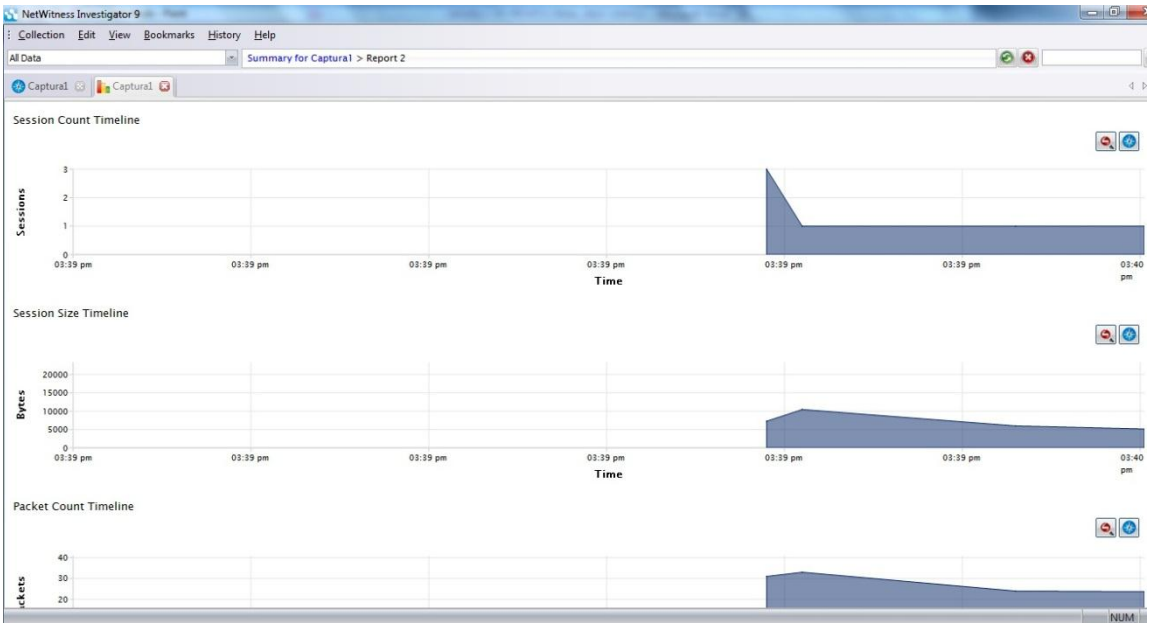


Figura 3.15 – Resultados gráficos do sumário

Replicou-se o mesmo procedimento para os dois outros dados coletados referentes aos outros dois bancos. E como resultado final extraiu-se as informações pertinentes que estão contidas na tabela 3.4 a partir das informações fornecidas pelos relatórios do "*Netwitness*":

Tabela 3.4 - Dados do relatório do Netwitness

Campo	**Banco 1**	**Banco 2**	**Banco 3**
Service Type	SSL - DNS	SSL - DNS	HTTP - SSL – DNS
Hostname Aliases			
Source IP Address	192.168.16.2	192.168.16.2	192.168.16.2
Destination IP Address	170.66.2.27	200.155.91.15	200.196.152.186, 200.192.152.168
Action Event	-	-	Get
Content Type	-	-	text/html
Extension	-	-	Jsp
Client Application	HTTPS	HTTPS	HTTPS
TCP Destination Port	443(https)	443(https)	443(https), 80(http)
UDP Target Port	53(domain)	53 (Domain)	53 (Domain)
Destination Country	Brazil	Brazil	Brazil
Destination Organization			
Destination City	Brasilia	São Paulo	-
Destination Domain			
Ethernet Protocol	IP	IP	IP
IP Protocol	TCP - UDP	TCP - UDP	TCP – UDP
Crypto	rsa-with-rc4-128-sha	rsa-with-aes-128-cbc-sha	rsa-with-rc4-128-md5
Ethernet Source	00:1C:10:20:C8:0F	00:1C:10:20:C8:0F	00:1C:10:20:C8:0F
Ethernet Destination	00:60:6E:00:00:96	00:60:6E:00:00:96	00:60:6E:00:00:96

Novamente, é necessário frisar que, para os fins deste trabalho foram suprimidos alguns dados do relatório, de modo a manter o anonimato dos Bancos. Dessa forma, alguns campos foram apagados da tabela acima. Em dados quantitativos, para os bancos 1, 2 e 3, obtiveram-se os resultados apresentados nos gráficos das figuras 17, 18 e 19 presentes no Anexo I, II e III, respectivamente.

4. CONCLUSÃO

A partir dos conhecimentos sobre interceptação de dados, telefones inteligentes e ferramentas de rede, foi apresentado neste trabalho um método simples e objetivo, capaz de extrair dados da comunicação usuário – instituição financeira, e com o auxílio de analisadores de pacote e softwares forenses, obteve-se uma visualização mais apurada dos dados. A metodologia foi apresentada de forma sucinta e objetiva através do fluxograma presente no capítulo 3, que posteriormente foi apresenta de forma detalhada juntamente com os passos do processo. Foi visto que o método apresenta quatro diferentes fases: A fase de configuração, a fase de captura, a fase de seleção dos dados e por fim a fase de análise.

Apesar de a metodologia apresentada fazer referência exclusiva a telefones inteligentes, mais especificamente a um único aparelho com o sistema operacional Android, ela não se restringe unicamente a esse modelo e sistema operacional. É possível estender o mesmo método, utilizando os mesmos procedimentos para dispositivos móveis diferentes. Além disso, outras plataformas de dispositivos móveis também poderiam ser utilizadas. A metodologia deste trabalho é flexível tanto em termos de dispositivo móvel, quanto em termos de sistema operacional, desde que existam aplicativos aos quais se desejam interceptar os dados.

A partir das informações obtidas nesse trabalho é possível, sob uma visão macro, notar diferenças importantes entre os dados interceptados dos três bancos. De acordo com o software “Netwitness”, o tipo de serviço é o mesmo para o banco 1 e para o banco 2, apresentando os protocolos SSL (Security Sockets Layer) e DNS (Domain Name System), o primeiro é um protocolo criptográfico da camada de aplicação do modelo OSI, assim como o segundo, um protocolo também da camada de aplicação responsável por associar e distribuir nomes de domínio hierarquicamente de acordo com endereços IP mapeados. O banco 3, além do DNS e do SSL apresenta no campo “tipo de serviço” o protocolo HTTP (Hyper Text Transfer Protocol). Outro campo de fundamental importância é o campo criptografia. Notavelmente, apesar de todos os três bancos utilizarem cifras RSA (Rivest-Shamir-Adleman), que consite em um algoritmo criptográfico assimétrico desenvolvido para a criptografia de chave pública, o banco 1 utiliza-a juntamente com o RC4 – 128 – SHA, que consiste em uma cifra de fluxo com tamanhos de chave variável e operações orientadas a *byte*, seu algoritmo é baseado em permutação aleatória. O banco 2, por sua vez, utiliza o RSA combinado com os algoritmos AES – 128 – CBC – SHA, que é uma cifra de bloco simétrica com tamanho de bloco igual a 128 bits e suporte para tamanhos de chave iguais a 128, 192 e

256 bits. O CBC (Cipher Block Chaining) consiste em um modo de operação da cifra de bloco no qual ocorre o encadeamento de blocos cifrados, de modo que a entrada do algoritmo criptográfico equivale à operação booleana “ou exclusivo - XOR” dos próximos 64 bits de texto claro com os 64 bits anteriores de texto cifrado; a mesma chave é usada para cada bloco. Por fim, o banco 3 utiliza a mesma cifra RC4 – 128 – MD5. Contudo, utiliza outra função de *hash*, o MD5 (Message Digest 5), que é uma função de *hash* amplamente utilizada e que produz um valor de *hash* de 128 bits, é utilizada para checar integridade de dados. O SHA (Secure Hash Algorithm), presente na criptografia dos bancos 1 e 2, consiste em um algoritmo que foi desenvolvido pelo NIST. Ele produz um *hash* de 160 bits e é baseado nos princípios usados no MD4 e MD5.

Apesar do mesmo método ter sido aplicado nos três casos, notaram-se diferenças no número de pacotes e no tempo de captura, pois o procedimento de acesso à conta não é o mesmo para cada banco. A partir dos gráficos gerados é possível verificar que para o banco 1 tem-se inicialmente 3 sessões, atingindo um pico de 10 Kbytes e 34 pacotes, aproximadamente. O banco 2 apresenta incialmente 2 sessões, atingindo um pico de 12,5 Kbytes e 36 pacotes, aproximadamente. Por fim, o banco 3 apresenta inicialmente 2 sessões, posteriormente passando a 3 sessões, atingindo um pico de 75 Kbytes e 220 pacotes.

Dessa forma, mesmo com uma análise superficial das informações encontradas, conseguiu-se extrair informações importantes sobre os dados coletados. Dessa forma é conclusivo que o método proposto fornece ferramentas eficazes para obter informações.

4.1. Trabalhos Futuros

Com a finalidade de prosseguir o trabalho desenvolvido, é interessante aperfeiçoar e aprofundar a análise das informações bancárias. Além disso, espera-se que futuros trabalhos possam estudar os dados de diversas operações bancárias a fim de evidenciar possíveis vulnerabilidades e propor soluções para uma comunicação mais segura e repetir os procedimentos apresentados para outros tipos de dispositivos.

Como a ferramenta “Netwitness” apresenta muitos outros recursos, pode-se ainda, utilizar conceitos avançados de criptografia e segurança da informação e realizar uma análise voltada à área da ciência forense.

REFERÊNCIAS BIBLIOGRÁFICAS

A. Freier, P. Karlton, P. Kocher (August 2011): “The Secure Sockets Layer (SSL) Protocol Version 3.0”. Disponível em: <http://tools.ietf.org/html/rfc6101> Acesso em: 15 Julho 2012.

CIAB FEBRABAN 2012. “O setor bancário em números”. Ciab, 27 abril 2012. Disponível em: < http://www.ciab.com.br/_pdfs/publicacoes/Pesquisa2012.pdf> Acesso em: 16 julho 2012.

Degusta M. (2012): “Are Smart Phones Spreading Faster than Any Technology in Human History”, 9 de maio de 2012. Disponível em: < http://www.technologyreview.com/news/427787/are-smart-phones-spreading-faster-than-any/> Acesso em: 11 Julho 2012.

ETSI, Handover interface for the lawful interception of telecommunications traffic, ETSI TS 101 671, version 3.6.1, August 2010. Disponível em: <http://www.etsi.org/deliver/etsi_ts/101600_101699/101671/03.09.01_60/ts_101671v030901p.pdf> Acesso em: 30 de Julho 2012

Fielding, Roy T.; Gettys, James; Mogul, Jeffrey C.; Nielsen, Henrik Frystyk; Masinter, Larry; Leach, Paul J.; Berners-Lee (June 1999). "RFC 2616: Hypertext Transfer Protocol -- HTTP/1.1". Disponível em: <http://tools.ietf.org/html/rfc2616> Acesso em: 15 Julho 2012.

Google Inc. What is Android? Android Developers, 2011f. Disponível em: <http://developer.android.com/guide/basics/what-is-android.html> Acesso em: 30 junho 2012.

Jansen, W.; Ayers, R. Guidelines on Cell Phone Forensics – Recommendations of the National Institute of Standards and Technology. [S.q]. 2007.

Kevin J. Connolly (2003). *Law of Internet Security and Privacy*. Aspen Publishers. pp. 131.

P. Mockapetris (November 1987), The Internet Society. “RFC 1034: Domain Names - Concepts and Facilities”. Disponíve em: <http://tools.ietf.org/html/rfc1034> Acesso em: 15 Julho 2012.

Ramachandran V. Backtrack 5 Wireless Penetration Testing. 1ª Edição. Birmingham: Packt, 2011.

SANTOS, Deborah Oliveira; VEIGA, Ricardo Teixeira and SOUZA, Sarah Ituassú. Mobile banking como novo canal de disseminação de informações e disponibilização de serviços: um teste da teoria do comportamento planejado decomposto. Perspect. ciênc. inf. [online]. 2011, vol.16, n.4, pp. 150-170.

SIMÃO, André Morum de L. Proposta de Método para Análise Pericial em Smartphone com Sistema Operacional Android. [Distrito Federal] 2011. xiv, 96p.

Stallings, William. Criptografia e Segurança de Redes: Princípios e Pratica. 4º Edição. São Paulo: Pearson, 2007.

Tiwari, R., S. Buse, and C. Herstatt (2007): “Mobile Services in Banking Sector: The Role of Innovative Business Solutions in Generating Competitive Advantage”, in: *Proceedings of the International Research Conference on Quality, Innovation and Knowledge Management*, New Delhi, pp. 886-894.

Vaidya, S. (2011): “Emerging Trends on Functional Utilization of Mobile Banking in Developed Markets in Next 3-4 Years”, in: International Review of Business Research Papers Vol. 7. No. 1. January 2011. Pp. 301 – 312.

Yankee Group. Yankee Group Sees Global Mobile Transactions Exceeding $1 Trillion by 2015. 2011. Disponível em: <http://www.yankeegroup.com/about_us/press_releases/2011-06-29.html> Acesso em: 10 Julho 2012.

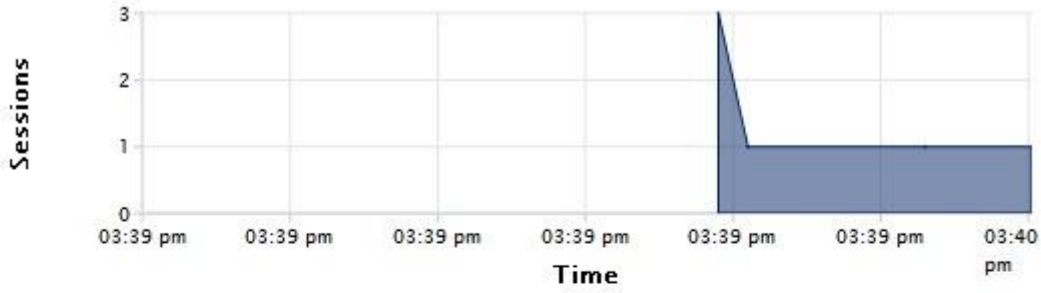
ANEXOS

Anexo 1 – Gráficos Banco 1.

Anexo 2 – Gráficos Banco 2.

Anexo 3 – Gráficos Banco 3.

Session Count Timeline

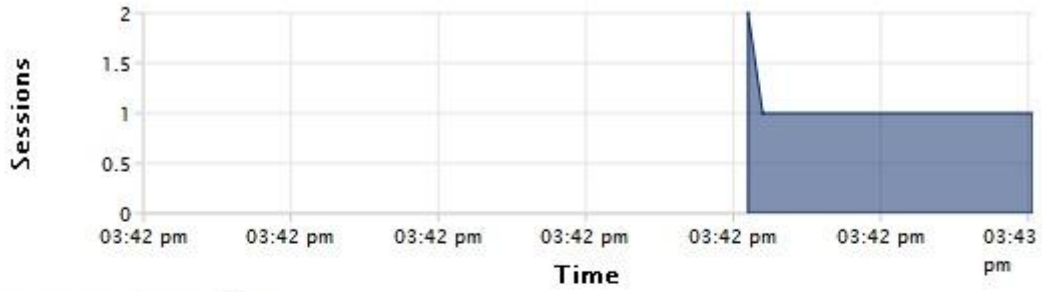


Session Size Timeline

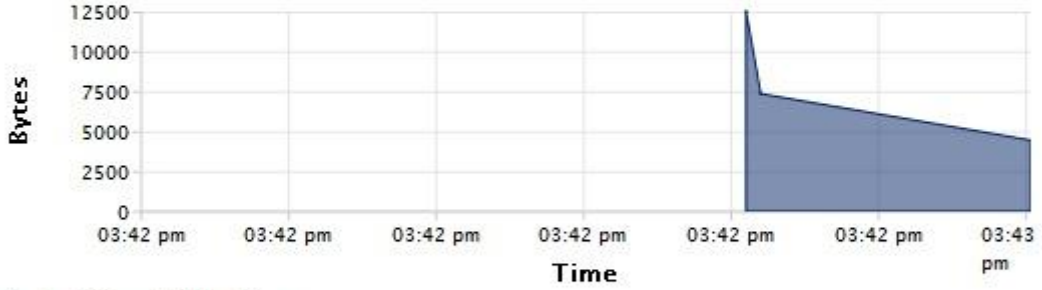
Packet Count Timeline

ANEXO 2: GRÁFICOS BANCO 2

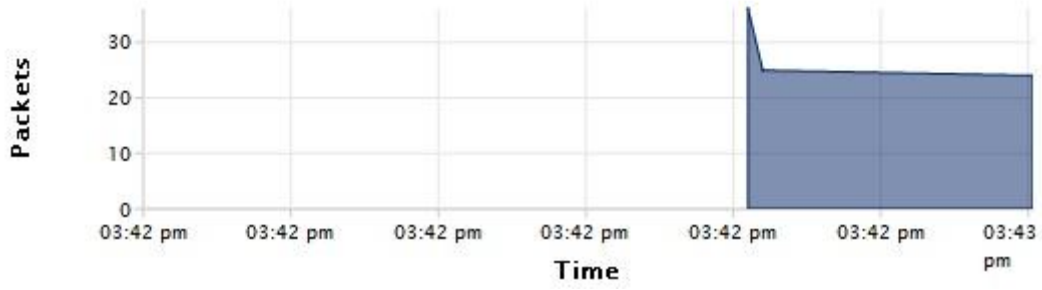
Session Count Timeline



Session Size Timeline

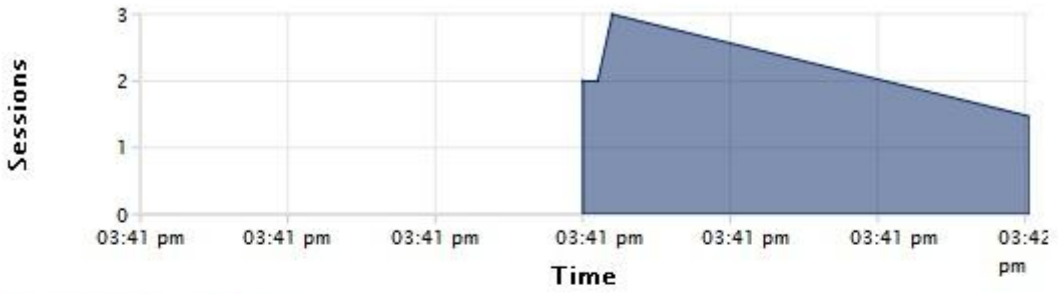


Packet Count Timeline



ANEXO 3: GRÁFICOS BANCO 3

Session Count Timeline



Session Size Timeline

Packet Count Timeline