número 7 Semestral I Junho 2003

Instituto Superior Politécnico Gaya

Politécnica

7

Investigação I Divulgação I Curiosidades

Sumário

Revista Politécnica nº 7

Director	João de Freitas Ferreira
Director Adjunto	José Manuel Moreira
Corpo Editorial	Mário Dias Lousã
	António Inácio do Carmo
	Manuel Jorge Sá
	Joaquim Moura Relvas
Comissão Científica	Armando Coelho Silva (Univ. Porto)
	Augusto Ferreira da Silva (ISPGaya)
	Ferreira da Silva (Univ. Porto)
	João Álvaro Carvalho (Univ. Minho)
	Joaquim Agostinho (Univ. Porto)
	José Manuel Moreira (ISPGaya)
	Maciel Barbosa (Univ. Porto)
	Moura Relvas (ISPGaya)
	Nelson Neves (ISPGaya)
Marketing e Relações com o Exterior	José Duarte Santos
Secretariado	Andreia Reis
Editor	João de Freitas Ferreira
Design	José Eduardo
	Jeduardo_designer@clix.pt
Pré-impressão e impressão	Claret - Companhia Gráfica do Norte
	Rua do Padrão 83
	4415-284 Pedroso

Tiragem: 500 exemplares

Preço número avulso: € 3,25

Propriedade da CEP - Cooperativa de Ensino Politécnico, CRL

Administração e redação:
Instituto Superior Politécnico Gaya
Rua António Rodrigues da Rocha 291, 341 – Santo Ovídio
4400-025 Vila Nova de Gaia
Tels. 22 374 57 30
Fax 22 374 57 39

ISSN: 0874-8799
Registo DGCS nº 123623
Depósito Legal nº 153740/00
Publicação semestral

Editorial

Serão as Instituições do Ensino Superior Privado empresas lucrativas?

João de Freitas Ferreira
Presidente do Instituto Superior Politécnico Gaya
Rua António Rodrigues da Rocha, 291, 341
Santo Ovídio, 4400-025 Vila Nova Gaia

Faz parte do consciente colectivo dos portugueses conceber as instituições do ensino superior privado, em Portugal, como sendo empresas lucrativas, que buscam criar património com as propinas pagas pelos alunos. Trata-se de uma visão menos justa e algo redutora. Por isso vamos abordar este tema, tentando provar que os objectivos do ensino superior privado são outros, bem mais altos e mais nobres.

1. A comparação da escola a uma empresa é já de si pouco feliz, se tivermos em consideração o seu objecto e a matéria que transforma.
A empresa é uma unidade de produção ou de prestação de serviços característica da economia de mercado capitalista. Adquire determinadas matérias primas e transforma-as adicionando-lhes mais valias cobiçadas pelo mercado; cria ou inventa artigos, que promovem o progresso e são de aplicação directa na vida quotidiana das pessoas; ou presta serviços directos à comunidade. Em suma, as empresas produzem e transaccionam mercadorias. Trata-se de uma actividade fria e neutra que implica pouco mais do que a realização de tarefas repetitivas a exigirem, sim, grande responsabilidade, fino trato e rigor de execução. Todavia, entre o mestre e o objecto criado não há revelação de sentimentos nem marcas pessoais, mesmo que o artista plasme na sua obra algo de si e nela deixe a sua assinatura. O ensino superior (público ou privado), ao contrário, não lida com mercadorias. A matéria prima que as escolas superiores trabalham é a pessoa humana. Do ponto de vista individual, as escolas superiores devem formar cada um dos seus estudantes para a liberdade responsável, a maturidade em ordem a tomar decisões pessoais, a abertura ao futuro, a flexibilidade na mudança de atitudes e a adaptação a situações novas, a sensibilidade perante os problemas locais, regionais, nacionais e internacionais e a originalidade pessoal apoiada numa atitude crítica. Dentro da dimensão comunitária, o ensino superior deve formar cada um dos seus estudantes para a solidariedade com o mundo em que está inserido, a responsabilidade participativa, o respeito pelas ideias e pela consciência dos outros e o compromisso na construção da fraternidade humana. Cientificamente, compete ao ensino superior "inovar e transferir conhecimentos", para que os seus alunos possam desenvolver as suas capacidades teórico-práticas, de modo a que, conciliando a investigação e a prática profissional, atinjam altos graus de qualidade e excelentes níveis de desempenho nas empresas.
O relacionamento entre o professor e a matéria em transformação tem características profundamente pessoais e humanas, pois de pessoas se trata. O aluno não é aquele diamante bruto que se deixa lapidar, passivamente, pelo professor; ele recebe do mestre o espírito criador, e torna-se o verdadeiro ourives do seu próprio carácter e cria a sua marca pessoal. O valor acrescentado com que o novo técnico se apresenta no mercado de trabalho pertence ao seu património pessoal, é um misto de valor real e valor estimativo. Totalmente inalienável.
Por aqui se vê que as escolas superiores não são, stricto sensu, empresas; mas, sim, sociedades de interesse público, com funções complementares de apoio à comunidade e às empresas, pois lhes prestam serviços qualificados pela "mais valia de conhecimento e de inovação" que comportam.

2. Quando se rotulam, vulgarmente, as instituições do ensino superior privado como empresas, pretende-se fazer uma referência elogiosa à sua gestão interna como sendo muito boa, em oposição à gestão das escolas públicas, que se considera menos boa. Neste ponto, concordamos com a opinião do Prof. José Lopes da Silva, Reitor da UTL, quando escreve: "ataca-se a gestão universitária (pública) como se ela fosse generalizadamente caótica, despesista, alheada do mundo que a rodeia. Os critérios empresariais, válidos e seguros para os domínios para os quais foram concebidos, não podem ser transpostos, sem mais, para a

Universidade, seja ela pública ou privada. Não pode haver enxertos. São dois mundos distintos, que devem colaborar e ter pontes. Agora, o que é fundamental quer nas empresas, quer nas Universidades é que haja boa gestão" (Jornal da FENPROF, Sup ao nº 183, Fev. 2003, pág. 19). Nada mais certo. Por vezes, cai-se no exagero de se dar mais importância ao rigor formal da ciência da gestão do que ao relacionamento pessoal e humano que deve presidir a todo o acto educativo.

3. Serão estas sociedades, de facto, lucrativas? José Manuel Fernandes no seu editorial do Público, publicado no dia 30-10-02 com o título "o pecado do lucro" põe o dedo na ferida. A propósito do debate sobre a empresarialização da gestão hospitalar, conclui que grande parte dos portugueses aceita "como axioma irrefutável: lucro e serviço público são inconciliáveis; ter lucro é quase tão vergonhoso como roubar; e não há pior pecado do que ter lucro com a doença alheia". O mesmo pensarão muitos portugueses acerca da gestão escolar, sobretudo no que se refere ao subsistema do ensino superior privado.
Na verdade, há três tipos de sociedades: umas são *sem fins lucrativos*, pois assumem atitudes altruístas e visam apenas dar resposta às necessidades dos seus sócios; outras são *de fins não lucrativos*, dado que pretendem satisfazer as necessidades dos seus associados sem, contudo, procurarem o lucro pelo lucro; e outras são *com fins lucrativos*, que intentam o lucro pelo lucro, isto é, através de actividades económicas, procuram incrementar o património da sociedade, obtendo ganhos, que se destinam a ser distribuídos pelos sócios. Em qualquer destas sociedades, o lucro está sempre presente e é bem visível, variando apenas a maneira como ele é procurado ou o processo como é repartido. Em nenhum dos casos, todavia, se vê razão para que o lucro seja anatematizado como um pecado pessoal ou social. As instituições privadas de ensino superior são sociedades de fins não lucrativos. Portanto têm lucros oriundos das propinas dos alunos, que se destinam a assegurar o bom funcionamento dos cursos e a garantir novos investimentos. O retorno destes investimentos, em princípio, não é distribuído pelos sócios. Mais, enquanto que as sociedades com fins lucrativos, concluído o produto final, o vendem no mercado, integrando as mais valias de produção, as escolas superiores, terminada a formação dos seus alunos, atribuem-lhes um diploma profissional e oferecem-nos às empresas de modo gratuito.

4. Dissemos atrás que os lucros do ensino superior não são para repartir pelos sócios. Será então o ensino superior um investimento sem retorno? Se há retorno a quem se destina? Quem são os seus beneficiários?
O investimento feito no ensino superior tem realmente retorno. Os grandes beneficiários do mesmo são os próprios alunos e os contribuintes em geral. Todo o retorno vai direitinho para eles.
Os alunos, ao longo do seu curso, adquirem conhecimentos e desenvolvem capacidades que lhes permitirão aceder a empregos bem remunerados, criar a sua própria empresa e acompanhar o desenvolvimento do progresso, promovendo, se necessário, a sua auto-reconversão profissional.
Mas não é só o aluno que beneficia com o aumento da sua qualificação científica e técnica. O desenvolvimento de um país depende, em grande parte, do nível de escolaridade e da qualificação profissional da sua população. Eugénio Rosa, no seu recente estudo "Baixa escolaridade e qualificação: obstáculos ao desenvolvimento", embora reconheça não dispor de dados rigorosos, afirma que a produtividade média de um licenciado (€ 56.629,8) é 4,25 vezes superior à de um trabalhador com apenas o 1º ciclo básico (€ 13.324,7), 2,83 vezes superior à de um trabalhador com o 2º ciclo básico (€ 19.987,0), 1,89 vezes superior à de um trabalhador com o 3º ciclo básico (€ 29.980,5) e 1,42 vezes superior à de um trabalhador com o secundário completo (€ 39.974,0). Estes dados, só por si, já são muito reveladores da importância da escolaridade dos trabalhadores na

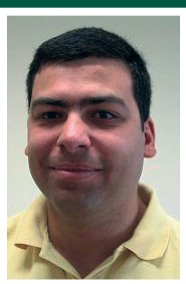
melhoria dos índices de produção. Mas o autor é ainda mais cáustico, quando refere que a causa da baixa produtividade das nossas empresas reside na falta de licenciados, sobretudo nas áreas científicas e tecnológicas. Em Portugal, só 7,8% da população empregada tem o grau de licenciatura, menos de metade da média dos países da União Europeia.

Poderíamos ser levados a pensar que, mesmo assim, só os licenciados é que beneficiam deste retorno. Eugénio Rosa desfaz o equívoco, dizendo que "apenas uma parte do que produz - 37% - reverte directamente para cada trabalhador. A outra parcela, que é a maior, e que em valor absoluto (em euros) é tanto maior quanto maior é a escolaridade do trabalhador, reverte para outros portugueses".
Portanto o investimento feito no ensino superior público e privado tem retorno. Os contribuintes e os portugueses em geral é que beneficiam, em grande parte, do valor acrescentado que o ensino superior promove.

5. Concluindo: As instituições do ensino superior público ou privado não podem ser vistas como empresas lucrativas. São antes sociedades de fins não lucrativos, dado que não procuram o lucro pelo lucro. Prestam um serviço público de alta qualidade e da maior importância, pois não é possível aumentar o desenvolvimento e o bem-estar nacionais sem aumentar a riqueza criada por cada trabalhador. E esta só pode ser aumentada se promovermos, a todos os níveis, a escolaridade e a qualificação profissional de todos os portugueses.
Assim sendo, não vemos motivos para que a sociedade portuguesa continue apreensiva com a iniciativa privada ao nível do ensino superior, como referimos no início deste trabalho. Cada vez mais serviços públicos são, hoje, geridos por sociedades privadas com sucesso. É apenas isto o que incomoda e se pretende desvirtuar. Como escreve J.M. Fernandes, "olha-se para o sucesso com inveja e condena-se o lucro como aberração, quando se deveria antes aferir se o sucesso foi obtido com mérito e se o lucro é legítimo e está a ser reinvestido. E sobretudo não se entende que, em lugar de tentar controlar tudo e abafar a iniciativa privada, se devia antes cultivar a ética empresarial e promover a responsabilidade social das empresas" (idem). Sejam dados, portanto, à iniciativa privada os meios para ela poder expandir a sua actividade e, através de auditorias rigorosas, garanta-se a alta qualidade do seu desempenho e fiscalize-se a aplicação dos seus "lucros".

Estabilidade/Instabilidade de Tensão

A Estabilidade de Tensão é um tema que tem vindo a ganhar cada vez mais importância, pois o aumento das cargas, as grandes distâncias entre os centros de consumo e de produção e o estado das redes de transporte e distribuição levam o Sistema Eléctrico de Energia (SEE) a operar em situações cada vez mais próximas do seu limite de estabilidade. Os próprios equipamentos de controlo automático existentes no SEE podem, eles próprios, conduzir o sistema para uma situação de instabilidade, se não forem tomados alguns cuidados.
Este documento pretende fazer uma apresentação deste fenómeno e das suas causas, bem como de algumas das formas de o controlar.
Futuramente será publicado um outro artigo onde é feita a apresentação de um método que permite medir a aproximação do sistema ao seu limite de instabilidade.



Jorge Leite dos Santos
jls@ispgaya.pt
ISPGaya
Rua Rodrigues da Rocha, 291, 341
Santo Ovídio, 4400-025 Vila Nova Gaia

Palavras Chave: Sistema Eléctrico de Energia, Estabilidade de Tensão, Limite de Estabilidade de Tensão, Colapso de Tensão.

1. Estabilidade e Instabilidade de Tensão

O problema da Estabilidade de Tensão é algo que tem vindo a preocupar os responsáveis pela exploração das redes eléctricas de transporte e distribuição de energia. Além de todos os outros problemas associados à garantia de fornecimento de energia a todos os clientes, à exploração óptima da rede e à manutenção de níveis de segurança de exploração, há que acrescentar mais este problema da Estabilidade de Tensão da rede.
Enquanto o sistema se mantiver estável, é possível controlar os níveis de tensão, em todos os barramentos, mantendo-os dentro dos valores desejados, mesmo que ocorram algumas perturbações. Ultrapassado o Limite de Estabilidade o sistema torna-se instável e o valor das tensões baixa de forma incontrolável.
A Estabilidade de Tensão num Sistema Eléctrico de Energia pode ser caracterizada como sendo a capacidade de manutenção dos níveis de tensão em todos os barramentos dentro de limites especificados [Fukunaga, Isono e Kondo 1982], quer em situações de funcionamento normal quer após o sistema ter sido sujeito a uma perturbação [Seifi e Imhof 1996].
Considera-se que o sistema entra numa situação de instabilidade quando uma perturbação, um aumento da carga ou uma alteração das condições do sistema provocam uma diminuição progressiva e incontrolável da tensão em pelo menos um dos barramentos do sistema.
A velocidade com que o fenómeno se processa, permite-nos tratar/estudar o sistema de uma forma estática [Kundur 1983], evitando assim a análise transitória (mais complexa).

2. Colapso de Tensão

A diminuição, de forma incontrolável, da tensão nos barramentos, poderá evoluir para o Colapso de Tensão do sistema. Normalmente, sempre que se verifica o colapso de tensão, grande parte da rede sai de serviço, o que implica longas horas de espera até que a rede volte a uma situação normal [Kundur 1983]. Muitas horas com a rede total ou parcialmente deslastrada significa grandes perdas monetárias (e não só) para as empresas vendedoras de energia eléctrica, já para não falar nos problemas associados à falta de energia nos consumidores industriais e domésticos.
O fenómeno de colapso de tensão é um processo complexo que se desenvolve em avalanche, lentamente no início, mas que evolui rapidamente na parte final, normalmente quando o ponto de funcionamento do sistema se situa na vizinhança da potência máxima transmissível [Erenia e Balan 1996, Barbier e Barret 1980].

3. Abordagem Matemática

Como primeira abordagem do problema da estabilidade de tensão, podemos considerar uma rede apenas com dois barramentos, conforme ilustrado na Figura 1.

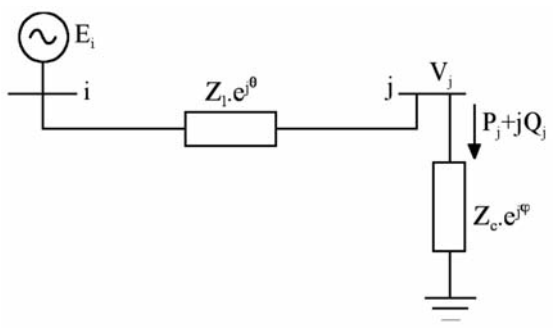


Figura 1 – Rede com 2 barramentos

Partindo da Figura 1, podemos construir o Gráfico 1:

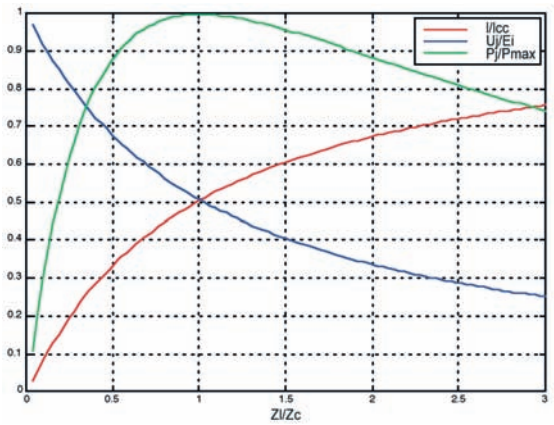


Gráfico 1 – Corrente, Tensão e Potência Activa

Conforme se pode verificar, após se ter atingido a igualdade entre a impedância da carga e a impedância da rede ($Z_l = Z_C$), por mais que a impedância da carga diminua, verifica-se que a potência entregue à carga vai também diminuir, não sendo o sistema capaz de acompanhar a crescente solicitação de potência da carga.

$$P_{max} = \frac{E_i^2}{Z_l} \cdot \frac{\cos\varphi}{2 + 2 \cdot \cos(\theta - \varphi)}$$

Quando é pedida à rede uma carga superior a P_{max}, a que corresponde $Z_l/Z_C>1$, o aumento da corrente não consegue compensar a queda de tensão verificada, passando o sistema para uma situação de instabilidade de tensão.

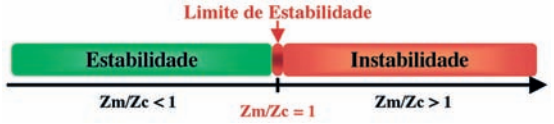


Figura 2 – Limite de estabilidade de tensão

4. Causas da Instabilidade de Tensão

A principal causa da instabilidade é a incapacidade de o sistema acompanhar a sua crescente necessidade de potência reactiva [Seifi e Imhof 1996], não compensado o aumento da queda de tensão provocada pelo trânsito de potência activa e reactiva nas reactâncias indutivas associadas à rede transporte e distribuição.
É cada vez mais difícil construir centrais geradoras junto dos centros de consumo, quer por razões económicas quer por questões ambientais, pelo que a distância entre centros produtores e consumidores é cada vez maior [Ajjarapu 1991]. Como é sabido, a reactância associada às linhas que efectuam o transporte de energia é proporcional ao seu comprimento, logo, esta situação é uma fonte de problemas para a estabilidade de tensão.

4.1. Regulação automática dos transformadores

Um outro aspecto a ter em conta é a regulação automática dos transformadores existentes nas subestações das redes de transporte e distribuição. De acordo com o esquema da Figura 3, a impedância montante vista do barramento 3 é dada por

$$Z_{m3} = Z_m/m^2 + jX_T \ ^*$$

se se considerar que a reactância de fugas do transformador se mantém constante com a alteração da relação de transformação.

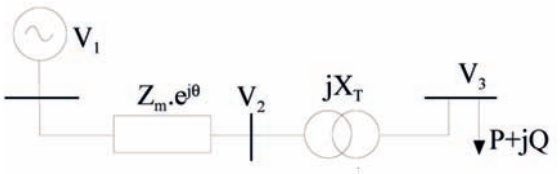


Figura 3 – Rede com transformador

Verifica-se, desta forma, que caso a regulação automática da tensão associada ao transformador decida aumentar a tensão à saída do transformador, por esta apresentar um valor baixo (normalmente associado a um aumento da carga), a relação de transformação irá baixar. Consequentemente, o valor da impedância montante vista pelo secundário do transformador irá aumentar. Esta situação pode piorar ou conduzir o sistema a uma situação de instabilidade. Se isso acontecer, sempre que o sistema de regulação automática tentar elevar a tensão, diminuindo a relação de transformação dos transformadores, verificar-se-á, na realidade, uma diminuição desta, entrando num ciclo vicioso que pode levar o sistema ao colapso de tensão.

* m representa a relação de transformação do transformador: $m=U_{1N}/U_{20}$.

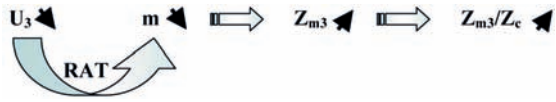


Figura 4 – Regulação Automática de Tensão

5. Evitar a Instabilidade de Tensão

Existem diversas formas para se tentar não atingir uma situação de instabilidade de tensão. Uma delas é a instalação de baterias de condensadores na rede, pois passaremos a ter uma injecção local de potência reactiva, diminuindo a queda de tensão nas linhas de transporte e distribuição.

Por outro lado, visto que tipicamente a rede a montante da carga tem características indutivas, a colocação de baterias de condensadores irá diminuir a impedância montante vista pela carga, afastando o sistema da instabilidade de tensão.

A configuração da rede é também muito importante, pois existem configurações que permitem explorar o sistema de transporte/distribuição mais ou menos próximas de um situação de instabilidade. A configuração a utilizar estará dependente do nível de segurança desejado e, obviamente, de questões económicas associadas à exploração óptima da rede.

Conforme foi referido em 4.1, os reguladores automáticos de tensão podem levar o sistema a uma situação de instabilidade, pelo que o seu funcionamento deverá ser bloqueado quando o sistema se aproximar do limite de estabilidade de tensão. Esta forma de controlo terá que estar obrigatoriamente associada a um sistema que consiga determinar a proximidade de uma situação de instabilidade de tensão.

Num próximo artigo será apresentada uma forma de "medir" o quão próximo o sistema se encontra do seu limite de estabilidade, por forma a permitir o controlo preventivo do sistema.

Referências

a) Artigos:

Venkatarama Ajjarapu, "Identification of Steady-State Voltage Stability in Power Systems", International Journal of Energy Systems, Vol. 11, Nº 10, 1991

Claudine Barbier, Jean Paul Barret, "Analyse des phénomènes d'écroulement de tension sur un réseau de transport", Paper RGE, Tome 89, N°10, CIGRE, Outubro de 1980

J. Trecat, M. Erenia, C. Bulac, Gh. Balan, "Voltage Stability Evaluation Indices", Paper APT 426-20-09, Power Tech, Atenas, Agosto de 1986

S. Abe, Y. Fukunaga, A. Isono, B. Kondo,"Power System Voltage Stability", Paper 82 WM 121-2, IEEE/PES Winter Meeting, Janeiro de 1982

H. Seifi, K. Imhof, "Voltage Stability Analysis in an Energy Management System – A Practical Implementation", 12th Power Systems Computation Conference, Dresden, Agosto de 1996

b) Livros:

Prabha Kundur, "Power System Stability and Control", McGraw Hill, 1983

Sistemas de Informação: uma abordagem introdutória

Os Sistemas de Informação são parte integrante de uma organização moderna e pró-activa. Neste documento efectua-se uma breve caracterização dos diversos Sistemas de Informação e apresentação do seu papel na gestão organizacional.

António Mendes Pereira
amp@ispgaya.pt
ISPGaya
Rua Rodrigues da Rocha, 291, 341
Santo Ovídio, 4400-025 Vila Nova Gaia

José Duarte Santos
jdsantos@ispgaya.pt
ISPGaya
Rua Rodrigues da Rocha, 291, 341
Santo Ovídio, 4400-025 Vila Nova Gaia

Palavras chave: Sistemas de Informação, Tecnologias de Informação.

1. A importância dos Sistemas de Informação

O aparecimento de uma economia global, a transformação da economia baseada na indústria para uma economia baseada em serviços e conhecimento tem vindo a alterar o posicionamento das organizações no mundo dos negócios [Laudon e Laudon, 2003].

A utilização da informação correcta proporciona à organização um planeamento mais eficaz, uma tomada de decisão mais consciente e proporciona melhores resultados. A informação é vital para a sobrevivência de um organização no mundo moderno, reduzindo a incerteza adjacente que a rodeia [Adeoti-Adekeye, 1997].

Os Sistemas de Informação (SI) providenciam ao gestor a possibilidade de aceder a essa informação, permitem alargar o conhecimento que é um recurso importante para a organização, tendo vindo a alterar a forma de fazer negócio [Laudon e Laudon, 2003].

A informação como recurso deve ser gerida de forma conveniente, pois existem custos associados [Adeoti-Adekeye, 1997], com a sua obtenção e manipulação, que não devem ser menosprezados, e que nem sempre são possíveis de calcular. Mas, o facto de não ser possível determiná-los não implica que as organizações não devam aproveitar uma oportunidade por falta de informação [Rodrigues, 2002].

A rentabilização de um SI influencia a competitividade da organização [Rodrigues, 2002]. Kenneth Laudon e Jane Laudon [2003] reforçam esta ideia afirmando que os Sistemas de Informação e Comunicação são vitais para as empresas serem competitivas, devendo o SI ser visualizado e planeado como parte integrante do plano estratégico [Williams, 1997]. A escolha da tecnologia apropriada é assim influenciada não só pelo Sistema de Informação a implementar na organização, mas também pelo próprio *Business Plan* [Williams, 1997].

As empresas procuram adaptar-se às mudanças operadas na esfera da sua acção, recorrendo aos Sistemas de Informação e às Tecnologias de Informação (TI), mas por sua vez são também influenciadas, assim como a sociedade em geral, pelas mudanças operadas nos SI e nas TI [Rodrigues, 2002].

2. O conceito Sistema de Informação

Na definição de SI, podemos encontrar alguns aspectos comuns a diversos autores, como o facto de ser referenciado como um elemento que não é uno [Adeoti-Adekeye, 1997; Rodrigues, 2002; Laudon e Laudon, 2003]. É apresentado como um conjunto, de componentes [Laudon e Laudon, 2003], "procedimentos, actividades, pessoas e tecnologia" [Rodrigues, 2002, p. 18], que permitem recolher, processar, armazenar [Adeoti-Adekeye 1997; Rodrigues 2002; Laudon e Laudon, 2003], distribuir/transmitir [Laudon e Laudon, 2003; Adeoti-Adekeye 1997], "informação que vai servir de suporte à tomada de decisão, coordenação e controlo" [Laudon e Laudon, 2003, p. 7]. Adeoti-Adekeye [1997] refere ainda que o SI deve permitir encontrar os elementos guardados, ou seja, a "disponibilização da informação às pessoas que dela necessitam" [Rodrigues, 2002, p. 18].

Um SI deve ser encarado como o resultado da tecnologia implementada (hardware, software, comunicações...), dos componentes organizacionais (cultura, estrutura, políticas, pessoas, procedimentos,...) e da gestão existente (liderança, estratégias, parcerias,..) [Laudon e Laudon, 2003]. A figura seguinte retrata o enquadramento dos Sistemas de Informação.

Figura nº 1 – Enquadramento dos Sistemas de Informação.
Fonte: Laudon e Laudon, 2003, p. 11.

3. Dados e Informação

"Dados são factos isolados, representações não estruturadas" [Rodrigues, 2002, p. 12], sendo a informação o processamento desses dados que são apresentados de forma a serem úteis a um determinado objectivo [Laudon e Laudon, 2003].

A gestão da informação pressupõe disponibilizar a informação correcta, no local ideal, no momento certo, ao custo mais baixo possível, não esquecendo que deve estar na posse da pessoa correcta para a sua utilização [Adeoti-Adekeye, 1997]. A informação não tem o mesmo valor para todos os utilizadores e a sua relevância varia de acordo com a situação e a necessidade da organização [Rodrigues, 2002].

Celinas, Sutton e Oram [1999] mencionam as seguintes qualidades da informação:

- Eficácia: a informação deve ser relevante e pertinente, entregue atempadamente, de forma correcta, consistente e de modo utilizável.
- Eficiência: informação deve ser fornecida através da utilização mais produtiva e económica de recursos.
- Confidencialidade: protecção da informação sensível a utilizações não autorizadas.
- Integridade: cuidado na perfeição, na validação dos valores para irem de encontro às expectativas empresariais.
- Disponibilidade: a informação deve estar disponível quando solicitada pela organização, no presente e no futuro. É também importante salvaguardar os recursos e as capacidades organizacionais.
- Condescendência (submissão): a informação deve estar de acordo com as leis, regulamentos ou contratos externamente impostos aos critérios empresariais.
- Confiança: a informação deve ser credível para a gestão poder trabalhar.

4. As Tecnologias de Informação

As tecnologias têm vindo a proporcionar diferentes formas de recolher, processar, armazenar, disseminar e utilizar a informação [Adeoti-Adekeye, 1997].

A utilização de computadores, software, tecnologia de armazenamento, tecnologia de comunicação, constituem a infraestrutura tecnológica do Sistema de Informação, que deve ser concebida de acordo com os objectivos e as especificidades da organização e gerida de forma a prestar um serviço de alto nível [Laudon e Laudon, 2003].

5. A relação entre os níveis de gestão e os SI

Uma organização é única, apresentando aspectos únicos, como a missão, objectivos, dimensão, estrutura e outros factores caracterizantes, verificando-se no entanto, elementos comuns como a existência de níveis de gestão e áreas funcionais [Varejão, 1998], que são comuns aos diversos níveis do Sistema de Informação: vendas/marketing, produção, finanças, contabilidade e recursos humanos [Laudon e Laudon, 2003].

A complexidade dos Sistemas de Informação depende do nível de gestão, identificando Williams [1997] e Senn [2000] três níveis de sistema, enquanto Kenneth Laudon e Jane Laudon [2003] consideram quatro, situando-se a diferença no nível do conhecimento.

Nível estratégico: nível mais complexo e envolvendo custos avultosos no SI, está orientado para a análise externa, para o meio envolvente, onde a organização opera, sendo a proveniência da informação essencialmente externa [Williams, 1997]. Situa-se no topo de uma organização, facilitando a tomada de decisão a longo prazo [Laudon e Laudon, 1999].

Nível táctico: as decisões de gestão são tomadas num espaço temporal mais curto, comparativamente com o nível anterior, devendo o SI proporcionar elementos que permitam à organização analisar o seu desempenho a nível global, departamental e aferir sobre a utilização de recursos [Williams, 1997], estabelecendo comparações entre os resultados num determinado período [Laudon e Laudon, 1999]. A origem da informação é interna e externa [Williams, 1997]. As necessidades de informação nem sempre são objectivas, devido às decisões nem sempre serem completamente estruturadas [Laudon e Laudon, 1999].

Nível conhecimento: núcleo que suporta o *know-how* e controla o fluxo de documentação, permitindo um maior desempenho por parte dos técnicos [Laudon e Laudon, 1999; Laudon e Laudon, 2003].

Nível operacional: neste patamar, a informação é quotidiana e importante para executar as tarefas básicas para o

funcionamento organizacional [Williams, 1997]. Regista as actividades e transacções, permitindo obter respostas a solicitações de rotina [Laudon e Laudon, 2003]. Conforme se vai descendo de nível verifica-se uma maior necessidade de quantidade de informação (menos sumária) e um aumento da existência de estrutura nas decisões [Senn, 2000].

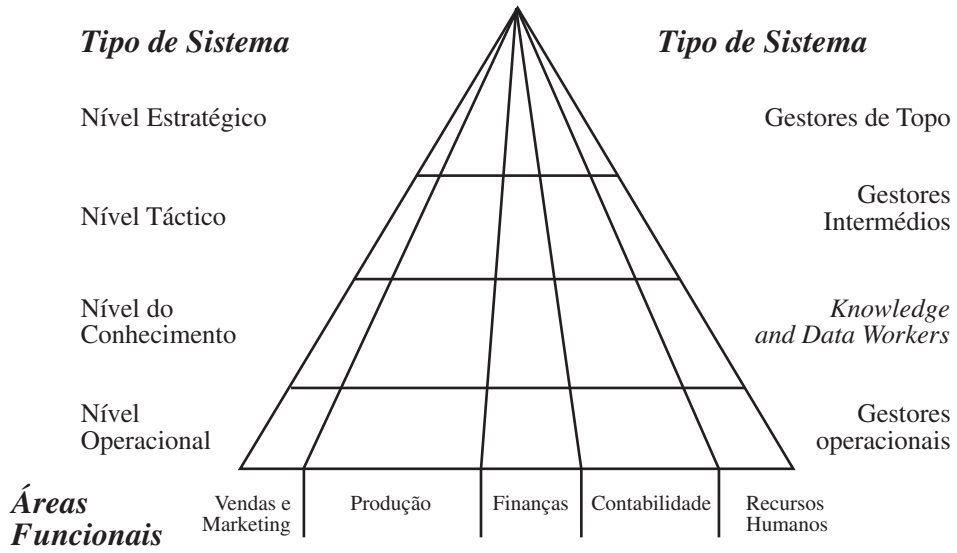


Figura nº 2 – Níveis de Sistemas de Informação.
Fonte: Laudon e Laudon, 2003, p. 39.

Os Sistemas de Informação descritos não se apresentam isolados nas principais funções organizacionais que suportam, verificando-se também a sua presença nos diversos níveis de gestão, conforme se pode verificar nos exemplos apresentados no quadro seguinte.

	Vendas/MKT	Produção	Finanças e Contabilidade	Recursos Humanos
Estratégia	Previsão de tendência das vendas	Localização de unidades de produção	Planeamento do lucro	Planeamento de recursos humanos
Táctico	Análise de preço	Planeamento da produção	Orçamentação	Sistema de compensações
Conhecimento	Análise de mercado	Desenho Assistido por Computador (CAD)	Análise da carteira de investimentos	Planeamento de carreiras
Operações	Processamento de encomenda	Controlo de máquina	Facturas a receber	Formação e desenvolvimento

Figura nº 3 – Exemplos de Sistemas de Informação nos diversos níveis e áreas funcionais.
Fonte: Adaptado de Laudon e Laudon, 2003, pp. 47, 49, 50.

A função financeira, operações, produção utilizam tradicionalmente os SI, enquanto Vendas/Marketing e os Recursos Humanos só recentemente começaram a tirar partido dos benefícios dos SI [Williams, 1997].

6. Categorias de SI

As necessidades da organização levaram ao aparecimento de diferentes categorias de Sistemas de Informação [Senn, 2000]. Segundo Senn [2000] existem três categorias: TPS (Transaction Processing Systems) Sistemas de Processamento de Transações, MIS (Management Informations Systems) sistema de informação de gestão, DSS (Decision Support Systems) Sistemas de Suporte à Decisão. Por sua vez, Laudon e Laudon [2003] consideram seis categorias, acrescendo às mencionadas, ESS (Executive Support Systems)[1], KWS (Knowledge Support Systems) e OAS (Office Automation Systems).

Tipos de Sistemas						
		Sistemas de Nível Estratégico				
	ESS	Previsão da tendência de vendas para 5 anos	Plano operacional para 5 anos	Previsão orçamental para 5 anos	Previsão de lucros	Planeamento de recursos humanos
		Sistemas de Nível Táctico				
	MIS	Gestão de vendas	Controlo do inventário	Orçamento anual	Análise dos capitais investidos	Análise de realocações
	DSS	Análise de vendas por região	Planeamento da produção	Análise de custos	Análise do preço/lucro	Análise de custos contratuais
		Sistemas de Nível do Conhecimento				
	KWS	Estações de engenharia		Estações gráficas		Estações administrativas
	OAS	Processador de texto		Arquivo electrónico de documentos		Agendas electrónicas
		Sistemas de Nível Operacional				
	TPS	Seguimento de encomendas	Controlo de máquinas	Estações gráficas	Facturas a pagar	Formação e desenvolvimento
		Processamento de encomendas	Controlo da movimentação de material	Gestão da caixa	Facturas a receber	Registo dos empregados
		Vendas e Marketing	Produção	Finanças	Contabilidade	Recursos Humanos

Figura nº 4 – Exemplos de Sistemas de Informação nas seis categorias.
Fonte: Adaptado de Laudon e Laudon, 2003, p. 40.

Executive Suport Systems (ESS)

Mais intuitivos de utilizar, com interface simplificado permite ao gestor de topo, aceder a informação resumida [Varejão, 1998]. Permitem ajudar a tomar decisões não rotineiras sobre problemas não estruturados e relacionados com a estratégia da organização, como por exemplo identificar oportunidades de negócio. São ferramentas flexíveis que possibilitam análises, comparação e prever tendências, apoiando-se em informação externa e interna. Dentro deste sistema é possível encontrar outros subsistemas como o Business Intelligence [Laudon e Laudon, 2003].

Management Informations Systems (MIS)

Tendo aparecido na década de 60, são uma consequência do aumento das capacidades de processamento dos computadores. Permitem uma selecção dos dados mais significativos, organizando-os de uma forma sumária [Varejão, 1998], com a finalidade de ajudar os gestores na tomada de decisão que é estruturada e resolução de problemas [Senn, 2000].

No MIS há um aproveitamento de informação proveniente das transações fornecida pelos TPS e de dados externos à organização [Senn, 2000].

Este sistema integra subsistemas de informação, dos quais se destaca o Sistema de Informação de Contabilidade (AIS-Accounting Information System) que interage e aglutina informação de outros subsistemas operacionais: Sistema de Informação de Vendas/Marketing, Sistema de Informação de Produção, Sistema de Informação de Finanças e o Sistema de Informação de Pessoal (RH) [Celinas *et al,* 1999].

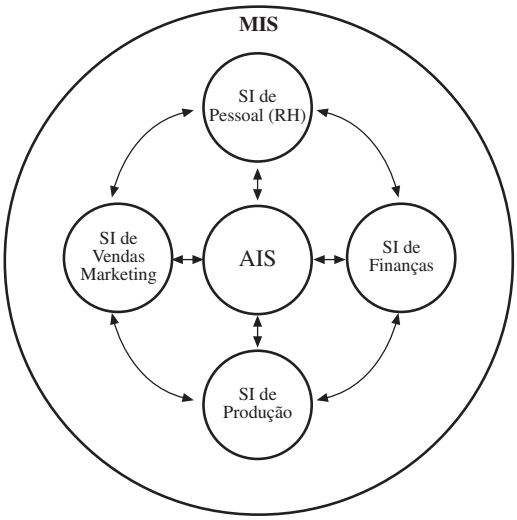


Figura nº 5 – O Sistema de Informação de Contabilidade como um subsistema do MIS.
Fonte: Celinas *et al*, 1999, p. 1-16.

Decision Support Systems (DSS)

A necessidade de tomar decisões no âmbito da gestão com base nos dados transaccionais levou ao aparecimento no início dos anos setenta, aos designados sistemas DSS [Rodrigues, 2002].

[1] Varejão (1998), refere-se a estes sistemas como EIS-Executive Information Systems.

Apoiam os processos de tomada de decisão, através das capacidades analíticas que possuem, sendo a sua construção muitas vezes realizada à medida de quem os utiliza por forma a permitir um melhor acesso e análise dos dados [Varejão, 1998].
Permitem condensar grande volume de dados, usando informação proveniente do TPS e do MIS [Laudon e Laudon, 2003].
A tomada de decisão é facilitada por estes sistemas, mesmo quando as situações estão semi-estruturadas [Senn, 2000].

Knowledge Support Systems (KWS) e Office Automation Systems (OAS).

Estes sistemas visam ajudar os trabalhadores do conhecimento, indivíduos cuja principal tarefa é ajudar a organização a possuir nova informação e novo conhecimento, e *os trabalhadores de dados,* que tem como principal função processar informação [Laudon e Laudon, 2003].
Os OAS apoiam a automatização dos escritórios, integrando os serviços de fax, processamento de texto, agendas electrónicas, correio electrónico, arquivo em formato electrónico de documentos e recorrem a outras aplicações que permitam aumentar a produtividade e comunicar com fornecedores e clientes [Laudon e Laudon, 2003].

Transaction Processing Systems (TPS)

Apareceram ao mesmo tempo que os primeiros computadores na década de 50 e têm como função processar os grandes volumes de dados provenientes das actividades operacionais das organizações [Varejão, 1998]. Visam substituir procedimentos manuais, melhorando as actividades rotineiras e estão relacionados com transações [Senn, 2000]. Permitem substituir a grande maioria do trabalho manual existente neste tipo de actividades, proporcionando o tratamento de encomendas, facturação, stocks, transacções financeiras, etc. [Varejão, 1998].
Disponibilização dos dados a partir dos TPS revela-se por vezes muito pouco funcional em termos de gestão, atendendo ao facto de lidarem com grandes volumes de dados que são criados em tabelas e listas [Varejão, 1998], sendo no entanto, os sistemas que providenciam informação para ser manipulada pelos outros sistemas apresentados [Laudon e Laudon, 2003].
Os sistemas estão integrados entre si, conforme se pode verificar na figura seguinte.

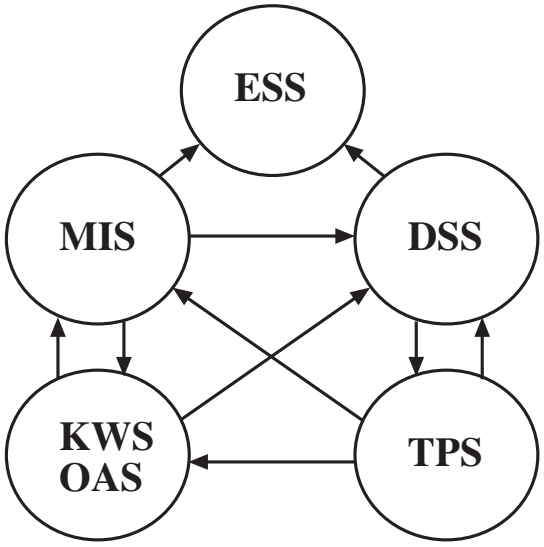


Figura nº 6 – Interligação ente os diferentes tipos de Sistemas de Informação.
Fonte: Laudon e Laudon, 2003, p. 46.

Os diferentes SI partilham informação que é recolhida através dos TPS e que reside numa base de dados, desempenhando os DMBS [Database Management Systems) um papel importante na sua gestão [Varejão, 1998]. A base de dados pode ser relacional, hierárquica, de rede ou orientada aos objectos [Laudon e Laudon, 2003].

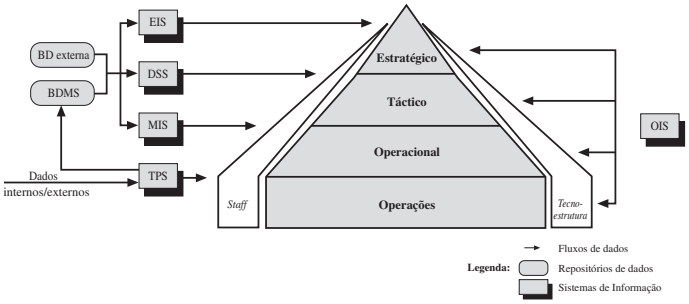


Figura nº 7 – Visão conceptual do suporte dos diversos tipos de SI à organização.
Fonte: Varejão, 1998, p. 67.

Além dos SI poderem ser analisados do ponto de vista do nível organizacional ou na perspectiva funcional, existem determinados Sistemas de Informação que são transversais e que suportam processos de negócio[2], como o CRM – Customer Relationship Management e o SCM – Supply

[2] "Processo de negócio refere-se à forma como o trabalho está organizado, coordenado e focalizado para introduzir valor no produto ou serviço" (Laudon e Laudon, 2003, p. 51).

Chain Management. Enquanto o primeiro centraliza-se nos clientes, o segundo diz respeito às actividades de aquisição, negociação e logística de matérias-primas, componentes e produtos, com o fornecedor, mas também na distribuição ao cliente [Laudon e Laudon, 2003].

7. Considerações finais

As organizações não conseguem sobreviver sem informação que pode ser de origem interna ou externa. Para conseguir rendibilizar essa informação, há necessidade de as instituições com ou sem fins lucrativos investirem em Sistemas de Informação, existindo diversas categorias com características específicas orientadas para as necessidades dos diversos níveis de gestão.

Independentemente desses níveis e das diferentes áreas funcionais existentes, a informação deve ser partilhada pelos diversos Sistemas de Informação que não são estanques.

A informação é considerada um activo chave que contribui para a ampliação do conhecimento da organização.

Referências

Adeoti-Adekeye, W. B., "The importance of management information systems", Library Review, Vol. 46, Nº 5, (1997), 318-327.

Celinas, Ulric J. Jr., Sutton, Steve G. e Oram, Allan E. - Accounting Information Systems, Cincinnati, South-Western College Publishing, 1999, 4th ed..

Laudon, Kenneth C. e Laudon, Jane P. - Administración de los Sistemas de Información, Prentice Hall, 1999, 3ª ed..

Laudon, Kenneth C. e Laudon, Jane P. - Essentials of Management Information Systems, Prentice Hall International Editions, 2003, 5th ed..

Rodrigues, Luís Silva - Arquitecturas dos Sistemas de Informação, FCA – Editora de Informática Lda, Lisboa, 2002.

Senn, James A. - Análisis y diseño de Sistemas de Información, McGraw-Hill, 2000, tercera edición.

Varejão, João Eduardo Quintela - *Arquitectura da Gestão* de Sistemas de Informação, FCA – Editora de Informática Lda, Lisboa, 1998.

Williams, L. T., "Planning and manging the information system – a manager's guide", *Industrial Management & Data Systems*, Vol. 97, Nº 5, (1997), 187-191.

Electromagnetismo e Relatividade Restrita

CONFERÊNCIA PROFERIDA
NA TARDE DE 16 DE MAIO DE 2003
NA SALA HENRY TILLO DA EXPONOR

O conhecimento da relação existente entre o Electromagnetismo e a Relatividade Restrita tem quase um século de existência. Surge em 1905, ano em que Albert Einstein publicou um artigo intitulado *Sobre a Electrodinâmica dos Corpos em Movimento*. Mas não é ainda suficientemente conhecida de um certo número de alunos dos cursos superiores de Engenharia. Começa-se por fazer um resumo histórico acerca da electricidade, do magnetismo e da relatividade restrita. Tenta-se depois mostrar, ainda que resumidamente, que as leis do magnetismo se podem considerar resultantes de algumas leis da electrostática e de algumas leis simples da relatividade restrita. Este procedimento mostra assim que a electricidade, o magnetismo e a relatividade restrita não constituem compartimentos estanques, mas sim uma entidade única e indivisível. Termina-se mostrando como chegar à *contracção de Lorentz* de uma maneira muito mais compreensível do que aquela que é habitualmente apresentada.

Joaquim Albuquerque de Moura Relvas
jmrr@ispgaya.pt
ISPGaya
Rua Rodrigues da Rocha, 291, 341
Santo Ovídio, 4400-025 Vila Nova Gaia

Parte 1 – Resumo histórico

Poderá parecer estranho, mas não o é, começarmos por nos referir a um acontecimento ocorrido há 65 milhões de anos: Um cometa, ou um asteróide, com 10 quilómetros de diâmetro, depois de ter atravessado a nossa atmosfera com a surpreendente velocidade de 30 quilómetros por segundo, embateu, com uma violência extrema, no local onde hoje se situa Chicxulub, no norte da península de Iucatão, no México. Este impacto provocou uma explosão equivalente à de centenas de milhões de bombas de hidrogénio, que deu origem à extinção da maior parte da vida na Terra, incluindo a dos dinossauros, entre os quais se situavam os grandes sáurios carnívoros. Mas sobreviveram alguns pequenos mamíferos, entre os quais o *purgatorius*, antepassado do homem.

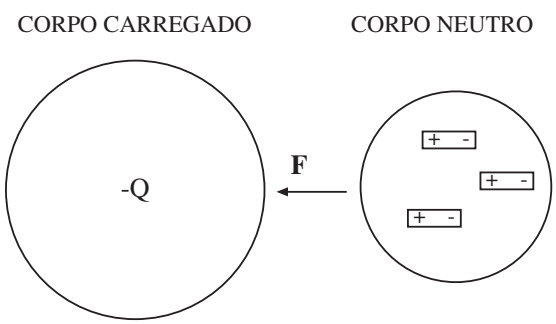
A explosão define o começo (fronteira K-T) da *Era Terciária*, que terminou há cerca de 1,64 milhões de anos. Foi durante essa era que os continentes tomaram a sua posição actual: a América do Sul uniu-se à América do Norte, deu-se a formação dos Alpes, que resultou da colisão das placas africana e euro-asiática, e deu-se a formação dos Himalaias, quando a Índia, que era então uma grande ilha triangular, se esmagou contra a Ásia. Foi também durante essa era que os mamíferos tomaram conta de todos os recantos ecológicos deixados vagos pela extinção dos dinossauros, tornando-se então os animais dominantes sobre a Terra. Foi ainda durante essa era que floresceram grandes florestas de coníferas. Entre as diferentes espécies dessas árvores, destacava-se uma espécie, já extinta, de pinheiros, o *Pinus succinifer.* Pelas cascas destes pinheiros escorria, em épocas mais quentes, a resina que deles brotava.

Vamos deixar agora que decorram alguns milhões de anos para dar tempo a que a resina dessas coníferas fossilize, transformando-se no que é actualmente designado por *âmbar*, mas que tem o nome científico *succinite*. A transparência do âmbar que, às vezes, se apresenta apenas translúcido e a sua cor amarela, com as mais variadas tonalidades, emprestavam-lhe uma beleza que foi muito apreciada, já na Antiguidade, pelos gregos. O âmbar foi conhecido desde o ano 600 a.C., ano em que Tales de Mileto observou que se podia fazer com que um pedaço dessa resina fossilizada adquirisse a propriedade de atrair pequenas partículas desde que fosse friccionado com um pedaço de pano. Essa propriedade resulta do que é hoje designado por *electricidade*, designação que resulta do nome «electron» (ηλεχτρον), dado pelos gregos ao âmbar.

E o que é a electricidade? A electricidade pode ser definida como a propriedade fundamental de certas partículas de matéria, tais como os protões e os electrões (que fazem parte dos átomos, constituintes normais da matéria), responsável pelas forças que se verificam entre duas delas, forças essas que, pela sua intensidade e natureza, não podem ser justificadas pela sua massa. Assim, por exemplo, entre dois electrões, ou entre dois protões, a força que se verifica é de repulsão. E a força atractiva verificada entre um electrão e um protão é muito maior do que a que resulta das suas massas. Dado que existem forças de atracção e de repulsão, infere-se a existência de duas formas, ou de dois "sinais", de electricidade: a *electricidade negativa*, atribuída, por razões de ordem histórica, aos electrões, e a *electricidade positiva*, atribuída, por razões idênticas, aos protões.

Dado que a propriedade *electricidade* se pode manifestar com maior ou menor intensidade, esta propriedade é associada a uma grandeza a que se pode dar o nome de *quantidade de electricidade*. Há, no entanto, agora que fazer aqui uma observação importante. É que a Comissão Electrotécnica Internacional considera actualmente obsoleto o termo *quantidade de electricidade*, que deve ser substituído pelo termo *carga eléctrica* [IEC, 1998]. O termo *carga eléctrica* deve também ser utilizado para substituir o termo *electricidade* utilizado para definir a referida propriedade dos electrões e dos protões. A Comissão Electrotécnica Internacional reserva actualmente [IEC, 1998] o termo *electricidade* para exprimir o *conjunto dos fenómenos associados às cargas eléctricas* (electrões e protões) e *às correntes eléctricas* (movimentos de electrões).

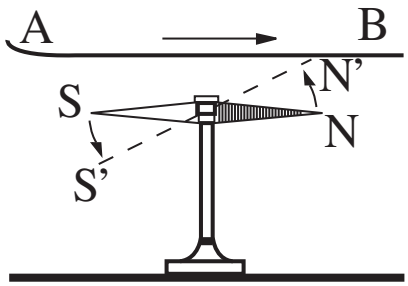
Estamos agora na posse dos elementos necessários para explicar a propriedade do âmbar, quando friccionado,



observada por Tales de Mileto. É que a fricção do âmbar com um pedaço de pano dá lugar a uma troca de cargas eléctricas entre o âmbar e o pano, ficando o âmbar com excesso de electrões, isto é, o âmbar passa, de corpo electricamente neutro, a constituir um corpo carregado com uma carga eléctrica negativa. Esta carga passa a repelir os electrões dos átomos de qualquer corpo neutro, colocado na sua vizinhança, e a atrair os seus protões. Se este pequeno corpo neutro for isolante, os seus átomos esticam, como se mostra na figura, formando os chamados *dipolos eléctricos elementares*, em que o centro de repouso estatístico de cada um dos seus protões fica mais próximo do âmbar com carga negativa do que o centro de repouso estatístico dos seus electrões. E, por conseguinte, a força eléctrica de atracção exercida pela carga negativa do âmbar sobre os protões do corpo neutro passa a ser maior que a de repulsão exercida sobre os seus electrões e então o corpo neutro é atraído pelo âmbar.

Tal como a electricidade, também o magnetismo já era conhecido na Antiguidade. Séculos antes da era Cristã, os gregos já sabiam que a magnetite, a que chamaram «pedra magnetica» (λίθοζ Μαυήτηζ), tinha a capacidade de atrair o ferro. De acordo com o que Lucretius Carus escreveu em *De Rerum Natura*, este mineral teve a sua origem na região dos «Magnetes» (Μαγνήτηζ) que eram os habitantes de Magnésia, em Tessália, na Ásia Menor. Vários filósofos gregos e romanos, nomeadamente o grego Tales de Mileto (640-546 a.C.), o grego Anaxágoras (500-430 a.C.) e o romano Lucretius Carus (99-55 a.C.), explicaram o poder atractivo dos magnetes, ou ímans, atribuindo-lhes uma alma ou uma origem interior de movimento, ou, alternativamente, uma emanação que passava através dos poros do ferro atraído, de modo que o ferro era puxado contra o magnete e aí ficava fixado. Curiosamente essa *alma* ou *emanação* existe de facto: é o que hoje se designa por *fluxo magnético*.

Decorreram vários séculos, desde o início da era Cristã, durante os quais se considerava que a electricidade e o magnetismo (conjunto de fenómenos associados aos campos magnéticos) tinham origens diferentes, até que, no decorrer do ano de 1820, o



físico dinamarquês Hans Christian Oersted descobriu que uma corrente eléctrica fazia mover uma agulha magnética colocada nas proximidades, como se a própria corrente eléctrica se comportasse como um íman. Meses mais tarde esta descoberta foi confirmada por Ampere quando verificou que uma bobina de fio percorrida por uma corrente eléctrica se comportava como um íman, ao atrair pequenos pedaços de ferro e, por isso, baptizou a bobina com o nome de *electroíman*. Estas descobertas chegaram ao conhecimento de Michael Faraday, filho do ferreiro James Faraday. Embora com uma formação escolar rudimentar, Michael Faraday, que durante a sua adolescência exercia o ofício de encadernador assalariado, era um autodidacta com conhecimentos apreciáveis de electricidade e de magnetismo obtidos com a leitura dos livros que encadernava. O conhecimento das descobertas de Oersted e de Ampere levaram Faraday à realização de numerosas experiências, donde resultaram as leis fundamentais do electromagnetismo, às quais, em 1831, Faraday, então com 40 anos e membro da Royal Institution, deu a seguinte forma verbal: *Sempre que uma força magnética aumenta ou diminui, produz electricidade; quanto mais depressa se dá esse aumento ou diminuição, mais electricidade se produz.* Em 1832 o físico escocês James Clerk Maxwell reduziu, na sua célebre obra *Tratado da Electricidade e Magnetismo*, a descoberta de Faraday à seguinte forma matemática:

$$\nabla \times \mathbf{E} = -\partial \mathbf{B}/\partial t$$

para significar que a "*quantidade de electricidade*" *produzida pelo magnetismo era igual à taxa de variação da força causadora.* A esta forma matemática Maxwell acrescentou as três seguintes:

$$\text{div}\ \mathbf{D} = \rho$$

$$\nabla \times \mathbf{H} = \mathbf{J} + \partial \mathbf{D}/\partial t$$

$$\text{div}\ \mathbf{B} = 0$$

Estas quatro equações constituem o que hoje se designa por

equações de Maxwell. Elas são afinal o elo final que unifica a electricidade e o magnetismo numa única entidade: o *electromagnetismo*.

No ano de 1905, Albert Einstein, então ainda um jovem funcionário da Repartição Suíça de Patentes em Berna, publicou, na revista *Annalen der Physik*, um artigo intitulado *Electrodynamik Bewegter Korper* (Electrodinâmica de Corpos em Movimento), que constitui a essência do que é hoje conhecido sob a designação *Teoria da Relatividade Restrita*. Este seu artigo inspirou-se no electromagnetismo, como, aliás, se pode verificar pela sua introdução que vale a pena ser aqui lembrada:

Como é sabido, a Electrodinâmica de Maxwell – tal como actualmente se concebe – conduz, na sua aplicação a corpos em movimento, a assimetrias que não parecem ser inerentes aos fenómenos. Consideremos, por exemplo, as acções electrodinâmicas entre um íman e um condutor. O fenómeno observável depende aqui unicamente do movimento relativo do condutor e do íman, ao passo que, segundo a concepção habitual, são nitidamente distintos os casos em que o móvel é um, ou o outro, desses corpos. Assim, se for móvel o íman e estiver em repouso o condutor, estabelecer-se-á em volta do íman um campo eléctrico com um determinado conteúdo energético, que dará origem a uma corrente eléctrica nas regiões onde estiverem colocadas porções do condutor. Mas se é o íman que está em repouso e o condutor que está em movimento, então, embora não se estabeleça em volta do íman nenhum campo eléctrico, há no entanto uma força electromotriz que não corresponde a nenhuma energia, mas que dá lugar a correntes eléctricas de grandeza e comportamento iguais às que tinham no primeiro caso as produzidas por forças eléctricas – desde que, nos dois casos considerados, haja identidade no movimento relativo.

Exemplos deste género, assim como o insucesso das experiências feitas para constatar um movimento da Terra em relação ao meio luminífero («Lichtmedium») levam à suposição de que, tal como na Mecânica, também na Electrodinâmica os fenómenos não apresentam nenhuma particularidade que possa fazer-se corresponder à ideia de um repouso absoluto. Pelo contrário, em todos os sistemas de coordenadas em que são válidas as equações da mecânica, também são igualmente válidas leis ópticas e electrodinâmicas da mesma forma – o que, até à primeira ordem de aproximação, já está demonstrado. Vamos erguer à categoria de postulado esta nossa suposição (a cujo conteúdo chamaremos daqui em diante «Princípio da Relatividade»); e, além disso, vamos introduzir o postulado – só aparentemente incompatível com o primeiro – de que a luz, no espaço vazio, se propaga sempre com uma velocidade determinada, independente do estado de movimento da fonte luminosa. Estes dois postulados são suficientes para chegar a uma electrodinâmica de corpos em movimento, simples e livre de contradições, baseada na teoria de Maxwell para corpos em repouso. A introdução de um «éter luminífero» revelar-se-á supérflua, visto que na teoria que vamos desenvolver não necessitaremos de introduzir «um espaço em repouso absoluto», nem de atribuir um vector velocidade a qualquer ponto do espaço vazio em que tenha lugar um processo electromagnético. Esta teoria vai apoiar-se – como qualquer outra Electrodinâmica – na cinemática do corpo sólido rígido, uma vez que as proposições de uma teoria deste género consistem na afirmação de relações entre corpos rígidos (sistemas de coordenadas), relógios e processos electromagnéticos. A insuficiente atenção a este facto é a raiz das dificuldades com que presentemente se defronta a electrodinâmica dos corpos em movimento.

Durante as décadas que se seguiram à publicação do artigo de Einstein de 1905 houve vários autores que obtiveram, a partir da Teoria da Relatividade, algumas leis do magnetismo que, até então, eram consideradas como conseguidas apenas a partir da experiência. Aqui basta que se faça referência apenas a dois autores. Um deles é Rosser que, no seu livro *An Introduction to the Theory of Relativity,* mostrou como obter a lei de atracção entre correntes paralelas, com o mesmo sentido, a partir da Teoria da Relatividade Restrita. O outro é o Professor Dias de Deus que, no seu livro *Introdução à Física*, calculou a influência de uma corrente eléctrica sobre cargas em movimento recorrendo apenas ao Campo Eléctrico e à Relatividade Restrita. Os dois mostram assim, entre muitos outros, que a Electricidade, o Magnetismo e a Relatividade Restrita não são entidades distintas.

Parte 2 – Uma revista e um livro

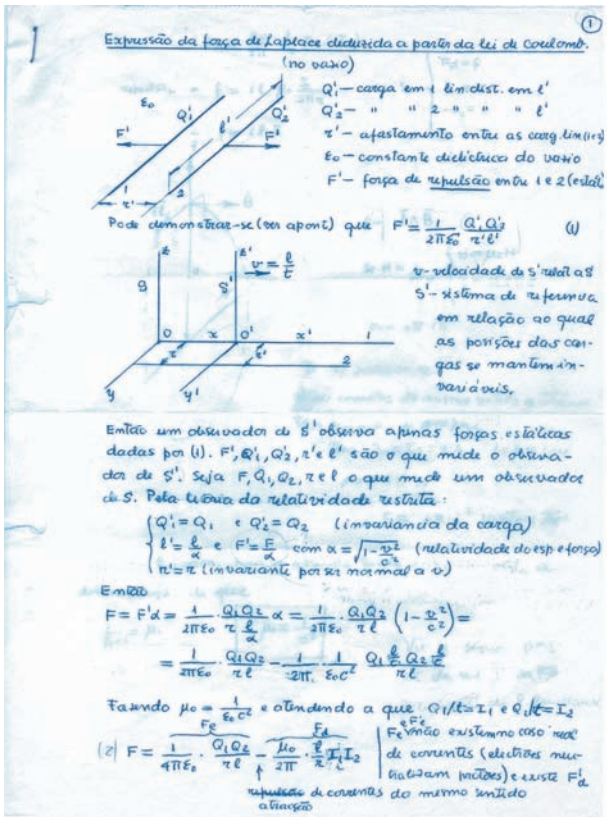
A relação existente entre o Electromagnetismo e a Relatividade Restrita chegou ao nosso conhecimento quando, há mais de 40 anos, ao consultarmos a Encyclopaedia Britannica, se nos deparou o seguinte trecho:

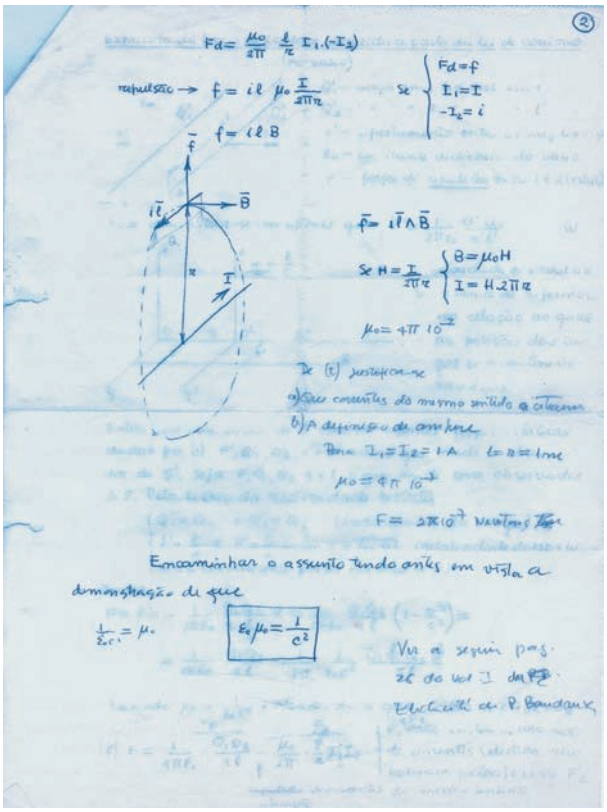
V. MAGNETIC FIELDS OF DIRECT CURRENTS

Under *Amperes and Volts*, above, the ampere was defined in terms of the force of attraction between long, straight, parallel wires carrying a direct current, and it was said that the law governing this force can serve well as a prototype for laws about electromagnetic forces in general: "Like charges repel, but like currents attract."

Like currents attract, one may say, *because* like charges repel. We saw why in the section *Special Relativity*. This magnetic attraction was required by relativity as a consequence of the motion of the electrons which carry the currents. In general, all magnetic forces can be regarded as requirements imposed by relativity on moving charges. The mathematics of these requirements is usually more complicated than in the case of straight wires, but the main idea is the same. So the contrast between the laws of "like charges" and "like currents" sets the tone for the whole system: the laws of steady magnetic fields are related to those of electrostatic fields by a system of contrasts.

donde se conclui que a frase <u>corrente</u> "*duas cargas eléctricas com o mesmo sinal repelem-se, <u>mas</u> duas correntes com o mesmo sentido atraem-se*" deve ser substituída pela frase <u>correcta</u> "*duas correntes com o mesmo sentido atraem-se <u>porque</u> duas cargas com o mesmo sinal se repelem*". Esta ocorrência levou-nos à elaboração do seguinte manuscrito:



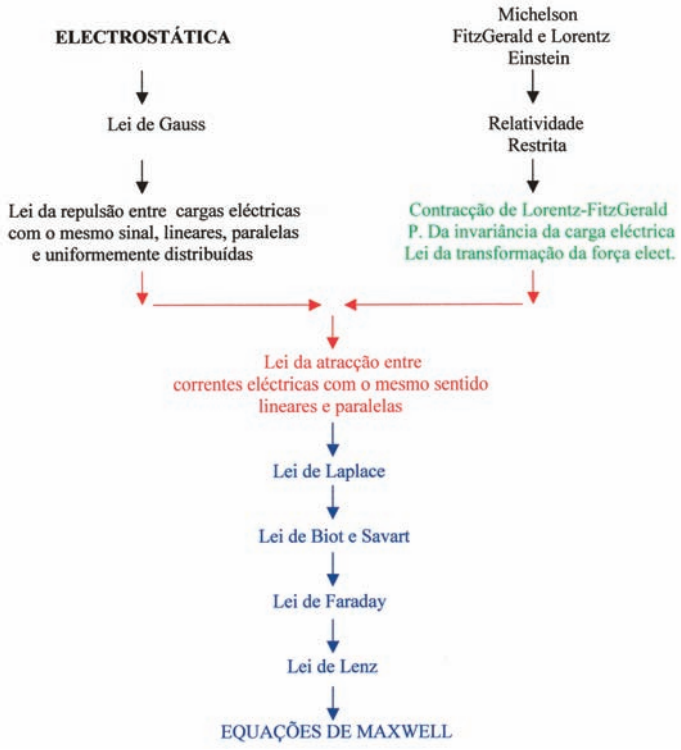


A elaboração deste manuscrito foi-nos possível graças aos conhecimentos que adquirimos, há 60 anos, na Universidade de Coimbra[*]. O manuscrito foi metido numa gaveta e aí ficou esquecido durante 40 anos, até que, no segundo semestre de 1999, fomos convidados para fazer parte da direcção da revista *Politécnica*. Sentimos então a obrigação moral de, para ela, contribuir com qualquer coisa escrita que fosse de utilidade para os estudates. Foi então

[*] Frequentávamos então a cadeira de Física Geral, ministrada pelo Professor Mário Silva, discípulo da notável cientista Madame Curie, que o orientou na sua tese de doutoramento. Dois anos mais tarde foi injustamente demitido das suas funções pelo Doutor Oliveira Salazar. A mesma sorte tiveram outros notáveis cientistas, tais como os matemáticos Bento de Jesus Caraça, Rui Luis Gomes, etc. Com actuações como estas, e com o desprezo que temos para com os nossos dois prémios Nobel, o nosso país não vai lon-ge. Por exemplo, notícia de que o Professor Egas Moniz tinha sido laureado com o Nobel da Medicina veio referida nos jornais, numa página interior, em apenas 2 linhas.

Primeiro número da Politécnica

que nos lembrámos de o tirar da gaveta e, com base nele, escrever uma série de artigos para a *Politécnica*, a que démos o título *Contribuições para um Ensino Racional da Electricidade*, que tem a seguinte estrutura:



A boa aceitação que esta série teve, da parte dos leitores da *Politécnica*, animou-nos a completá-la com as leis fundamentais da electrostática e da corrente eléctrica, com o objectivo de conseguir, num número mínimo de páginas, mas sem prejuízo para a clareza da exposição, uma síntese do electromagnetismo. E o resultado foi a escrita de um livro a que demos o título *Electromagnetismo e Relatividade Restrita*. Contém apenas cinco capítulos com os seguintes conteúdos:

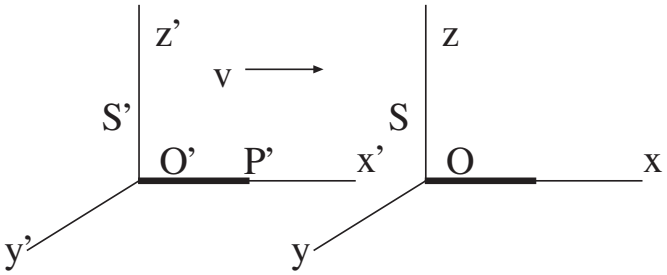
1. CONCEITOS FUNDAMENTAIS.
1.1. A carga eléctrica.
1.2. A corrente eléctrica. Meios condutores e meios isolantes.
2. O CAMPO ELÉCTROSTÁTICO.
2.1. Conceito de campo eléctrico e de diferença de potencial.
2.2. O condensador e a capacidade de um condensador.
2.3. Associações de condensadores.
2.4. A capacidade de um condensador plano.
2.5. A lei de Gauss.
2.6. A lei de Coulomb.
3. A CORRENTE ELÉCTRICA.
3.1. Conceito de corrente eléctrica.
3.2. A lei de Ohm.

Parte 3 – Uma das bases da Relatividade Restrita

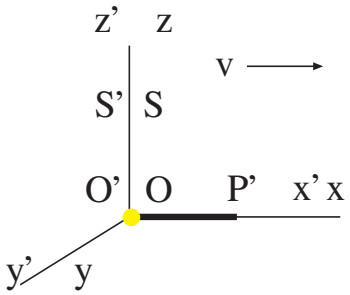
Uma das ferramentas básicas que utilizámos na elaboração da série de artigos para a *Politécnica* foi a chamada *contracção de Lorentz,* que resulta de um conjunto de equações denominado *transformação de Lorentz.* A demonstração deste conjunto de equações faz-se habitualmente a partir do conceito de *continuum quadrimensional espaço-tempo*. Mas a demonstração assim feita, embora tenha grande rigor, não se revela ser de compreensão fácil para alguns alunos. Entendeu-se, por isso, ser útil apresentarmos aqui uma maneira simples de obter a contracção de Lorentz. Para esse efeito, comecemos por recordar os dois princípios fundamentais da Teoria da Relatividade Restrita:

1. *Não existe nenhum sistema que se possa considerar em repouso absoluto. As leis da natureza são as mesmas para todos os sistemas em movimento relativo de translação uniforme.* Não há, portanto, sistemas privilegiados. Há uma reciprocidade perfeita entre todos eles.
2. *A luz, no espaço vazio, propaga-se sempre com uma velocidade determinada, independente do estado de movimento da fonte luminosa.*

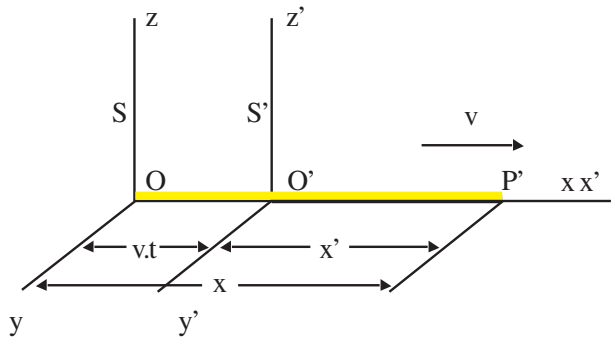
Considere-se agora que, na figura a seguir ilustrada, o segmento *O'P'* representa um comboio que rola, com uma



velocidade constante *v*, ao longo de um comprido troço rectilíneo de uma linha de caminho de ferro. Seja *O'* um dos cantos superiores da parte traseira da última carruagem onde se supõe existir uma fonte de luz, por enquanto apagada. Seja *O'x'* uma recta horizontal que passa por *O'* na direcção da linha de caminho de ferro e que intersecta em *P'* o plano vertical que passa pela frente da locomotiva. Seja *O'y'* outra recta horizontal que também passa por *O'*, mas na direcção das travessas, e *O'z'* a recta vertical que passa por *O'*. A estas rectas daremos a designação *eixos coordenados do sistema S',* sistema a que pertence o comboio e os seus passageiros. O *sistema S*, que consta na mesma figura, representa o sistema a que pertence um apeadeiro sem paragem para o comboio em questão.
É claro que, se não houver qualquer contratempo, o comboio acaba por passar pelo apeadeiro. Seja *t=0* o instante em que *O'* passa por *O* e em que os dois sistemas são então coincidentes como se mostra na figura seguinte. Admita-se que, nesse instante, a fonte de luz em *O'* emite um clarão (indicado a amarelo na figura), não importando saber qual a causa da sua emissão, com um dos seus raios a seguir na direcção da locomotiva.



Seja *t* o tempo, medido pelo chefe do apeadeiro, necessário para que o raio de luz atinja *P'*, e *t'* o correspondente tempo medido por um passageiro do comboio.
Chamaremos *observador do sistema S* ao chefe do



apeadeiro e *observador do sistema S'* a um passageiro do comboio. Como, para o observador do sistema *S*, a distância percorrida pelo raio de luz foi *x*, e, para o observador do sistema *S'* foi *x'*, as medidas da velocidade da luz feitas pelos dois observadores são respectivamente:

$$V = \frac{x}{t} \quad (1)$$

e:

$$V' = \frac{x'}{t'} \quad (2)$$

Por outro lado, como a distância *OO'* medida pelo observador do sistema *S'* é *v.t'* e medida pelo observador de *S* é *v.t*, as distâncias *O'P'* e *OP'*, medidas em *S'* e em *S*, são:

$$O'P'(\text{em } S') = x' \quad (3)$$

$$O'P'(\text{em } S) = x - vt \quad (4)$$

$$OP'(\text{em } S) = x \quad (5)$$

$$OP'(\text{em } S') = x' + v.t' \quad (6)$$

De acordo com os conceitos da física newtoniana, os valores das medidas de *O'P'*, respectivamente feitas em *S'* e em *S*, deveriam ser iguais. Mas não há qualquer inconveniente em admitir que o não são, e que o valor medido em *S'* se pode obter do valor medido em *S*, multiplicando este último por um factor de proporcionalidade α:

$$x' = \alpha.(x - v.t) \quad (7)$$

De facto, se os dois valores forem, na realidade, iguais, a continuação do desenvolvimento algébrico que se está a fazer mostrará que $\alpha=1$, mas se o não forem, o mesmo desenvolvimento algébrico dirá qual o valor α.
De acordo com a reciprocidade inerente ao primeiro princípio da Teoria da Relatividade Restrita, se, para obter o valor da medida, feita num dado sistema *S'*, de uma determinada distância, a partir do valor da medida, feita em *S*, da mesma distância, podemos fazê-lo multiplicando por um coeficiente α este segundo va-lor, o valor da medida, feita em *S*, de outra distância, pode ser obtido a partir do valor da medida desta, feita em *S'*, utilizando o mesmo procedimento. Então para a distância *OP'* pode escrever-se:

$$x = \alpha.(x' + v.t') \quad (8)$$

Da multiplicação, membro a membro, das equações (7) e (8) resulta:

$$x'.x = \alpha^2.(x - v.t).(x' + v.t') \quad (9)$$

donde, atendendo a (1) e a (2):

$$\alpha^2 = \frac{x.x'}{(x - v.t)(x' - v.t')} = \frac{\frac{x}{t}\cdot\frac{x'}{t'}}{\left(\frac{x}{t} - v\right)\left(\frac{x'}{t'} + v\right)} = \frac{V.V'}{(V - v)(V' + v)} \quad (10)$$

Na física newtoniana a velocidade da luz em *S* é a soma:

$$V = V' + v \quad (11)$$

donde:

$$V' = V - v \quad (12)$$

E então de (10) obtém-se:

$$\alpha^2 = \frac{V.V'}{V'.V} = 1 \quad (13)$$

e então $\alpha=1$, donde, devido a (7):

$$x' = x - v.t \quad (14)$$

isto é, a medida do comprimento do comboio feita pelo passageiro é igual à medida do comprimento do comboio pelo chefe do apeadeiro.
Mas como, de acordo com o segundo princípio da Teoria da Relatividade Restrita, a velocidade da luz tem um valor bem determinado (*c=299,776 km/s* para o vazio e aproximadamente o mesmo valor para o ar), independente do estado de movimento da fonte luminosa, na equação (10) tem de se considerar *V=V'=c* e então:

$$\alpha^2 = \frac{c.c}{(c-v)(c+v)} = \frac{1}{1-\frac{v^2}{c^2}} \quad (15)$$

donde:

$$\alpha = \frac{1}{\sqrt{1-\frac{v^2}{c^2}}} \quad (16)$$

donde, fazendo na equação (7) *x-vt=ℓ* e *x'=l'*

$$\ell = \ell' \cdot \sqrt{1-\frac{v^2}{c^2}} \quad (17)$$

isto é *o chefe do apeadeiro vê o comboio contraído na direcção do seu movimento* (contracção de Lorentz).

Fecho

Terminamos com um agradecimento a todos os presentes, nomeadamente à Associação dos Estudantes do ISPGAYA, para quem esta conferência foi especialmente concebida.

Planeamento de uma Biblioteca Universitária Digital

Com este artigo pretende-se clarificar o conceito de biblioteca digital e definir a sua planificação. Salientaremos também algumas vantagens na implementação da biblioteca digital.

Sérgio Bernardo *
sbernardo@ispgaya.pt
ISPGaya
Rua Rodrigues da Rocha, 291, 341
Santo Ovídio, 4400-025 Vila Nova Gaia

1. Introdução

Uma biblioteca universitária, segundo a *American Library Association* é "...uma combinação orgânica de pessoal, colecções e instalações cujo propósito é ajudar os seus utilizadores no processo de transformar a informação em conhecimento[1]".

A biblioteca, enquanto centro de difusor do conhecimento, tem de se aliar sempre às novas tecnologias para poder efectivamente prestar um serviço de qualidade ao maior número de utilizadores.

Várias são as bibliotecas universitárias que se renderam às potencialidades das bibliotecas digitais. Têm surgido nesse sentido vários projectos de implementação de bibliotecas digitais, como a "*UC Berkeley Digital Library Project*"[2], "*University of Michigan Digital Library Project*"[3], a "*Alexandria Digital Library*"[4], "*Building the Interspace: Digital Library Infrastructure for a University Engineering Community*"[5] e "*Digital Libraries Project*" da Stanford University[6].

É neste contexto actual que nos inserimos como profissionais da informação e apresentamos um projecto de implementação de uma biblioteca digital. Tentamos desmistificar também as dúvidas inerentes quanto ao conceito e funções deste novo tipo de bibliotecas.

2. A importância da implementação de uma biblioteca digital

A biblioteca digital é uma etapa da evolução dos suportes, dos instrumentos da escrita e métodos de difusão que o homem tem vindo a utilizar ao longo da sua história para dar a conhecer e difundir os seus conhecimentos e sentimentos[7].

Os suportes físicos actualmente utilizados são inúmeros, tais como, *Disquettes, CD-rom, Cdi, DVD-rom*, etc., relativamente ao formato, os documentos electrónicos poderão ser do tipo: *.doc, .pdf, .jpeg, .gif., .tif., .mpg., .avi.*, etc.

A biblioteca digital tem várias vantagens em relação às bibliotecas convencionais, das quais, destacaremos as que nos parecem mais relevantes.

1. Acesso mais rápido à informação;
2. Redução dos custos de aquisição;
3. Tem um importante papel na conservação;
4. Não tem limites geográficos de acção;
5. Facilita a colaboração educacional e aprendizagem;
6. Permite uma maior diversidade de documentos[8].

A biblioteca digital tem também um papel determinante na organização do "caos" da informação que é actualmente a Internet, definindo critérios de qualidade, organizando e disponibilizando ligações acreditadas para que os utilizadores possam estar seguros quanto à fiabilidade e à credibilidade dos dados acedidos.

Muitas das funções da biblioteca digital não são muito diferentes da tradicional, pois têm denominadores comuns nas tarefas de avaliação e selecção, conservação, descrição e indexação dos novos documentos[9].

3. Definição de Biblioteca Digital

Actualmente, deparamo-nos com várias terminologias, os britânicos utilizam o termo de biblioteca electrónica, biblioteca digital é utilizada pelos norte-americanos e europeus e há ainda uma terceira denominação comummente utilizada que é a de biblioteca virtual. Apesar

---

* Licenciado em Ciências Históricas, com pós-graduação em Ciências Documentais - variante Bibliotecas. Responsável da Biblioteca do ISPGaya.

[1] GOMEZ HERNÁNDEZ, José António – La biblioteca universitária. In ORERA ORERA, Luisa. Manual de Biblioteconomia. Madrid: Editorial Sintesis, reimp. 1998. ISBN 84-7738-363-4. p. 363

[2] http://elib.cs.berkeley.edu/

[3] http://www.si.umich.edu/UDML/

[4] http://alexandria.sdc.ucsb.edu/

[5] http://dli.grainger.uiuc.edu/default.htm

[6] http://Walrus.stanford.EDU/diglib/

[7] GARCÍA CAMARERO, Ernesto; GARCÍA MELERO, Luis Ángel – La biblioteca digital. Madrid: Arco/Libros, cop. 2001. 380 p. ISBN 84-7635-486-X

[8] ISAÍAS, Pedro - Bibliotecas digitais. Lisboa: Universidade Aberta, 1999. 176 p. ISBN. 972-674-277-3

[9] GARCÍA CAMARERO, Ernesto; GARCÍA MELERO, Luis Ángel – *Ibidem*.

desta aparente confusão na terminologia, relativamente ao conceito todas elas significam o mesmo.
A biblioteca digital é uma instituição que selecciona, adquire, cataloga e guarda uma colecção de documentos, armazenados em suporte digital e que os coloca em acesso público através de redes informáticas[10].
Em que consiste uma biblioteca digital? Ela é um serviço de uma biblioteca tradicional já automatizada, em que disponibiliza documentos em formato digital para uso dos seus utilizadores. Estes documentos são geralmente os livros electrónicos (*e-books*), as revistas electrónicas (*e-magazines*), os jornais electrónicos (*e-journals*), bases de dados em linha, etc.
Muitas vezes denomina-se de biblioteca digital, uma página-web que disponibilize livros electrónicos, porém esta definição não é considerada adequada[11], independentemente da variedade e/ou da relevância da sua colecção.
Se fazemos uma pesquisa num motor de busca da Internet acerca da denominação "biblioteca digital" encontramos registos que não correspondem ao que nós bibliotecários e cientistas da informação entendemos como biblioteca digital, como é o caso, da "biblioteca digital da Porto Editora[12]" que disponibiliza clássicos da literatura digitalizados e dicionários.
A título de exemplo consideramos excelentes e adequados modelos de bibliotecas digitais, a Biblioteca Virtual de Cervantes[13] e a Biblioteca Nacional Digital[14] que, embora em fase de preparação, já nos disponibiliza no item "literatura" um vasto conjunto de obras literárias portuguesas[15]. Em relação à Biblioteca Nacional Digital, felicitamo-la por ter a feliz ideia de utilizar a digitalização da imagem da capa original[16], hiperligando-a à obra integral em *html*.

4. Missão do Projecto da Biblioteca digital:

Desenvolver na biblioteca o serviço de disponibilização de recursos acessíveis via Internet pela comunidade académica da Universidade. Este serviço será alcançado através da digitalização de obras, captura de recursos disponíveis na Internet e posterior catalogação e indexação, através de computadores, digitalizadores[17] e software, tais como de gestão de bibliotecas[18] e o programa de leitura Acrobat Reader.

4.1 Objectivos:

Colocar em livre acesso as teses defendidas nas Universidades, os analíticos de jornais e revistas científicas existentes no fundo documental, assim como, os analíticos electrónicos disponíveis em linha pela *página-web* da Biblioteca.

4.2 Metas:

1. Acesso rápido à informação em documentos electrónicos;
2. Maior diversidade de suportes de documentos;
3. Maior interactividade entre a biblioteca e o utilizador.

5. Avaliação dos Riscos

Os riscos na implementação de uma biblioteca universitária não são muitos, mas a probabilidade da ocorrência é muito elevada e os danos consideráveis nos *items* um e dois. Uma biblioteca digital com as ligações aos documentos e/ou aos recursos desactualizadas sugere descuido e falta de rigor para com o projecto.
Os riscos a considerar são os seguintes:
1. As ligações na Internet frequentemente ficam inactivas
2. Invasão de Vírus Informáticos
3. Ataques informáticos dos *hackers*
4. Falta de corrente eléctrica de apoio ao servidor

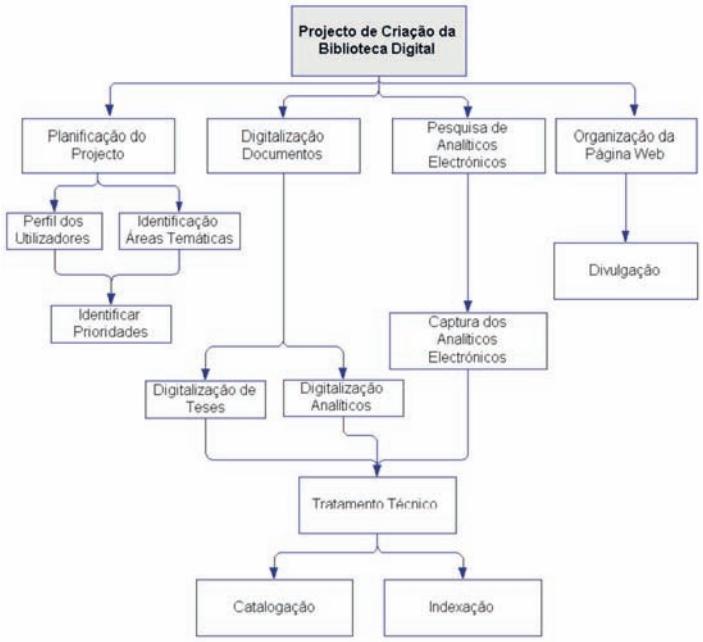
O risco dos vírus informáticos é constante e as probabilidades de sermos "infectados" são elevadas, o que nos leva a ter precauções logo desde o início. Precauções essas que passam pela instalação de uma *firewall*, programas de antivírus actualizados regularmente e pelas cópias de segurança.

6. Exemplo de Estrutura de Decomposição das Tarefas

A estrutura de decomposição das tarefas (EDT) é a análise das tarefas necessárias para a implementação do projecto em prática. Este é o primeiro passo para implementação de um serviço.

---

[10] Id. *Ibidem*.
[11] Veja-se o caso do Gutemberg Project (http://promo.net/pg/)
[12] http://portoeditora.pt/bdigital/default.asp
[13] http://cervantesvirtual.com/index.shtml
[14] http://bnd.bn.pt/ecrans/main-menu.html
[15] http://bnd.bn.pt/ecrans/literatura.html
[16] http://bnd.bn.pt/ecrans/fichas/ficha_007d.html
[17] *Scanners*
[18] Em Portugal há três tipos de software que são regularmente utilizados, são eles o Porbase, o Docbase e o Aleph



7. Exemplo de Planeamento financeiro

Para a implementação de uma biblioteca digital será necessário um número mínimo de recursos humanos[19] e materiais que se traduzirão obviamente em recursos financeiros.

Os recursos materiais necessários para a implementação deste projecto-exemplo são três computadores e dois digitalizadores. Tendo em conta que a maior parte das bibliotecas universitárias dispõem destes recursos materiais, não iremos efectuar a sua representação no projecto.

Relativamente ao pessoal, iremos seleccionar cinco elementos[20] de outras secções da biblioteca. Todavia e mesmo sendo canalizados de outras secções, o pessoal usufrui de uma remuneração mensal, então determinamos o preço por hora de trabalho de acordo com a remuneração auferida para podermos quantificar de forma rigorosa os custos do projecto.

A seguinte tabela determina o preço por hora por categoria em escudos e em euros, assim como o preço total por categoria que o projecto acarretará.

Nome	Euros/hora	Esc./hora	Total Horas	Total Euros	Total Escudos	Categoria
Joana	7,08 €/hr	1.420,00 Esc./hr	582,92 hrs	4.128,70 €	827.730,91 Esc.	Bibliotecário
Raquel	7,08 €/hr	1.420,00 Esc./hr	1.528 hrs	10.822,72 €	2.169.760,00 Esc.	Bibliotecário
Marco	3,40 €/hr	681,82 Esc./hr	1.212 hrs	4.121,90 €	826.365,84 Esc.	Téc. Prof.
Manuel	3,40 €/hr	681,82 Esc./hr	1.296 hrs	4.407,57 €	883.638,72 Esc.	Téc. Prof.
Fernando	3,40 €/hr	681,82 Esc./hr	2.592 hrs	8.815,14 €	1.767.277,44 Esc.	Téc. Prof.

[19] Personalizamos os recursos humanos, não optando por designações como: funcionário 1, Funcionário 2, etc.

[20] Partimos do princípio que a biblioteca tem os funcionários necessários. No caso de uma biblioteca com poucos funcionários, a implementação de um projecto deste tipo levar-nos-ia à contratação de pessoal que suprimisse as necessidades do projecto.

8. Exemplo de mapa de responsabilidades

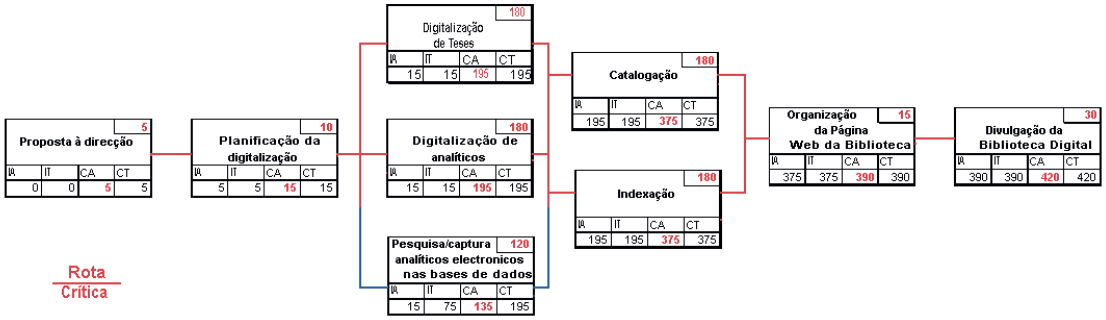
Tarefas / Elementos	A	B	C	D	E	F	G	H	I
Joana	2	1	1		1	1	1	1	
Raquel	1	2		1			2		1
Marco					2			2	2
Manuel			2						
Fernando				2		2			

Legenda:
1. Responsável
2. Executor
A = Proposta à direcção
B = Planificação da digitalização
C = Digitalização das teses
D = Digitalização dos analíticos
E = Pesquisa/captura de analíticos electrónicos
F = Catalogação
G = Indexação
H = Organização da *página-web*
I = Divulgação da Biblioteca Digital

Na tabela seguinte são definidos os recursos humanos e as tarefas subjacentes em que o responsável pela tarefa tem um peso de 10% e o executor de 90%.

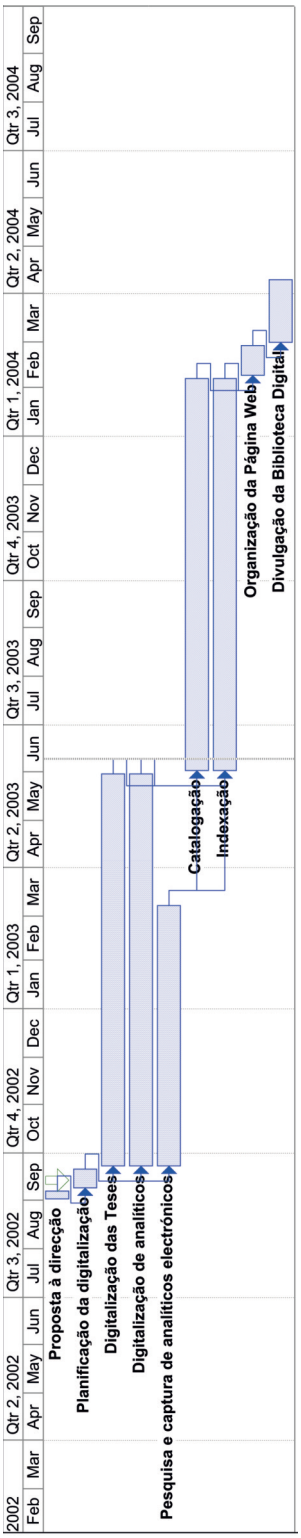
Recursos Humanos	Horas	Custo-Esc	Custo-Euros
Joana - Bibliotecária	582,92 hrs	827.730,91 Esc	4.128,70 €
Proposta à direcção	*36 hrs*	*51.120,00 Esc.*	
Planificação da digitalização	*8 hrs*	*11.360,00 Esc.*	
Digitalização das Teses	*130,92 hrs*	*185.890,91 Esc.*	
Pesquisa e captura de analíticos electrónicos	*96 hrs*	*136.320,00 Esc.*	
Catalogação	*144 hrs*	*204.480,00 Esc.*	
Indexação	*144 hrs*	*204.480,00 Esc.*	
Divulgação da Biblioteca Digital	*24 hrs*	*34.080,00 Esc.*	
Raquel - Bibliotecária	1.528 hrs	2.169.760,00 Esc	10.822,72 €
Proposta à direcção	*4 hrs*	*5.680,00 Esc.*	
Planificação da digitalização	*72 hrs*	*102.240,00 Esc.*	
Digitalização de analíticos	*144 hrs*	*204.480,00 Esc.*	
Indexação	*1.296 hrs*	*1.840.320,00 Esc.*	
Organização da Página Web	*12 hrs*	*17.040,00 Esc.*	
Marco - Técnico Informática	1.212 hrs	826.365,84 Esc	4.121,90 €
Pesquisa e captura de analíticos electrónicos	*864 hrs*	*589.092,48 Esc.*	
Organização da Página Web	*108 hrs*	*73.636,56 Esc.*	
Divulgação da Biblioteca Digital	*240 hrs*	*163.636,80 Esc.*	
Manuel - Técnico BAD	1.296 hrs	883.638,72 Esc	4.407,57 €
Digitalização das Teses	*1.296 hrs*	*883.638,72 Esc.*	
Fernando - Técnico BAD	2.592 hrs	1.767.277,44 Esc	8.815,14 €
Digitalização de analíticos	*1.296 hrs*	*883.638,72 Esc.*	
Catalogação	*1.296 hrs*	*883.638,72 Esc.*	

9. Modelo exemplificativo de Diagrama CPM



Legenda:
IA – Início Antecipado
IT – Início Tardio
CA – Conclusão Antecipada
CT – Conclusão Tardia

10. Modelo exemplificativo de Gráfico Gantt



Conclusão

A biblioteca digital é já uma realidade da actual sociedade da informação na qual estamos inseridos e com este trabalho tentamos incentivar de algum modo a sua implementação ou, no mínimo, reforçar a importância de uma biblioteca universitária actual evoluir nos seus serviços e áreas de acção.

Uma biblioteca digital não visa somente disponibilizar na sua *página-web* um conjunto de *links* credíveis das várias áreas temáticas, mas sim colocar em *linha*, para os seus actuais e potenciais utilizadores, um vasto leque de recursos documentais sob diversos tipos de suportes digitais.

A Biblioteca deverá estar em contínuo desenvolvimento e ao serem implementados novos serviços permitimos à universidade avançar na investigação e em novas áreas de ensino, nomeadamente, o ensino à distância via Internet (*e-learning*).

O bibliotecário responsável deverá ser o grande impulsionador de novos serviços, exigindo-se para tal, que procure aprofundar sempre as suas competências profissionais e acompanhar a evolução das bibliotecas de todo o mundo, o que requer uma assídua presença em conferências temáticas anuais, designadamente da *IFLA*[21], *IATUL*[22] e da Biblioteca Nacional.

Referências

GARCÍA CAMARERO, Ernesto; GARCÍA MELERO, Luis Ángel – *La biblioteca digital*. Madrid: Arco/Libros, cop. 2001. 380 p. ISBN 84-7635-486-X

ORERA ORERA, Luisa. *Manual de Biblioteconomia.* Madrid: Editorial Sintesis, reimp. 1998. ISBN 84-7738-363-4. p. 363

HOBBS, Peter – Gestão de projecto. [S.l.]: Livros e Livros, 2001. ISBN 972-791-059-9

ISAÍAS, Pedro – *Bibliotecas digitais.* Lisboa: Universidade Aberta, 1999. 176 p. ISBN. 972-674-277-3

JAMES, Lewis P. - *Fundamentals of project management*. New York: Amacon, 1995.

[21] IFLA – International Library Association (www.ifla.org)
[22] International Association of Tecnological University Libraries (www.iatul.org)

Anti-Análise Forense

A ciência forense permite-nos chegar aos factos através das evidências.
Tal como esta ciência é usada na justiça no campo da medicina legal, com o avanço das tecnologias, ela foi também levada para o campo da informática.
A análise forense informática é o campo que estuda o "como", "quando" e o "porquê" de um ataque a um computador. Através dela é possível determinar informação vital que poderá ser usada como prova para levar o criminoso à justiça.

Luís Miguel Silva
lms@ispgaya.pt
ISPGaya
Centro de Informática (CIISP)
Rua Rodrigues da Rocha, 291, 341
Santo Ovídio, 4400-025 Vila Nova Gaia

1-Introdução

A análise forense é em si um campo de estudo fascinante, qualquer que seja a área em que seja aplicada.
Os especialistas forenses são os detectives dos nossos tempos. Analisam os mais pequenos pormenores e conseguem chegar a conclusões extremamente precisas acerca do "crime".
Tal como o médico legista faz uma autópsia procurando padrões e anomalias num cadáver, o especialista informático forense procura nos pequenos bits do disco informação deixada pelo atacante que possivelmente o acabará por incriminar.
Este detective é capaz de vasculhar os mais obscuros cantos de um dispositivo físico à procura de provas.
No campo da informática entende-se por "análise forense" o uso da ciência e tecnologia para investigar e estabelecer factos sobre acções criminosas.
A "anti-análise forense" é então a *arte* de esconder dados, informações e pistas após uma penetração num sistema informático. Este tipo de análise digital forense está a ganhar terreno como resposta a incidentes criminosos.
Surgiu uma nova geração de analistas assistidos por ferramentas inovadoras e sofisticadas. Curiosamente, estas ferramentas funcionam todas sobre a mesma base e raramente se fala sobre o campo da anti-análise forense.
Os exemplos mostrados neste artigo serão feitos sobre o tipo de sistema de ficheiros extfs (do Linux) visto este sistema ser o mais amplamente utilizado.
Neste artigo iremos mostrar como é que os analistas geralmente procuram pelo rasto de um atacante e como estes tentam eliminar esse rasto.
Este artigo não pretende de forma alguma incentivar a actos criminosos mas sim mostrar o lado do analista e do atacante tentando encontrar e explicar quais as falhas mais comuns de ambos.

2-Como funciona a Anti-Análise Forense

Um atacante depois de penetrar num sistema tem que ser capaz de garantir o acesso posterior a esse mesmo sistema.
Hoje em dia, é boa prática de administração de sistemas a despistagem de padrões das anomalias detectadas no servidor. Significa, regra geral, que o sistema tem um administrador zeloso por trás.
Ora, há aqui uma contradição. Se existem boas práticas, como justificar a intrusão?
Nenhum administrador pode prevenir ataques contra falhas ainda não conhecidas. Aliás, é daí que vem a famosa afirmação de que "o único computador seguro é aquele que está desligado da corrente, fechado num cofre anti-fogo e anti-bomba, rodeado de guardas e se possível no fundo do oceano". E mesmo assim, tal como o autor Kevin Mitnick dizia "podemos sempre convencer alguém a ligá-lo...".
Ninguém pode proteger um sistema de um *0'day exploit* que aproveita uma determinada falha e que apenas é distribuído no "underground"). Por outro lado, mais cedo ou mais tarde, o referido *exploit* é tornado público o que fará com que o administrador analise o seu sistema, detecte as respectivas vulnerabilidades e tente monitorizar se alguém está a tirar partido delas. A arte da anti-análise está em conseguir vaguear livremente por um sistema sem ser detectado.
Para garantir isto o atacante recorre a várias "tecnologias" sobre as quais se fala a seguir.

Se um atacante quer manter acesso a um sistema tem que esconder o seu rasto. Procede então à criptografia dos seus ficheiros, à instalação de "*rootkits*" (conjuntos de ferramentas completas que garantem o acesso ilegítimo a um sistema por parte de um atacante sem este ser detectado), de "*backdoors*", esconde os seus ficheiros em *fluxos de dados alternados* (vulgo ADS – Alternate Data Streams existente no sistema de ficheiros NTFS), esconde ficheiros no chamado "*slack space*",
re-aloca e mascara os seus ficheiros como uma biblioteca, processo ou dispositivo que passe despercebido num sistema e recorre à "*esteganografia*" (escondendo a sua informação em ficheiros de imagem ou de som).

2.1- A encryptação dos dados

Quando um atacante penetra num sistema geralmente utiliza-o para guardar ficheiros.
Estes ficheiros podem ser o software utilizado (ou que ainda será utilizado) para conseguir o acesso ilegítimo aquele sistema (ou a outros, visto que um computador ligado a uma rede é sempre um novo ponto de acesso para partir para novos ataques).
Se o atacante deixasse estes ficheiros espalhados num directório chamado **exploits** ou num simples directório escondido iria levantar muitas suspeitas para o administrador. Surge então a necessidade de os esconder para evitar ser detectado.
Uma das soluções é recorrer à criptografia dos seus ficheiros de forma a que, mesmo que estes sejam detectados, o administrador não seja capaz de decifrar o que são ou para que servem.
O atacante então comprime todos os ficheiros num só e criptografa-os de forma a não ser detectado.
A partir deste momento a única forma que o administrador tem de descobrir os conteúdos desse ficheiro é descobrir a cifra para o descriptografar ou, mais simplesmente ainda, descobrir a localização física do atacante e obter dele a colaboração necessária.

2.2-Rootkits

O primeiro passo a tomar por parte do atacante após penetrar num novo sistema é garantir o seu acesso posterior (sem levantar muitas suspeitas).
Os *rootkits* são bastante populares para fazer isso mesmo.
Um *rootkit* é um conjunto de ferramentas completo que contém todo o software necessário para remover os rastos do atacante dos "*logs*" do sistema, instalar *backdoors* em ficheiros binários, criar contas às quais o sistema não regista informação e que possibilitam a administração remota do sistema.
O interessante destes *rootkits* é que geralmente não é necessário grandes conhecimentos informáticos para os instalar. Isto levanta um problema para o atacante. Se algo corre mal, este perde o acesso ao sistema sem remover convenientemente os seus rastos.
Há algum tempo o autor presenciou um problema enquanto prestava serviço numa conhecida instituição.
Misteriosamente, um dos servidores utilizado num dos projectos nessa instituição demonstrou "algumas" anomalias. Apenas o servidor web funcionava e não era possível fazer uma simples autenticação no sistema.
Qualquer acção feita por parte do administrador nesse servidor apenas resultava em erros atrás de erros sobre "*bibliotecas*" que não existiam e cujas versões eram mais antigas ou mais recentes do que as necessárias.
O que se passou neste caso foi que o *hacker* entrou naquele servidor e tentou instalar um *rootkit* sem tomar as devidas precauções primeiro. Instalou um rootkit antigo que falhava perante as dependências de ficheiros binários e "*bibliotecas*" existentes no sistema. Isto fez com que o sistema se tornasse completamente inutilizável.

2.3 – Sniffers

A informação flutua livre e anarquicamente por uma rede. É então altura do atacante a interceptar e guardar para uso posterior (novamente, sem ser detectado).
Admita-se que o atacante já penetrou no sistema, possui privilégios de administrador e instalou o seu rootkit para garantir acesso posterior.
Pode agora entrar noutros servidores que estejam acessíveis através da rede física (quer seja cablada, quer seja por tecnologia wireless, como está cada vez mais na moda) simplesmente interceptando a informação circulante.
Então num esquema muito simples de uma *LAN* (Local Area Network), temos o exemplo de 5 computadores ligados a um "*HUB*" (dispositivo físico que permite ligar 2 ou mais computadores em rede).

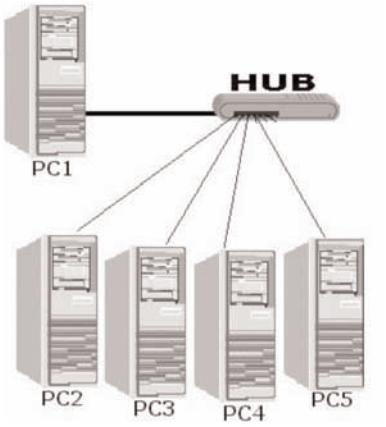


Imagem 1: esquema simples de uma rede

O atacante consegue então comprometer a segurança do "**PC1**". Visto esta rede estar toda interligada por um HUB, se for implementado um "*sniffer*" nesse computador, o atacante vai conseguir interceptar informação que circule entre os 5 pcs.
Então imaginemos que o "**PC2**" contém um serviço de partilha de ficheiros por FTP (File Transfer Protocol), o "**PC1**" tem um "*sniffer*" que analisa o tráfego que circula na rede e o "**PC3**" faz uma ligação por ftp para o "**PC2**".

Podemos ver um exemplo de um "*sniffer*" chamado "ettercap" a funcionar na imagem seguinte.

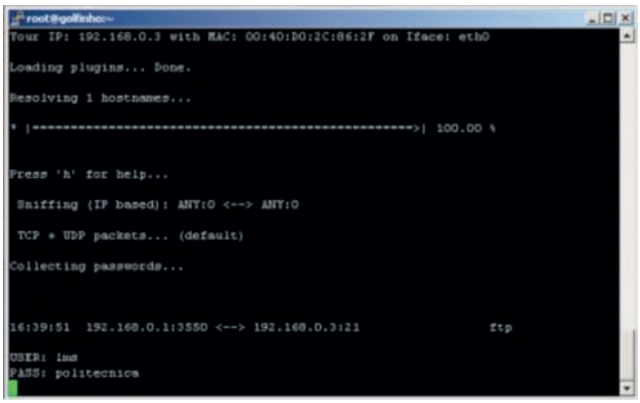


Imagem 2: um sniffer intercepta um login e password enviados por ftp.

Este tipo de software é deixado a correr em segundo plano no servidor e guarda a informação interceptada em ficheiros.
A partir do momento em que o atacante consegue interceptar uma conta válida no sistema que comprometeu vai poder começar a utilizá-la como segunda via de entrada no sistema (no caso de algum dia as suas "*backdoors*" serem descobertas).
Se o administrador não tomar as devidas precauções nunca saberá que o seu sistema está a interceptar passwords de outros computadores na mesma rede (ou do próprio computador).
Uma maneira de descobrir se estamos a interceptar informação é verificar se a placa de rede se encontra em modo "*promíscuo*" (o que, tal como no termo sexual da palavra significa "manter relações sexuais com grande número de parceiros", na informática significa "capturar a informação de um grande número de parceiros").
O administrador pode confirmar isso através do comando "*ifconfig*", isto claro, se o atacante não tiver modificado esse binário.

```
[root@golfinho root]# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:40:D0:2C:86:2F
          inet addr:192.168.0.3  Bcast:192.168.0.255
Mask:255.255.255.0
          UP BROADCAST RUNNING PROMISC MULTICAST
MTU:1500  Metric:1
          RX packets:1611 errors:0 dropped:0 overruns:0
frame:0
          TX packets:1416 errors:0 dropped:0 overruns:0
carrier:0
          collisions:0 txqueuelen:100
          RX bytes:180440 (176.2 Kb)  TX bytes:166061 (162.1
Kb)
          Interrupt:10 Base address:0x8000
[root@golfinho root]#
```

De qualquer forma o "output" de um programa como o ifconfig nunca é completamente fiável visto que o atacante pode alterar a "*flag*" que mostra que o *interface* se encontra em modo *promíscuo* de forma a despistar o administrador.

2.4 – IDS (Intrusion Detection Systems)

É vital para o administrador analisar periodicamente o seu servidor à procura de anomalias. Se esta tarefa não for levada a sério e o atacante souber o que está a fazer, o administrador nunca saberá que o seu sistema foi comprometido, a não ser que atacante esteja farto de "estar no escuro" e se queira mostrar. Afinal, este é o grande problema do "hacker" (e de todos os seres humanos, em especial os criminosos). Qual é a piada de fazer algo "emocionante" como penetrar num sistema se não pudermos contar a alguém? Geralmente os miúdos mais novos que comprometem a segurança de servidores são quem mais cedo se mostram. Quer pela sua inexperiência, quer pela necessidade de se mostrarem ao mundo.
Este desejo vai-se perdendo à medida que o atacante vai ganhando maturidade.
Existe então a necessidade de instalar um software que detecte a actividade de possíveis intrusos. A esse sistema de análise chamamos **IDS** (intrusion detection system).
Um exemplo de um IDS é o **tripwire**. Este sistema monitoriza atributos chave de ficheiros que "apenas se modificariam" no caso de uma intrusão. Os atributos analisados são a assinatura binária, tamanho, modificação esperada no tamanho, etc.
O seu funcionamento não é muito complexo. Primeiro analisa e guarda informações sobre todos os ficheiros no sistema (ou ficheiros contidos em directórios "estratégicos" no sistema) para mais tarde os comparar com as assinaturas dos ficheiros actuais.
Como o leitor pode imaginar isto causa uma grande sobrecarga no sistema o que faz com que muitos administradores não utilizem um IDS deste tipo.
Em qualquer dos casos, a sua utilização é fortemente aconselhada. Imagine-se que um atacante consegue comprometer um sistema e modifica binários chave como o "ps" (programa que mostra todos os processos a correr no sistema), o "lsof" (programa que mostra todos os ficheiros abertos no momento) ou o "netstat" (programa que mostra as ligações TCP/UDP abertas no momento).
Por exemplo, o "lsof" é um comando dos mais úteis no sistema. Num sistema UNIX, tudo se implementa à base de

ficheiros. Os directórios e os periféricos surgem retratados no sistema como ficheiros.

2.5 – ADS (Alternate Data Streams) – fluxos de dados alternados

Neste ponto do artigo, fala-se sobre formas que existem para esconder o rasto de um atacante.
No Microsoft Windows NT e seus sucessores (2000 e XP, em todas as suas variantes), existe um sistema de ficheiros chamado NTFS. Este sistema de ficheiros é um sistema de ficheiros especialmente concebido para computadores multi-utilizador. Assim sendo, existem algumas diferenças acentuadas entre este sistema de ficheiros e o formato anterior (FAT16 ou FAT32) presente nos sistemas Microsoft Windows 95/98 e Millenium.
Existe uma "característica não documentada" (como a Microsoft prefere chamar-lhe) no NTFS que possibilita guardar dados em ficheiros escondidos que por sua vez estão associados a ficheiros visíveis (não suspeitos).
Os fluxos de informação criados por estas sequências de ficheiros representam um sério risco de segurança porque são completamente invisíveis com as ferramentas normalmente instaladas nos sistemas operativos, tornando-os locais perfeitos para se esconderem ficheiros indesejados tais como vírus e "cavalos de tróia" (vulgo *backdoors*).
Se por um lado esta característica do "SF" pode ser muito facilmente utilizada, por outro lado é apenas detectada com software especializado para o efeito.Um programa como o "explorer" do windows consegue apenas ver os ficheiros normais não mostrando assim que existem fluxos de dados escondidos nem mostrando o espaço realmente ocupado por eles. Visto que esta capacidade do "SF" NTFS é pouco conhecida para os programadores, existe muito pouco software de segurança que detecte ficheiros escondidos através dela.
Interessante também será mencionar que a única maneira de eliminar um fluxo de dados alojado num sistema de ficheiros NTFS e escondido através do ADS é eliminando o ficheiro "hospedeiro".

2.6 – Esconder informação no "slack space"

O chamado "slack space" é o espaço em disco entre o final de um ficheiro e o final de um grupo de blocos ("cluster") no disco físico.
Com os programas certos, o atacante é capaz de utilizar esse espaço para esconder os seus ficheiros. Visto que os ficheiros são guardados em blocos inutilizados (como por exemplo blocos marcados como "corrompidos"), o atacante consegue despistar a maior parte do software existente de análise forense.
A maioria do software de análise forense não procura informação escondida nestes espaços sendo assim, tal como o "ADS" no NTFS um sitio perfeito para o atacante esconder informação maliciosa.
O espaço disponível em cada um destes blocos inutilizados é minúsculo pelo que o atacante necessita de um software especial para unir todos os pequenos bits disponíveis de forma a conseguir um único fluxo de informação suficientemente grande para alojar os seus ficheiros (quer sejam eles um "log" de informação interceptada por um sniffer, ficheiros interessantes encontrados no sistema, *backdoors, vírus*, etc).
Mais à frente neste artigo, demonstrar-se-á como fazer isso mesmo utilizando um software chamado "runefs", um conjunto completo de ferramentas para fazer "manutenção" a um nível bastante baixo do disco rígido.

2.7 – Esteganografia

A esteganografia foi catalogada pelos gregos como "escrita secreta".
É uma técnica utilizada há mais de 2500 anos e já foi utilizada com intuitos militares, políticos, pessoais e como forma de resguardar a propriedade intelectual.
Actualmente podemos dizer que é a arte e ciência de qualquer processo que permita esconder uma mensagem num qualquer objecto fazendo com que essa mesma mensagem não seja aparente ao observador.

Um abade alemão, Johannes Trithemius (1462-1516), no seu livro intitulado "Steganographia:hoe est ars per occultam scripturam animi sui voluntatem absentibus aperiendi certa", descreve formas de comunicar com os espiritos. A sua tradução de latim para português significa algo como "Esteganografia: a arte através da qual se escondem escrituras que só são decifráveis através da mente do homem".
Os primeiros livros conhecidos e editados sobre criptografia são precisamente os dois primeiros volumes da sua triologia. O terceiro livro

Imagem 3: Johannes Trithemius (1462-1516), um abade alemão que escreveu a primeira obra conhecida sobre esteganografia

versava a astrologia oculta.
Já no nosso tempo, dois investigadores, Dr. Thomas Ernst e Dr. Jim Reeds encontraram mensagens escondidas em tabelas presentes na terceira obra da triologia de Johannes Trithemius. A tradução de latim das mensagens encontradas é algo como "A raposa rápida castanha salta por cima do cão preguiçoso", "O portador desta carta é um ladrão e escumalha. Protege-te contra ele, ele quer fazer-te algo" e a terceira mensagem era o início do vigésimo terceiro salmo.
Podemos dizer que a segunda mensagem escondida é como uma protecção engenhosamente inventada por Johannes Trithemius para proteger a sua propriedade intelectual.

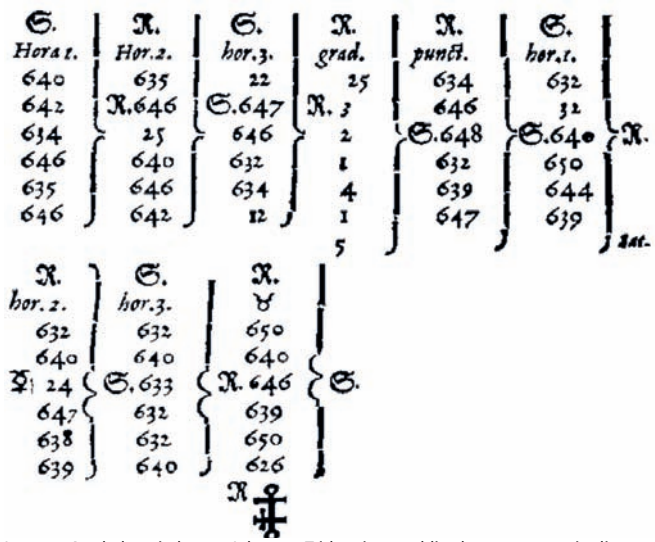


Imagem 4: tabelas criadas por Johannes Trithemius e publicadas no seu terceiro livro sobre estaganografia.

No entanto, a esteganografia é usada há bastante mais tempo.
Segundo documentos existentes, foi utilizada pela primeira vez em 480 aC.
Nessa altura eram utilizadas tábuas de madeira cobertas com cera onde eram gravadas as escrituras.
Um grego chamado Demaratus derreteu então a cera de uma tábua, escreveu uma mensagem na própria madeira e cobriu-a de cera novamente conseguindo assim escondê-la e avisar os espartanos de iminência de uma invasão.
Outro exemplo ilustrativo, este bastante mais recente, é o de uma mensagem, aparentemente inocente e inofensiva, publicada durante a 2ª Guerra Mundial que dizia "Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils".
Se retirarmos a segunda letra de cada palavra desta frase conseguimos então encontrar a mensagem escondida, "Pershing sails from NY June I".
Actualmente a esteganografia é frequentemente denominada como "watermarking" (marca de água).
Se o leitor olhar para uma simples nota contra a luz, consegue ver uma imagem escondida, a marca de água. Esta imagem só é visível desta forma, sendo assim um método de esteganografia.
Na informática, a esteganografia é utilizada escondendo informação em ficheiros inofensivos (ficheiros de som, imagem, texto, html, etc) usando para tal os bits inutilizados presentes nesses formatos de ficheiros.
A informação escondida pode ser texto normal, cifrado ou até imagens.
Ao contrário dos dados criptografados, a esteganografia não é facilmente detectada. É portanto, um substituto bem sucedido da criptografia como método de esconder informação.

Imagem 5: Imagem sem informação escondida

Imagem 6: Imagem com informação escondida.

É necessário software especial para esconder ficheiros através desta técnica. Um destes programas freeware e opensource, é o **steghide**.
O programa **steghide** (freeware e opensource) permite esconder ficheiros dentro de outros, estes últimos habitualmente de tipo inofensivo, sem quebrar a sua funcionalidade. Veja-se o exemplo seguinte.

Imagine-se um ficheiro chamado "politecnica.jpg":
[wc@golfinho steg]$ file politecnica.jpg
politecnica.jpg: JPEG image data, JFIF standard 1.01, aspect ratio, 1 x 1
[wc@golfinho steg]$

Cria-se agora o ficheiro a esconder...
[wc@golfinho steg]$ cat > ficheiro_privado.txt
isto é um ficheiro privado que se esconde num ficheiro .jpg
^C
[wc@golfinho steg]$

E esconde-se o primeiro ficheiro com o **steghide**
[wc@golfinho steg]$ steghide embed -cf politecnica.jpg -sf politecnica-steg.jpg -pf ficheiro_privado.txt
Enter passphrase: **inserir_password_aqui**
Re-Enter passphrase: **inserir_password_aqui**
[wc@golfinho steg]$

Como o leitor pode confirmar, existem agora um ficheiro novo chamado **politecnica-steg.jpg.**
[wc@golfinho steg]$ ls -l
total 80
-rw-rw-r-- 1 wc wc 64 Feb 24 21:56 ficheiro_privado.txt
-rwxr-xr-x 1 wc wc 39800 Feb 24 21:26 politecnica.jpg
-rw-rw-r-- 1 wc wc 33190 Feb 24 21:56 politecnica-steg.jpg
[wc@golfinho steg]$ file politecnica-steg.jpg
politecnica-steg.jpg: JPEG image data, JFIF standard 1.01, aspect ratio, 1 x 1
[wc@golfinho steg]$

Este ficheiro contém o primeiro escondido e, no entanto, mantém toda a funcionalidade de uma imagem em formato "jpeg". Será também de notar que o seu tamanho diminuiu.

É então altura de voltar a recuperar o ficheiro que se escondeu no **politecnica-steg.jpg...**
[wc@golfinho steg]$ steghide extract -sf politecnica-steg.jpg
Enter passphrase: **inserir_password_aqui**
writing plain file to "ficheiro_privado.txt".
[wc@golfinho steg]$ cat ficheiro_privado.txt
isto é um ficheiro privado que vamos esconder num ficheiro .jpg
[wc@golfinho steg]$

Esta técnica é bastante eficaz para mover ou guardar informação crucial sem levantar muitas suspeitas. Visto que os ficheiros ficam protegidos com uma palavra passe, um administrador que suspeite de um ficheiro não o conseguirá abrir para investigar.
O algoritmo utilizado pelo **steghide** para mascarar os ficheiros faz com que a única maneira de extrair um ficheiro escondido seja através da palavra passe inserida durante a "metamorfose". Caso contrário, os cabeçalhos do ficheiro hospedeiro não fazem qualquer sentido para o programa que o toma como corrompido, como se pode ver no exemplo seguinte:
[wc@golfinho steg]$ steghide extract -sf politecnica-steg.jpg
Enter passphrase: **password_errada_inserida_aqui**
steghide: the distribution method saved in the stego header is unknown (file corruption ?).
[wc@golfinho steg]$

Quando se junta este técnica a outras como a "criptografia", o "ADS" do NTFS ou esconder ficheiros no chamado "slack space", a análise forense torna-se uma tarefa quase impossível e bastante árdua.

3 – Casos práticos...análise forense e anti-análise forense

Nos parágrafos seguintes, demonstrar-se-á o uso de software específico para análise forense e camuflagem do rasto deixado pela intrusão no sistema hospedeiro. Analise-se então o sistema de ficheiros Unix.

3.1 – Um sistema de ficheiros genérico UNIX.

Os ficheiros num sistema operativo Unix são fluxos contínuos de bytes de tamanho arbitrário e são a principal fonte de "input"/"output" do sistema.
Os dados contidos num disco são geralmente divididos em dois grupos. O da informação sobre os ficheiros e o da informação neles contida.
Chama-se de **meta-dados** à forma como os dados se dispõem no interior dos ficheiros.
Para criar a abstracção do ficheiro, o kernel necessita de transparentemente traduzir e fazer a associação de um ou mais sectores no disco físico, unindo-os e tornando-os num único fluxo de informação. O sistema de ficheiros serve então para fazer a correspondência entre os sectores do

disco de forma a ser possível unir esse mesmo fluxo.
O conteúdo de um ficheiro é armazenado em blocos de dados que são guardados nos sectores do disco. Quanto maior for o número de sectores por blocos de dados, maior será a velocidade de transferência do disco melhorando assim a performance do sistema. É por esta razão que a desfragmentação de uma partição melhora o desempenho do computador. A transferência é feita "de uma só vez" em vez de ser necessário ao sistema procurar os bocados de informação espalhados anarquicamente pelo disco rígido.
Os blocos de dados são juntos e organizados em ficheiros pelos *inodes*. Os *inodes* são as estruturas de *meta-dados* que representam os ficheiros visíveis pelo utilizador (um inode por cada ficheiro). Cada *inode* contém um vector de apontadores para os blocos de dados e outras informações adicionais, tais como, o código do utilizador proprietário (UID), o código do seu grupo (GID), as suas permissões de acesso, o seu tamanho, entre outros. Os inodes são guardados num vector especial (a chamada "inode table") e são referidos pelo primeiro elemento dessa tabela (o índice 0). O estado de um *inode* (livre ou ocupado) é então guardado num mapa de bits a que chamamos o "*inode bitmap*".
Os *inodes* estão associados a um nome de um ficheiro através de estruturas de dados especiais chamadas *entradas de directórios* que são guardadas dentro de ficheiros do tipo "directório". A estrutura básica de um ficheiro deste tipo segundo os "standards" é:

```
struct dirent {
    int   inode;
    short rec_size;
    short name_len;
    char  file_name[NAME_LEN];
};
```

O campo "inode" desta estrutura contém um valor que é associado ao nome do ficheiro (que por sua vez fica guardado no vector "file_name"). Para poupar espaço, o tamanho real do nome do ficheiro fica guardado no campo 'name_len' da estrutura e o espaço restante do vector "file_name" é utilizado pela próxima estrutura de um directório. O tamanho desta estrutura é geralmente arredondado para a mais próxima potência de base dois cujo valor é guardado no elemento "rec_size" da estrutura. Quando um ficheiro/inode é removido, o valor do elemento "inode" é alterado para "0" e o valor do campo "rec_size" da estrutura "dirent" anterior é aumentado de forma a englobar o "*inode*" eliminado. Isto provoca o efeito de guardar o nome de ficheiros eliminados dentro dos ficheiros do tipo directório.

De cada vez que um ficheiro é associado a outro, um contador interno é incrementado. Da mesma forma, quando uma associação é removida, o contador é decrementado. Quando esse contador atinge o valor "0" significa que já não existem mais referências para aquele "*inode*" dentro da estrutura do directório e o ficheiro é eliminado. Os ficheiros que tenham sido eliminados podem então libertar os recursos ocupados, ou seja, o blocos de dados e o próprio "*inode*". Isto é possível marcando os *bitmaps* apropriados.
Os próprios ficheiros do tipo directório estão logicamente organizados como uma árvore (começando no directório root "/"). Este directório root utiliza sempre o "*inode*" "2" do disco rígido de forma a que o *kernel* saiba localizá-lo e fazer o "mount" ao sistema de ficheiros.
Para poder fazer um "mount" ao sistema, o *kernel* necessita de saber o tamanho e a localização das estruturas do tipo *meta-dados*. A primeira parte da estrutura, o super bloco, é guardada numa localização conhecida. Contém informações variadas tais como, por exemplo, o número de *inodes* e o número de blocos, o tamanho de cada bloco, entre outras. Baseando-se na informação lida no super bloco, o *kernel*, consegue calcular as localizações e os tamanhos das tabelas de *inodes* e os respectivos dados associados.

3.2 – Análise-forense

Independentemente da causa que o motivou a realizar uma análise forense digital, deve o administrador de sistemas sistematizar os seguintes procedimentos:
Independentemente da razão, os seguintes passos devem ser efectuados:
1- Efectuar uma cópia de segurança de todo o sistema de ficheiros;
2- Reunir toda a informação nele contida;
3- Dividir a informação em provas;
4- Examinar essas provas.

Após examinar atentamente todas as provas, o analista deverá tentar:
1- Reunir informação sobre o(s) atacante(s)
2- Determinar o que aconteceu
3- Construir um quadro temporal do compromisso do sistema
4- Descobrir quais as ferramentas e exploits foram utilizadas para comprometer o sistema

Tal como foi explicado no ponto anterior e de acordo com o funcionamento genérico de um sistema de ficheiros "Unix", quando um ficheiro é eliminado o "link" interno correspondente ao seu "inode" é decrementado até ao seu valor ser "0". Após o "inode" ser apagado, o kernel vai

marcar os seus recursos como disponíveis para serem utilizados por outros ficheiros. No entanto, o "inode" continua a conter toda a informação que estava no ficheiro eliminado e os blocos de dados para o qual ele aponta continuam a alojar os conteúdos desse mesmo ficheiro. Este estado manter-se-á assim, até que os *inodes* sejam realocados e reutilizados e, consequentemente, a respectiva data seja reescrita.
Através disto o leitor pode facilmente perceber que simplesmente removendo um ficheiro do sistema não o elimina na realidade.
Este é o funcionamento normal da maior parte dos sistemas visto que demoraria bastante mais tempo a reescrever os blocos ocupados com dados avulsos ou com "zeros". É muito mais simples e rápido o sistema de ficheiros referenciar o espaço como utilizável de forma a ser reescrito.
Um dos programas mais utilizados na ciência forense digital é o **"The Coroners Toolkit"** (TCT).
O analista forense percorre então o disco a um nível bastante baixo de forma a procurar referências de ficheiros eliminados recuperando-os para análise posterior.
Atendendo à típica inexperiência da maior parte dos jovens *hackers*, é vulgar eliminarem-se os ficheiros que se utilizaram durante uma sessão de trabalho recorrendo tão somente às ferramentas nativas do sistema operativo, deixando assim provas que poderá levar o analista até ao autor da intrusão.

3.3 – Anti-análise Forense

A arte e ciência da anti-análise forense parte das falhas da análise forense.
Para o atacante poder camuflar-se completamente do analista forense é necessário conhecer o software especializado geralmente utilizado procurando assim falhas que possam ser usadas em seu proveito.
De acordo com a secção anterior, o analista irá procurar ficheiros eliminados de acordo com o sistema de ficheiros mas ainda referenciados no disco rígido. Ora uma forma bastante simples de corromper a investigação é eliminando completamente os ficheiros a baixo nível.
Isto pode ser feito com software opensource disponível na internet como o **"The Defiler's Toolkit"** (TDT).
O sistema de ficheiros geralmente guarda um registo de toda a actividade "Input"/"Output" a ficheiros. Os analistas forenses tentam ver esse registo de forma a extrairem o máximo de informação deixada para trás pelo atacante.
Além do facto de que as suas ferramentas de análise forense podem reportar incorrectamente informação sobre os dados encontrados, elas são completamente inúteis se os dados simplesmente não existirem no disco. Estas metodologias foram implementadas no "TDT".

Num sistema de ficheiros UNIX, pode-se obter informações sobre a existência de ficheiros através de:
1- inodes;
2- entradas de directórios;
3- blocos de dados.
Todos eles representam provas cruciais para o analista.
A maior parte das ferramentas existentes para erradicar por completo um ficheiro do sistema apenas eliminam as provas dos blocos de dados deixando assim os inodes e as entradas de directórios intactos.
O "TDT" contém dois programas utilizados para remover a informação de um disco rígido por completo. O **necrofile** e o **klismafile**.

3.3.1- O necrofile

O necrofile é um programa que permite procurar todos os "inodes" inutilizados ainda contendo informação (devido a uma eliminação deficiente por parte de um programa normal) eliminando-os depois por completo.
Para isso este programa utiliza como argumento a partição que contém os "inodes" a eliminar por completo.
Analise-se pois o "output" do "TCT" e do "necrofile".

```
[root@golfinho root]$ ./ils /dev/hda6
classlhostldevicelstart_time
ilslXXXl/dev/hda6l1026771982
st_inolst_alloclst_uidlst_gidlst_mtimelst_atimelst_ctimelst_dti
melst_model\
st_nlinklst_sizelst_block0lst_block1
12lfl0l0l1026771841l1026771796l1026771958l102677195
8l100644l0l86l545l0
13lfl0l0l1026771842l1026771796l1026771958l102677195
8l100644l0l86l546l0
14lfl0l0l1026771842l1026771796l1026771958l102677195
8l100644l0l86l547l0
15lfl0l0l1026771842l1026771796l1026771958l102677195
8l100644l0l86l548l0
16lfl0l0l1026771842l1026771796l1026771958l102677195
8l100644l0l86l549l0
17lfl0l0l1026771842l1026771796l1026771958l102677195
8l100644l0l86l550l0
18lfl0l0l1026771842l1026771796l1026771958l102677195
8l100644l0l86l551l0
19lfl0l0l1026771842l1026771796l1026771958l102677195
8l100644l0l86l552l0
20lfl0l0l1026771842l1026771796l1026771958l102677195
8l100644l0l86l553l0
```

21|f|0|0|1026771842|1026771796|1026771958|1026771958|100644|0|86|554|0
22|f|0|0|1026771842|1026771796|1026771958|1026771958|100644|0|86|555|0
23|f|0|0|1026771842|1026771796|1026771958|1026771958|100644|0|86|556|0
24|f|0|0|1026771842|1026771796|1026771958|1026771958|100644|0|86|557|0
25|f|0|0|1026771842|1026771796|1026771958|1026771958|100644|0|86|558|0
26|f|0|0|1026771842|1026771796|1026771958|1026771958|100644|0|86|559|0
27|f|0|0|1026771842|1026771796|1026771958|1026771958|100644|0|86|560|0
28|f|0|0|1026771842|1026771796|1026771958|1026771958|100644|0|86|561|0
29|f|0|0|1026771842|1026771796|1026771958|1026771958|100644|0|86|562|0
30|f|0|0|1026771842|1026771796|1026771958|1026771958|100644|0|86|563|0
31|f|0|0|1026771842|1026771796|1026771958|1026771958|100644|0|86|564|0
32|f|0|0|1026771842|1026771796|1026771958|1026771958|100644|0|86|565|0
33|f|0|0|1026771842|1026771796|1026771958|1026771958|100644|0|86|566|0
34|f|0|0|1026771842|1026771796|1026771958|1026771958|100644|0|86|567|0
35|f|0|0|1026771842|1026771796|1026771958|1026771958|100644|0|86|568|0
36|f|0|0|1026771842|1026771796|1026771958|1026771958|100644|0|86|569|0
37|f|0|0|1026771842|1026771796|1026771958|1026771958|100644|0|86|570|0
[root@golfinho root]$

Utilize-se agora o "necrofile" para localizar e erradicar por completo todos os "inodes" eliminados.
[root@golfinho root]$ ./necrofile -v -v -v -v /dev/hda6
Scrubbing device: /dev/hda6
12 = m: 0x3d334d4d a: 0x3d334d4d c: 0x3d334d4f d: 0x3d334d4f
13 = m: 0x3d334d4d a: 0x3d334d4d c: 0x3d334d4f d: 0x3d334d4f
14 = m: 0x3d334d4d a: 0x3d334d4d c: 0x3d334d4f d: 0x3d334d4f
15 = m: 0x3d334d4d a: 0x3d334d4d c: 0x3d334d4f d: 0x3d334d4f
16 = m: 0x3d334d4d a: 0x3d334d4d c: 0x3d334d4f d: 0x3d334d4f
17 = m: 0x3d334d4d a: 0x3d334d4d c: 0x3d334d4f d: 0x3d334d4f
18 = m: 0x3d334d4d a: 0x3d334d4d c: 0x3d334d4f d: 0x3d334d4f
19 = m: 0x3d334d4d a: 0x3d334d4d c: 0x3d334d4f d: 0x3d334d4f
20 = m: 0x3d334d4d a: 0x3d334d4d c: 0x3d334d4f d: 0x3d334d4f
21 = m: 0x3d334d4d a: 0x3d334d4d c: 0x3d334d4f d: 0x3d334d4f
22 = m: 0x3d334d4d a: 0x3d334d4d c: 0x3d334d4f d: 0x3d334d4f
23 = m: 0x3d334d4d a: 0x3d334d4d c: 0x3d334d4f d: 0x3d334d4f
24 = m: 0x3d334d4d a: 0x3d334d4d c: 0x3d334d4f d: 0x3d334d4f
25 = m: 0x3d334d4d a: 0x3d334d4d c: 0x3d334d4f d: 0x3d334d4f
26 = m: 0x3d334d4d a: 0x3d334d4d c: 0x3d334d4f d: 0x3d334d4f
27 = m: 0x3d334d4d a: 0x3d334d4d c: 0x3d334d4f d: 0x3d334d4f
28 = m: 0x3d334d4d a: 0x3d334d4d c: 0x3d334d4f d: 0x3d334d4f
29 = m: 0x3d334d4d a: 0x3d334d4d c: 0x3d334d4f d: 0x3d334d4f
30 = m: 0x3d334d4d a: 0x3d334d4d c: 0x3d334d4f d: 0x3d334d4f
31 = m: 0x3d334d4d a: 0x3d334d4d c: 0x3d334d4f d: 0x3d334d4f
32 = m: 0x3d334d4d a: 0x3d334d4d c: 0x3d334d4f d: 0x3d334d4f
33 = m: 0x3d334d4d a: 0x3d334d4d c: 0x3d334d4f d: 0x3d334d4f
34 = m: 0x3d334d4d a: 0x3d334d4d c: 0x3d334d4f d: 0x3d334d4f
35 = m: 0x3d334d4d a: 0x3d334d4d c: 0x3d334d4f d: 0x3d334d4f
36 = m: 0x3d334d4d a: 0x3d334d4d c: 0x3d334d4f d: 0x3d334d4f
37 = m: 0x3d334d4d a: 0x3d334d4d c: 0x3d334d4f d: 0x3d334d4f
[root@golfinho root]$

Execute-se novamente o "TCT" para verificar se todos os inodes foram eliminados com sucesso.
[root@golfinho root]$ ./ils /dev/hda6
classlhostIdevicelstart_time
ilslXXXl/dev/hda6l1026772140
st_inolst_alloclst_uidlst_gidlst_mtimelst_atimelst_ctimelst_dti

```
melst_model\
st_nlinklst_sizelst_block0lst_block1
[root@golfinho root]$
```

Após esta operação, os *inodes* foram eliminados com sucesso, restando apenas as entradas de directório como possível prova incriminatória.
Proceda-se então ao uso do "klismafile" para eliminar estas entradas.

3.3.2- O klismafile

O "klismafile" consegue eliminar com segurança as entradas de directório removidas por programas normais. Quando um ficheiro ou "inode" é eliminado, o conteúdo continua descriminado na estrutura do directório. Este programa procura "inodes" nessas circunstâncias e erradica-as por completo do sistema.
Utiliza-se o "fls", programa incluído no "TCT", para procurar entradas de directório apagadas:

```
 [root@golfinho root]$  ./fls -d /dev/hda6 2
? * 0:  a
? * 0:  b
? * 0:  c
? * 0:  d
? * 0:  e
? * 0:  f
? * 0:  g
? * 0:  h
? * 0:  i
? * 0:  j
? * 0:  k
? * 0:  l
? * 0:  m
? * 0:  n
? * 0:  o
? * 0:  p
? * 0:  q
? * 0:  r
? * 0:  s
? * 0:  t
? * 0:  u
? * 0:  v
? * 0:  w
? * 0:  x
? * 0:  y
? * 0:  z
[root@golfinho root]$
```

É então altura de executar o "klismafile" para eliminar por completo estas entradas:

```
[root@golfinho root]$ ./klismafile -v /mnt
Scrubbing device: /dev/hda6
cleansing /
-> a
-> b
-> c
-> d
-> e
-> f
-> g
-> h
-> i
-> j
-> k
-> l
-> m
-> n
-> o
-> p
-> q
-> r
-> s
-> t
-> u
-> v
-> w
-> x
-> y
-> z
Total files found:      29
Directories checked:    1
Dirents removed :       26
[root@golfinho root]$ ./fls -d /dev/hda6 2
[root@golfinho root]$
```

A partir deste momento, é completamente impossível detectar a actividade do atacante do sistema uma vez que o seu rasto foi completamente eliminado. Mas completamente?

3.4- Análise Forense HighTech

Por fantástico que o conceito possa parecer, é efectivamente possível "ver" um bit. Existem dois tipos de microscópios capazes de visualizar o aspecto de um bit num disco rígido ou outro qualquer tipo de suporte magnético.
O *Magnetic Force Microscope* (MFM) – Imagem 8, que utiliza o electromagnetismo como princípio de funcionamento, e o *Scanning Tunneling Microscope* (STM) têm efectivamente a capacidade de visualizar a

Imagem 8: Magnetic Force Microscopy

estrutura molecular das superfícies magnéticas dos suportes, nomeadamente, da área onde um bit possa estar gravado.
Actualmente, existem empresas especializadas que se dedicam à recuperação dos dados em material informático danificado. Têm sido observados alguns casos de sucesso, nomeadamente, na recuperação de dados em discos danificados em incêndios, terramotos e inundações.
As figuras seguintes mostram algumas observações feitas com o microscópio sobre a superfície de vários tipos de discos.

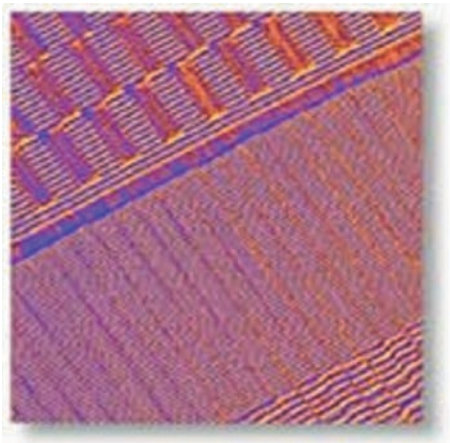


Imagem 9: bits num disco rígido

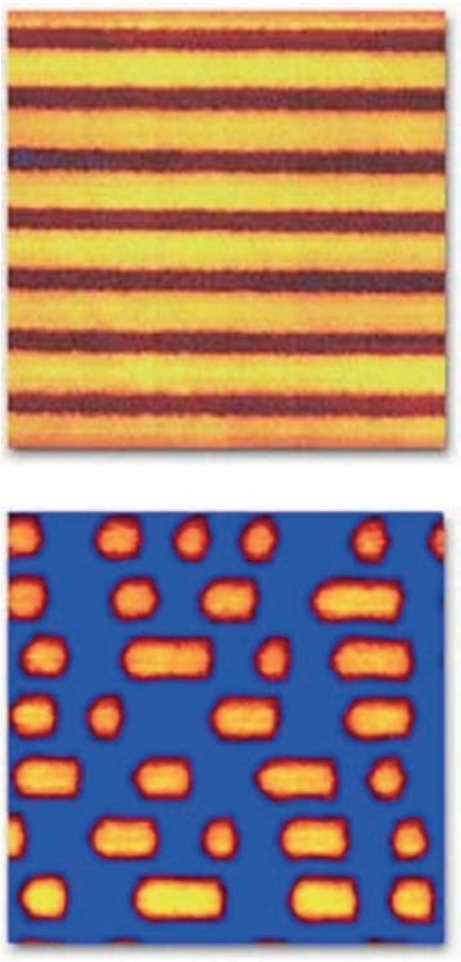


Imagem 10: bits num dvd-rw

4-HoneyPots

Um "honeypot" é um sistema cuja segurança é especialmente desenhada para ser testada, atacada e comprometida.
Pretende-se desta forma analisar padrões de ataques, preveni-los e encontrar falhas não reportadas. Esta ideia surgiu quando alguns *whitehats* (*hackers* sem intenções maliciosas) desenvolveram plataformas de ensaio para estudarem actividades de *blackhats* (*hackers* com intenções contrárias).
Um *honeypot* mais não é do que um sistema antigo a funcionar com bastantes serviços, propositadamente negligenciado no tocante a actualizações de segurança, no qual deliberadamente se colocaram processos de monitorização de intrusão. É um excelente exemplo de análise forense.

4.1-O vmware e a análise-forense

O vmware é um software que permite executar vários sistemas operativos simultaneamente num único computador. Isto é o ideal para um sistema do tipo "honeypot".

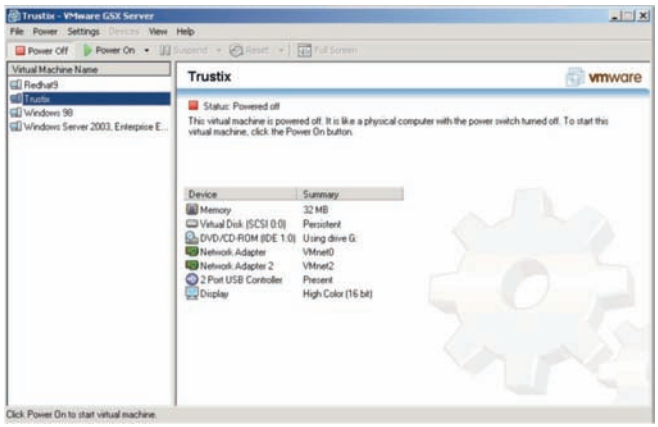


Imagem 7: Vmware GSX Server

Este software permite utilizar uma partição "física" ou criar um espaço virtual. Este espaço virtual é na realidade um único ficheiro embora os sistemas operativos executados o detectem como um disco rígido. Esta aplicação funciona como uma "gateway" entre o sistema operativo "emulado" e o hardware real criando periféricos virtuais para cada um dos sistemas executados.

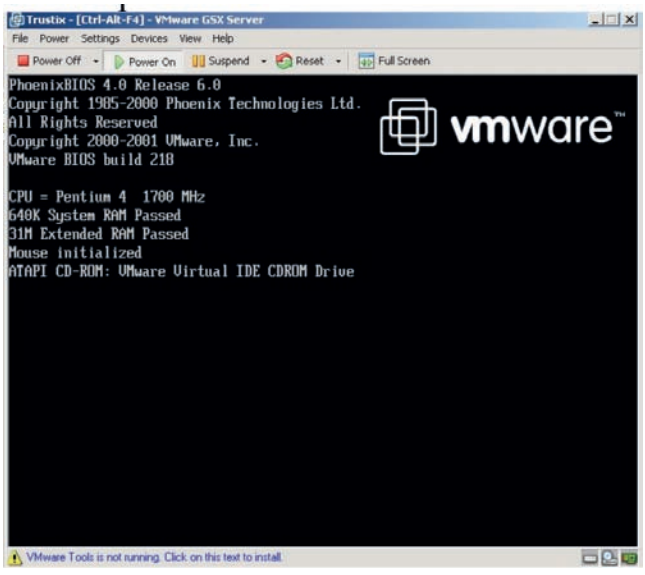


Imagem 8: boot do vmware

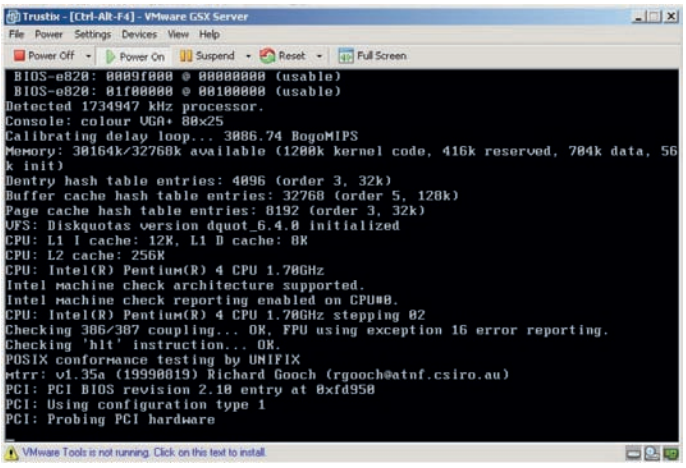


Imagem 9: boot do linux no vmware

Outra característica deveras interessante para o uso do vmware nos honeypots é a possibilidade de fazer um "standby" a um sistema em execução, o que o torna ideal para uma análise forense.

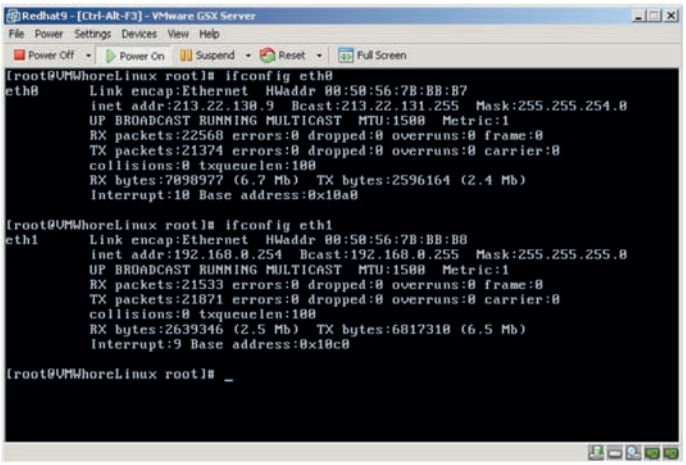


Imagem 10: Interfaces de rede de um sistema operativo linux emulado.

Esta é então uma boa opção para proteger o seu sistema e estudar os atacantes analisando assim as últimas técnicas utilizadas por eles.

4.2- O honeyd

Como desenvolvimento da ideia do projecto "honeypot" foi (e está neste momento) a ser desenvolvido o "honeyd". O "honeyd" é um serviço cuja finalidade é emular outros serviços de forma a enganar um atacante iludindo sobre o sistema que está a tentar comprometer.

A ideia final deste projecto é criar um sistema tão completo e que pareça tão real que seja capaz de iludir qualquer atacante.
Todas as actividades são interceptadas e registadas para serem levadas a cabo análises forenses.
A diferença básica entre um *honeypot* e um *honeyd* reside no facto deste último correr num ambiente virtual separado do sistema operativo que o abriga.
Este sistema é de fácil configuração e permite emular sistemas operativos tão conhecidos como o Microsoft Windows, Linux ou CISCO IOS.

Um ficheiro de configuração possível para emular um servidor windows NT seria:
•create windows
•set windows personality "Windows NT 4.0 Server SP5-SP6"
•set windows default tcp action reset
•set windows default udp action reset
•add windows tcp port 80 "perl scripts/iis-0.95/iisemul8.pl"
•add windows tcp port 139 open
•add windows tcp port 137 open
•add windows udp port 137 open add windows udp port 135 open
•set windows uptime 3284460
•bind 192.168.1.101 windows

Outra configuração para emular um servidor Linux poderia ser:
•create linux
•set linux personality "Linux 2.4.16 - 2.4.18"
•set linux default tcp action reset
•set linux default udp action reset
•add linux tcp port 110 "sh scripts/pop3.sh"
•add linux tcp port 25 "sh scripts/smtp.sh"
•add linux tcp port 21 "sh scripts/ftp.sh"
•set linux uptime 3284460
•bind 192.168.1.102 linux

E um pseudo router CISCO poderia ser criado através de:
•create router
•set router personality "Cisco IOS 11.3 - 12.0(11)"
•set router default tcp action reset
•set router default udp action reset
•add router tcp port 23 "/usr/bin/perl scripts/router-telnet.pl"
•set router uid 32767 gid 32767
•set router uptime 1327650
•bind 192.168.1.104 router

Estas configurações dizem ao serviço (honeyd) para abrir determinadas portas, executar alguns scripts de forma a enganar os atacantes, mostrar um determinado "uptime" (tempo total que o sistema se encontra ligado), em suma, moldar a sua "personalidade" ao sistema em questão.

5-Precauções a tomar numa análise forense

Existem alguns passos vitais a seguir caso um sistema tenha sido comprometido e se queira proceder a uma **correcta** análise forense.
Geralmente quando um servidor é penetrado, a grande prioridade é "voltar a garantir o funcionamento mínimo do servidor...o mais rapidamente possível". É claro que isto traz desleixos e, muito provavelmente, novas portas para os atacantes entrarem.
Quando um sistema é penetrado deve-se proceder a uma análise minuciosa detectando o quando, como e o porquê da intrusão registada.
Então as precauções principais a tomar são:
1-Desligar o sistema da rede
2-Remover os discos e fazer backups com software especializado (que faça cópias integrais dos discos, inclusive do "slack space"
3-Informar as devidas autoridades
4-**Nunca** voltar a usar o sistema comprometido sem antes proceder a uma reinstalação completa do sistema (visto que o mais certo é o atacante ter modificado ficheiros chave do sistema e instalado "rootkits")

6-Conclusões

Cada vez mais vivemos num mundo dominado pelas novas tecnologias. Estas tecnologias estão em constante mutação e evolução.
Devemos ter sempre em conta que com os avanços na **tecnologia** surgem os avanços na **anti-tecnologia**, E, mais importante ainda, na maior parte dos casos o último grito na tecnologia é controlado pelo *equipa adversária* e dependemos das situações aprendidas com eles para nos defendermos. É isso que torna a análise forense uma ciência tão aliciante e importante nas nossas vidas.

Links úteis:

[1] Defeating Forensic Analysis on Unix
http://www.phrack.org/phrack/59/p59-0x06.txt

[2] HoneyPot project
http://project.honeynet.org

[3] VMWare
http://www.vmware.com

[4] Webopedia
http://www.webopedia.com

[5] Free Forensics Tools for Unix
http://online.securityfocus.com/infocus/1503

[6] Steganography
http://steghide.sourceforge.net/download.html

[7] ADS – Alteranate Data Streams
http://www.diamondcs.com.au/streams/streams.htm

[8] Linux Data Hiding and Recovery
http://www.linuxsecurity.com/feature_stories/data-hiding-forensics.html

[9] TCT – The Coroners Toolkit
http://www.fish.com/tct/

[10] Basic Steps in Forensic Analysis of Unix Systems
http://staff.washington.edu/dittrich/misc/forensics/

[11] HardDisk Recovery
http://www.harddisk-recovery.com/

ISSN 0874-8799