UNIVERSIDADE DO SAGRADO CORAÇÃO

ALEXANDRE DI GIOVANNI GOUVÊA

ANÁLISE DE FERRAMENTAS DE AUXÍLIO AO GERENCIAMENTO DE REDES DE COMPUTADORES

BAURU
2010

ALEXANDRE DI GIOVANNI GOUVÊA

ANÁLISE DE FERRAMENTAS DE AUXÍLIO AO GERENCIAMENTO DE REDES DE COMPUTADORES

Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Exatas e Naturais como parte dos requisitos para a obtenção do título de bacharel em Ciência da Computação, sob orientação do Professor Dr. Kelton Augusto Pontara Costa.

BAURU
2010

ALEXANDRE DI GIOVANNI GOUVÊA

ANÁLISE DE FERRAMENTAS DE AUXÍLIO À AUDITORIA DE REDES DE COMPUTADORES

Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Exatas e Naturais como parte dos requisitos para a obtenção do título de bacharel em Ciência da Computação, sob orientação do Professor Dr. Kelton Augusto Pontara Costa.

Banca examinadora:

_____
Prof. Dr. Kelton Augusto Pontara Costa
Universidade do Sagrado Coração

_____
Prof. Esp. Henrique Pachioni Martins
Universidade do Sagrado Coração

_____
Prof. Esp. André Luiz Ferraz Castro
Universidade do Sagrado Coração

Bauru, 14 de Dezembro de 2010.

AGRADECIMENTOS

Agradeço primeiramente aos meus pais, Paulo e Angela que me deram educação e formaram meu caráter, sem essa base não teria chegado a lugar algum.

Meus irmãos Vanessa e Daniel que fazem parte da minha vida de maneira interessante, me ensinando muito.

Minha família de maneira geral, por apoiar e participar de forma integral na minha vida.

Aproveito o momento para agradecer também aos amigos João Paulo, Miréla, Hareton, Andréa, Leandro, Alice que contribuíram nessa jornada, seja com um exemplo, um apoio nas horas difíceis ou com a companhia para uma cerveja, pessoas que estarão sempre na lembrança pelos momentos únicos vividos com cada um deles.

A todos os outros colegas e companheiros do dia a dia, Eliete sempre paciente com meus rolos pra pagar, colegas de ônibus, foram várias viagens, aventuras, conversas, risadas.

Gostaria de agradecer aos professores Kelton, Ronaldo, Henrique, André, Júlião, Patrícia, Anderson, Patrick, Élvio, Glória que fizeram parte dessa jornada, ensinando, ajudando e aconselhando, muitas vezes sendo mais que simples professores, sendo amigos, essa ajuda foi fundamental para que eu pudesse chegar onde estou agora.

Agradeço ao meu antigo chefe Bruno que me ensinou muito e ajudou sempre durante os anos que trabalhamos juntos.

À minha atual chefe Cristina, que me trata como um de seus filhos e me ensina muito sobre informática e sobre viver.

Todos os citados direta e indiretamente, fazem parte da minha vida e têm um lugar especial guardado na minha lembrança, cada um com sua importância. Mas todos responsáveis pelo que sou hoje, quero dividir a conquista dessa etapa com todos vocês.

O único lugar onde o sucesso vem antes do trabalho é no dicionário. (Albert Einstein)

RESUMO

As redes de computadores necessitam compartilhar informações em tempo real e assim agilizar processos. Porém essas informações devem ser protegidas para que só sejam utilizadas por pessoas autorizadas. Nessa hora entra a Segurança em sistemas de informação e o Gerenciamento de redes de computadores. O gerenciamento das redes de computadores permite que sejam analisadas as informações em tempo real para se ter certeza que não há nada errado com os dados que trafegam na rede. Esse estudo comparou certas ferramentas especificas, analisando desde a facilidade para a instalação das mesmas, a configuração, os resultados obtidos e a licença de uso de cada uma delas. Aspectos primordiais na escolha de qual ferramenta utilizar em uma empresa. A escolha dessas ferramentas foi feita através da popularidade das mesmas, sendo elas as mais escolhidas por profissionais de TI para a análise em ambiente corporativo. Os testes foram realizados em uma rede genérica com três computadores pessoais (PC) e dois notebooks, interligados através de um roteador, notebooks em rede sem fio e PCs em rede via cabo de rede. Para cada ferramenta foram simuladas possíveis falhas e analisadas as respostas de cada ferramenta. Ao final os dados obtidos foram expostos em forma de tabela com graduações em vários quesitos preestabelecidos, permitindo uma comparação entre as soluções para que facilite a escolha para cada tipo de problema, por parte do usuário.

Palavras - Chave: Gerenciamento de Redes. Segurança de Redes. Auditoria. Tecnologia da Informação. TI.

ABSTRACT

Computer networks need to share information in real time and thus speed up processes. But this information must be protected so that only authorized persons are used. At this time enter the security in information systems and management of computer networks. The management of computer networks allows us to review the information in real time to make sure that there is nothing wrong with the data that travels over the network. This study compared certain specific tools, since analyzing the ease of installing the same, the setting, the results obtained and license to use each one. Fundamental issues in choosing which tool to use in an enterprise. The choice of these tools was done by the popularity of them, and they most often chosen by professionals for analysis in the corporate environment. The tests were performed on a generic network with three computers (PCs) and two laptops, connected through a router, laptop wireless networking and networked PCs via network cable. For every tool possible failures were simulated and analyzed the responses of each tool. At the final data were displayed in table form with predetermined degrees in many areas, allowing a comparison between the solutions for facilitating the choice for every type of problem, by the user.

Key words: Management of Computer Networks. Network Security. Audit. Information Technology. IT.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS

AD – Active Directory (Diretório Ativo);
AES - Advanced Encryption Standard (Padrão de Criptografia Avançado);
COBIT (Control Objectives for Information and related Technology - Objetivos de Controle de Tecnologia de Informação e afins);
DES - Data Encryption Standard (Padrão de Criptografia de Dados);
GB – Gigabyte equivalente a 1024 Mb;
GNU GPL – General Public License;
ICMP – Internet Control Message Protocol (Protocolo de Controle de Mensagem da Internet);
IETF - Internet Engineering Task Force (Força Tarefa Aplicada a Internet);
IGMP – Internet Group Management Protocol;
IP – Internet Protocol (Protocolo de Internet);
IPSec – Internet Protocol Security (Protocolo Seguro da Internet);
IPv4 – Internet Protocol version 4 (Protocolo de Internet versão 4);
IPv6 – Internet Protocol version 6 (Protocolo de Internet versão 6);
ISACA (Information Systems Audit and Control Association - Associação de Controle e Fiscalização de Sistemas de Informação);
ISO/IEC – International Organization for Standardization / International Electrotechnical Commission;
ITIL (Information Technology Infrastructure Library – Biblioteca de infra-estrutura de Tecnologia de Informação);
KB – Kilobyte equivalente a 1024 bytes;
LAN – Local Area Network (Rede de Área Local);
MAN – Metropolitan Area Network (Rede de Área Metropolitana);
MB – Megabyte equivalente a 1024 Kb;
MIB – Management Information Base (Base de Informações de Gestão);
MRTG – Multi Router Traffic Grapher;
NMAP – Network Maper
OSI – Open Systems Interconnection (Sistema Aberto Interconectado);
RFC – Request for Comments (Pedidos de Comentários);
SNMP – (Simple Network Management Protocol – Protocolo de Gerenciamento de Rede Simples);
TCP – Transmission Control Protocol (Protocolo de Controle de Transmissão);
TI – Tecnologia da Informação;
UDP – User Datagrama Protocol;
VPN (Virtual Private Network – Rede Privada Virtual);
WAN – Wide Area Network (Rede de Área Ampla);

SUMÁRIO

1 Introdução

Atualmente com o avanço da informática, que diminuiu os preços de computadores e aumentou a capacidade de processamento destas máquinas, e a importância de se compartilhar as informações processadas pelos computadores, surgiu à necessidade de se criar uma conexão entre os computadores, essa conexão é a rede de computadores.

O exemplo mais comum de rede de computadores é a internet, onde todos estão ligados juntos trocando informações, em tempo real.

É nesse cenário de troca de informações em tempo real, de facilidade de comunicação e aquisição de informações que surge um problema muito questionado atualmente, a segurança das informações.

A mesma rede capaz de interligar computadores em empresas, disponibilizar informações bancárias em tempo real de qualquer lugar, é capaz de permitir roubos de dados, e informações sigilosas das empresas. É nessa hora que surge a Segurança de Informações. Empresas investem em departamentos especializados em segurança de Redes de Computadores, para proteger o maior patrimônio digital de uma empresa, suas informações.

Segundo STEEN E TANENBAUM (2007), o conceito de Segurança de sistemas está diretamente relacionado com dois outros conceitos, são eles confiabilidade e integridade. Um sistema só é devidamente seguro se estiver livre de invasões que gerem danos às informações, podendo assim retornar resultados corretos e precisos, conforme o esperado destes sistemas.

Se a segurança é algo tão importante, como saber se uma rede é segura? Como saber se os dados que estão compartilhados entre os computadores estão livres de invasões de terceiros, vírus ou de outras ameaças capazes de prejudicar a integridade e assim a confiabilidade do sistema?

Uma solução para responder a essas perguntas é a aplicação de gerenciamento de rede, para com a utilização de algumas ferramentas, conseguir detectar e corrigir possíveis falhas de segurança, evitando assim vulnerabilidade nestas redes.

Esse estudo verificou o que é Gerenciamento de rede, quais são os benefícios de gerenciar uma rede de computadores, em que ajuda gerenciar essas redes, quais são as mais famosas ferramentas disponíveis no mercado atualmente. Lembrando que devido ao curto espaço de tempo e da infinidade de informações a esse respeito, foi abordada somente pontos chave destes assuntos, e também foi analisado somente algumas ferramentas na prática.

1.1 Objetivo Geral

Este estudo visa analisar na prática o funcionamento de algumas ferramentas de auxílio ao gerenciamento de redes de computadores, ferramentas essas escolhidas por popularidade.

1.2 Objetivo Específico

Essa análise tem por objetivo auxiliar profissionais de TI (Tecnologia da Informação), que necessitem detectar falhas de segurança e estabilidade dentro da empresa, a encontrar a melhor ferramenta, e se decidirem sobre qual é a melhor opção específica para cada problema em especial.

Pontuar as vantagens e desvantagens da utilização de cada ferramenta, visando um melhor conhecimento do que existe no mercado atualmente.

Apontar situações atualmente deficientes de soluções para que sejam criadas novas ferramentas mais completas e especificas que as existentes atualmente.

1.3 Justificativa

O gerenciamento de redes, por ser uma área relacionada à segurança que é um assunto muito visado e comentado atualmente, encontra muitos problemas na área e muitas soluções. Porém como saber qual solução resolve o problema encontrado por um usuário? Essa análise servirá para pontuar prós e contras de cada ferramenta e assim ajudar o usuário a escolher qual a ferramenta mais indicada para o seu problema, facilitando o serviço dele, e economizando tempo para os testes que esse usuário deveria fazer.

Para o meio científico este estudo visa pontuar as vantagens e desvantagens de cada sistema com o intuito de localizar possíveis falhas não corrigidas, para que futuramente as mesmas possam receber o tratamento devido.

1.4 Estrutura do Trabalho

No primeiro capítulo foi abordado o trabalho, com uma breve introdução sobre o assunto, especificando quais os objetivos dessa pesquisa, e a estrutura de desenvolvimento. No segundo capítulo foi exposto o conteúdo pesquisado durante o desenvolvimento, neste

capítulo são abordados alguns tópicos baseado em autores, e pesquisadores, especialistas na área de redes de computadores, segurança, e auditoria. Os temas abordados são: Conceitos, Internet, Protocolos, Segurança, Gerenciamento e Auditoria.

No terceiro capítulo foi abordada a forma como o trabalho foi desenvolvido, ou seja, metodologia, ferramentas escolhidas, infra-estrutura para o teste, metodologia dos testes, padrão de notas para cada item testado, e os resultados obtidos.

No quarto capitulo foi descrita a análise do autor do estudo, pontuando os prós e contras das ferramentas e uma breve analise de como um usuário com pouco conhecimento trabalharia com cada ferramenta.

E no final estão as referências bibliográficas, ou seja, os autores que serviram de base para o desenvolvimento do projeto, criadores ou organizadores das idéias contidas nesse trabalho.

Por último estão os anexos que contêm tutoriais de instalação de todas as ferramentas, instruções para configurar as mais complicadas.

2 Levantamento Bibliográfico

Segundo CANTÚ (2003) dois ou mais computadores interligados podem ser considerados uma rede de computadores, permitindo assim o compartilhamento de informações entre os computadores dessa rede e permitindo também que outros dispositivos, como impressoras, possam ser utilizados por todos os computadores dessa rede.

Ainda de acordo com CANTÚ (2003) a aplicação prática de redes de computadores vai desde um pequeno escritório que tem vários computadores e apenas uma impressora para todos usarem, até a Internet que também é uma rede de computadores compartilhando informações ao redor do mundo.

As redes são classificadas de acordo com a complexidade de conexão, baseado em FERREIRA (1994), sendo consideradas *LAN (Local Area Network ou Rede de Área Local)* aquelas que estão interligadas por fios, estão próximas fisicamente, por exemplo, em laboratórios ou em escritórios. Quando várias *LAN´s* estão interligadas formando redes entre elas, de acordo com FERREIRA (1994) classificam como *MAN (Metropolitan Area Network ou Rede de Área Metropolitana)*, como exemplo pode-se citar as redes em campus universitários. E interligando as *LAN´s* e *MAN´s* existem as redes classificadas como *WAN (Wide Area Network ou Rede de Área Ampla)* que são redes globais, transmitem dados entre os terminais via satélite, ondas eletromagnéticas, fios telefônicos ou outros meios de longo alcance.

2.1 Internet

Segundo TANENBAUM (2003), a Internet não é uma rede de computadores, e sim a interligação de varias redes menores e independentes umas das outras, através de roteadores rápidos e linhas de banda larga, formando *backbones* (conexões de alta velocidade que interligam redes regionais), onde são conectados as *LAN´s* e *MAN´s*.

De acordo com TANENBAUM (2003) a transmissão de dados na internet funciona através de pacotes de no máximo 64 *KB (Kilobytes – unidade de medida de dados de computadores)* que tem a informação total particionada em datagramas**,** dessa forma a informação vai em partes, de um computador para o outro. O responsável pela interligação dos computadores, das redes e do transporte desses pacotes é chamado de Protocolo.

2.2 Protocolos

De acordo com FOROUZAN (2008), a comunicação entre as entidades (todo o equipamento capaz de enviar e receber dados) não ocorrem desordenadamente, os dados não podem ser enviados de qualquer forma. Os pacotes recebem um conjunto de normas padrão nas duas pontas.

Segundo FERREIRA (1994) os protocolos são as regras para que os computadores de uma mesma rede se comuniquem entre si, esses comandos são preestabelecidos e não dependem do usuário para funcionar, para criação destes protocolos existem regras e durante a criação é necessária uma documentação explicativa desta ferramenta.

Conforme FOROUZAN (2008) os protocolos são divididos em três partes:

- Sintaxe: Define a estrutura dos dados, dessa forma as entidades sabem o que é informação e o que é endereçamento de dados;
- Semântica: É a interpretação das informações identificando a ação contida no pacote de dados, como o endereço e a rota;
- Sincronismo: Verifica se as entidades estão integras e operando na mesma velocidade para não sobrecarregar as mesmas.

Para a internet usa-se o protocolo *TCP/IP (Transmission Control Protocol/Internet Protocol ou Protocolo de Controle de Transmissão/Protocolo de Internet)*, segundo FERREIRA (1994).

2.2.1 TCP (Transmission Control Protocol)

Segundo DAVIE e PETERSON (2004), o *TCP* é um protocolo de transporte que oferece confiabilidade ao fluxo de dados, evitando que as aplicações tenham que analisar a integridade dos dados trocados, gerando também uma melhora no desempenho. Transmite os dados em *full-duplex*, ou seja, os dados transitam em dois sentidos simultaneamente.

Devido essas características, de acordo com COMER (2006), *TCP* é um protocolo fundamental na transmissão de dados da internet, pois ele exerce uma série de funções necessárias para a transferência dos dados entre os hosts, essas funções são especificações dos formatos dos dados que trafegam pela rede, confirmação da conectividade de dois computadores, ou seja, verificar se os dois computadores que trocarão informações estão devidamente conectados à rede e acessíveis para assim iniciar uma transferência segura, sem perda de dados. O *TCP* verifica também a questão de rotas numa máquina e como os *hosts*

que estão trocando informações se recuperam de problemas como perda de pacotes ou duplicação dos mesmos. Também gerencia o início e o fim de uma transmissão de fluxo entre dois *hosts*.

Segundo FOROUZAN (2008), o protocolo *TCP* envia dados pela rede como se criasse um tudo para interligar origem e destino, conforme figura 1 que exemplifica o uso deste protocolo.

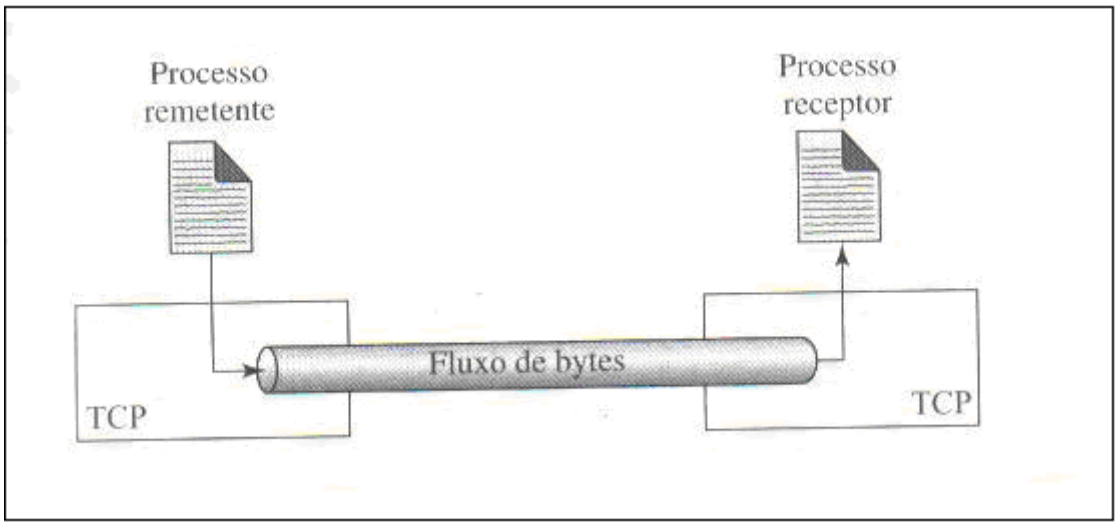


Figura 1 - Envio de dados via TCP.

2.2.2 IP (Internet Protocol), Ipv4 (Internet Protocol version 4) e Ipv6(Internet Protocol version 6)

Conforme COMER (2006), o Protocolo *Ipv4*, que é utilizado por padrão atualmente na internet, é responsável por três tarefas fundamentais para a transferência de dados entre computadores, a primeira é a definição do formato dos dados que será enviada em forma de datagrama para outro *host*, a segunda tarefa é o encaminhamento dos dados, ou seja, o caminho pelo qual o datagrama percorrerá para chegar ao *host* de destino, e a última é a tarefa de informar a roteadores e *hosts* a forma exata de processamento das informações, para que os equipamentos consigam identificar a origem e o destino da informação sem perda de dados.

De acordo com DAVIE e PETERSON (2004), *IP* é um protocolo sem conexão e não confiável, pois não controla erros como perda, desordem ou duplicidade dos dados.

Ainda segundo COMER (2006), para verificações de desvios, extravios, ou chegar a *hosts* e roteadores desligados, é necessário uma informação de retorno comunicando o problema chamado *ICMP (Internet Control Message Protocol – Protocolo de Controle de Mensagem da Internet)*, que é uma parte da informação obrigatória em qualquer datagrama

que use protocolo *TCP/IP*, que permite que roteadores enviem um status de erro sempre que o destino não for alcançado.

Ainda segundo COMER (2006), o *IPv6* é uma evolução do *IPv4*, onde as principais mudanças foram o aumento no tamanho do endereço de 32 *bits* o *IPv4* para 128 *bits* no *IPv6*. Expansão nos níveis de hierarquia dos endereços e o maior espaço de endereço na versão seis foram as novidades mais significativas desta versão. O formato de datagrama foi totalmente modificado, se tornando incompatível com o modelo antigo, podendo receber inclusive informações opcionais. Permite atribuir endereço automaticamente, e reatribuir o endereço de forma dinâmica.

Ainda segundo COMER (2006) essa nova versão vem com o intuito de ser mais segura e resolver um problema no ano de 2022, a falta de endereços livres para utilização (ou 2028 se os endereços sem uso fossem reutilizados) de acordo com cálculos de engenheiros, pois o crescimento da quantidade de *hosts* ligados em rede vem crescendo muito rápido e o atual padrão já não poderia se expandir mais.

2.2.3 DNS (Domain Name System)

Segundo DAVIE e PETERSON (2004) a identificação dos *hosts* através de endereços de *IP*, como utiliza - se hoje é muito eficiente para roteadores, porém usuários não teriam facilidade para lembrar os endereços para servidores e computadores da rede ou da internet dessa forma.

De acordo com FOROUZAN (2008) a forma para facilitar o uso de redes pelos usuários e permitir a facilidade de acesso, foi criado *o DNS (Domain Name System - Sistema de Nome de Domínio)* que funciona como uma tabela armazenando os nomes e os endereços dos *hosts*, onde cada computador mapeia o endereço desse servidor *DNS* e sempre que solicitado uma informação por nome, é feita a referencia do endereço solicitado, conforme figura 2

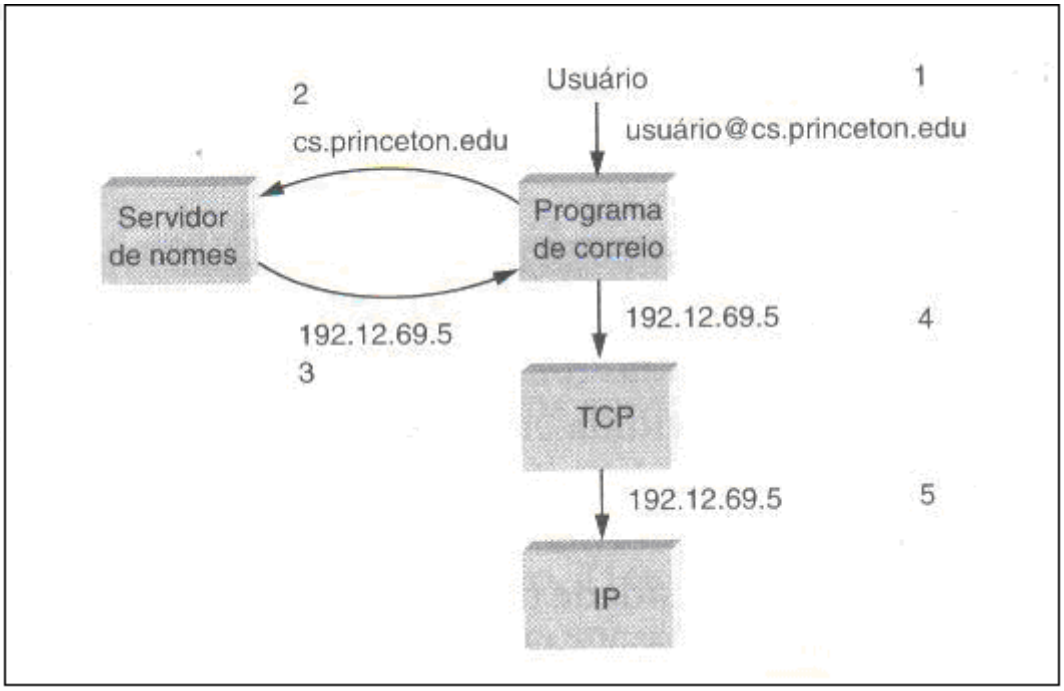


Figura 2 - Funcionamento do DNS.

2.3 Segurança

De acordo com o Dicionário Aurélio Online, a palavra Segurança tem vários significados dentre eles, manter protegido, afastar o perigo, garantia, confiança. Conforme mencionado na norma *ISO/IEC 17799* que regulamenta a prática de segurança de informações, os dados de uma empresa são bens tão preciosos quanto qualquer outro dentro da empresa, e devem ser protegido assim como existem normas para proteção do maquinário contra roubo ou dos funcionários contra acidentes. Dessa forma a segurança visa evitar paradas na produção por problemas com as informações, minimizar possíveis prejuízos e aumentar o retorno de investimentos e oportunidades comerciais, aumentando assim os lucros dessa instituição.

É nesse contexto que segundo BRAHM et al, a internet da mesma forma que gerou uma globalização das informações, gerou facilidade de adquirir formas de se tirar vantagem, principalmente depois da criação do *e-business* (comércio eletrônico) e do *e-cash* (dinheiro eletrônico) e da popularização de ferramentas de administração de contas bancárias via internet *(bankline)*. Surgiram então os *hackers* e *crackers*, que são usuários com grandes conhecimentos de redes de computadores, que usam esse conhecimento para tirar vantagem de falhas de segurança de empresas e pessoas que trabalham com as ferramentas acima citadas.

Neste contexto, de acordo com STEEN e TANENBAUM (2007), os administradores de Redes e sistemas online têm que basear suas políticas de segurança (regras de segurança de um sistema) prestando atenção em alguns pontos chave.

Segundo STEEN e TANENBAUM (2007) a segurança está diretamente relacionada à confiabilidade, essa sendo dividida e analisada em alguns aspectos como fidedignidade, disponibilidade, capacidade de manutenção, confidencialidade e integridade das informações.

Segundo a *ISO/IEC 17799* confidencialidade é restringir o acesso a informações somente a grupos autorizados a acessá-las, evitando assim acessos indevidos aos dados que trafeguem na rede.

Ainda de acordo com a *ISO/IEC 17799* integridade é manter as informações, processos ou métodos reais e exatos de acordo com a realidade, sem sofrer nem um tipo de intervenção que possa modificar a forma de armazenar ou interpretar as informações contidas na rede.

E por fim a *ISO/IEC 17799* analisa também o termo disponibilidade, tendo em seu contexto que as informações devem ser acessíveis a quem de direito for, sempre que necessário respeitando as outras regras de segurança, porém sem que haja perda de tempo ou impossibilidade de usar alguma informação contida na rede.

Segundo PFLEEGER (2003 apud STEEN e TANENBAUM 2007) existem quatro tipos principais de ameaças relevantes à segurança, que são: Interceptação, Interrupção, Modificação e Invenção.

De acordo com PFLEEGER (2003 apud STEEN e TANENBAUM 2007) a Interceptação o ato de se ter acesso a informações que trafegam na rede sem ter permissão para acessá-las, informações confidenciais roubadas após invasões de diretórios privados, escutas telefônicas, ou seja, toda informação acessada por outro usuário que não seja o dono ou alguém que tenha permissão para acessá-la acaba sendo classificada como informação interceptada.

Baseado em PFLEEGER (2003 apud STEEN e TANENBAUM 2007) a interrupção é um caso parecido com a interceptação, porém ao invés de acessar essa informação como no caso anterior, o usuário invasor gera uma falha nessa informação deixando a mesma corrompida ou ilegível, fazendo assim com que um sistema inteiro deixe de funcionar ou então que o arquivo fique inutilizável, provisoriamente ou em alguns casos permanentemente.

Segundo PFLEEGER (2003 apud STEEN e TANENBAUM 2007) as modificações são casos parecidos com os outros dois citados acima, porém nesse caso o usuário invasor não destrói um arquivo, ou rouba um dado importante, nesse caso o usuário, modifica trechos de

sistemas ou partes de arquivos visando alterar os resultados obtidos do processamento desses arquivos destruindo assim a confiabilidade destes sistemas, ou então gerando o envio de informações sigilosas automaticamente e secretamente para que possam ser usadas para vantagem própria.

O quarto e último caso citado por PFLEEGER (2003 apud STEEN e TANENBAUM 2007) é a invenção de informações, ou seja, criar entradas de arquivos novos ou dados que não deveriam existir visando modificar um sistema em vantagem própria. Esse caso é comum em sites de bancos que são clonados e seus clientes acessam e digitam senha, ficando estas armazenadas em banco de dados de terceiros.

Ainda segundo PFLEEGER (2003 apud STEEN e TANENBAUM 2007) todas essas formas de burlar a segurança de um sistema são consideradas falsificações de dados, ou seja, de uma forma direta ou indireta essas informações deixam de ser confiáveis, falhando assim em um dos princípios da segurança de redes de computadores citados acima.

Segundo STALLINGS (2005) existem dois tipos de ataques comuns às redes de computadores, sendo eles:

Ataques Passivos, de acordo com STALLINGS (2005), são tentativas de roubar informações sem corrompê-las, ou modificá-las somente acompanhando o tráfego de informações e capturando pacotes que se mostrem interessantes, ou que contenham informações relevantes. As interceptações são através do vazamento de informações de mensagem, ou seja, roubar conteúdo de um e-mail, ou uma ligação telefônica. Ou as interceptações também ocorrem através da análise do tráfego da rede, ou seja, verificando os pacotes que trafegam na rede buscando uma lógica para se quebrar a criptografia, ou até mesmo encontrar pacotes sem chave criptográfica nenhuma.

Baseado em STALLINGS (2005) essas formas de ataque, não são fáceis de detectar, portanto a melhor forma de proteção contra esse tipo de problema é a prevenção, com criptografia de dados complexas e robustas.

Ataques Ativos, conforme STALLINGS (2005) são os ataques que de alguma forma geram modificações no sistema de dados, ou no fluxo de informações, gerando a falsificação de dados, danificando as informações e prejudicando empresas.

Atualmente segundo a norma *ISO/IEC 17799*, a competitividade contida no ambiente empresarial, é muito grande e os sistemas de computadores interligados em redes, se fazem cada vez mais necessários por serem ferramentas poderosas na gestão de empresas, o problema é que sem a segurança certa de acordo com as necessidades de cada empresa, essa se torna cada vez mais vulnerável, podendo ter suas informações falsificadas conforme citado

acima e fazendo com que prejuízos financeiros, físicos venham prejudicar a empresa e até denegrir sua imagem perante seus clientes e fornecedores. Algumas medidas devem ser tomadas para evitar os problemas abaixo citados.

Conhecendo os problemas genéricos de segurança que uma rede de computadores sofre, já está dado o primeiro passo para torná-la mais segura, porém só conhecer os problemas não é tudo, segundo STEEN e TANENBAUM (2007) é necessário descrever quais são os riscos específicos que o sistema corre para que assim eles possam ser evitados, essa lista de possíveis riscos se chama política de segurança, é ela quem determina o que cada entidade de um sistema, ou seja, usuários, processos, dados, tem permissão de fazer e o que essas entidades são proibidas visando aumentar assim a segurança das mesmas, e podendo focalizar os mecanismos de segurança de acordo com cada caso especifico. Os mecanismos de segurança mais comuns de serem implantados são quatro, Criptografia, Autenticação, Autorização e Auditoria, sendo que:

Segundo STEEN e TANENBAUM (2007) criptografia é uma ferramenta imprescindível nas redes de computadores, para evitar problemas como interceptação, intervenção e modificação dos dados, pois essa ferramenta é capaz de modificar o conteúdo dos arquivos de certa forma que somente o destinatário do arquivo é capaz de remontá-lo novamente, dessa forma um arquivo criptografado mesmo se for interceptado não poderia ser lido, e nem corrompido por um invasor, e se por algum motivo fosse modificado o destinatário perceberia na hora de remontar esse arquivo, sabendo então que houve algo errado com essa informação.

Conforme STEEN e TANENBAUM (2007), na autenticação o usuário é obrigado a colocar um nome de usuário e uma senha para reconhecer a sua identidade corretamente, somente quem sabia daquela senha e estivesse liberado a acessar poderia ver as informações.

Ainda segundo STEEN e TANENBAUM (2007) temos a Autorização, dentro cada configuração de usuário é colocado também o que esse usuário pode acessar no sistema, e somente aquilo que lhe é permitido é liberado, deixando assim o usuário somente com acesso ao que realmente lhe interessa nas informações.

E por último de acordo STEEN e TANENBAUM (2007) temos a Auditoria, que na verdade não age diretamente para evitar um problema de segurança, e sim existe para ajudar na identificação de quem cometeu a invasão e o que foi feito de diferente neste sistema.

2.3.1 Criptografia

Do grego significa “Escrita Secreta”, e segundo TANENBAUM (2003) a utilização de criptografia mais famosa e que deu mais certo na história foi quando os Estados Unidos usaram um idioma indígena para se comunicar entre suas tropas, assim os Japoneses não conseguiram entender as mensagens e foram surpreendidos em várias ocasiões.

Ainda segundo TANENBAUM (2003), a criptografia é uma técnica muito utilizada, principalmente por militares muito antes da informática se difundir como atualmente. Porém a limitação da criptografia antes dos computadores sempre foi o trabalho que dava criar a mensagem, depois convertê-la manualmente para um dado criptografado, enviar a mensagem, e do outro lado descriptografar, para que possa entender o que estava escrito, isso somado ao grande quantidade de informações que deveriam ser transmitidas, principalmente em uma guerra fazia com que muitas pessoas fossem mobilizadas para atuar nessa tarefa.

Outra dificuldade segundo TANENBAUM (2003) foi criar criptografias novas toda vez que houvesse a desconfiança de que a antiga deixou de ser sigilosa. Até que *Kerkhoff*, elaborou o sistema de chave, ou seja, o algoritmo que gera a criptografia é público, o que é secreto é a chave (*string* que contém a forma como aquele dado deve ser decodificado).

Segundo STEEN e TANENBAUM (2007), na informática não é diferente, a mensagem passa por um algoritmo que codifica, obedecendo aos padrões pré-estabelecidos pela chave de segurança, em seguida essa mensagem é enviada ao destinatário, quando o destinatário recebe essa informação, ele já possuí uma chave semelhante à de codificação, para que aconteça o processo de decodificação dessa mensagem.

Segundo STALLINGS (2005), existem alguns algoritmos de criptografia, porém os mais utilizados são *Data Encryption Standard (DES)* e *Advanced Encryption Standard (AES).* Ainda segundo STALLINGS (2005), o *DES* foi predominante desde sua criação em 1977, porém só suporte chaves de segurança de no máximo 56 *bits*, o que passou a ser pouco seguro, levando-se em conta que devido à velocidade de processamento dos computadores atuais em algumas horas todas as combinações possíveis já teriam sido testadas e a mensagem não seria mais secreta.

Já o *AES*, de acordo com STALLINGS (2005) veio para substituir o *DES* que atualmente é algo obsoleto. Essa nova ferramenta suporta chaves de até 256 *bits*, tornando a descoberta por força bruta (tentativas de todas as combinações possíveis visando descobrir a lógica do algoritmo) muito mais complexa que a anterior.

Existem vários tipos de chaves de segurança citados de acordo com STALLINGS (2005), o tipo mais comum é o de chaves simétricas, ou seja, os dois computadores emissor e receptor da informação devem ter a mesma chave. Neste caso a alteração da chave constantemente é fundamental para garantir a segurança, e o sigilo das partes com relação aos dados dessa chave também são imprescindíveis para o funcionamento seguro do sistema, conforme figura a seguir.

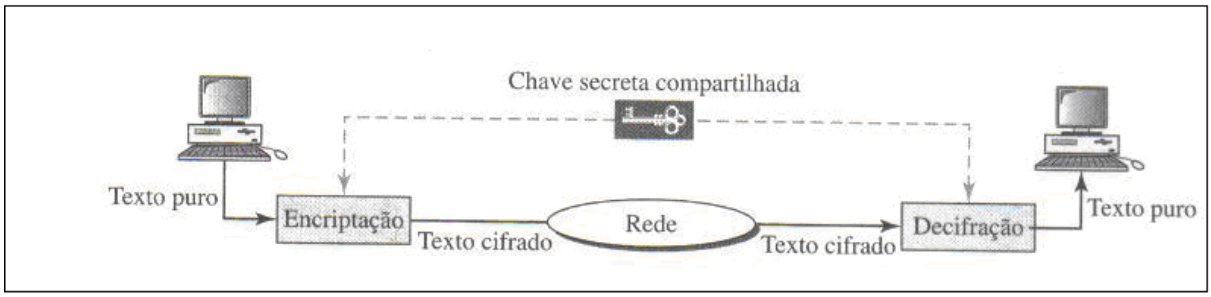


Figura 3 - Processo de envio de informação criptografada

2.3.2 ISO (International Organization for Standartization) Certificação de Segurança

De acordo com o site da *ISO (International Organization for Standartization – Organização Internacional de Normalizações)*, a *ISO* é o órgão não governamental que mais contribui para a padronização de métodos, processos do mundo. Com sede do secretariado em Genebra na Suíça, conta com a participação de cento e sessenta e um países representados por uma pessoa. Os órgãos membros estão ligados aos governos de seus respectivos países, porém seus representantes são diretamente envolvidos com o setor privado, gerando assim uma visão ampla, com pontos de vista de todas as partes envolvidas nos processos.

Na área de segurança de redes de computadores existem duas normas vigentes, são elas *ISO17799* e *ISO27001*.

Segundo a norma *ISO 17799*, que é um código de prática para gestão da segurança de informações, as informações contidas nessa norma servem como recomendações para aumentar a segurança, e garantir a rastreabilidade da rede de computadores.

Segundo a norma *ISO 27001*, que são Técnicas de segurança — Sistemas de gestão de segurança da informação têm em vista parametrizar a segurança da informação para a certificação, que é o processo de excelência da área de atuação.

2.3.3 IETF (Internet Engineering Task Force) e RFC (Request for Comments)

Segundo o site da *IETF - Internet Engineering Task Force (Força Tarefa Aplicada a Internet)* é uma comunidade aberta para usuários, pesquisadores, desenvolvedores, e pessoas em geral com o intuito de contribuir para a melhoria da internet, evolução da arquitetura e da segurança.

Ainda segundo o site da *IETF, RFC – Request for Comments (Pedidos de Comentários)* são as normas criadas pelas equipes técnicas da *IETF*, através de fóruns e grupos de discussões, e servem como referência para utilização, configuração e análise de segurança.

2.3.4 Firewall

Segundo KUROSE e ROSS (2006), *firewalls* são a combinação de *software* e *hardware* configurados para separar a rede interna de uma empresa da internet, através de uma filtragem dos dados que entram e saem passando por ele, onde esses dados são verificados e descartados se forem pouco seguros ou permitidos se forem conhecidos ou se não houver nenhuma regra que os impeçam de transitar na rede. Em analogia a um castelo medieval o *firewall* serve como uma muralha com um portão, somente acessam o castelo quem puder passar pelo portão. Para o perfeito funcionamento destes equipamentos, existem duas camadas que compõem o *firewall*.

Segundo STEEN e TANENBAUM (2007) os *firewalls* são divididos em duas partes, que se completam na segurança das redes, *gateways* de filtragem de pacotes que são responsáveis por verificar todas as informações que trafegam na rede, selecionando se os pacotes podem ou não ser entregues no destino, essa verificação é superficial onde somente os cabeçalhos dos pacotes são verificados com o intuito de barrar pacotes não autorizados. A outra parte do *firewall* são os *gateways* de nível de aplicação, esses são responsáveis pelo conteúdo dos pacotes, verificando a segurança das informações que entram e saem. Em casos específicos o *gateway* pode servir para filtrar *spams* em servidores de *e-mails*. Outro caso comum é o *proxy gateway*, que controla a navegação na internet tornando-a mais segura.

A figura 4 ilustra o funcionamento do firewall, que separa a *LAN* da Internet.

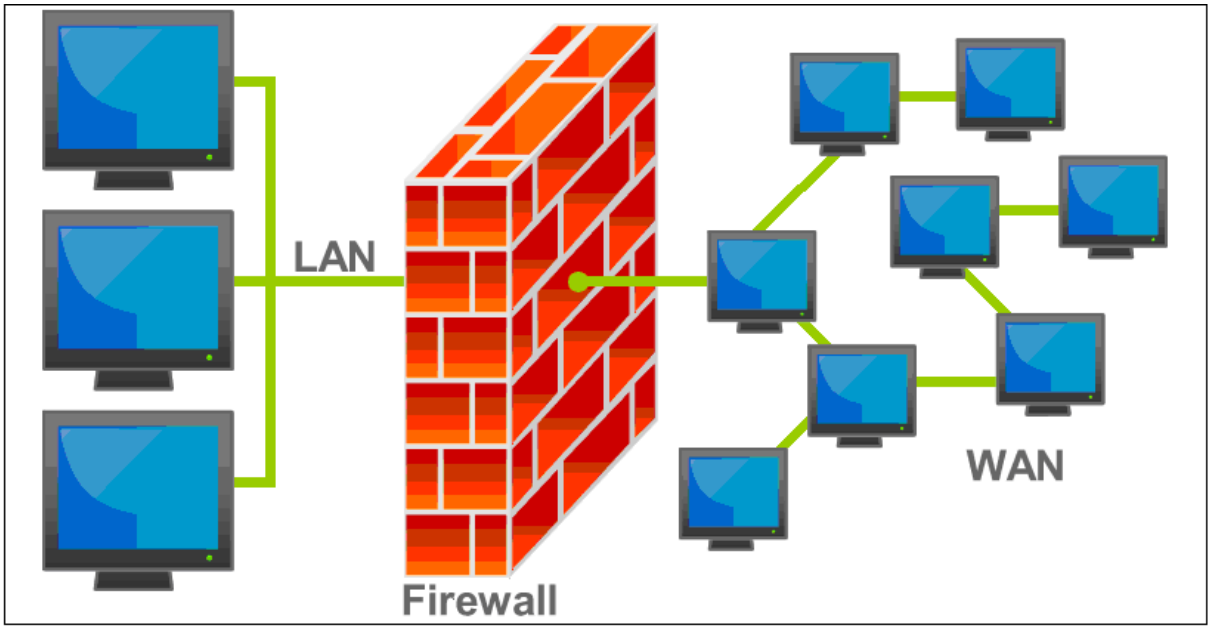


Figura 4 - Ilustração do funcionamento de um firewall

2.3.5 VPN (Virtual Private Network)

De acordo com STALLINGS (2005), *VPN (Virtual Private Network – Rede Privada Virtual)*, é uma forma de conectar duas ou mais redes através de um meio não seguro como a internet, por exemplo, gerando uma conexão livre de invasões e demais falhas de segurança que já foram citadas acima.

Segundo TANENBAUM (2003), o surgimento das *VPNs* aconteceu devido à necessidade de algumas empresas com escritórios separados fisicamente necessitarem de uma conexão segura para transmitir suas informações, sendo que até então existiam duas formas de fazer essa transferência, a primeira era através de linhas telefônicas, criando-se assim as redes privadas, custo elevado e segurança garantida. A segunda forma era transmitir essas informações pela internet correndo o risco de tê-las interceptadas.

De acordo com TANENBAUM (2003), como solução de baixo custo e alta eficiência surgiram então as *VPNs*, seguindo o conceito principal de Rede Privada, que não recebia acesso externo, a *VPN* não pode ser acessada por alguém de fora, funciona como se fosse um túnel entre dois *firewalls*, transportando as informações pela internet sem que elas possam ser interceptadas por outras pessoas.

A figura 5 mostra um exemplo de redes diferentes que se interligam através de uma *VPN*.

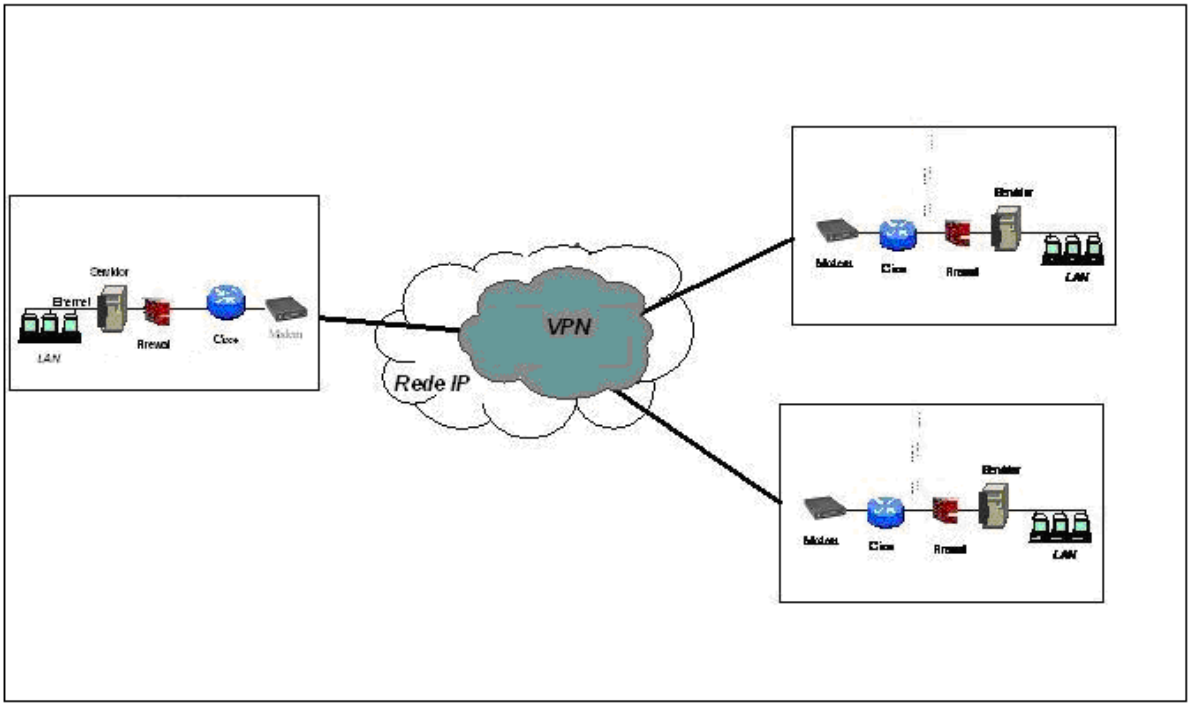


Figura 5 - Redes interligadas via *VPN*

2.3.6 IPSec (Internet Protocol Security)

Durante anos, segundo TANENBAUM (2003) a internet tinha carência de uma forma segura de transmitir informações, porém especialistas discutiam como implementar essa segurança, já que a idéia de muitos desses especialistas era criar uma serie de mudanças na hierarquia de camadas do protocolo *TCP/IP* gerando assim uma mudança muito grande no protocolo como um todo, ou então gerando modificações em todos os programas na rede para que assim fosse implementado o projeto de segurança. Porém isso não ocorreu, e o que houve no lugar disso tudo foi a criação do *IPSec*, que é uma verificação dos dados e criptografia das informações antes delas saírem para a rede e descriptografia e nova verificação dos dados antes deles entrarem novamente no computador, gerando assim uma garantia maior que não chegaram dados errados, e uma maior capacidade de descobrir onde essa informação foi alterada se for o caso. Para o caso do usuário não precisar de segurança, existe o algoritmo nulo que não gera criptografia nem verificação dos dados. O *IPSec* oferece três serviços a escolha do usuário sigilo, proteção dos dados e proteção contra ataque para reproduzir as informações contidas nas mensagens. Sua criptografia é de chave simétrica visando desempenho e possui vários algoritmos visando não depender de uma única forma de criptografia que pode ser descoberta a qualquer instante.

Segundo COMER (2006), o *IPSec* foi criado pela *IETF* para ser um protocolo flexível, permitindo autenticação assimétrica (de um lado somente da conexão), que os pares contidos na transmissão de dados escolham o tipo de chave criptográfica que iram trabalhar, operar com o *IPv4* e *IPv6*, entre outras facilidades.

Ainda segundo COMER (2006), é importante deixar claro que *IPSec* não é um protocolo isolado de segurança, e sim um conjunto de algoritmos que permite que os pares se comuniquem usando sua própria criptografia e seu próprio modo de utilização.

Conforme TANENBAUM (2003) existem dois modos de utilização do *IPSec*, o Modo Transporte inclui um cabeçalho antes do cabeçalho do *IP*, neste novo cabeçalho vão informações sobre a segurança e uma verificação de integridade dos dados. No Modo Túnel, o pacote *IP* é colocado dentro de uma cápsula que recebe uma outra identificação *IP* totalmente diferente, direcionando essa informação para um *firewall* da rede para onde essa informação vai, sendo esse *firewall* o responsável por desencapsular a informação e redirecioná-la para quem deve recebê-la dessa forma os computadores não tomam conhecimento da criptografia, a responsabilidade é toda do *firewall* da rede.

2.3.7 Malware

Termo extraído das palavras em inglês *Malicious Software*, o *malware* segundo FIGUEIREDO, é um programa malicioso que de forma ilícita é instalado no computador e causa danos ou roubo de informações. Programas legais que por falha de programação (intencional ou não) causem roubo de dados ou danos ao computador também se enquadram no grupo de *malwares*.

Ainda segundo FIGUEIREDO, os *malwares* são divididos em alguns tipos, Vírus (programa que se instala e se propaga como um vírus biológico buscando danificar equipamentos), *Worm* (do inglês verme, ao contrário do vírus que depende de um programa para ele infectar o *worm* já é esse programa, logo o torna independente, o estrago e finalidade são muito parecidos com o dos vírus), *Trojan horse* (em português, Cavalo de Tróia se aloja a algum programa que quando executado abre portas de acesso para controle externo do computador infectado), *Adware* (trazem propagandas na tela do computador contra vontade do usuário), *Bot* (são softwares responsáveis por se passar por humanos, ou seja, eles fazem coisas na internet como se fosse um humano navegando na internet, porém muito mais rápido, são utilizados para derrubar servidores), *Backdoor* (executa em segundo plano, buscando informações privilegiadas do sistema como um todo), *Hijacker* (em português, sequestradores

são responsáveis por alterar informações de pagina inicial, ou redirecionamento de páginas na internet visando aumentar a quantidade de acessos e cliques em sites específicos e assim ganhar dinheiro), *Hoax* (são as famosas correntes que contaminam as caixas de entrada de e-mails com histórias fantasiosas, falsas caridades), *Keylogger* (são instalados no computador como cavalos de tróia e visam captar todas as informações digitadas, como senhas de banco, números de contas bancárias, enviando essa informação para o criador da ferramenta), *Phishing* (é a busca no computador por informações privilegiadas como números de cartão de crédito, números de conta bancaria, senha de banco, o *keylogger* é uma forma de *Phishing*), *Rootkits* (programas que rodam camuflados no Sistema Operacional do computador, verificando solicitações e até mudando os resultados, de acordo com o interesse do criador dessa ferramenta).

2.4 Gerenciamento de Redes

Segundo STALLINGS (2005), gerenciar redes de computadores com o crescimento e a complexidade das mesmas atualmente se torna cada vez mais difícil, deixando de ser possível de se fazer manualmente, e se tornando cada vez mais necessário o uso de ferramentas automatizadas para exercer essa função.

De acordo com KUROSE e ROSS (2006) gerenciamento de rede é tão importante para a segurança das informações de uma empresa quanto, o gerenciamento de um avião pelo piloto que acompanha os equipamentos no painel do avião para detectar algum problema que possa acontecer durante o vôo. O administrador da rede deve ficar atento a algumas áreas pré-estabelecidas, visando detectar possíveis problemas.

Ainda segundo STALLINGS (2005), existem requisitos estabelecidos pelas normas *ISO* que ajudam a pontuar as áreas a serem gerenciadas, são elas:

- Gerenciamento de Falhas: Para que haja um melhor aproveitamento das ferramentas de rede, é necessário que o sistema funcione perfeitamente, mas para o caso de se ocorrer uma falha, que é diferente de um erro, pois, no caso da falha acontece intermitentemente oscilando o funcionamento da rede e o erro acontece e interrompe o funcionamento definitivamente da rede, é necessário localizar a falha, isolar ela do restante da rede, permitir que a rede funcione da melhor maneira possível sem aquele ponto que está sofrendo falhas, detectar os motivos e corrigir o problema para que não haja perda de

informações nem de desempenho na rede. Para o usuário o importante é que a rede se mantenha operacional e confiável.

- Gerenciamento de Contabilidade: Para que haja uma otimização da utilização da rede, é necessário que o gerente da rede conheça a utilização da rede de seus usuários visando verificar se não há abusos nos privilégios de acesso da parte de usuários fazendo com que eles sobrecarreguem a rede, permitindo também analisar se o sistema não está fazendo processos redundantes, ou ineficientes e se a segurança necessária para as informações está sendo suficiente. Para o usuário é importante que o sistema lhe entregue as informações da maneira mais rápida e com segurança necessária para se confiar nesses dados.
- Gerenciamento de Configuração e Nome: Para que haja um melhor aproveitamento de todos os dispositivos da rede, é necessária uma configuração feita da maneira certa, para aperfeiçoar os resultados desse dispositivo, e cabe ao gerente de configuração de rede, analisar a melhor maneira de se configurar esse dispositivo, também cabe ao gerente perceber se a necessidade de desligar parte ou toda a rede para essa configuração e se necessário o desligamento, fazê-lo da melhor maneira possível, tendo em vista que para o usuário é fundamental que o sistema não pare, e que as modificações sejam informadas para que o serviço seja adaptado de acordo com a modificação feita.
- Gerenciamento de desempenho: Para que haja uma melhor utilização da rede por parte dos usuários, é necessário que o desempenho das aplicações seja verificado, para essa análise existem o monitoramento e o controle, que permite ao gestor verificar como anda o desempenho da rede e modificar algumas configurações caso existam problemas, respectivamente. No campo do monitoramento o gestor da rede tem que verificar através de relatórios e estatísticas de desempenho, se o tempo de espera do usuário final vem aumentando, ou se o processamento das informações está comprometido e dessa forma deve analisar as possíveis causas para o problema, e utilizar o controle sobre a rede para fazer as alterações necessárias para que seja resolvido o problema, pois para o usuário é imprescindível que o sistema de respostas em tempo aceitável de utilização.

- Gerenciamento de Segurança: Para que haja confiabilidade nos dados de um sistema é necessário saber que esse sistema é seguro, para ter essa certeza existem ferramentas que ajudam na segurança das informações, como criptografia, controle de acesso, *logs* de atividades, e cabe ao gestor da rede administrar todas essas ferramentas para que o sistema se mantenha funcionando e seguro como deve ser. Para o usuário é fundamental que essa segurança não falhe, pois disso depende a confiança nas informações contidas nesse sistema.

2.4.1 SNMP (Simple Network Management Protocol)

De acordo com DAVIE e PETERSON (2004), quando se trabalha com muitos hosts espalhados, a única forma de gerenciar o funcionamento afim de verificar e corrigir falhas de hardware ou software, é utilizando a própria rede para isso.

Ainda conforme DAVIE e PETERSON (2004) o protocolo mais utilizado para esse tipo de gerenciamento é o *SNMP (Simple Network Management Protocol – Protocolo de Gerenciamento de Rede Simples).*

Segundo STALLINGS (2005) o *SNMP* está dividido em quatro partes que são:

- **Estação de Gerenciamento:** Serve como interface para o gestor da rede acessar as ferramentas de gestão, no mínimo ela deve ter aplicações de gerenciamento de dados, recuperação de falhas, análise de informações da rede, visando auxiliar o gestor ampliando as informações do funcionamento da rede. Interface para o usuário controlar a rede, monitorando acessos, solicitações, falhas, segurança, para subsidiar a tomada de decisões do gestor. Capacidade de implementar as modificações que o gestor fizer no sistema para a realidade da rede. Uma base de dados completa de todos os pontos da rede, que armazene tudo que foi feito em relação à gestão de rede em qualquer parte gerenciada. Sendo esses dois últimos necessários para a padronização do *SNMP*.
- **Agente de Gerenciamento:** É o software instalado em hosts, roteadores, hubs, ou qualquer outro dispositivo da rede, que tem o intuito de dar acesso a informações necessárias na gestão da rede, e também manter a estação gerenciamento informada com os dados de rede do equipamento *(MIB)*.

- **Informações de Gerenciamento *(MIB)*:** O *MIB* auxilia o gestor através da estação de gerenciamento a tomar medidas e decisões para melhorar o desempenho a segurança e a confiabilidade da rede.
- **Protocolo de Gerenciamento de Rede:** Interliga os agentes à estação de gerenciamento, chamado de *SNMP*, tem uma versão melhorada para ser usada em redes *TCP/IP* e *OSI* conhecido como *SNMPv2*. Esse protocolo é composto das funções de *Get* (a estação de gerenciamento busca informações nos agentes), *Set* (a estação de trabalho define um valor especifico para algum dado de algum agente) e *Notify* (O agente envia informações não solicitadas, que possam ter alguma relevância para a estação de gerenciamento).

Com base em FOROUZAN (2008) a tarefa de gerenciamento *SNMP* é composta por três protocolos que trabalham juntos, são eles:

- *SNMP (Simple Network Management Protocol):* Define padrões no diálogo entre agente e gerente, recebe resultados, geram estatísticas, mostra informações ao usuário;
- *SMI (Structure of Managed Information):* Padroniza as regras do gerenciamento, evitando divergências devido às diferenças dos *hosts* analisados;
- *MIB (Management Information Base):* Busca informações nos agentes e as organiza, para enviar ao gerente respeitando as regras e padrões estabelecidos pelo *SMI.*

Segundo STALLINGS (2005), para redes pequenas e médias um *host* é designado como estação de gerenciamento e todos os outros equipamentos são agentes, porém conforme a quantidade de agentes aumenta, criam-se problemas de excesso de trafego, como relatórios, notificações, que são enviados constantemente pelos agentes á estação de gerenciamento, isso acaba prejudicando o desempenho da rede como um todo, verificando-se então a necessidade de descentralizar as informações, ou seja, criar subestações de gerenciamento interligadas ao gerenciador principal, as informações vão até as subestações, e essa subestação que envia relatórios para a estação principal diminuindo assim o fluxo de dados cruzando a rede toda para chegar à estação principal.

2.5 Auditoria

Segundo o dicionário Aurélio On-Line, auditoria é o ato de examinar formalmente operações de uma empresa gerando relatórios imparciais especializados que auxiliam na correção de problemas apontando erros e aperfeiçoando operações.

De acordo com LUDWIG e SILVA, as empresas atualmente padronizam métodos e processos visando atender suas necessidades de negócios, tornando imprescindível para o bom funcionamento do sistema, e para retirada de informações precisas e confiáveis que controles internos sejam criados, para que as rotinas sejam cumpridas a risca é necessário criar controles internos de procedimentos.

De acordo com DAVIS, SCHILLER e WHEELER (2007 apud LUDWIG e SILVA), o papel da auditoria é verificar esses controles, visando detectar falhas de segurança, ou a necessidade de aprimoramentos nessas rotinas.

Ainda segundo esses autores, os tipos de controles se dividem em três partes, que são:

- Prevenção: São aqueles controles que permitem evitar algum acontecimento contra o sistema, como pedir autenticação para evitar que pessoas não autorizadas acessem informações importantes e sigilosas no sistema.
- Detecção: São aqueles controles que permitem visualizar o que aconteceu com o sistema, detectando invasões, acessos indevidos, falhas de sistema, como exemplos deste tipo de controle existem os arquivos de *LOG*, que armazenam informações de acesso ao sistema permitindo verificar o que aconteceu, a hora e o usuário envolvido no evento.
- Reação: São aqueles controles que não impedem que aconteça algo ao sistema, porém servem para identificar o problema e dão subsídios para a solução, permitindo assim que o sistema permaneça o menor tempo possível instável ou parado.
- Também segundo DAVIS, SCHILLER e WHEELER (2007 apud LUDWIG e SILVA), as implementações ocorrem de três maneiras, que são:
- Administrativa: São as políticas que regem o funcionamento do sistema, ou seja, são responsáveis pela padronização da forma de utilizar o sistema em uma empresa. Um exemplo é o padrão utilizado para senhas como a quantidade de caracteres, essa política visa aumentar a segurança dos usuários, e do sistema, pois evita a quebra de senhas facilmente.

- Técnicas: São as políticas que verificam se as políticas administrativas estão sendo seguidas à risca, um sistema de verificação do padrão das senhas como o *Microsoft Active Directory (AD)* é um exemplo dessas políticas.
- Físicas: São as políticas responsáveis pela segurança física, ou seja, pela segurança de servidores, *switchs*, roteadores, computadores. Portas de acesso para servidores, *racks* trancados a chave, proteção de energia elétrica, são exemplos de políticas de segurança física.

2.5.1 Fases da Auditoria

De acordo com DAVIS, SCHILLER e WHEELER (2007 apud LUDWIG e SILVA), a auditoria é dividida em seis fases principais, sendo elas descritas abaixo:

- Planejamento: É nesse ponto que começa a surgir os procedimentos que serão adotados pela auditoria, cria-se um escopo do que será auditado e a forma como os dados serão auditados na empresa, uma decisão tomada errado neste ponto compromete o restante do projeto.
- Pesquisa e Documentação: É a parte mais trabalhosa e, portanto, a mais demorada do processo, o auditor analisa todos os processos seguindo o planejamento inicial e cria um relatório detalhado sobre cada área especifica, verificando prováveis falhas de segurança, pontos críticos e pontos que merecem atenção.
- Descoberta e Validação: O auditor em parceria com o responsável pela área auditada deve analisar o levantamento criado, visando pontuar os reais riscos, e processos que podem afetar as regras de negócio prejudicando os resultados do sistema.
- Desenvolvimento de Soluções: É nesse ponto que o auditor começa a criar os planos para resolução dos problemas encontrados e validados com os responsáveis, as soluções encontradas pelo auditor são sugeridas ao responsável pelo departamento que tem a obrigação de escolher a mais adequada, o projeto de solução tem que ser claro e específico discriminando quem deverá fazer o que, deixando claro nome e cargo dos envolvidos e atribuindo uma data limite para o término do processo e entrega dos resultados.

- Relatório: Esse documento visa discriminar todos os passos do processo a fim de registrar tudo que foi encontrado de problema e quais foram às soluções sugeridas e tomadas para resolução. Obrigatoriamente o relatório tem que conter três informações essenciais, que são o escopo deixando claro o que foi verificado durante a auditoria, e esclarecendo também o que não foi verificado, o sumário que contem um resumo da auditoria com os principais problemas encontrados e as medidas sugeridas para cada problema, e por último a lista de problemas onde se pontua detalhadamente todos os problemas encontrados e quais ações foram tomadas para solucioná-los.
- Acompanhamento: Não basta para o auditor encontrar os problemas, cabe a ele também acompanhar o processo de solução e cobrar os resultados, portanto nessa etapa o auditor marca reuniões periódicas com os responsáveis, visando se interar do andamento do processo, cobrar atrasos, e corrigir possíveis desvios que o processo de solução possa tomar.

2.5.2 Governança de TI (Tecnologia da Informação)

Segundo HANASHIRO (2007), Governança de *TI* é o conjunto de processos que tem por interesse fazer a *TI* administrar e melhorar as estratégias e o desempenho de negócio da instituição. Algumas empresas criaram normas para aplicação de governança em suas instituições, serão citadas duas que são as mais populares.

De acordo com ISACA (2000 apud HANASHIRO 2007) o *COBIT (Control Objectives for Information and related Technology - Objetivos de Controle de Tecnologia de Informação e afins)* é uma metodologia que visa pesquisar, desenvolver, publicar e promover normas de padronização internacional de práticas capazes de aumentar o aproveitamento para gerentes de *TI* e auditores do setor corporativo.

Conforme ISACA (2000 apud HANASHIRO 2007) a metodologia *COBIT* que é considerada a base da governança em *TI*, foi criada pela *ISACA (Information Systems Audit and Control Association - Associação de Controle e Fiscalização de Sistemas de Informação)* organização independente que cria documentos com normas para auxiliar empresas na área de segurança e infra-estrutura.

Segundo HANASHIRO (2007), dentro da metodologia *COBIT* estão documentados desde o início do projeto, passando pela fase de implementação, a administração dos

processos, a correção de falhas, detalhadamente para auxiliar os gerentes de *TI* a obterem o melhor resultado possível da infra-estrutura, sistema e segurança da empresa.

Para fins parecidos segundo HANASHIRO (2007), existe também o *ITIL (Information Technology Infrastructure Library – Biblioteca de infra-estrutura de Tecnologia de Informação),* que foi criado pelo governo britânico no fim da década 1980 sendo reconhecido como padrão internacional somente no meio da década de 1990, visando o operacional e a gerência da infra-estrutura tecnológica da empresa. O *ITIL* entende que um serviço de *TI* é composto por várias regras e padrões de *TI* que devem ser seguidos para aumentar a excelência do serviço.

Ainda segundo HANASHIRO (2007), o *ITIL* visa principalmente a excelência no suporte a *TI*, da maneira mais eficiente e com custos justificáveis para a organização, aumentando a qualidade dos serviços sem perder o foco estratégico.

3 Metodologia

O projeto foi dividido em quatro partes fundamentais que são:

Pesquisa Bibliográfica onde aprofundou - se o conhecimento sobre o funcionamento específico de redes de computadores, riscos de segurança às redes de computadores, protocolos de funcionamento dessas redes, medidas a serem tomadas para aumentar a segurança, problemas causados por falta de segurança, ferramentas físicas para proteção dessas redes, softwares e configurações capazes de proteger essas redes, o funcionamento da internet e seus protocolos de transporte de dados, a utilização de sistemas integrados em redes de computadores. Estudo detalhado, visando o entendimento teórico e prático do tema abordado.

Classificação das ferramentas que foram utilizadas na parte prática do projeto, levando – se em conta a popularidade da ferramenta e o tipo de licença da ferramenta.

Parte prática onde parâmetros de análise foram determinados, tais como usabilidade, agilidade, queda no desempenho da rede, qualidade da ferramenta em funcionamento, com problemas reais citados durante a pesquisa, visando encontrar os pontos positivos e negativos de cada ferramenta analisada e para assim ao final poder comparar essas informações;

Análise dos resultados e elaboração das conclusões específicas de cada ferramenta e comparações entre as ferramentas analisadas.

Para a pesquisa e classificação das ferramentas foram utilizados como material de base artigos científicos, livros impressos, livros digitais, aulas universitárias.

Para a parte prática foi utilizada uma rede genérica de computadores, onde foi feita a simulação de utilização comum, que serviram de base para as análises e que foram listados em forma de tabela comparativa entre as ferramentas, e baseado nessas informações, surgiu à nota média de cada ferramenta.

3.1 Infra Estrutura do Teste

A figura 6 mostra a estrutura da rede onde foram feitos os testes.

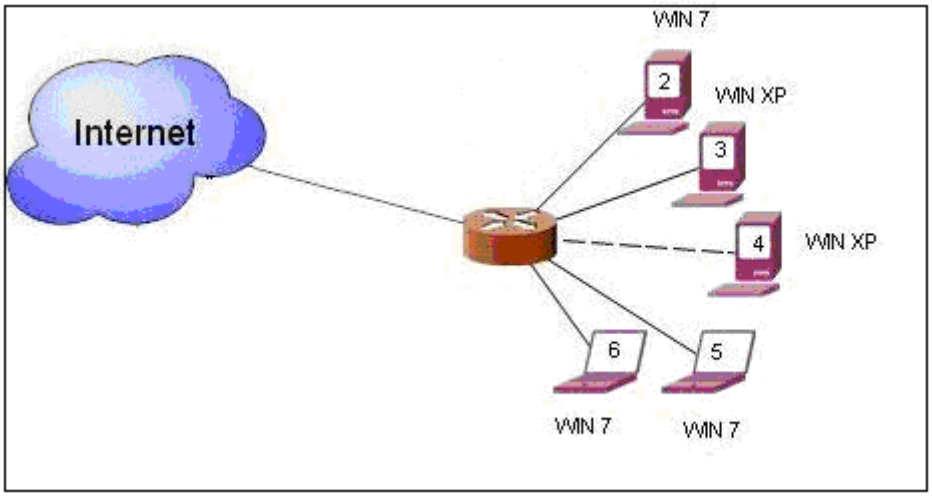


Figura 6 - Infra-estrutura do teste

A estrutura da rede é composta por cinco equipamentos, sendo eles, dois notebooks e três desktops, conectados à rede através de um roteador, tendo as configurações descritas na tabela abaixo.

Tabela 1 - Configurações dos computadores da rede

Equip.	Processador	Memória	HDD	S.O.	IP	Conexão
Desktop 2	Sempron	768 Mb	40 Gb	Windows XP	192.168.1.254	Cabo
Desktop 3	Celeron	768 Mb	80 Gb	Windows XP	192.168.1.150	Cabo
Desktop 4	Core 2 Duo	3 Gb	320 Gb	Windows 7	192.168.1.89	Cabo
Notebook 1	Dual Core	4 Gb	250 Gb	Windows 7	192.168.1.60	Sem fio
Notebook 2	Dual Core	3 Gb	160 Gb	Windows 7	192.168.1.58	Sem fio

Os computadores pertencentes a essa rede são originalmente para uso doméstico e estão adaptados para simular utilização corporativa, da mesma forma que os testes serão realizados focando o uso corporativo dos equipamentos.

3.2 Metodologia do teste

Para cada teste foi aplicada uma metodologia específica, pois se tratam de ferramentas úteis para diversos casos de gerenciamento de rede. Dessa forma para cada teste foi criado um anexo com o processo de instalação, configuração das ferramentas. As telas com resultados obtidos por cada uma delas foi apresentada e explicada em partes, para dessa forma classificar cada uma das ferramentas de acordo com os padrões estabelecidos neste projeto.

A primeira ferramenta foi o *MRTG – Multi Router Traffic Grapher*, que segundo o site do desenvolvedor, serve para analisar o tráfego na rede através do protocolo *SNMP*. Com o *MRTG* as informações são capturadas e transformadas em gráficos, o que facilita a visualização e a criação de relatórios para controle em empresas.

Ainda segundo o site do desenvolvedor, *MRTG* é um programa desenvolvido em *Perl*, linguagem que permite o funcionamento em várias plataformas como *Unix, Linux, Windows* e plataforma *Netware*.

Sua licença *GNU GPL*, permite que o usuário utilize seu conhecimento para alterar cópia e utilizá-la sem limitações, somente sendo proibido a venda de cópias originais ou modificadas.

O site da ferramenta contém informações para download, e instruções para a instalação e configuração. Dessa forma a instalação que não é muito simples fica mais fácil, e prática. O anexo A mostra a instalação e configuração passo a passo.

Para o teste utilizou - se a versão 2.16.2 para Windows XP e a versão 5.8.9.827 ActivePerl, que serve para o *MRTG* possa funcionar no Windows. Estas não são as últimas versões das ferramentas, porém elas são as versões testadas e totalmente funcionais, e são as versões sugeridas no tutorial do site.

A ferramenta foi instalada no computador que compartilha a internet com os outros da rede, dessa forma controla-se o tráfego de internet solicitado por todos os computadores da rede e quais horários o tráfego é maior.

Para uma empresa, essa ferramenta serve para analisar quanto de banda está sendo utilizado, e quais horários essa banda é utilizada. Para dessa forma saber se a rede atende as necessidades da empresa, se não existe tráfego indevido, ou fora dos horários permitidos.

A ferramenta mostra gráfico do trafego diário, semanal, mensal e anual, permitindo aos gestores de *TI* comparações de utilização entre os dias, as semanas, os meses e os anos.

Os gráficos permitem ao gestor de *TI* apresentar relatórios de utilização da rede de forma clara e agradável sem muito trabalho, já que eles são completos e bem apresentados.

Com relação ao funcionamento, é simples e prático basta terminar a configuração e já está disponível para visualização o primeiro gráfico com a análise até aquele momento. Para facilitar o acesso aos dados, foi configurado o *IIS (Internet Information Services)*, que é o servidor de internet nativo do Windows, para acessar as informações via *Browser*.

Em relação a desempenho quase não é possível notar o funcionamento da ferramenta no computador, pois ela fica em segundo plano e utiliza pouco processamento. No caso do

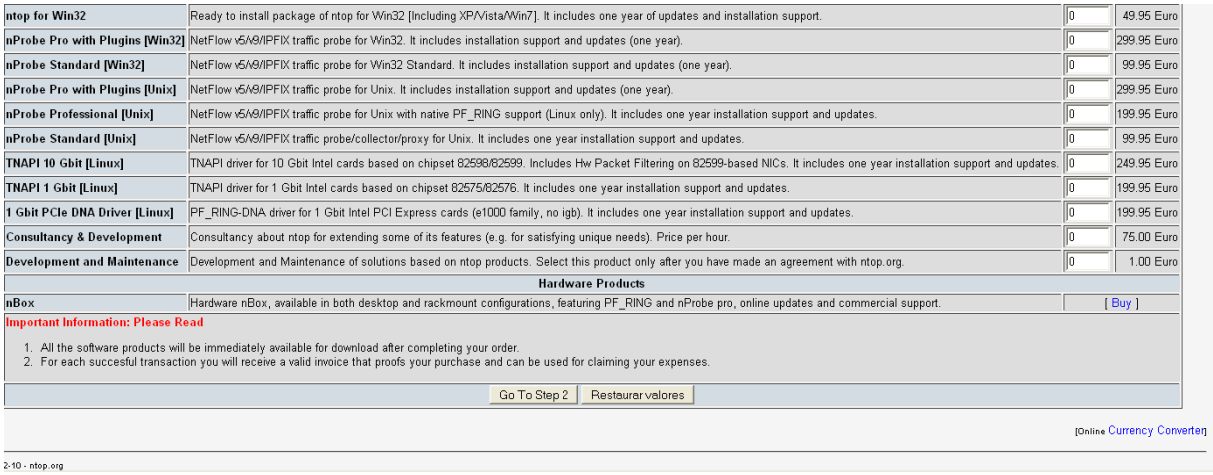
teste não foi possível perceber queda no rendimento da rede, pois são poucos computadores monitorados.

A segunda ferramenta foi o *Wireshark* que é uma ferramenta de análise de rede e permite ao usuário controlar o que trafega na rede, verificando pacote por pacote que navegue em cada protocolo de uma rede. Programa desenvolvido para trabalhar em vários sistemas operacionais, como *Linux, Unix, Windows, Solaris, FreeBSD* entre outros.

No teste foi utilizada a versão 1.2.12 para Windows XP. A instalação é simples, pois utiliza um assistente que instala e configura a ferramenta no computador. Para o funcionamento do *Wireshark* é necessário outro software *WinPCap*, que serve para fazer a interface do W*ireshark* e os pacotes de rede, dando ao programa um acesso de baixo nível à rede.

A versão instalada do *WinPCap* é a 4.1.2, utilizada em outras ferramentas que serão citadas, e acompanha o assistente de instalação do *Wireshark*, instalação que foi demonstrada no Anexo B.

A terceira ferramenta foi o *NTOP* que serve para analisar o tráfego da rede, gerando gráficos ilustrativos de utilização. Desenvolvida preferencialmente para funcionar baseada em *SMNP*, oferece uma quantidade significativa de informações para o usuário identificar exatamente o que está acontecendo em sua rede em tempo real. É possível encontrar para download as opções para o *Linux / Unix* e plataforma *Win32*, sendo que para o *Win32* existe um custo pelo licenciamento do produto de aproximadamente 50 euros, conforme figura 7.



ntop for Win32	Ready to install package of ntop for Win32 [Including XP/Vista/Win7]. It includes one year of updates and installation support.	0	49.95 Euro
nProbe Pro with Plugins [Win32]	NetFlow v5/v9/IPFIX traffic probe for Win32. It includes installation support and updates (one year).	0	299.95 Euro
nProbe Standard [Win32]	NetFlow v5/v9/IPFIX traffic probe for Win32 Standard. It includes installation support and updates (one year).	0	99.95 Euro
nProbe Pro with Plugins [Unix]	NetFlow v5/v9/IPFIX traffic probe for Unix. It includes installation support and updates (one year).	0	299.95 Euro
nProbe Professional [Unix]	NetFlow v5/v9/IPFIX traffic probe for Unix with native PF_RING support (Linux only). It includes one year installation support and updates.	0	199.95 Euro
nProbe Standard [Unix]	NetFlow v5/v9/IPFIX traffic probe/collector/proxy for Unix. It includes one year installation support and updates.	0	99.95 Euro
TNAPI 10 Gbit [Linux]	TNAPI driver for 10 Gbit Intel cards based on chipset 82598/82599. Includes Hw Packet Filtering on 82599-based NICs. It includes one year installation support and updates.	0	249.95 Euro
TNAPI 1 Gbit [Linux]	TNAPI driver for 1 Gbit Intel cards based on chipset 82575/82576. It includes one year installation support and updates.	0	199.95 Euro
1 Gbit PCIe DNA Driver [Linux]	PF_RING-DNA driver for 1 Gbit Intel PCI Express cards (e1000 family, no igb). It includes one year installation support and updates.	0	199.95 Euro
Consultancy & Development	Consultancy about ntop for extending some of its features (e.g. for satisfying unique needs). Price per hour.	0	75.00 Euro
Development and Maintenance	Development and Maintenance of solutions based on ntop products. Select this product only after you have made an agreement with ntop.org.	0	1.00 Euro
	Hardware Products		
nBox	Hardware nBox, available in both desktop and rackmount configurations, featuring PF_RING and nProbe pro, online updates and commercial support.		[Buy]

Important Information: Please Read

1. All the software products will be immediately available for download after completing your order.
2. For each succesful transaction you will receive a valid invoice that proofs your purchase and can be used for claiming your expenses.

Go To Step 2 | Restaurar valores

[Online Currency Converter]

2-10 - ntop.org

Figura 7 - Valor da licença *NTOP* em Euros, 16/11/2010
Fonte: http://www.nmon.net/shop/cart.php

Para o teste utilizou - se a versão para demonstração 4.0.3 para *Win32*, essa versão é limitada a montar gráficos e análises com no máximo 2000 pacotes.

A instalação da ferramenta é simples e não requer muito conhecimento técnico para a tarefa basta seguir o assistente, conforme Anexo C.

Para o funcionamento da ferramenta no Windows, foi necessário a instalação do *WinPcap*, a mesma versão utilizada para o *Wireshark.*

A instalação foi feita no computador que compartilha a internet com os demais micros da rede, com Windows XP e foi verificado o tráfego durante um período e os gráficos gerados analisam vários protocolos, mostrando em detalhes o funcionamento da rede.

Em ambiente corporativo, essa ferramenta ajuda a analisar o uso da rede permitindo ao gestor da rede, verificar o funcionamento e a utilização de cada protocolo, permitindo corrigir erros e monitorar uso excessivo, ou abusivo da rede.

A quarta ferramenta analisada foi o *NMAP (Network Maper)*, que serve para gerenciamento e auditoria de rede, analisa *host a host* da rede colhendo informações do sistema operacional e da rede, possibilitando o controle dos equipamentos.

Disponível para instalação em vários sistemas operacionais como *Linux / Unix, Windows, MAC OS*, entre outros. Oferece uma interface gráfica (*Zenmap*), que facilita a utilização por leigos, ou pessoas com pouco conhecimento na área.

Distribuído sob licença gratuita e com código aberto para modificações de acordo com a necessidade, licença *GNU GPL*.

Possuí uma documentação bem completa em vários idiomas, disponível no site do desenvolvedor da ferramenta.

Disponível por padrão em alguns sistemas operacionais como *FreeBSD* e *Linux Debian*, de acordo com o site do fabricante, milhares de downloads são feitos diariamente o que torna a ferramenta muito popular e com isso facilita ao usuário encontrar ajuda sobre configuração e utilização.

Para o teste utilizou-se o *Windows XP* e a versão 5.21 que necessita da ferramenta *WinPcap* para o funcionamento, a instalação é simples e rápida conforme Anexo D.

A última ferramenta testada foi a Ethereal, que é bastante parecida com o Wireshark, a utilidade prática da ferramenta é muito parecida com o Wireshark que permite ao usuário analisar os pacotes que trafegam pela rede, bem como o conteúdo dos pacotes, permitindo um controle maior dos dados que trafegam e facilitando a correção de possíveis erros em ambiente empresarial.

Ferramenta sob licença *GNU GPL* permite que desenvolvedores adaptem o código fonte para as suas necessidades, ou realizem melhorias para aprimorar o funcionamento do software, contribuindo para o aumento da qualidade da ferramenta.

Com versões para vários Sistemas Operacionais, o Ethereal conta com suporte para *Windows, Linux, Solaris, FreeBSD, Mac OS* entre outras opções. Segundo o site do desenvolvedor, atualmente a ferramenta reconhece e trabalha com mais de 750 protocolos diferentes, o que garante que a maior parte das informações serão reconhecidas durante a análise na rede. A instalação foi feita no Windows XP, o computador é o servidor de internet, e foram analisados os pacotes que trafegaram na rede durante um intervalo de tempo. Para o funcionamento da ferramenta é necessário que esteja instalado o *WinPcap*, caso não esteja o assistente de instalação possuí essa ferramenta inclusa. A versão utilizada nos testes foi a 0.10.14, a instalação é simples e prática conforme Anexo E.

3.3 Formas de classificação das ferramentas

A classificação das ferramentas será feita seguindo o padrão adotado pela revista INFO (2010), aonde as notas avaliativas vão de 0 a 10, sendo 0 a menor nota e 10 a maior nota.

Essa avaliação seguindo um padrão conhecido tem o intuito de facilitar ao leitor o entendimento da avaliação, bem como a interpretação dos resultados de forma clara e simples.

Abaixo a figura 8 mostra o modelo de classificação adotado no projeto que foi retirado da revista INFO (2010).

10,0	Impecável
9,0 a 9,9	Ótima
8,0 a 8,9	Muito bom
7,0 a 7,9	Bom
6,0 a 6,9	Médio
5,0 a 5,9	Regular
4,0 a 4,9	Fraco
3,0 a 3,9	Muito fraco
2,0 a 2,9	Ruim
1,0 a 1,9	Bomba
0,0 a 0,9	Lixo

Figura 8 - Tabela Notas Utilizada na Avaliação
Fonte: Revista Info (Julho/2010)

3.4 Resultados Obtidos

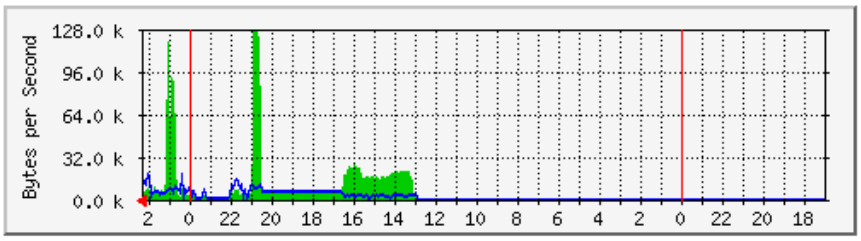
A primeira ferramenta testada foi o *MRTG* de acordo com a figura 9 que apresenta o resultado da análise durante um dia do computador responsável por compartilhar a internet para os computadores da rede utilizada nos testes.

Traffic Analysis for 2 -- ALEXANDRE

System: ALEXANDRE in
Maintainer:
Description: SiS-900-PCI-Fast-Ethernet-Adapter---Miniporta-do-agendador-de-pacotes
ifType: ethernetCsmacd (6)
ifName:
Max Speed: 12.5 MBytes/s
Ip: 192.168.1.254 (Alexandre)

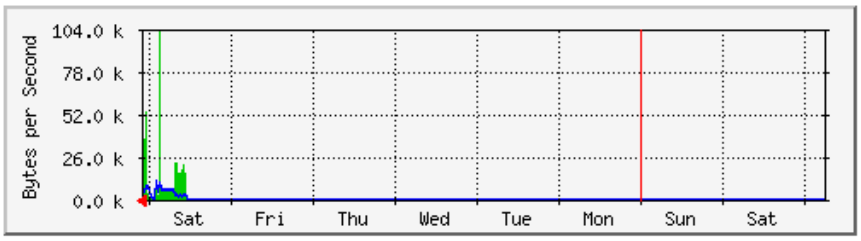
The statistics were last updated **Sunday, 7 November 2010 at 2:20**,
at which time '**ALEXANDRE**' had been up for **14:44:47**.

`Daily' Graph (5 Minute Average)



	Max	Average	Current
In	127.5 kB/s (1.0%)	14.7 kB/s (0.1%)	7960.0 B/s (0.1%)
Out	18.4 kB/s (0.1%)	4977.0 B/s (0.0%)	15.9 kB/s (0.1%)

`Weekly' Graph (30 Minute Average)



	Max	Average	Current
In	102.5 kB/s (0.8%)	14.4 kB/s (0.1%)	5569.0 B/s (0.0%)
Out	11.3 kB/s (0.1%)	4592.0 B/s (0.0%)	7038.0 B/s (0.1%)

Figura 9 - Resultados obtidos após um dia de análise

Dividida em três partes a figura 9 apresenta na primeira divisão um cabeçalho com as informações do computador que executa a ferramenta como o *IP* do computador, o nome da placa de rede, o nome do computador na rede e a velocidade máxima de conexão durante a análise.

Na segunda divisão nota-se a data da análise e um gráfico do volume de conexão no dia, dividido em colunas de duas horas, e com traços vermelhos separando os dias, o gráfico foi montado utilizando cores verdes para representas os pacotes que entram no computador, e cores azuis para os pacotes que saem do computador. Logo abaixo seguem três informações para cada sentido dos pacotes (entrada e saída), que são da esquerda para a direita a velocidade máxima de conexão aferida no período, a velocidade mínima de conexão e a média no intervalo. Percebe-se que o gráfico aponta dois picos de transmissão de dados às 21 horas do sábado e à 1 hora do domingo na entrada de dados. Na saída de dados o tráfego não excede muito a normalidade, fica basicamente na mesma média.

Na terceira divisão, verifica-se um gráfico semanal, onde as colunas de divisão são os dias da semana, e existe um traço em vermelho separando as semanas. Como no gráfico acima, existe a divisão de cores sendo verde a entrada de pacotes e azul a saída de pacotes. Como no gráfico diário também existe as informações de entrada e saída mínima, máxima e média. Verifica-se que o pico de informação acontece no fim do sábado para a entrada de dados, e uma transmissão média na saída de dados.

A segunda ferramenta testada foi o *Wireshark* que conforme a figura 10 mostra os pacotes transmitidos pela porta 80 do computador, detalhando a origem, destino, protocolo, e informando alguns detalhes sobre o pacote enviado ressaltando o controle de cores para cada tipo de pacote, neste caso os pacotes em verde foram transmitidos corretamente, os que aparecem em preto tiveram problemas na transmissão e estão sendo reenviados. Dessa forma um gestor de rede consegue acompanhar o tráfego de rede e verificar falhas no envio repetidas que podem acarretar em um problema de rede.

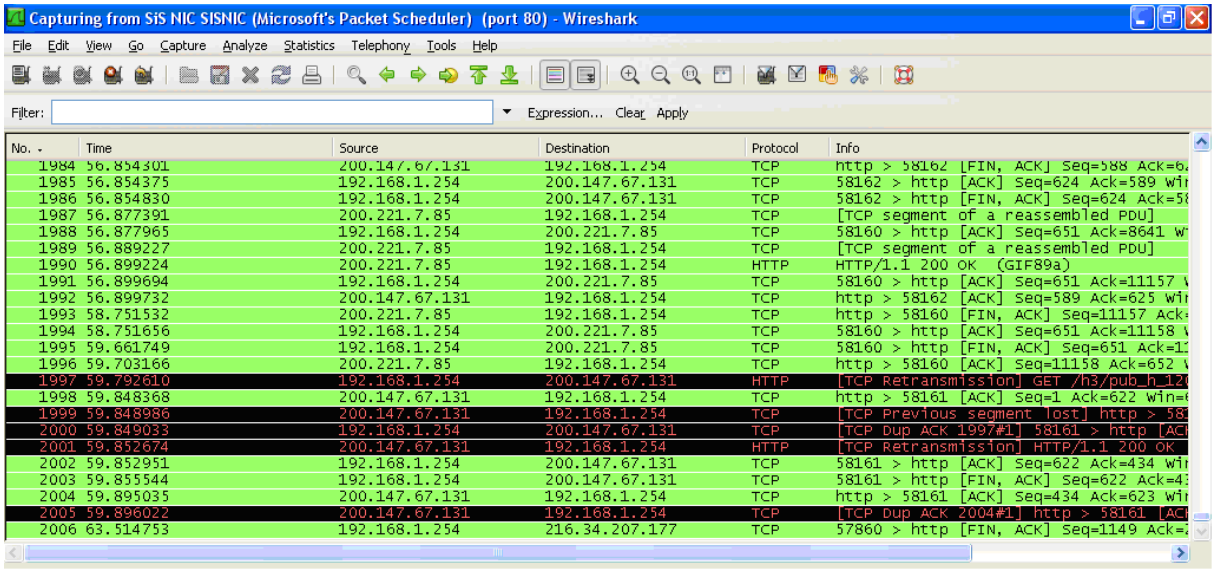


Figura 10 - Controle dos pacotes transmitidos

Percebe-se na Barra de Título o nome da placa de rede onde transitam as informações e a porta verificada.

Abaixo em verde e preto estão os pacotes enviados com sucesso, em preto e vermelho estão os pacotes que encontraram erro e por isso deverão ser reenviados.

As colunas da esquerda para a direita são Número que identifica qual é o numero do pacote. Time indica o tempo em segundo que o pacote foi transmitido em relação ao inicio do teste. Source mostra a origem do pacote, ou seja, qual *host* enviou o pacote para a rede. Destination é o destino do pacote, ou seja, para qual *host* vai o pacote. Protocol é o protocolo do pacote. Info é a descrição resumida da porta do pacote, se o envio foi correto, se o pacote foi reenviado.

Como mostra a figura 11, que demonstra a funcionalidade da ferramenta que permite abrir um pacote e verificar o que transitou no mesmo.

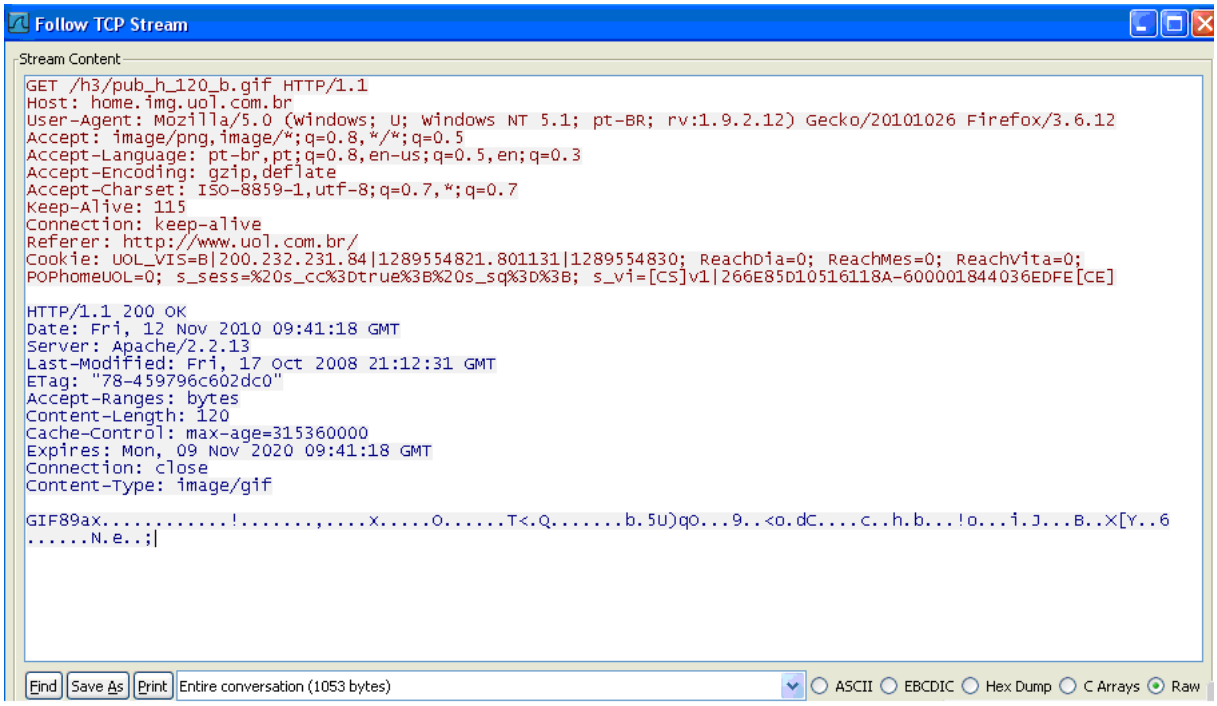


Figura 11 - Dados contido no pacote transmitido

Como visto na figura 11, esse pacote teve origem no servidor do *UOL* e contém um *GIF* referente ao site *http://www.uol.com.br*, foi transmitido no dia 12 de novembro às 9:41, a imagem tem 120 bytes, entre outras informações como a codificação, o navegador e outras informações interessantes para controlar o que trafega na rede. Podemos assim verificar o conteúdo dos dados entre usuários da rede.

Uma ferramenta bastante prática na instalação, basta executar o assistente e avançar até que termine. Para o funcionamento do *Wireshark* é necessário a instalação do *WinPCap* que já vem incluso no pacote de instalação.

A utilização é um pouco mais complicada, pois precisa configurar filtros, a placa de rede que será analisada. Na tela inicial do programa existe uma opção que oferece um tutorial passo a passo de como utilizar a ferramenta, porém esse tutorial é em inglês dificultando para quem não domina o idioma.

No teste notou-se que a ferramenta apresentou uma perda de desempenho considerável no computador onde estava instalada, exigindo processamento e travando o computador durante os testes, conforme figura 12. No desempenho de rede não existe perda, sendo que a ferramenta não atrapalha ou congestiona o tráfego normal.

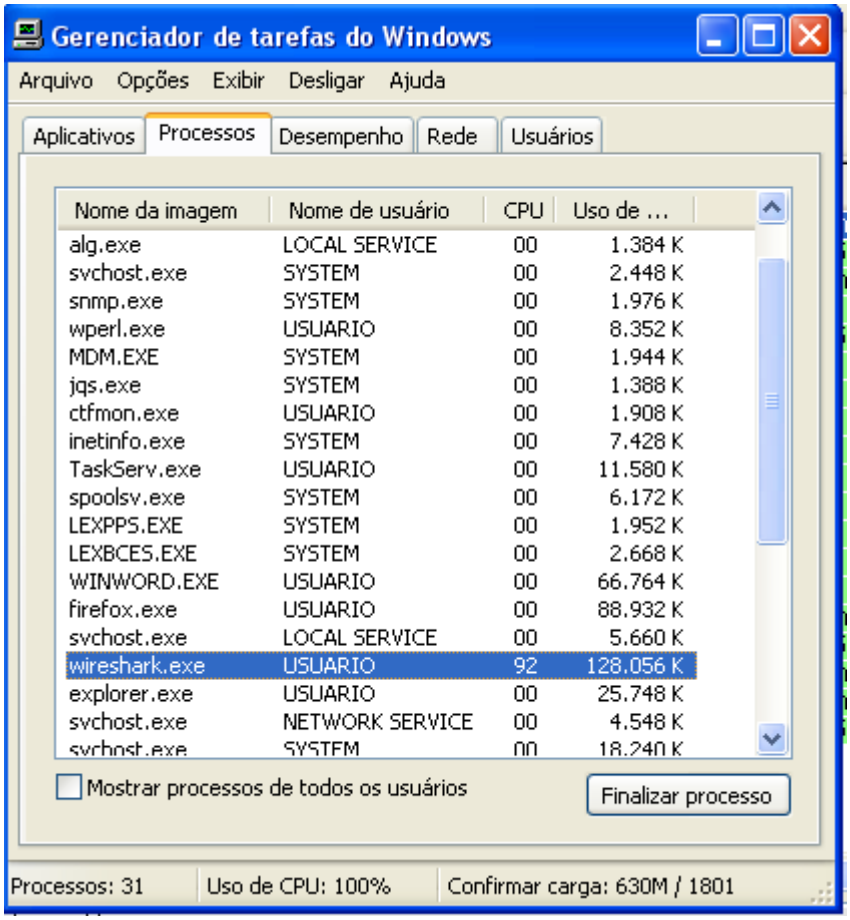


Figura 12 - Perda de desempenho utilizando o *Wireshark*

Conforme a figura 12 em destaque está o uso do processador para utilizar a ferramenta, se comparado com a utilização do *Firefox* e *Word*, é o dobro e um terço maior respectivamente.

Em ambiente corporativo esse teste visa identificar o trafego de pacotes entre computadores, permitindo então, analisar o que está sendo enviado de um computador para o outro e assim coibir abusos por parte dos usuários, ou até mesmo quebra de sigilo de informações.

A terceira ferramenta testada foi o *NTOP*, abaixo a figura 13 mostra a identificação da placa de rede utilizada no teste.

Network Interface(s)	Name	Device	Type	Speed	Sampling Rate	MTU	Header	Address	IPv6 Addresses
	SiS_NIC_SISNIC_0	_Device_NPF_{679F2A12-827D-4A5A-991C-43ED7C863028}			0	1514	14	192.168.1.254	
Sampling Since	Sun Nov 21 10:44:07 2010 [10:14:44]								

Figura 13 - Identificação da placa de rede utilizada no teste

De acordo com a figura 13, podemos observar o nome da placa de rede utilizada no teste, bom como o registro do dispositivo, o *IP* utilizado na placa.

A figura 14 mostra um gráfico com o tamanho dos pacotes transmitidos pela rede durante o teste

Packets	Shortest		54 bytes
	Average Size		298 bytes
	Longest		1,494 bytes
	Size <= 64 bytes	37.5%	749
	64 < Size <= 128 bytes	21.8%	435
	128 < Size <= 256 bytes	21.6%	432
	256 < Size <= 512 bytes	0.8%	15
	512 < Size <= 1024 bytes	0.2%	3
	1024 < Size <= 1518 bytes	18.3%	365
	Size > 1518 bytes	0.0%	0

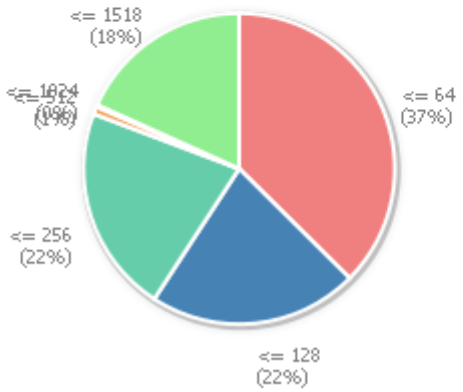


Figura 14 - Tamanho dos pacotes transmitidos na rede.

Na figura 14 podemos verificar que os pacotes pequenos (shortest) representam o menor fluxo de dados transmitidos como visto na primeira linha de informações da figura. Logo abaixo percebemos que os pacotes de médio porte (avarege size) representam 298 bytes de informação e os pacotes grandes (longest) representam mais de 1 Kb de dados. Mais abaixo podemos ver a quantidade de pacotes transmitidos de acordo com o tamanho e o gráfico ilustrando essas informações.

A figura 15 mostra a quantidade de pacotes de cada protocolo trafegaram pela rede durante o tempo do teste.

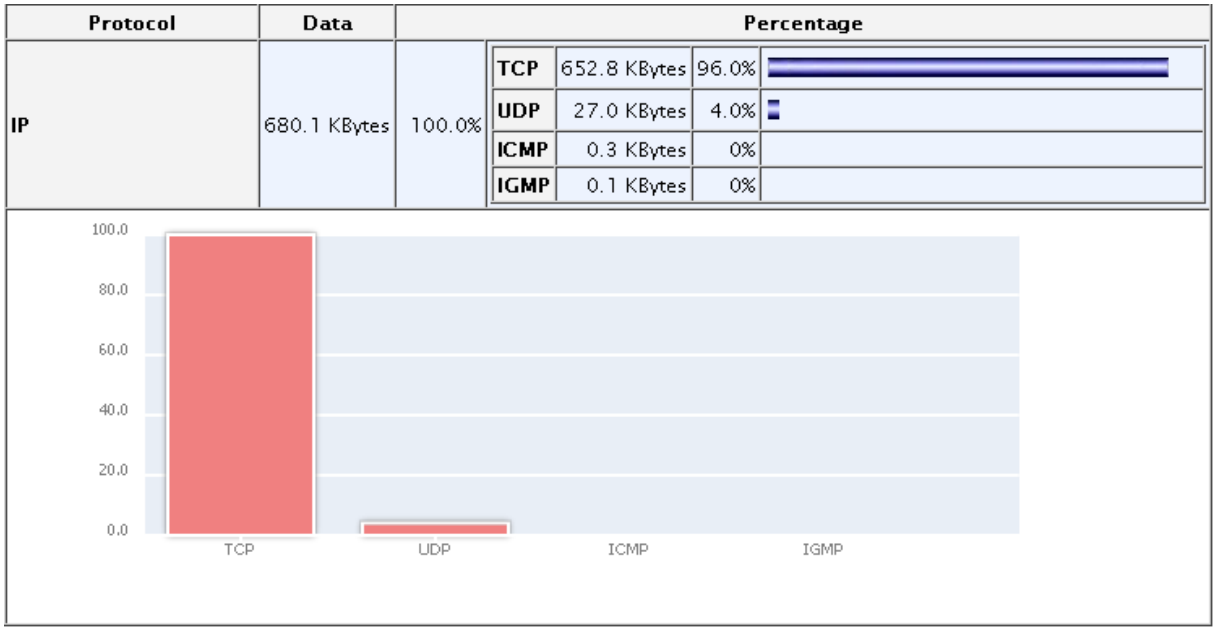


Figura 15 - Protocolos utilizados durante o teste

Na figura 15 podemos observar que mais de 95% das informações dessa rede trafegaram via protocolo *TCP*, e pouco menos de 5% trafegam em protocolo *UDP*, enquanto os protocolos *ICMP* e *IGMP*, não tiveram tráfego nenhum durante o teste.

A ferramenta é muito completa e oferece várias análises diferentes de diversos aspectos da rede, sendo mais eficiente e completa que sua concorrente *MRTG*, em alguns aspectos ela oferece até algumas informações um pouco desnecessárias para uma empresa, que seriam muito mais úteis para o meio acadêmico por mostrar de forma palpável toda a teoria que faz parte dos cursos de redes de computadores.

A quarta ferramenta testada foi o *NMAP*, de acordo com a figura 16 varre o host em busca de todas as informações da rede.

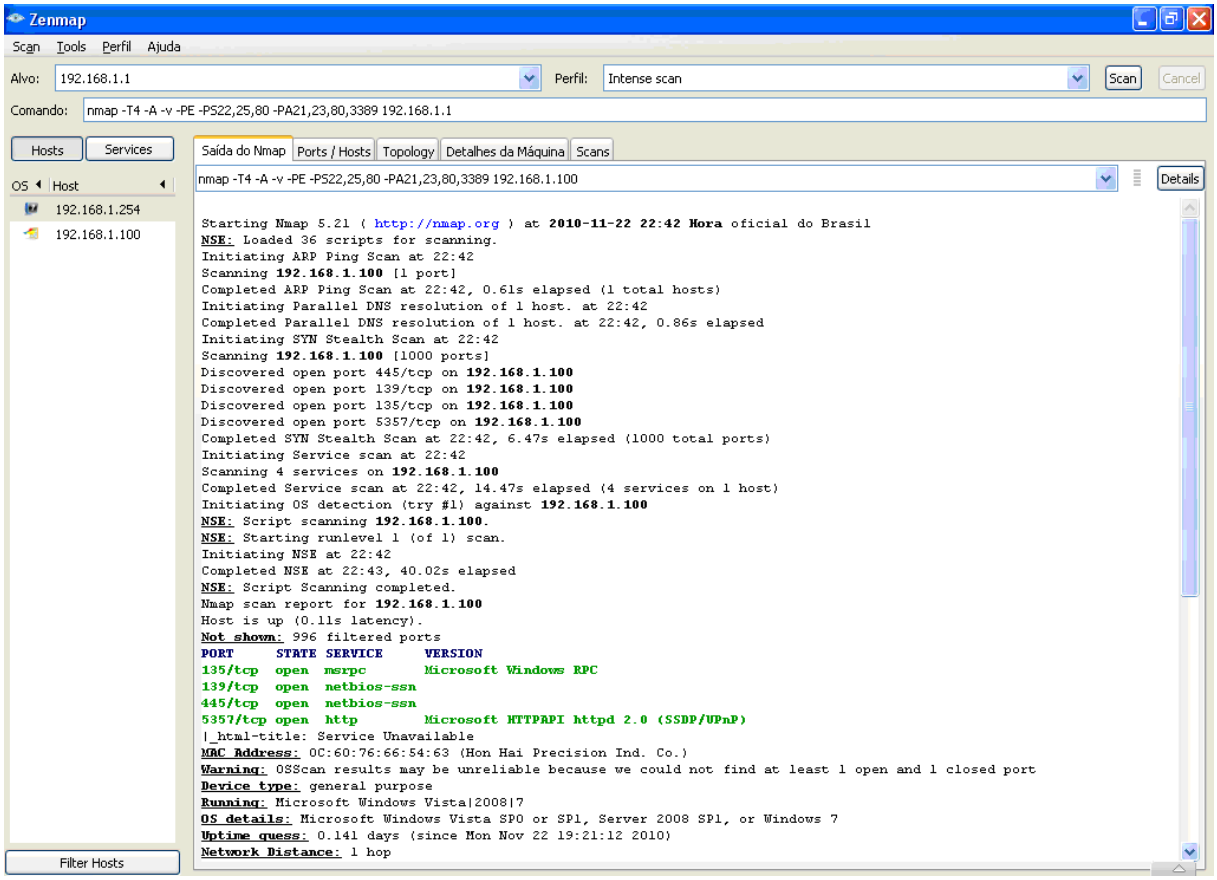


Figura 16 - Resultado do teste do host da rede

De acordo com a imagem acima, percebe-se que no topo da imagem pode-se escolher qual *host* deseja-se verificar, e o tipo de *scan*. Logo abaixo existe o campo comando, onde a ferramenta gera o comando que seria manual nos casos em que o sistema roda nativo do sistema operacional. A esquerda existe uma lista com os hosts examinados até o presente momento. No centro da imagem existem cinco abas, quem mostram o resultado do teste, as portas abertas e fechadas do *host*, a topologia física da rede, uma breve descrição do *host* acessado e por último as informações sobre os testes.

Logo abaixo destas abas existe as informações que a ferramenta buscou, percebe-se que durante o teste, vários processos rodam como um ping no host acessado, um tente de resolução de *DNS*, teste de portas de acesso, onde podemos perceber que quatro portas estão abertas sobre o protocolo *TCP* podemos ver o *MAC Address* da placa de rede, e o sistema operacional do computador.

Já na figura 17 podemos verificar a estrutura física da rede no momento do teste.

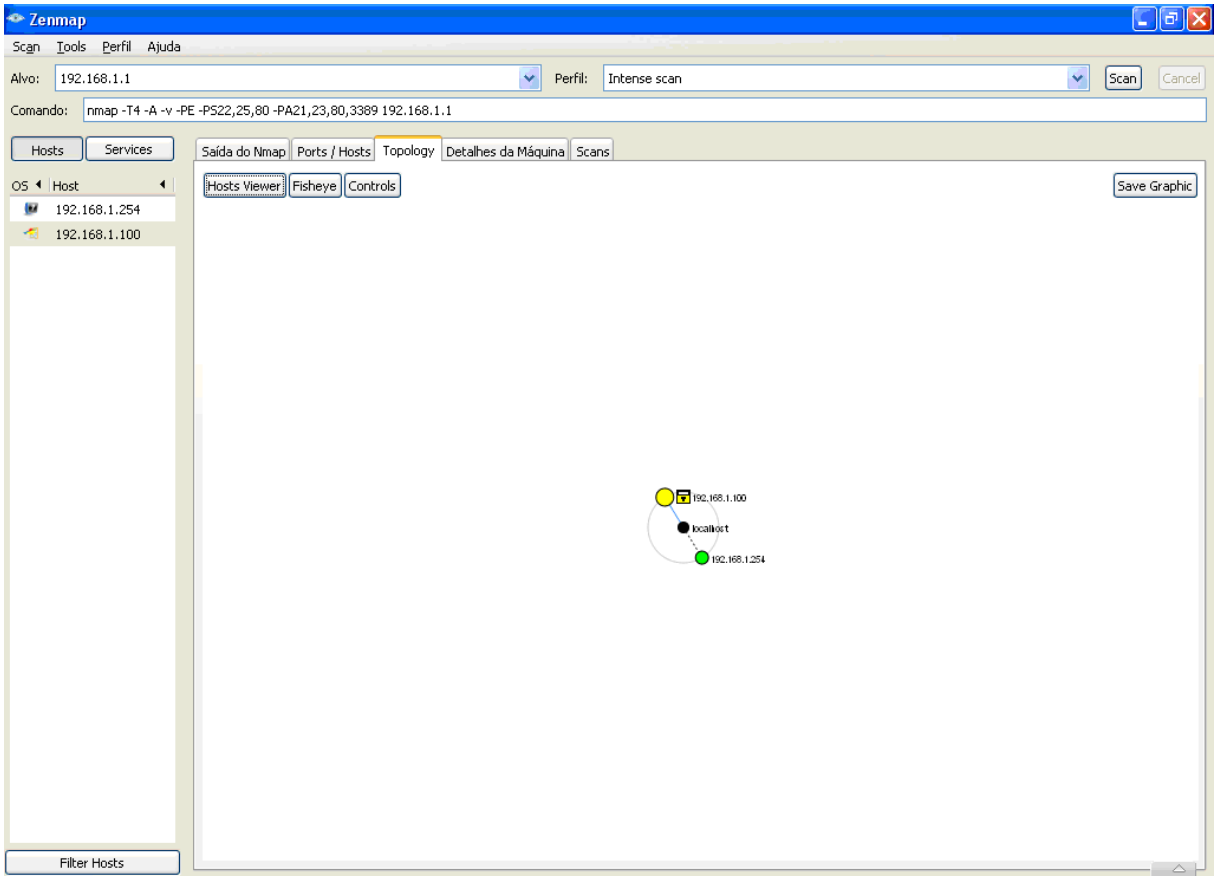


Figura 17 - Topologia da rede no momento do teste

Conforme a figura 17 percebe-se que até o presente momento a rede contava com dois computadores testados, essa estrutura mostra que estes computadores estão interligados entre eles e operacionais, para o ambiente corporativo essa ferramenta ajuda a monitorar a estrutura física que é muito maior do que dois computadores, permitindo controlar se todos os hosts estão conectados e operacionais.

A última ferramenta testada foi a *Ethereal*, que conforme a figura 18 mostra tem uma análise de tipo de pacotes em tempo real.

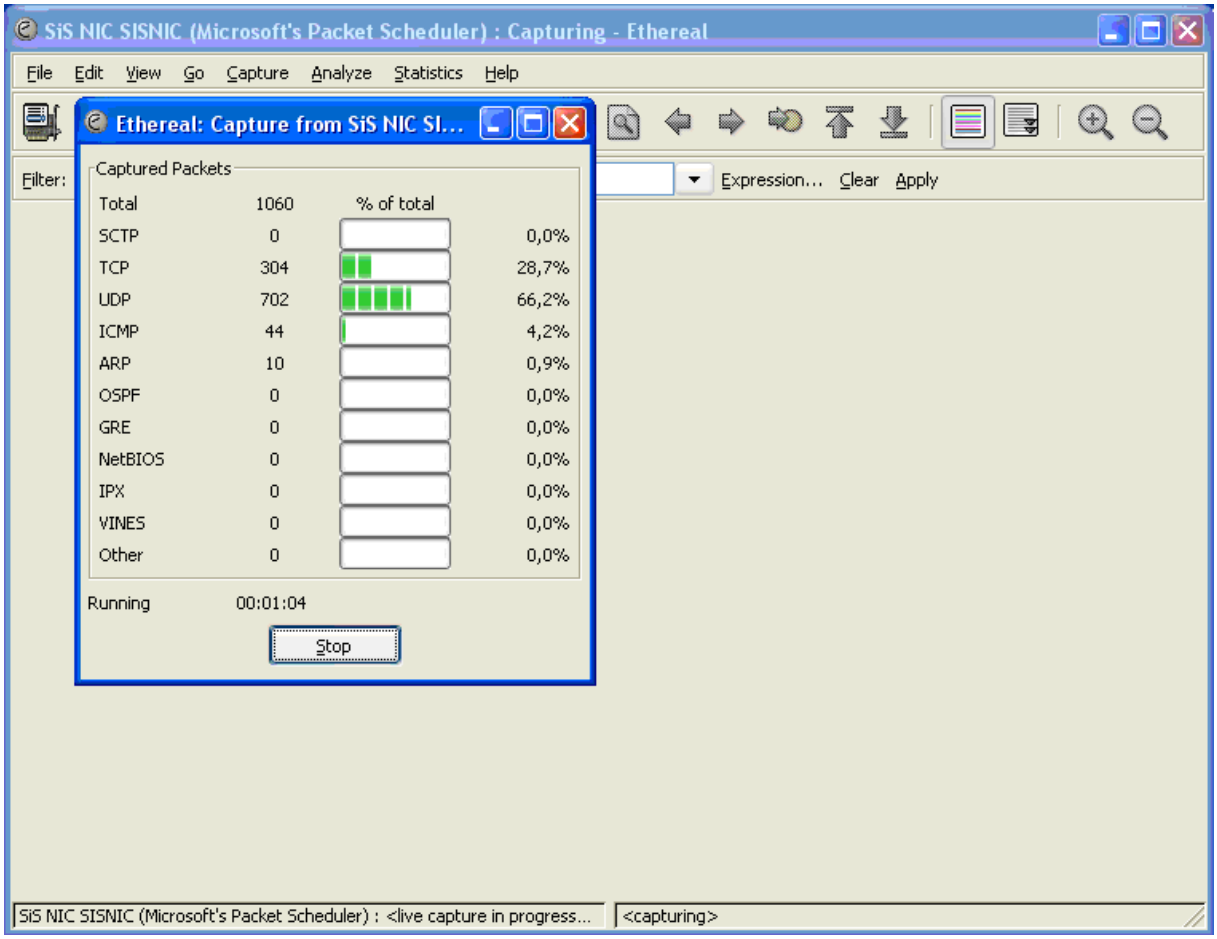


Figura 18 - Captura de pacotes em tempo real

De acordo com a figura 18 a captura dos pacotes acontece em tempo real, e é mostrada em porcentagem, com o tempo de teste abaixo. Na parte inferior da tela e na barra de título aparece o nome da placa de rede onde é feita a captura. Esses pacotes capturados serão listados com detalhes como mostra a figura 19.

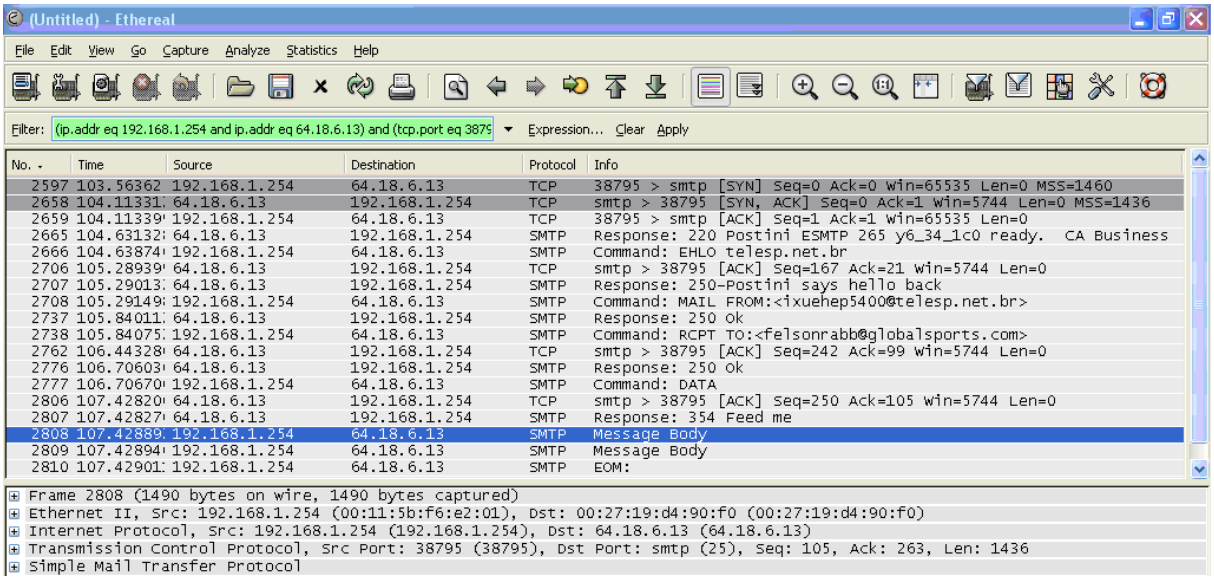


Figura 19 - Detalhamento dos pacotes transmitidos na rede

Esses pacotes que foram transmitidos aparecem listados, conforme a figura 19, separados por cores para cada tipo de transmissão, percebe-se que em destaque existe um pacote do protocolo *SMTP*, que podemos ver logo abaixo o tamanho do pacote, qual o *IP* e qual o *MAC Address* da placa de rede que transmitiu esse pacote e recebeu esse pacote, a porta de transmissão deste protocolo. No alto da imagem podemos ver também o campo *filter* em verde, onde são colocadas as informações para a captura de dados da rede.

3.5 Análise dos Resultados

Em relação às ferramentas foram escolhidos alguns critérios importantes para quantificar a qualidade de cada ferramenta, conforme Tabela 2

Tabela 2 - Avaliação das ferramentas

	Instalação	Utilização	Documentação	Desempenho	Licença	Resultados
MRTG	7,0	9,0	9,5	10,0	10,0	8,0
Wireshark	9,0	7,0	8,0	7,0	10,0	9,0
NTOP	9,0	9,0	7,0	9,0	7,0	10,0
NMAP	9,0	9,0	9,5	9,0	10,0	10,0
Ethereal	9,0	8,0	8,0	9,0	10,0	9,0

De acordo com a tabela acima, as notas foram dadas levando - se em conta alguns aspectos como a Instalação que considera o conhecimento necessário para a instalação levando - se em conta o processo desde o download até a configuração, do ponto de vista de um usuário com conhecimentos básicos de Sistema Operacional. Utilização levou em conta a dificuldade que o usuário encontra para utilizar cada ferramenta. Documentação considerou a facilidade de encontrar tutoriais e informações sobre instalação, configuração e utilização de cada ferramenta. Desempenho analisou o consumo de processador e de banda da rede de cada ferramenta, bem como se alguma delas fez o computador de teste travar ou gerou gargalo de rede. Licença analisou o custo, a disponibilização de código fonte de cada ferramenta, considerando que quanto menor o custo maior a nota, e que o software com código livre permite maior liberdade para o usuário adequar e utilizar a melhor maneira a ferramenta, por tanto, obteve nota maior. E por último verificou - se os Resultados, como eles foram transmitidos para o usuário, a facilidade em interpretar, a quantidade de informações mostradas, a qualidade dessas informações e a confiabilidade desses dados.

O *MRTG* obteve nota em instalação por não ser um processo simples para todos os usuários existem algumas configurações que exigem um conhecimento maior de quem utiliza a ferramenta. A utilização é simples demais, chegando a faltar alguns aspectos que se encontra em outras ferramentas do mesmo estilo. A documentação é a melhor de todas as ferramentas testadas, só não é perfeita por ser em inglês, o que se torna um problema para quem não é acostumado com o idioma estrangeiro. Em relação a desempenho, quase não se percebe a diferença na rede quando se está usando o *MRTG*, e no computador também é mínima a perda de desempenho. A licença é “livre” como já foi explicado sendo perfeita para quem deseja modificar, ou simplesmente investir pouco em uma solução para problemas de

rede. Os resultados ficaram um pouco abaixo do esperado, pois são simples demais, poucas informações, sobre poucos aspectos foram adquiridas durante o teste.

Para o Wireshark, a instalação foi considerada ótima, pois é simples e completa, e não exige conhecimento para efetuá-la. A utilização acabou perdendo pontos, pois é um pouco complicada, exige certo conhecimento e não serve para ser utilizada por qualquer pessoa. A documentação é boa, porém em inglês acaba sendo um empecilho para quem não domina o idioma estrangeiro. O desempenho percebe-se que é o ponto fraco da ferramenta, o consumo de processamento de dados é muito grande, e a quantidade de pacotes analisados era relativamente pequena, pois eram somente cinco computadores ligados em rede. Em uma empresa com 100 computadores, por exemplo, o processamento seria muito alto, tornando inviável a aplicação dessa ferramenta em ambiente corporativo. A licença livre como já foi citada é a ponto alto destas ferramentas, o código aberto favorece os usuários avançados e aprimora a ferramenta. Os resultados obtidos agradaram pelo poder que está ferramenta oferece, analisar o conteúdo do pacote é algo que pode ajudar muito a prevenir problemas de segurança, resolver problemas e controlar a rede.

O *NTOP*, em relação à instalação é simples prática e completa, proporcionando ao usuário pouca dificuldade. A utilização é simples, porém são muitas informações que poderiam ser melhores agrupadas, para facilitar a visualização. A documentação existe, em inglês, e é a pior entre as ferramentas testadas. O desempenho quase não se altera nem na rede nem no computador que executa o programa. A licença é o problema dessa ferramenta, existe um custo, somente para *Windows*, que torna a ferramenta um pouco questionável na hora da escolha. Porém os resultados obtidos por essa ferramenta no seu segmento são os melhores, dados completos, bastante informação, dados que servem até para a área acadêmica, pois tem muita teoria.

O *NMAP* é uma ferramenta simples de se instalar, o assistente faz todo o processo. A utilização exige um pouco de conhecimento, porém com a interface gráfica os comandos ficam automáticos e bastam alguns cliques e a ferramenta começa a analisar a rede. A Documentação é uma das melhores do teste, pois é bastante completa e traduzida para vários idiomas, o que torna possível para qualquer usuário conseguir ajuda. Em relação a desempenho não houve queda significativa da rede, nem do processamento. Possuí licença *GNU GPL*, e por isso recebe graduação máxima nesse quesito. E apresenta uma quantidade significativa de informações interessantes em ambiente corporativo, possuí testes rápidos e que colhem informações preciosas para a análise de segurança, desempenho, conectividade dos hosts, tornando a ferramenta ideal para o auxílio de gestores em ambiente corporativo.

Por último o *Ethereal*, quem tem uma instalação baseada em um assistente que simplifica e agiliza o processo sem necessitar de conhecimentos específicos para tal tarefa. A utilização é um pouco complicada, pois exige certo conhecimento, dando mais trabalho para o gestor aprender a utilizá-la. A documentação no site é boa, porém em inglês como a maioria das ferramentas testadas. Em relação a desempenho existe uma perda muito pequena de desempenho na rede e no processamento, não sendo esse um problema para a ferramenta. A licença *GNU GPL* lhe garante máxima pontuação nesse quesito. E os resultados obtidos através dessa ferramenta são muito interessantes, pois assim como o *Wireshark* permite um controle de segurança e resolução de problemas muito grande ao gestor que souber utilizá-la.

4 Considerações Finais

Durante o teste foram analisados basicamente três tipos de ferramentas, podendo então agrupá-las como análise de tráfego, sendo a *MRTG* e *NTOP* para esse fim. Análise de pacotes, sendo *Wireshark* e *Ethereal* destinadas a isso. E análise de hosts, sendo a *NMAP* para essa função.

Com esse teste percebemos que nenhuma dessas ferramentas sozinha é totalmente capaz de auxiliar um gestor a controlar uma rede corporativa, pois cada uma deles é capaz de desenvolver somente um papel no gerenciamento de redes.

Portanto para controlar com máxima eficiência uma rede de computadores, analisar tráfego, conectividade, controlar informações que transitam entre os hosts é necessário associar uma ferramenta de cada grupo citado acima, para então juntamente com um firewall bem configurado, antivírus bons, o gestor tenha condições de proteger ao máximo as informações da rede, permitindo relatórios e análises em tempo real. Dessa forma as chances de perdas de informações, diminuí bastante e com isso a produtividade aumenta significativamente.

No meio cientifico esse estudo pode servir como início de uma análise para desenvolver novas ferramentas, ou novas formas de gerenciamento de redes de computadores. Em ambiente corporativo esse estudo proporciona informações sobre problemas e soluções de gerenciamento de rede.

REFERÊNCIAS BIBLIOGRÁFICAS

BRAHM, D. R. et al. **Certificação de Firewalls.**

CANTÚ, E. **Redes de Computadores e Internet**. Santa Catarina: CEFET, 2003.

COMER, D. E. **Interligação de redes com TCP/IP**. 5 Ed. Vol. 1. Rio de Janeiro: Elsevier, 2006.

DAVIE, B. S., PETERSON, L.L. **Redes de Computadores:** uma abordagem de sistemas. 3 Ed. Rio de Janeiro: Elsevier, 2004.

Dicionário Aurélio On-line <http://www.dicionariodoaurelio.com> acesso em 23/05/2010.

FERREIRA, S M S P. **Introdução às Redes Eletrônicas de Comunicação**. Ci. Inf., Brasília, v. 23, n. 2, p. 258-263, maio/ago. 1994.

FIGUEIREDO, L. **Segurança da Informática**. Material de aula.

FOROUZAN, B. A. **Protocolo TCP/IP.** 3 Ed. São Paulo: McGraw-Hill, 2008.

HANASHIRO, M. **Metodologia para desenvolvimento de Procedimentos e Planejamentos de Auditorias de TI aplicadas à Administração Publica Federal.** Distrito Federal, 2007.

KUROSE, J. F., ROSS, K. W. **Redes de Computadores e a Internet**: Uma abordagem top-down. 3 Ed. Pearson Addison Wesley, 2006.

LUDWIG, G. A., SILVA F. **Desenvolvimento de uma Metodologia para Auditoria em Redes Sem Fio IEEE 802.11b/g.**

Site Ethereal <http://ethereal.com> acesso em 20/11/2010.

Site IETF <http://www.ietf.org> acesso em 31/05/2010.

Site ISO <http://www.iso.org/> acesso em 28/05/2010.

Site MRTG <http://oss.oetiker.ch/mrtg/> acesso em 07/11/2010

Site NMAP <http://www.nmap.org> acesso em 19/11/2010

Site NTOP <http://www.ntop.org> acesso em 12/11/2010

Site Wireshark <http://www.wireshark.org> acesso em 07/11/2010

STALLINGS, W. **Redes e Sistemas de Comunicação de Dados:** teoria e aplicações corporativas. Rio de Janeiro: Elsevier, 2005.

STEEN, M V., TANENBAUM, A S. **Sistemas Distribuídos**: princípios e paradigmas 2 Ed. São Paulo: PEARSON Pretice Hall, 2007.

TANENBAUM, A S. **Redes de Computadores**. 4 Ed. Rio de Janeiro: Elsevier, 2003.

Tecnologia da Informação – Código de Prática para Gestão da Segurança de Informações Norma ISO/IEC 17799.

ANEXO A – INSTALAÇÃO MRTG

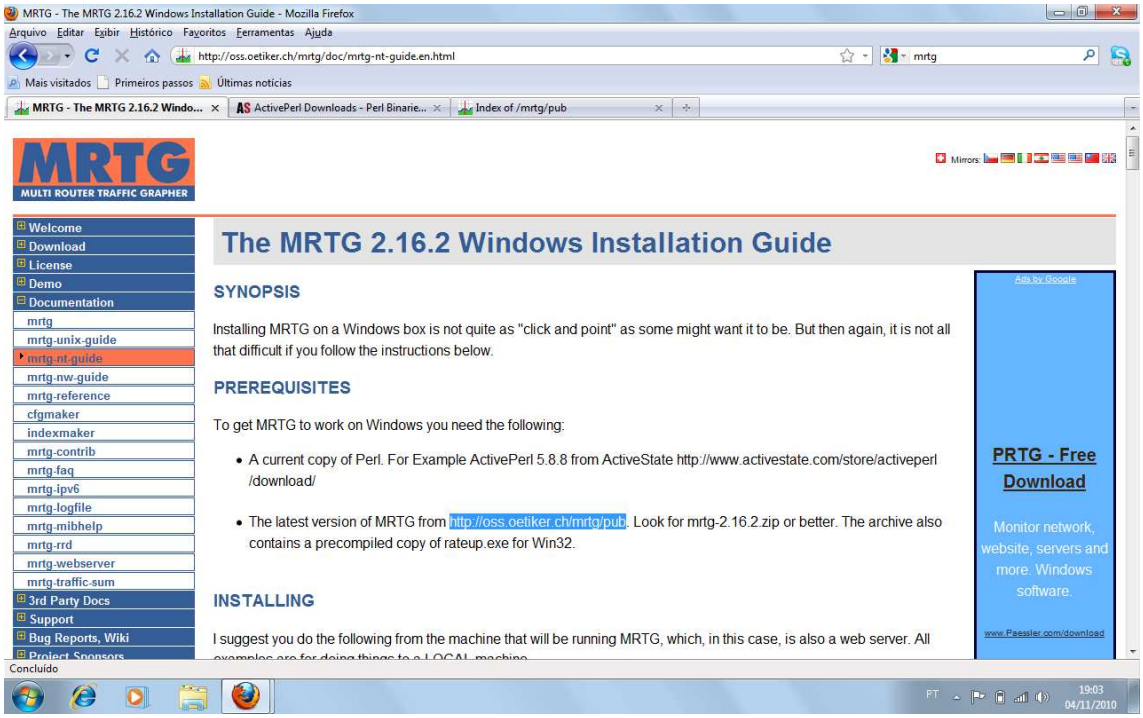


Figura 20 - Tutorial de instalação do MRTG 2.16.2
Fonte: http://oss.oetiker.ch/mrtg/doc/mrtg-nt-guide.en.html

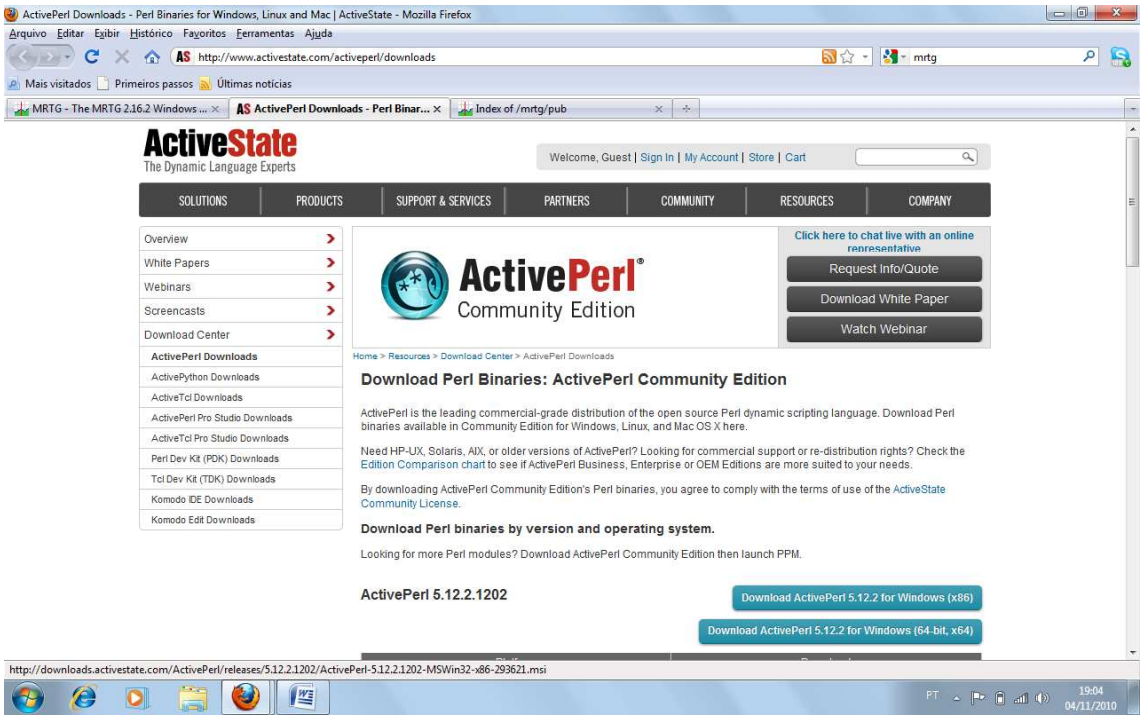


Figura 21 - Página de download do ActivePerl 5.8.9.827
Fonte: http://www.activestate.com/activeperl/downloads

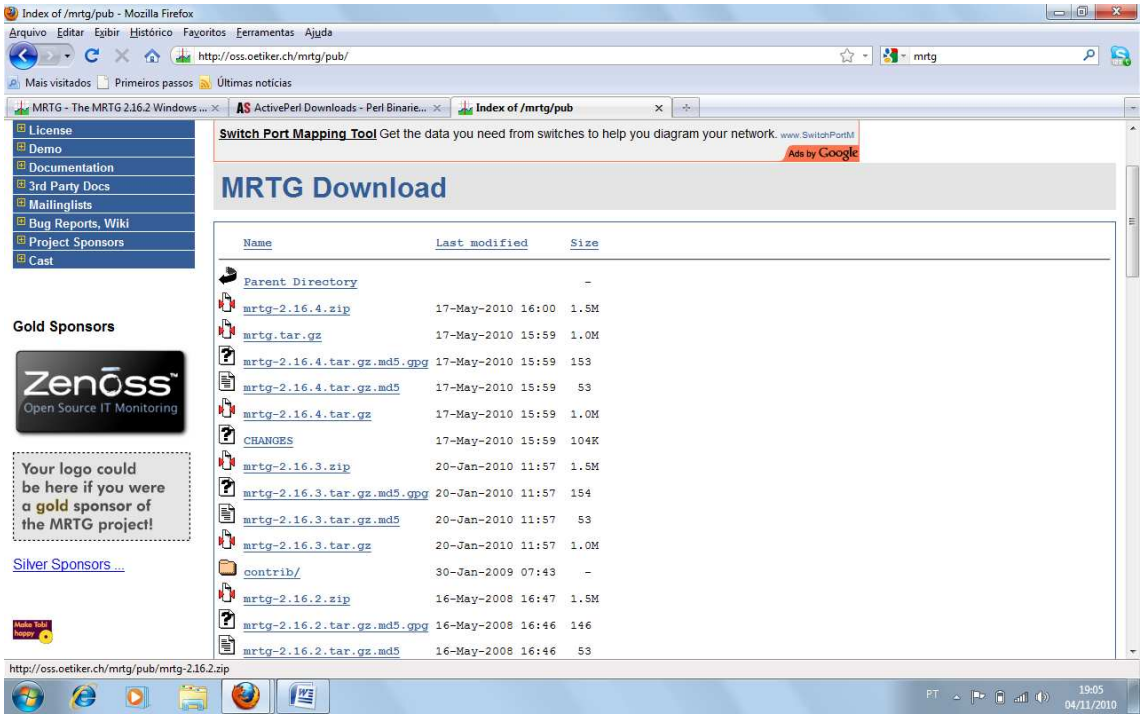


Figura 22 - Página de download do MRTG 2.16.2
Fonte: http://oss.oetiker.ch/mrtg/pub/

A instalação da ferramenta começa com o ActivePerl que serve para que a ferramenta funcione na plataforma Windows.

Figura 23 - Primeira tela da instalação do ActivePerl.

Figura 24 - Segunda tela da instalação do ActivePerl.

Figura 25 - Terceira tela da instalação do ActivePerl.

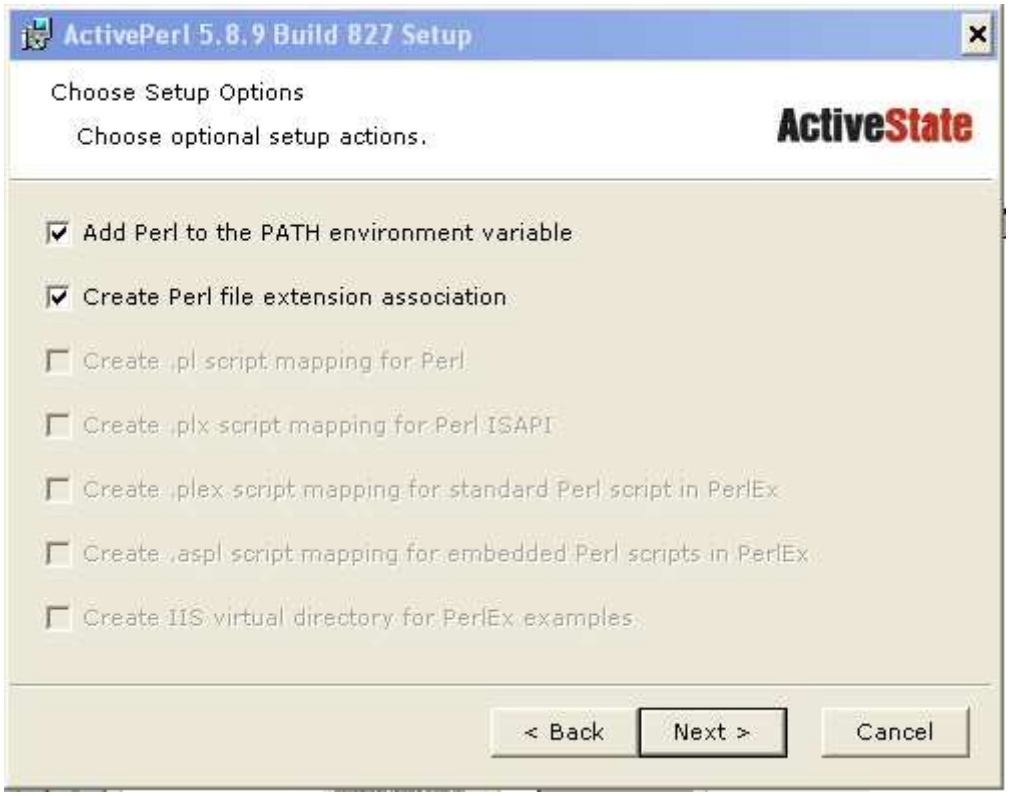


Figura 26 - Quarta tela da instalação do ActivePerl.

Figura 27 - Quinta tela da instalação do ActivePerl.

Figura 28 - Sexta tela da instalação do ActivePerl.

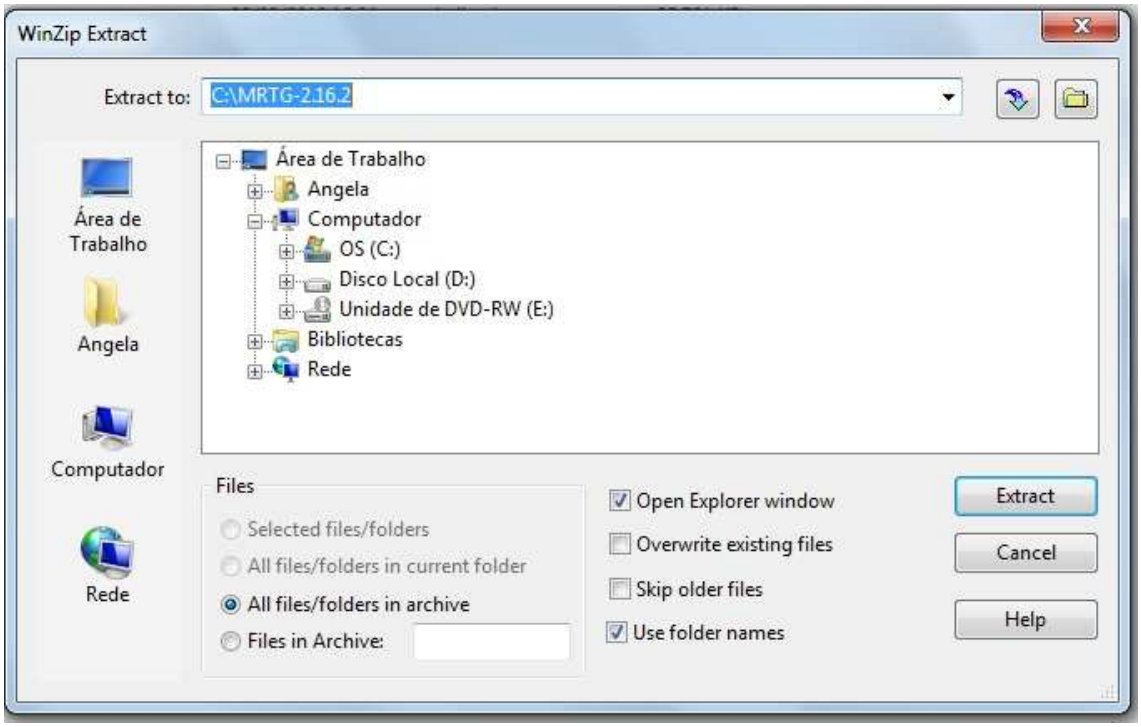


Figura 29 - Extração dos arquivos do programa MRTG

Depois de instalado o ActivePerl, extrai -se os arquivos do MRTG para a pasta raiz do Windows, e através do Prompt de Comando executa-se os comandos:

```
perl cfgmaker public@192.168.1.254 --global "WorkDir: c:\www\mrtg" --
output mrtg.cfg
```

Com esse comando cria-se um arquivo que fará a monitoria do equipamento, gerando as informações necessárias para a criação dos gráficos de análise do tráfego de rede.

Após criar deve-se editar o arquivo e colocar a seguinte linha no topo do arquivo, para que seja repetido a cada cinco minutos a monitoria do tráfego de rede.

```
RunAsDaemon: yes
```

E para iniciar a análise deve-se executar o seguinte comando no prompt de comando:

```
start /Dc:\mrtg-2.16.2\bin wperl mrtg --logging=eventlog mrtg.cfg
```

Dessa forma a análise será feita em intervalos fixos de 5 minutos e acontecerá em segundo plano, sem abrir janelas ou aparecer para o usuário.

ANEXO B – INSTALAÇÃO DO WIRESHARK

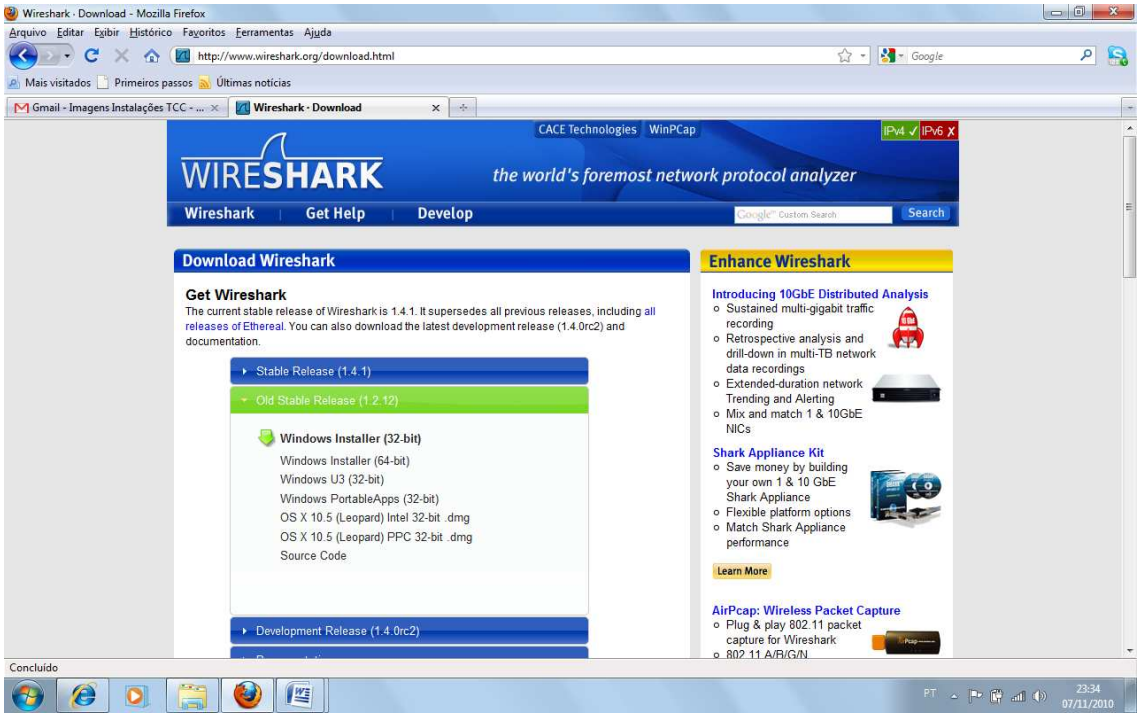


Figura 30 - Página de download da ferramenta.
Fonte: http://www.wireshark.org/download.html

Figura 31 - Primeira tela de instalação do Wireshark.

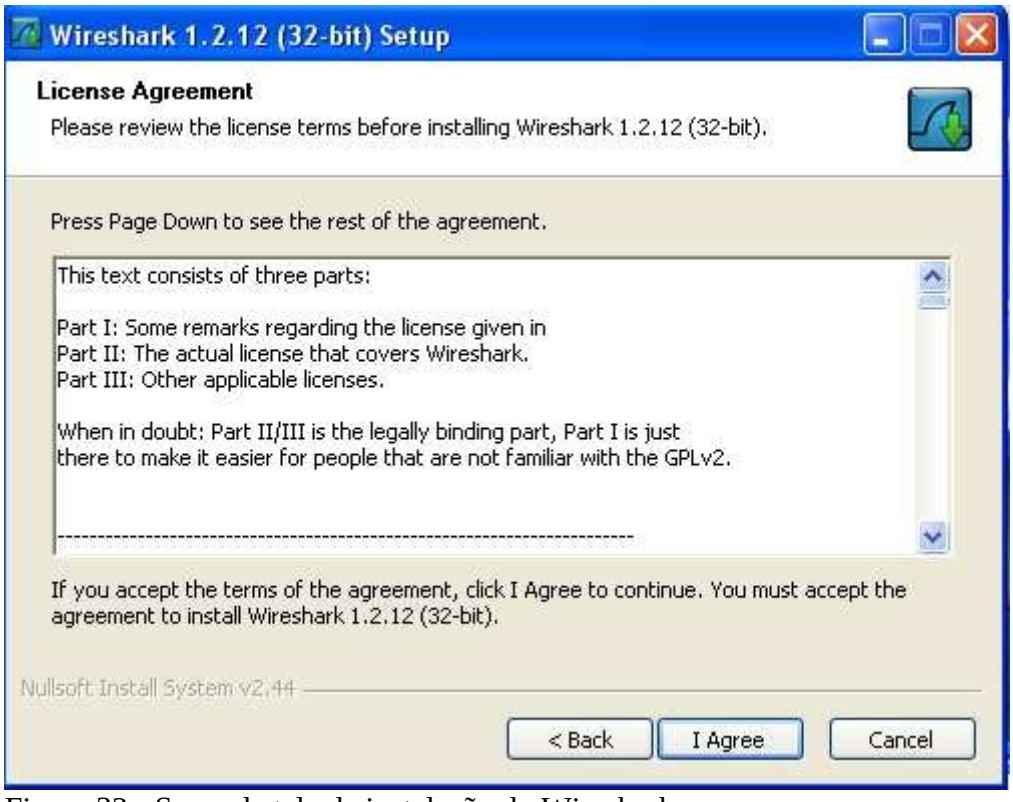


Figura 32 - Segunda tela de instalação do Wireshark.

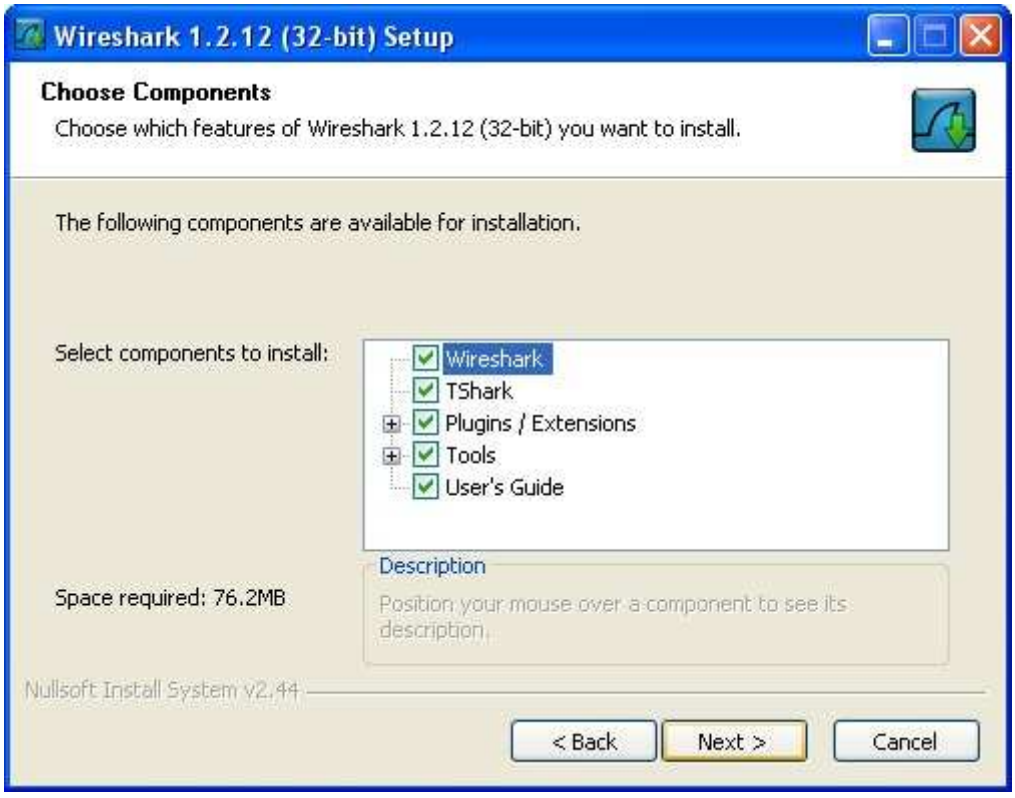


Figura 33 - Terceira tela de instalação do Wireshark.

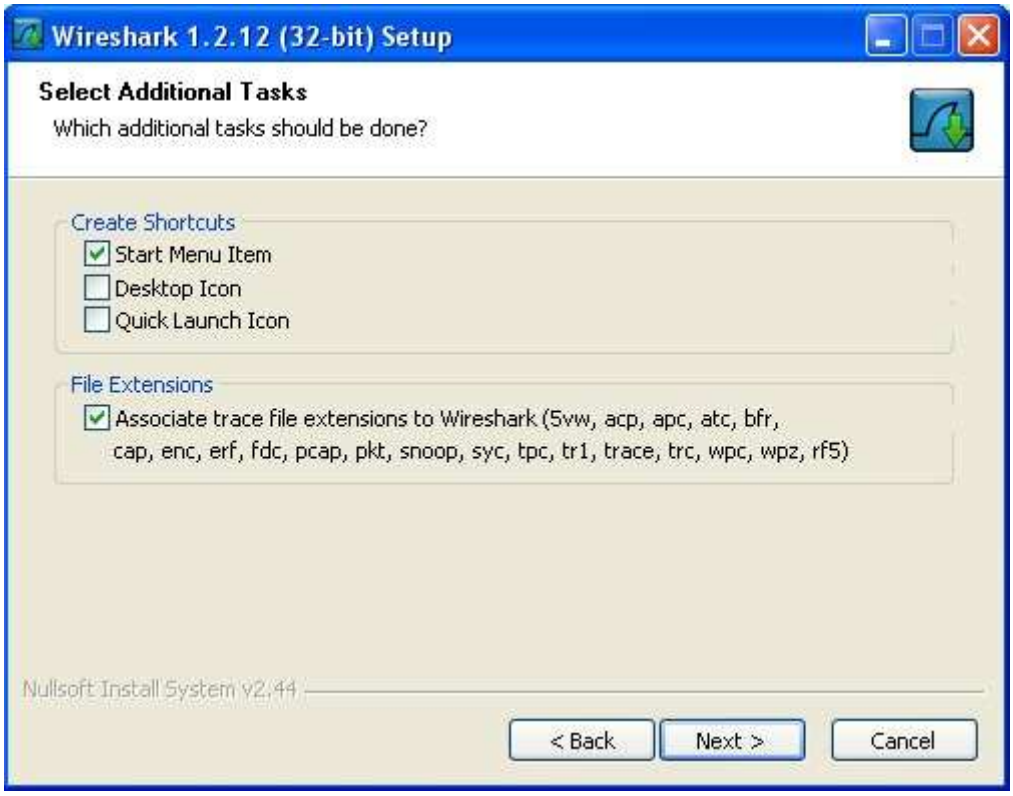


Figura 34 - Quarta tela de instalação do Wireshark.

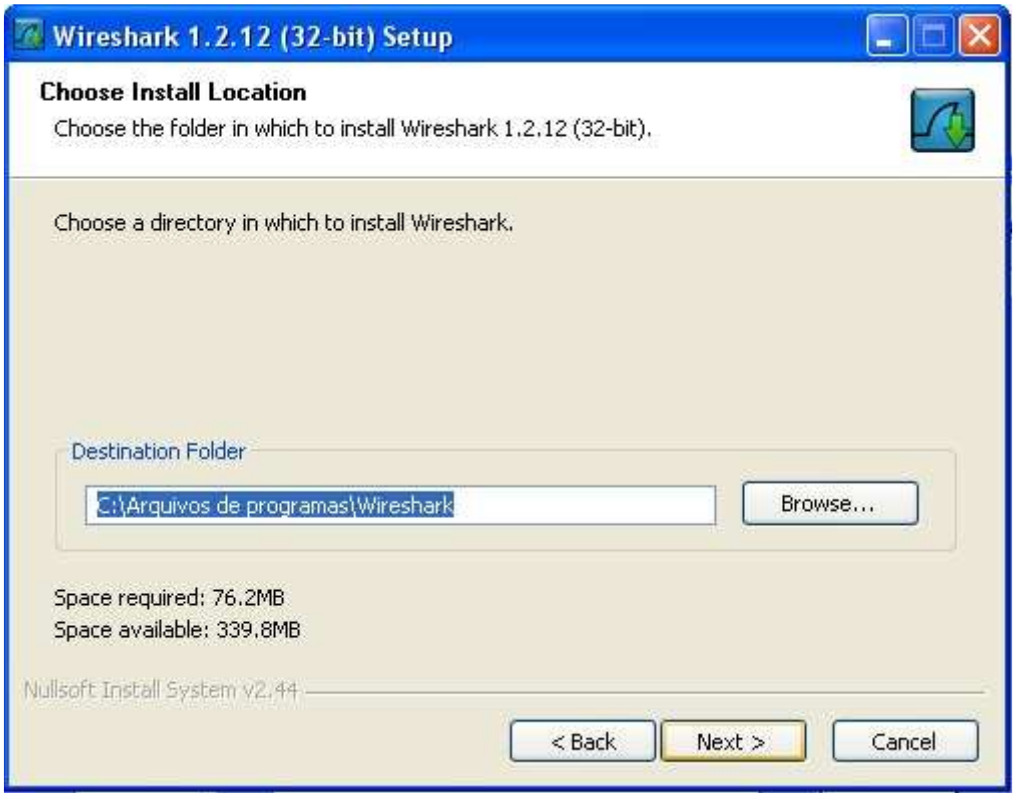


Figura 35 - Quinta tela de instalação do Wireshark.

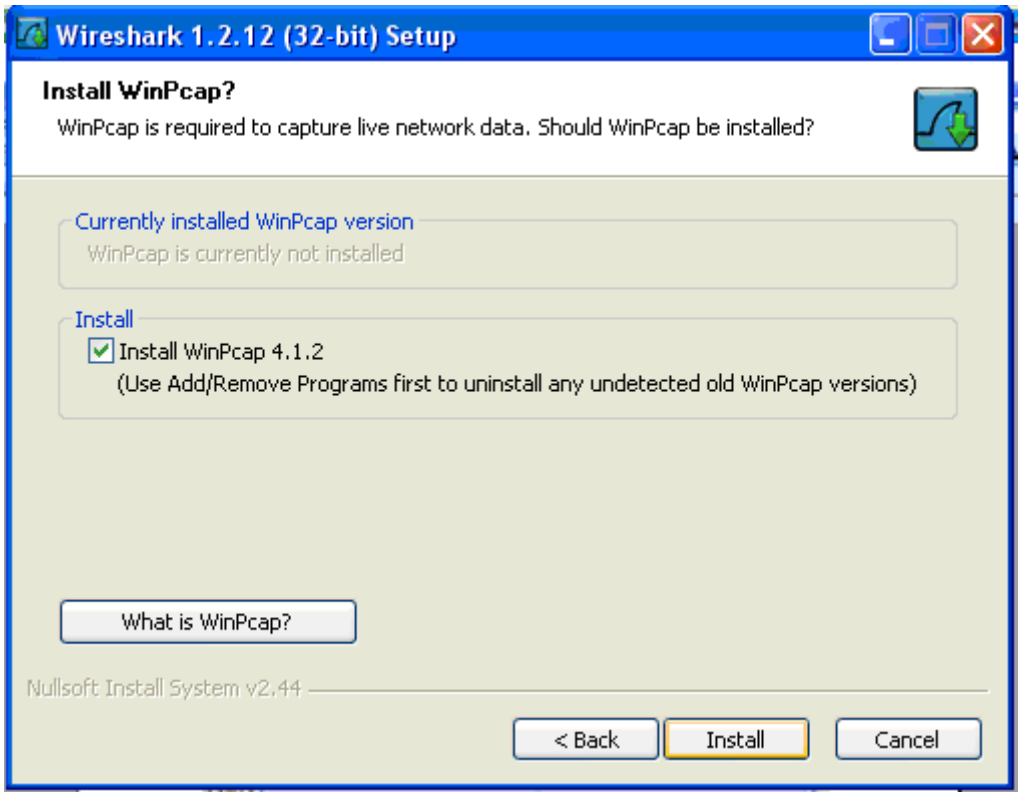


Figura 36 - Sexta tela de instalação do Wireshark.

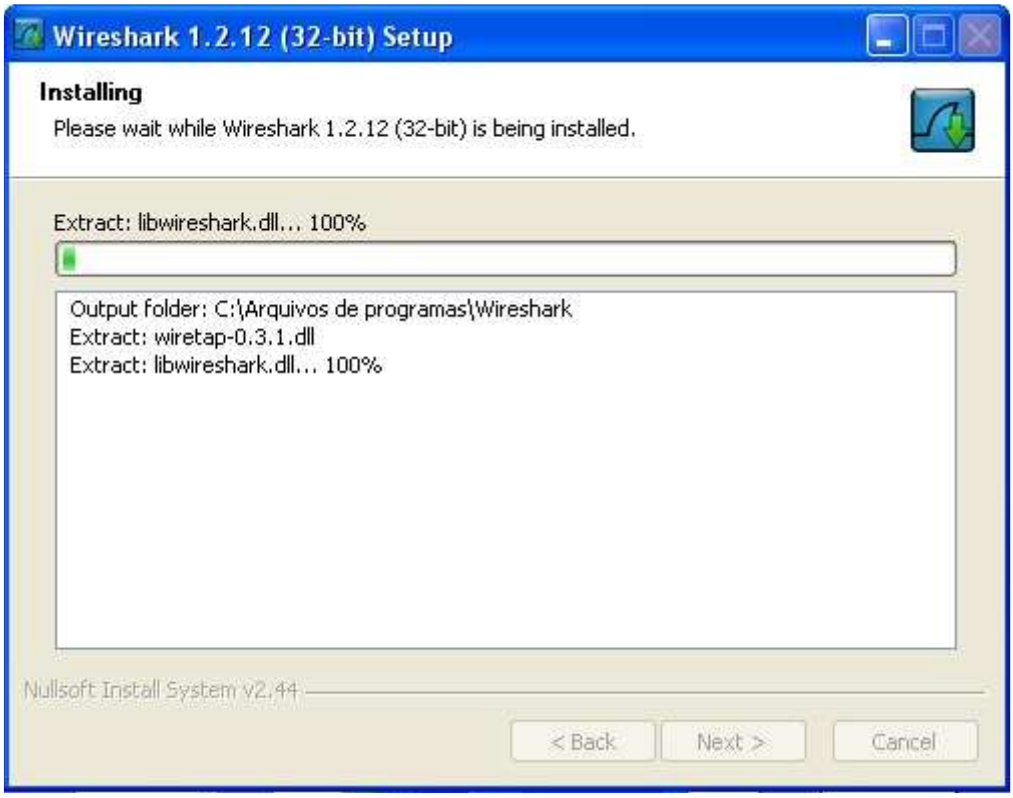


Figura 37 - Sétima tela de instalação do Wireshark.

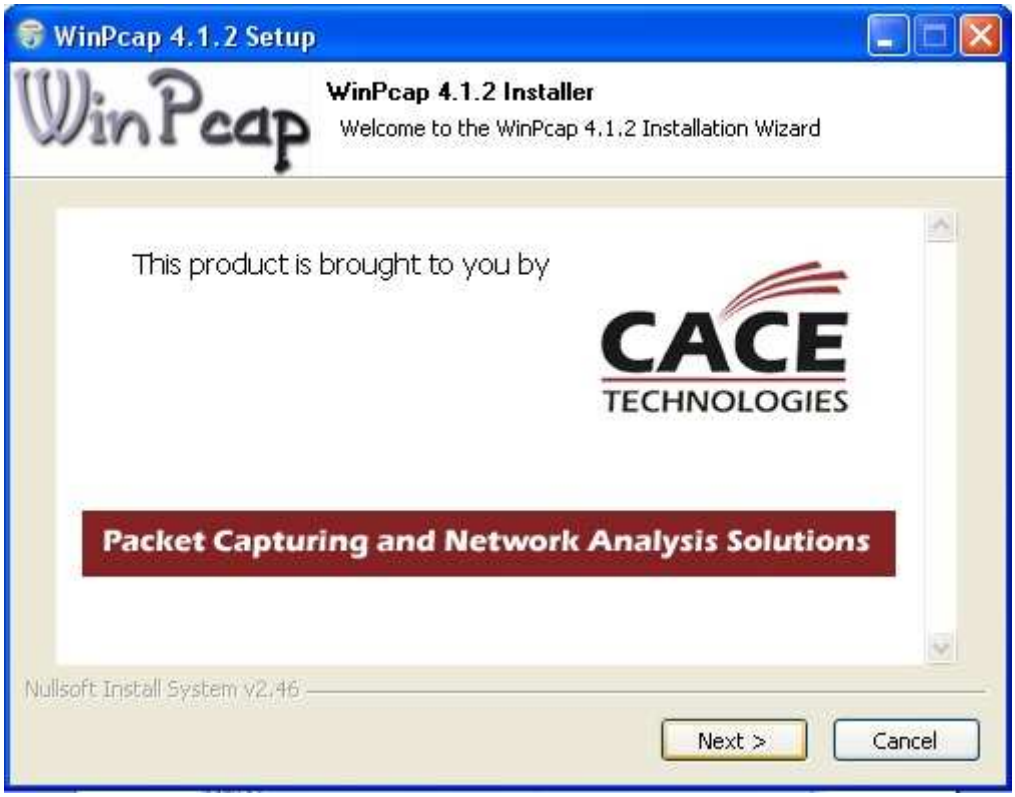


Figura 38 - Primeira tela de instalação do WinPCap.

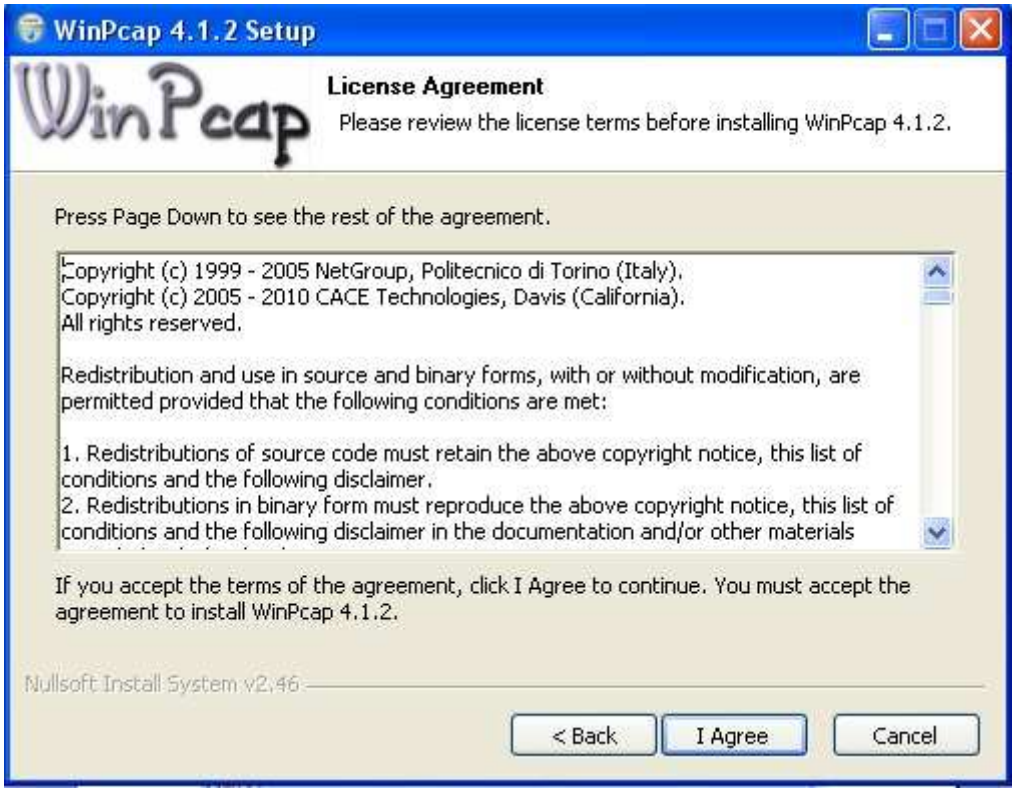


Figura 39 - Segunda tela de instalação do WinPCap.

Figura 40 - Terceira tela de instalação do WinPCap.

ANEXO C – INSTALAÇÃO DO NTOP

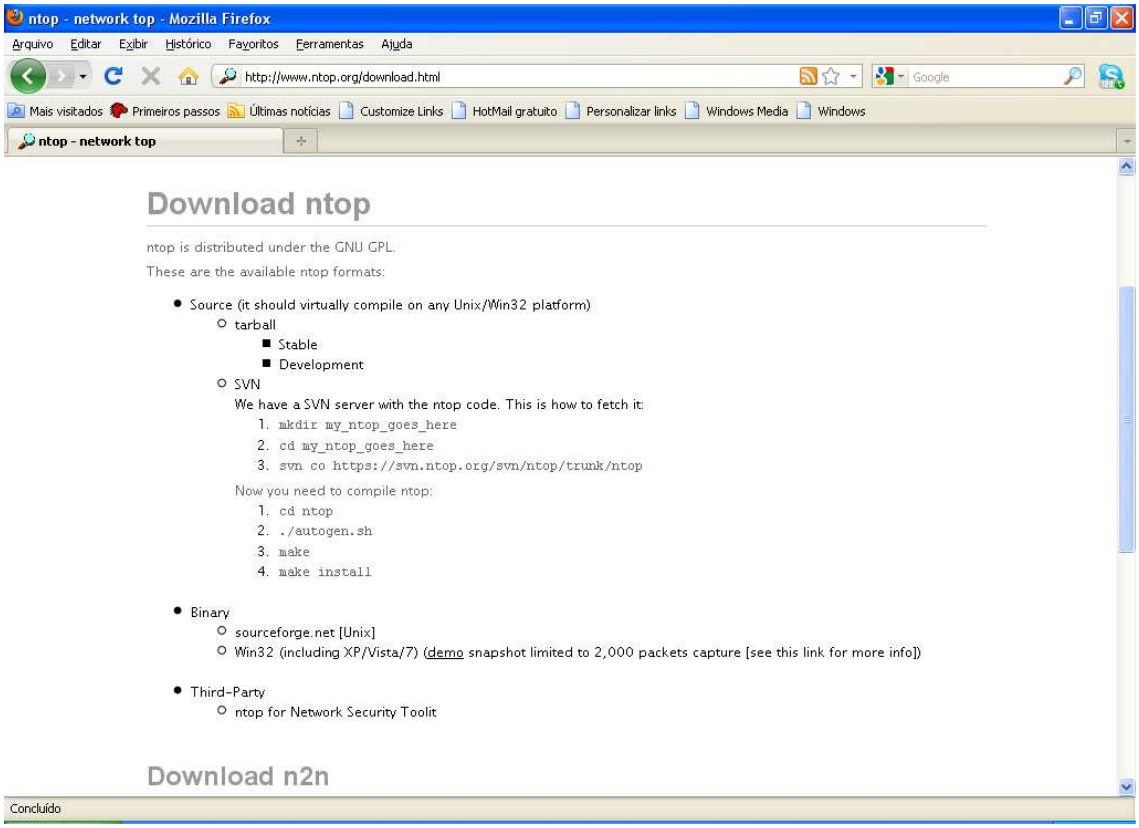


Figura 41 - Página de download do NTOP

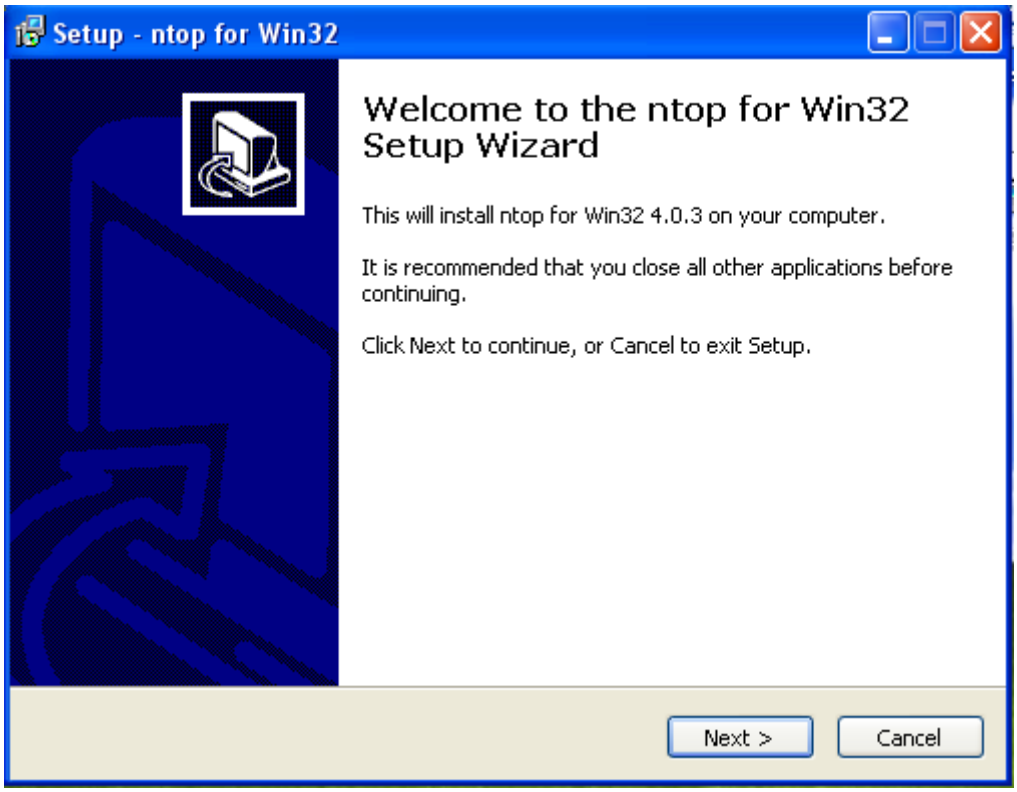


Figura 42 - Primeira tela de instalação do NTOP

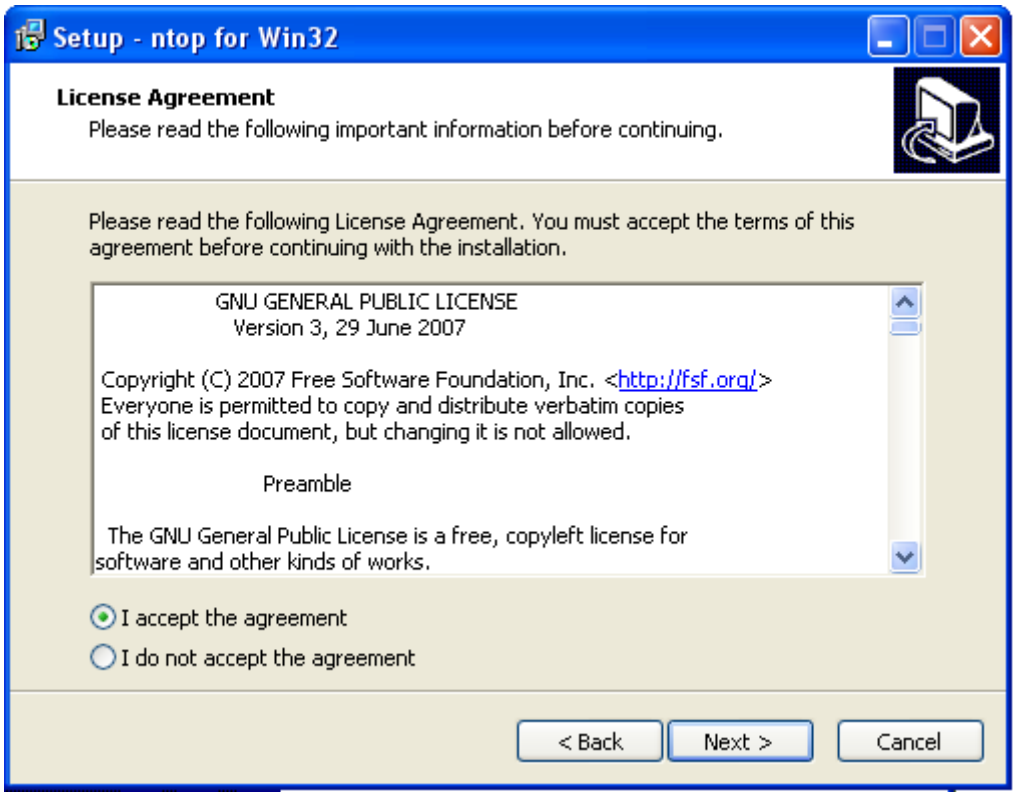


Figura 43 - Segunda tela de instalação do NTOP

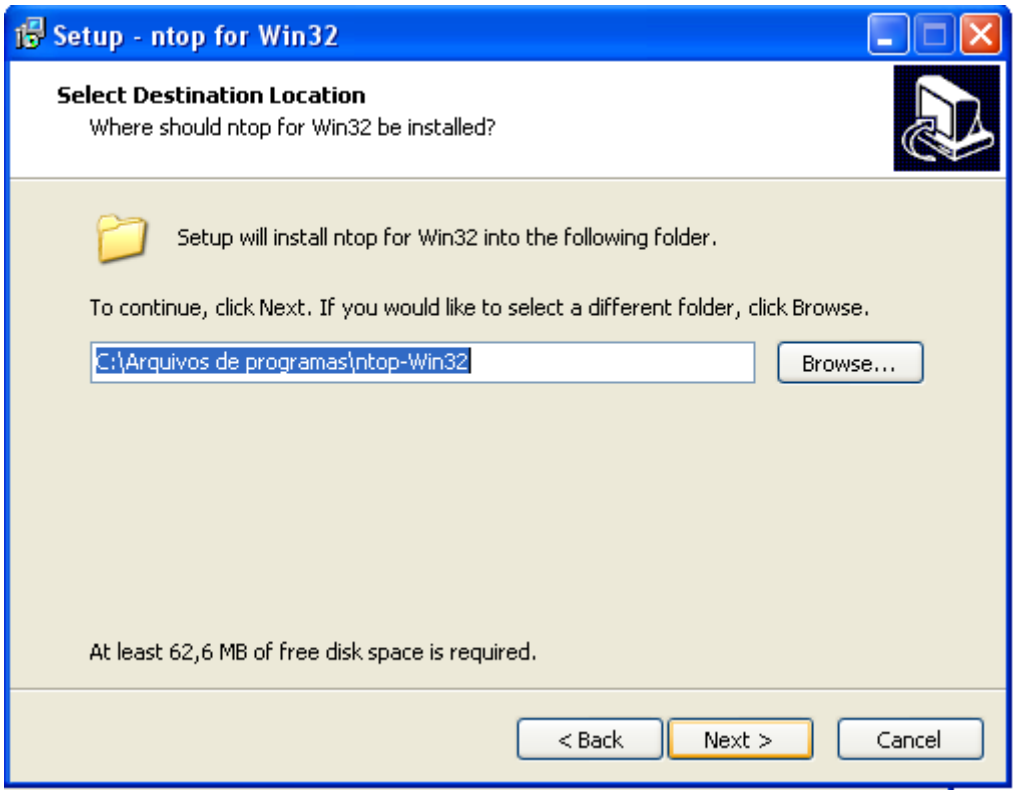


Figura 44 - Terceira tela de instalação do NTOP

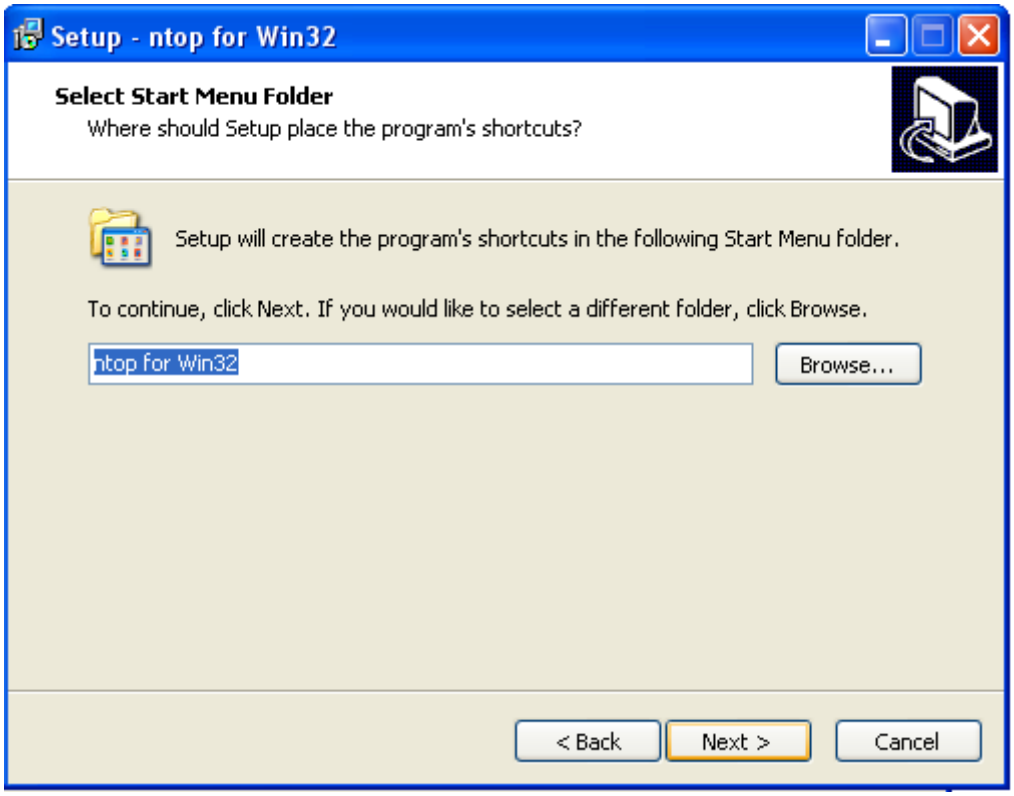


Figura 45 - Quarta tela de instalação do NTOP

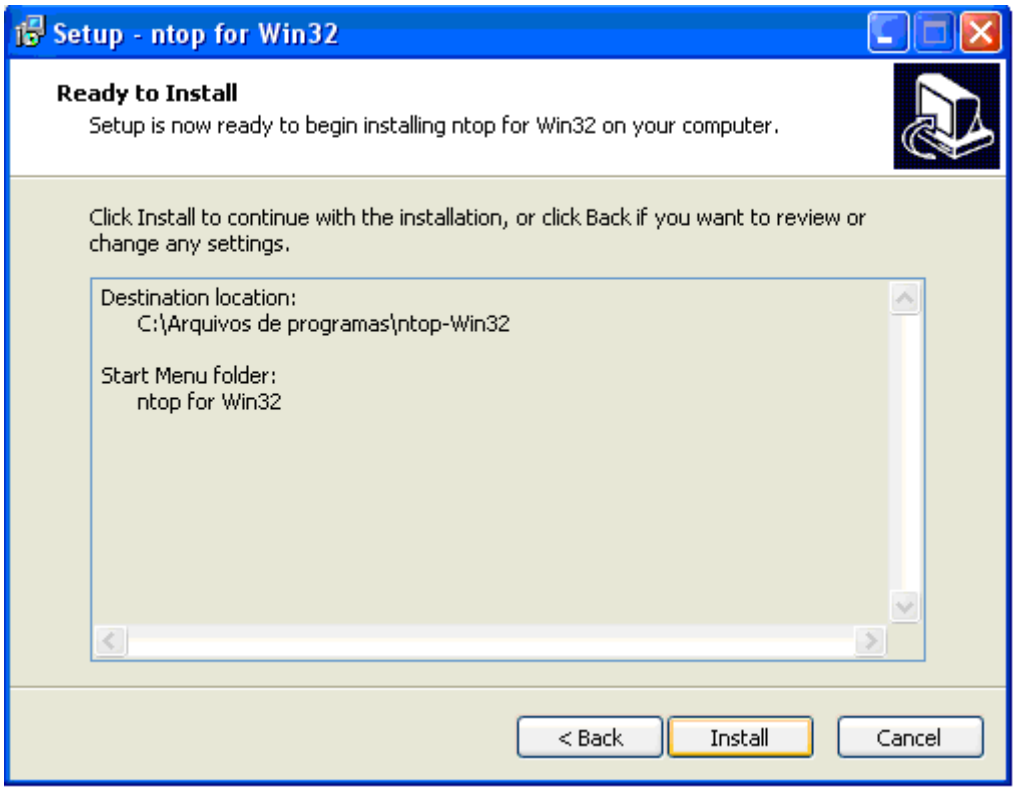


Figura 46 - Quinta tela de instalação do NTOP

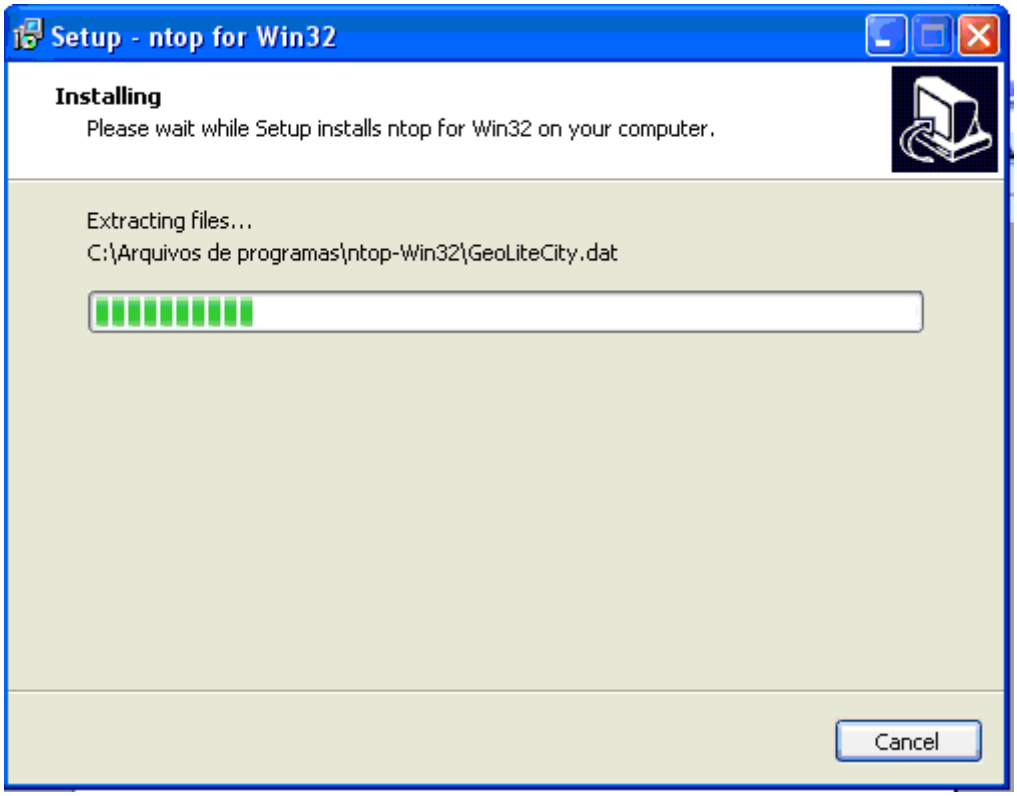


Figura 47 - Sexta tela de instalação do NTOP

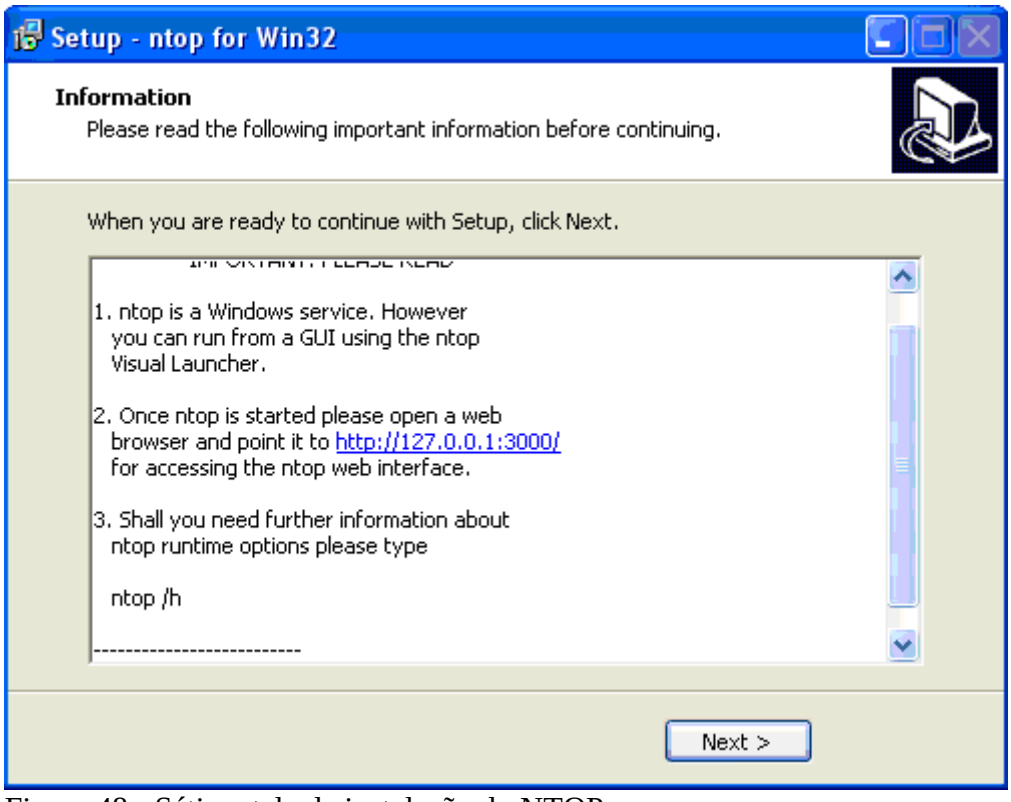


Figura 48 - Sétima tela de instalação do NTOP

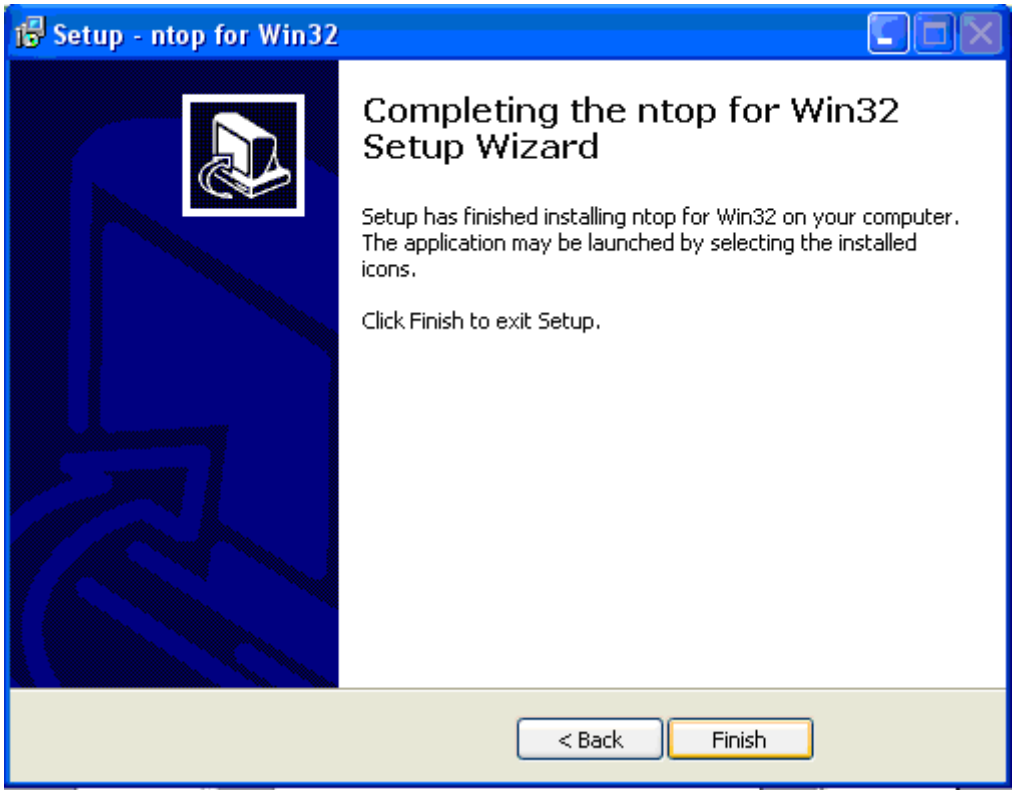


Figura 49 - Oitava tela de instalação do NTOP

ANEXO D - INSTALAÇÃO NMAP

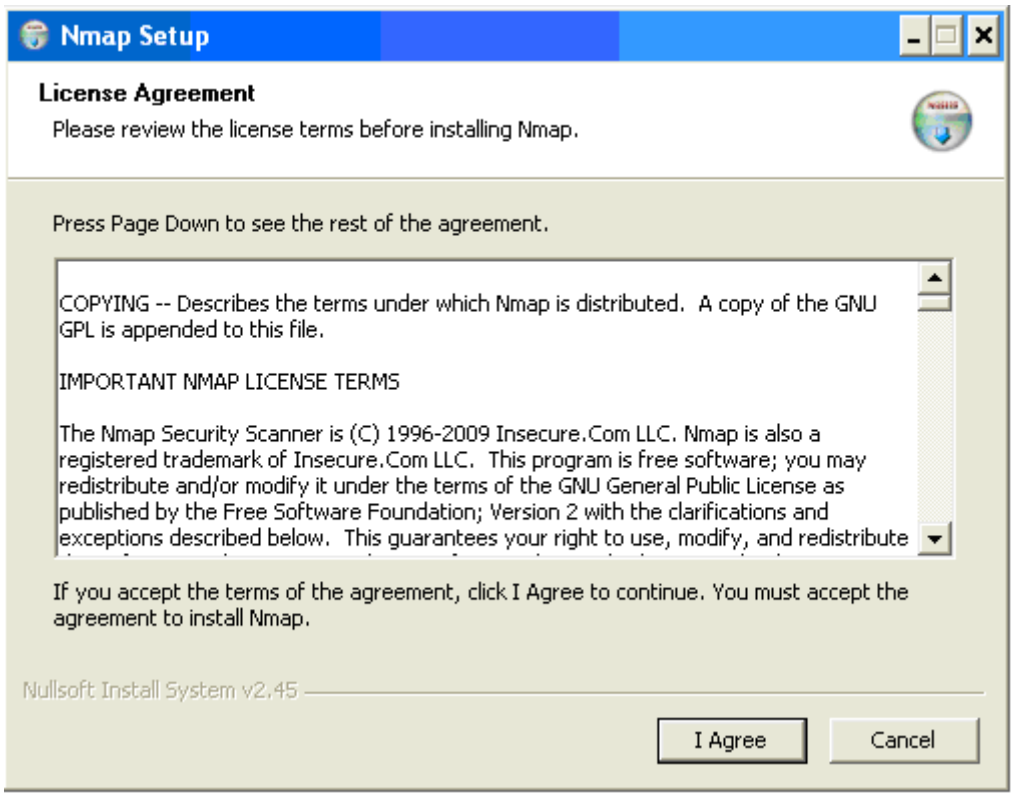


Figura 50 - Primeira tela de instalação do NMAP

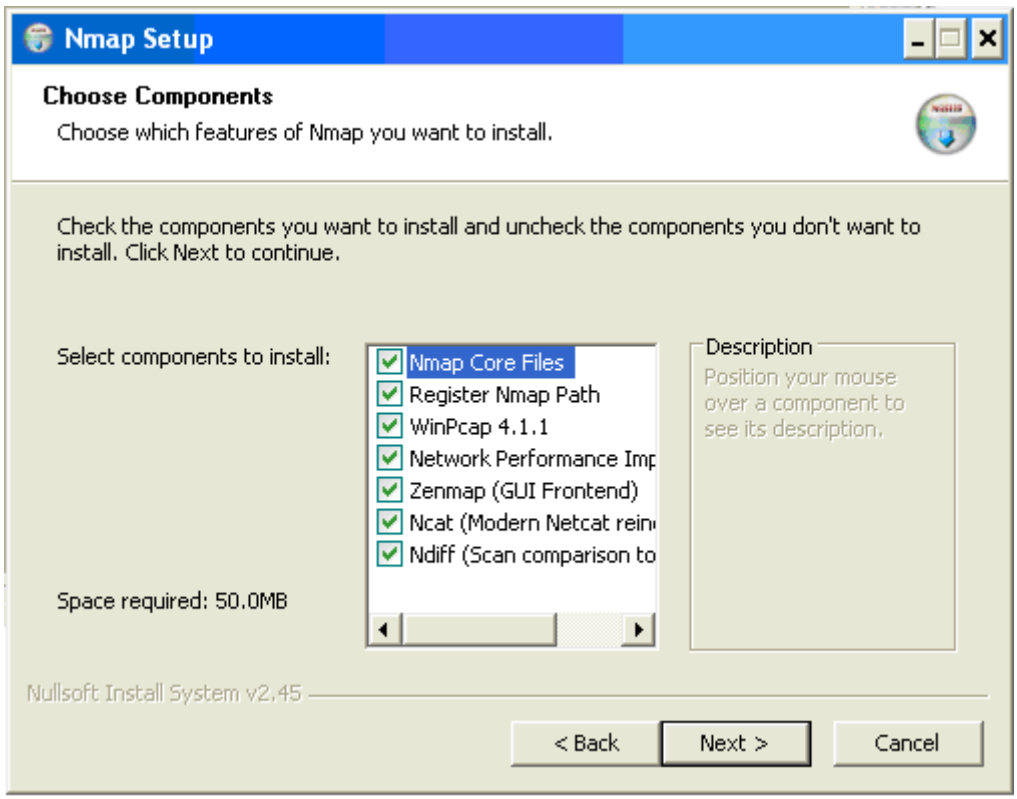


Figura 51 - Segunda tela de instalação do NMAP

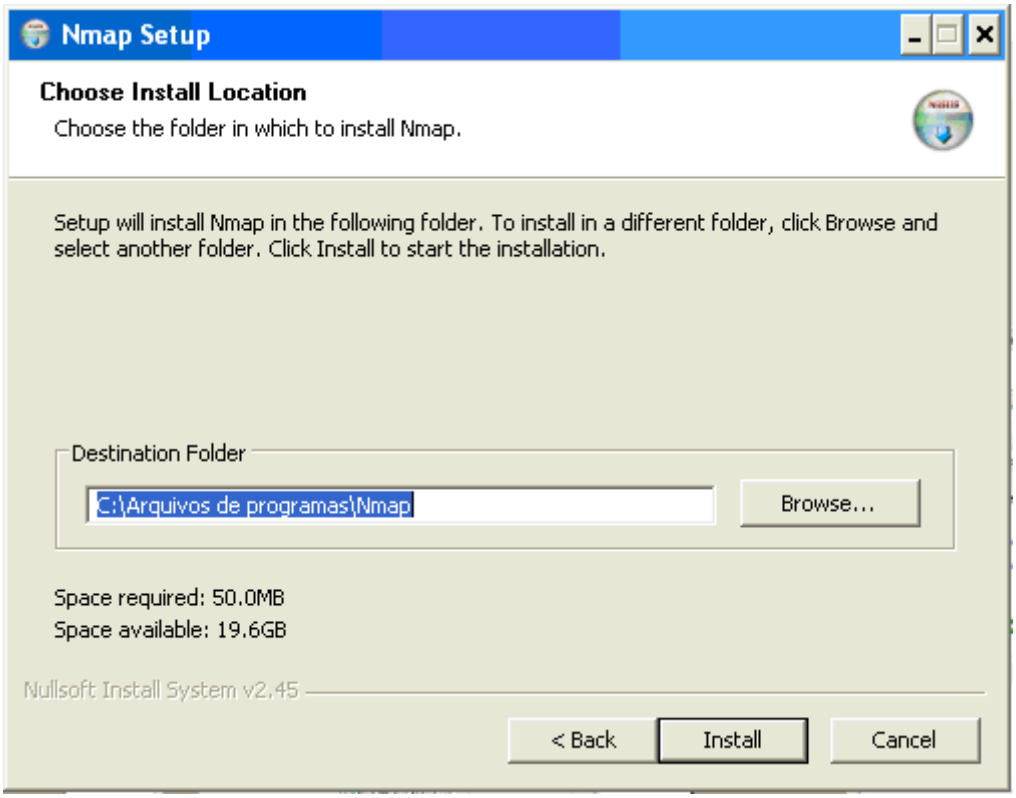


Figura 52 - Terceira tela de instalação do NMAP

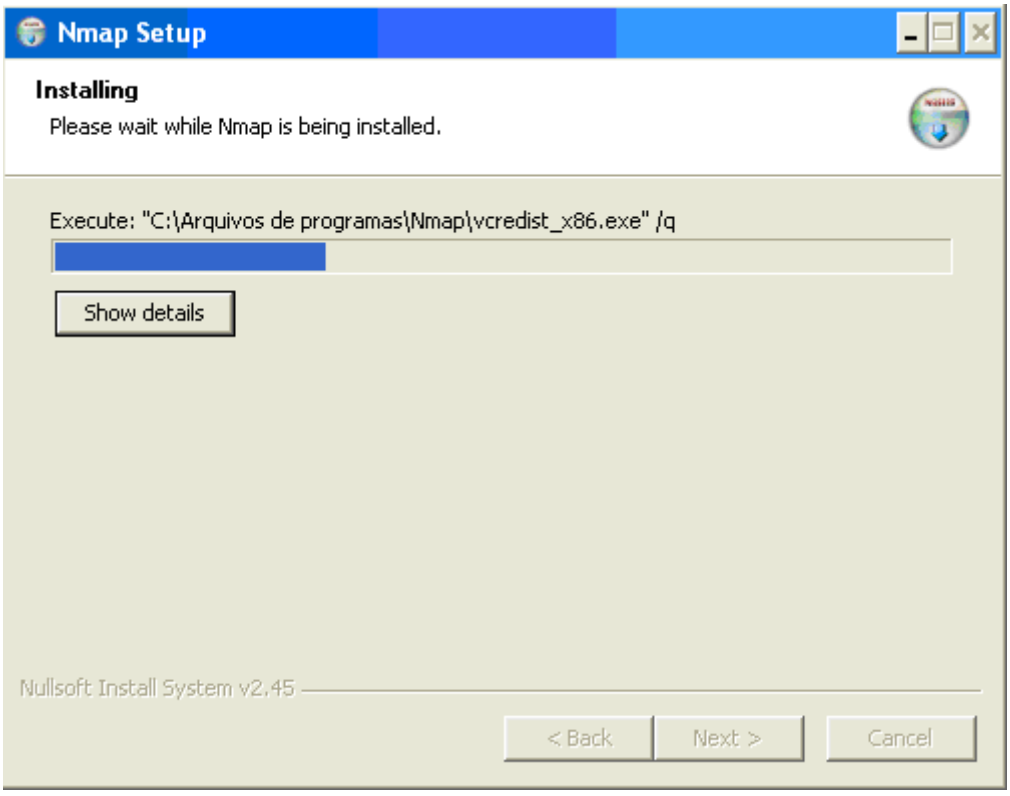


Figura 53 - Quarta tela de instalação do NMAP

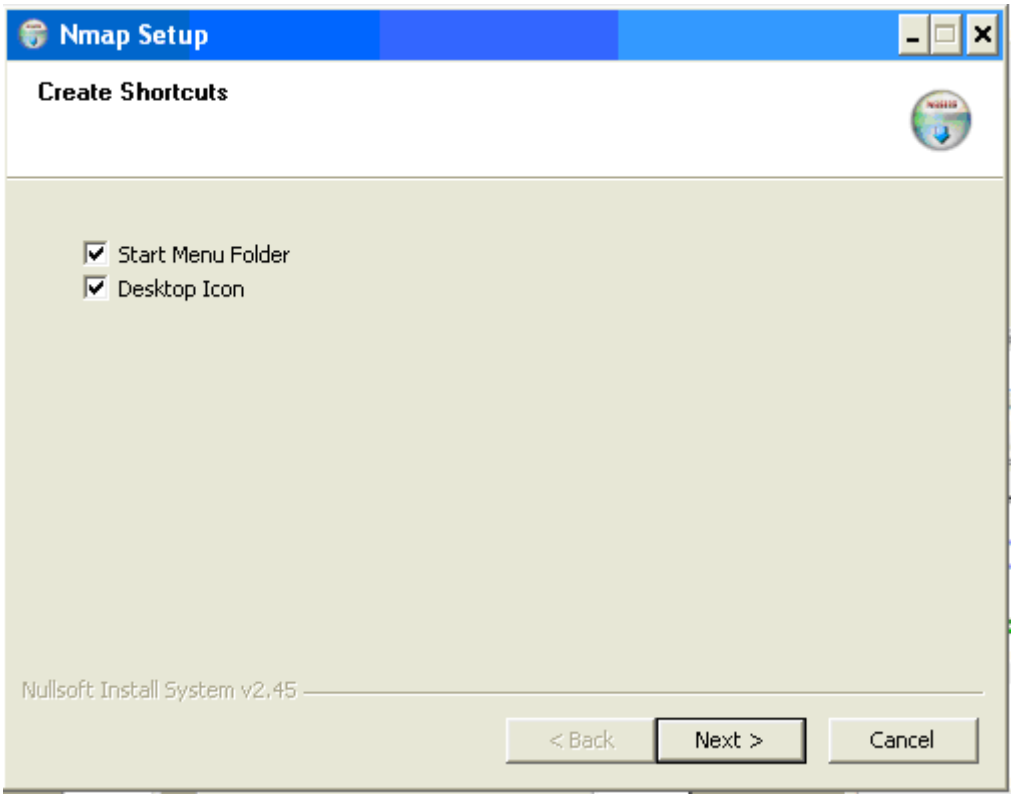


Figura 54 - Quinta tela de instalação do NMAP

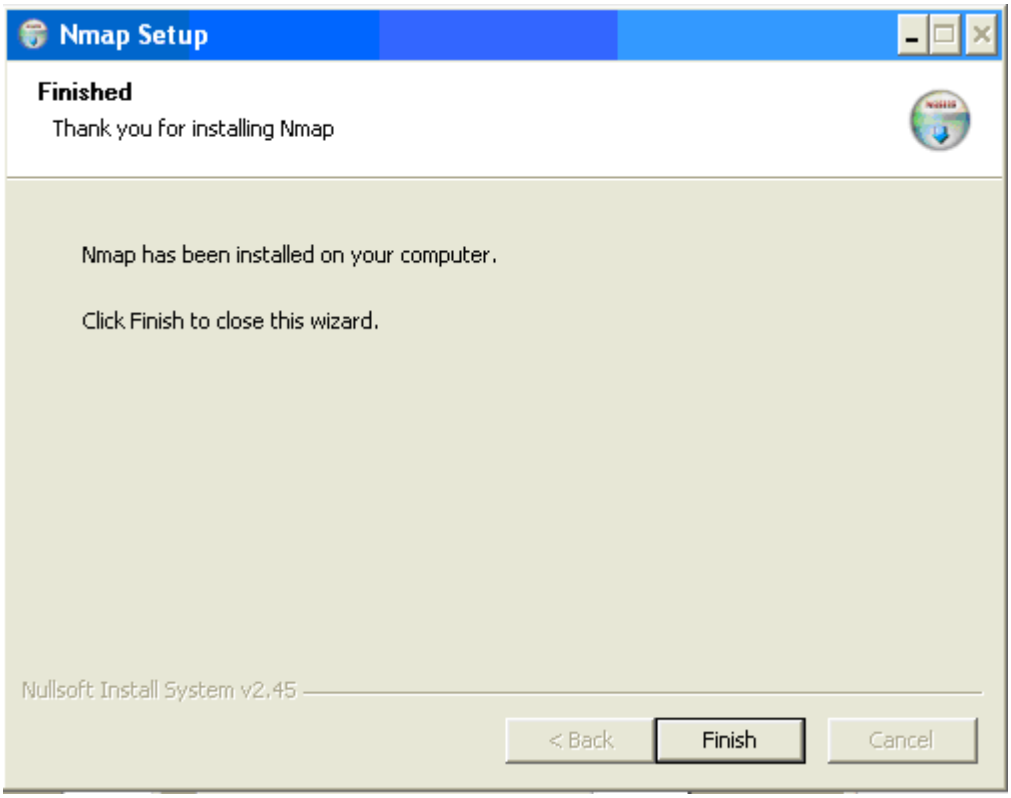


Figura 55 - Sexta tela de instalação do NMAP

ANEXO E - INSTALAÇÃO ETHEREAL

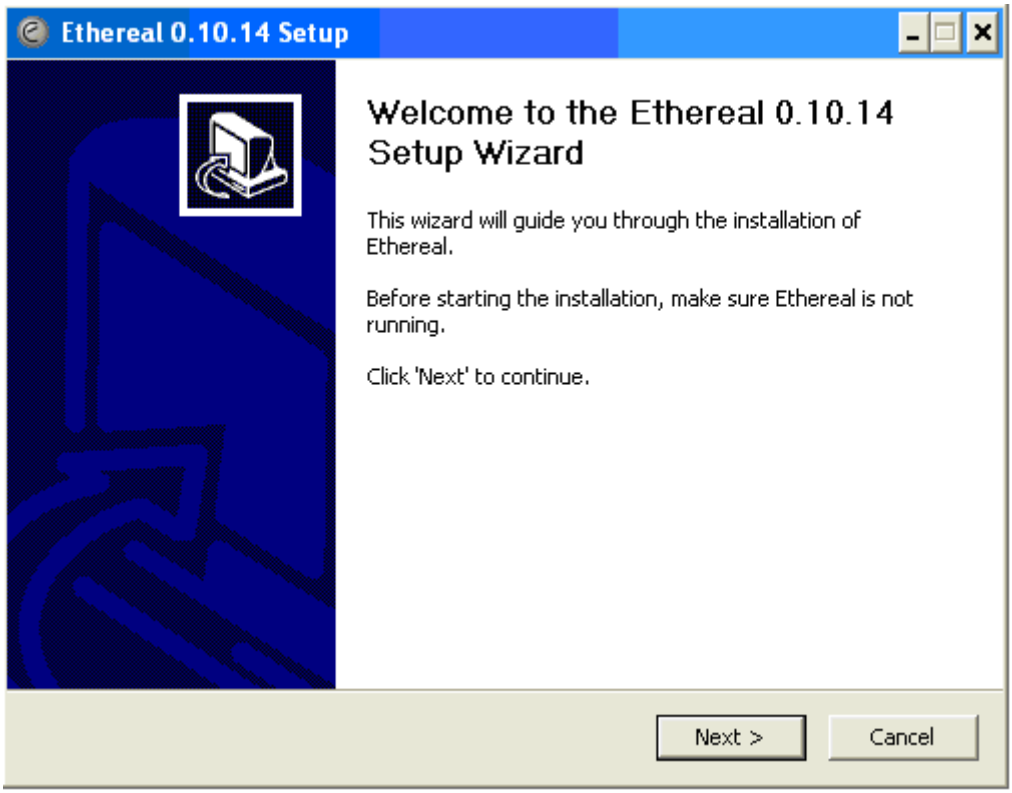


Figura 56 – Primeira tela de instalação do Ethereal

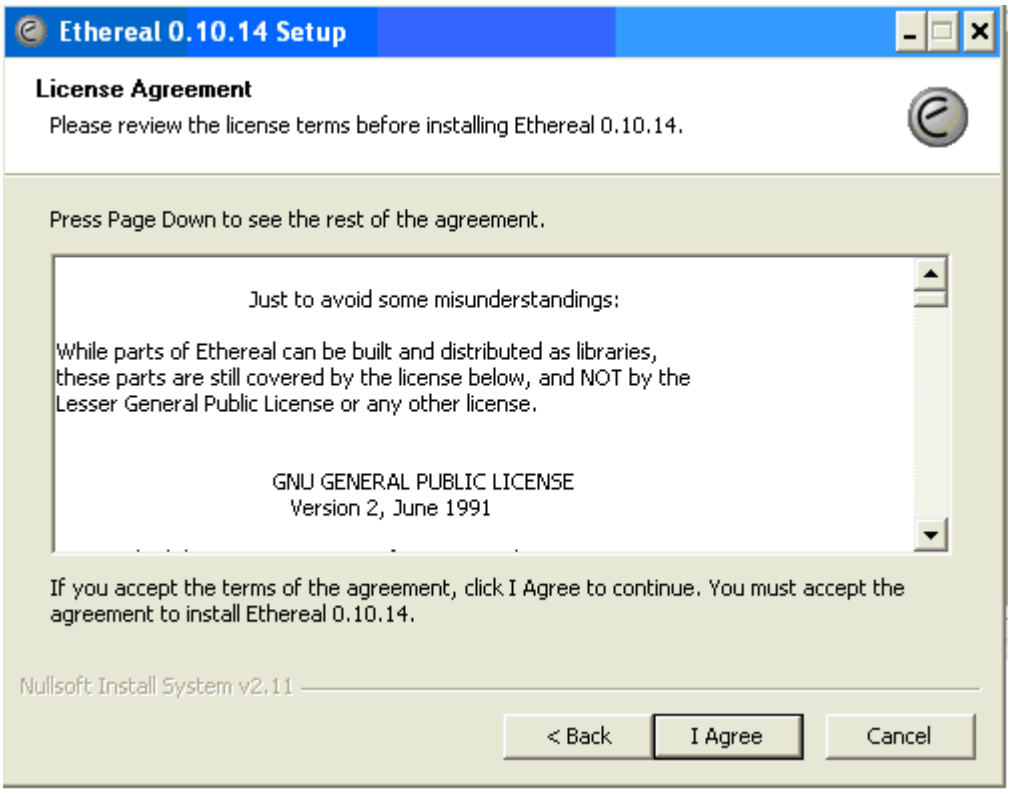


Figura 57 – Segunda tela de instalação do Ethereal

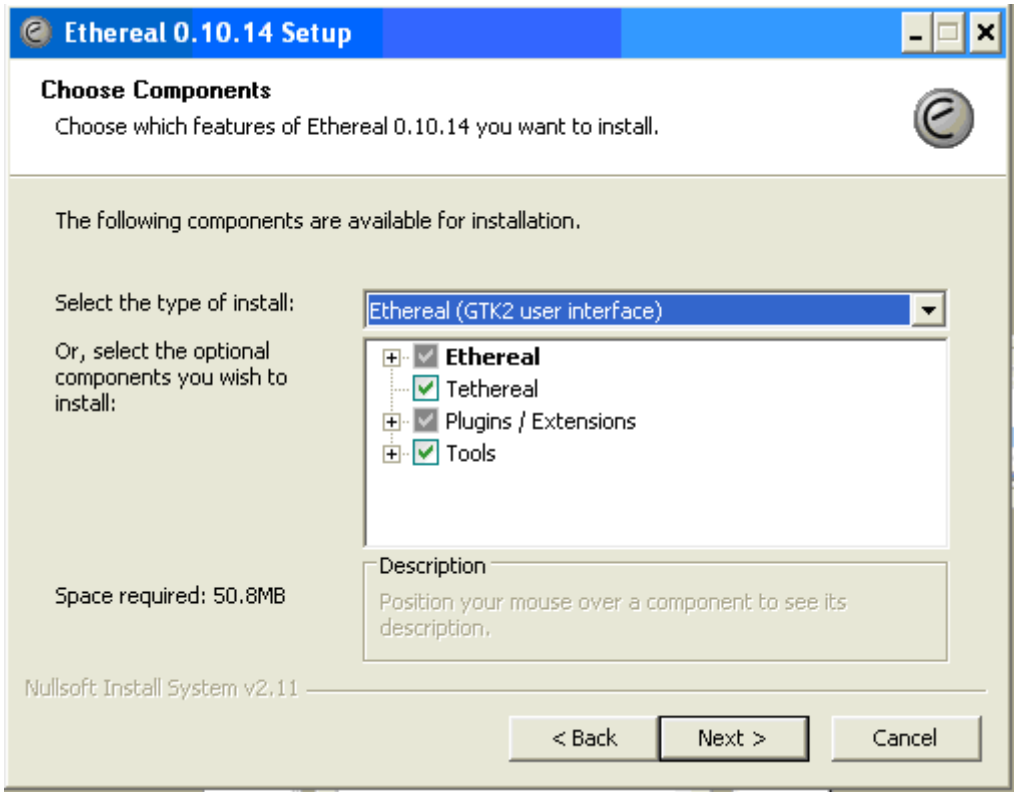


Figura 58 – Terceira tela de instalação do Ethereal

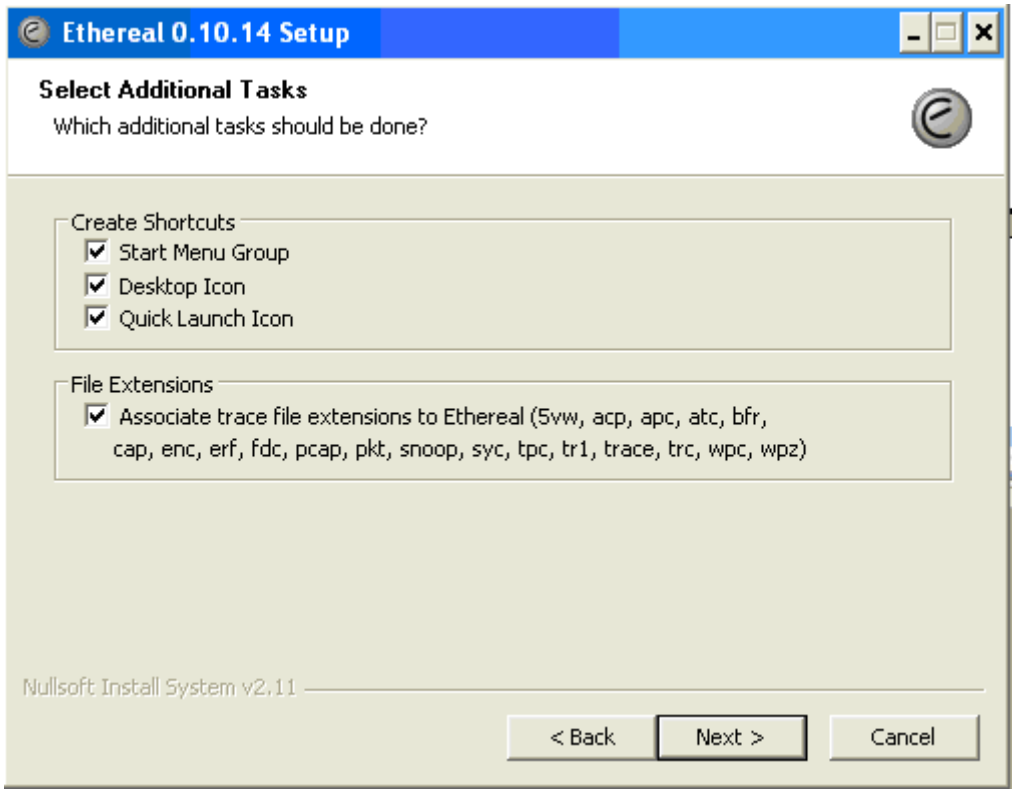


Figura 59 – Quarta tela de instalação do Ethereal

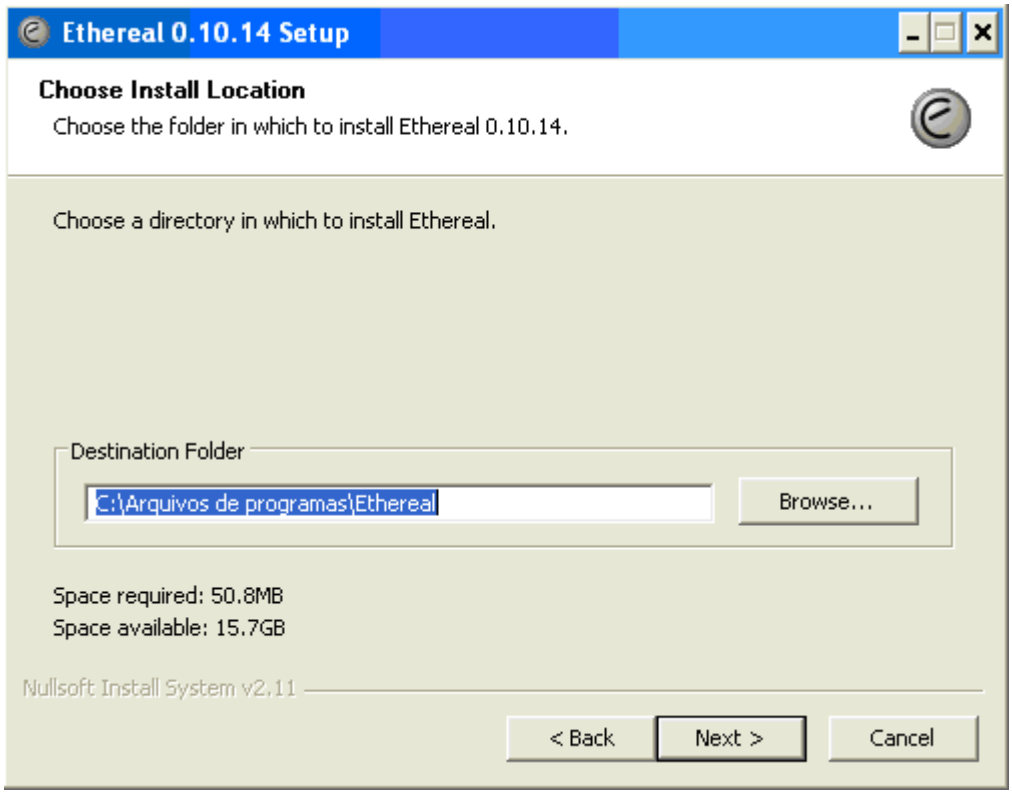


Figura 60 – Quinta tela de instalação do Ethereal

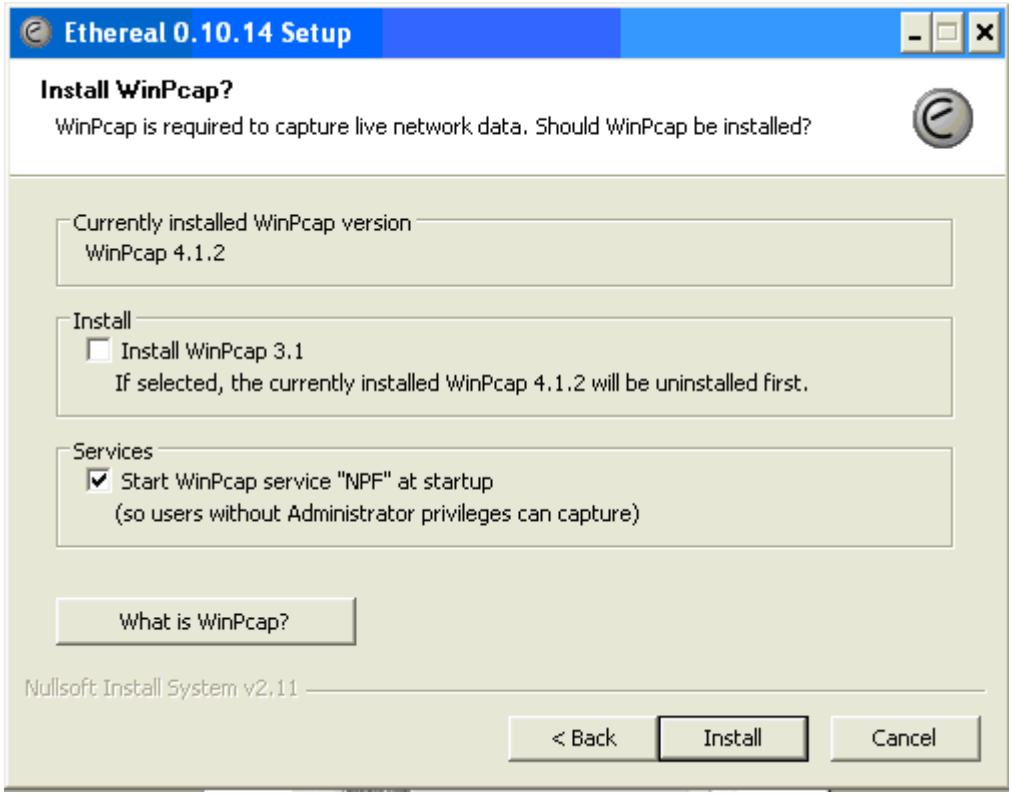


Figura 61 – Sexta tela de instalação do Ethereal

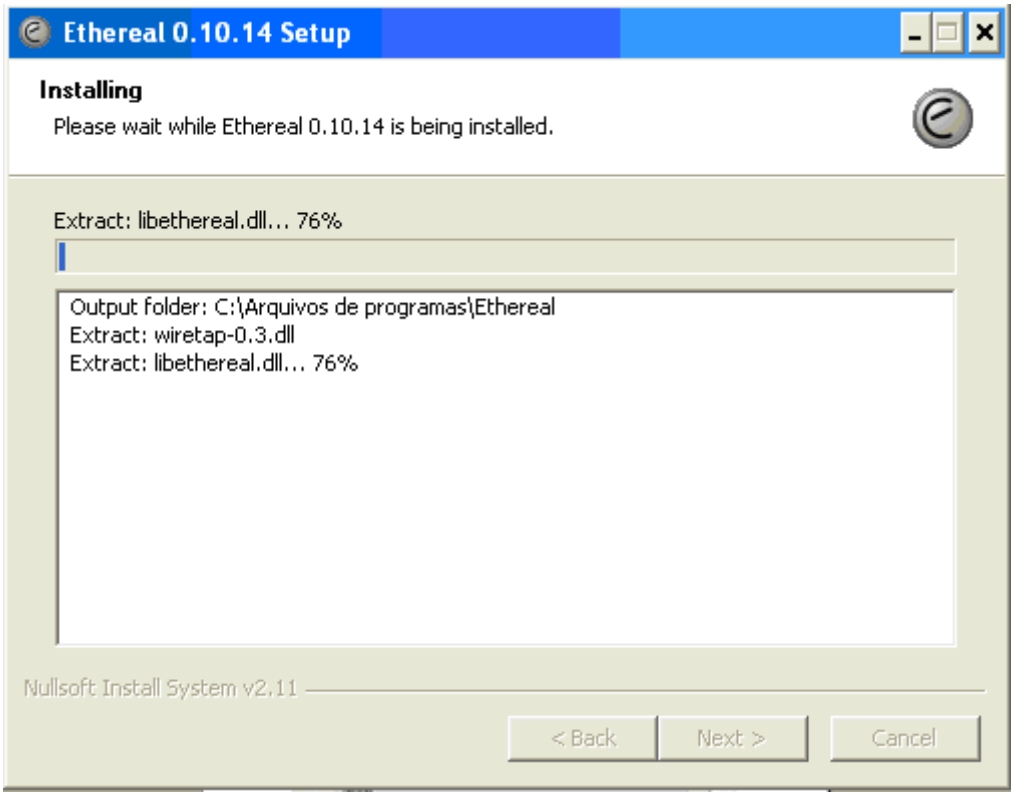


Figura 62 – Sétima tela de instalação do Ethereal

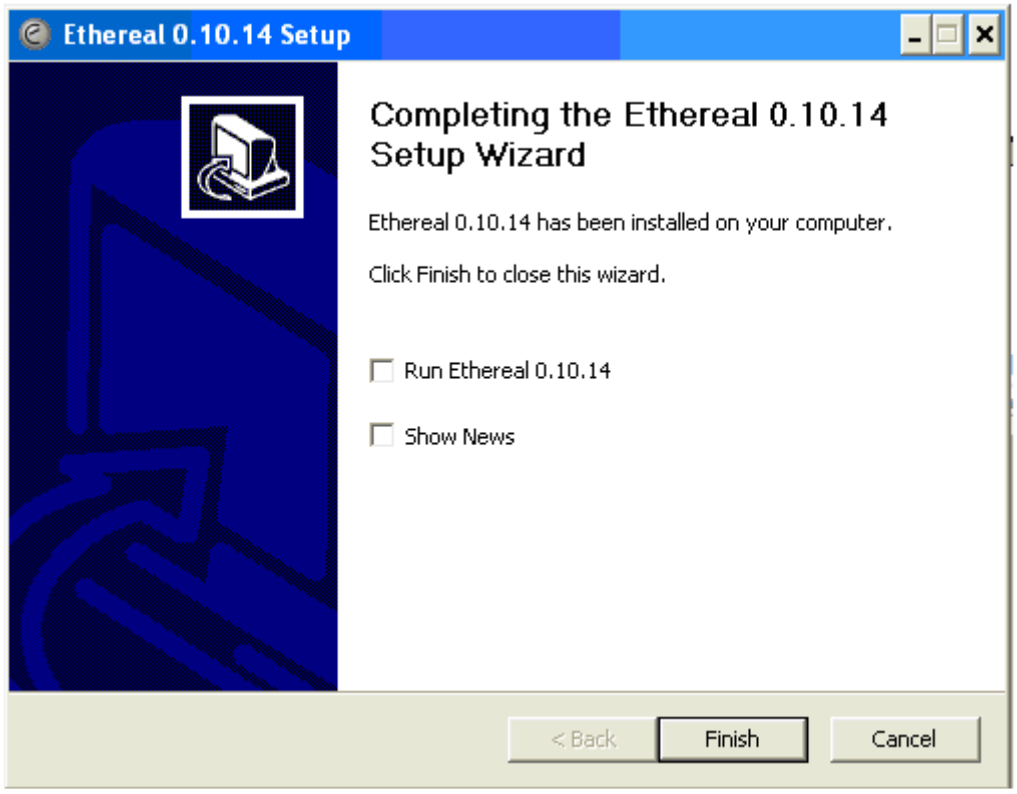


Figura 63 – Oitava tela de instalação do Ethereal