CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

SEGURANÇA DE DADOS FIM A FIM

UTILIZANDO O PRETTY GOOD PRIVACY

Americana, SP

2015

CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA
Curso Superior de Tecnologia em Segurança da Informação

DANIEL BARBOSA

SEGURANÇA DE DADOS FIM A FIM
UTILIZANDO O PRETTY GOOD PRIVACY

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso de Segurança da Informação, sob a orientação do Prof. Rodrigo Brito Battilana.
Área de concentração: Segurança de Dados Fim a Fim.

Americana, SP
2015

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

B196s	Barbosa, Daniel Segurança de dados fim a fim. / Daniel Barbosa. – Americana: 2015. 58f. Monografia (Graduação em Tecnologia de Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza. Orientador: Prof. Rodrigo Brito Battilana 1.Segurança de sistemas de informação. Battilana, Rodrigo Brito II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana. CDU: 681.518.5

Daniel Barbosa

SEGURANÇA DE DADOS FIM A FIM

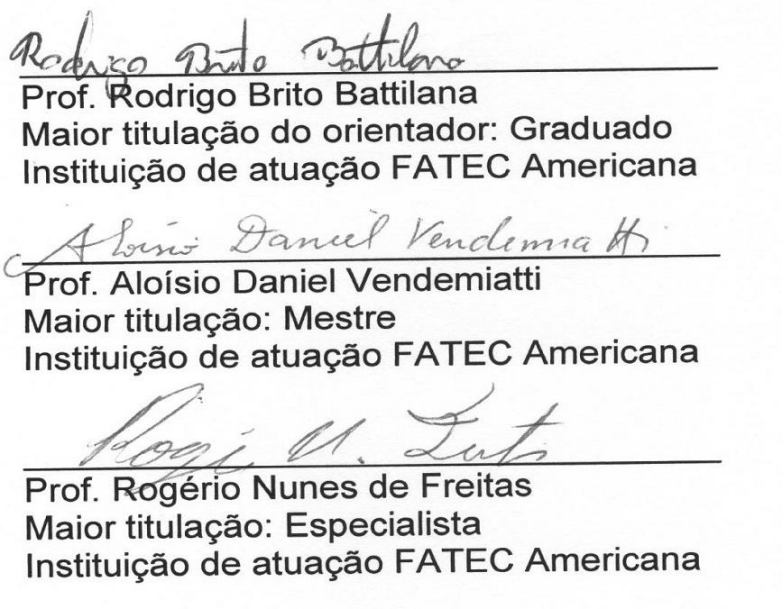
UTILIZANDO O PRETTY GOOD PRIVACY

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.

Área de concentração: Segurança de Dados Fim a Fim.

Americana, 22 de Junho de 2015.

Banca Examinadora:



Prof. Rodrigo Brito Battilana
Maior titulação do orientador: Graduado
Instituição de atuação FATEC Americana

Prof. Aloísio Daniel Vendemiatti
Maior titulação: Mestre
Instituição de atuação FATEC Americana

Prof. Rogério Nunes de Freitas
Maior titulação: Especialista
Instituição de atuação FATEC Americana

AGRADECIMENTOS

Agradeço primeiramente a Deus pela oportunidade que ele tem me dado de estudar, esteve comigo nos momentos de alegria e de dificuldades e me forneceu capacidade para finalizar mais esta etapa de minha vida.

Eu quero agradecer também a todos os professores da Fatec Americana pela dedicação, pela atenção ao longo desse período ao qual estivemos juntos.

Quero agradecer a empresa Xeefdesigner pela oportunidade do estágio, também pelas amizades ali conquistadas, por compartilhar o conhecimento e me auxiliar em todas as dúvidas presentes.

A saudosa professora Mestre Maria Cristina Luz Fraga Moreira Aranha, pela atenção, e sugestões que, sem sombra de dúvida, foi essencial para a conclusão desse projeto.

Também agradeço ao meu orientador Rodrigo Brito Battilana por aceitar o desafio e me orientar ao longo desse projeto, pela paciência. Obrigado por tudo.

DEDICATÓRIA

À minha esposa Michele Andrade de Oliveira Barbosa, primeiramente pela confiança, atenção, pela amizade, e pelo amor que temos um para com o outro e que sempre me motivou, me apoiou nos momentos difíceis e aceitou a minha ausência quando se fez necessário.

Aos meus pais Aparecida Antonio Barbosa e Waldemar Barbosa pelo carinho e atenção, e pela confiança depositada em min.

Aos meus amigos, pela ajuda e incentivo, que fizeram com que essa jornada fosse concluída com alegria.

RESUMO

Esta monografia tem por objetivo demonstrar o funcionamento do trafego de dados através da Internet, demonstrando as vulnerabilidades e também como fazer para melhorar a proteção. Muitas das vezes não sabemos os caminhos que as informações estão trafegando, pode estar em outra cidade, estado, ou até mesmo em outros países. Além disso, a Internet é muito ampla e os periféricos usados são os mais diversos, traçando rotas que nem mesmo sabemos. Pouco importa o seu funcionamento desde que atinja um objetivo comum, enviar e receber informações. Por isso surgiu à necessidade de desenvolver algo que venha responder todas as perguntas, tanto para o usuário leigo em segurança como também para o especialista no assunto. Afinal a segurança não é um problema de tecnologia, mas sim quem utiliza a tecnologia. Alguns métodos serão abordados nesse projeto: o funcionamento do certificado digital, a diferença entre o certificado assinado e o auto-assinado, e a importância de uma entidade certificadora. Mas o ponto mais importante desse trabalho é a utilização da criptografia para obter a integridade, privacidade, e o não repudio da informação, e tornar o envio de dados um pouco mais seguro.

Palavras-chave: Segurança de dados fim a fim. Criptografia, Certificados Digitais.

ABSTRACT

This monograph’s objective is to demonstrate the working of data trafficking thought the Internet, demonstrating vulnerabilities and how to improve protection.

We often do not know where the information is traveling through; it may be in another city, state or even other country. The Internet is vast, and the peripheral used are diverse, tracing unknown routes; as long as a common goal is reached – sending and receiving information – it doesn’t really matter how that works. From this arose?

The need to develop something that will answer all the questions from both the layman and expert in security.

After all, safety is not an issue for the technology, but rather for the user. Some methods will be addressed in this project: how digital certificates work, the difference between the signed certificate and the self-signed, and also the use of the certifying entity. But the most important point of this work is the use of encryption for the integrity, privacy and non-repudiation of the information, and making sending data a little safer.

Keywords: Data security end to end, Encryption, digital certificates.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIAÇÕES

HTTP – Hypertext Transfer Protocol

HTTPS – Hypertext Transfer Protocol Secure

SSL – Secure Sockets Layer

WWW – Word Wide Web

PGP - Pretty Good Privacy

IDEA - International Data Encryption Algorithm

TCP – Transmission Control Protocol

IP-Protocol Internet

AES - Advanced Encryption Standard

HTML – Hypertext Markup Language

URL – Uniform Resource Locator

NSA – National Security Agency

MD5 - Message-Digest algorithm 5

RFC – Request for Comments

MIME - Multipurpose Internet Mail Extensions

MIT - Instituto de tecnologia de Massachusetts

CERN - Organização Européia para Pesquisa Nuclear

ITI - Instituto Nacional de Tecnologia da Informação

DES - Data Encryption Standard

ASCII – American Standard Code for Information Interchange

ICP-Brasil – Infraestrutura de Chaves Pública – Brasil

SHA1 – Secure Hash Algorithm

RFC - Request for Comments

AC - autoridade certificadora

AR - Autoridades Responsáveis

SUMÁRIO

1 INTRODUÇÃO

A segurança e a privacidade da informação é algo que muitas pessoas buscam, seja o usuário comum, como também o usuário mais experiente. As organizações são as mais interessadas no assunto, no que tange privacidade, integridade e a segurança de suas informações. A Internet proporciona uma série de benefícios, só que em algumas ocasiões é necessário o uso de ferramentas para dificultar o extravio das informações.

As ferramentas que serão abordadas são: certificados digitais, criptografia e dentre outros, que ao ser usado faz com que o ambiente de envio e recebimento de dados fique mais seguro. Esse projeto contém alguns capítulos, no qual o primeiro é uma breve introdução de todo o projeto. No segundo capítulo é descrito como funciona a segurança da informação e como que é formado o tripé da segurança. No terceiro capitulo é descrito alguns métodos de criptografia como: RSA, DES, AES e suas principais aplicações, como também o uso de certificados digitais assinados, auto-assinado, e o uso do SSL no protocolo HTTPS. No quarto capítulo é descrito o funcionamento da segurança no envio de email usando PGP. O capítulo subseqüente tem a finalidade de demonstrar o envio de dados usando o protocolo HTTP padrão. E também o uso SSL no protocolo HTTP, que gera então o HTTPS.

No protocolo HTTP as informações foram obtidas de forma clara, no qual os dados ficaram expostos, no segundo teste usando o HTTPS, também foi possível obter as informações através da quebra do túnel SSL, ou seja, a criptografia foi rompida.

No ultimo teste foi usado o Protonmail para o envio e recebimento de e-mails, no qual, não foi possível a captura das informações, o Protonmail usa o protocolo HTTPS que aumenta o nível de segurança.

2 SEGURANÇA DE INFORMAÇÃO

A segurança da informação pode ser entendida como um conjunto de dados, no qual possui um valor significativo para cada individuo ou organização. Com o avanço tecnológico nos dias atuais, é muito comum os sistemas informatizados estarem interconectados, com isso os benefícios são enormes, mas também é importante atentar-se aos riscos e as vulnerabilidades (TANEMBAUM, 2007).

A segurança da informação tem por objetivo fazer com que à consistência do sistema não seja afetada, garantindo assim a redução das ameaças, fraudes, roubo ou extravio da informação. Essa segurança pode ser implantada em níveis de acordo com as informações a serem protegidas, isso depende muito de cada usuário. No caso da segurança ser em uma organização, uma boa política de segurança pode trazer mais benefícios, diminuindo os riscos, ameaças ou vulnerabilidades (TANEMBAUM, 2007).

Serão abordados nesse projeto os riscos inerentes ao uso de mensagem eletrônica e a utilização da Internet para fazer comunicação (TANEMBAUM, 2007).

2.1 A BASE DA SEGURANÇA

A base da segurança pode ser descrita ou representada como um tripé, mais conhecida como tripé da segurança, são elas: Confidencialidade, Integridade e Disponibilidade. Demonstrado na figura 1 Tripé da Segurança (CAMPOS, 2007).

2.1.1 CONFIDENCIALIDADE

A confidencialidade dos dados tem por objetivo deixar as informações restritas somente para pessoas de confiança e autorizadas para seu manuseio. Garantir a confidencialidade é ter informações classificadas em níveis de acesso, por exemplo: baixa, média, alta ou extremamente confidencial (CAMPOS, 2007).

Qualquer incidente que possa ocorrer devido a pessoas não autorizadas acessando o sistema pode causar à quebra da confidencialidade, um exemplo bem básico é uma quebra de senha (CAMPOS, 2007).

2.1.2 INTEGRIDADE

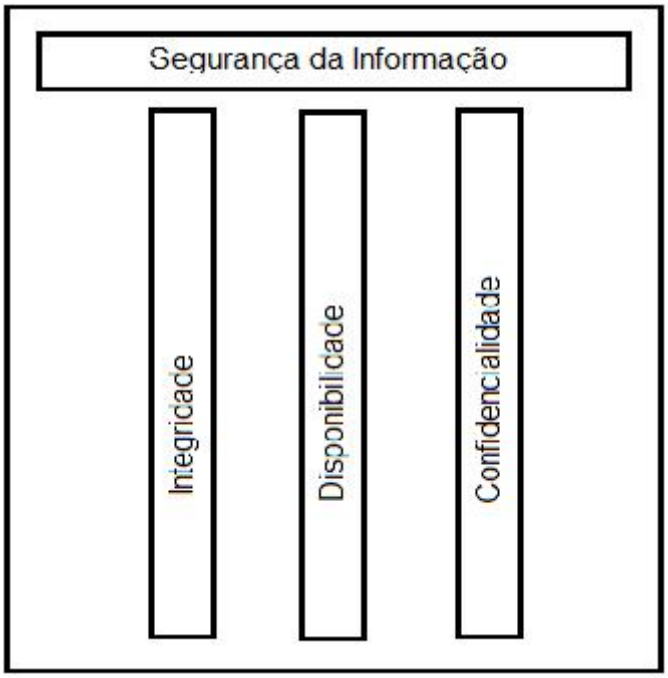
Integridade refere-se na certeza de que as informações não foram adulteradas ou corrompidas de nenhuma forma. Existem alguns processos em que as informações podem ser corrompidas: Armazenamento da informação, durante um *download* ou qualquer forma de envio ou recebimento da informação, em banco de dados e dentre outros (CAMPOS, 2007).

2.1.3 DISPONIBILIDADE

Disponibilidade da informação é manter os dados disponíveis quando necessário. Os sistemas dependentes de disponibilidade têm que fornecer algumas garantias contra riscos ou falhas, por exemplo: falta de energia, desastres naturais, falha de *hardware* e *software*, dentre outros (CAMPOS, 2007).

O grande desafio da disponibilidade é permitir que os usuários acessem as informações necessárias com um tempo de espera bem curto. Por isso o uso de sistemas de redundância é essencial para manter os sistemas operantes e disponíveis (CAMPOS, 2007).

Figura 1-Tripé da Segurança



Fonte: (CAMPOS, 2007, Pág. 17).

3 CRIPTOGRAFIA

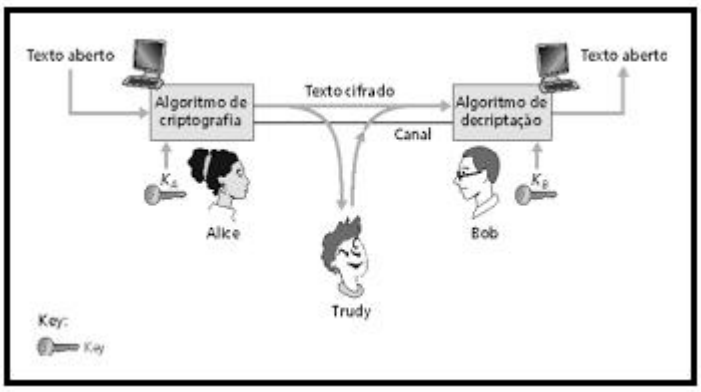
A palavra criptografia vem da palavra grega que significa "escrita secreta". A criptografia tem uma longa e interessante história de milhares de anos. Historicamente, quatro grupos de pessoas utilizaram ou contribuíram para a arte da criptografia: os militares, os diplomatas, as pessoas que gostam de guardar memórias e os amantes. Dentre eles, os militares tiveram o papel mais importante e definiram as bases para a tecnologia (TANENBAUM, 2007).

As mensagens a serem criptografadas, conhecidas como textos simples são transformados por uma função que é parametrizada por uma chave. Em seguida, a saída do processo de criptografia conhecida como texto cifrado, é transmitida normalmente através de um mensageiro ou via rádio. Presumimos que o inimigo, ou intruso, ouça e copie cuidadosamente o texto cifrado completo. No entanto, ao contrário do destinatário pretendido, ele não conhece a chave para descriptografar o texto e, portanto, não pode fazê-lo com muita facilidade. Às vezes, o intruso pode não só escutar o que se passa no canal de comunicação (intruso passivo), como também pode gravar mensagens e reproduzi-las mais tarde, injetar suas próprias mensagens ou modificar mensagens legitimas antes que elas cheguem ao receptor (intruso ativo). A arte de solucionar mensagem cifrada é conhecida como criptoanalise. A arte de criar mensagens cifradas (criptografia) e solucioná-las (criptoanalise) e ambas são chamadas coletivamente de criptologia (TANENBAUM, 2007).

3.1 CRIPTOGRAFIA SIMÉTRICA

O algoritmo mais conhecido até o dia de hoje é sem duvida o do imperador “Julio Cesar”, que usava a criptografia como meio para se comunicar com suas tropas. Desenvolvido pelo próprio imperador Cesar na Roma antiga, essa técnica de substituição da ordem do alfabeto era muito eficaz em sua época. Com isso as mensagens eram cifradas através do deslocamento de três casas do alfabeto para a esquerda (KUROSE; ROSS, 2006).

Figura 2-Criptografia Simétrica



Fonte: (KUROSE; ROSS, 2006).

Quando a cifra de Cesar foi quebrada, surgiram novos métodos para criptografar mensagens, como a cifra indecifrável que é nada mais nada menos do que a própria cifra de Cesar melhorada, que também foi quebrada (TANENBAUM, 2007).

Com o passar do tempo foram surgindo novos conceitos de criptografia, como a máquina desenvolvida pelos alemães na segunda guerra mundial. A máquina enigma ilustrada na figura 3, foi sem dúvida uma peça fundamental para o desfecho da segunda guerra mundial, já que os aliados conseguiram decifrar as mensagens enviadas pelos alemães e se adiantaram a frente do inimigo, conseguindo assim êxito em suas missões (ILHA, 2015).

Figura 3-Máquina Enigma

Fonte: (ILHA, 2015).

3.1.1 DES – DATA ENCRYPTION STANDARD

O algoritmo *data encryption standard* é um padrão de criptografia de chaves simétricas desenvolvido em meados de 1977 e atualizado recentemente em 1993, pelo U.S *National Bureau of Standards* para uso comercial e não classificado do governo norte americano. O DES codifica texto aberto em porções de 64 bits usando uma chave de 64 bits. Na verdade, oito desses 64 bits são de paridade ímpar, sendo assim a chave DES possui efetivamente 56 *bits.* O algoritmo passa por diversas etapas, sendo que o início dele tem um bloco de 64 *bits* e a saída de uma mensagem criptografada com os mesmos 64 *bits*. As mesmas etapas feitas para a criptografia são feitas para a descriptografia com o algoritmo DES (KUROSE; ROSS, 2006).

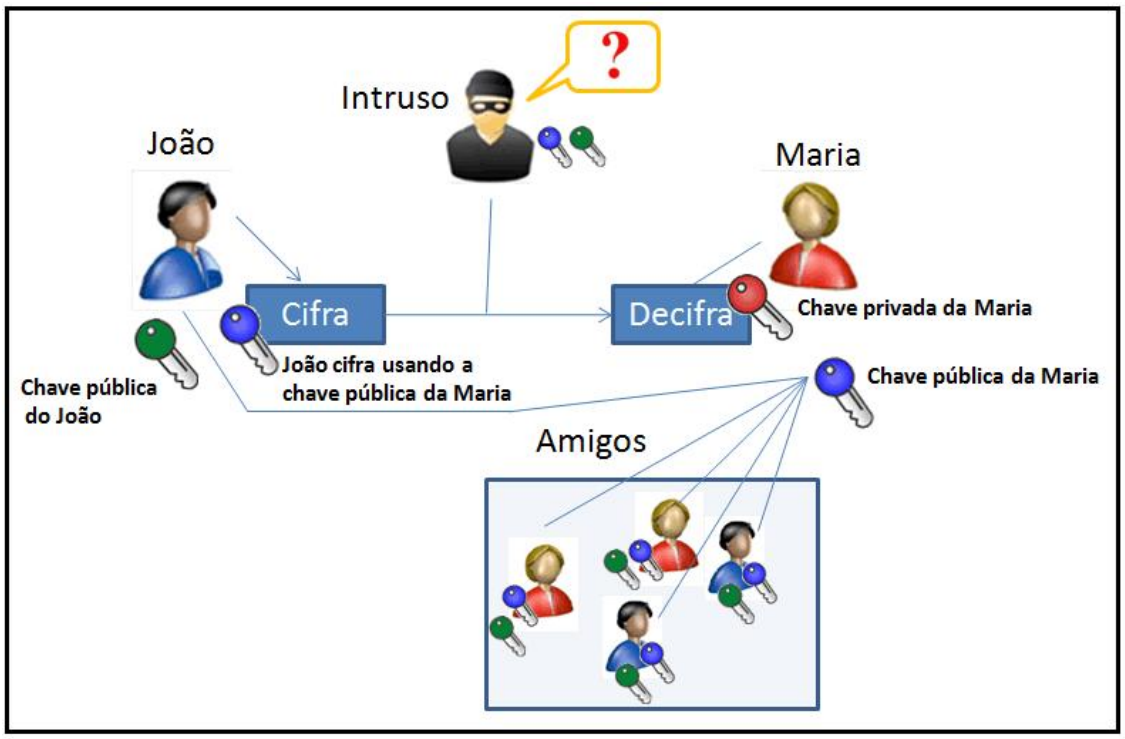
Em 1997, uma empresa de segurança de redes chamada RSA lançou um desafio chamado *challenge* e codificaram uma frase: (a boa criptografia faz do mundo um lugar mais seguro) foi decodificada em menos de quatro meses por uma equipe que usou voluntários por toda a Internet para explorar sistematicamente os espaços das chaves. Depois foi lançado novo desafio o *challenge* III também decifrado em 22 horas também por uma equipe de voluntários (KUROSE; ROSS, 2006).

3.2 CRIPTOGRAFIA ASSIMÉTRICA

Segundo Stallings (2008) o funcionamento da criptografia assimétrica pode criar um esquema de chaves e nesse esquema criptografar mantendo sigilo, autenticidade ou as duas coisas ao mesmo tempo dependendo do uso.

A figura 4 demonstra um cenário criando com dois personagens para entender melhor: João e Maria. Cada um gera um par de chaves, uma chave publica e uma chave privada. A chave privada não será compartilhada com ninguém, já no caso da chave pública, essa sim será compartilhada entre os amigos (STALLINGS, 2008).

Figura 4-Gerando chaves



Fonte: (COSTAFILHO; TELLESCOSTA, 2015).

Se a intenção é obter sigilo da mensagem então utiliza se da chave pública de seu amigo para criptografar a mensagem. No caso de requerer autenticidade, então criptografa com a própria chave privada a mensagem (STALLINGS, 2008).

E pra finalizar se a intenção é requerer sigilo mais autenticidade, então usa se primeiro a sua chave privada e depois com a chave pública de seu amigo (STALLINGS, 2008).

3.2.1 RSA

As letras RSA correspondem às iniciais dos nomes dos inventores do código, que são três matemáticos, Ronald Rivest, Adi Shamir e Leonard Adleman criaram em 1977 o que ainda hoje é muito utilizado na criptografia assimétrica. A criptografia e a decriptação do RSA parecem mágicas. Por que será que, quando aplicada no algoritmo de criptografia e, em seguida, o de decriptação, pode-se recuperar a mensagem original? Para entender como o RSA funciona é preciso colocar em prática o algoritmo para funcionar (MORENO; PEREIRA; CHIARAMONTE, 2005).

Todo o conceito é baseado na aritmética modular e a criação de chaves que está voltada para números primos de alta escala, o que torna mais difícil a descoberta das chaves (MORENO; PEREIRA; CHIARAMONTE, 2005).

A criptografia RSA é um sistema de criptografia onde a chave de codificação é pública, permitindo então que qualquer pessoa codifique mensagens, e a chave de descodificação é privada. A chave torna-se inviável de ser quebrada, uma vez que, não existem algoritmos eficientes para a fatoração de números inteiros em fatores primos, o que levaria muito tempo para a quebra da chave, por se trabalhar com números primos e com valores de grande ordem. Este tipo de criptografia é amplamente utilizado na Internet, seja em *sites* de *e-commerce*, transações bancarias, para conseguir manter as informações sigilosas são utilizadas assinaturas digitais para possibilitar a segurança em transações via Internet (KUROSE; ROSS, 2006).

Segundo Matos (2009), foi lançado um desafio, ou seja, uma competição para a quebra da criptografia RSA, no qual Matos foi o grande vencedor do desafio. Para a quebra da criptografia RSA foi usada uma linguagem de programação e várias horas de muito processamento. Quando o desafio ficou mais difícil, foi necessário o uso de dois computadores, com dois núcleos de processamento em conjunto e com decremento de oito em oito, foi necessário também usar *multi-threading* para não exigir muito esforço computacional. Ao fazer o uso de *single-thread* o processamento estava demorando muito e exigindo muito das máquinas que efetuavam as operações matemáticas, então surgiu à idéia de empregar o uso de *multi-threading* no último desafio, aí veio à surpresa, o desafio mais difícil foi vencido em 30 minutos com a resposta da mensagem.

3.3 PROTOCOLO HTTP

O protocolo de HTTP especifica as mensagens que os clientes podem enviar aos servidores e que respostas eles receberão. Cada interação consiste em uma solicitação ASCII, seguida por uma resposta RFC 822 semelhantes ao MIME. Todos os clientes e todos os servidores devem obedecer a esse protocolo. Ele é definido na RFC 2616, e ilustrado na tabela 1 (TANEMBAUM, 2007).

Tabela 1 Protocolo HTTP

Fonte: (TANEMBAUM, 2007).

Ao digitar um endereço para navegar em um *site* é muito comum que o protocolo “http://” apareça, porque o HTTP é o protocolo padrão para a transferência de dados em *sites*. O HTTP não fornece nenhum tipo de segurança para quem esta navegando pela Internet, é possível notar que ao clicar com mouse na barra de endereços e analisar a conexão, nota-se que a identidade do *site* será confirmada e também será possível ver os detalhes dessa conexão (CERT.BR, 2012).

3.4 SSL – SECURE SOCKETS LAYER

Segundo Tanembaum (2007), assim que surgiu o conceito Internet, essa era usada somente para distribuição de páginas estáticas. Com isso algumas empresas tiveram a percepção de usar a Internet para realizar trabalhos, ou seja, transações financeiras com cartões de crédito; compra e venda de mercadoria e dentre outras. Ao utilizar esses serviços, surgiu a necessidade de conexões seguras por meio de criptografia. Então surgiu o conceito de colocar um soquete no meio de duas camadas para gerar uma conexão segura. As camadas escolhidas foram à camada de aplicação (HTTP) e a camada de transporte (TCP), demonstrada na tabela 2 a seguir.

Com isso a comunicação se torna secreta e as proteções da integridade dos dados se tornam fundamentais. O SSL consiste em dois subprotocolos, um para estabelecer uma conexão segura e outra para usá-la. O funcionamento é muito simples: o navegador realiza solicitações e envia-as ao TCP para transmissão para ser-

vidor. Depois que a conexão segura é estabelecida, a principal tarefa da SSL é manipular a compactação e a criptografia (TANEMBAUM, 2007).

Tabela *2* Camada SSL

Fonte: (TANEMBAUM, 2007).

3.5 PROTOCOLO HTTPS

Acrescentando a camada SSL entre a camada de aplicação e a camada de transporte, aí se denomina HTTPS (*Secure* HTTP), embora seja o protocolo HTTP padrão. Às vezes, ele esta disponível em uma nova porta (443), no lugar da porta padrão (80). A propósito, o SSL não se limita ao uso apenas com navegadores da Internet, mas essa é sua aplicação mais comum (TANEMBAUM, 2007).

Quando realizamos acessos a *sites* mais específicos, no qual necessita de maior segurança, é bom utilizar uma conexão mais segura para que os dados não venham a ser interceptados. Geralmente os bancos, *e-commerce* e dentre outros visam buscar tipos de autenticação para dificultar os acessos indevidos, essa segurança tem por objetivo obter a integridade e confidencialidade das informações (CERT.BR, 2012).

Ao acessar um *site*, alguns requisitos devem ser notados como, por exemplo: observar no início da URL se possui a sigla https:// e logo em seguida a imagem de um cadeado fechado que é visto na URL, ou seja, no endereço do *site*. Também é possível adquirir informações sobre o certificado que esta sendo usado, para que isso aconteça é preciso clicar com o botão direito do mouse em cima do cadeado e

será aberta uma aba chamada conexão, dentro dessa aba é possível ver detalhes do certificado digital que esta sendo utilizado (CERT.BR, 2012).

3.6 SEGURANÇAS EM CONEXÕES

Segundo o Cert.br (2012), quando é realizado um acesso via Internet é muito provável que envolvam o tráfego de informações sigilosas, os acessos geralmente são feitos pelo protocolo HTTP que não possui nenhum tipo de segurança para esses dados, podendo deixar as informações vulneráveis.

O protocolo HTTP não possui criptografia, isso faz com que as informações possam ser capturadas, modificas e usadas de forma inadequada, e também não garante o acesso correto. O HTTP não é indicado para transações bancarias, envio de números de cartões de crédito, *e-commerce* e dentre outros que necessita do sigilo das informações, por isso é recomendado o uso do HTTPS, que fornece uma conexão criptografada usando o SSL. O uso de certificados digitais é muito usado para assegurar a confidencialidade e a integridade dos dados, isso junto com o protocolo HTTPS que fornece uma segurança extra por causa do SSL, que criptografa os dados ao enviar e receber informações sigilosas (CERT.BR, 2012).

Um fator muito importante é ficar atento ao navegar pela Internet, para que não venha cair em armadilhas, para isso é muito importante identificar o uso das conexões, e sempre verificar os alertas expedidos pelo navegador. Os tráfegos de dados sigilosos são muitas das vezes necessários, então todo o cuidado é pouco para não ter o extravio das informações (CERT.BR, 2012).

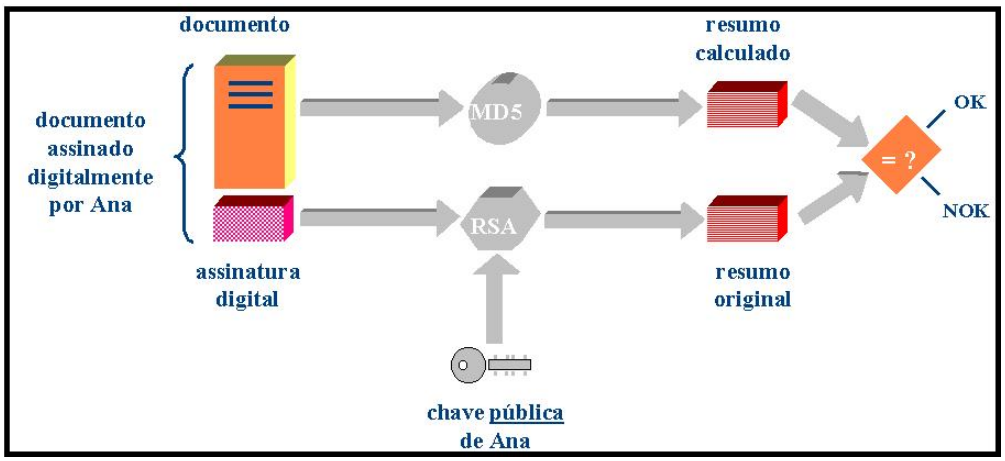
3.7 CERTIFICADOS DIGITAIS

Certificado Digital é muito utilizado na rede mundial de computadores e os principais usos são: Comércios eletrônicos, transferências bancárias, notas fiscais, assinatura de documentos integralmente digital e dentre outros. Nesse caso pode ser usada uma assinatura digital simétrica ou uma assinatura digital assimétrica, a grande diferença é quantidade de chaves a ser usada. Na assinatura simétrica é usada apenas uma única chave tanto para criptografar, como para descriptografar a mensagem, pouco utilizada (MORENO; PEREIRA; CHIARAMONTE, 2005).

A outra mais usada é a criptografia assimétrica, onde cada usuário terá seu par de chaves para criptografar e descriptografar, nesse caso o algoritmo ideal para conseguir tal feito seria o RSA. Ainda assim, teria que ter alguém para gerar as chaves, para que não houvesse o chamado não repudio (MORENO; PEREIRA; CHIARAMONTE, 2005).

Segundo Stallings (2007), no uso de certificado de chave publica é possível criar um canal seguro para transmitir as mensagens, tornando inviável a tentativa de captura e quebra da mensagem enviada, esse canal que é criado utiliza uma função de *hash*, que transmite a mensagem de forma muito rápida, isso pode acelerar o processo, já que se fosse criptografado com algoritmos seria um processo mais demorado. O *hash* envia textos claros em um canal seguro e se por ventura alguém tentar capturar a mensagem, não conseguira obter o texto claro, porque não saberá o *hash* que foi usado para tal codificação, Ilustrado na figura 5 abaixo.

Figura 5-Hash na codificação



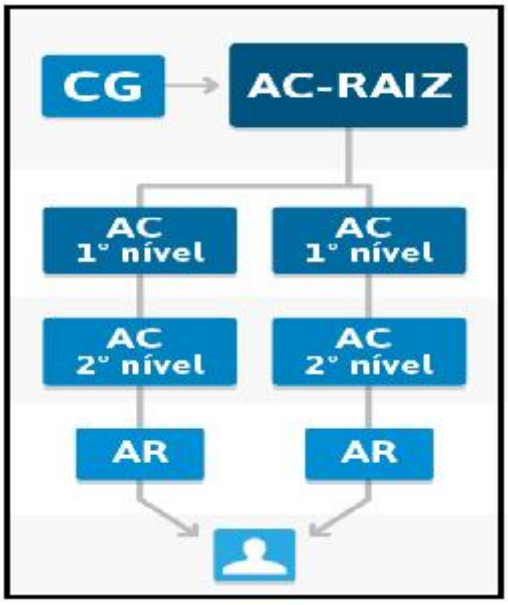
Fonte: (MAIA; PAGLIUSI, ACESSO 10/04/2015).

3.7.1 CERTIFICADOS DIGITAIS ASSINADOS

A certificação Digital é realizada de modo digital e não requer a presença da pessoa física para realizar transações via Internet, os usos são os mais variados: assinar documentos, comércios eletrônicos (*e-commerce),* transações bancárias e dentre outros (ITI, 2015).

Para ser autêntico e seguro os certificados digitais dependem de uma série de requisitos para tais finalidades, por isso foi criada uma infra-estrutura de chave pública Brasileira (ICP-Brasil). A ICP-Brasil foi criada através da Medida Provisória em meados de agosto de 2001, com o intuito de garantir validade jurídica dos documentos eletrônicos, das aplicações de suporte e das aplicações habilitadas que utilizam certificados digitais, com isso conseguindo o principal a “autenticidade, integridade”. O certificado digital possui uma hierarquia, no qual cada entidade é responsável por um processo, para entender esse funcionamento, segue a figura 6 demonstrando toda a estrutura dos certificados. (ITI, 2015).

Figura 6-Hierarquia da ICP-Brasil



Fonte: (VICTORINO; FORTUNATO, 2012).

O Instituto Nacional de Tecnologia da Informação (ITI) juntamente com o Comitê Gestor da ICP-Brasil, são responsáveis pela ICP-Brasil que é a primeira autoridade da estrutura de certificação, ou seja, é a autoridade certificadora Raiz. A ICP-Brasil é o órgão responsável por expedir, emitir, distribuir, revogar e gerenciar os certificados, também compete a ela emitir a lista de certificados revogados e também auditar e fiscalizar as autoridades de níveis mais baixos, outro trabalho da ICP-Brasil é executar políticas de certificados e normas técnicas aprovadas pelo comitê gestor (MACHADO, 2010).

Essas autoridades podem ser públicas ou privadas e a ICP-Brasil é quem verifica se a chave pública corresponde com a chave privada, ela tem o dever de analisar se os registros estão ligados a uma Autoridade Certificadora (AC). Que por sinal tem como função o recebimento, a validação, a emissão e revogação do certificado digital Autoridade Responsáveis (AR). Na ordem cronológica em primeiro lugar vem a ICP-Brasil como a autoridade certificadora raiz, seguida pela certificadora de primeiro nível, depois as autoridades certificadoras de segundo nível, o próximo órgão é a Autoridade Responsável (AR) que é responsável pelo gerenciamento dos certificados digitais (MACHADO, 2010).

A ICP-Brasil desenvolve diversos documentos e normas a serem seguidos por todos que fazem parte da estrutura ICP-Brasil, tudo isso visando aumentar a segurança e obter maior credibilidade em seus serviços (ITI, 2015).

3.7.2 NÍVEIS DOS CERTIFICADOS

Segundo Machado (2010), as entidades certificadoras de primeiro nível podem emitir certificados para “AC” de segundo nível e também podem emitir certificados para o público final. Já no caso das certificadoras “AR”, essas apenas gerenciam o público final e trabalham também à parte física da estrutura através de dispositivos como *tokens,* chaves, e certificando a validade do certificado.

A obtenção de um certificado digital é muito simples e pode ser adquirida por pessoas físicas ou jurídicas, através de uma entidade certificadora. Os tipos de certificados são os mais variados, depende de cada caso: o certificado A1 é um certificado que fica no próprio computador e é válido por um ano, depois desse prazo é necessário fazer a compra de um novo certificado. O certificado A3 possui validade de até cinco anos e é preciso o uso de um cartão e um token para emitir o certificado, demonstrado a seguir na figura 7. Além desses, também tem o certificado T3 e também o certificado S3 que possui o mesmo prazo de validade do A3, que é de cinco anos (MACHADO, 2010).

Já segundo Victorino e Fortunato (2012), o certificado A4 e S4 que possui uma chave com tamanho de 4096 bits (quatro mil e noventa e seis) e possui duração de seis anos de validade. A pessoa física ou pessoa jurídica interessada se dirige até uma autoridade certificadora, realiza um cadastro com sua documentação e depois escolhe o tipo de certificado ideal para satisfazer a sua necessidade.

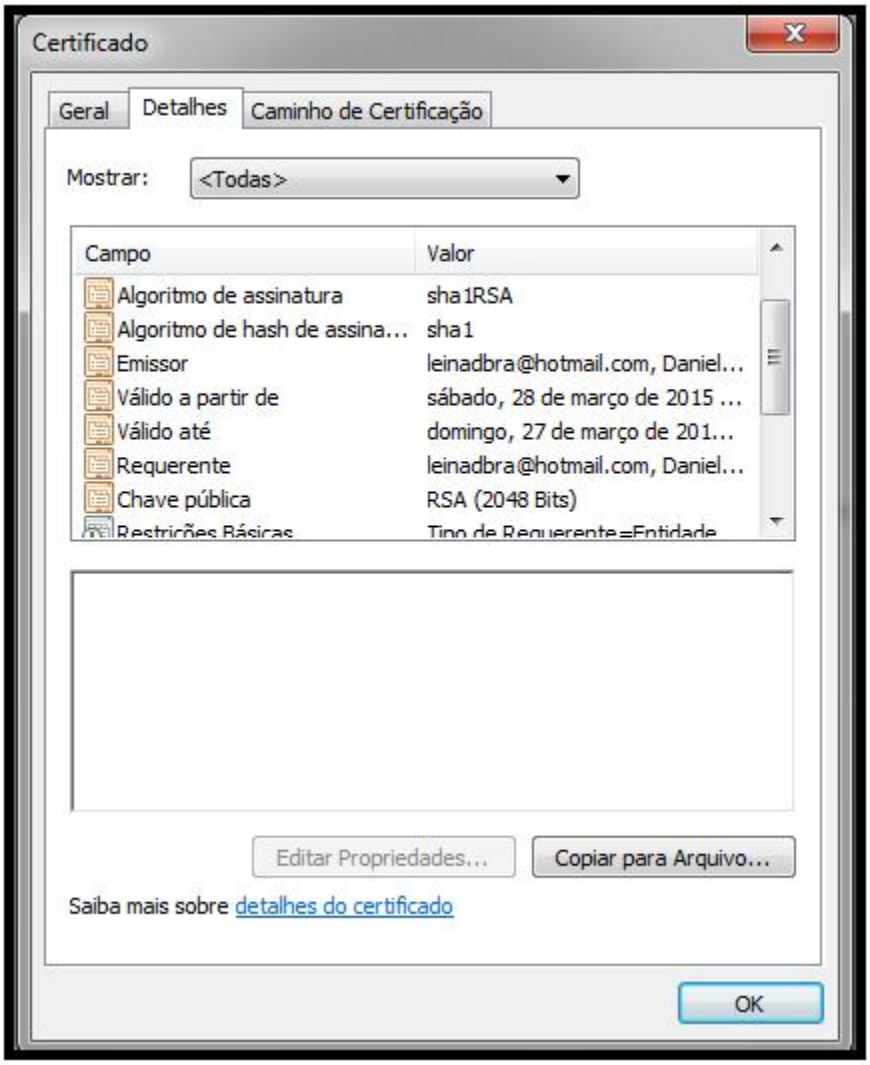
Caso o usuário tenha alguma dúvida no momento da instalação ou caso haja algum erro no certificado, a própria certificadora fornece suporte técnico e ajuda para os usuários (ITI, 2015).

Figura 7-Token para certificados

Fonte: (ITI, 27/03/2015).

Os Certificados Digitais Assinados tem como componentes os seguintes dados: Nome da pessoa ou entidade a ser associados à chave pública, período de validade do certificado, chave pública, nome e assinatura da entidade que assinou o certificado e o número de série (MACHADO, 2010).

Figura 8-Detalhes do Certificado Digital



Fonte: (PRÓPRIO AUTOR).

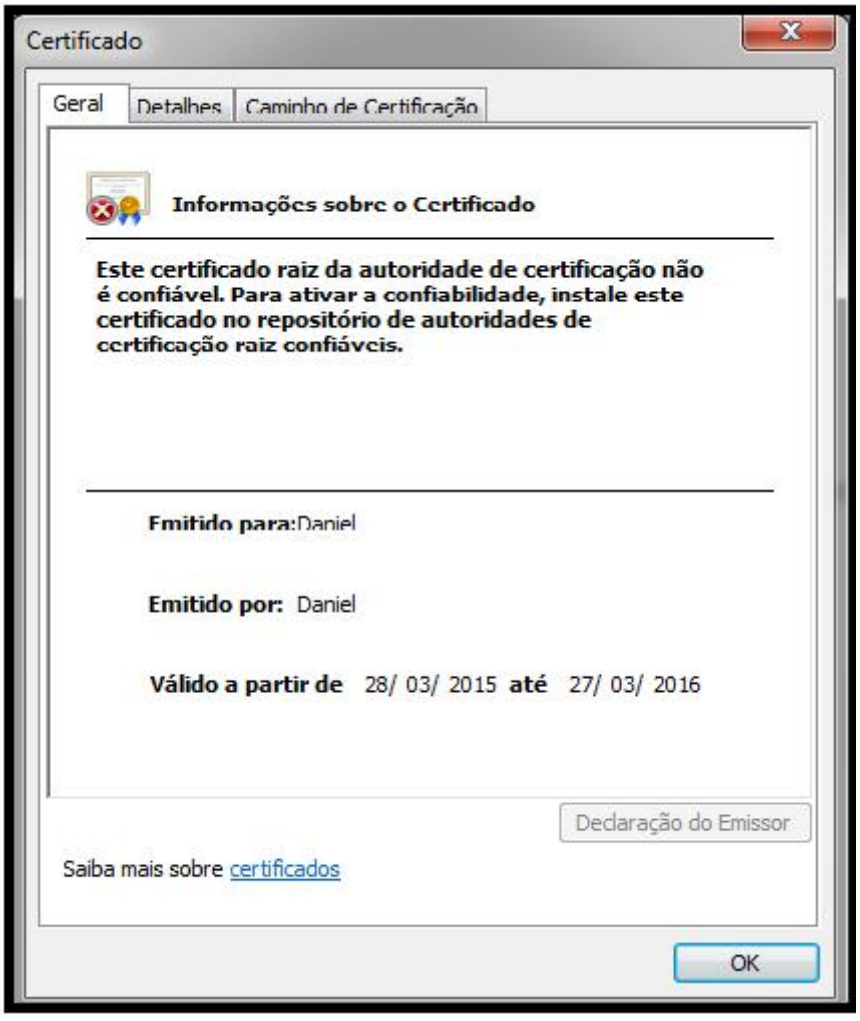
3.7.3 CERTIFICADOS DIGITAIS AUTO-ASSINADOS

Segundo Machado (2010), para obter um certificado digital auto-assinado não é preciso ter uma certificadora, porque a própria pessoa pode desenvolver um certificado, assinar e emitir o certificado por ela mesma.

Para observar que tipo de certificado esta em uso, podemos verificar quando abrimos o navegador com o protocolo HTTPS em um determinado *site*, realizamos os seguintes passos: esperamos o site carregar completamente, depois vai até a barra de endereços e clicamos com o botão direito do mouse no cadeado, feito isso, irá abrir uma aba chamada conexões, nessa barra irá conter informações e o padrão

do certificado que está sendo utilizado. São diversas as informações: validade do certificado, tipos de restrições, impressão digital, número de série do certificado, identificador da chave, versão do certificado, Algoritmo de *hash* usado (*sha*1), tipo de chave usada (pública RSA de 2048 bits) entre outras informações ilustradas na figura 8, também é possível verificar a data de validade do certificado como mostra a figura 9 (MACHADO, 2010).

Figura 9-Dono do Certificado Digital

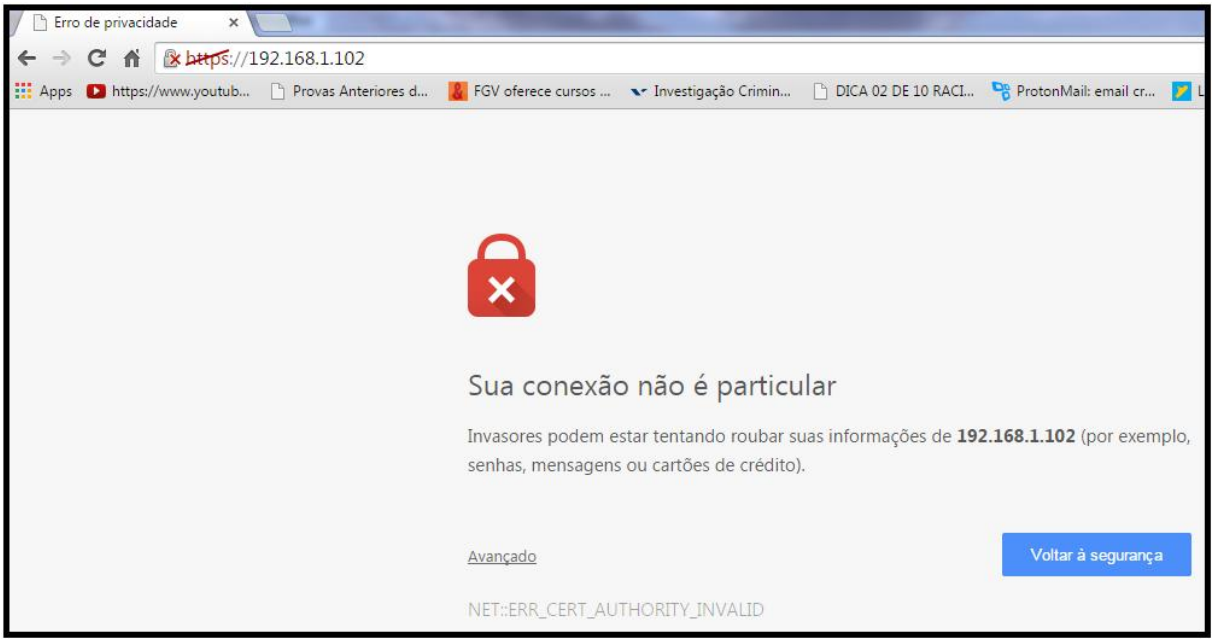


Fonte: (PRÓPRIO AUTOR).

Quando se utiliza o certificado auto-assinado surge um aviso na tela dizendo que o site pode não ser confiável, deseja continuar mesmo assim? Para acessar é necessário clicar em “continuar mesmo assim”, para então, abrir uma exceção de acesso ao *site* (MACHADO, 2010).

Assim entende-se que muitas vezes o site que não possui uma autoridade certificadora e que pretendem utilizar uma conexão segura de alguma maneira poderá levar alguns usuários a terem certos receios de continuar com a conexão. Isso é muito comum quando o usuário não tem conhecimento sobre a certificação ou por não conhecer o *site*. A figura 10 ilustra a mensagem que será exibida na tela caso não haja uma autoridade certificadora para aquele *site* (ITI, 2015).

Figura 10-Gerando exceções



Fonte: (PRÓPRIO AUTOR).

Ao abrir uma exceção, o usuário poderá também abrir uma vulnerabilidade, não é aconselhável esse tipo de certificado, o ideal é que o usuário compre um certificado emitido por uma entidade certificadora (MACHADO, 2010).

4 SEGURANÇA DE CORREIO ELETRÔNICO

Quando uma mensagem de correio eletrônico é enviada entre dois *sites* distantes, geralmente ela transita por milhares de dispositivos até chegar a seu destino. Qualquer um desses dispositivos pode ler e armazenar a mensagem para usá-la posteriormente. Na prática, não há privacidade, apesar de muita gente achar o contrario. Todavia, muitas pessoas gostariam de enviar mensagens de correio eletrônico para que fossem lidas pelos destinatários pretendidos e por ninguém mais: (nem seu chefe, nem o governo, nem administrador, nem a NSA e nem outros). Esse desejo estimulou muitas pessoas e grupos a aplicarem os princípios da criptografia que estudamos anteriormente para produzir mensagens seguras (STALLINGS, 2008).

4.1 PGP — PRETTY GOOD PRIVACY

O PGP é muito fácil de ser usado, além disso, é o pacote mais completo para mensagens de correio eletrônico, ele fornece privacidade, assinaturas digitais, autenticação e compactação de maneira muito simples. O pacote completo do PGP inclui o código fonte, que é distribuída via *download* pela Internet. O PGP é extensamente usado nos dias de hoje, por ter uma ótima qualidade, por ser grátis e disponibilidade em diversas plataformas como *Windows*, *Linux*, *Unix* e *Mac Os* (TANENBAUM, 2007).

O PGP codifica os dados usando o sistema IDEA que utiliza chaves de 128 bits. O sistema de criptografia IDEA foi desenvolvido na suíça na época em que o AES se encontrava numa decadência e o DES ainda não tinha surgido. O sistema IDEA é igual ao DES e ao AES, onde se mistura bits em uma série de rodadas, mas as funções de mixagem são diferentes do DES e do AES. O gerenciamento de chaves utiliza o RSA e a integridade de dados usa o sistema *hash* MD5. O PGP permite três tamanhos de chaves RSA e isso permite ao usuário selecionar o mais apropriado:

1. Casual (384 bits): pode ser decifrado com facilidade atualmente;

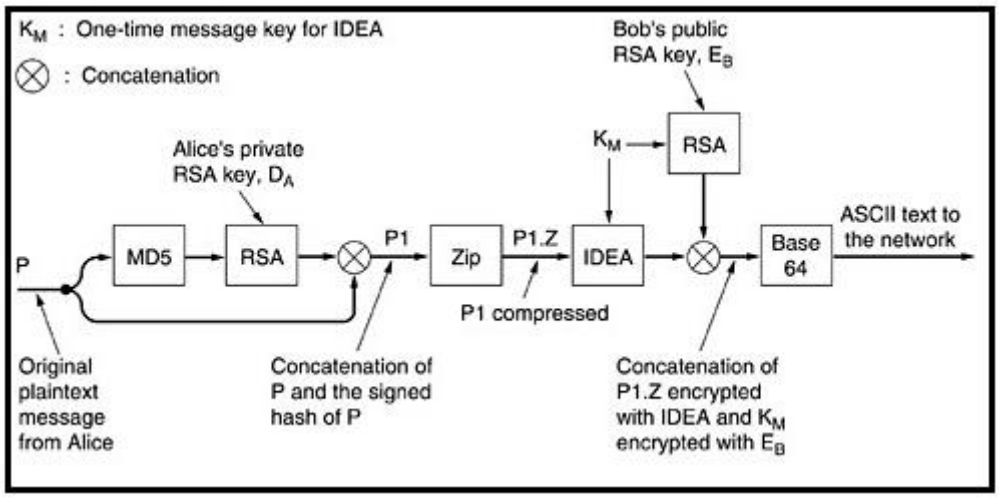
2. Comercial (512 bits): pode ser decifrado por empresas de informática;

3. Militar (1024 bits): ninguém no planeta consegue decifrar;

4. Alienígena (2.048 bits): não pode ser decifrado por ninguém de outros planetas (TANEMBAUM, 2007).

O PGP é muito parecido com um processador que recebe texto simples como entrada e produz texto cifrado assinado em base64 como saída. Essa saída pode então ser enviada por correio eletrônico. Algumas efetivações do PGP chamam um usuário na etapa final para enviar de fato a mensagem. O PGP aceita a compactação de textos, assinaturas digitais, sigilo e também oferece amplos recursos de gerenciamento de chaves, mas estranhamente, é pouco usado como correio eletrônico (TANEMBAUM, 2007).

Figura 11-PGP em Operação



Fonte: (TANEMBAUM, 2007).

Estrutura do funcionamento do PGP demonstrado na figura 11, Alice começa invocando o programa PGP em seu computador. Primeiro, o PGP submete sua mensagem P a um processo de *hash*, utilizando o MD5; em seguida, criptografa o resultado empregando sua chave privada RSA. Quando recebe a mensagem, Bob poderá descriptografar o *hash* com a chave publica de Alice e confirmar que o *hash* está correto. Mesmo que alguma outra pessoa (por exemplo, Trudy) pudesse adquirir o *hash* nesse estágio e descriptografa-lo com a chave publica de Alice, a robustez

do MD5 garante que seria inviável em termos computacionais produzir outra mensagem com o mesmo *hash* MD5 (TANEMBAUM, 2007).

4.2 PROTONMAIL

Mesmo a criptografia existindo há vários anos, muitas pessoas não se preocupavam com o conteúdo que trafegava pela rede mundial de computadores, até que surgiu o analista da NSA, “Edward Snowden” revelando informações sigilosas de que a NSA espionava o mundo através da Internet, por meio de e-mails. Desde que Edward Snowden revelou os procedimentos da NSA, a preocupação foi geral por parte dos usuários. Foi aí que surgiu uma pequena equipe de desenvolvedores com membros na MIT (Instituto de Tecnologia de Massachusetts), e do CERN (Organização Européia para Pesquisa Nuclear) de Harvard e projetaram o Protonmail (HENRIQUE, 2015).

Em 2013 na Suíça onde as leis de privacidades são mais fortes, foi onde iniciou o projeto Protonmail, com a promessa de que os usuários estariam 100% anônimos, e de que o seu IP não seria rastreado e que nenhum log de Dados do Protonmail seria registrado, e também outro ponto importante é que a criptografia seria feita no próprio computador da pessoa e não no servidor igual a Google faz. O Gmail da Google mantém todas as informações em servidores e verifica as informações dos e-mails e usa os dados, alimentando os seus anúncios. Para usar o Protonmail é preciso se cadastrar de forma gratuita, o sistema permite o uso de 100 *Mega Bytes* de armazenamento que dá pra armazenar 500 mensagens por mês (HENRIQUE, 2015).

Atualmente os servidores do Protonmail se encontram na Suíça por questões extras de segurança, o que irá aumentar a privacidade, evitando assim que os Estados Unidos da América (EUA) possam desligar os servidores a força. Muito semelhante ao Gmail da Google, se o usuário não possuir um *login* e senha, é realizado um cadastro para que a pessoa possa utilizar o gerenciador de e-mail. Além de possuir uma interface muito simples, não é necessário instalar nenhum *software* em seu computador, como mostra a figura 12 (HENRIQUE, 2015).

Figura 12-Tela de login Protonmail

Fonte: (HENRIQUE, ACESSO 2015).

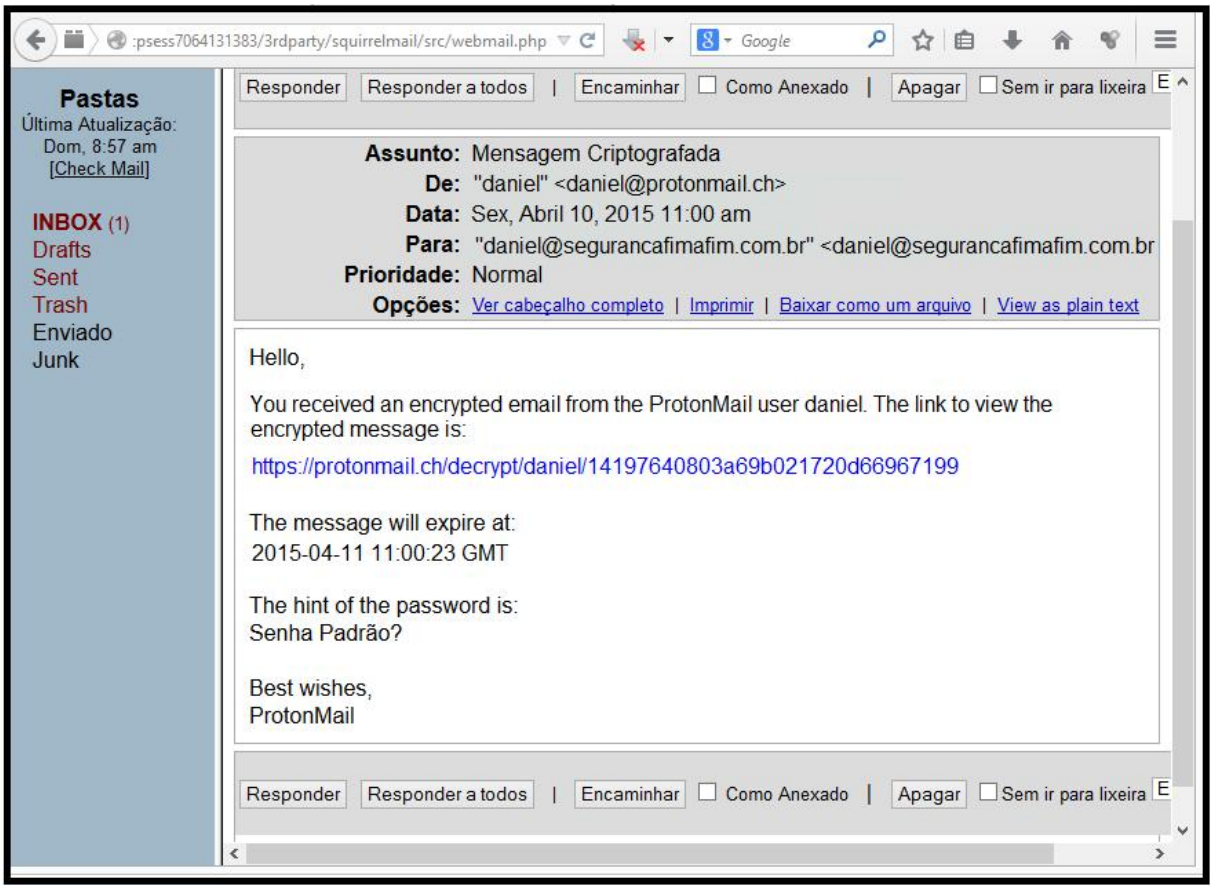
Nesse ponto se encontra o corpo da mensagem, onde pode se escrever a mensagem a ser enviada, também possui algumas opções como *expiration* onde define o tempo em que a mensagem vai existir. Depois do período estipulado, a mensagem será excluída automaticamente. Também possui *encrypt for outside* (criptografar para fora), no qual define a senha usada para visualizar a mensagem, além disso, é possível colocar uma dica, ou seja, um lembrete de senha, a figura 13 realiza essa demonstração (HENRIQUE, 2015).

Figura 13-Tela corpo da mensagem Protonmail

Fonte: (HENRIQUE, 2015).

Recebida a mensagem, virá junto um *link* para acessar o email criptografado, e junto com ele vem à dica, ou seja, o lembrete de senha. Então é só clicar no *link* e o usuário será direcionado para digitar o *login* e a senha, se por ventura não lembrar a senha terá a dica para ajudar, ilustrada na figura 14 (HENRIQUE, 2015).

Figura 14-Tela recebendo código criptografado Protonmail



Fonte: (HENRIQUE, 2015).

Para finalizar, o último passo é digitar a senha e ver a mensagem descodificada demonstrada a seguir na figura 15 (HENRIQUE, 2015).

Figura 15-Decriptação da mensagem Protonmail

Fonte: (HENRIQUE, 2015).

5 ESTUDO DE CASO

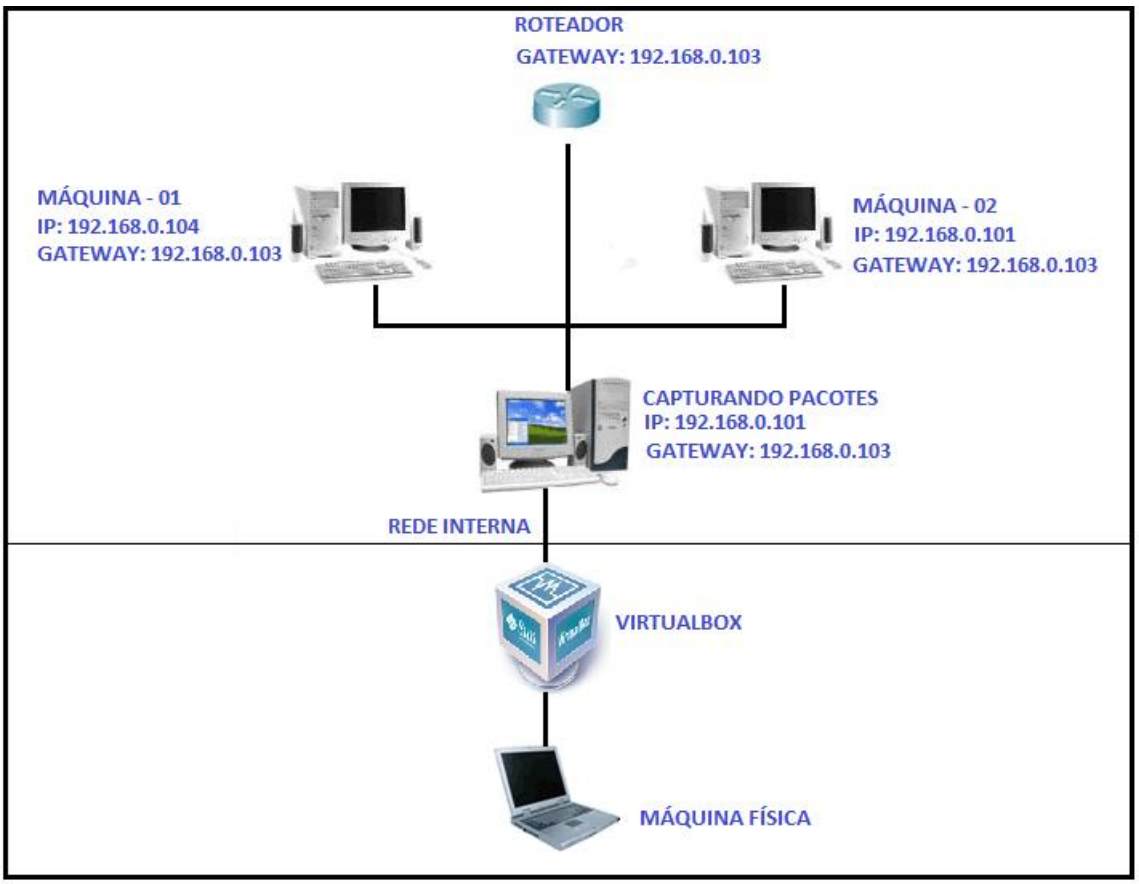
Este estudo de caso tem o objetivo de criar um ambiente no qual foi possível visualizar dois servidores em ambiente virtual com apache ativo, realizando tarefas e podendo colher resultados do protocolo HTTP e HTTP *secure*, demonstrando como é possível a obtenção dados, isso ilustrado na figura 16. No primeiro teste realizado com o protocolo HTTP é possível visualizar as informações trafegando em forma de texto claro, podendo então visualizar, capturar e usar essas informações para um suposto ataque.

O segundo teste foi realizado com o protocolo HTTP *secure* que possui um *Socket* que fica entre a camada de aplicação e a camada de transporte, o que cria uma espécie de túnel para a comunicação, e faz com que o protocolo se torne um pouco mais seguro, mas esse túnel pode ser quebrado através de *softwares* específicos fazendo com que a informações venham ser capturadas e usadas para fins ilícitos.

Sendo assim um terceiro teste foi realizado usando o servidor de e-mail Protonmail, que possui um método de criptografar a mensagem antes de enviá-la. O Protonmail utiliza o protocolo HTTP *secure,* o que aumenta significativamente a segurança, dificultando então um suposto roubo das informações.

Todos os testes foram realizados dentro de máquinas virtuais, no qual o escolhido foi o *Virtual Box da Oracle*, também foi usado os softwares *Wireshark* e *Cain & Abel* para a captura dos pacotes e para a visualização e obtenção dos resultados.

Figura 16-Estudo de caso

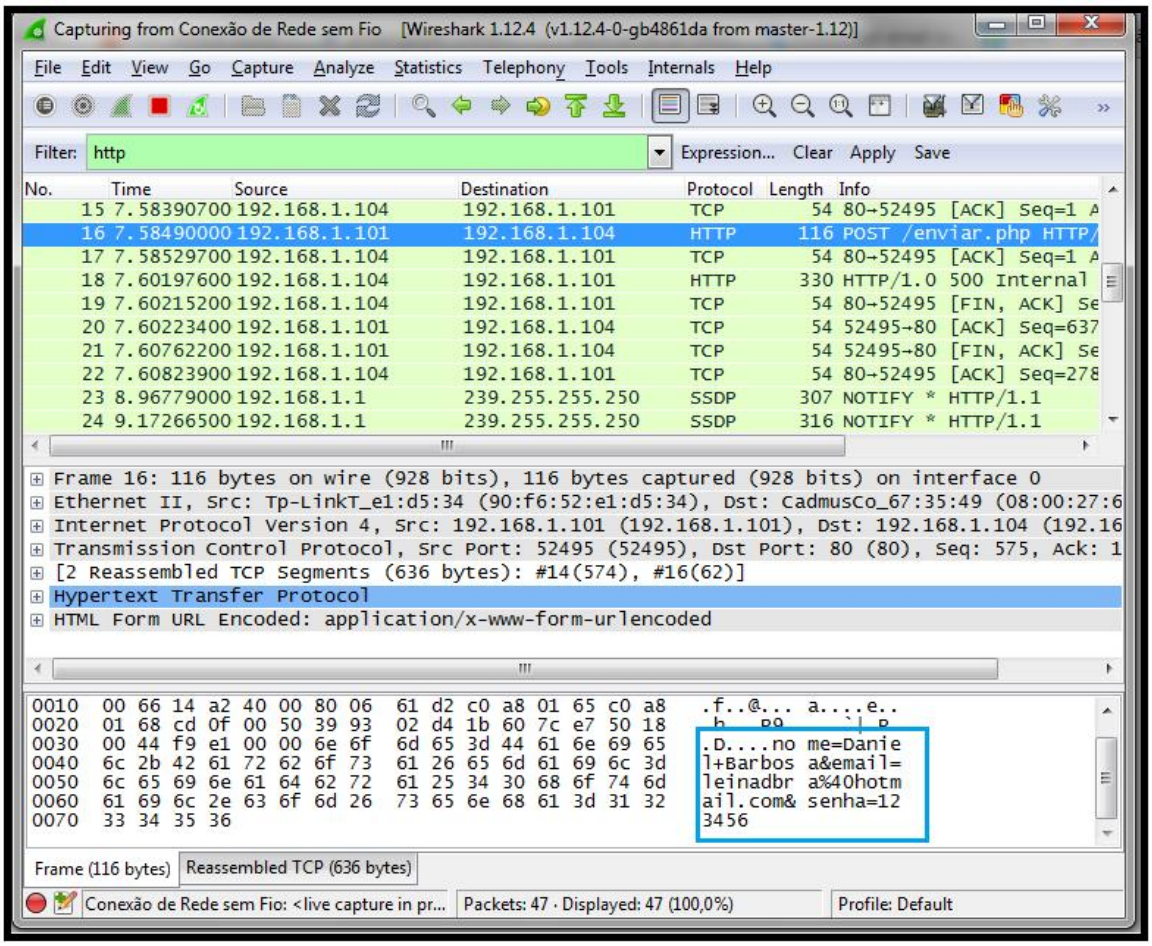


Fonte: (PRÓPRIO AUTOR).

5.1 COLETAS DADOS HTTP

Ao realizar testes com o protocolo HTTP, foi verificado que as informações estarão sujeitas a ficarem expostas de maneira muito clara. Se observarmos a figura 17 a seguir, percebemos nitidamente que a ferramenta de captura de pacotes *Wireshark* capturou alguns dados como o nome, email e até mesmo a senha do usuário. Isso demonstra toda a fragilidade do protocolo HTTP em suas configurações originais. O HTTP não é recomendado em algumas ocasiões como: transações bancárias, sites de comércio eletrônicos e dentre outros, pelo simples fato do protocolo HTTP não fornecer nenhum sistema de segurança.

Figura 17-Captura do Protocolo HTTP



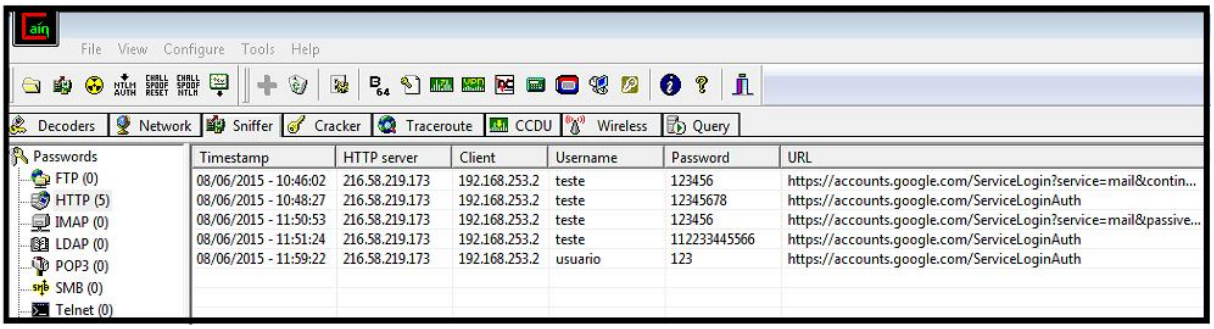
Fonte: (PRÓPRIO AUTOR).

5.2 COLETAS DADOS HTTPS

Já no caso do protocolo no modo HTTP *secure* que utiliza o SSL, ou seja, um túnel para trafegar informações pela rede, o processo de captura dos dados se torna mais trabalhoso, tem que ser alguém experiente no assunto para quebrar o túnel e obter a captura de dados.

Este tipo de aplicação é muito usado em comercio eletrônico como: *e-commerce*, transações bancárias, para enviar e receber emails dentre outros. Ao Analisar veremos que as informações como: nome, email e senha também ficaram expostos mesmo usando o SSL, demonstrado na figura 18.

Figura 18-Captura do Protocolo HTTPS

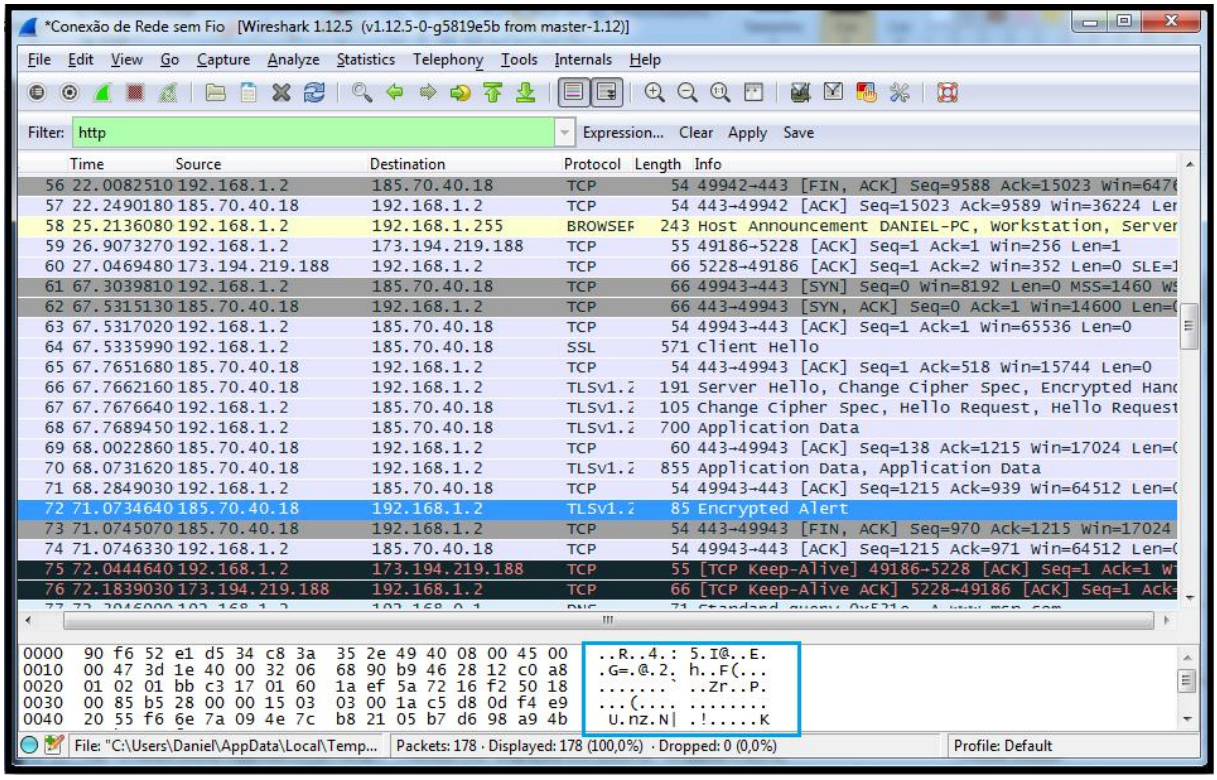


Fonte: (PRÓPRIO AUTOR).

5.3 COLETA DE DADOS CRIPTOGRAFADO

A seguir foi aplicada a captura de dados em um sistema de mensagem criptografada, usando o sistema Protonmail para o envio e recebimento de informações, no qual resulta em uma captura criptografada dos dados como segue na figura 19.

Figura 19- Coleta de Dados Criptografados



Fonte: (PRÓPRIO AUTOR).

5.4 CONCLUSÃO DO ESTUDO DE CASO

Primeiramente realizei testes com o protocolo HTTP e pude observar que o mesmo não possui nenhuma segurança, ou seja, as informações podem ser capturadas de forma muito fácil. O segundo teste que realizei foi com o HTTP *secure* e por existir uma criptografia SSL entre as camadas de aplicação e de transporte, isso dificultou um pouco mais a captura das informações. Mas mesmo assim foi possível romper o chamado túnel SSL e obter as informações.

E por fim, foram realizados testes com o servidor de e-mail Protonmail que por sua vez criptografa as informações no computador do usuário, o IP do usuário não é registrado e nenhum log de dados fica armazenado, além disso, também utiliza o protocolo HTTP *secure,* que garante uma segurança extra no envio e recebimento de dados.

Para finalizar cheguei à conclusão que o Protonmail é sem dúvida um sistema muito seguro que pode garantir a integridade, confidencialidade, e o não repudio das informações. E sem sombra de dúvidas uma inovação, para o sistema de envio e recebimento de e-mails. Os pacotes foram capturados pelos softwares, porém os dados estavam criptografados, o que frustrou um suposto ataque, diminuindo assim, a perda das informações, garantindo para os usuários a privacidade das informações.

6 CONSIDERAÇÕES FINAIS.

Esta monografia acrescentou em meus conhecimentos vários quesitos, por que abordaram diversos temas como: criptografia, certificado digital, segurança em correio eletrônico e dentre outros.

A evolução da tecnologia é muito rápida e com isso é necessário alguns cuidados com esses avanços, um desses avanços é a criptografia que se faz presente em vários lugares, como no envio e recebimento de informações de forma confidencial. Existem dois tipos distintos de criptografia; a criptografia simétrica que é uma técnica de transposição e substituição e a criptografia assimétrica que utilizam de cálculos matemáticos.

A criptografia fornece aos usuários uma forma segura de poder realizar uma compra on-line, acessar contas bancárias, comprar e vender pela Internet e dentre outras funções, isso pode ser usado tanto por um usuário leigo no assunto como também por especialistas e grandes corporações. Muitas pessoas têm certos receios na hora de realizar transações pela Internet, o medo é que seus dados sejam roubados, clonados ou usados de forma que venha trazer prejuízos materiais e morais.

Para que isso não venha ocorrer, os certificados digitais vêm garantindo aos usuários a autenticidade e o sigilo das informações que trafegam pela Internet, os certificados digitais criam um canal seguro entre o remetente e o destinatário, fazendo com que as informações possam transitar de forma segura, evitando então que as informações venham cair em mãos erradas.

Este estudo de caso vem demonstrando todo o funcionamento do protocolo HTTP e HTTP *secure*, criptografia e também do certificado digital. No protocolo HTTP as informações trafegam sem segurança, já no protocolo HTTPS é um pouco mais seguro por conter uma criptografia entre as camadas de aplicação e a camada de transporte, isso faz com que crie um túnel criptografado. Também foi criado um certificado auto-assinado, sem a utilização de uma entidade certificadora, junto com o uso do HTTPS. Para simular um aumento da segurança.

O roubo das informações é possível dentre outras maneiras pela técnica de *fishing,* onde o atacante simula um ambiente seguro para que consiga capturar as

informações dos usuários sem conhecimento do mesmo. Por isso o uso de uma entidade certificadora é essencial para que isso não venha a ocorrer.

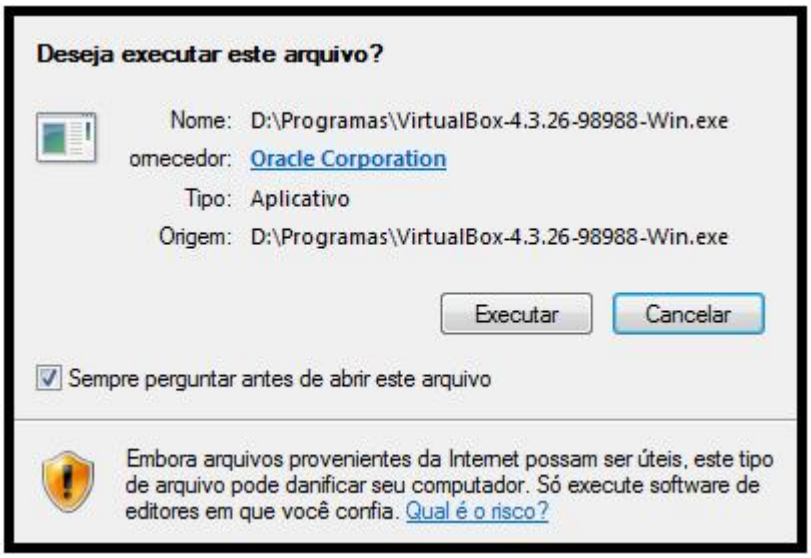
Ao fazer uso da Internet é de suma importância que o usuário tenha no mínimo um conhecimento básico, de como usar a Internet de forma segura. É importante conhecer as formas de ataques, quais os dados que podem ser roubados, que tipos de ferramentas utilizarem para se defender de um suposto ataque, quais são as vulnerabilidades dentre outros. Muitas das vezes as pessoas têm suas informações extraviadas por não saberem de que forma se comportar ao usar a rede mundial de computadores.

Por fim, o estudo de caso apresenta o Protonmail com envio de dados criptografados junto com o protocolo HTTP *secure* e o conteúdo da própria mensagem também criptografado. Mesmo que o atacante venha quebrar a criptografia do protocolo SSL, ou seja, quebrar o túnel, ele terá outra dificuldade, que é quebrar a mensagem criptografada, isso aumenta, e muito, a segurança principalmente no envio de mensagens eletrônicas, como email. O servidor de email, Protonmail trás esse tipo de criptografia, no qual dificulta muito que as mensagens sejam bisbilhotadas por entidades ou pessoas não autorizadas. Essas são medidas de segurança para o envio de dados criptografados juntamente com o protocolo HTTP *secure*.

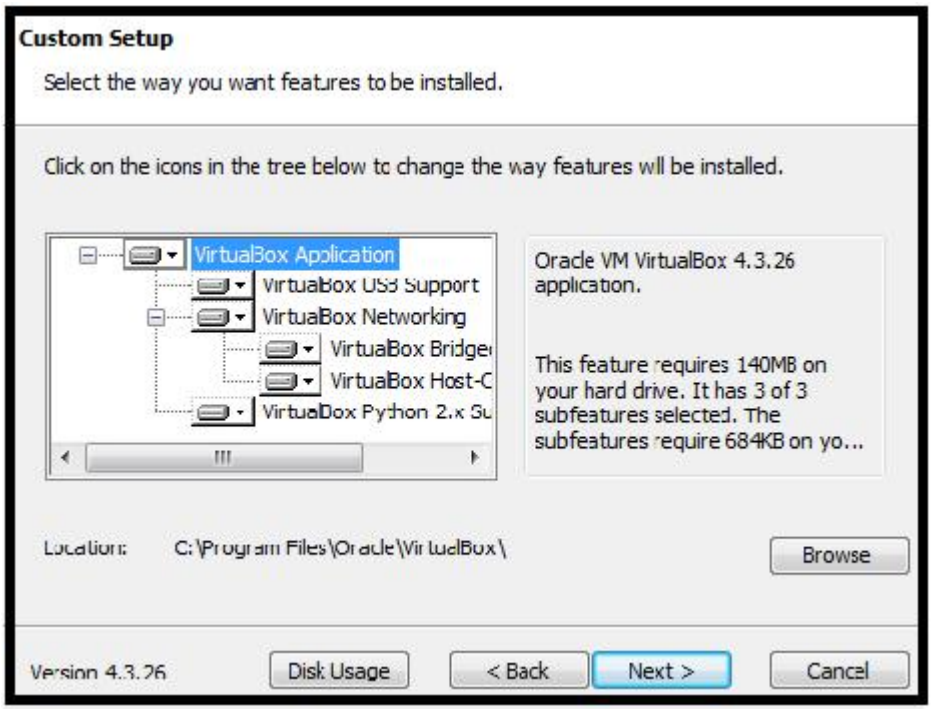
Mesmo assim algumas perguntas ainda são visíveis, usando essas ferramentas o ambiente estará totalmente seguro? É uma pergunta difícil de responder, pelo simples fato da tecnologia evoluir a todo instante. Por isso a cada dia devemos buscar soluções novas e acompanhar a evolução da tecnologia constantemente.

ANEXOS A – Configurações

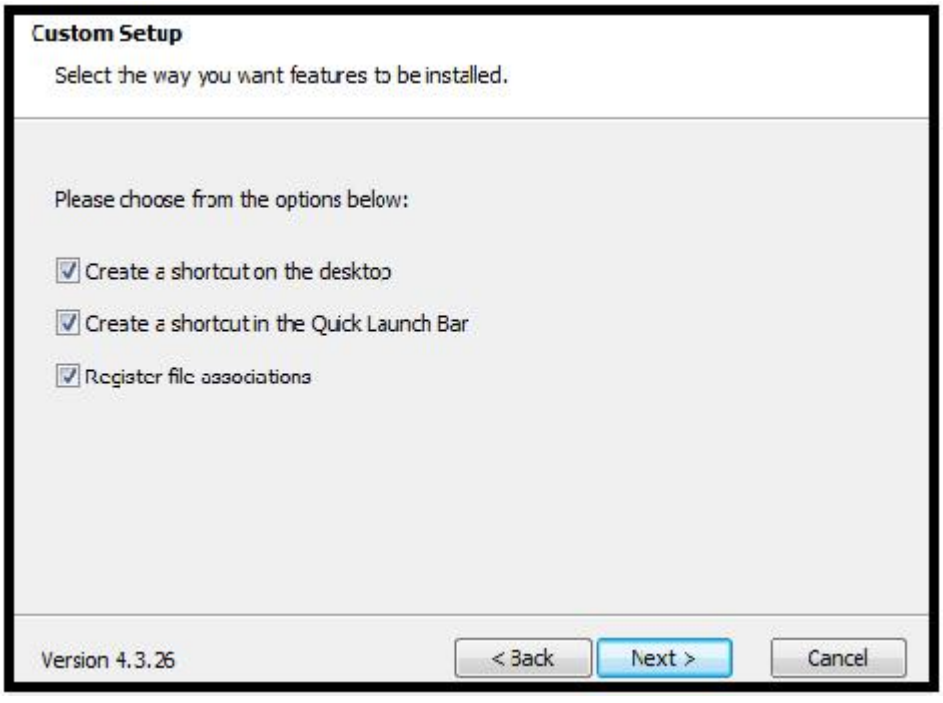
Primeiramente realizei o acesso ao *site* da *Oracle* e fiz o download do software Virtual Box pelo *link*: https://www.oracle.com/downloads/index.html. Logo em seguida cliquei em Executar. Para esse experimento realizei a instalação padrão do Virtual Box.



Cliquei em *next*.

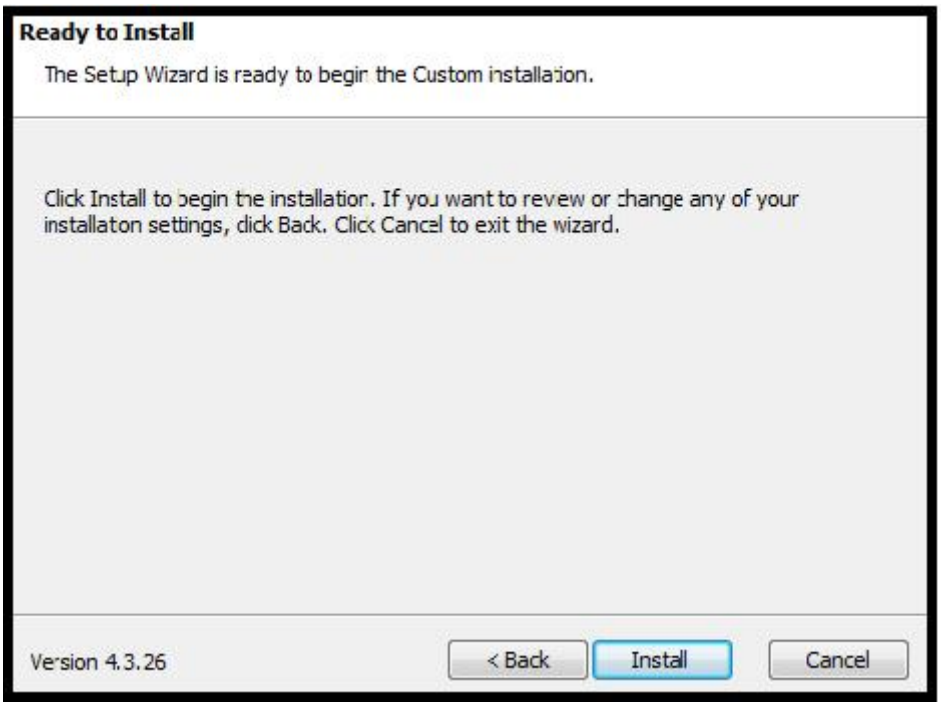


Cliquei em *next* novamente.

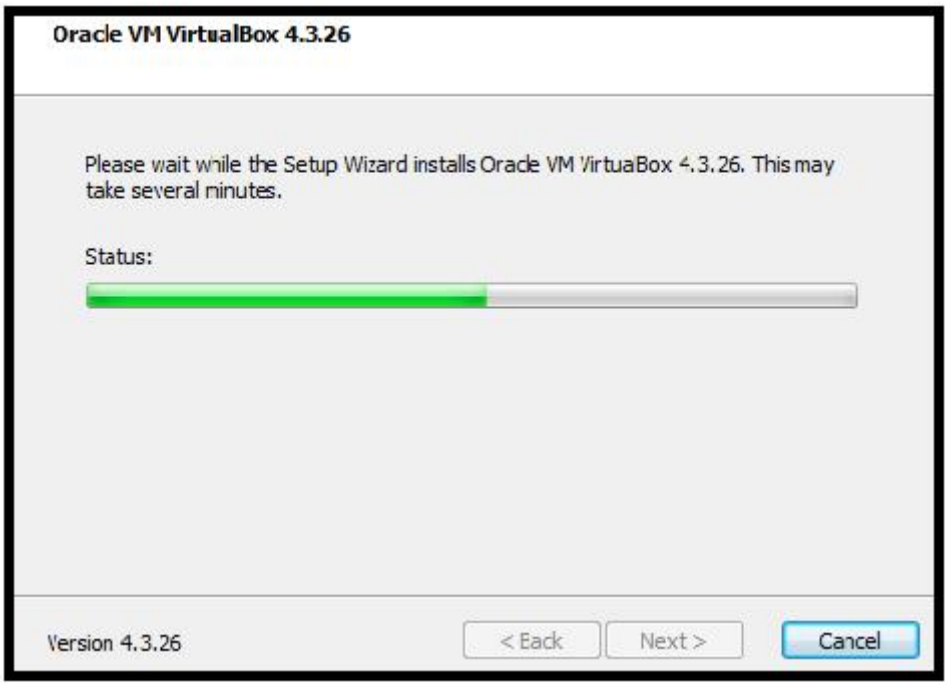


Novamente em *next*.

Nesse ponto surge um aviso que a placa de rede será desconectada, cliquei em *Yes*, ou seja, sim.



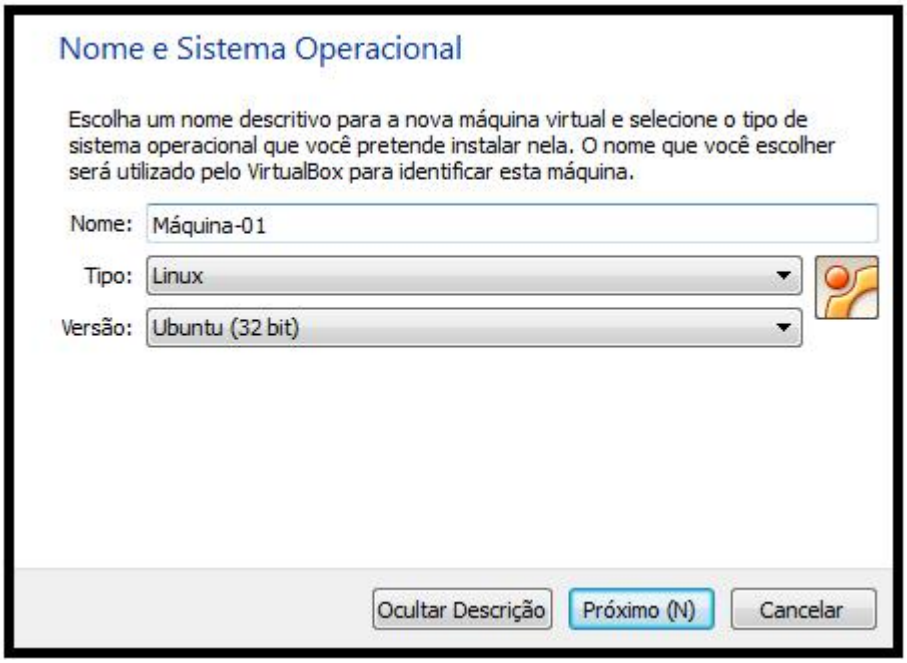
Para finalizar cliquei em *install*, que é instalar.



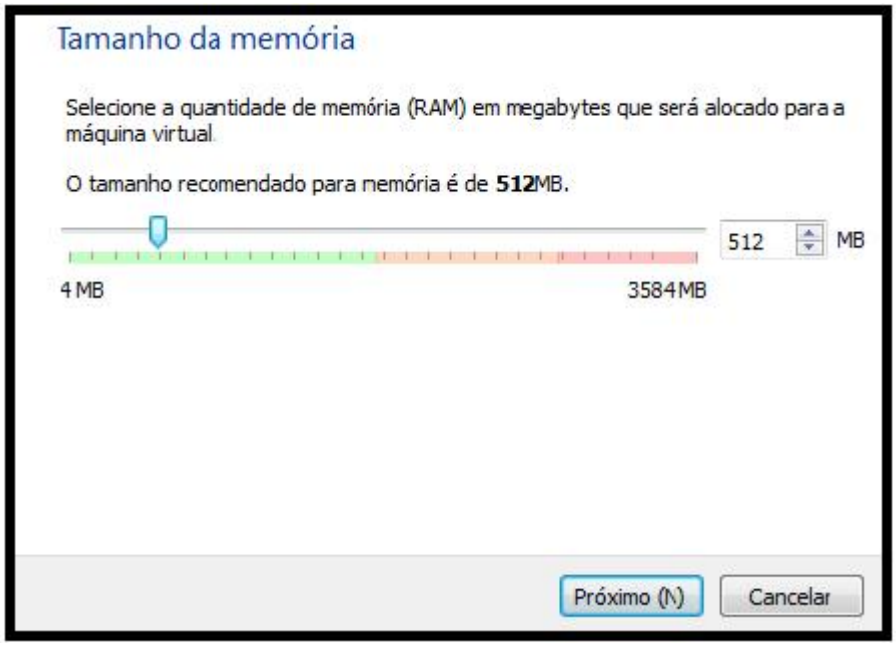
Aguardando instalação.

Cliquei em *Finish* para Finalizar a instalação.

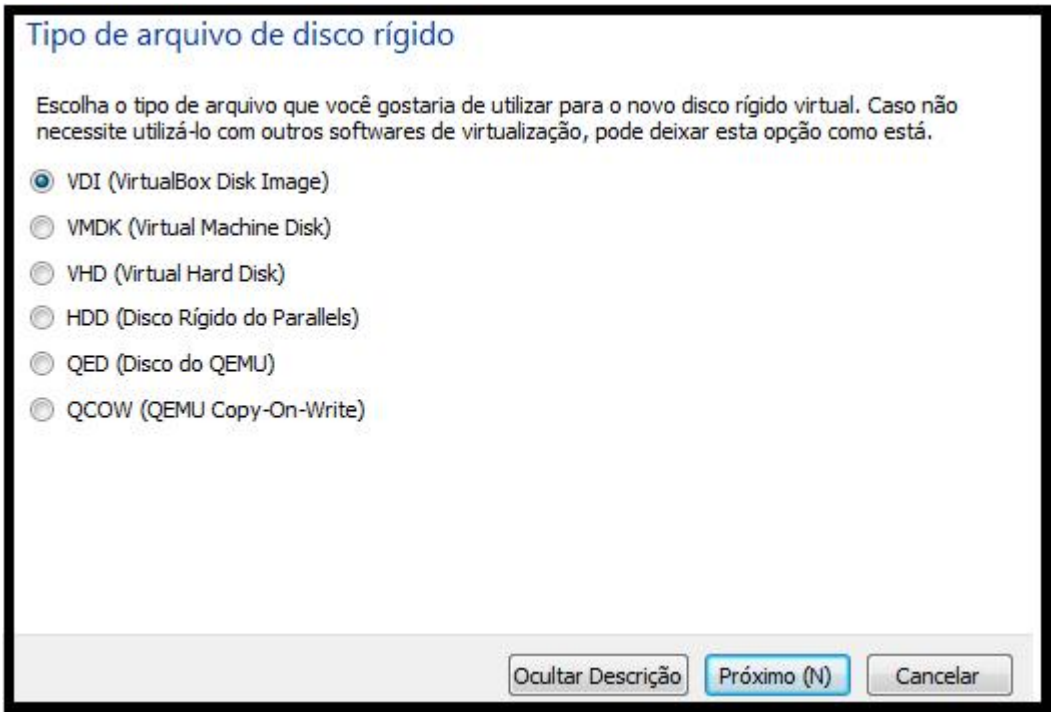
Nesse ponto cliquei em novo para criar uma máquina virtual. O próximo passo foi escolher um nome para a máquina, tipo da máquina no caso Linux, e a versão foi *Ubuntu* (32bit).



Esse ponto é usado para fazer a alocação de memória para a máquina virtual, nesse caso foi utilizado 512MB memória.



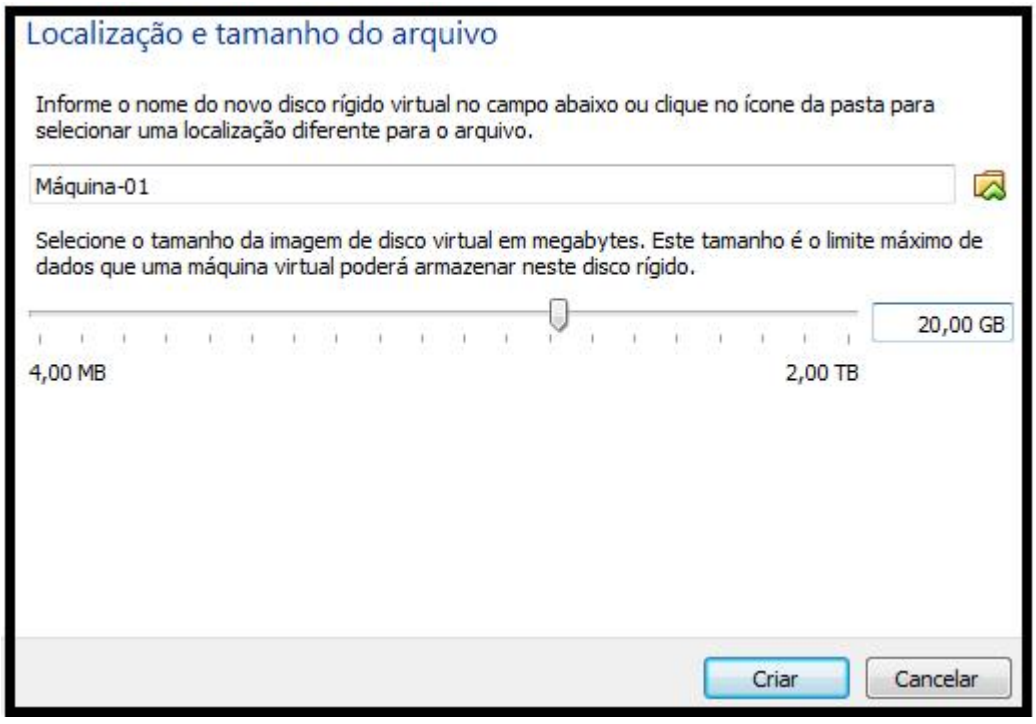
Deixei por padrão o tipo de disco *Virtualbox Disk Image* (VDI) e cliquei em próximo.



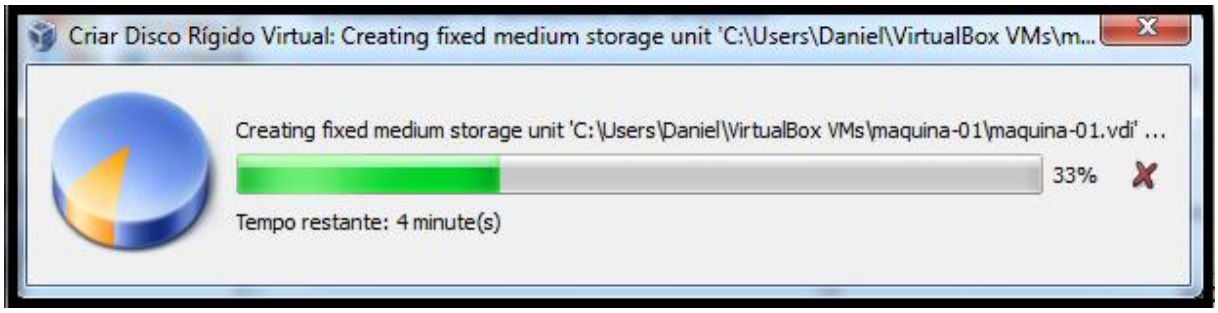
Outro passo importante é escolher o tipo de disco a ser usado, deixei por padrão criar um disco rígido virtual agora e cliquei em criar.

Nesse ponto utilizei o tamanho fixo para armazenamento, cliquei em próximo.

Selecionei 20 GB de disco rígido e cliquei em criar.

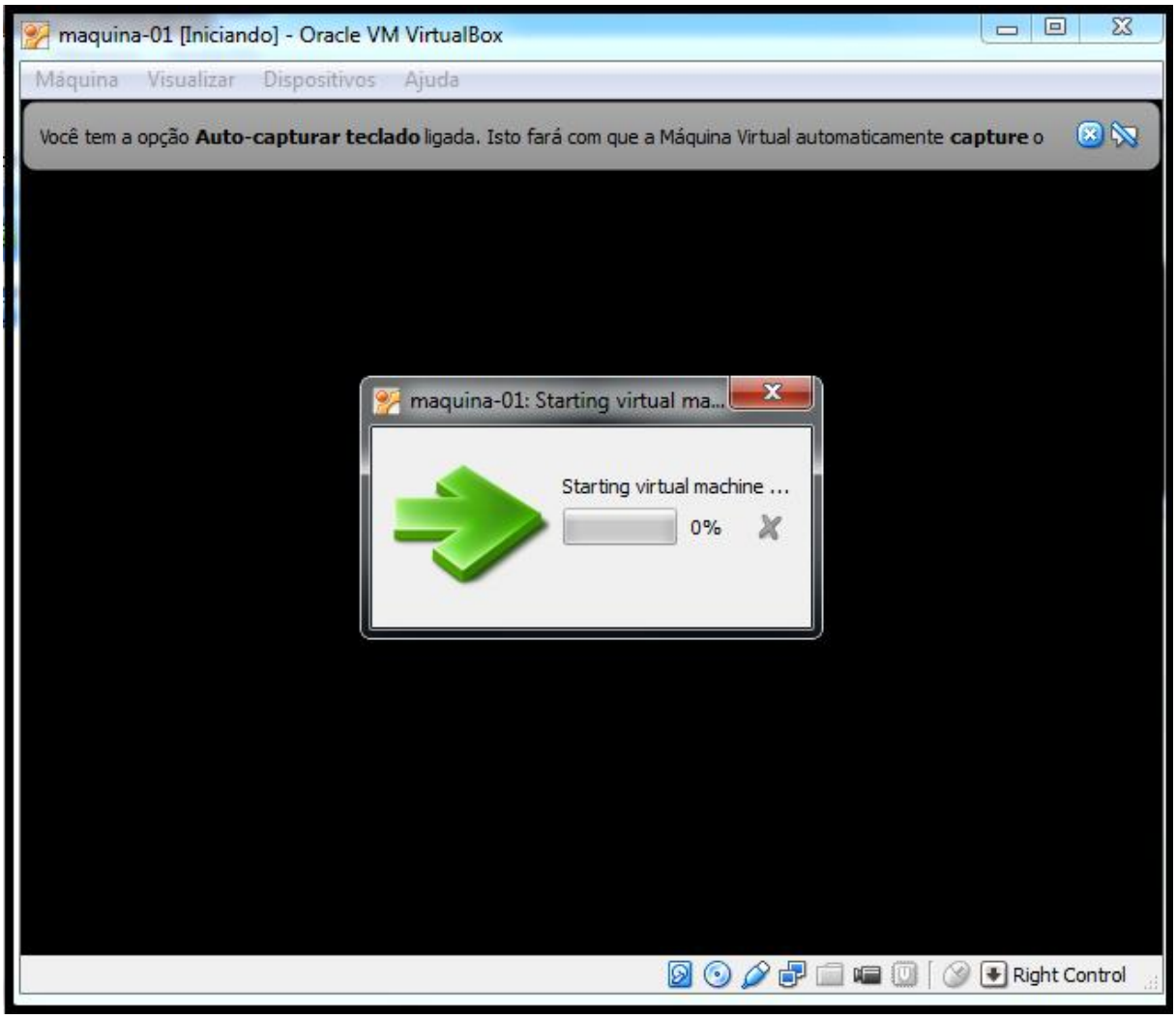


Aguardei o disco ser criado.

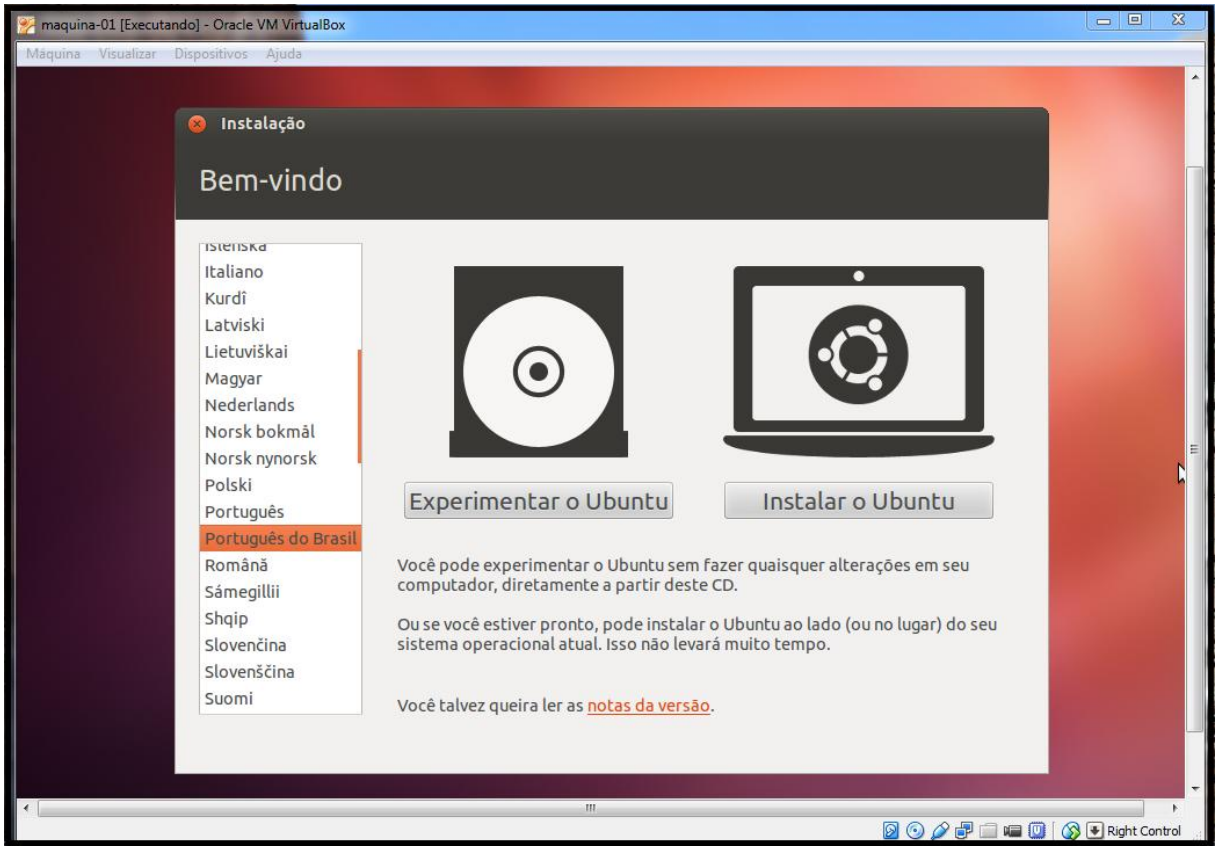


Instalando o sistema

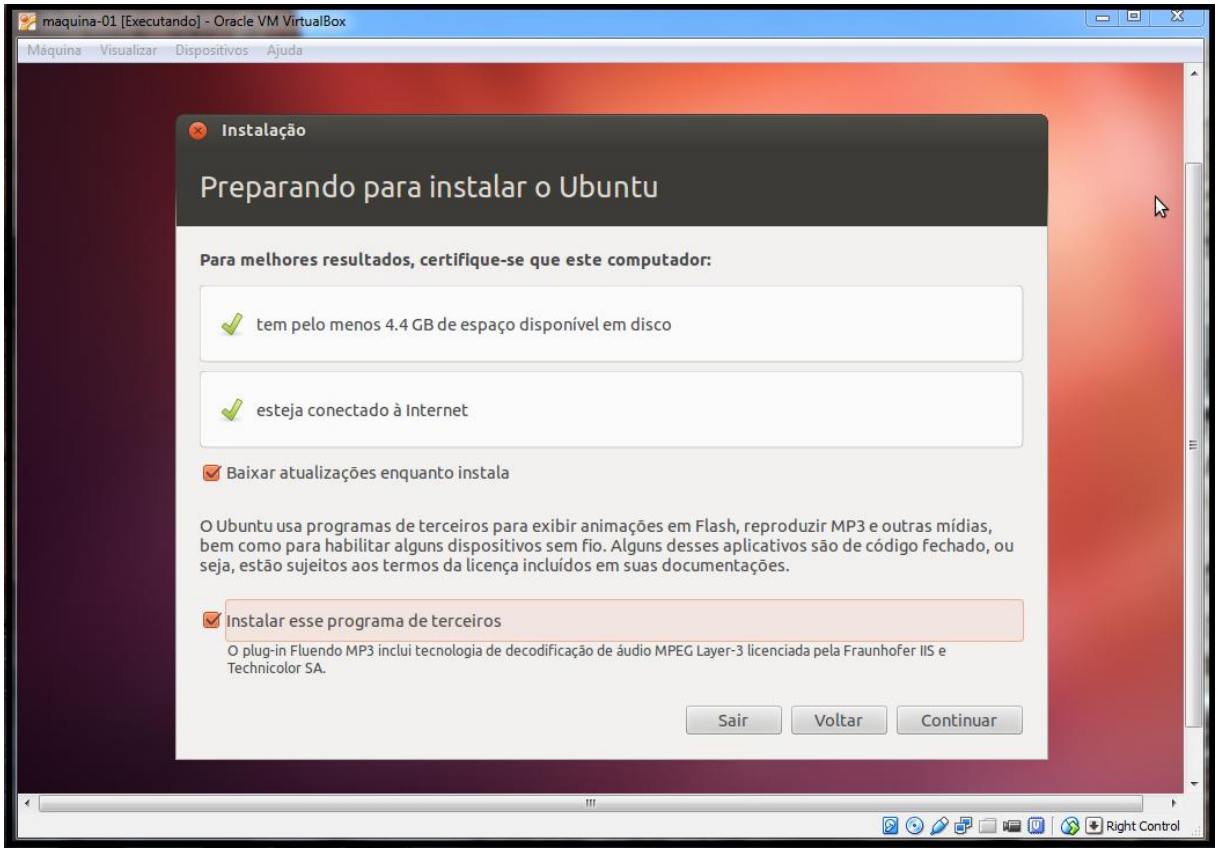
Nesse passo iniciei a máquina virtual, instalando o sistema operacional.



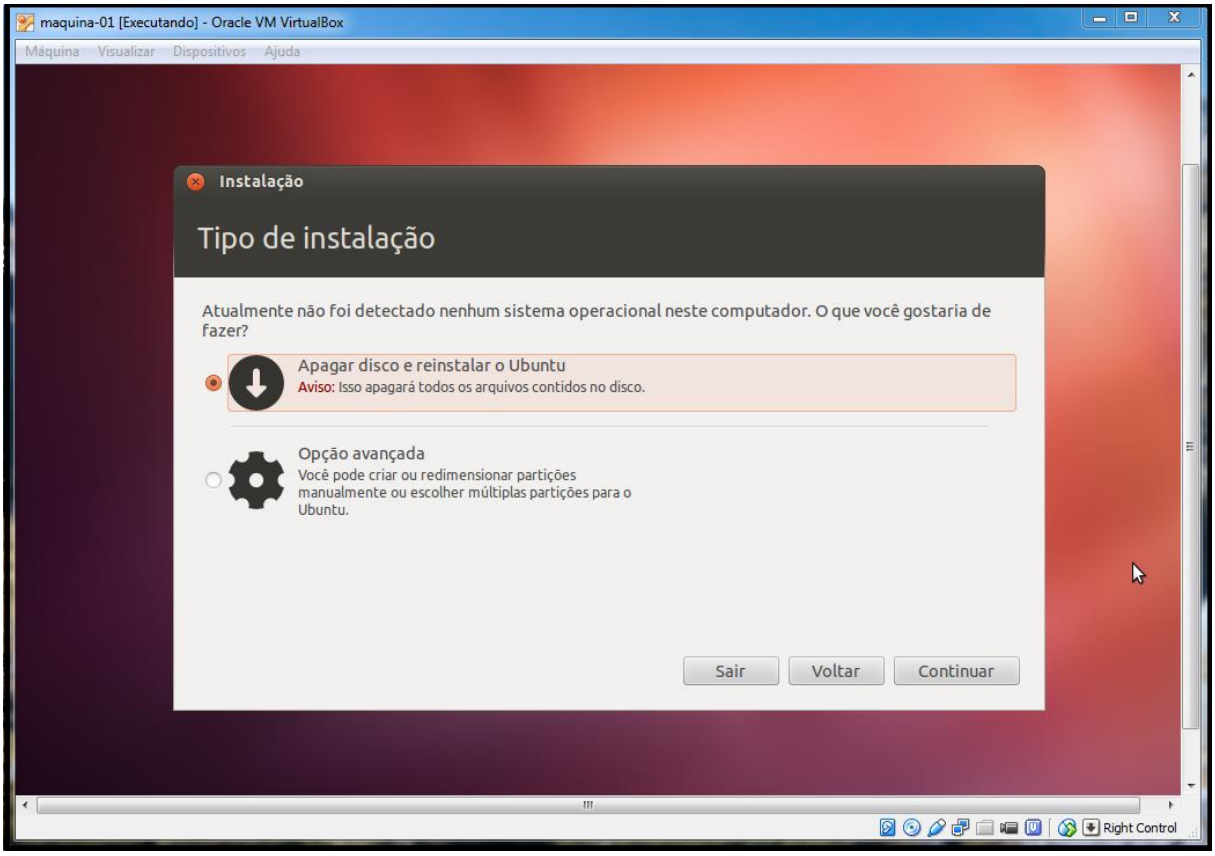
Escolhi o idioma e cliquei em instalar o *Ubuntu*.



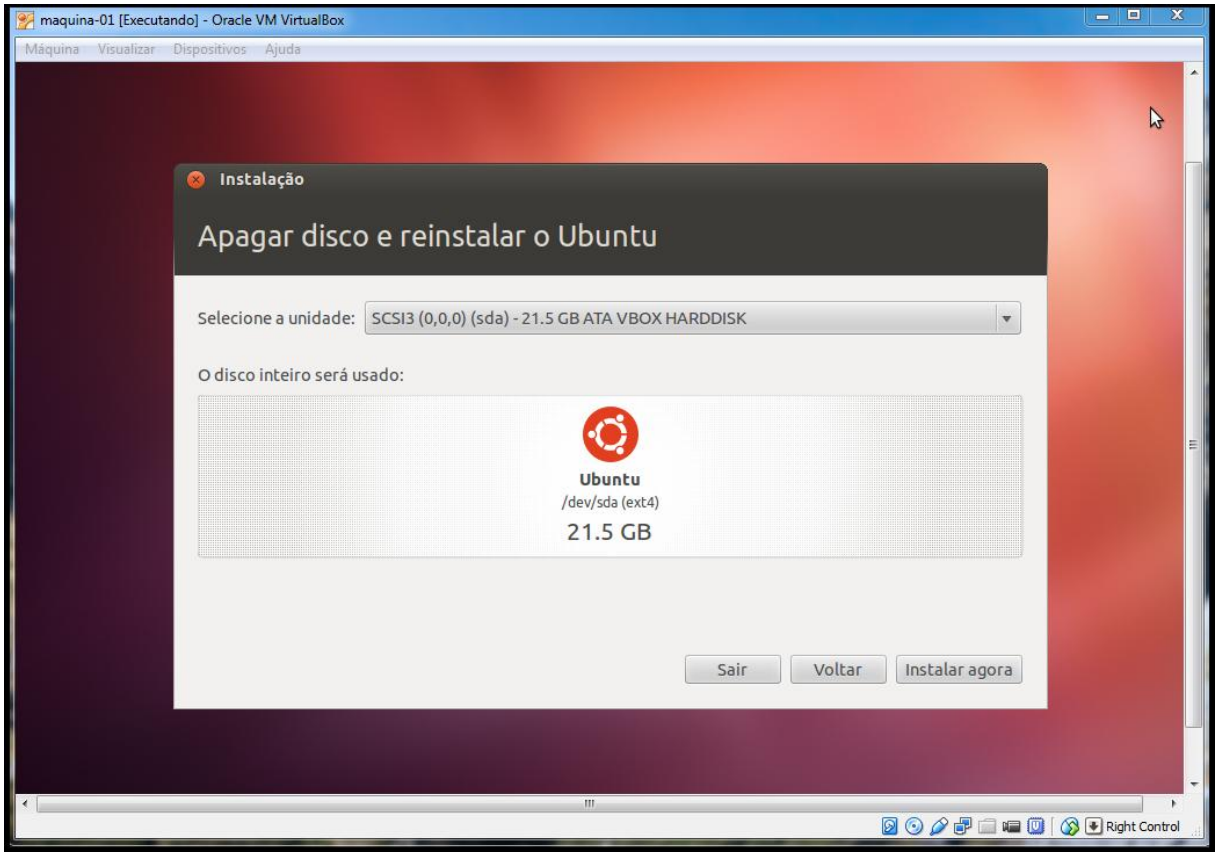
Cliquei em continuar.



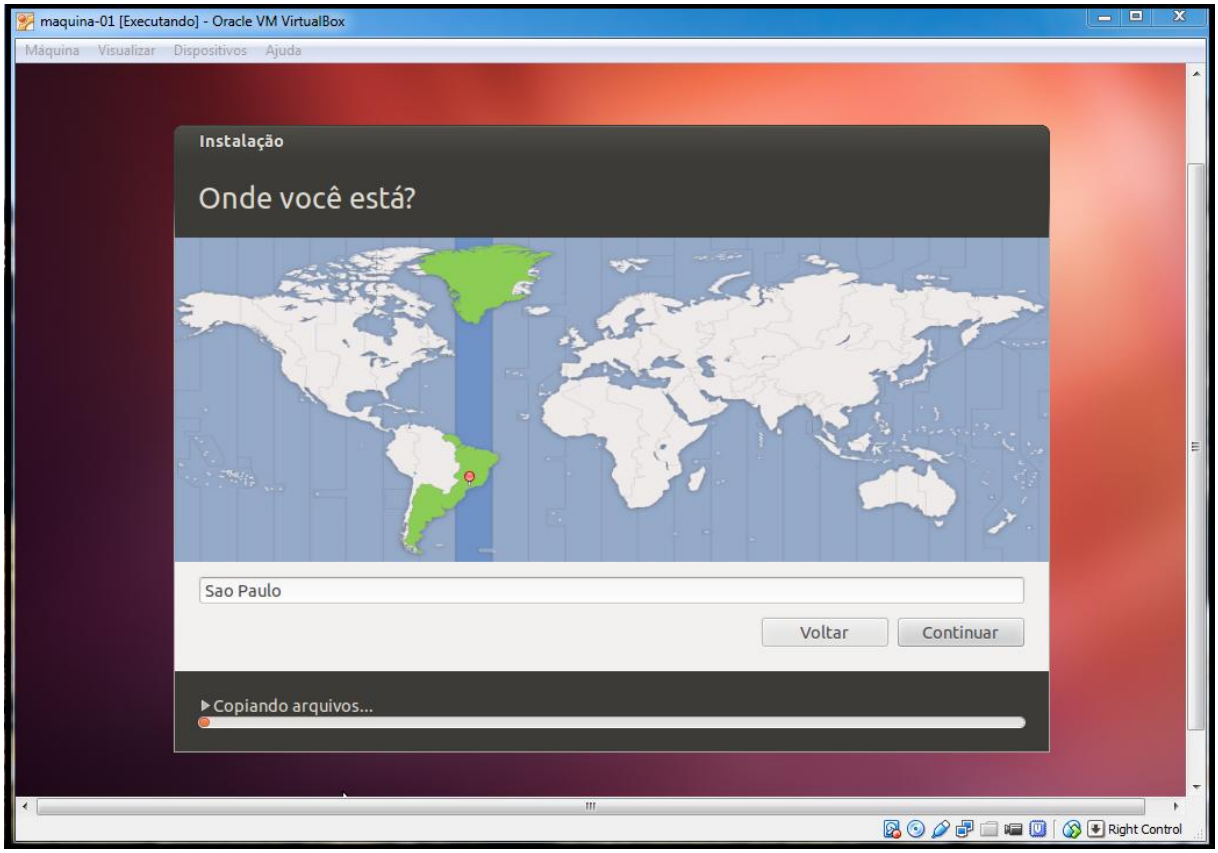
Deixei selecionado em apagar disco e reinstalar o *Ubuntu* e cliquei em continuar.



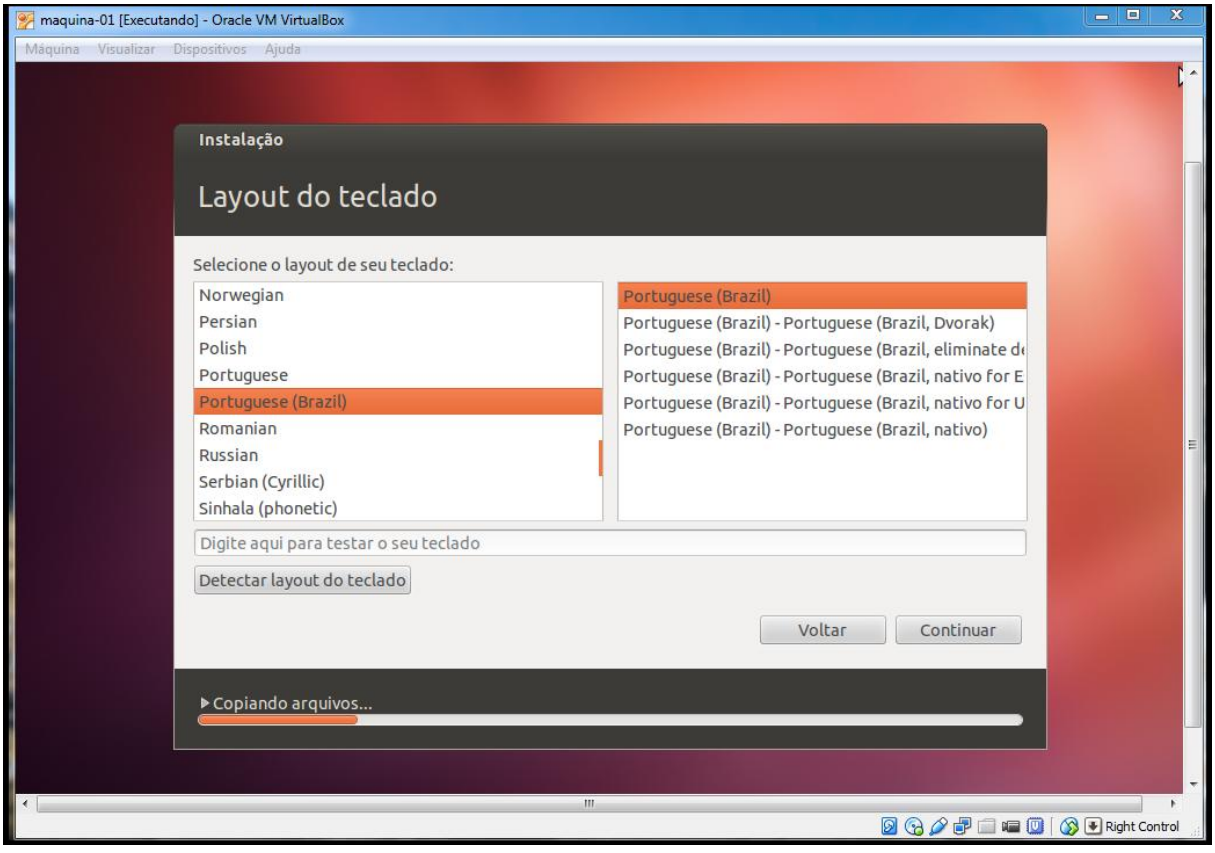
Cliquei em instalar agora.



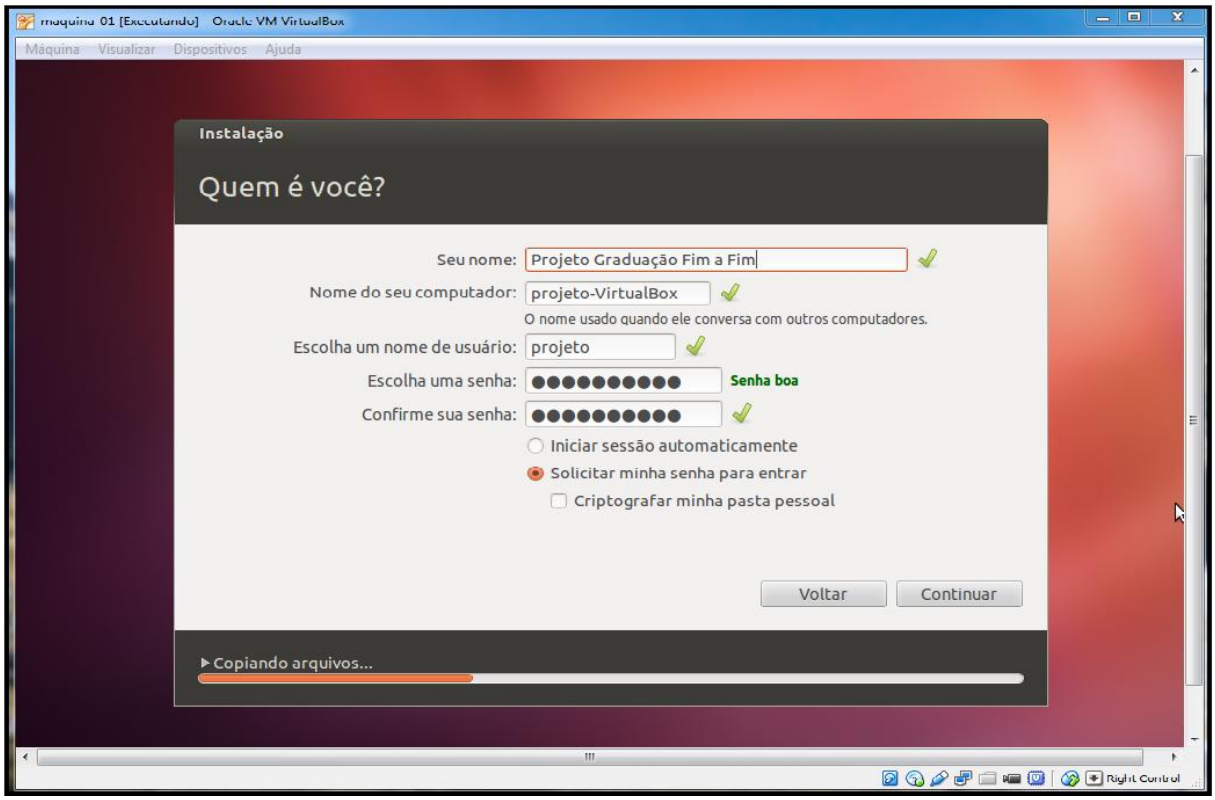
Cliquei em continuar.



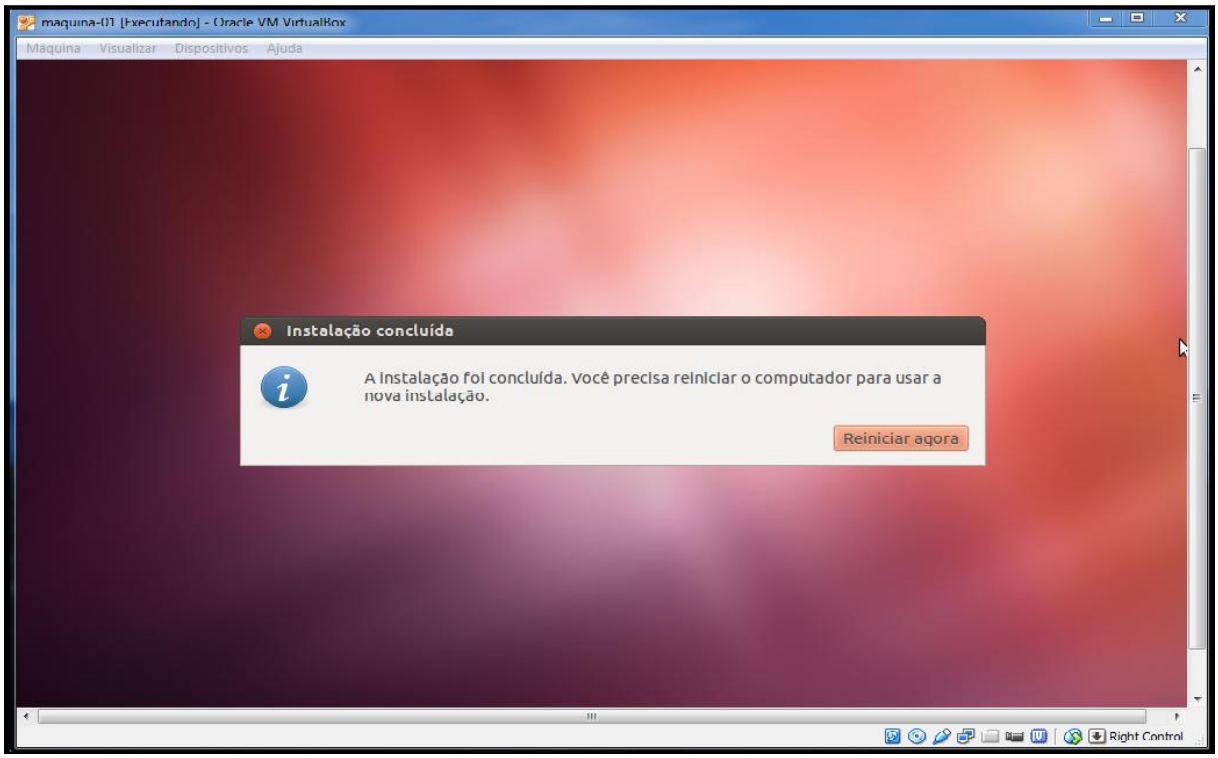
Nesse passo, verifiquei o idioma e cliquei em continuar.



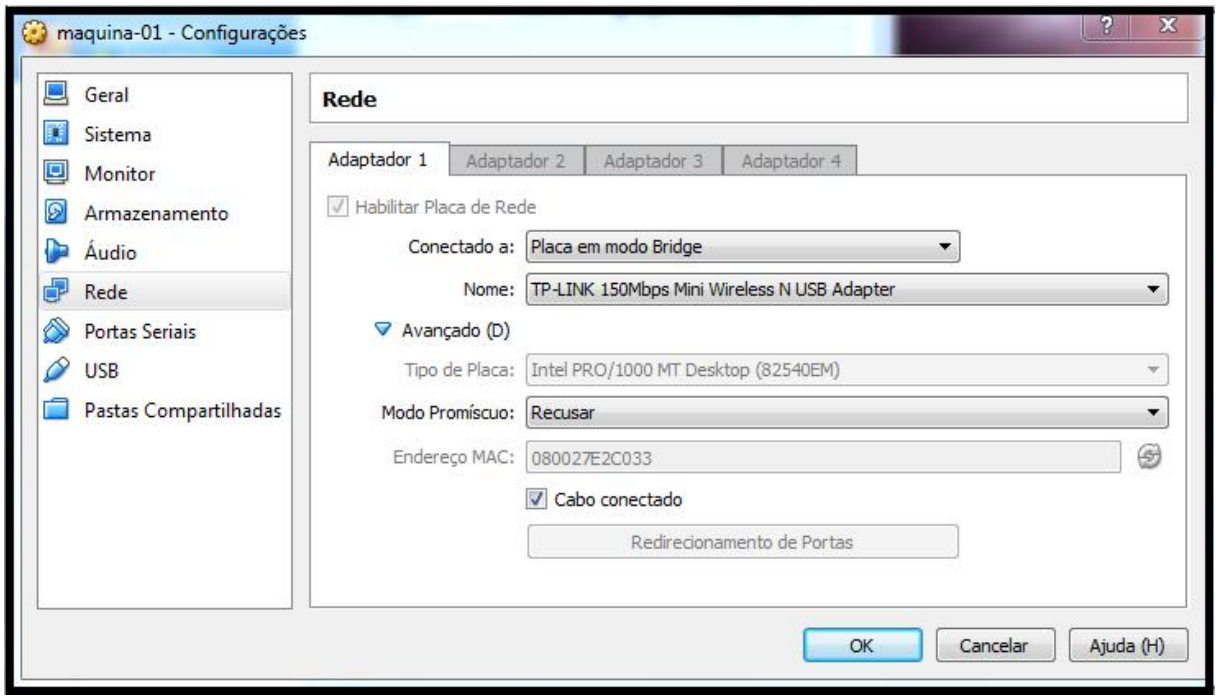
Coloquei um nome para o sistema e também configurei uma senha, deixei selecionado “solicitar minha senha para entrar” e cliquei em continuar.



Terminada a instalação eu cliquei em “reiniciar agora” e finalizei a instalação.



O último passo a ser configurado foi à placa de rede, para acessar as configurações da placa de rede é só entrar em rede. Para esse experimento foi configurada a placa de rede, de modo NAT para o modo *Bridge*, para que pudesse fazer a conexão de rede na máquina física com as máquinas virtuais.

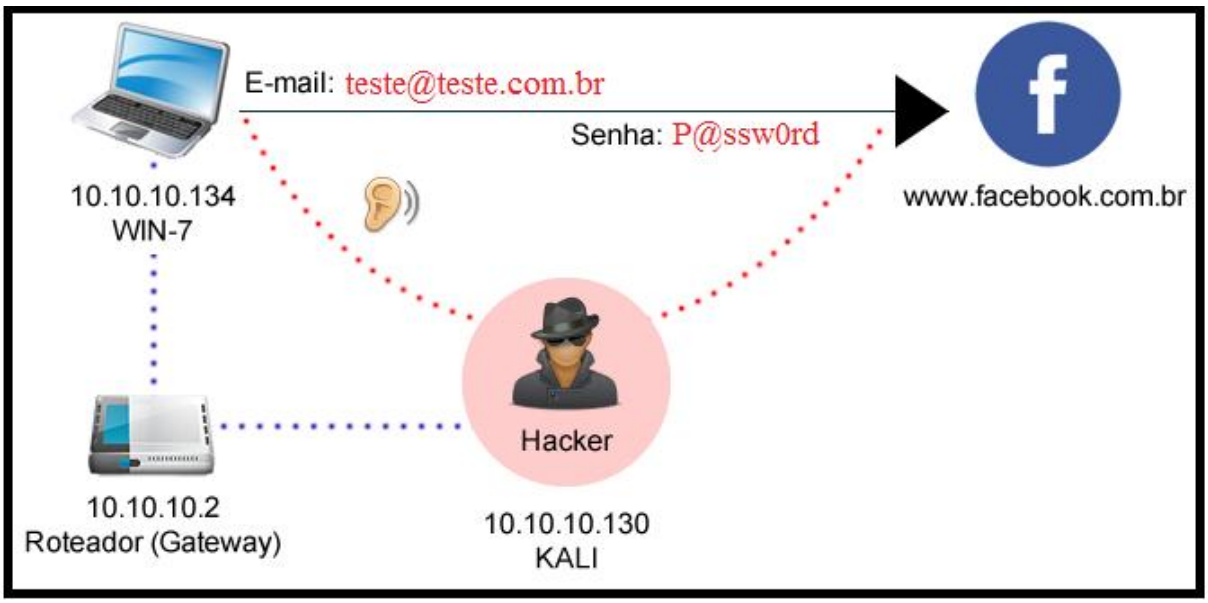


Configurações para o ataque

Essa é sem duvida uma técnica muito eficaz, ela é chamada *Man-in-the-Middle* (MITM), literalmente “Homem no Meio”, esse tipo de ataque ocorre quando um atacante se posiciona no meio de uma transmissão de dados, ou seja, todas as informações passam primeiramente pela máquina do atacante antes de chegarem ao destino.

Esse tipo de ataque pode ser configurado para funcionar em apenas um sentido ou em ambos (do Host A para o B e do B para o A), como ilustra a figura 20. Note que nesse caso a máquina com IP: 10.10.10.134 não consegue identificar o ataque que está em andamento, ou seja, a vítima não tem nenhuma noção que seus dados estão sendo capturados e sua privacidade esta sendo invadida.

Figura 20-Homem no Meio



Fonte: (HENRIQUE, 2015).

REFERÊNCIAS

CAMPOS, A. Sistemas de segurança da informação. Editora Visual books, 218p, 2º Edição 2007.

CERT.BR, Centro de estudos, resposta e tratamento de incidentes de segurança no Brasil. São Paulo, SP: Editora Comitê Gestor da Internet no Brasil, 2012. 140p. 2ª Edição.

FILHO, R. T. C.; COSTA, R. T. Rtell informática. Rio de Janeiro, RJ. Disponível em: <http://www.rtell.com.br/Pcp/paginas/redes/dredes44.htm>, acesso em: 16 Abr. 2015.

HENRIQUE, M. PROTONMAIL. Disponível em: <http://www.100security.com.br/protonmail-email-criptografado/> Acesso em 17 Abr. 2015.

ITI, Instituto de Tecnologia da Informação. Brasília, DF. Disponível em: <http://www.iti.gov.br>. Acesso em 30 Mar. 2015.

ILHA, F. Do UOL. Porto Alegre, SC: 2013; Disponível em: <http://www.noticias.uol.com.br/cotidiano/ultimas-noticias/2013/01/10/maquina-de-criptografar-mensagens-usada-por-nazistas-na-segunda-guerra-sera-mostrada-no-brasil.htm>. Acesso em 10 Abr. 2015.

KUROSE, James F; ROSS Keith W; Redes de Computadores e a Internet Editora Pearson Education do Brasil, 720p. 2006. 3º Edição.

MACHADO, Robson: Certificação digital ICP-Brasil. Editora Impetus, 2010. 243p. 1º Edição.

MAIA, L. P.; PAGLIUSI, P. S. Assinatura Digital. Disponível em: <http://www.training.com.br/lpmaia/pub_seg_cripto.htm>. Acesso em 10 Abr. 2015.

MATOS, A. V. L. Quebrando a criptografia RSA. Campinas, SP, 2009. Disponível em: <http://www.vivaolinux.com.br/artigo/Quebrando-a-criptografia-RSA?pagina=1>. Acesso 14 Abr. 2015.

MORENO, E. D.; PEREIRA, F. D.; CHIARAMONTE, R. B. Criptografia em Software e Hardware. Editora Novatec. 288p. 2005.

STALLINGS, W, Arquitetura e Organização de Computadores. São Paulo, SP. Editora Prentice Hall, 787p. 2003. 5º Edição.

STALLINGS, William, Criptografia e segurança de redes. São Paulo, SP. Editora Pearson Prentice Hall, 512p. 2008. 4º Edição.

TANENBAUM, Andrew S; Redes de Computadores. Rio de Janeiro, RJ. Editora Campus, 632p. 2007. 4º Edição.

VICTORINO, C. R.; FORTUNATO, C. Benefícios a aplicações da certificação digital. Estúdio grafen Edição 2012. 34p. Disponível em: <http://www.fenacon.org.br/usuarios/arquivos%5Cpublicacoes%5CBenef%C3%ADcios_Aplica%C3%A7%C3%B5es_CD.pdf>. Acesso em 29 Mar. 2015.