Universidade Católica Portuguesa
Faculdade de Engenharia

Informática Forense

Recolha e preservação da prova digital

Pedro Penha Leitão da Costa Marques

Dissertação para obtenção do grau de Mestre em Segurança em Sistemas de Informação

Orientador: Prof. Doutor Rui Alves Pires

Maio de 2013

Conteúdo

Resumo

A proliferação das redes de comunicações digitais na sociedade levou a um concomitante aumento do seu envolvimento em atividades ilícitas. O exame e análise forense dos sistemas informáticos tornaram-se assim numa importante e fundamental ajuda a todos aqueles que têm de lidar com incidentes informáticos, sejam eles do foro criminal, cível ou simplesmente laboral.

A correta execução dos procedimentos quer em termos técnicos quer jurídicos, que regem a identificação, a recolha e a preservação da prova digital, torna-se assim fundamental por se tratar do primeiro passo na cadeia de custódia da prova, fundamental para a sua admissão legal.

A presente dissertação agrega num único documento as melhores práticas, recomendações e normas que regem a identificação, recolha e preservação da prova digital, enquadrando estas práticas no ordenamento jurídico português. Todos os procedimentos sugeridos estão enquadrados pela lei portuguesa, apresentando-se alguns exemplos de procedimentos que embora tecnicamente lógicos e corretos seriam no entanto legalmente inadmissíveis e eventualmente até consubstanciar crime.

São levadas em conta as determinações da norma ISO 27037:2012 e as recomendações de diversos organismos internacionais tão diversos como o Concelho Europeu, o G8 ou a IOCE.

Esta dissertação descreve os procedimentos de planeamento e execução de uma operação de recolha e preservação de suportes digitais.

Adicionalmente, apresenta os procedimentos e ferramentas utilizados na preparação e utilização dos suportes de armazenamento da prova digital, incluindo a sua validação através de assinatura digital.

Apresenta ainda os procedimentos de recolha de prova em sistemas corporativos, em fontes abertas, de interpretação de cabeçalhos de mensagens de correio eletrónico e por essa via da identificação da sua origem.

Finalmente e sob uma forma que pode ser facilmente adaptada a pequenos manuais ou guias de bolso, consolida os procedimentos, direcionando-os para agentes de primeira resposta, independentemente do seu nível técnico.

Palavras-chave: incidentes informáticos, prova digital, procedimentos, admissibilidade legal, normas e melhores práticas.

Abstract

The proliferation of digital communication networks in society has led to a concomitant increase in their involvement in illicit activities. The examination and analysis of all computer equipments has become an important aid to those that must deal with computer incidents, criminal, civil or labour related.

The correct technical and juridical execution of the proceedings, that rules the identification, recovery and collection of digital evidence, is fundamental since it becomes the first step in the evidence chain of custody.

This thesis consolidates in a single document the best practices, recommendations and norms that rule the identification, collection and preservation of the digital evidence, according to the Portuguese law. Every proceeding is according to the Portuguese law and some examples are presented whereas technically logical and correct would be legally inadmissible and possibly even a crime if undertaken.

The ISO 27037:2012 is taken into consideration as well as the recommendations of several international organizations such as the European Council, the G8 or the IOCE.

This thesis describes the correct proceedings of the planning and execution of a collection and preservation of digital evidence operation.

In addiction it presents the proceedings of the preparation of the digital evidence supports, including their validation through digital signature.

It also presents the proceedings of evidence collection in corporate systems, through open sources, the interpretation of email headers and through that way the identification of their source.

Finally and under a format that can easily be converted into a small manual or pocket guide, all the proceedings are consolidated independently of technical knowledge and directed to a first responder.

Keywords: computer incidents, digital evidence, proceedings, legal admittance, norms and best practices.

1 Introdução

1.1 Motivação

A proliferação da utilização da informática e das plataformas digitais, o crescimento exponencial da utilização dos recursos disponíveis através da Internet na sociedade atual (ver figura 1.1 e 1.2) e sendo a sua utilização transversal a toda a sociedade, tanto na vertente profissional como particular, trouxe inegáveis vantagens na forma como os países, as empresas e as pessoas comunicam nos dias de hoje.

Esta realidade trouxe também novos problemas. O cibercrime é uma realidade inegável com a qual há que saber lidar. As organizações em geral, os seus departamentos de Tecnologias de Informação (TI), de auditoria de TI e utilizadores em particular, têm de se consciencializar desta realidade de forma a prepararem as respostas adequadas. O primeiro passo na mitigação deste problema é estar consciente da sua existência.

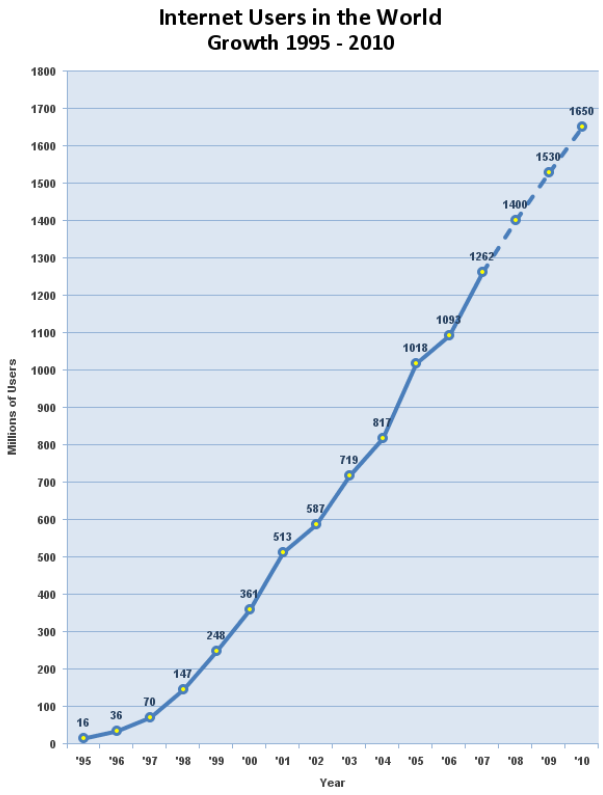


Fig. 1.1 – Evolução do número de utilizadores de Internet
(Fonte: http://www.internetworldstats.com/)

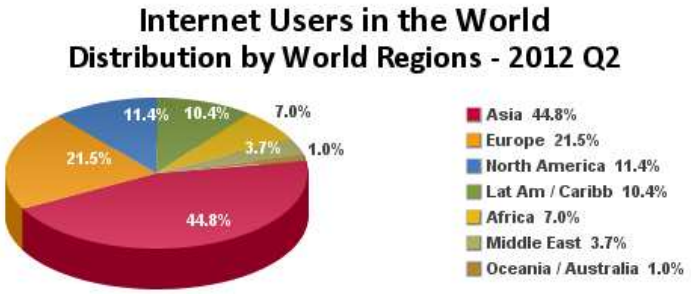


Fig. 1.2 - Distribuição de utilizadores de Internet por regiões do planeta (http://www.internetworldstats.com/)

Casos de enorme impacto mediático como a sabotagem do oleoduto Russo no Cazaquistão em 1992, do ataque à Estónia e da operação Israelita "*Orchard*" em 2007, da ciberguerra entre a Geórgia e a Federação Russa em 2008, do "*GhostNet*" em 2009, do *Stuxnet* em 2010, ou de ações recentes de grupos de ativistas como o "*Anonymous*", são exemplos de ataques para os quais as organizações têm de estar preparadas.

Uma empresa pode ser um alvo apenas pelo facto de ser suficientemente grande para poder atrair as atenções mediáticas de um ataque informático, ou porque se trata de uma empresa do estado ou lhe presta serviços e alguém quer tomar uma posição política, ou porque um empregado quer vingar o seu despedimento, ou porque a informação é um ativo que é alvo de um qualquer ransomware ou porque simplesmente produz artigos com recurso a pele de algum animal em vias de extinção.

A complexidade das organizações modernas, a sua dependência face às tecnologias de informação e a crescente interconectividade entre as empresas, os sistemas financeiros e os próprios países, que são em si mesmo o resultado e o motor do e-business, criam um grande leque de oportunidades para a prática de diversos crimes praticados dentro e fora das organizações, não olhando a jurisdições e fronteiras.

Vulnerabilidades tradicionais e novas, quer seja no *software* quer no *hardware* que sustentam as organizações e os países, podem ser exploradas em segundos, de um qualquer ponto do nosso planeta globalizado e põem em causa o funcionamento das organizações, dos países e em ultima análise da vida em sociedade, tal como demonstram os últimos números disponíveis sobre o impacto financeiro do Malware. (ver figura 1.3)

Financial Impact of Malware Attacks 1997–2006

Worldwide Impact (U.S. $)	
2006	$13.3 Billion
2005	14.2 Billion
2004	17.5 Billion
2003	13.0 Billion
2002	11.1 Billion
2001	13.2 Billion
2000	17.1 Billion
1999	13.0 Billion
1998	6.1 Billion
1997	3.3 Billion

Fig. 1.3 - Impacto Financeiro do Malware, estimado pela Computer Economics em 2007

De acordo com os números de 2012, o número de ataques por *Malware* foi superior a 200 milhões[1]. Em 2010 a McAfee revelou que os custos em horas de trabalho das organizações, devido a ataques de vírus foram de 6.3 milhões de dólares por dia[2].

No relatório anual de 2012 da Symantec, estima-se um impacto anual de 110 mil milhões de dólares de prejuízos na economia mundial, causado por programas maliciosos[3].

Neste contexto, as organizações necessitam ter consciência das suas vulnerabilidades, dos riscos que correm e de que maneira a impreparação as pode deixar expostas a um ataque ou sem uma resposta adequada caso assintam a desvios de ativos financeiros, a furtos de propriedade intelectual, à descredibilização pública da imagem ou até ao completo bloqueamento da atividade da empresa.

Os sistemas informáticos podem estar relacionados com a atividade criminosa de três formas. Como armas para os cometer, como arquivo de indícios ou prova de crimes ou como as próprias vítimas de um ataque.

À medida que as empresas vão progressivamente integrando os seus serviços com os dos seus fornecedores, distribuidores e clientes, a sua exposição ao risco aumenta exponencialmente. A deslocalização para um paradigma de sistemas de TI e de um modelo de negócio assente no outsourcing, como o cada vez mais utilizado “cloud computing”, seja ela ao nível do serviço, do software ou do hardware, ao mesmo tempo que oferece enormes oportunidades de redução de custos e aumento de eficiência em termos humanos e de infraestruturas, também introduz um novo nível de riscos.

De igual modo, a crescente utilização de plataformas digitais móveis e a necessidade de as integrar no normal funcionamento das redes corporativas, também acarreta novos desafios de segurança que não podem ser ignorados.

É uma certeza que o aumento do número de internautas, estimados atualmente em dois mil milhões[4] e com um crescimento na ultima década de 566 %, vai provocar inevitavelmente um aumento proporcional do cibercrime.

Sendo uma certeza que um sistema informático vai mais tarde ou mais cedo estar envolvido numa atividade ilícita, é imprescindível que quem seja responsável por estes ativos saiba dar uma resposta adequada, não só para minimizar o impacto no negócio como também, para maximizar a possibilidade de vir a imputar responsabilidades aos autores dos atos praticados, para em sede de responsabilidade civil, poderem vir a ser recuperados parte ou a totalidade dos prejuízos provocados.

1.2 Descrição do problema

Após a ocorrência de um ato ilícito num sistema informático e pelas suas características intrínsecas, ficam registados uma série de indícios e provas, que importa saber recolher, preservar e apresentar para que, tal como já referido, se possam identificar os autores dos factos praticados, de forma inequívoca e legalmente admissível.

O autor, ao longo dos mais de 15 anos de atividade profissional na área da investigação criminal em crimes relacionados com tecnologia, tem constatado inúmeras situações em que uma deficiente recolha e preservação da prova digital, deitou por terra toda uma investigação, por vezes com consequências graves para as vítimas e lesados.

Uma simples não conformidade na armazenagem da prova e a consequente quebra da cadeia da prova, provoca a sua imediata anulação por inadmissibilidade legal.

E este problema não se esgota em sede de processos-crime, verificando também vários casos em sede de processo civil, de trabalho ou em situações de regulação de poder paternal.

Visto o problema pelo outro prisma, também tem o autor verificado que é raro o defensor preocupar-se em verificar a validade probatória da prova digital.

1.3 Desafio

Verifica-se que o cerne do problema do tratamento da prova digital, tem a ver essencialmente com a ponte que é necessário estabelecer entre a técnica e a legalidade da sua aplicação.

Invariavelmente, os técnicos não têm uma formação jurídica adequada e os juristas têm muita dificuldade em entender as nuances técnicas dos equipamentos e da informação neles armazenada.

Os problemas relacionados com as comunicações eletrónicas e em particular o correio eletrónico, onde para os técnicos a apreensão e tratamento dos seus conteúdos não é diferente de outra sequência de bytes e para um jurista e de acordo com a lei, o seu tratamento requer cuidados diferenciados ou as questões de competência jurisdicional levantadas pela vulgarização da utilização do "*cloud Computing*", são apenas dois exemplos do problema do equilíbrio que é necessário estabelecer entre as técnicas utilizadas e a sua admissibilidade legal.

1.4 Definição do âmbito

A emergência do fenómeno tecnológico, a sua geração e o nascimento da sociedade da informação trouxe mudanças no desenvolvimento social e económico, mas simultaneamente criou novas formas de prejudicar interesses e direitos fundamentais privados e coletivos. Com o surgimento destas novas condutas ilícitas ou abusivas, os sistemas de justiça viram-se obrigados a intervir nos denominados crimes informáticos.

Na Informática forense, não se analisam os dispositivos informáticos através de técnicas tradicionais de recolha de prova, já que a prova digital assume carácter temporário e de grande volatilidade.

Envolve a aplicação de técnicas que visam analisar conteúdos digitais de memória de massa ou outros ao nível do bit, com o intuito de recolher prova da prática de um ou mais crimes mantendo no entanto as características principais da cadeia probatória, ou seja, a prova digital deve ser tratada como os demais meios de prova, devendo ser:

- Admissível. Deve estar em conformidade com os requisitos legais para que possa ser admitida em tribunal;
- Autêntica. Tem de ser atribuível a autoria da mesma e deve ser possível associar o material probatório ao incidente;
- Precisa. Não pode haver ambiguidades na sua relação com os factos e nenhum aspeto da recolha e armazenamento de informação deve por em causa a autenticidade e veracidade da prova recolhida;
- Completa. Tem provar por si só determinado facto e deve ser possível contar toda a história e não apenas uma perspetiva particular.

Pode afirmar-se que a análise forense é de uma forma genérica a aplicação de técnicas científicas a questões de interesse legal. No contexto das TI e da segurança da informação, pode-se defini-la de uma forma mais precisa como sendo a inspeção sistemática e tecnológica de um sistema informático e dos seus conteúdos, para a obtenção de provas de um crime ou qualquer outro uso que seja investigado.

A análise forense é hoje em dia uma peça chave para a investigação criminal e civil, nos processos de resposta a incidentes de segurança e visa encontrar as respostas às tradicionais perguntas da investigação criminal, "o quê?", "quem?", "quando?", "como?", "onde?" e "porquê?".

A informática forense envolve a análise de suportes de armazenamento de informação e de todo o seu conteúdo, com o objetivo de descobrir provas de uma determinada ação ou ato criminoso. Este processo efetuado por técnicos especializados, por norma, envolve a investigação de um determinado suporte de informação, não estando limitado a discos rígidos de computador, podendo ser efetuado em dispositivos tão diversos como memória USB, discos externos, telemóveis ou cartões de telemóvel.

O processo de uma análise forense deve ser dividido em quatro fases:

1. Identificação da origem da prova digital;
2. Preservação da prova (pode implicar a duplicação da prova);
3. Análise e investigação das provas;
4. Apresentação de relatórios ou resultados.

O principal objetivo da informática forense é a criação de relatórios especializados ou estudos em profundidade de qualquer incidente relacionado com as TI, que podem ser tão diversos como o uso fraudulento de equipamentos, a pirataria, a destruição de informação por colaboradores ou *hackers* externos à empresa ou a ocultação de ficheiros, entre muitas outras possibilidades.

Foi nos anos 70 do século passado, mas com especial incidência nos anos 80, que se começaram a verificar os primeiros crimes informáticos[5] nos EUA, tendo sido a partir daí que houve a necessidade de dotar as forças policiais e os investigadores militares dos meios necessários para combater criminosos com elevados conhecimentos técnicos. Agentes governamentais encarregues de proteger informações importantes, secretas e confidenciais, tiveram igualmente de adaptar as normas, os procedimentos e os meios para dar resposta a estes novos desafios, permitindo analisar não só essas violações como aprender a evitar situações idênticas futuras.

Ao longo dos anos tem-se assistido a uma crescente interligação entre os domínios da segurança da informação, que se concentra na proteção da informação como ativo, e da informática forense, que incide sobre a resposta a situações ilícitas sobre esse mesmo ativo.

As forças policiais e militares continuam a marcar uma forte presença nas áreas da segurança da informação e da informática forense, embora as empresas privadas tenham igualmente seguido a estratégia de empregar directamente profissionais de segurança informática e informática forense, ou como alternativa, contratar outras empresas especializadas com base nas suas necessidades.

No sector privado tem-se assistido a um aumento do recurso a investigações de informática forense em disputas jurídicas de carácter civil, o que provoca um crescimento da informática forense. Cada vez mais empresas privadas de informática forense e investigadores privados estão a obter um nível

de conhecimento mais alargado nesta área, disponibilizando recursos e serviços imprescindíveis a empresas e entidades oficiais.

As empresas de *software* continuam a produzir novos e mais robustos programas de software forense e ao nível da lei e das forças policiais existe uma contínua procura para identificar e treinar mais e melhor os peritos e investigadores criminais, em resposta à evolução da prática de crimes que envolvem tecnologia.

1.5 Objetivo da tese

Tendo presente o problema acima referido, o objetivo da presente dissertação é contribuir para a sua mitigação, definindo um conjunto de regras, métodos e boas práticas, de forma a tornar a prova legalmente admissível em sede de processo-crime ou cível e de acordo com o ordenamento jurídico português.

Esta dissertação debruçar-se-á sobre os dois primeiros pontos do processo da análise forense, que são a identificação da prova digital e a sua recolha e preservação.

1.6 Estrutura

Para atingir o objetivo estabelecido, o autor recorrerá à experiencia que acumulou ao longo de 15 anos, durante os quais lidou diariamente com esta realidade. Serão igualmente contempladas as recomendações das principais organizações internacionais que lidam com esta temática, enquadrando-as na realidade nacional e no seu enquadramento jurídico.

Todos os procedimentos sugeridos nesta dissertação estão de acordo com a lei portuguesa e em algumas situações serão enunciados exemplos de pequenos passos adicionais, que tecnicamente poderão fazer sentido, mas que juridicamente poderão já enquadrar a prática de crime.

Será também levada em conta a norma ISO/IEC FDIS 27037:2012, recentemente publicada e que define os procedimentos internacionalmente aceites, sendo pelo levantamento destas recomendações que a dissertação se inicia.

A estrutura do documento segue a sequência lógica do que seria encontrado numa situação prática, começando por detalhar os passos de uma operação de recolha da prova.

Os capítulos seguintes servem de suporte a este primeiro, nomeadamente naquilo que tem a ver com os meios a utilizar na preservação dos meios de prova, ou seja, os suportes, a sua sanitização e a validação dessa prova através da utilização de assinatura digital.

Atendendo a que em muitas situações, parte da prova que importa preservar não se encontra armazenada em dispositivos fisicamente presentes e antes do capítulo dedicado ao quadro legislativo português relevante, são apresentados capítulos dedicados a recolha de prova em fontes abertas e em mensagens de correio eletrónico.

No final, são apresentados nos anexos e de uma forma mais sistemática e ordenada, os procedimentos a executar em cada uma das situações previstas, com o objetivo de estes poderem ser facilmente transformados em pequenos guias de bolso ou manuais de procedimentos.

2 Estado-da-arte

O propósito deste capítulo não é o de apresentar um estudo comparativo entre as várias propostas de boas práticas entre os vários países e organizações internacionais, que sairia do âmbito da presente dissertação. Procura-se apenas fazer um levantamento das soluções atualmente preconizadas pelas principais organizações que lidam com a prova digital, assinaladas as suas principais linhas de recomendações e identificados os *standards* internacionais.

2.1 Nacionais

A prova digital em Portugal é regulada pelas leis criminais, tal como discutido no capítulo dedicado ao enquadramento legislativo desta temática.

Em termos do sector público e sendo a Polícia Judiciária a entidade que em Portugal tem atribuída a competência para a investigação criminal dos crimes informáticos, tem sido através desta que têm sido ao longo dos anos adotadas as melhores práticas na interação com a prova digital.

As organizações internacionais das quais a Polícia Judiciária faz parte tal como a Interpol e a Europol, têm vindo a emitir ao longo dos anos diversos documentos com recomendações de boas práticas, criados em grupos de trabalho onde têm assento diversas autoridades policiais e judiciais de diversos países, entre os quais elementos da própria Policia Judiciária.

Estes documentos têm permitido criar um *standard* de boas práticas que é seguido por todos os países, já que no âmbito das diversas investigações transnacionais é necessário garantir a idoneidade da prova recolhida em determinado país, para que esta possa ser relevada nos demais países.

É por esta razão que ao analisarmos os manuais de diversos países, encontramos grandes semelhanças ou até recomendações que parecem decalcadas umas das outras.

Este facto permitiu que a norma ISO/IEC FDIS 27037:2012 publicada em Outubro de 2012, fosse criada à imagem e semelhança dos standards já existentes.

Assim sendo deverá ser sobre esta norma que se deverão reger todas as boas práticas em Portugal.

Até à publicação desta norma em 2012, não existia nenhum padrão que pudesse ser utilizado em Portugal, encontrando-se apenas uma recomendação no CERT.PT[6], que remete para um documento publicado pela FCCN em Maio de 2012[7]. Trata-se de um documento de 15 páginas, que traça em linhas gerais quais deverão ser os cuidados que uma organização deverá ter em relação à recolha de dados de prova, dando alguns concelhos em função do tipo de crime de que se foi vítima e referindo algumas ferramentas a que se pode recorrer.

Em relação ao sector privado e no que se relaciona com as grandes empresas nacionais e multinacionais instaladas em Portugal, não existem documentos públicos que permitam uma análise detalhada, sendo uma constatação que estas adotam as boas práticas emanadas das respetivas casas mãe ou adotam políticas das suas congéneres internacionais, como é o caso da banca.

2.2 Internacionais

Apresentam-se de seguida diversas organizações internacionais, que ao longo dos anos têm publicado documentos relacionados com a recolha e preservação da prova digital e que dessa forma foram contribuindo para a unificação de boas práticas, que levou à recente publicação da norma ISO/IEC FDIS 27037:2012.

G8[8]

Em Março de 1998 a IOCE[9] foi encarregada de definir os princípios que deveriam reger a nível internacional, os procedimentos na interação com a prova digital, de forma a garantir uma harmonização entre os diversos métodos e práticas até então adotadas em diversos países. Desta forma garantir-se-ia a possibilidade legal de utilizar prova digital recolhida num determinado pais, noutro, desde que cumpridas essas recomendações.

Em Março de 2000 e no seguimento da conferência "International high-tech crimes and forensics", que teve lugar em Outubro de 1999 em Londres, foram feitas as seguintes recomendações:

1. Cada estado membro foi encorajado a seguir os princípios recomendados quando definir os seus procedimentos para a recolha, preservação e manipulação de prova digital, adaptando-os aos respetivos ordenamentos jurídicos e organizações nacionais, devendo no entanto estar preparados para responder às diferentes exigências de cada país.
2. Estes princípios deviam ser comunicados pela IOCE para revisão, a todos os organismos internacionais, nacionais e regionais, responsáveis pela definição e implementação de standards e pela promoção de recomendações de boas práticas nesta área.
3. A IOCE em coordenação com as entidades do ponto 2, ficou encarregue de desenvolver um guia genérico de boas práticas para a recolha, preservação e manipulação de prova digital.
4. O documento produzido pelo IOCE deverá ser revisto regularmente pelo grupo de trabalho do "high tech crime".

Os princípios então definidos foram:

- Quando se lida com prova digital, devem ser aplicados todos os procedimentos e regras que se aplicam aos demais tipos de prova;
- Quando se interage com prova digital, nenhuma ação deve provocar qualquer alteração;
- Quando é necessário aceder à prova digital, a pessoa que o faz deve ter treino adequado;
- Toda a atividade relacionada com a recolha, apreensão, acesso, transporte e armazenagem da prova digital, deve ser exaustivamente documentada e preservada para futura auditoria e revisão;
- Cada indivíduo que interage com a prova digital ao longo da sua cadeia da prova, é responsável pelas suas ações/omissões sobre esta, quando a tem à sua responsabilidade;
- Cada organismo que é responsável pela apreensão, acesso, armazenamento ou transporte da prova digital ao longo da sua cadeia da prova, é responsável pelas suas ações/omissões sobre esta, quando a tem à sua responsabilidade;

Foram definidos também os conceitos gerais relacionados com a prova digital:

- Prova digital
  Informação guardada ou transmitida em formato binário que possa ser relevada em tribunal.
- Prova digital original
  Objetos físicos e dados, que estão associados no momento da apreensão.
- Prova digital duplicada
  Uma cópia forense é um duplicado exato de todos os objetos de dados contidos no objeto físico original.
- Copia
  Uma cópia é uma reprodução exata de toda a informação contida nos objetos de dados independentemente do objeto físico original.

Estes princípios têm norteado todos os organismos que se têm debruçado por esta temática.

"Forensic Computing Group", Reino Unido

Este grupo de trabalho é provavelmente o mais antigo que se dedica a esta temática, é formado por diversas agências de investigação criminal e de ciências forenses que se dedicam à prova digital, incluindo a "Association of Chief Police Officers (ACPO)[10] Computer Crime Working Group (CCWG)".

O CCWG da ACPO foi o primeiro a produzir um guia de boas práticas para a busca, recolha, apreensão e exame da prova digital[11]. Este primeiro guia foi adotado por todas as agencias de investigação criminal em Inglaterra, tem vindo a ser melhorado ao longo dos anos e foi adotado pelo "National High Tech Crime Unit" quando esta unidade foi criada e que se encontra atualmente integrada no SOCA[12].

Este manual era inicialmente apenas dirigido a "*first responders*", mas foi evoluindo ao longo dos anos, sendo atualmente um guia também para exames forenses.

European Network of Forensic Science Institutes - Forensic Information Technology Working Group (FIT-WG)

Em 1998, o "Forensic Information Technology Working Group" foi criado sob os auspícios da Rede Europeia de Institutos de Ciências Forenses[13].

Este grupo de trabalho que inicialmente trocava unicamente informação técnica forense, em 2001 e em coordenação com a IOCEO começou a debruçar-se na elaboração de um manual [14], que para além das questões técnicas e de qualidade das boas práticas, também trata de questões ligadas à formação de quem tem de lidar com a prova digital.

National Institute of Justice (NIJ), United States Department of Justice

O Instituto Nacional de Justiça dos EUA[15] produz um manual [16] desde o ano 2000, que tem vindo a evoluir desde a versão inicial apenas direcionada para os "first responders" até à versão atual que também trata os exames forenses, estando como seria de esperar, juridicamente direcionada para a legislação federal dos EUA.

Scientific Working Group on Digital Evidence (SWGDE)

Este grupo foi inicialmente criado por membros das agências Norte Americanas FBI e Secret Services, mas integra atualmente membros de muitos países e tem como principal missão a criação de boas práticas na gestão da prova digital e a criação de canais de cooperação entre as diversas agencias que integram o grupo.

O comité Forense é aquele responsável pelo desenvolvimento de técnicas e boas práticas na área forense digital.[17]

International Organization on Computer Evidence (IOCE)

É um dos mais antigos organismos internacionais que lida com a prova digital. Foi formado em 1995 e tem servido como fórum para troca de informações e como líder no desenvolvimento de standards. Foi encarregue pelo "High Tech Crime Sub-Group" do G-8, no âmbito de um simpósio organizado pela Interpol, de desenvolver standards que regulem a troca de prova digital entre sistemas jurídicos de diversos países.
Partindo dos princípios gerais definidos pelo G8, foi criado no ano de 2000 e em colaboração com diversos grupos de trabalho de diversos países e da Interpol, o primeiro guia de recomendações e boas práticas[18].

Concelho Europeu

O comité europeu dedicado ao fenómeno criminal, CDPC[19], mais concretamente aquele dedicado ao cibercrime[20] definiu a convenção europeia sobre o cibercrime[21], que entre muitas outras normas também define uma série de regras na manipulação da prova digital.

A norma ISO/IEC FDIS 27037:2012

A norma ISO / IEC 27037:2012 "Tecnologias de informação - Técnicas de segurança - Diretrizes para identificação, aquisição, recolha e preservação de prova digital", publicada em 15 de Novembro de 2012, é um corolário das orientações e recomendações da RFC 3227, atualizada para dispositivos mais atuais e de muitas outras recomendações utilizadas por diversos organismos internacionais, tais como aqueles já especificados.

Está claramente orientada para o desempenho de especialistas num cenário de busca, recolha e apreensão de provas digitais, não entrando na análise forense da mesma.

Debruça-se sobre os seguintes dispositivos e ambientes:

- Equipamentos e meios de armazenamento e periféricos;
- Sistemas críticos de alta disponibilidade;
- Computadores e dispositivos de rede;
- Dispositivos móveis;
- Circuitos CCTV digitais;
- Sistemas de navegação móvel;

Baseia a norma nos seguintes princípios:

- Aplicação de Métodos

  A prova digital deve ser recolhida do modo o menos intrusivo possível, procurando preservar a originalidade da prova, recorrendo tanto quanto possível a cópias de backups.

- Processo auditável

  Os procedimentos e documentação produzidos devem ser validados e verificados pelas boas práticas profissionais. Devem ser registados os passos dados e os resultados obtidos.

- Processo repetível

  Os métodos e procedimentos utilizados devem ser repetíveis, verificáveis e discutíveis ao nível da compreensão pelos especialistas na matéria, que por essa via lhes podem dar credibilidade.

- Processo defensável

  As ferramentas utilizadas devem ser referidas no relatório do processo e estas devem ter sido validadas e comprovadas para o fim utilizado.

Para cada tipo de dispositivo a norma estabelece o tratamento e atuação da prova neles contida, em três processos distintos de processamento:

- Identificação

  É o processo de identificação das provas e consiste em localizar e identificar informações potenciais ou elementos de prova nos seus dois estados possíveis, o físico e o lógico, conforme o caso de cada tipo de prova.

- Recolha e/ou aquisição

  Este processo é definido como o conjunto de dispositivos e documentação (apreendidos e recolhidos) que podem conter provas ou a cópias de informação existente nos dispositivos.

- Conservação / preservação

  A prova deve ser preservada para garantir a sua utilidade probatória, ou seja, a sua originalidade deve ser mantida para esta seja admissível como prova completa. Todas as ações sobre esta devem claramente garantir a cadeia da custódia da prova.

3 Recolha da prova

O presente capítulo define uma série de recomendações e boas práticas, que permitem criar um protocolo de procedimentos que possibilita a uma organização acautelar e recolher prova digital de forma a ela poder ser entregue em condições legal e tecnicamente admissíveis.

A organização deve estar preparada para que computadores ou suportes digitais pertencentes ou presentes na empresa, possam ter de ser apreendidos pelas autoridades para serem examinados pela prática de crimes tão diversos como a violência doméstica, o furto de identidade, as burlas, as falsificações, o tráfico de estupefacientes, os homicídios, o abuso sexual de crianças, as ameaças, as difamações ou o jogo ilegal.

Deve ainda ter em atenção àquelas situações em que a empresa é a própria vítima, como em casos de acessos ilegítimos ou indevidos a informação, situações que envolvam ransomware ou relacionadas com o desempenho dos seus colaboradores, em que embora se entenda não haver motivos de participação criminal às autoridades, há que estar preparado para recolher de forma eficaz a prova digital, que pode vir a ser de capital importância num processo cível ou de trabalho.

Atendendo a esta realidade, o que vai ser apresentado vai mais além daquilo que é recomendado pelas boas práticas aplicadas pelas autoridades judiciárias.

A sequência de recomendações pretende simular os passos de uma situação real, começando-se pela identificação das provas potenciais, pelo planeamento da abordagem, pela abordagem propriamente dita, pela entrevista do alvo e pela recolha e acondicionamento da prova, aquilo a que na gíria normalmente se refere como “Bag&Tag”, utilizando a referência anglo-saxónica.

Todas estas recomendações têm sempre em conta o enquadramento jurídico português.

3.1 Identificação de potenciais provas

Como em qualquer investigação criminal devem de ser acautelados e fundamentados os motivos da abordagem ao sistema informático. Devem ser acauteladas as questões jurídicas envolvidas no acesso ao sistema, quando estão em causa os dispositivos que têm uma utilização pessoal, ainda que pertençam à empresa.

Este tema será tratado com mais detalhe no capítulo dedicado às questões jurídicas.

A preservação de prova digital implica responsabilidades críticas adicionais, tais como:

- Utilização de um conjunto de técnicas que não alterem ou destruam a prova.
- As análises dos sistemas devem ser realizados por pessoas treinadas e habilitadas para o efeito e que possam em sede judicial testemunhar sobre os passos realizados.

Os motivos do acautelamento da prova digital podem incluir:

- O computador é contrabandeado ou o resultado de um crime.
- O computador contém prova de um crime ou de uma atividade ilícita.
- O computador foi uma ferramenta de um crime ou de uma atividade ilícita.
- O computador é o instrumento e contém o resultado de um crime ou de uma atividade ilícita.

3.2 Planeamento da abordagem

Todos os protocolos de segurança utilizados pelas autoridades na execução de uma busca judicial, devem ser especialmente atendidos. A segurança vem sempre primeiro. Qualquer tarefa a executar deve sempre ter como primeira preocupação, a segurança de quem a executa.

Adicionalmente devem ser estabelecidos protocolos na organização, para definir os procedimentos que são críticos para o sucesso da operação de preservação da prova.

- No briefing da operação, devem ser atribuídas áreas de responsabilidade;
- Definir quem coordena a operação;
- Definir quem procede à entrevista do funcionário;
- Definir quem faz parte da equipa de pesquisa e quem no local vai proceder à apreensão;
- Deve certificar-se que quem vai proceder à preservação da prova, tem o treino adequado nas melhores práticas no manuseamento de prova digital.

Deve ser recolhido o máximo de informação possível sobre o sistema que vai ser alvo da averiguação.

Para além da normal recolha de informação de "intelligence", tal como localização e layout físico do espaço, outra informação que deve ser recolhida deve incluir:

- A informação a preservar é da empresa ou do funcionário?
- Que sistemas são esperados no cenário?

Pode estar em causa um simples PC, vários e ligados em rede, informação armazenada no data center, num portátil ou PDA ou armazenada em sistemas subcontratados com localização remota, que pode inclusivamente estar alojada num país estrangeiro.

Equipamentos a considerar

Objetos imprescindíveis a ter sempre preparados e em condições de operacionalidade deverão incluir um kit de ferramentas que inclua uma chave de fendas com diversas cabeças, sacos de prova de papel de embrulho, pastas de arquivo, etiquetas de prova, lanterna, tesoura, fita de prova e fita de embrulho, marcador fino e grosso, etiquetas, luvas e abraçadeiras de plástico.

3.3 Execução da operação

É importante frisar aqui que a abordagem que se vai realizar não é uma bordagem policial. Nos casos em que seja detetada uma atividade ilícita de um colaborador, deve tal facto ser comunicado às autoridades judiciárias que procederão em conformidade.

De qualquer maneira, muitos dos princípios por estes aplicados podem ser úteis nas intervenções necessárias realizar no âmbito interno de uma organização ou até numa primeira intervenção de acautelamento de prova digital até que as autoridades procedam à sua apreensão.

Assim sendo, todos os princípios básicos utilizados pelas autoridades na apreensão de prova digital, devem ser levados em conta, estudados e executados aqueles que tenham aplicação numa organização.

No local

A regra número um na abordagem a uma preservação de prova digital é:

Afastar todas as pessoas dos sistemas informáticos a analisar. Não permitir que ninguém (especialmente o funcionário alvo) toque no teclado ou rato. Este aspeto é de capital importância, pois pode evitar que seja introduzida uma sequência de teclas que inicie um processo pré-programado de destruição de conteúdos.

É necessário ter muita atenção aos meios de acesso remoto aos sistemas, tais como dispositivos com capacidade de acesso *wireless*, através da rede corporativa interna ou através de um acesso por VPN.

Encarar a possibilidade de existirem programas destrutivos, com funcionalidades *antiforensic* ou armadilhas físicas no próprio computador. Não seria inédito encontrar uma caixa de um PC eletrificada, razão pela qual a boa prática recomenda que se use sempre as costas da mão para tocar pela primeira vez em objetos metálicos, evitando dessa forma que a contração muscular decorrente de uma descarga elétrica, provoque que se fique "agarrado" ao objeto o que pode ter consequências graves para a integridade física do interveniente. Embora este tipo de cenários seja raro, importa ter a consciência de que tal pode acontecer. Um exame cuidado do sistema e da sua envolvente são cruciais antes de se tocar em qualquer objeto.

Utilizadores mais qualificados tecnicamente poderão utilizar *batch file* destrutivos para apagar ou destruir ficheiros, recorrendo por exemplo à realização de um *wipe* ao disco, evitando dessa forma que o seu conteúdo possa ser recuperado pelos programas forenses disponíveis

Caso se detete que um destes programas está a ser executado, deve ser retirada a energia elétrica do sistema o mais rapidamente possível.

Exemplos:

- As Armadilhas & bombas (o termo mais usual que se encontra na literatura é a denominação anglo-saxónica "Traps & Bombs), embora não sejam muito comuns, não são inéditas.
- "teclas bomba"(o termo mais usual que se encontra na literatura é a denominação anglo-saxónica "hot key bomb") são uma sequencia de teclas que quando introduzida, inicia um ou mais comandos.
- Uma armadilha (o termo mais usual que se encontra na literatura é a denominação anglo-saxónica "Booby Trap") é um programa que aparenta ter uma determinada funcionalidade, mas na realidade tem outra funcionalidade, que pode ser destrutiva.
- Um "TSR" é um programa que fica residente em memória à espera que algo aconteça, seja um time-out ou uma sequência de teclas digitadas.

Protocolos

Se o computador estiver ligado, deve-se fotografar o que está no ecrã, para registar o que estava a ser efetuado no momento em que foi abordado.

Se o computador aparenta estar em "*sleep mode*", deve-se mover o rato ou digitar a tecla "SHIFT" para "acordar" o sistema. Nunca deve ser carregada a tecla "*enter*".

Nesta altura deve ser ponderada a utilização de uma ferramenta que registe o que está na memória do computador, caso se entenda que nesta poderão existir dados que importa registar e que caso se desligue o computador se perderão irremediavelmente.

Nesta situação poderão estar documentos abertos ainda não gravados, locais do disco ou discos cifrados que estejam nesse momento "abertos" ou ligações remotas ativas.

Existem várias ferramentas que permitem fazê-lo, tais como o FTK® *Imager* da *AccessData*®.

Após esta ponderação e a tomada de decisão, deve-se desligar o cabo de energia do sistema a partir do aparelho e não da tomada da parede, da extensão elétrica ou da UPS.

No entanto há exceções, tais como:

- Sistemas informáticos de empresas
- Sistemas em rede
- *Boxes* Unix
- Computadores Macintosh

Nestes cenários, desligar a energia pode provocar grandes danos no sistema ou danificar irremediavelmente os seus dados. Pode interromper a atividade legítima da empresa o que pode acarretar graves prejuízos com possíveis responsabilidades a serem imputadas aos seus autores.

Por outro lado, a remoção do sistema de determinado equipamento, pode suspender unidades de negócio o que tem sempre de ser levado em conta em função dos objetivos a atingir.

Nestas situações pode ser ponderado um *shutdown* controlado do sistema ou recorrer-se à cópia selectiva de dados.

Outro aspecto que deve ser levado em conta é a de permitir ou não a cópia selectiva de determinada informação do computador, antes de este ser desligado e recolhido.

Depois de um computador ou um suporte de armazenamento ser recolhido e preservado para análise forense, podem passar vários meses ou anos até que este possa voltar a ser utilizado.

Tal pode dever-se ao facto de ser normal os departamentos de análise forense terem muitos equipamentos para analisar, a este ter de ser entregue às autoridades judiciárias nos casos em que está em causa um processo-crime ou ainda a estes terem de ser preservados tal como foram recolhidos mesmo após a sua análise forense, até que o processo cível, crime ou disciplinar com os quais estão relacionados esteja concluído, uma vez que pode sempre vir a ser solicitada uma contra análise forense, tal como prevê o CPP no art.º 158º.

Por esta razão pode ser importante permitir que o alvo identifique que ficheiros pessoais ou profissionais devem ser copiados pelo técnico (nunca pelo alvo), de forma a aliviar a "pressão" que pode vir a ser exercida sobre o objecto apreendido para que este seja analisado apressadamente ou que no limite venha a ser determinada judicialmente a devolução dos objectos ao alvo, ainda que não analisados, caso venha a ser entendido que o prejuízo decorrente da privação do acesso a determinados documentos é superior ao valor da prova que se pretende acautelar.

Neste caso deve constar de forma detalhada no relatório da operação, que ficheiros foram identificados pelo alvo como importantes e porquê, quais foram copiados e caso o alvo refira que nada de importante há a copiar, tal também deve ser registado e assinado pelo alvo.

Etiquetar e embalar

Corresponde àquilo a que normalmente se identifica pela denominação anglo-saxónica "Bag & Tag" e envolve as seguintes tarefas:

- Desabilitar ou desligar todas as ligações externas (modem interno, cabo, DSL, etc.); este passo tem de ser feito para assegurar que nenhuma comunicação é efetuada entre o equipamento a recolher e o mundo externo. O sistema pode ainda ser acedido através de uma qualquer ligação enquanto tiver energia. Igualmente, devem ser registados todos os números de telefone ligados ao sistema, que podem ser diferentes nas ligações de voz e dados.
- Registar e marcar as localizações de todos os cabos.
- Registar a marca, modelo e número de série do sistema.
- Recolher igualmente todo o software, manuais, notas e outros documentos manuscritos encontrados no local. Pode vir a ser necessário que no exame forense, se venha a necessitar de instalar *software* desconhecido de forma a replicar o sistema tal como o alvo o tinha. Por esta razão é fundamental recolher também o *software* e os respetivos manuais.
- Optar sempre por recolher também o monitor, teclado e outros periféricos. Tomando esta opção pode obviar-se deixar para trás um qualquer dispositivo de armazenamento cujo aspeto exterior dissimula o seu conteúdo e que pode vir a mostrar-se imprescindível na recreação do cenário que estava instalado.
- Dar muita atenção a pequenos dispositivos de armazenamento, tais como Discos externos, PDAs, PENs e media de armazenamento genérica e proprietária, como é o caso das máquinas fotográficas.
- Caso se recolha suportes de armazenamento como CDs, disquetes ou tapes, deve-se acautelar que o dispositivo que permite a leitura deste suporte, também seja recolhido.
- Recolher e etiquetar todo o *hardware* e periféricos que estavam ligados ao computador, etiquetando todas e cada uma das ligações. Embora seja possível voltar a ligar todo o cenário sem as referidas etiquetas, é importante sobe o ponto de vista da prova, poder-se afirmar inequivocamente que tudo foi testado e analisado conforme estava instalado quando foi acautelado. Sugere-se inclusivamente a realização de uma reportagem fotográfica do cenário. Imagine-se ter de reconstruir o cenário da figura 3.3.1 abaixo sem ter etiquetado os cabos e sem uma reportagem fotográfica:

Fig. 3.3.1 – Ligações de cabos

- Há que ter especial atenção com a marcação de suportes de armazenamento tais como disquetes, discos opticos ou PENs. Usar sempre caneta de feltro para escrever em alternativa a esferográficas, uma vez que estas por ser necessário exercer força para escrever, podem danificar os suportes.
- Quando se embalam dispositivos eletrónicos, deve-se protege-los das normais fontes de possível ameaça de danos. Como precaução deve ser usado material de enchimento e de proteção dentro das caixas quando se armazenam os monitores, discos, computadores e outros periféricos. Um disco danificado não vai permitir recolher qualquer tipo de prova. A prova digital deve ser tratada como sendo muito frágil.
- Os sistemas também devem ser protegidos de fontes eletromagnéticas tais como rádios, ímanes de colunas de som e dispositivos de telecomunicações tais como telemóveis e rádios de transmissão. Quando armazenados, devem ser guardados em salas com pouca humidade e sem a influência de campos eletromagnéticos, calor, frio e qualquer tipo de bichos.
- Não utilizar sacos de plástico (tais como os de zip-lock), para embalar e ou armazenar dispositivos eletrónicos. Usar sempre sacos de papel, caixotes de cartão, sacos anti estáticos ou outro qualquer especificamente destinado ao armazenamento de dispositivos eletrónicos.

Palavras-chave

O termo mais usual que se encontra na literatura e também utilizada na linguagem corrente é a denominação anglo-saxónica “Password”. Especial atenção deve ser dada a todas as palavra-chave utilizadas pelo alvo, uma vez que estas podem ser de capital importância na posterior análise da prova recolhida, para aceder a sistemas, a discos ou a ficheiros cifrados. Se o alvo não fornecer estas chaves de acesso, pode haver outro tipo de elementos e suportes junto aos pertences do alvo, que as podem ter anotadas ou conter informação que as permita apurar.

Ter também em linha de conta que é na fase da primeira abordagem ao suspeito, que a probabilidade de este fornecer livremente as suas palavras-chave é maior. Este ainda está sob o efeito surpresa, ainda não teve tempo de racionalizar o que lhe está a acontecer e ainda não foi aconselhado numa estratégia de defesa que invariavelmente determina o seu silêncio.

Atendendo a que ainda não foi constituído arguido nos termos do art.º 58º do CPP, não se aplicam os direitos e deveres estipulados no art.º 61º, pelo que todas as informações fornecidas pelo alvo deverão

constar do relatório da operação. Não é demais referir que este poderá remeter-se ao silêncio, sem que daí resulte qualquer consequência do foro criminal ou disciplinar.

Ter o cuidado de perguntar não apenas "pela" palavra-chave. Deve ser-se mais minucioso, perguntando pela chave do acesso à BIOS do sistema, pela chave de utilizador e administrativa. Pode haver diversas palavras-chave para diversas contas de correio, ficheiros cifrados e para o acesso ao sistema operativo. O tempo gasto nesta recolha de informação não é verdadeiramente gasto, mas sim ganho em dores de cabeça e muitas horas de trabalho para aceder posteriormente à prova.

Chama-se à atenção que o arrombamento de locais onde o alvo guarda objectos pessoais, tais como gavetas, armários ou cacifos, e ainda que instalados na empresa, pode ter consequências penais para quem o executa ou ordena, sem que exista um mandado judicial que o autorize.

Para construir dicionários que vão auxiliar na descoberta das palavras-chave por *brute force*, pode ser crucial a recolha de todo o tipo de informação sobre o alvo, os seus interesses, os temas e as palavras por estes normalmente utilizados, os nomes dos seus animais de estimação, familiares ou datas de nascimento de filhos.

As palavras-chave são muitas vezes "escondidas à vista" ou guardadas em locais de fácil acesso, tais como um post-it debaixo do teclado, no monitor ou na parte de baixo da gaveta da secretária. Podem estar escritas na margem do manual do próprio equipamento. Podem estar manuscritas algures na proximidade do computador. Palavras ou sequências de caracteres anotadas isoladamente ou no meio de muitas outras notas pode indiciar tratarem-se de palavras-chave.

Pense-se na imensidade de sistemas a que hoje em dia acedemos, que torna quase impossível ter uma palavra-chave diferente para cada um dos sistemas sem que tomemos nota delas nalgum lugar. Especial atenção deve ser dada aos PDAs, smartphones e outros dispositivos eletrónicos pessoais, que têm grande probabilidade de armazenar todas as palavras-chave de que necessitamos.

A entrevista ao alvo

Algumas dicas podem ser muito importantes, na recolha de informação numa primeira conversa com o alvo e embora saia um pouco fora do âmbito da presente dissertação, a sua inobservância pode inviabilizar ou tornar muito mais difícil a posterior análise dos conteúdos recolhidos:

- Não permitir que o alvo tenha a verdadeira consciência do nível de conhecimentos do técnico que o entrevista – deve-se simular um nível básico de conhecimentos técnicos e "ficar" deslumbrado com o sistema as implementações e os "truques" técnicos do alvo, sobrevalorizando habilmente os seus conhecimentos técnicos. Este posicionamento pode levar o alvo a gabar-se das suas capacidades técnicas mostrando mais do que inicialmente poderia ou levá-lo a avançar intencionalmente com explicações técnicas incorretas, convencido de que está a enganar os seus interlocutores, podendo essas declarações vir a ser utilizadas contra ele numa fase posterior do processo de investigação.
- Deve-se adotar um papel de "irmão mais velho" e de "eu só quero entender…"
- Nunca deixar o alvo junto ao seu computador, mesmo que ele queira mostrar ou demonstrar como algo funciona ou onde estão determinados ficheiros. Caso ele queira demonstrar algo, é positivo que o faça, mas dando instruções ao técnico que interage com o sistema. Neste caso deve ser ponderada a importância do que se vai fazer, porque as instruções que este dá podem vir a destruir prova. Só em casos muito especiais e onde de outra forma não seja possível preservar determinada informação, é que se deve interagir com o sistema.

3.4 Embalar e etiquetar a prova

Deve ser utilizado um formulário básico de inventário logo na altura da recolha dos objetos; esta é uma ferramenta relevante na assistência a quem tem de proceder à recolha da prova e fundamental para aqueles que com menos experiencia tiverem de a realizar.

Todos os objetos soltos devam ser etiquetados, onde deve constar informação detalhada sobre o mesmo. A título de exemplo pode ser utilizada uma adaptação do exemplo da figura 3.4.1:

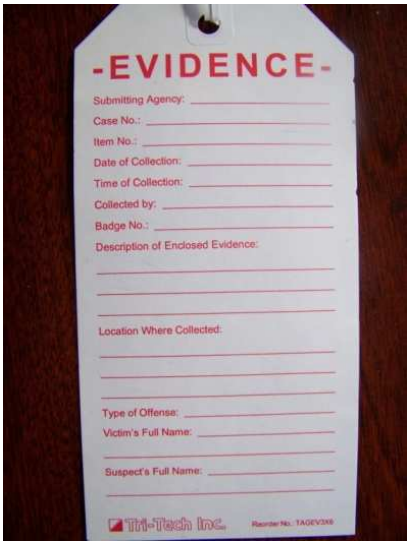


Fig. 3.4.1 - Etiqueta de prova.

Utilizar fita de prova nas aberturas de caixas ou envelopes de discos óticos e outros objetos soltos (fig.3.4.2).

Fig. 3.4.2 - Fita de prova.

A fita de prova tem a característica de não ser possível abri-la sem que esta parta. Desta forma é sempre possível saber se houve alguma tentativa de interagir com a prova. Quem procedeu à colocação da fita de prova deve rubrica-la, para que esta não possa ser substituída por outra idêntica.

Embalar cabos, teclados, ratos e pequenos periféricos todos juntos, bem como pequenos dispositivos de armazenamento, tais como disquetes, discos óticos ou memórias flash.

Devem ser utilizados sempre que possível, as embalagens originais dos equipamentos.

Para suportes de *media* soltos, devem ser utilizados sacos em papel (fig. 3.4.2) ou anti estáticos (fig.3.4.4).

Fig. 3.4.3 - Sacos de prova em papel

Fig. 3.4.4 - Sacos de prova digital anti estático

Caso seja necessário transportar os objetos recolhidos, devem ser acauteladas as ameaças externas extremas tais como calor, frio, rádio frequência, líquidos e campos magnéticos.

O que fazer:

- Fotografias do estado da máquina — panorâmica geral e pormenores.
- Etiquetagem e diagrama das ligações do computador e periféricos.
- Uso de um *checklist* de tarefas a realizar no cenário.
- Uso de sacos de papel de prova ou de sacos antiestáticos para armazenar os suportes digitais.
- Uso de auxilio técnico quando perante vários sistemas interligados ou quando importa decidir o que recolher e não recolher.

O que não fazer:

- Permitir pessoas junto às máquinas.
- Dar uma “vista de olhos” pelos ficheiros do computador.
- Ligar o computador se estiver desligado.
- Permitir que se faça um "*shutdown*" normal do computador (atenção às exceções!).
- Utilizar sacos de plástico para armazenar discos rígidos, zip drives, disquetes e outros suportes de media
- Pretender saber tudo. Pedir ajuda se necessário.

Utilizar formulários estandardizados

Registar os passos da custódia da cadeia da prova com detalhes:

- De onde vem a prova,
- Quando foi recolhida,
- Quem a recolheu,
- Quem a empacotou,
- Quem a armazenou,
- Quem tem acesso e
- Onde está armazenada.

Atenção especial em relação aos portáteis: Quando se recolhe um portátil deve-se começar por lhe retirar a bateria e só depois retirar o cabo de energia. Só assim se tem a garantia de que não há energia no portátil. Deve ser sempre também recolhido o respetivo transformador, uma vez que estes são muitas vezes de especificação proprietária da marca e sem ele pode não ser possível aceder ao portátil para o analisar.

Atenção especial também em relação aos PDA: Quando se armazena um PDA, deve-se ter em atenção que este armazena informação em memória RAM e que se a bateria perder toda a sua energia, os dados nela contida serão perdidos. Alguns PDA mais antigos podem ainda utilizar baterias AA ou AAA, pelo que a sua substituição deve ser considerada.

Sistemas corporativos

Existem situações em que se torna necessário preservar prova digital a partir do sistema informático da empresa, quando se verificam incidentes de segurança em que este se vê envolvido.

São situações em que por motivos óbvios não se procede à apreensão dos equipamentos, mas em que é no entanto necessário preservar de imediato prova digital. Alguns exemplos típicos dessas situações são de seguida apresentados, bem as respetivas medidas a executar.

Situação 1:

Modificação, alteração ou supressão de dados, como a mistificação de páginas de Internet para captura de credenciais e a distribuição de mensagens de correio eletrónico para *phishing*:

- Registo através de captura do ecrã (*printscreen*) que demonstre as alterações efetuadas no sistema;
- Preservação dos ficheiros do sistema operativo introduzidos ou alterados pelo atacante;
- Registo dos dados alterados nas bases de dados;
- Preservação dos logs dos servidores que comprovem o *upload* de ficheiros para a referida página.
- Preservação dos cabeçalhos técnicos das mensagens de email, indicando todos os servidores SMTP por onde estas passaram até à origem.

Situação 2:

Interrupção do funcionamento do sistema informático, suprimindo ou tornando inacessível qualquer componente de software ou hardware, tais como nas situações de ataques de negação de serviço (DDoS):

- Preservação dos logs dos servidores que comprovem o elevado e anormal número de pedidos.

- Registo dos dados de monitorização remotos, tais como capacidade dos sistemas, tráfego de rede, IDS e ou IPS, que comprovem o elevado e número de pedidos. Útil para quando o sistema alvo atinge a sua capacidade máxima e deixa de responder.

Situação 3:

Acesso ou tentativa de acesso intencional e não autorizado à totalidade ou a parte do sistema informático, tal como o furto de informação que pode incluir segredo comercial, industrial ou dados confidenciais protegidos por lei, onde se incluem os pessoais:

- Registo do logs dos servidores que comprovem a intrusão do atacante.
- Registo das atividades (histórico) levadas a cabo por esse atacante no sistema afetado, que podem ser úteis no caso de o sistema ter sido utilizado para a prática de outras atividades maliciosas.
- Registo dos logs dos sistemas ou mecanismos de proteção (firewall, IDS, IPS, Honeypot) que comprovem as repetidas tentativas de intrusão no sistema.

Situação 4:

Ação intencional ou tentativa não autorizada de apagar, danificar, deteriorar, alterar, suprimir ou tornar inacessíveis dados do sistema informático, onde se podem incluir as situações que envolvem malware e a sua distribuição por correio eletrónico:

- No caso de envio de malware por correio eletrónico. Preservação dos cabeçalhos técnicos das mensagens, indicando todos os servidores SMTP por onde estas passaram até à origem e preservação de uma amostra do malware enviado, com relatório técnico de uma análise do mesmo, indicando o nome, tipo e variante de malware em causa.
- No caso de injeção de malware. Preservação de uma amostra do malware utilizado na tentativa de infeção dos sistemas, incluindo igualmente um relatório técnico de uma análise do mesmo, indicando o nome, tipo e variante de malware em causa.
- No caso de ataques internos e ou de abuso confiança. Preservação dos logs dos sistemas que comprovem as atividades ilícitas.

Situação 5:

Ação intencional e não autorizada de reunir informação sobre a infraestrutura, nomeadamente sobre as redes e sistemas informáticos, numa ação normalmente designada por Scan à rede:

- Preservação dos logs dos servidores que comprovem os scans efetuados.
- Preservação dos dados de tráfego dos dispositivos de monitorização remota, tais como firewall, IDS ou IPS, que comprovem os scans efetuados.

Situação 6:

A situação normalmente designada por SPAM, onde se verifica uma recepção ou envio de mensagens de correio eletrónico não solicitadas, quer sejam produzidas para efeitos de marketing direto ou sem motivação aparente e que não inclui a distribuição de malware ou ataques de phishing

- Preservação dos cabeçalhos técnicos das mensagens de email, indicando todos os servidores SMTP por onde estas passaram até à origem.

Telemóveis & PDA's

No caso destes dispositivos, há que levar em linha de contas as suas especificidades próprias.

A primeira dessas especificidades determina também a primeira regra e que é se o telefone estiver desligado, não se deve ligá-lo. Se este estiver ligado, não se deve desligá-lo.

Quando se recolhe e preserva dispositivos tais como PDA's e telemóveis, é fundamental recolher também os respetivos cabos, transformadores adaptadores e/ou carregadores.

- Se a bateria fica sem energia, perdem-se dados. Nunca se deve remover a bateria de um telemóvel.
- Ligar o dispositivo a uma fonte de energia logo que possível.
- O dispositivo deve ser isolado de todas as redes de comunicação o mais rapidamente possível e se possível recorrer a uma caixa de Faraday (ver capitulo dedicado a este assunto)
- Procurar o pacote de ligações do operador do respetivo serviço, que pode conter informação relevante.
- Recolher os PIN e PUK dos dispositivos.

O kit forense especifico para estes dispositivos deve incluir:

- Cabos, cabos e cabos
- Carregador de baterias universal
- Adaptadores de Bluetooth
- …e provavelmente sacos ou caixas de Faraday ou um dispositivo portátil de extração e análise de dispositivos móveis como o UFED da Cellebrite.

Vestígios lofoscópicos

Um aspeto normalmente descurado nos ambientes fora da esfera de atuação das autoridades é a dos vestígios lofoscópicos, normalmente designados por impressões digitais.

Não se deve esquecer o grande potencial que este tipo de prova tem e que pode ser vital em alguns casos. Constitui muitas vezes a estratégia de defesa de quem é acusado de algum crime, afirmar que determinado suporte onde foram encontradas provas, não é do suspeito, que este nunca tinha visto tal dispositivo ou que nunca o tinha utilizado ou manuseado. Impressões digitais em disquetes, discos óticos, memória flash, discos externos ou outros podem ser nestes casos fundamentais.

É importante também realçar que alguns métodos de recolha de vestígios lofoscópicos são destrutivos de suportes digitais, tais como no caso da utilização de pós de alumínio.

Por esta razão e nos casos em que seja relevante a recolha deste tipo de vestígios, o dispositivos deve ser manuseado de forma a não os destruir até que seja feita a imagem forense das memórias e só depois devem ser os mesmos recolhidos.

E outros tipos de prova

Deve-se ter atenção que em algumas circunstâncias, o examinador pode ser confrontado com equipamento apreendido que esteja contaminado com bactérias ou vírus de doenças contagiosas, que podem pôr em risco a saúde dos examinadores.

Por maioria de razão e uma vez que quem é responsável pela recolha/apreensão é o primeiro a contactar com os objetos, especiais medidas de proteção devem ser utilizadas.

Para minimizar os riscos de contaminação, equipamento de proteção deve ser usado, tais como luvas, máscaras, batas ou fatos de recolha de prova e proteção de olhos e devem ainda ser incluídos no kit de recolha, materiais de limpeza e gel de desinfeção antibacteriano de mãos.

Estas medidas devem ser sempre ponderadas em função das circunstâncias e com bom senso, colocando no entanto sempre a segurança como primeira preocupação.

Documentação em cenário

Deve-se documentar todo o sistema e toda a sua envolvente incluindo uma reportagem fotográfica. Deve ser registado o estado do computador, se está ligado ou não. O mesmo deve ser feito em relação aos seus periféricos.

Deve-se também documentar todos os dispositivos eletrónicos que não vão ser recolhidos. (pode ser difícil provar que determinada pessoa imprimiu um documento a cores quando a sua impressora era apenas a preto e branco)

Deve ser considerada a implementação de um *checklist* estandardizado na organização, para ser utilizado quando necessário.

Formação

Em muitas organizações existe apenas uma ou até nenhuma pessoa treinada na recolha e preservação da prova digital. Deve ser considerado um programa de formação com a distribuição de guias de consulta rápida, para auxílio posterior. A formação deve ter uma componente prática e uma atualização/treino com uma periodicidade não superior a um ano. Pode ser interna, caso a dimensão da organização justifique a formação do número suficiente de técnicos que a torne viável ou pode optar-se pela formação e certificação externa (ver capítulo dedicado às organizações externas que têm formação e certificações nesta área).

Deve ser levado em conta que deve existir sempre pelo menos uma pessoa habilitada a atuar nesta área, pois embora não sejam competências utilizadas todos os dias numa empresa, quando esta é necessária é imprescindível e pode ter um impacto financeiro muito relevante para a empresa.

3.5 Etapas na recolha de prova digital.

O seguimento dos procedimentos realçados neste capítulo vai ajudar a garantir a correta recolha e preservação da prova digital, de forma a garantir uma entrega da prova digital legal e tecnicamente admissível para análise forense, dando assim início à cadeia da prova.

O cuidado planeamento da operação deve antecipar as necessidades de recursos técnicos e humanos.

A identificação e etiquetagem dos objetos, a sua proteção e correta armazenagem é fundamental na sua futura admissibilidade legal.

Sistematizando, as etapas a executar são:

- Afastar todas as pessoas (especialmente o alvo) dos computadores, periféricos e *datacenters*;
- No caso de existir uma rede *wireless* que permite o acesso remoto aos sistemas, considerar a sua desativação prévia;
- Fotografar o ecrã do computador e considerar se se deve remover a energia de imediato ou não.
- Retirar a energia ao sistema.
- Desligar ou desconectar todas as ligações externas de dados, sejam o *modem*, o router ou o cabo de rede.
- Desligar todos os periféricos, incluindo a impressora.
- Remover disquetes, discos óticos e PENs, tratando-as como prova, etiquetando-as e tapando as respetivas entradas com fita de prova.
- Entrevistar de imediato o alvo em relação ao seu sistema, configurações particulares e palavras-chave de acesso.
- Elaborar uma reportagem fotográfica de todas as ligações do computador, incluindo vista panorâmica de todo o cenário.
- Fazer croquis e etiquetar todas as ligações do computador de forma a permitir a sua futura ligação de acordo com o seu estado inicial.
- Procurar na documentação próxima do sistema, toda a informação escrita relevante para a situação em concreto, sem esquecer palavras-chave utilizadas.
- Recolher também todos os livros, manuais, discos, *software*, hardware e demais informação relacionada com o sistema informático recolhido.
- Embalar e transportar cuidadosamente todo o material recolhido, evitando a proximidade a campos eletromagnéticos.
- Voltar a fotografar o cenário uma vez terminada a operação de forma a documentar como tudo foi deixado, evitando futuras alegações de equipamentos desaparecidos ou danificados.

4 *Hashing* e *Hash sets*

Uma parte essencial da admissibilidade legal em tribunal de uma evidência científica é se essa evidência é válida, idónea e fiável, conforme estipulado nos art.º 124º, 125º e 126º

A validação dos dados está relacionada com a verificação da igualdade entre as cópias forenses e os originais, que devem de ser exatamente iguais.

Para a validação das cópias realizadas, podem ser usados algoritmos de *hashing*.

Também podem ser utilizados na *triagem* de ficheiros no sistema a ser analisado para recolha. Permite excluir ficheiros conhecidos tais como aqueles pertencentes ao sistema operativo e a programas conhecidos, limitando as pesquisas aos restantes ficheiros, conseguindo desta forma efetuar pesquisas de triagem muito mais rápidas.

O objetivo deste capítulo é introduzir o conceito de *hashing*, enumerar os algoritmos mais conhecidos, as suas utilizações forenses, as coleções de resumos digitais e as principais ferramentas de *hashing*.

4.1 O *Hashing* na recolha de prova

Na computação forense o *hashing* é um método de representação de uma coleção de dados através de um número único, que resulta da aplicação de um algoritmo matemático a esses mesmos dados. É simplesmente uma representação matemática de dimensão fixa, de um conjunto variável de dados, sejam eles um sector de um disco, um conjunto individual de bytes, um texto, um ficheiro, um grupo de ficheiros, uma partição ou um disco inteiro.

Dois ficheiros com exatamente a mesma sequência de bits, devem produzir o mesmo código *hash* quando se utiliza o mesmo algoritmo.

Normalmente é utilizada a analogia com as impressões digitais humanas, onde cada pessoa tem uma combinação única de cristas e sulcos que lhe dão uma impressão digital que a identifica inequivocamente.

O *hashing* é uma excelente forma de verificar a integridade de um conjunto de dados e foi por isso adotada pela informática forense para diversos fins.

O valor produzido pelo algoritmo resulta de uma fórmula de sentido único, ou seja, a partir do resumo digital não é possível reverter o processo para chegar aos dados de início.

Esta característica também é muito importante porque permite a partilha de valores de *hash* com terceiros, sem que haja a necessidade de trocar os ficheiros propriamente ditos, o que pode ser muito relevante quando se trata de conteúdos ilícitos que não podem ser partilhados.

Permite por exemplo a uma empresa ter um *hash set* (ver capítulo específico sobre *Hash Sets*) de ficheiros reconhecidos pelas autoridades como tendo conteúdos de abusos sexuais de crianças, sem ter a necessidade de ter os ficheiros propriamente ditos, o que seria lamentável e ilegal, mas permite por exemplo, ter um controlo de conteúdo de um *fileserver*.

Por outro lado também permite controlar conteúdos de um fileserver, emailserver ou outra qualquer forma de armazenamento de informação numa empresa, sem que se viole a privacidade dos colaboradores.

4.2 Algoritmos de *Hashing*

De uma forma geral existem três tipos de algoritmos que podem ser encontrados no campo da informática forense: CRC, MD5 e SHA. O objetivo de qualquer um deles é o mesmo – certificar com grande grau de confiança que os dados em causa não possuem erros e que estes correspondem de facto a uma cópia exata do original.

Cyclic Redundancy Check (CRC)

Existe em variantes de 16 ou 32 bit. Foi desenvolvido para garantir integridade de dados e ainda é utilizado com esse mesmo fim. Um exemplo da sua aplicação é na verificação de sectores, garantindo que determinado sector de dados está íntegro, executando um CRC nos dados presentes nesse sector. Também são usados na verificação de integridade nas transmissões de dados. Como ferramenta de validação está ultrapassada e é considerada bastante fraca. O CRC na informática forense, e de uma forma geral, já não é utilizado para verificação de ficheiros.

Uma área onde ainda é utilizado na informática forense é na verificação da esterilização de suportes digitais utilizando 00h (todo a zeros). Utilizando um CRC num suporte supostamente esterilizado depois de um wipe, deve-se obter um resultado de "0".

Um exemplo da utilização do cálculo de um *hash* CRC 32-bit num simples ficheiro, pode ser visto nas figuras 4.2.1 e 4.2.2, onde se utilize o programa WinHex.

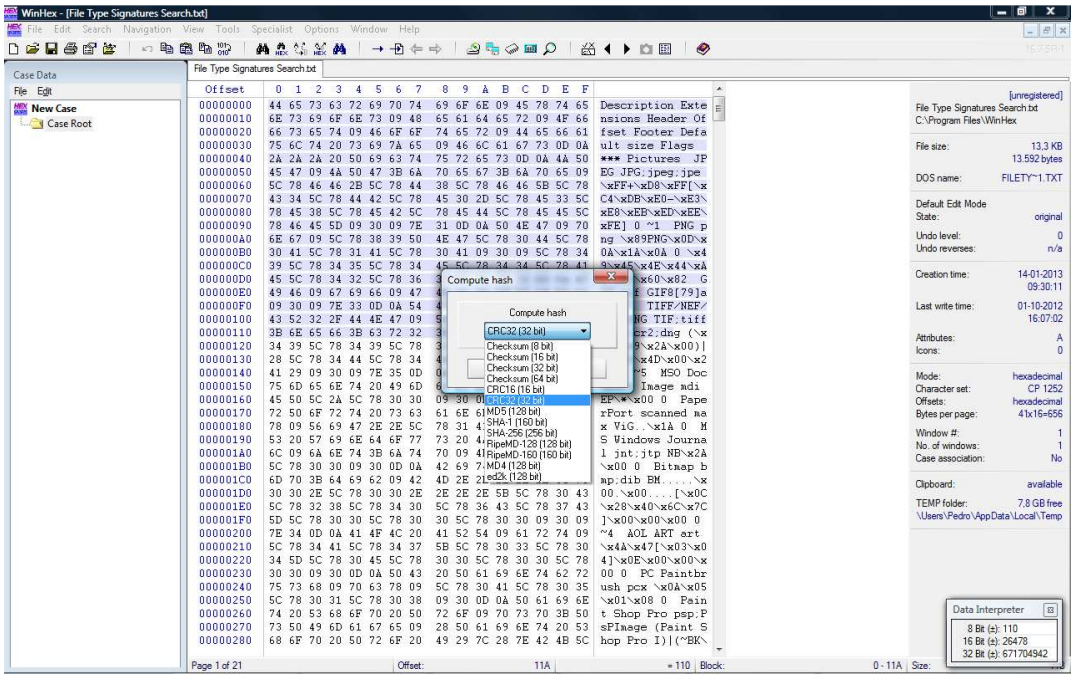


Fig. 4.2.1 – Várias hipóteses de algoritmos disponíveis

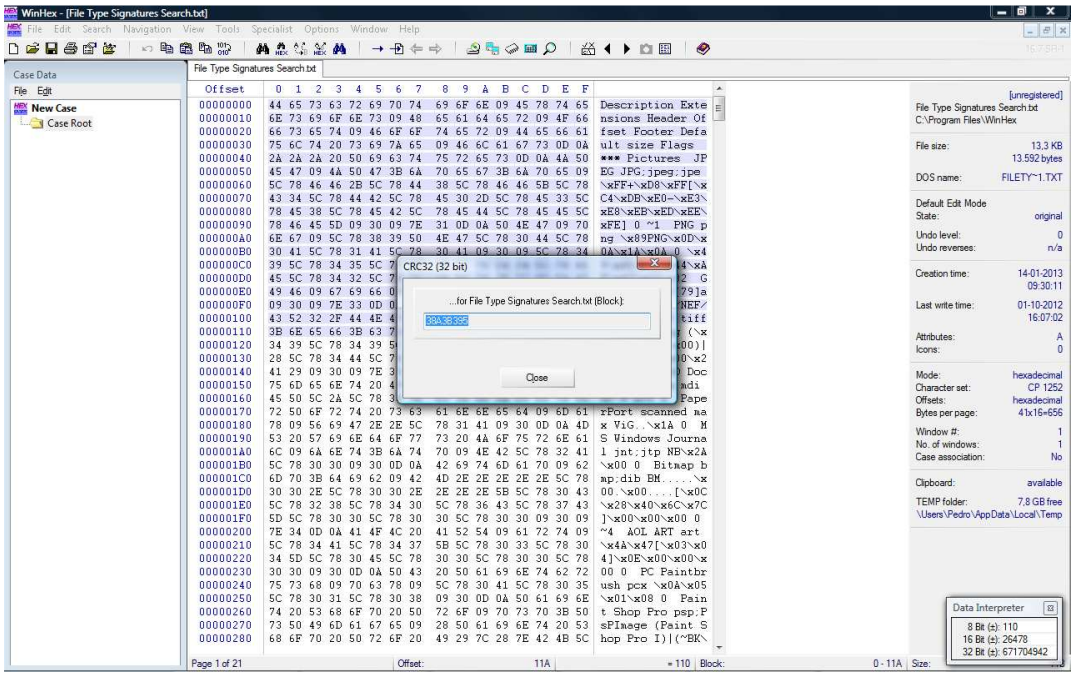


Fig. 4.2.2 – Resultado da aplicação de um CRC-32

Message Digest 5 (MD5)

É um algoritmo para calcular uma representação condensada de uma mensagem ou de um ficheiro de dados. Esta representação condensada é de dimensão fixa e é conhecida por "*Message Digest*" ou "*hash value*". É utilizado há bastante tempo com popularidade na informática forense, foi desenvolvido pelo Professor Ronald L. Rivest em 1994[22] e é um resumo digital de 128-bit (16 byte) que é relativamente rápido e simples de implementar.

Considerando o seguinte exemplo:

Na figura 4.2.3 mostra-se o resultado da aplicação do algoritmo MD5 a um ficheiro de texto que contem "abc" e onde se obteve a palavra:

900150983CD24FB0D6963F7D28E17F72

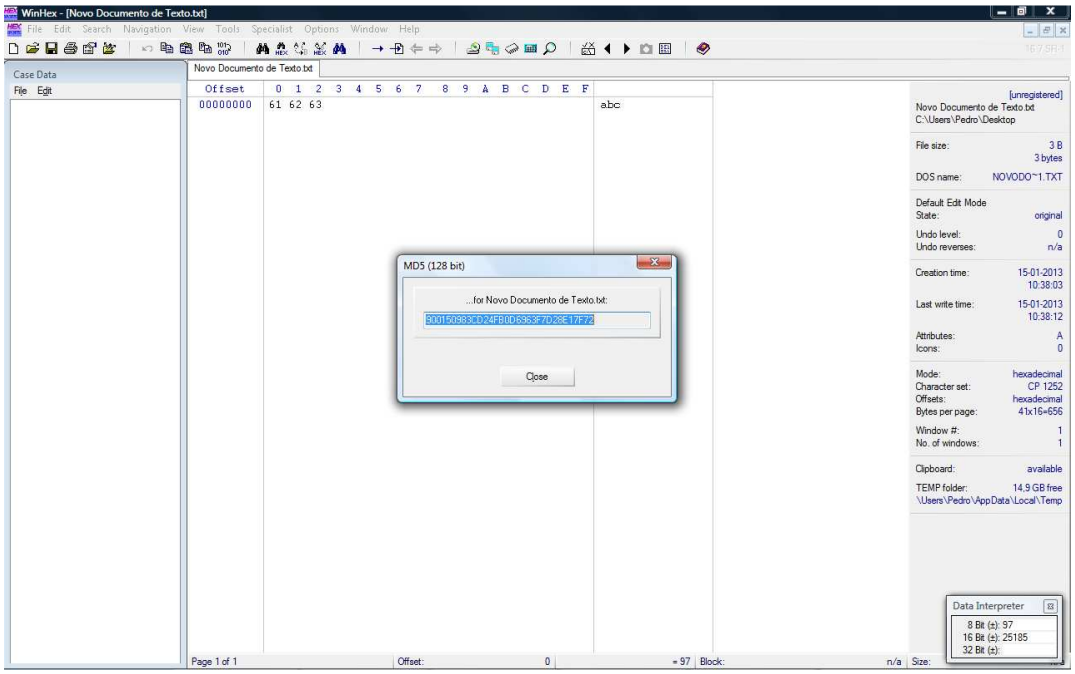


Fig. 4.2.3 – Resultado da aplicação de um MD5 a "abc"

Se o mesmo ficheiro contiver "abd", obtém-se uma palavra totalmente diferente da anterior:

4911E516E5AA21D327512E0C8B197616:

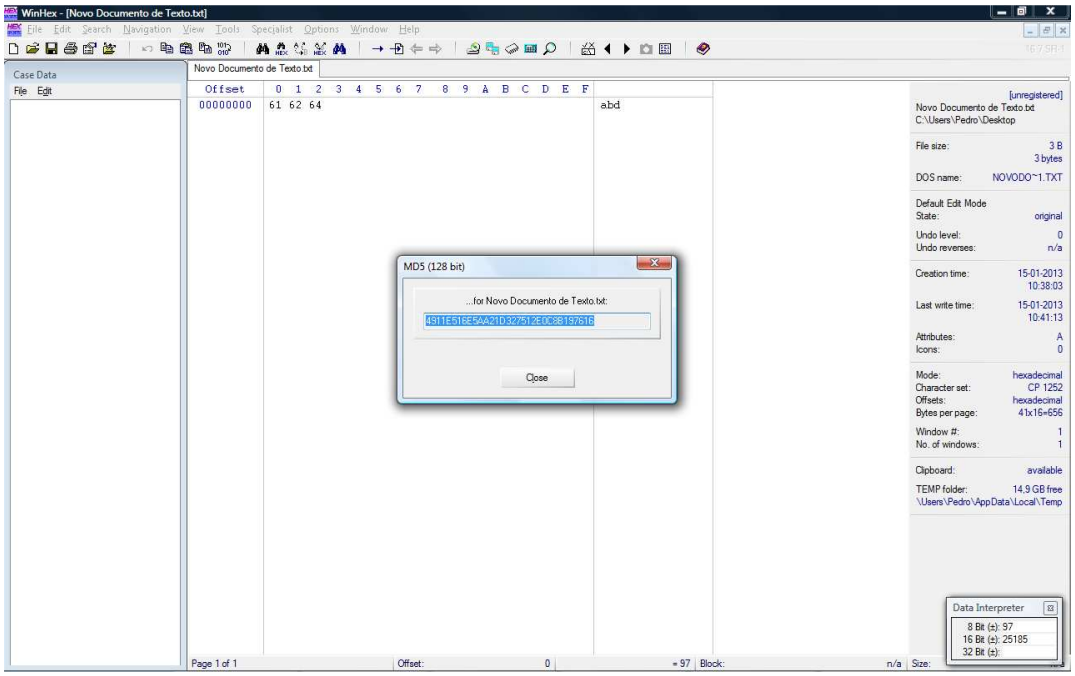


Fig. 4.2.4 – Resultado da aplicação de um MD5 a "abd"

Da mesma forma, se calculássemos o código de outro ficheiro ou de um disco inteiro, obteríamos um *hash* diferente, mas sempre composto por 128 bits.

A probabilidade de duas mensagens terem o mesmo resumo é de aproximadamente $1/2^{64}$, enquanto a probabilidade de encontrar uma mensagem com um determinado código é da ordem dos $1/2^{128}$.

É inviável mas não impossível, que duas mensagens tenham o mesmo *hash*, já que:

$$2^{128} = 3.4028 \times 10^{38} \text{ ou } 340\ 282\ 366\ 920\ 938\ 463\ 463\ 374\ 607\ 431\ 768\ 211\ 456.$$

Se um disco de um computador apreendido tiver 340 282 366 920 938 463 463 374 607 431 768 211 456 ficheiros, é certo que haverá um problema com a aplicação do algoritmo!

Secure Hash Algorithm (SHA)

Embora mais recente é um algoritmo de representação condensada de uma mensagem ou de um ficheiro de dados. A representação condensada é de tamanho fixo e também é conhecido por valor *hash* ou resumo digital. É um resumo de 160 bit e tem ganho preponderância na informática forense. Foi desenvolvido pelo NIST (*National Institute of Standards and Technology*) e é detalhado na Secure *Hash* Standard (SHS, FIPS 180). O SHA-1 é uma primeira revisão publicada em 1994. Florent Chabaud e Antoine Joux encontraram em 1998 uma colisão diferencial na SHA[23]. Não se conhecem até ao momento ataques criptográficos com sucesso ao algoritmo SHA-1, embora tenha sido demonstrado teoricamente que tal é possível (ver tabela 4.2.1). O SHA-1 produz uma palavra de 20 bytes ao contrário da mais pequena de 16 bytes produzida pelo algoritmo MD5.

Depois de terem sido identificadas algumas fragilidades do SHA-1, a NIST impos em 2010 a utilização do SHA-2 em agencias federais norte americanas.

Embora não tenha até ao momento sido reportada nenhuma fragilidade no SHA-2, uma vez que ele é algoritmicamente similar ao SHA-1, a NIST introduziu um novo algoritmo em 2013, o Keccak, que denominou de SHA-3.

Na tabela 4.2.1 pode observar-se alguns termos de comparação entre os algoritmos mais usados.

Algoritmo e variante		Tamanho do resumo (bits)	Tamanho interno (bits)	Bloco (bits)	Tamanho máximo da mensagem (bits)	Colisões identificadas	Exemplo de performance (MiB/s)[24]
MD5		128	128	512	$2^{64} - 1$	Sim	255
SHA-0		160	160	512	$2^{64} - 1$	Sim	-
SHA-1		160	160	512	$2^{64} - 1$	Ataque teórico $(2^{51})^{25}$	153
SHA-2	*SHA-224*	224	256	512	$2^{64} - 1$	Não	111
	SHA-256	256					
	SHA-384	384	512	1024	$2^{128} - 1$	Não	99
	SHA-512	512					
	SHA-512/224	224					
	SHA-512/256	256					
SHA-3		224/256/384/512	1600 (5x5 array de 64 bit words)			Não	

Tab.4.2.1 – Quadro comparativo de características de algoritmos de *Hash*

Embora seja mais lento que o MD5, o facto de apresentar um tamanho maior, torna o SHA mais forte do ponto de vista de vulnerabilidade a ataques em relação ao MD5.

Por exemplo, ao aplicar o SHA-1 ao mesmo ficheiro de texto com a palavra “abc”, obtem-se a palavra:

A9993E36 4706816A BA3E2571 7850C26C 9CDOD89D

4.3 A utilização forense do *Hashing*

À medida que os dispositivos de armazenamento vão aumentando de capacidade, sendo comum encontrar atualmente discos de computadores pessoais com 1 TB ou 2 TB, aumenta na mesma proporção a possibilidade de se encontrar uma quantidade inimaginável de ficheiros nesses discos. Se houver a necessidade de efetuar uma triagem num sistema deste tipo, pode passar-se horas a fio a examiná-los, chegando-se à conclusão que nada existia de relevante. Este facto também decorre do grande número de ficheiros que os sistemas operativos atuais possuem, aliado ao também grande número de ficheiros utilizados por muitas aplicações normalmente instaladas nos sistemas.

O recurso ao *hashing* é uma forma de mitigar este problema, porque elimina a necessidade de pesquisar todos os ficheiros conhecidos, ou seja todos aqueles que pertencem ao sistema operativo ou aos programas já conhecidos. Por outro lado permite procurar um determinado ficheiro através do seu *hash*.

Resumindo, o *hashing* (ou a análise de códigos *hash*) pode ser uma ferramenta muito útil e eficaz na poupança de tempo a quem tem de efetuar uma triagem num sistema informático:

As principais vantagens podem ser resumidas da seguinte forma:

1. Verificação. Utilizado na certificação de que determinado objeto (ficheiro, disco ou suporte digital) não foi alterado. Também pode certificar a esterilização dos dados contidos no suporte, tal como já referido.
2. Exclusão de ficheiros. A análise por *hash* pode ser utilizada para "eliminar" de uma pesquisa todos os ficheiros "conhecidos". Podem-se ter arquivados os "*hash set*" dos sistemas operativos e dos programas comercias mais usados, reduzindo de forma automática o tempo de pesquisa num sistema, uma vez que esta só vai analisar os restantes. Este método é conhecido na comunidade forense como "*Negative Hashing*".
3. Identificação de ficheiros. Pode ser criada uma lista de valores *hash* de determinados ficheiros, usando-a para os procurar e encontrar num sistema. Este método é conhecido na comunidade forense como "*Positive Hashing*".
4. Autenticação de clone. O *hash* de um determinado suporte pode ser comparado com o da cópia forense que foi efetuada, certificando assim a sua integridade.

4.4 *Hash Sets* ou coleções de *hash*

"*Hash Sets*" são listas de valores *hash*. Tipicamente correspondem ou a ficheiros que se pretende eliminar da pesquisa a efetuar ou a ficheiros que se pretendem encontrar. É por exemplo comum entre as autoridades de vários países, a partilha de listas de códigos *hash* com ficheiros reconhecidos, tais como contendo filmes ou fotografias que retratam abusos sexuais de crianças ou de *Malware* identificado. Desta forma evita-se a partilha dos ficheiros propriamente ditos e facilita-se as pesquisas deste tipo de conteúdos.

Normalmente, os programas de informática forense possuem ferramentas de utilização de listas de *hash* de diversas proveniências.

Embora possa haver alguma discrepância entre diversas listas de códigos *hash*, existem valores que são únicos, pelo que merece a pena importar e analisar algumas listas conhecidas. Duas dessas listas são:

1. *Hash*keeper — é uma lista de valores de *hash* MD5 de ficheiros conhecidos, que podem ser utilizados para eliminação nas pesquisas ou para identificação de outros. O programa foi desenvolvido por Brian Deering do "National Drug Intelligence Center" dos EUA e é disponibilizado de forma gratuita a autoridades judiciárias de todo o mundo. Pode também ser solicitado por particulares que terão de se registar no serviço e assinar um termo de responsabilidade. Recentemente o "National Drug Intelligence Center" foi encerrado, tendo as suas funções sido assumidas pela Departamento de Justiça[26].
2. NIST NSRL — O "National Institute of Standards and Technology" mantem uma listagem de códigos denominada "National Software Reference Library" (NSRL) que contém atualmente 28,530,178 códigos SHA-1, MD5 e CRC32.[27]

4.5 Problemas com o *Hashing*

Com o algoritmo MD5 que produz códigos de 128 bit, considerou-se durante muito tempo que era computacionalmente improvável encontrar uma colisão, ou seja, duas entradas que produzissem a mesma saída (o mesmo código *hash*), fenómeno a que se chamou colisão. Em Agosto de 2004 na conferência Crypto2004, os investigadores chineses Xiaoyun Wang e Hongbo Yu anunciaram ter descoberto um método para quebrar diversos algoritmos entre os quais o MD5[28]. De acordo com o *paper* publicado, foram produzidos dois ficheiros diferentes que depois de aplicado o MD5 foram obtidos dois resumos *hash* iguais. Utilizando dois ficheiros de 1024 bit que diferem em apenas 6 bit, foram capazes de produzir o mesmo *hash* utilizando os algoritmos MD4, MD5, HAVAL-128 e RIPEMD. Esta teoria é vulgarmente designada por "birthday attack" e deve ser assinalado que não foi demonstrada nenhuma colisão entre ficheiros conhecidos de sistemas operativos ou de programas, mas apenas de ficheiros “fabricados” propositadamente para provocarem colisões nos algoritmos conhecidos. As boas práticas recomendam a utilização simultânea de MD5, SHA-1 ou SHA-2, obtendo assim uma garantia acrescida. A NIST recomenda atualmente a utilização do SHA-2 ou SHA-3.

Todos os valores *hash* têm o potencial de sofrer colisões, especialmente se o número da amostra de objetos a serem codificados for suficientemente grande para exceder o número de valores possíveis desse tipo de codificação. Ou seja, existe sempre uma probabilidade de dois ficheiros diferentes produzirem o mesmo código *hash*, mas essa probabilidade é extremamente pequena. Por exemplo, usando o MD5 para gerar valores *hash*, existem 128 posições que podem ter dois valores possíveis, o que resulta em 3.4028×10^{38} valores possíveis. Para se ter uma probabilidade de 50 % de se ter dois códigos iguais no mesmo sistema, este teria de ter 1.8×10^{18} ficheiros, o que é manifestamente muito improvável.

Por vezes a utilização de códigos *hash* durante uma operação introduz vários desafios. O primeiro a considerar é o do tempo, uma vez que por exemplo o cálculo do *hash* de uma drive de 200 GB pode levar cerca de meia hora. O outro a considerar é o facto da aplicação do algoritmo sobre o mesmo objeto, seja ele um ficheiro, uma partição ou um disco, poder dar resultados diferentes. Existem circunstâncias em que o *hash* resultante é diferente ainda que não tenha existido nenhuma alteração do objeto. Essas circunstancias podem resultar de:

1. Erros de *hardware*. Estão reportados exemplos de falhas em chips de memória provocarem resultados diferentes no cálculo do *hash*. Erros de leitura dos suportes, por exemplo resultantes de sectores com erro, também podem resultar em resultados diferentes de *hash*.
2. Erro do utilizador. Inicialmente pode ter sido calculado o *hash* sobre todo o dispositivo e depois o cálculo ter sido feito ao nível das partições. Outro erro comum é o cálculo sobre *drives* físicas de tamanhos diferentes. Por exemplo, algumas aplicações veem o último setor de uma *drive* enquanto outras não. O utilizador deve ter especial cuidado ao iniciar o cálculo, assegurando que o número de sectores lido é o correto, para que se tenha um valor *hash* correto.
3. Questões de *software*. Há programas de *hash*ing que “acrescentam” informação ao fim dos ficheiros. Alguns programas que criam imagens de suportes clonados também acrescentam informação aos ficheiros o que resulta em valores diferentes de *hash* entre estes e os sues suportes. Ao serem utilizadas diferentes aplicações para calcular os códigos *hash* podem-se também obter valores diferentes, que resultam de diferentes implementações do algoritmo.

Por todas estas razões é recomendável no processo de certificação da prova que se pretende recolher, utilizar simultaneamente vários algoritmos, não limitar a escolha a um só e é aconselhável indicar no relatório, qual foi o programa utilizado no cálculo

4.6 Programas que utilizam funções de *Hash*

Existem inúmeros programas que utilizam funções *hash*. SPADA, "Karen's Power Tools", Jacksum, Cyo*hash* e muitos outros que permitem utilizações online.

O SPADA (System Preview And Data Acquisition)

Foi desenvolvido por Peter Kingsley e Darren Freestone, era um Linux Boot CD com base KNOPPIX que incorporava várias ferramentas forenses entre as quais o CHECK-SUM CALCULATOR que permite utilizar MD5 e SHA1. Esta ferramenta foi já descontinuada e era destinada a ser distribuída gratuitamente a forças de segurança espalhadas pelo mundo. Pode ainda ser utilizada embora já não haja suporte para a mesma[29].

Karen's Power Tools

São um conjunto de ferramentas freeware para uso não comercial, sendo necessária uma licença paga para utilização empresarial. Permite calcular *hash* MD5, SHA-1,SHA-224, SHA-256, SHA-384 e SHA-512 de texto, ficheiros e grupos de ficheiros[30].

Jacksum

É uma plataforma independente de ferramentas de checksum desenvolvida em Java, para cálculo e verificação de CRC e *hash*es, que suporta 58 tipos diferentes de algoritmos[31].

Cyo*hash*

É uma ferramenta grátis que é utilizada como add-in do Internet Explorer. Permite o cálculo de MD5, SHA1, CRC32, SHA256, SHA384 ou SHA512 através de um simples *click* sobre o ficheiro que abre uma janela com todas as possibilidades de codificação[32].

*Hash*r

É uma ferramenta semelhante ao Cyo*hash*, mas para Firefox e que permite a utilização de mais de 40 tipos diferentes de algoritmos. [33]

FileFormat.lnfo é uma ferramenta online que permite a utilização de 14 tipos diferentes de codificação[34]

5 Validação da prova e sanitização de suportes

A validação e esterilização dos suportes digitais é uma componente crucial de qualquer exame forense de prova digital. Para que um perito forense possa assegurar a idoneidade da prova recolhida, é necessário começar por garantir a correta utilização dos programas e equipamentos envolvidos nessa mesma recolha. Os métodos utilizados pelos envolvidos podem por vezes ser demorados e fastidiosos mas no entanto fundamentais. Da mesma forma, a preparação dos dispositivos de suporte a ser utilizados é também fundamental, passando obrigatoriamente pela utilização de ferramentas e processos que garantam a não contaminação da prova. A não conformidade com as melhores práticas que garantam a integridade da prova pode comprometer irremediavelmente a idoneidade da mesma bem como a dos técnicos envolvidos.

5.1 Validação

Existem dois pilares num exame forense. O examinador e as ferramentas que este usa. Os ataques à integridade da prova vão sempre incidir sobre um deles ou sobre os dois simultaneamente.

Os ataques ao técnico vão invariavelmente incidir sobre os seus conhecimentos técnicos, formação específica na área e métodos que utilizou.

A única forma de mitigar estes ataques é garantir que quem lida com estes processos tem a formação adequada para tal e a documentação adequada e detalhada de todo o processo

O treino e a experiencia dos técnicos deverá ser contínua e o mais abrangente possível, para que este esteja habilitado a interagir com todos os sistemas existentes na organização. Ainda que este não necessite de ser um perito em todos as áreas, o que seria manifestamente impossível, terá de ter um leque de conhecimentos bastante alargado. Colóquios, seminários e acompanhamento das tecnologias mais recentes através de livros técnicos são outras das fontes de conhecimento que deverão estar continuamente ao dispor dos técnicos.

Acima de tudo estes deverão acumular experiencia forense em casos concretos.

Os ataques ao software serão normalmente feitos com dois objetivos. Um deles é a esperança de “apanhar” o examinador numa pergunta que não pode ser por ele respondida, que este não sabe a resposta ou que este mostre grande hesitação na resposta. A segunda é a de capitalizar numa qualquer fragilidade do *software*, ainda que não tenha directamente a ver com as funcionalidades que foram utilizadas no caso concreto. O objetivo é ferir a credibilidade da ferramenta e criar a dúvida em quem tem por missão avaliar a validade probatória dos elementos reunidos. Há que ter sempre em mente o princípio do direito que determina que “in dubio pro reo”, ou seja, em caso de dúvida não se releva a prova incriminatória.

É preciso nunca esquecer que toda a prova pericial pode ser contestada em tribunal e reexaminada por outro perito, conforme prevê o art.º 158 do CPP e que esta deverá obter os mesmos resultados.

As defesas de quem é acusado estão cada vez melhor preparadas e assessoradas tecnicamente, sendo comum serem chamados a depor pela defesa, especialistas de informática e forenses, de forma a por em causa a prova produzida pela defesa.

Levando este aspeto em conta, é preciso não esquecer que o primeiro degrau na cadeia da prova é dado na empresa, quando se recolhe e preserva a prova.

A forma de defesa contra os ataques ao *software* utilizado, é estar o mais familiarizado possível com o seu funcionamento, documentar todos os passos dados e recorrer sempre a programas certificados e reconhecidos como idóneos para os fins utilizados.

5.2 Esterilização dos suportes de Media

A definição de esterilização de suportes magnéticos na comunidade forense, tem a ver com o facto de todos e cada um dos bytes do suporte terem sido reescritos por um valor hexadecimal conhecido ou aleatório, de forma a eliminar toda a informação previamente existente nesse suporte. Este processo é normalmente definido como "wipe", "limpeza" ou "esterilização".

Embora saia do âmbito do presente documento, não é demais recordar que as funções dos sistemas operativos para apagar e formatar os suportes, não efetuam nenhuma reescrita:

- A operação de apagar ficheiros deixa todo o seu conteúdo intacto no suporte.
- Uma normal formatação:
  - Não altera a "partition table". (discos)
  - Cria um "Boot Record" válido no disco ou disquete e uma FAT (para o caso deste sistema de ficheiros);
  - Deixa todos os dados intactos, removendo apenas as suas ligações (links);

Para fins forenses recomenda-se a utilização de uma ferramenta de "wipe" com reescrita por 00h (zeros), uma vez que facilita a verificação da esterilização do suporte, já que o seu checksum deverá ser "0".

5.3 Porquê utilizar suporte esterilizados

Em situações onde dados do suspeito têm de ser copiados para suportes digitais e para que sejam futuramente alvo de exame, é imperioso que nenhum dado exista nesses suportes de destino, sob pena de se misturar dados e contaminar irremediavelmente a prova. O melhor método é utilizar um utilitário que reescreva cada byte do suporte com 00h, ou confirmando que o seu *checksum* é "0" caso seja um suporte que seja fornecido como estando supostamente "limpo".

O seguimento deste procedimento assegura:

- A completa eliminação de todos os dados que eventualmente existam no suporte e
- A confirmação de que o suporte está esterilizado através da obtenção de um *checksum* de "0".

5.4 Quando utilizar suportes digitais esterilizados

- Quando se copiam (*restore*) dados para um suporte digital ou dito de outra forma, sempre que se pretende que em determinado suporte digital sejam colocadas cópias forenses de dados.
- Quando se recebe suportes de terceiros, sejam eles novos ou usados e estes se destinem a receber dados de prova.
- Sempre que se devolve suportes a terceiros, estes devem ser sempre esterilizados e não simplesmente apagados.

É importante salientar que uma simples cópia de ficheiros entre suportes de armazenamento, pode inadvertidamente colocar dados do nosso sistema no suporte de destino. Por exemplo, nas versões Windows 95 e anteriores, os sistemas operativos escreviam dados da memória RAM na zona que fica entre o último byte do ficheiro até ao fim do sector que contém esse byte, naquilo a que se designa como "*RAM slack*". Este espaço pode conter até 512 bytes de dados. Se estiver envolvido um disco

rígido e dependendo da versão de sistema operativo utilizado, pode chegar-se a copiar inadvertidamente todo o "*Recycle Bin*" no suporte de destino. Caso o ficheiro INFO/INFO2 do "*Recycle Bin*" seja um desses ficheiros e através de uma qualquer ferramenta forense, pode recuperar-se o seu conteúdo, acedendo a nomes de ficheiros, datas em que foram apagados e localização original. Este facto pode comprometer toda a prova, caso a prova venha a ser reexaminada por um outro perito e este venha a encontrar a prova "contaminada" com dados do sistema do examinado ou de quem preservou a prova.

Existem opções para lidar com esta realidade e mitigar os riscos que daí advêm.

A primeira é a de estar consciente de que dados do nosso sistema estão presentes na "*RAM slack*" ou "*file slack*" e em espaço não alocado, saber encontrá-lo e o que fazer. Pode verificar-se o que existe nessas áreas e decidir o que fazer.

Pode deixar-se esses dados onde estão ou pode utilizar-se programas que permitem a reescrita dos "file slack" e dos espaços não alocados, tais como:

- O Diskwipe do "Norton Utilities" da Symantec;
- NTI's"m M-Sweep Pro[35];
- BCWIPETM.

5.5 Como criar um suporte esterilizado

Existem diversos programas que permitem a reescrita de cada byte dos suportes digitais. Alguns programas não permitem a escolha do valor do byte a ser utilizado na reescrita enquanto outros sim. Tal como já referido, para efeitos forenses é sempre aconselhável utilizar o 00h. O "SPADA" permite esta última opção, reportando quantos sectores foram reescritos. Se soubermos de antemão quantos sectores tem o suporte que estamos a utilizar, pode facilmente confirmar-se que todos os seus sectores foram reescritos.

5.6 Como lidar com áreas protegidas (Host Protected Areas)

Alguns discos estão equipados com um chip programável, que permite aos programas definirem uma área no disco que é reservada e escondida do próprio sistema operativo. Esta área tem a denominação de "'host protected area" ou HPA. Os sectores que estão assignados ao HPA não estão acessíveis à maior parte dos programas e a maior parte dos utilizadores não têm conhecimento desta área do disco. A controladora do disco apenas reporta para a BIOS a quantidade de sectores que estão disponíveis, excluindo os sectores assignados ao HPA. Existem programas que permitem a criação e a modificação das HPA. Nem todos os programas que executam *Wipe* permitem lidar com o HPA, o que se deve ter sempre em atenção, uma vez que este espaço pode ser utilizado para esconder dados.

5.7 Como confirmar se os suportes estão esterilizados

Existem diversos programas que calculam um CRC (*Cyclic Redundancy Check*), um RSA (iniciáis dos nomes dos seus criadores Ronald L. Rivest, Adi Shamir e Leonard M Adleman), um MD5 (*Message Digest algorithm* versão 5) ou um *checksum* por valor de byte (*byte-value*), que baseia o cálculo na adição dos valores de todos os bytes. (ver capítulo 4)

Muitos programas MD5 e CRC requerem que os suportes sejam reconhecidos pelo sistema operativo. A utilização deste tipo de programas dificulta a verificação da esterilização do suporte, uma vez que o sistema operativo para reconhecer o suporte precisa de lá colocar dados.

Por exemplo, os utilitários do SPADA permitem o cálculo de *byte-value*, que não requer que o suporte seja reconhecido pelo sistema operativo, uma vez que acede ao suporte através da sua própria controladora.

Uma vez que o SPADA não requer um suporte formatado, pode facilmente confirmar-se que este foi reescrito com zeros. Tal como já referido, uma das características relevantes do SPADA é a de identificar o número de sectores que foram lidos. Uma vez que se pode saber antecipadamente o número de sectores desse suporte, facilmente se comprova de todos os sectores foram contemplados.

6 Recolha de informação em fontes abertas

A recolha de informação sobre determinado acontecimento que envolve uma organização ou uma pessoa pode mostrar-se fundamental na futura consubstanciação de prova num processo-crime, cível ou de trabalho.

Este capítulo debruçar-se-á sobre essa recolha de informação nas denominadas fontes abertas que estão disponíveis através da Internet, de forma gratuita e sem restrições de acesso.

Entre estas fontes abertas, podem-se destacar os motores de busca, as redes sociais, sejam elas com ligações do tipo ponto-a-ponto (iRC, MSN, Skype, iChat, LimeWire), de forma diferida (como os *newsgroups, fóruns ou blogs*) ou as que integram diversos serviços (hi5, LinkedIn, FaceBook).

Este capítulo tratará ainda de forma mais detalhada, da recolha de informação sobre a titularidade de páginas na internet, de quem as regista, de quem é responsável pela gestão destes registos e da atribuição de endereços, também abordado no capítulo dedicada ao correio eletrónico.

6.1 Motores de busca

Normalmente os motores de pesquisa permitem o recurso a opções avançadas, para aproximar os resultados obtidos ao tipo de informação pretendida, seja de modo passivo, através de alertas automáticos para atualizações verificadas nos resultados de determinada pesquisa, seja de modo ativo, aquele tido por tradicional.

Não cabe no âmbito do presente documento o estudo sobre como efetuar pesquisas em motores de busca, chamando-se apenas à atenção que estes permitem uma série de otimizações através de comandos avançados, como operadores booleanos ou filtros para tipos de ficheiros e que permitem otimizar as pesquisas.

Outro aspeto para que se chama à atenção e que é por vezes descurado é o facto de ser possível recuar no tempo ou dito de outra forma, saber qual era o conteúdo de determinada página no passado, o que pode ser de capital importância na recolha de prova em muitas circunstâncias, uma vez que estas gravações são feitas automaticamente e fora do controlo de quem publicou os conteúdos em causa.

Para efetuar estas pesquisas existem duas possibilidades.

Uma delas é através do operador “[cache:]” do Google. Contudo, esta memória ou cache do Google é de pouca duração, ou seja, a cache da página vai sendo atualizada, e pode acontecer já não existir o conteúdo da página que se pretende encontrar. Por outro lado, se a página que tinha esse conteúdo for apagada, o Google deixa de a indexar ao fim de algum tempo e a cache correspondente a essa página acaba por desaparecer.

O comando a introduzir na caixa de pesquisa do Google é “[cache:www.pagina_a_procurar.dominio]”.

A outra solução consiste no motor WaybackMachine, um serviço acessível através da ligação “www.archive.org”. (ver figura 6.1.1)

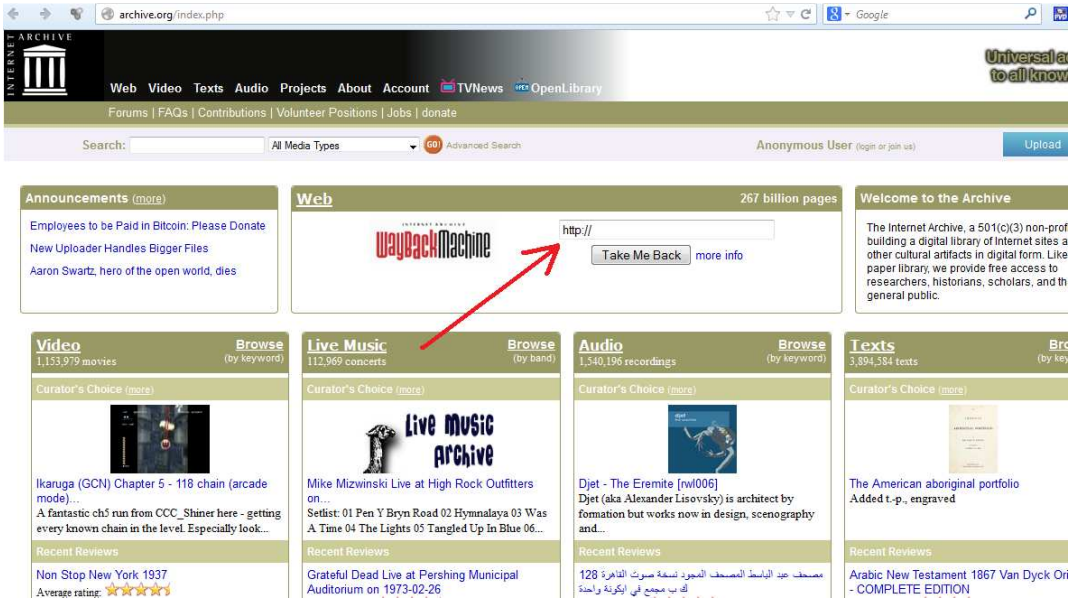


Fig. 6.1.1 - Motor WAYBACK de consulta de versões antigas de páginas Internet

Apresenta-se na figura 6.1.2, o resultado de uma pesquisa efetuada para a página "www.cnn.com", onde se observa uma tabela com gráficos de barras referentes à gravação da página em cada ano, desde o ano 2000.

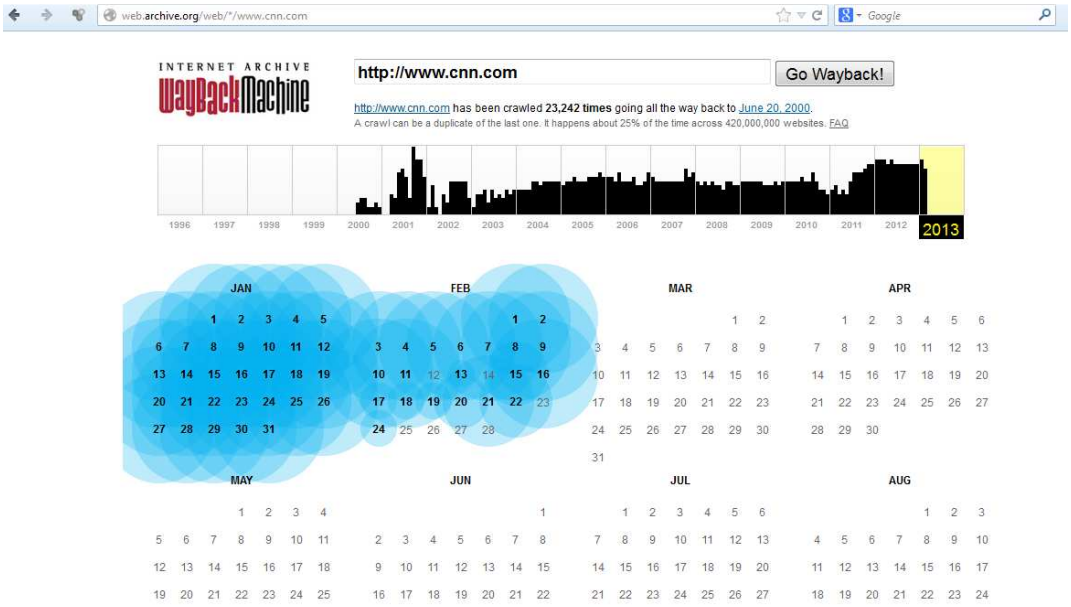


Fig. 6.1.2 - Resultado da pesquisa no WaybackMachine

De notar que nem sempre são efetuadas gravações do estado momentâneo da página, nem há garantia de que este motor consiga sequer gravar uma página, uma vez que as páginas podem ser configuradas para evitar estas gravações.

Por exemplo, no caso concreto e no dia 8 de Janeiro de 2013 foram efetuadas diversas gravações em diversas horas, conforme se pode ver na figura 6.1.3.

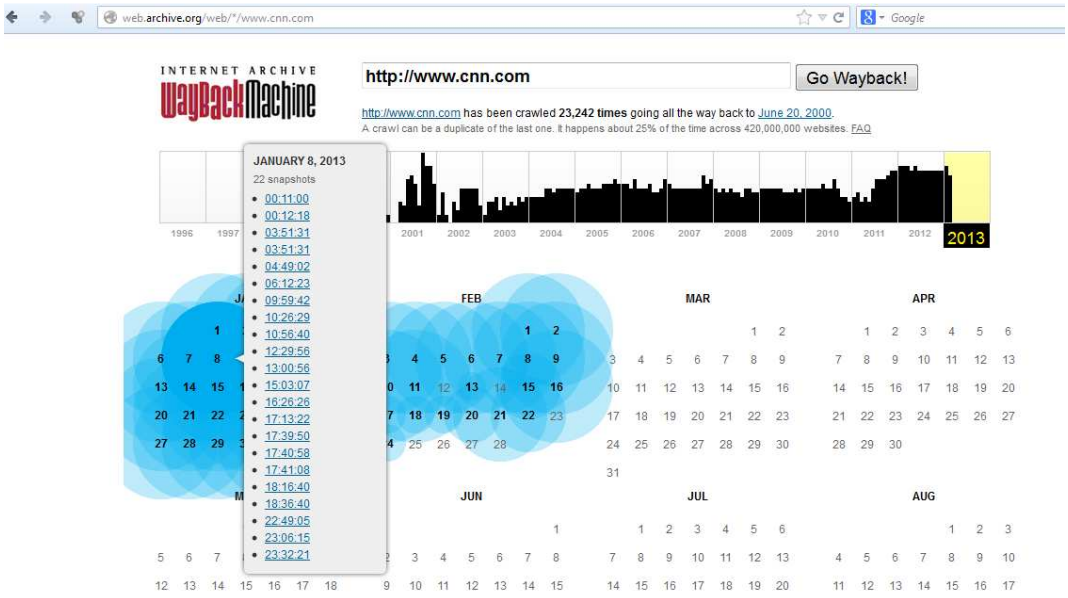


Fig. 6.1.3 - Páginas gravadas

A página gravada às 17:13 tinha o seguinte conteúdo:

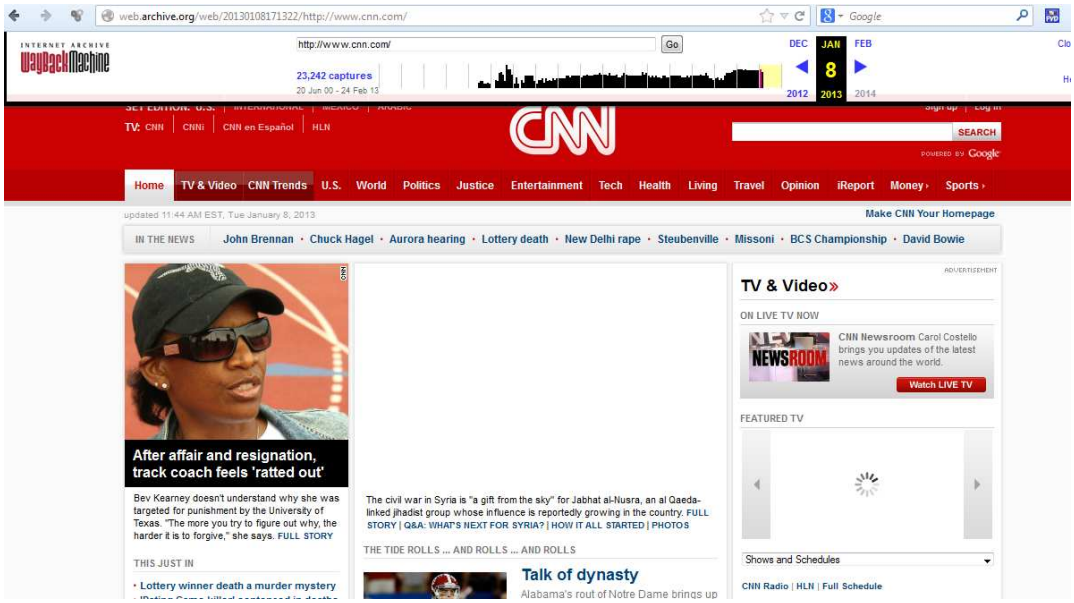


Fig. 6.1.42 - Página www.cnn.com no dia 8 de Janeiro de 2013 às 17:30

Ainda que o conteúdo da página na data em que este documento foi criado, tivesse o seguinte conteúdo:

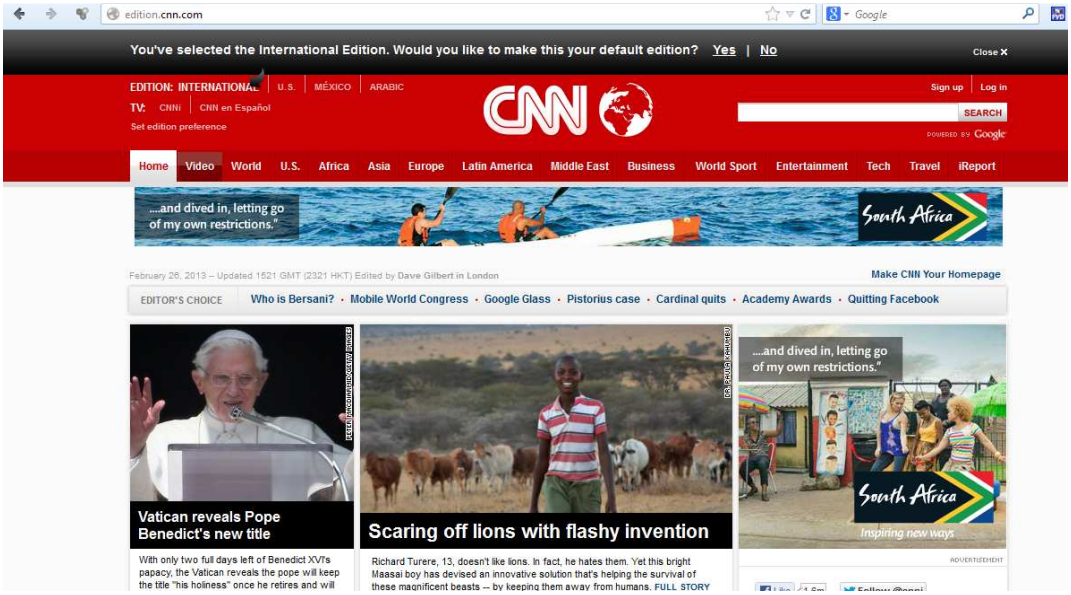


Fig. 6.1.5 - Página da cnn no dia 25 de Fevereiro de 2013.

Outra ferramenta a que também se pode recorrer é a disponibilizada pela Lococitato, que embora em princípio exclusiva para uso por autoridades, pode sempre ser solicitado um registo no endereço "http://www.lococitato.com". Esta ferramenta permite estabelecer um mapeamento entre os vários contactos de determinado perfil nas redes sociais como o *facebook* , o myspace ou o *youtube*.

Outra ferramenta relevante é disponibilizada pela "http://namechk.com/", que permite pesquisar em dezenas de redes sociais se um determinado nome de utilizador existe e aceder a ele de forma direta.

6.2 Domínios Internet e Endereços IP – Identificação

Endereço IP

Depois de identificado um endereço IP, tal como por exemplo no caso da identificação de um remetente de uma mensagem de correio eletrónico, ou da origem de um ataque tal como nos previstos nas situações enumeradas no capítulo 3.4, há que saber o que fazer de seguida para identificar o respetivo titular.

Existem serviços gratuitos na Internet, especificamente dedicados para fornecer a informação disponível sobre os titulares de endereços IP e de páginas Internet, e é a esses recursos que se pode recorrer.

Entre eles estão o "www.centralops.net", o "www.dnsstuff.com" e o "www.domaintools.com".

Estes serviços não são nada mais do que pesquisadores que recorrem às bases de dados dos denominados RIR (Regional Internet Registry), organizações que gerem a alocação e registo dos recursos de endereços da Internet numa particular região do mundo. Existem 5 RIR, responsáveis, tal como já enunciado:

1. RIPE NCC- Réseaux IP Européens Network Coordination Centre: http://ripe.net;
2. ARIN - American Registry for Internet Numbers: http://arin.net;
3. AFRINIC - African Network Information Centre: http://afrinic.net;
4. LACNIC - Latin America and Caribbean Network Information Centre: http://lacnic.net e
5. APNIC - Asia-Pacific Network Information Centre: http://apnic.net.

Alguns conceitos que importa ter presentes neste âmbito, são:

ICANN

Acrónimo de *Internet Corporation for Assigned Names and Numbers* e é uma empresa privada sem fins lucrativos cuja direção é formada por voluntários. Foi fundada em 1988 com o objetivo de coordenar os quatro pontos-chave da Internet e que são a gestão do DNS, a alocação do espaço de endereçamento IP, a atribuição dos parâmetros dos protocolos e a gestão dos sistemas de servidores de raiz.

Para uma empresa ou organização operar como *Registrar*, primeiro tem que obter a acreditação junto do ICANN.

Registry

Um *Registry* é uma empresa ou organização que mantém uma base de dados centralizada dos registos para os domínios de nível de topo ("Top Level Domains" ou TLD's). Correntemente só existe um Registry para cada TLD – ".org.", "com.", ".net", "gov", e "edu". A empresa norte-americana Network Solutions, Inc (NSI) mantém esse registo.

Registrar

Um Registrar é uma empresa ou organização acreditada pelo ICANN que se encontra autorizada a fornecer serviços de registo para domínios de topo (TLD), tais como ".org", ".com", ".net", "gov", "edu". Os Registrar têm acordos contratuais com os seus clientes. Um Registrar submete ao Registry todos os novos domínios registados.

Registrant

O *Registrant* é o proprietário do nome de domínio. O proprietário pode ser um indivíduo, uma empresa ou organização, para quem ou para a qual, um nome específico de domínio é registado. Quando um *Registrant* regista um nome de domínio e assume um contrato com o *Registrar*, torna-se o proprietário legal desse nome de domínio por um certo período de tempo. O *Registrant* fica sujeito aos termos do acordo de prestação de serviço.

Exemplo

Caso se pretenda identificar o titular da página na Internet da "Fundação para a Computação Científica Nacional", cujo endereço é "www.fccn.pt", pode começar-se por consultar um dos três serviços já referidos, o "www.centralops.net", o "www.dnsstuff.com" ou o "www.domaintools.com", que proporcionam resultados complementares embora basicamente idênticos. Alternativamente e conhecendo a localização geográfica do servidor onde a página se encontra alojada, pode recorrer-se directamente ao RIR correspondente, que contêm informação mais completa.

Centralops.net

No caso do "www.centralops.net", temos um dos mais completos serviços, embora limitado a 50 utilizações diárias a partir dum dado endereço IP. Pesquisando a "www.fccn.pt" no "*Domain Dossier*", obtém-se:

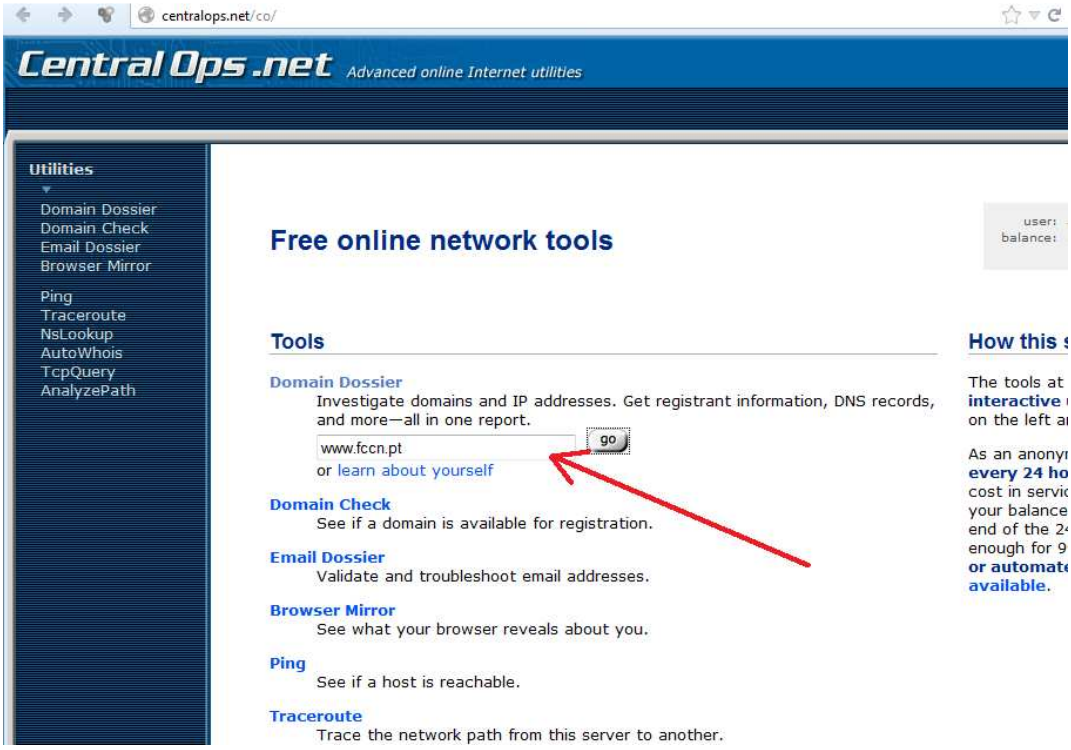


Fig. 6.2.1 - Pesquisa FCCN.PT no Centralops

O *Centralops* devolverá uma página de resultado com o aspeto da representada na figura 6.2.2, onde podemos ver os endereços IP da fccn.pt, tanto na versão IPV6, como na versão IPV4.

Address lookup

canonical name www.fccn.pt.
aliases
addresses 2001:690:a00:1036:1113::247
193.137.196.247

Domain Whois record

Queried whois.dns.pt with "fccn.pt"...

```
Nome de domnio / Domain Name: fccn.pt
Data de registo / Creation Date (dd/mm/yyyy): 08/10/1991
Data de expirao / Expiration Date (dd/mm/yyyy): 31/12/2013
Estado / Status: ACTIVE

Titular / Registrant
   Fundao para a Computao Cientifica Nacional
   Av. do Brasil, no. 101
   Lisboa
   1700-066 Lisboa
   Email: secretaria@fccn.pt

Entidade Gestora / Billing Contact
   Fundao para a Computao Cientifica Nacional
   Email: secretaria@fccn.pt

Responsvel Tcnico / Tech Contact
   Joao Nuno Urbano Ferreira
   Email: tcs-ra@fccn.pt;ferreira@fccn.pt

Nameserver Information
   Nameserver: fccn.pt  NS      ns01.fccn.pt.
   Nameserver: fccn.pt  NS      ns02.fccn.pt.
   Nameserver: fccn.pt  NS      ns03.fccn.pt.
   Nameserver: ns01.fccn.pt.    A       193.136.192.40
   Nameserver: ns02.fccn.pt.    A       193.136.2.228
   Nameserver: ns01.fccn.pt.    AAAA    2001:690:a00:4001::200
   Nameserver: ns02.fccn.pt.    AAAA    2001:690:a80:4001::200
   Nameserver: ns03.fccn.pt.    AAAA    2001:4ca0:106:0:250:56ff:fea9:3fd
   Nameserver: ns03.fccn.pt.    A       138.246.255.249
   Nameserver: fccn.pt DS CE99BC262CE36A9EB9EE0DF81293EF4DBEC8F173 RSA/SHA-1 (NSEC3) SHA-1 62196
   Nameserver: fccn.pt DS EE31B6B82E8FFD665220D4FD5A95D42F887249A76D2C7600F6A244EB 6D9E9E21 RSA/SHA-1 (NSEC3) SHA-256
62196
```

Fig. 6.2.2 - 3Resultado no CENTRALOPS para FCCN.PT

O campo Domain WHOIS fornece os elementos que identificam o titular do domínio FCCN.PT, bem como a data da sua criação, a entidade gestora e o *nameserver*.

De notar que esta informação referente ao titular (*Registrant*) poderá não ser válida, já que as entidades que procedem ao seu registo não verificam os dados fornecidos por quem alugou ou comprou o domínio.

Address lookup

canonical name www.fccn.pt.
aliases
addresses 2001:690:a00:1036:1113::247
193.137.196.247

Network Whois record

Queried whois.ripe.net with "-B 193.137.196.247"...

```
% Information related to '193.137.196.0 - 193.137.196.255'

inetnum:        193.137.196.0 - 193.137.196.255
netname:        DMZ-OPER-FCCN
descr:          DeMilitarised Zone for FCCN Servers
descr:          Housing at FCCN/LNEC and FCCN/ORIENTE
country:        PT
admin-c:        JNF1-RIPE
tech-c:         IF575-RIPE
status:         ASSIGNED PA
mnt-by:         AS1930-MNT
mnt-lower:      AS1930-MNT
changed:        ipadm@fccn.pt 20070903
source:         RIPE

role:           IPADM FCCN
address:        Fundacao para a Computacao Cientifica Nacional (FCCN)
address:        Av. do Brasil, 101
address:        1700-066 Lisboa
address:        Portugal
phone:          +351 218440101
e-mail:         ipadm@fccn.pt
admin-c:        JNF1-RIPE
tech-c:         AMTA2-RIPE
tech-c:         CF6277-RIPE
tech-c:         MD3842-RIPE
tech-c:         EM4720-RIPE
tech-c:         PL3961-RIPE
nic-hdl:        IF575-RIPE
remarks:        IP Address Administration
notify:         ipadm@fccn.pt
mnt-by:         AS1930-MNT
changed:        ipadm@fccn.pt 19991125
changed:        ipadm@fccn.pt 20000217
changed:        ipadm@fccn.pt 20020814
changed:        ipadm@fccn.pt 20090817
changed:        ipadm@fccn.pt 20111211
source:         RIPE

person:         Joao Nuno Ferreira
address:        Fundacao para a Computacao Cientifica Nacional (FCCN)
address:        Avenida do Brasil, 101
address:        P-1799 LISBOA CODEX
```

Fig. 6.2.3 - Identificação do titular da rede onde se encontra a FCCNError! Bookmark not defined.

Também é possível recolher informação sobre o titular da rede, tal como consta na figura 6.2.3, onde consta o "*Network Whois*", que se refere à atribuição física do endereço IP por parte das entidades RIR. Esta informação, ao contrário da anterior, já é devidamente verificada e validada pelo RIR.

A identificação do titular da rede é a mais importante na recolha de informação, pois é a entidade que sabe a quem foi alugado o domínio, ou o endereço IP em investigação.

Há ainda outros elementos na resposta do Centralops que são muito úteis para a recolha de informação sobre o titular de uma determinada página.

A título de exemplo, suponhamos que pretendíamos recolher informação sobre os titulares da página www.netviagens.com, uma vez que ou contrário do caso anterior a rede e o domínio não pertencem à mesma entidade:

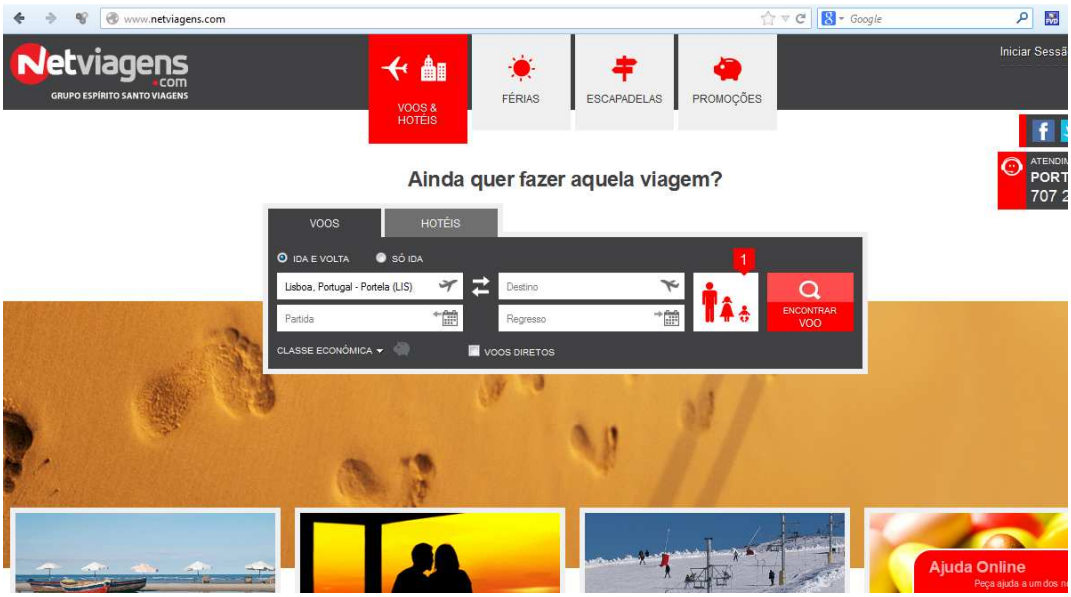


Fig. 6.2.4 - Página www.netviagens.com

A pesquisa sobre o Registrant dá o seguinte resultado:

Address lookup

canonical name **www.netviagens.com.**
aliases
addresses **94.46.4.97**

Domain Whois record

Queried **whois.internic.net** with "**dom netviagens.com**"...

```
Domain Name: NETVIAGENS.COM
Registrar: REGISTER.COM, INC.
Whois Server: whois.register.com
Referral URL: http://www.register.com
Name Server: NS1.XPERTSOFT.COM
Name Server: NS2.XPERTSOFT.COM
Status: clientTransferProhibited
Updated Date: 29-jan-2013
Creation Date: 01-feb-2000
Expiration Date: 01-feb-2014

>>> Last update of whois database: Fri, 01 Mar 2013 18:44:19 UTC <<<
```

Queried **whois.register.com** with "**netviagens.com**"...

```
Registrar Name....: Register.com
Registrar Whois...: whois.register.com
Registrar Homepage: www.register.com

Domain Name: netviagens.com
   Created on..............: 2000-02-01
   Expires on..............: 2014-02-01

Administrative Contact:
   Space Travel SA
   Sa Nogueira
   Av.D.Joao II Edificio ESV, Lote 1.16.1 piso 3
   Lisboa,   1990-083
   PT
   Phone: +1.351214201000
   Email: jose.carvalho@esviagens.com


Technical  Contact:
   Registercom
   Domain Registrar
   12808 Gran Bay Pkwy
   West Jacksonville, FL 32258
   US
   Phone: +1.9027492701
   Email: domainregistrar@register.com
```

Fig. 6.2.5 - Domain Record da www.netviagens.com

Deste resultado verificamos que o Registrant é a empresa *Registercom* sedeada nos EUA, embora conste deste registo a informação eventualmente correta de que o mesmo é administrador pela empresa Space Travel, SA.

Por outro lado o registo sobre o titular da rede onde a página está alojada, fornece a seguinte informação:

Address lookup

canonical name **www.netviagens.com.**
aliases
addresses **94.46.4.97**

Network Whois record

Queried **whois.ripe.net** with "**-B 94.46.4.97**"...

```
% Information related to '94.46.0.0 - 94.46.14.255'

inetnum:        94.46.0.0 - 94.46.14.255
netname:        PT-RACKSPOT
descr:          RACKSPOT.COM
descr:          powered by NFSI Telecom
descr:
descr:          ************************************************************
descr:          * We provide dedicated servers on this Subnet.
descr:          *
descr:          * Those services are self managed by our customers
descr:          * therefore, we are not using this IP space ourselves
descr:          * and it could be assigned to various end customers.
descr:          *
descr:          * In case of issues related with SPAM, DDoS, portscans
descr:          * or others, feel free to contact us with relevant info:
descr:          * abuse@nfsi.pt
descr:          ************************************************************
descr:
country:        PT
admin-c:        NFSI-RIPE
tech-c:         NFSI-RIPE
status:         ASSIGNED PA
notify:         hostmaster@nfsi.pt
mnt-by:         MNT-NFSI
mnt-lower:      MNT-NFSI
mnt-routes:     MNT-NFSI
changed:        hostmaster@nfsi.pt 20090412
source:         RIPE

role:           NFSI Telecom Lda
address:        Apartado 533
address:        2401-975 Leiria
address:        Portugal
phone:          +351 21 1142300
fax-no:         +351 21 1142301
e-mail:         hostmaster@nfsi.pt
abuse-mailbox:  abuse@nfsi.pt
admin-c:        JOAO-RIPE

% Information related to '94.46.0.0/16AS25137'

route:          94.46.0.0/16
descr:          NFSi Telecom, Lda.
origin:         AS25137
notify:         hostmaster@nfsi.pt
mnt-by:         MNT-NFSI
changed:        hostmaster@nfsi.pt 20080603
source:         RIPE
```

Fig. 6.2.6 - Network Record da www.netviagens.com

Deste registo verifica-se que o endereço IP associado à página pertence à gama de endereços IP fisicamente atribuídos e registados pelo RIR RIPE à Rackspot.com da empresa NFSI, o que nos fará supor que Space Travel, SA terá alojado a sua página nos servidores da NFSI, que também faz roteamento.

A última fonte de informação que pode ser utilizada para cruzar informação ou confirmar a já recolhida é a existente no DNS RECORDS.

Address lookup

canonical name www.netviagens.com.
aliases
addresses 94.46.4.97

DNS records

name	class	type	data	time to live
www.netviagens.com	IN	A	94.46.4.97	3600s (01:00:00)
netviagens.com	IN	SOA	server: ns1.xpertsoft.com email: hostmaster@netviagens.com serial: 2005041046 refresh: 3600 retry: 600 expire: 1209600 minimum ttl: 3600	3600s (01:00:00)
netviagens.com	IN	TXT	v=spf1 mx ptr ip4:94.46.2.129 ip4:94.46.4.99 ip4:62.28.15.118 ip4:62.28.15.113 -all	3600s (01:00:00)
netviagens.com	IN	A	94.46.4.97	3600s (01:00:00)
netviagens.com	IN	MX	preference: 5 exchange: mx1.feriaseviagens.com	3600s (01:00:00)
netviagens.com	IN	NS	ns2.xpertsoft.com	3600s (01:00:00)
netviagens.com	IN	NS	ns1.xpertsoft.com	3600s (01:00:00)
97.4.46.94.in-addr.arpa	IN	PTR	www.netviagens.com	7200s (02:00:00)
4.46.94.in-addr.arpa	IN	SOA	server: a.ns.nfsi.pt email: dnsmaster@nfsi.pt serial: 1359678735 refresh: 28800 retry: 7200 expire: 604800 minimum ttl: 3600	86400s (1.00:00:00)
4.46.94.in-addr.arpa	IN	NS	a.ns.nfsi.pt	86400s (1.00:00:00)
4.46.94.in-addr.arpa	IN	NS	b.ns.nfsi.pt	86400s (1.00:00:00)
4.46.94.in-addr.arpa	IN	NS	a.ns.nfsi.pt	86400s (1.00:00:00)
4.46.94.in-addr.arpa	IN	NS	b.ns.nfsi.pt	86400s (1.00:00:00)

Fig. 6.2.7 - DNS RECORDS da netviagens.com

Neste registo, constata-se a existência de campos MX (mailbox exchange), ou seja, os campos que identificam os servidores usados para o correio eletrónico no domínio netviagens.com. Neste caso, as caixas de correio estão localizadas nos servidores mx1.feriaseviagens.com, o que permite apurar, repetindo o processo anterior, quem é o titular de feriaseviagens.com, e questionar esta entidade sobre as caixas de correio e a sua relação com a netviagens.com.

dnsstuff.com

O www.dnsstuff.com é outro dos serviços a que se pode recorrer, em alternativa ao anterior.

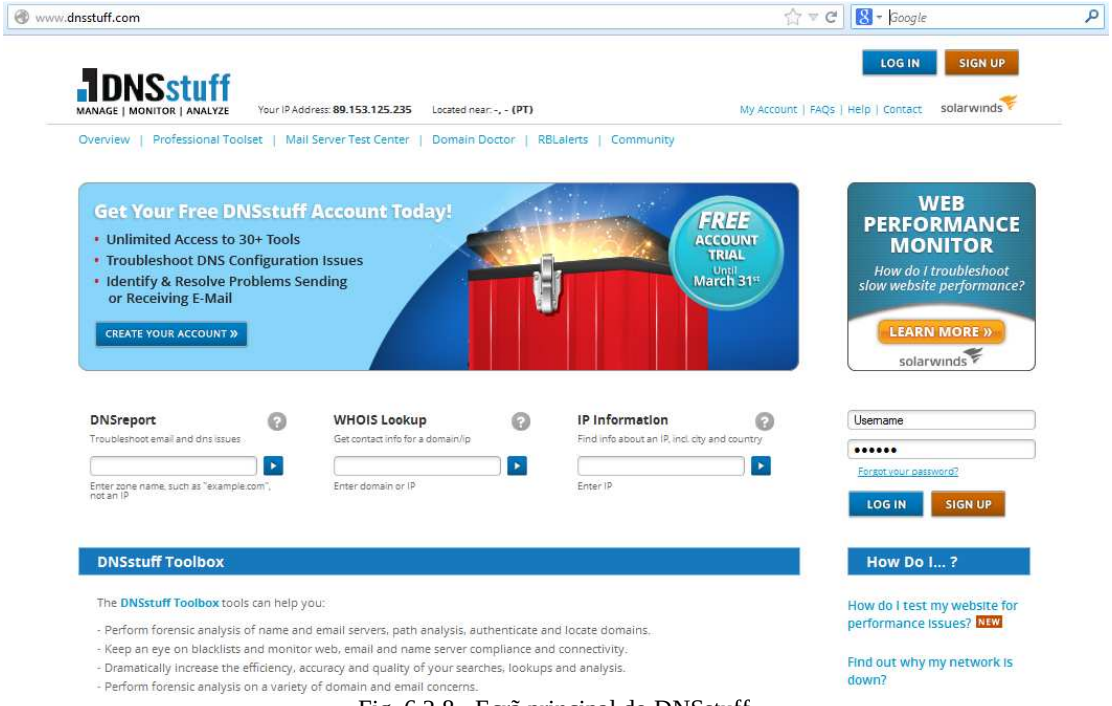


Fig. 6.2.8 - Ecrã principal do DNSstuff

Os resultados do dnssuff são normalmente menos completos do que os do centralops.

domaintools.com:

A página www.domaintools.com possui outro serviço semelhante ao Centralops e ao DNSstuff.

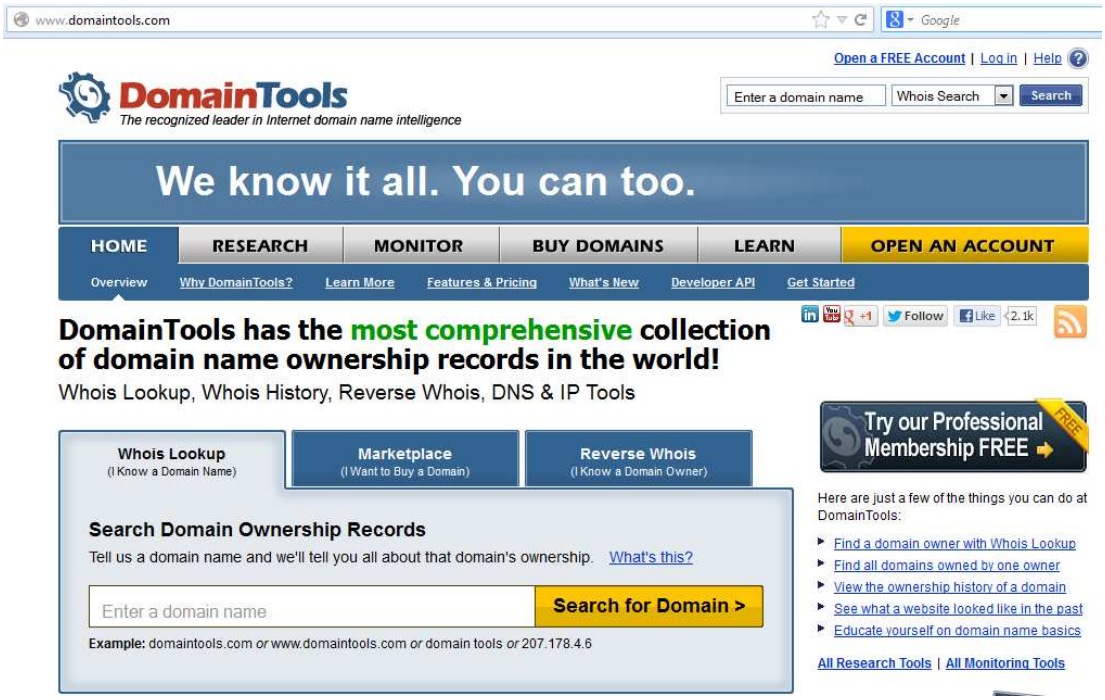
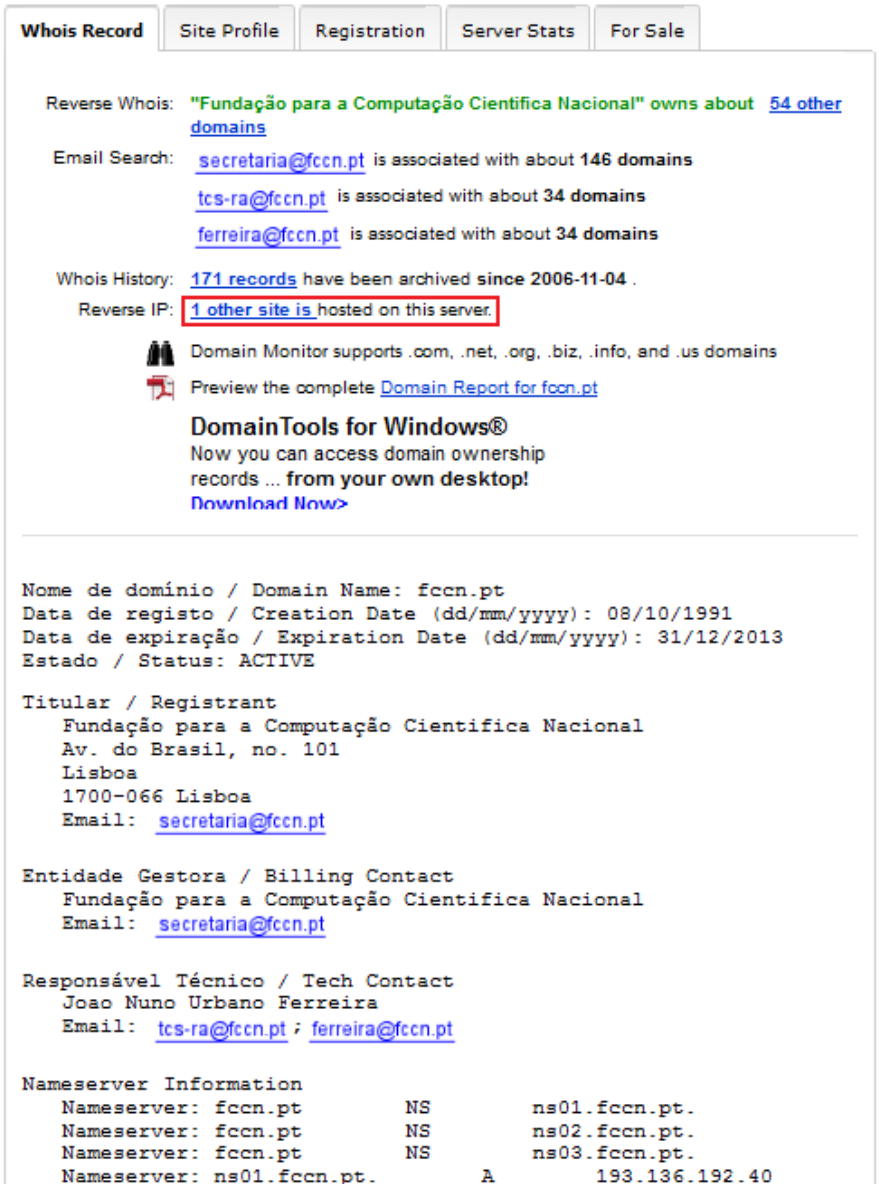


Fig. 6.2.9 - Ecrã principal de Domaintools

A mesma recolha de informação sobre a fccn, permite obter a seguinte informação:



Whois Record | Site Profile | Registration | Server Stats | For Sale

Reverse Whois: "Fundação para a Computação Cientifica Nacional" owns about 54 other domains

Email Search: secretaria@fccn.pt is associated with about 146 domains

tcs-ra@fccn.pt is associated with about 34 domains

ferreira@fccn.pt is associated with about 34 domains

Whois History: 171 records have been archived since 2006-11-04 .

Reverse IP: 1 other site is hosted on this server.

Domain Monitor supports .com, .net, .org, .biz, .info, and .us domains

Preview the complete Domain Report for fccn.pt

DomainTools for Windows®
Now you can access domain ownership records ... from your own desktop!
Download Now>

```
Nome de domínio / Domain Name: fccn.pt
Data de registo / Creation Date (dd/mm/yyyy): 08/10/1991
Data de expiração / Expiration Date (dd/mm/yyyy): 31/12/2013
Estado / Status: ACTIVE

Titular / Registrant
   Fundação para a Computação Cientifica Nacional
   Av. do Brasil, no. 101
   Lisboa
   1700-066 Lisboa
   Email:  secretaria@fccn.pt

Entidade Gestora / Billing Contact
   Fundação para a Computação Cientifica Nacional
   Email:  secretaria@fccn.pt

Responsável Técnico / Tech Contact
   Joao Nuno Urbano Ferreira
   Email:  tcs-ra@fccn.pt ; ferreira@fccn.pt

Nameserver Information
   Nameserver: fccn.pt          NS        ns01.fccn.pt.
   Nameserver: fccn.pt          NS        ns02.fccn.pt.
   Nameserver: fccn.pt          NS        ns03.fccn.pt.
   Nameserver: ns01.fccn.pt.          A         193.136.192.40
```

Fig. 6.2.10 - Resultado do Domaintools para a pesquisa Fccn.pt

Esta pesquisa introduz alguns elementos novos, tais como o facto da página da FCCN se encontrar associada a outros domínios e que outra página se encontra alojada no mesmo servidor.

Esta outra página pode ser consultada através do campo Reverse IP, onde se fica a saber que neste endereço IP também está alojada a página www.fccn.eu.

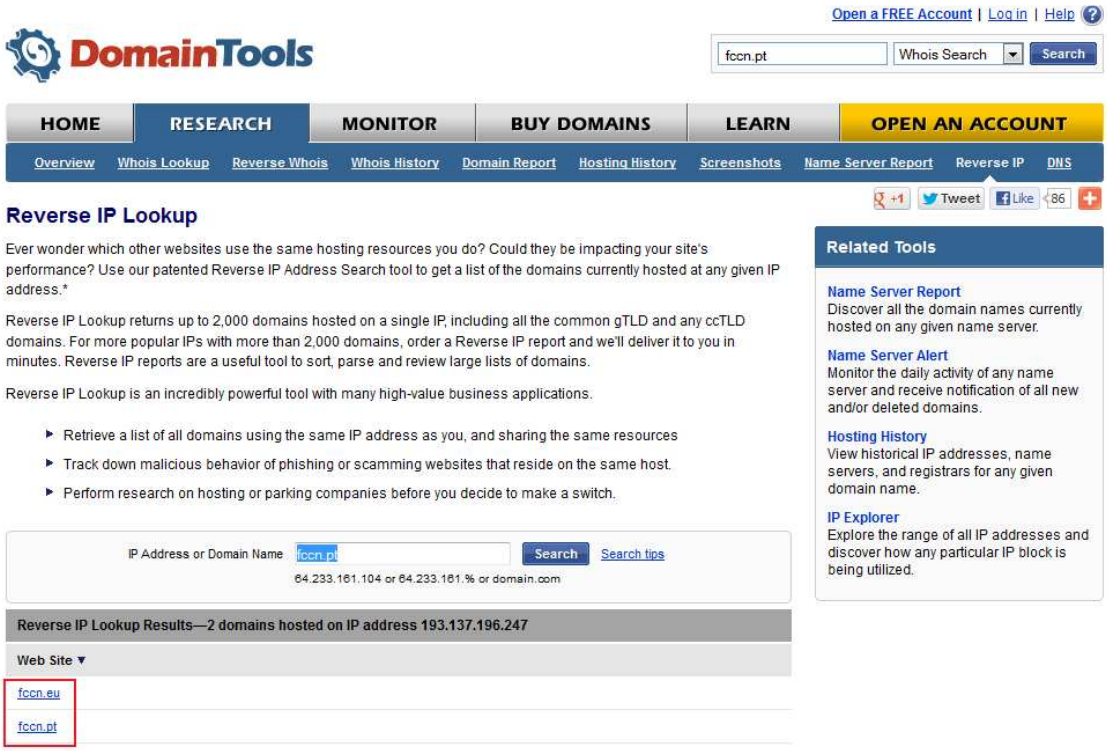


Fig. 6.2.11 - Resultado do reverse IP da pesquisa Fccn.pt

7 Correio eletrónico e cabeçalhos técnicos

Sendo o correio eletrónico uma das funcionalidades mais utilizadas na Internet, quer por particulares quer por empresas, faz com que frequentemente também seja através deste serviço que são praticados diversos ilícitos, como seja spam, difusão de malware, ameaças, difamação ou crimes de corrupção, entre outros.

Nesse sentido, torna-se fundamental saber recolher a informação técnica necessária, para identificar os autores de determinada mensagem e em tempo útil, já que esta é altamente volátil.

Neste capítulo serão abordados os programas de correio eletrónico mais utilizados no mercado e estudada a técnica para deles retirar a informação necessária no sentido de identificar o autor de determinada mensagem.

Não se pretende neste capítulo abordar pormenorizadamente os protocolos e serviços envolvidos, uma vez que sai fora do âmbito desta dissertação. No entanto será feita uma abordagem superficial de cada um deles, apenas para enquadrar o tema.

7.1 Internet Protocol (IP)

A Internet é uma rede global de redes de computadores interconectadas, que usam a pilha de protocolos TCP/IP. Esta rede é constituída por milhões de redes de computadores e outros sistemas, sejam eles privados, públicos, empresariais, governamentais ou universitários, ligados entre si através de tecnologias de rede diversas.

Esta rede disponibiliza vários serviços entre os quais aquele que normalmente é confundido com a própria Internet e que é a *World Wide Web* (WWW), que suporta o correio eletrónico, tratado neste capítulo.

Cada computador que se liga a uma rede necessita de possuir um endereço, sendo a Internet também uma rede, implica que cada computador que a ela se ligue necessite de um endereço.

Em relação ao correio eletrónico, pode estabelecer-se uma analogia entre números de telefone e endereços TCP/IP. Quando se telefona para alguém, antes de mais é necessário saber o seu número de telefone. De forma semelhante, quando um computador ligado à Internet precisa de enviar dados para outro, precisa conhecer o endereço TCP/IP do destinatário.

Se desconhecemos o número de telefone para onde queremos telefonar, recorre-se à lista telefónica para obter o número. De forma semelhante os computadores recorrem a um serviço de diretório, denominado DNS (*Domain Name System*) para traduzir os nomes em endereços TCP/IP. Por exemplo, o nome "http://www.fccn.pt" traduz-se atualmente para o endereço IP 193.137.196.247.

Todos os computadores ligados à Internet têm um endereço TCP/IP associado, que pode ser fixo ou de atribuição dinâmica, o que quer dizer que muda em função do tempo.

O IP (*Internet Protocol*) é um *standard* de endereços, descrito no RFC 791 da Internet Engineering Task Force (IETF).

Embora não seja do âmbito do presente documento, estudar detalhadamente o protocolo, importa no entanto realçar algumas das suas características.

Um datagrama IP contém dois endereços IP: o endereço de origem (do *host* emissor) e o endereço de destino (do *host* recetor).

Para que os pacotes "viagem" do computador de origem até ao seu destino, têm que ser encaminhados. Os routers são ativos de rede que encaminham pacotes da rede de origem para a rede de destino utilizando o protocolo IP. Os pacotes devem incluir identificadores da rede de origem e da de destino. Utilizando o endereço IP da rede de destino, um *router* pode entregar um pacote na rede do destinatário. Quando o pacote chega a um *router* ligado à rede de destino, esse *router* utiliza o endereço IP para localizar o computador específico ligado a essa rede.

Os endereços IP são compostos por duas partes: uma parte identifica a rede à qual o computador está ligado e a outra identifica o dispositivo na rede, que pode ser um computador ou uma impressora, para dar apenas dois exemplos.

7.2 Endereçamento

Inicialmente foi o InterNIC (*Internet Network Information Center*), que definiu a forma de endereçamento, mas atualmente é a *Internet Assigned Numbers Authority* (IANA) a entidade responsável pela coordenação a nível mundial do sistema de endereçamento IP.

Atualmente existem dois tipos de IP. O IP versão 4 (IPv4) e o IP versão 6 (IPv6).

Quer o IPv4 quer o IPv6 são distribuídos de forma hierárquica. Um utilizador comum recebe um endereço IP do seu prestador de serviços de Internet (*Internet service provider* – ISP). Os ISPs obtêm endereços para distribuir aos seus clientes a partir da *Local Internet Registry* (LIR) ou *National Internet Registry* (NIR), ou ainda a partir das *Regional Internet Registry* (RIR), tal como identificado no capítulo anterior.

Quando um cliente recebe um endereço IP público do seu ISP, pode dizer-se que lhe foi atribuído ou alocado dinamicamente um endereço IP. O cliente quando se desliga da Internet, "liberta" o endereço IP que tinha e o ISP pode atribuir aquele mesmo endereço IP ao próximo cliente que se pretenda ligar à Internet. Daqui resulta que um endereço IP sem grupo data/hora e respetivo fuso horário (*timezone*) pode ser irrelevante.

Este tipo de alocação é normalmente utilizado para clientes residenciais.

No caso de uma empresa ou instituição, não seria razoável que o endereço IP do seu servidor Web (por exemplo) fosse de alocação dinâmica, uma vez que seria necessário que os servidores DNS estivessem constantemente a atualizar a informação sobre o endereço IP de determinado endereço, o que tornaria o acesso à página da instituição muito mais lenta. Assim sendo, normalmente as empresas têm um endereço público estático configurado no seu servidor *Web*.

Os endereços IP estão ainda divididos em classes.

Os endereços de classe A são atribuídos a redes de grande dimensão. Os da classe B são usados para redes de dimensão média e os de classe C para redes pequenas. A classe D é de *Multicast* e a classe E é reservada para pesquisas. Os *ranges* de endereçamento para cada uma das classes estão resumidas na Tabela 7.2.1.

A primeira etapa para determinar que parte do endereço identifica a rede e que parte identifica a máquina é identificar a classe do endereço IP. Na Tabela 1 está resumida para as classes A. B e C, a forma de identificação da Rede e do *Host*.

Public IP Address Classes range

Class	1st Octet DEC range	1st Octet BIN	Start address	Finish address	1st Octet High order Bits	Network/ Host	Default Subnet Mask
A	1-126	**0**0000001-01111110	0.0.0.0	126.255.255.255	**0**	**N.H.H.H**	255.0.0.0
B	128-191	**10**000000-10111111	128.0.0.0	191.255.255.255	**10**	**N.N.H.H**	255.255.0.0
C	192-223	**110**00000-11011111	192.0.0.0	223.255.255.255	**110**	**N.N.N.H**	255.255.255.0
D	224-239	**1110**0000-11101111	224.0.0.0	239.255.255.255	**1110**		
E	240-255	**11110**000-11111111	240.0.0.0	254.255.255.255	**11110**		

Note: Class A address **127.0.0.0** - **127.255.255.255** cannot be used and is for **LOOPBACK** and diagnostic

Private IP Address Classes range

Class	1st Octet DEC range	1st Octet BIN	Start address	Finish address	1st Octet High order Bits	Network/ Host	Default Subnet Mask
A	10	**0**0001010	10.0.0.0	10.255.255.255	**0**	**N.H.H.H**	255.0.0.0
B	172	**10**101100	172.16.0.0	172.31.255.255	**10**	**N.N.H.H**	255.255.0.0
C	192	**110**00000	192.168.0.0	192.168.255.255	**110**	**N.N.N.H**	255.255.255.0

Tabela 7.2.1

Com o rápido consumo do espaço de endereçamento do IPv4, que disponibiliza aproximadamente 4.3 biliões (2^{32}) de endereços, a *Internet Engineering Task Force* (IETF) teve necessidade de estudar uma forma de expandir a capacidade de endereçamento na Internet. A solução encontrada, foi redesenhar o protocolo IP, sendo a versão que vai substituir o IPv4 denominada IPv6, que disponibiliza 2^{128} endereços, ou seja 3.4×10^{38} ou 340 triliões de triliões de triliões de endereços únicos.

Para resolver o problema da escassez de endereços IPv4, foram entretanto adotadas medidas para mitigar o problema, sendo uma delas a utilização de endereços privados, tal como descrito na Tabela 7.2.2.

Class	Private IP Addresses (RFC 1918)	Default Subnet Mask	Number of Networks	Hosts per Network	Total Hosts
A	10.0.0.0 to 10.255.255.255	**255.0.0.0**	**1**	**16,777,214**	**16,777,214**
B	172.16.0.0 to 172.31.255.255	**255.255.0.0**	**16**	**65,534**	**1,048,544**
C	192.168.0.0 to 192.168.255.255	**255.255.255.0**	**256**	**254**	**65,024**

Tabela 7.2.2

Como as redes privadas não estão ligadas directamente à Internet, podem utilizar quaisquer endereços de *host*, desde que cada *host* dentro dessa rede privada seja exclusivo.

Ligar uma rede que utiliza endereços privados à Internet exige a conversão dos endereços privados em endereços públicos. Este processo de conversão é denominado de NAT (*Network Address Translation*) e, geralmente, o equipamento que realiza esta operação é um *router*.

7.3 DNS - Domain Name System

É utilizado na Internet para converter os nomes de domínios em endereços IP. É mais fácil para qualquer pessoa recordar um endereço de um sítio na Internet, como seja o www.google.com do que o endereço IP 173.194.69.147, que é o endereço do servidor onde está alojada a página de Internet do motor de pesquisa.

Sempre que se chama um serviço como o http, a sessão só começa quando o nome do servidor a que queremos aceder é traduzido para um endereço IP. O nome só é usado por ser de mais fácil memorização. A tradução de um endereço IP num nome é realizada pelo servidor de DNS. Na realidade, a tarefa poderá ser efetuada por um conjunto de servidores de DNS, pois se o primeiro servidor não conseguir resolver o endereço, vai perguntar a um segundo servidor de DNS e por aí adiante até se obter o IP da máquina que se pretende aceder. Sempre que um servidor de DNS recebe um pedido para um domínio que não se encontra na sua *cache* (memória), reencaminha-o para um servidor que esteja hierarquicamente acima na cadeia, continuando a formular pedidos até que encontra a informação pretendida. O servidor que fez o pedido ao retornar um endereço guarda-o para satisfazer futuros pedidos.

A forma de funcionamento de um servidor DNS, está directamente relacionada com a estrutura de nomes. A organização dos domínios segue uma filosofia idêntica à da organização dos diretórios num disco rígido: no topo da estrutura existe o domínio raiz, que não tem qualquer denominação. A informação do domínio raiz está armazenada num pequeno número de computadores pela Internet. No patamar abaixo da raiz estão os domínios de topo como sendo o ".pt", o ".com" ou o ".edu", que são denominados *top-level domain* (TLD). Estes domínios correspondem a países ou organizações. De seguida encontram-se os domínios de segundo nível como o google.com, o microsoft.com ou o mycorp.com do exemplo da figura 7.3.1. Abaixo destes estão os de terceiro nível, como o mygrp.mycorp.com do exemplo da figura e assim sucessivamente.

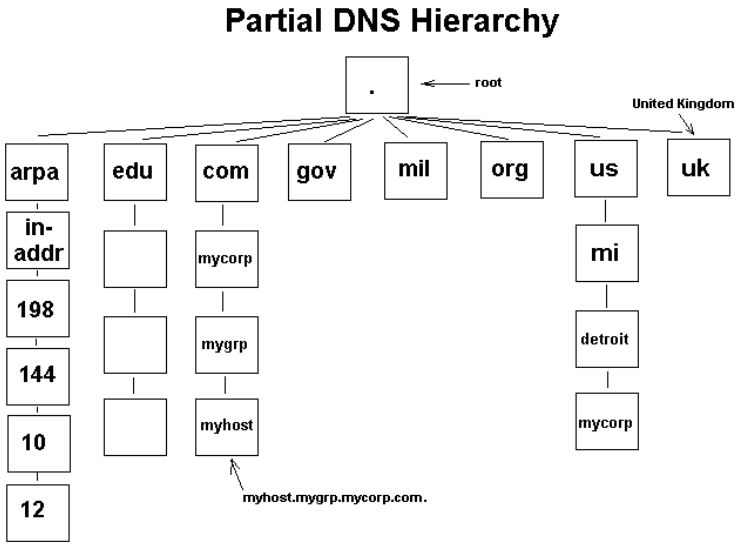


Figura 7.3.1

Em Portugal a Fundação para a Computação Cientifica Nacional (FCCN) é a *Registry* responsável pelo TLD "*.pt*". Uma *Registry* é a entidade responsável por coordenar a designação de domínios de um determinado TLD ou *Country Code Top Level Domain* (ccTLD). Apesar das *Registry* serem as

responsáveis pela manutenção dos domínios abaixo de um TLD, estas não estão autorizadas a vender endereços, sendo este processo feito pelas *Registrar* (agentes de registo de domínios).

7.4 Endereços

O *Uniform Resource Locator* (URL) é um endereço de um recurso, seja ele um ficheiro, uma impressora ou uma máquina e tem a seguinte estrutura:

protocolo://máquina/caminho/recurso

O Uniform Resource Name (URN) funciona como o nome ou entidade e o URL é o endereço para o recurso.

O *Uniform Resource Identifier* (URI) pode ser classificado como um localizador (URL) ou um nome (URN), ou ainda como ambos, conforme Figura 7.4.1.

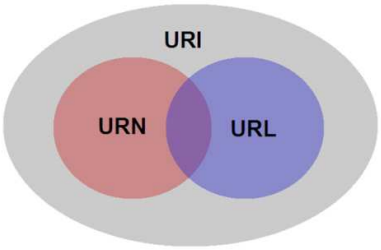


Fig. 7.4.1 – Relação entre URL, URN e URI

A Internet é uma rede de recursos que recorre a três mecanismos para tornar estes recursos disponíveis para toda a rede:

- Um esquema de nomes que permite localizar os recursos através de um nome único – *Uniform Resource Locator* (URL).
- Protocolos que permitam aceder a esse recursos, tais como o HTTP ou o FTP.
- Uma forma de introdução no texto legível aos utilizadores, que permite de uma forma intuitiva, navegar entre os recursos informativos, tal como o Hipertexto no HTML.

Por exemplo, para visualizar a página principal da União Europeia, digita-se no navegador (*browser)* o respetivo endereço:

- http://wwww.europa.eu/index_pt.htm.

Onde *http* é o método pelo qual a informação deve ser obtida; www.europa.eu é o nome do servidor onde a página que desejamos está armazenada. Pelo nome do computador, normalmente, pode inferir-se o tipo de informação a encontrar e a sua localização geográfica. Os que começam com *www* são servidores de *web* e contém principalmente páginas de hipertexto; / index_pt.htm é a localização do recurso no servidor que será visualizado no *browser*.

7.5 Recolha de cabeçalhos técnicos de mensagens de correio eletrónico

A introdução breve que foi feita de diversos conceitos, é fundamental para melhor entender o que se procura recolher na análise das mensagens de correio eletrónico.

Importa agora analisar os serviços mais populares existentes no mercado, que disponibilizam correio eletrónico e como é possível em relação a cada um deles, determinar o endereço IP e respetivo grupo data/hora que estiveram na sua origem.

Os pontos seguintes constituem um guia passo a passo, de como recolher os cabeçalhos técnicos das mensagens, nos quais constará a informação que se pretende recolher e cuja extração será estudada no capítulo 7.6.

Importa realçar que esta recolha de informação diz respeito a dados de tráfego, definidos na Lei nº 32/2008 de 17 de Julho, fazendo portanto apenas sentido a sua recolha se a situação envolver crimes informáticos previstos na Lei nº 109/2009 de 15 de Setembro ou o conceito de "crime grave" conforme previsto no art.º 2 da Lei 32/2008. Quer isto dizer que por exemplo, que em situações envolvendo situações de conflitos laborais, não se pode recolher dados de tráfego.

Acresce ainda, que especial cuidado devem ter os dados de conteúdo, ou seja, a informação propriamente dita, que não pode ser recolhida ou visionada, sob pena de se incorrer na prática de um crime de violação de correspondência ou de telecomunicações, tal como previsto no art.º 194º do CP.

Embora sejam abordados diversos produtos comerciais, o único critério foi o da popularidade dos mesmos, independentemente das plataformas em que são usados.

Microsoft Outlook:

1. Abrir a mensagem.
2. Na opção de menu "Ver" ou "*View*" selecionar "Opções" ou "*Options*".
3. Na janela que abriu (conforme Figura 7.5.1), na caixa "*Cabeçalhos de Internet" ou "Internet headers*" *clicar* com botão direito do rato, selecionar "*Selecionar tudo*" ou "*Select All*", depois *clicar* novamente com o botão direito do rato e selecionar "*Copiar*" ou "*Copy*".

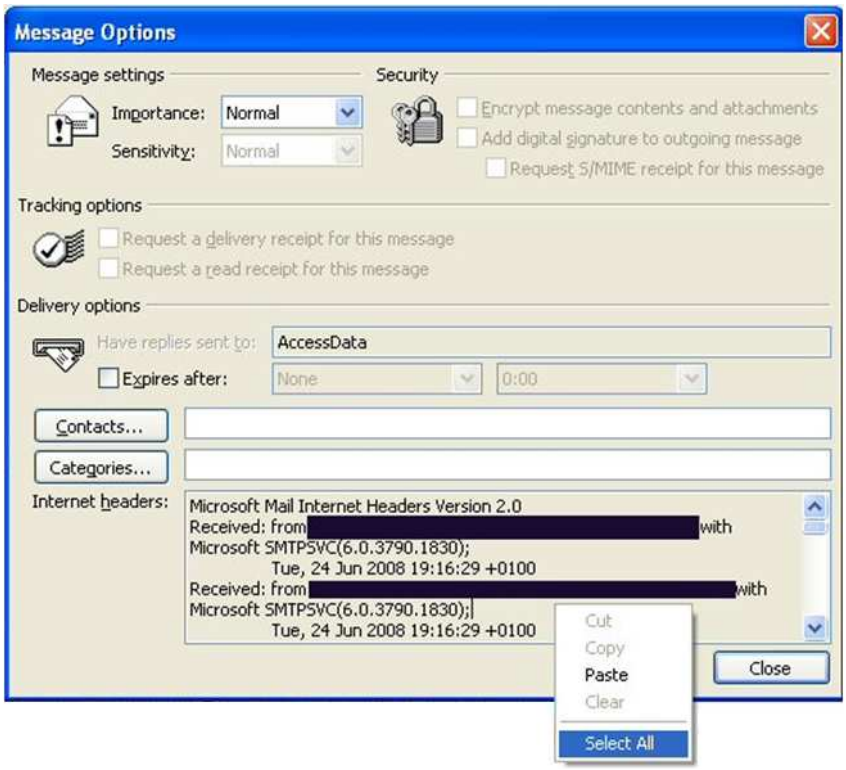


Fig. 7.5.1 – Outlook

4. Abrir um documento novo num processador de texto e realizar "*Colar*" ou "*Paste*".

Microsoft Outlook (2007):

1. Através do botão direito do rato e em cima da mesma e selecionar "*Opções das mensagens*…" ou "*Message Options*…", conforme Figura 7.5.2.

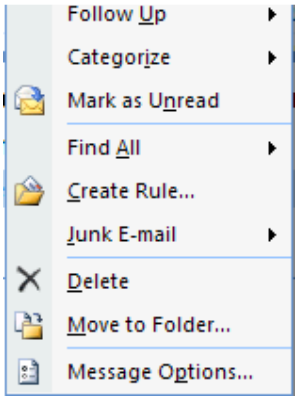


Fig. 7.5.2 – Outlook 2007

2. Na janela que abriu (ver figura 7.5.3), na caixa "*Cabeçalhos de Internet*" ou "*Internet headers*" *clicar* com botão direito do rato, selecionar "Selecionar tudo" ou "*Select All*", depois *clicar* novamente com o botão direito do rato e selecionar "*Copiar*" ou "*Copy*".

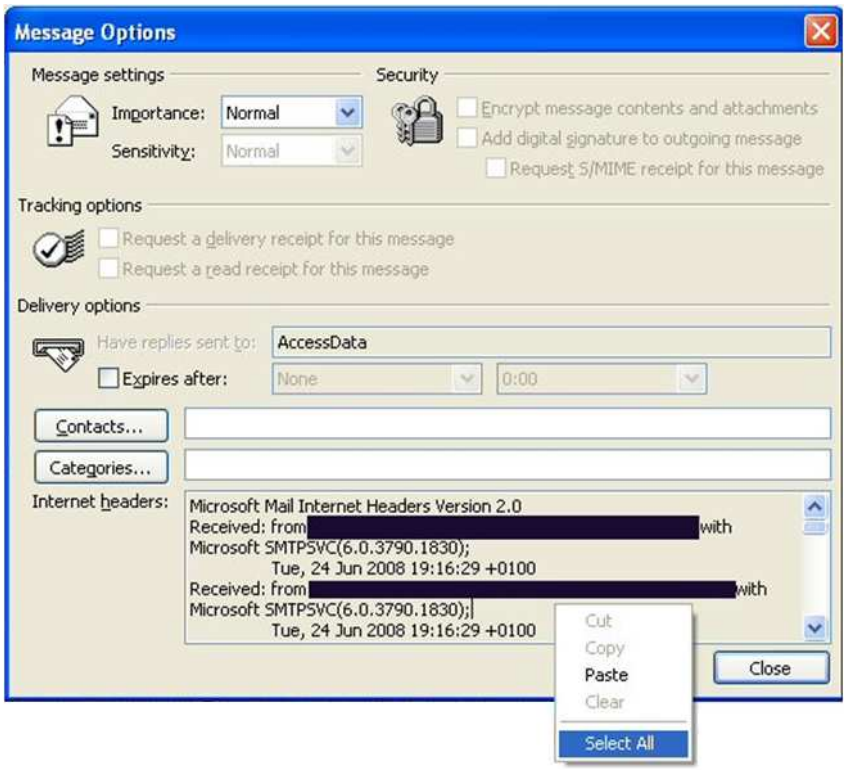


Fig. 7.5.3 - Outlook 2007

3. Abrir um documento novo no Word e realizar colar, o copiará o conteúdo da memória.

Microsoft Outlook (2010):

1. Abrir a mensagem.
2. Selecionar o tabulador “Ficheiro”.

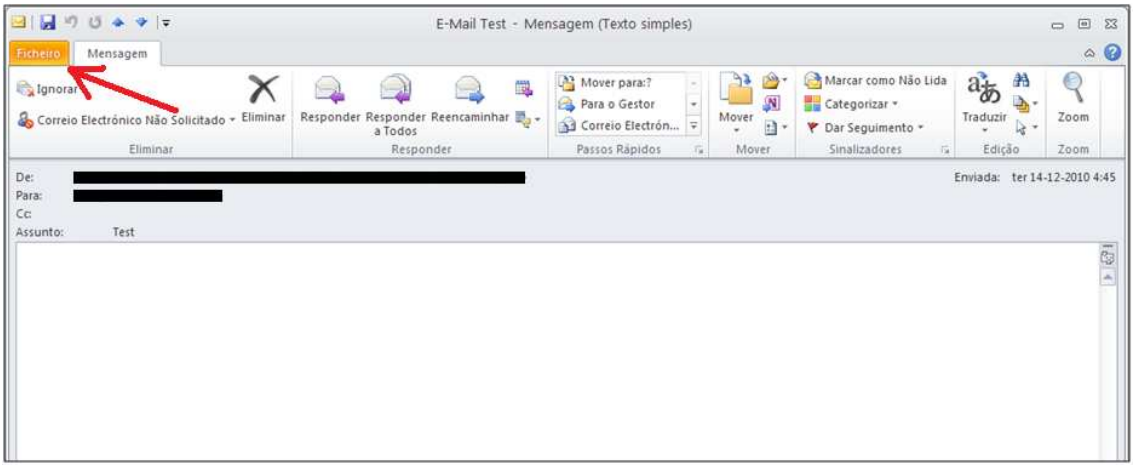


Fig. 7.5.4 - Outlook 2010

3. Na janela que abriu (conforme Figura 7.5.4), Selecionar a opção “*Informações*” e de seguida a opção “*Propriedades*”.

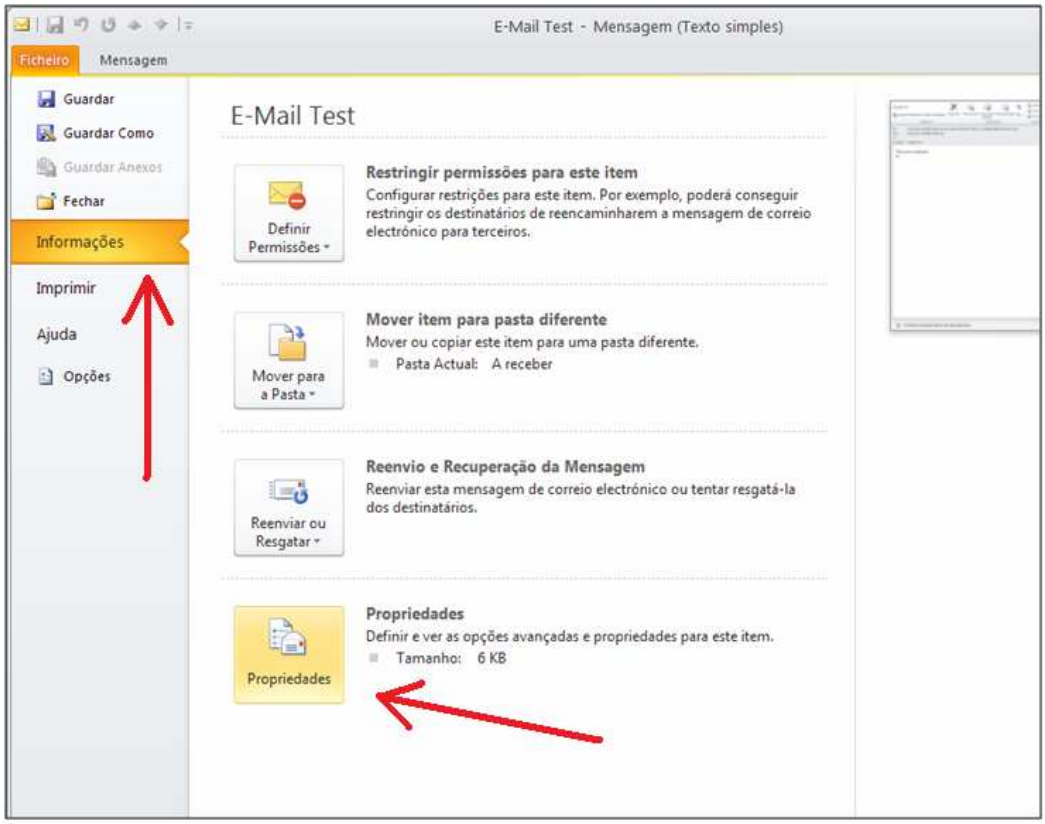


Fig. 7.5.5 - Propriedades da Mensagem em Outlook 2010

4. Na janela que abriu (conforme Figura 7.5.6), na caixa "*Cabeçalhos de Internet*" ou "*Internet headers*" *clicar* com botão direito do rato, selecionar "*Selecionar tudo*" ou "*Select All*", depois *clicar* novamente com o botão direito do rato e selecionar "*Copiar*" ou "*Copy*".

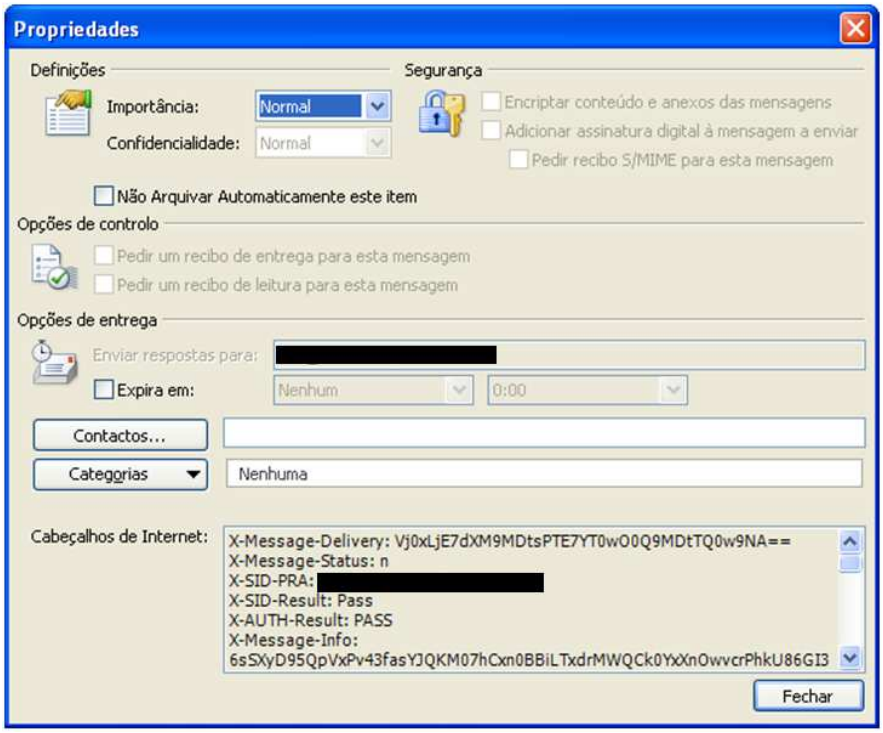


Fig. 7.5.6 - Propriedades da Mensagem em Outlook 2010

5. Abrir um documento novo no Word e realizar colar o que está em memória.

Microsoft Outlook Express:

1. Existem pelo menos duas formas de aceder aos cabeçalhos das mensagens. Se a mensagem for aberta, a partir do menu "Ficheiro" ou "*File*" acede-se à opção "Propriedades" ou "*Properties*" ou então ao *clicar* com o botão direito do rato em cima da mesma e selecionar "*Properties*" conforme Figura 7.5.7.

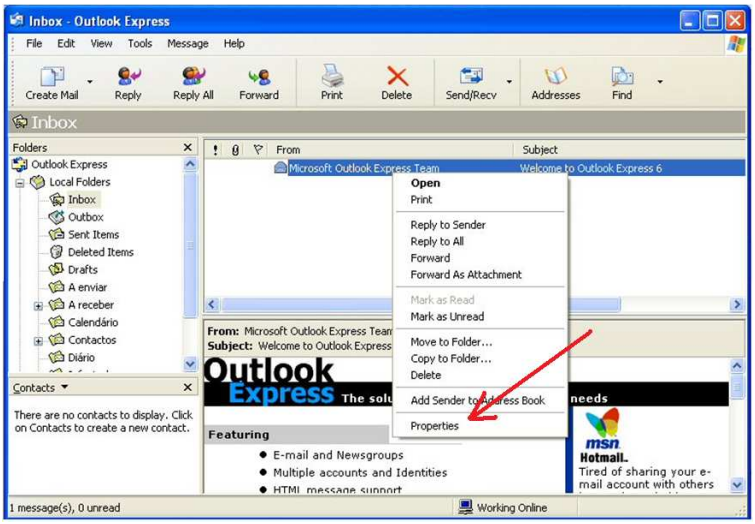


Fig. 7.5.7 - Outlook Express

2. Depois visualiza-se o conteúdo da Figura 7.5.8.

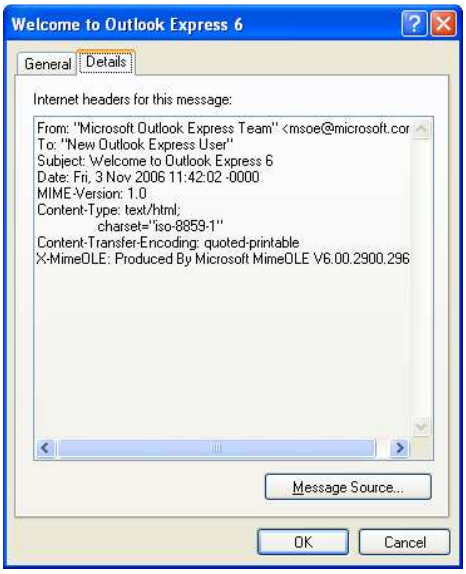


Fig. 7.5.8 - Detalhes das propriedades do Outlook Express

3. No tabulador "Detalhe" ou "*Details*" *clicar* com botão direito do rato, selecionar "Selecionar tudo" ou "*Select All*", depois *clicar* novamente com o botão direito do rato e selecionar "Copiar" ou "*Copy*".
4. Abrir um documento novo no Word e realizar colar o que está em memória.

Hotmail (nova versão Live):

1. Em cima da mensagem *clicar* botão direito e selecionar a opção "*View message source*", conforme Figura 7.5.9.

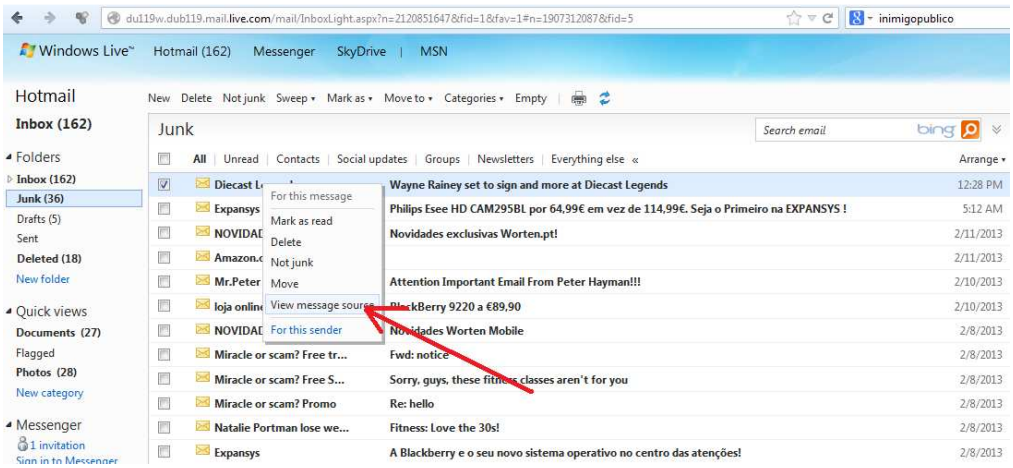


Fig. 7.5.9 - Hotmail Live (novo)

2. Abre-se automaticamente uma nova janela do *browser*.
3. Selecionar tudo (Crtl + A)
4. Copiar (Ctrl + C)
5. Abrir um documento novo no Word e realizar Colar (Ctrl + V).

Hotmail (versão Live):

1. Em cima da mensagem *clicar* botão direito e selecionar a opção "*View source*", conforme Figura 7.5.10.

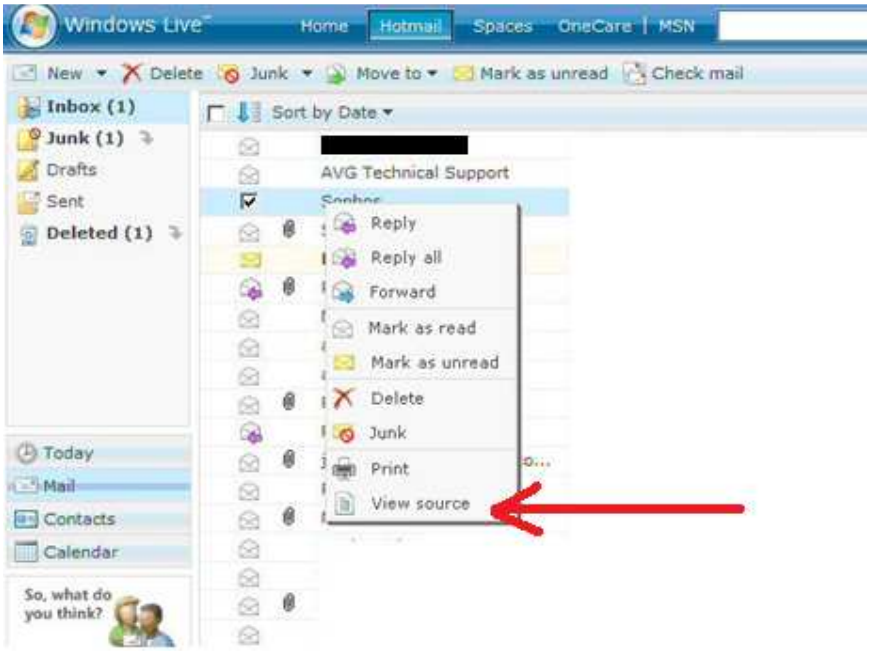


Fig. 7.5.10 - Hotmail Live

2. Abre-se automaticamente uma nova janela do *browser*.
3. Selecionar tudo (Crtl + A)
4. Copiar (Ctrl + C)
5. Abrir um documento novo no Word e realizar Colar (Ctrl + V).

Hotmail (versão Clássica):

1. Selecionar o menu "*Options*", posteriormente a opção "*Preferences*". Encontrar a opção "*Headers*" e selecionar a opção "*Advanced headers*".
2. Guardar as alterações
3. Voltar à mensagem, uma vez que já se encontram visíveis os cabeçalhos técnicos.

Sapo (Webmail):

1. Abrir a mensagem.
2. Abre-se uma nova janela com a mensagem, conforme Figura 7.5.11.
3. Agora é possível ter duas opções para ver os cabeçalhos:
   - Opção 1:
     - Selecionar a opção "Código-fonte da mensagem" (a destaque na Figura 7.5.11).
     - Vai ser aberta automaticamente uma nova janela do *browser*.
     - Selecionar tudo (Crtl + A)
     - Copiar (Ctrl + C)
     - Abrir um documento novo no Word e realizar Colar (Ctrl + V).
   - Opção 2:
     - Selecionar a opção Mostrar todos os cabeçalhos" (Figura 7.5.12).
     - Selecionar a informação pretendida

- Copiar (Ctrl + C)
- Abrir um documento novo no Word e realizar Colar (Ctrl + V).

Fig. 7.5.11 - Mensagem Sapo

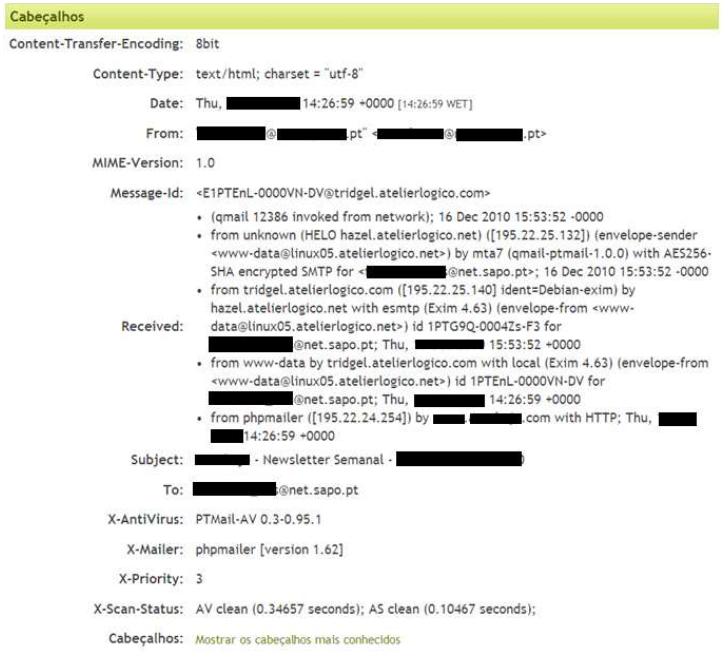


Fig. 7.5.12 - Mensagem com a opção "Mostrar todos os cabeçalhos"

Sapo (novo Webmail Beta):

1. Em cima da mensagem fazer duplo *click*.
2. Vai ser aberta uma nova janela com a mensagem, conforme Figura 7.5.13.

Fig. 7.5.13 - Sapo Webmail Beta

3. Selecionar a opção "CÓDIGO-FONTE DA MENSAGEM".
4. Vai ser aberta automaticamente uma nova janela do *browser*.
5. Selecionar tudo (Crtl + A)
6. Copiar (Ctrl + C)
7. Abrir um documento novo no Word e realizar Colar (Ctrl + V).

Sapo Webmail (antigo):

Existe outra forma de exibir os cabeçalhos, mas por problemas relacionados com a impressão das mensagens, deve ser utilizada esta opção.

1. Abrir a mensagem.
2. Selecionar a opção "Código-fonte da Mensagem", conforme Figura 7.5.14.
3. Vai ser aberta automaticamente uma nova janela do *browser*.
4. Selecionar tudo (Crtl + A)
5. Copiar (Ctrl + C)
6. Abrir um documento novo no Word e realizar Colar (Ctrl + V).

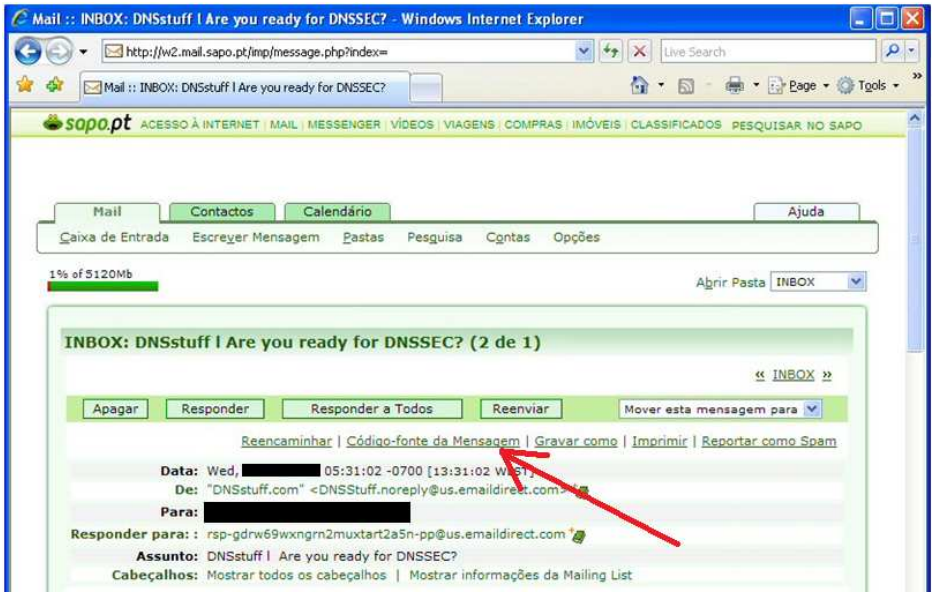


Fig. 7.5.14 - Sapo Webmail (antigo)

Gmail:

1. Selecionar o menu ao *clicar* na  , posteriormente a opção "*Show Original*", conforme Figura 7.5.15.
2. Vai ser aberta automaticamente uma nova janela do *browser*.
3. Selecionar tudo (Crtl + A)
4. Copiar (Ctrl + C)
5. Abrir um documento novo no Word e realizar Colar (Ctrl + V).

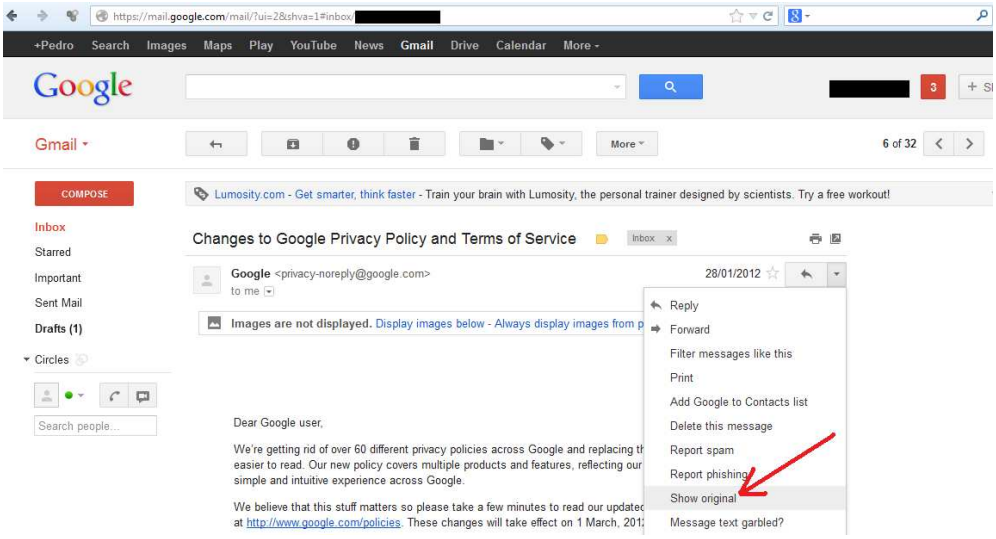


Fig. 7.5.15 - Gmail

Yahoo! Mail (Nova versão) :

1. Em cima da mensagem *clicar* botão direito e selecionar a opção "*View full headers*", conforme Figura 7.5.16.

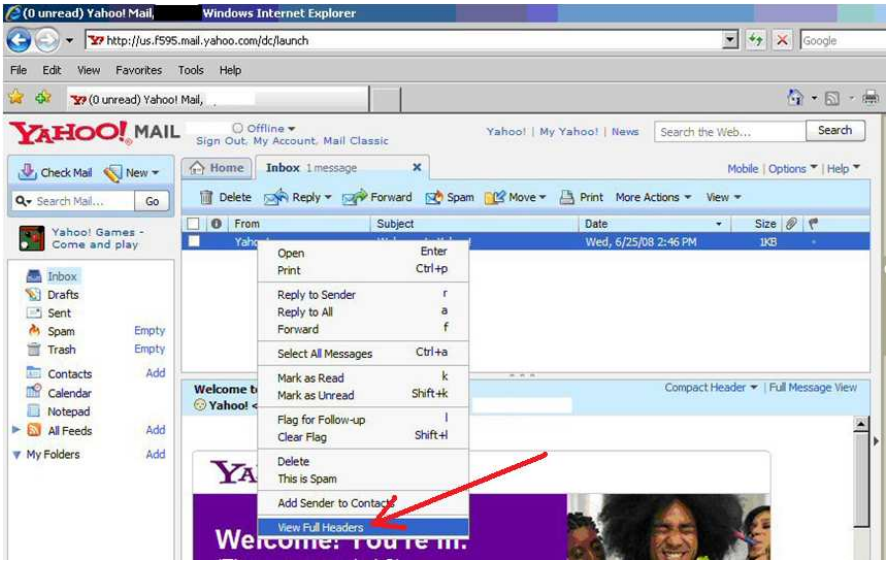


Fig. 7.5.16 – Yahoo! Mail

2. Vai abrir uma nova janela, conforme Figura 7.5.17.

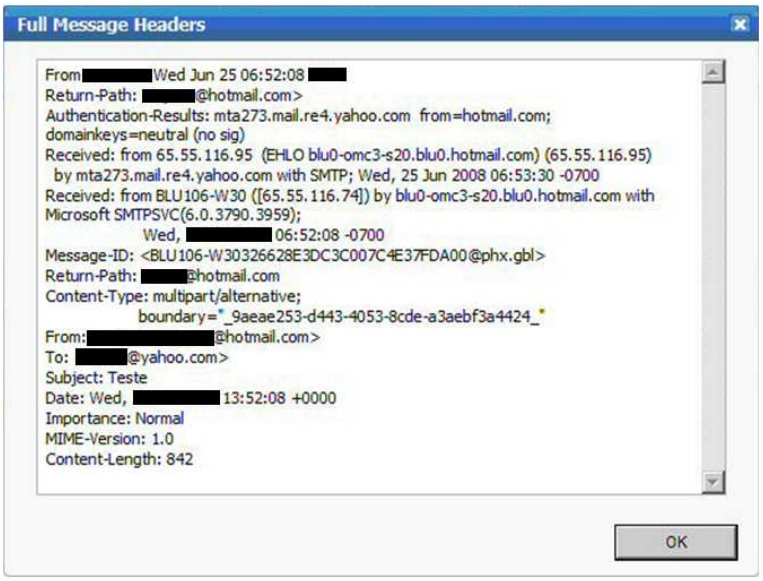


Fig. 7.5.17 - Cabeçalhos do Yahoo! Mail

3. *Clicar* com botão direito do rato, selecionar "Selecionar tudo" ou "*Select All*", depois *clicar* novamente com o botão direito do rato e selecionar "Copiar" ou "*Copy*".
4. Abrir um documento novo no Word e realizar "Colar" ou "*Paste"* através da Opção de Menu "*Edit/Paste*" ou botão direito do rato, opção "*Paste*".

Yahoo (antigo):

1. Selecionar o menu "*Options*", posteriormente a opção "*Mail Preferences*". Na opção "*Mail Viewing Preferences*", na parte dos "*Message Headers*" selecionar a opção "*All*".

Clix:

1. *Clicar* na opção  , conforme Figura 7.5.18.

Fig. 7.5.18 - Selecionar visualização dos cabeçalhos do Clix

2. Vai ser aberta automaticamente uma nova janela do *browser*, conforme Figura 7.5.19.
3. Selecionar tudo (Crtl + A)
4. Copiar (Ctrl + C)
5. Abrir um documento novo no Word e realizar Colar (Ctrl + V)

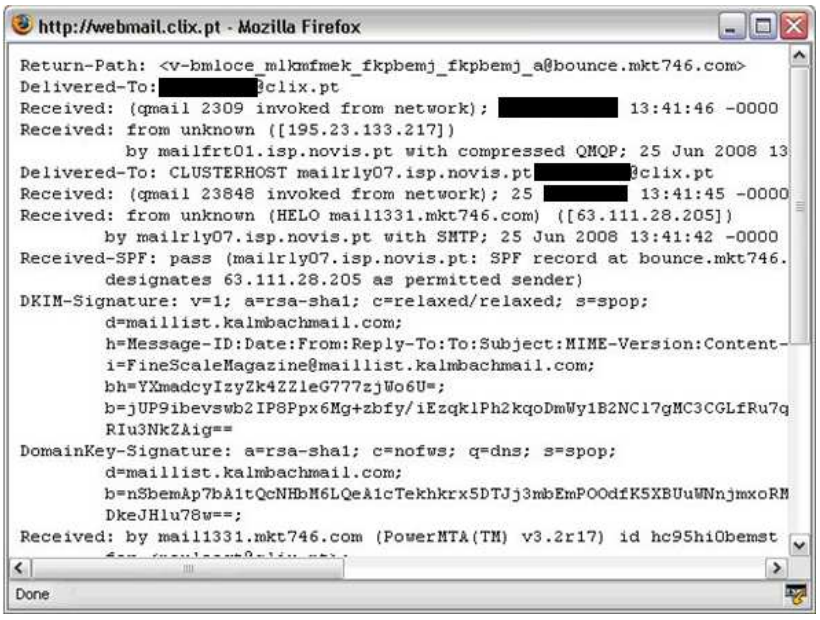


Fig. 7.5.19 - Cabeçalhos do Clix

7.6 Análise Forense de um cabeçalho de e-mail

Depois de recolhido o cabeçalho técnico de uma mensagem de correio eletrónico, há que saber lê-lo e dele recolher o endereço IP e respetivo grupo data/hora (timestamp), para assim determinar através do respetivo ISP (Internet Service Provider), de onde foi enviada a mensagem.

Entre os conceitos que importa ter bem presente na análise que se vai seguir, estão para além do já referido endereço IP, os seguintes:

SMTP: O Simple Mail Transfer Protocol permite a comunicação e entrega de mensagens entre duas entidades, também conhecidas como MTAs ou MUAs.

POP: O Post Office Protocol, ou POP3, é um protocolo utilizado no acesso remoto a uma caixa de correio eletrônico e permite a transferência de mensagens contidas numa caixa de correio eletrônico para um computador local, permitindo a sua leitura.

MTA: O Mail Transfer Agent é uma aplicação responsável pelo envio/receção de e-mail. Exemplos são o Postfix, o Exim ou o Qmail.

MUA: O Mail User Agent é um cliente de e-mail, isto é, onde as mensagens são escritas e lidas.

A interação entre estes conceitos, pode ser visualizada nas figuras 7.6.1 e 7.6.2.

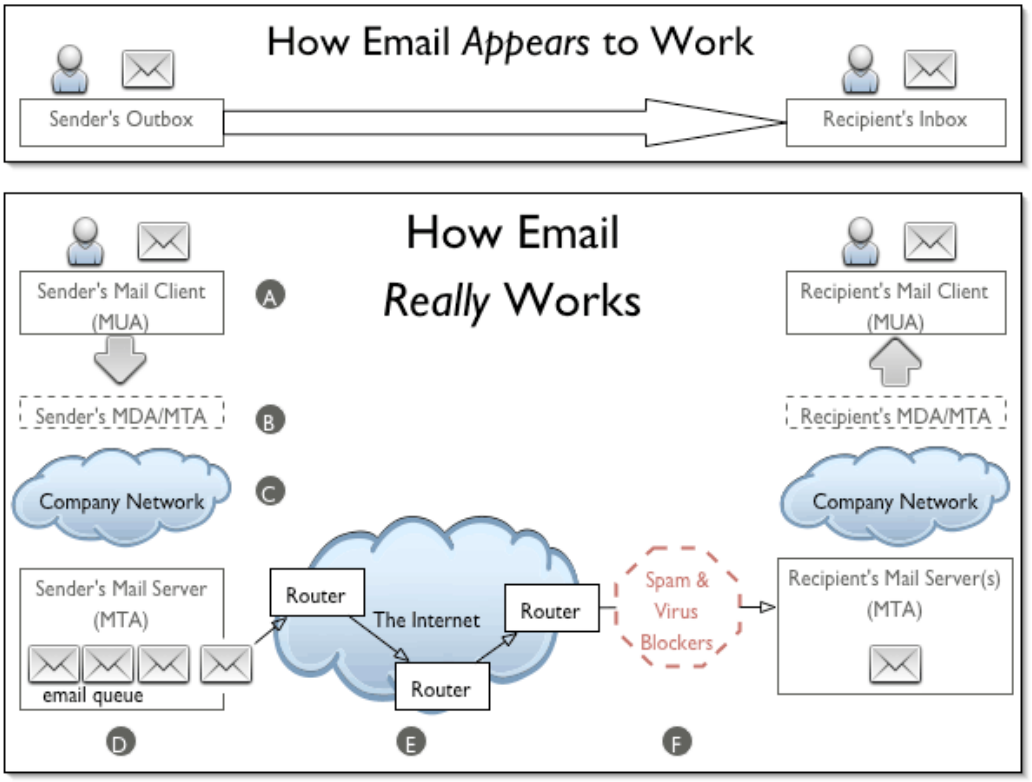


Fig. 7.6.1 – Entidades envolvidas no envio/receção de email

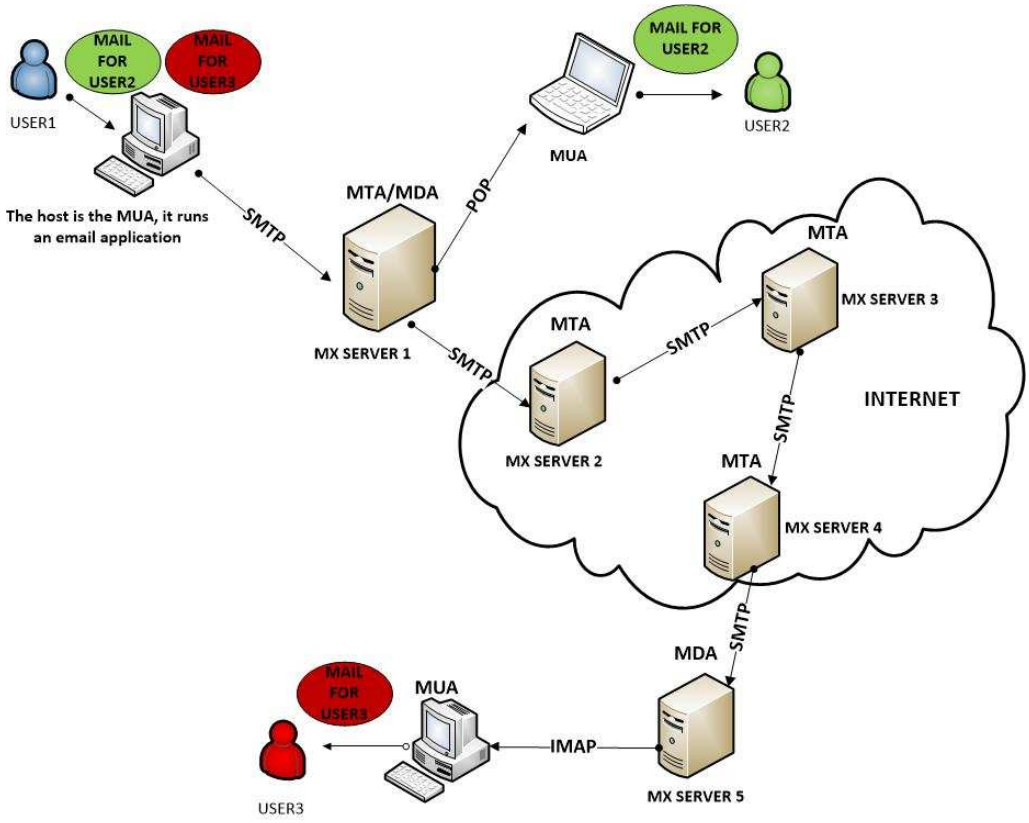


Fig. 7.6.2 – Entidades envolvidas no envio/receção de email

Utilizando estes protocolos uma mensagem de email vai "viajar" pela Internet, passando por diversos servidores entre a origem e o seu destino, conforme se pode ver pela figura 7.6.2. Cada servidor por onde a mensagem vai passar, vai-lhe acrescentar informação ao cabeçalho, sobrepondo informação à já existente. É por esta razão que os cabeçalhos devem ser lidos de baixo para cima, porque assim lidos, permitem ter uma ideia do percurso da mensagem desde a sua origem até ao seu destino.

Exemplo 1:

1. MIME-Version: 1.0
2. Received: by 10.143.12.8 with HTTP; Tue, 21 Oct 2009 21:31:52 -0700 (PDT)
3. Date: Wed, 21 Oct 2009 00:31:52 -0400
4. Delivered-To: XXXXXX@gmail.com
5. Message-ID:
6. Subject: header stat
7. From: Fulano de Tal
8. To: XXXXXX@gmail.com

9. Content-Type: text/plain; charset=ISO-8859-1

O exemplo 1 representa o envio de uma mensagem entre o "Fulano de Tal" e o "XXXXXX@gmail.com". Começando de baixo para cima, temos na linha 9 a indicação da forma de como o texto deve ser interpretado pelo seu cliente de e-mail (MUA).

As linhas 8, 7, 5 e 2 são mais as importantes do exemplo, indicando as linhas 7 e 8 o remetente e o destinatário. Segundo a RFC 822, o campo "From:" contém o endereço da pessoa que criou a mensagem, embora seja possível forjar este campo facilmente através de uma máscara.

Outro campo presente na RFC do e-mail é o Message-ID, conforme descrito na linha 5. Este campo é um identificador único que refere a versão desta mensagem. A linha 2 mostra que o servidor de e-mail (MTA), com o endereço 10.143.12.8, recebeu esta mensagem. Cada MTA que processar a mensagem deve carimbar o cabeçalho do e-mail com o campo: "Received:".

O exemplo 2 ilustra um cabeçalho onde vários MTAs carimbaram a mensagem permitindo rastreá-la.

Exemplo 2:

1. Return-Path: [fake@address.com]
2. Received: from server.mymailhost.com (mail.mymailhost.com [126.43.75.123]) by sys01.cl.msu.edu (8.10.2/8.10.2) with ESMTP id NAA23597; Fri, 12 Jul 2002 16:11:20 -0400 (EDT)
3. Received: from aol.com (127-34-56-98.dsl.mybigisp.com [127.34.56.98]) by server.mymailhost.com; Fri, 12 Jul 2002 13:09:38 -0700 (PDT)
4. Date: Fri, 12 Jul 2002 13:09:38 -0700 (PDT)
5. From: Hot Summer Deals
6. To: My.Friends@msu.edu
7. Subject: Just what you've been waiting for!!

Como pode ser observado na linha 3, a mensagem foi recebida pelo servidor "127-34-56-98.dsl.mybigisp.com [127.34.56.98]". Da linha 2 retira-se que este e-mail foi processado pelo servidor "server.mymailhost.com (mail.mymailhost.com [126.43.75.123])"

O Return-Path é um campo interessante que deve ser analisado com um pouco mais de paciência. Segundo a sua definição, este campo informa o endereço e a rota de volta de quem originou a mensagem. Por exemplo, na linha 1 temos:

1. Return-Path: [fake@address.com]

Isto quer dizer que no caso de algum problema no envio desta mensagem, um e-mail de erro deve retornar para o remetente, fake@address.com, informando sobre o problema.

Observando as linhas 5 e 6 desta mensagem, é razoável aceitar que um dos dois campos foi forjado, uma vez que os campos indicados divergem. Por outro lado, esta premissa não pode ser considerada

como verdade absoluta. Em alguns casos como listas ou grupos de e-mail, estes campos serão distintos como ilustra o exemplo 3.

Exemplo 3:

1. Return-Path: mailman-bounces@lists.DOMAIN.net

…

2. From: mailman-owner@lists.DOMAIN.net

O mailman possui alguns utilizadores que são responsáveis por determinadas atividades administrativas na lista de e-mail.

No exemplo 4, é apresentada uma mensagem onde tanto o remetente (FROM) como o "RETURN-PATH" são compatíveis. O remetente "REMOVIDO@uol.com" pode ser encontrado nos campos 1 e 4.

Exemplo 4:

1. Return-Path: [removido@uol.com]

2. Received: from relay5.uol.com (relay5.uol.com [200.221.4.168]) by gmr-mx.google.com with ESMTP id 25si512786qyk.7.2009.11.01.13.52.12; Sun, 01 Nov 2009 13:52:13 -0800 (PST)

   ….

3. Date: Sun, 1 Nov 2009 19:52:10 -0200

4. From: Beltrano da Silva [removido@uol.com]

Uma abordagem utilizada pelos spammers é enviar uma mensagem contendo o "Re:" no assunto, levando o cliente de e-mail a considerar este texto como uma suposta resposta ao e-mail enviado.

O exemplo 5.1 ilustra uma mensagem enviado pelo "Beltrano Silva" para o "Fulano Silva". Observe-se que o Message-ID desta mensagem será referenciada quando Fulano responder o e-mail.

Exemplo 5.1:

1. Message-ID: [9355e773091025180 3l522389eau9d7973ad0d909fcb@mail.gmail.com]

2. Subject: Telefone da Maria Fulana

3. From: Beltrano Silva [xxxxxxxx@gmail.com]

4. To: Fulano Silva [yyyyyyyy@gmail.com]

Após "Fulano Silva" responder a mensagem do "Beltrano Silva", o cabeçalho desta mensagem pode ser ilustrado no exemplo 5.2

Exemplo 5.2:

1. In-Reply-To:[9355e77309102518031522389eau9d7973ad0d909fcb@mail.gmail.com]
2. References: [9355e77309102518031522389eau9d7973ad0d909fcb@mail.gmail.com]

   ..
3. Message-ID: [c794d6fe0910281225x637be9d5y6277954229ad1511@mail.gmail.com]
4. Subject: Re: Telefone da Maria Fulana
5. From: Fulano Silva [yyyyyyyy@gmail.com]
6. To: Beltrano Silva [xxxxxxxx@gmail.com]

Aparecem dois novos campos no cabeçalho da mensagem, In-Reply-To e References. É importante realçar que os campos 1 e 2 fazem referência ao Message-ID do exemplo 5.1, 9355e77309102518031522389eau9d7973ad0d909fcb. Enquanto isso, o Message-ID do exemplo 5.2 é diferente, pois este campo deve ser único para cada mensagem.

Outro exemplo que pode ser identificado através do cabeçalho da mensagem é quando é utilizada uma página Web comprometida capaz de enviar a mensagem.

Exemplo 6:

1 Received: by hm1277.DOMAIN.com (Postfix, from userid 1242)

id E5A08B85E8; Mon, 4 May 2009 16:29:40 -0300 (BRT)

…

2 content-type: text/html

3 Subject: assunto da mensagem

4 From: torpedo@vivotorpedo.com

5 To: XXXXXXXXX@gmail.com

6 Message-Id: [20090504192940.E5A08B85E8@hm1277.DOMAIN.com]

A linha 1 do exemplo 6 traz uma informação adicional ao cabeçalho. O MTA recebeu esta mensagem do utilizador “userid 1242″. Por outras palavras, esta conta pode ter sido comprometida pelo atacante para enviar mensagens maliciosas.

Identificado o endereço IP que originou a mensagem, algumas ferramentas podem ser aplicadas para ajudar no processo de investigação, tal como explicado no capítulo 6.2, identificando-se o respetivo

código ISO do país, país de origem, Estado, Cidade, Código Postal, latitude e longitude e o provedor de Internet (ISP) que possui autoridade em delegar o IP.

As informações contidas no Whois permitem entrar em contato com o provedor de acesso (ISP) a fim de solucionar algum problema, ou identificar o respetivo titular através dos meios judiciais, como será estudado no capítulo 8, dedicado aos temas jurídicos.

Identificar a origem de uma determinada mensagem pode não ser uma tarefa muito complicada. Alguns crimes podem ser revelados a partir de simples abordagens, mas nem tudo é muito fácil. Atacantes experientes utilizam inúmeras máquinas comprometidas para dificultar sua identidade, ou recorrem a locais públicos de acesso à Internet, onde a sua identidade vai permanecer anonima. Portanto, analisar o cabeçalho do e-mail é apenas o começo de um processo e obter logs de outros componentes o passo seguinte no processo investigatório.

Existem ainda outros campos que podem aparecer no cabeçalho do e-mail, uma vez que cada MUA (cliente de e-mail) pode adicionar um campo, dependendo da sua configuração. Geralmente estes campos iniciam-se com X-[Qualquer-Coisa].

Analise-se agora um caso real de uma mensagem recebida numa conta de Hotmail através do Windows Live, tal como a que consta da figura 7.6.3

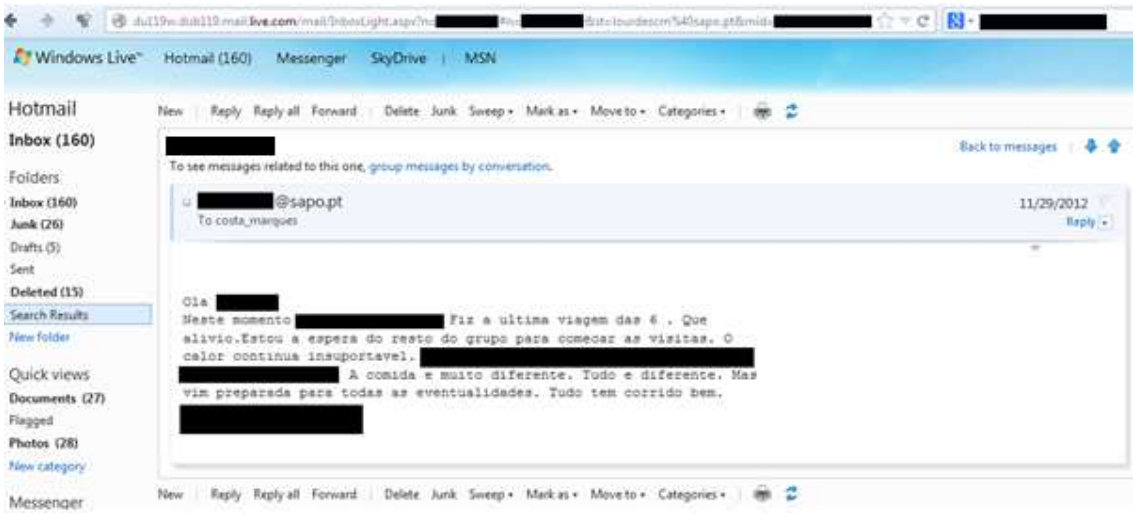


Fig. 7.6.3 – Mensagem de Hotmail no Windows Live

Depois de retirado o respetivo cabeçalho técnico, identificam-se o endereço IP e o grupo data/hora (timestamp), tal como assinalado pelos retângulos da figura 7.6.4:

Fig. 7.6.4 – Cabeçalho técnico

Ou com mais detalhe:

Fig. 7.6.5 – Detalhe do cabeçalho técnico

Recorrendo ao serviço disponibilizado no "http://whois.domaintools.com", obtém-se a seguinte informação:

IP Information for 203.189.136.228

IP Location:	Cambodia Phnom Penh Static Ip Pool
ASN:	AS23673
Resolve Host:	mydsl128-136-228.online.com.kh
IP Address:	203.189.136.228 W R P D T

```
inetnum:        203.189.136.0 - 203.189.136.255
netname:        AZCOM
descr:          Static IP Pool
country:        KH
admin-c:        CL965-AP
tech-c:         CON1-AP
status:         ASSIGNED NON-PORTABLE
mnt-by:         MAINT-KH-BPC
changed:        network@azcom.net.kh  20120606

mnt-irt:        IRT-COGETEL-KH
source:         APNIC

route:          203.189.128.0/19
descr:          ONLINE
origin:         AS23673
mnt-by:         MAINT-KH-BPC
changed:        network@azcom.net.kh  20120606

source:         APNIC

role:           Cogetel Limited
address:      #60 Monivong Boulevard
address:        Phnom Penh
address:        Cambodia
country:        KH
```

Fig. 7.6.6 – ISP remetente da mensagem

Que permite saber que a mensagem terá sido enviada através de um ISP localizado no Cambodja, a quem deverá ser solicitada informação através das autoridades judiciais sobre o titular deste endereço, em 29 de Novembro de 2012 às 00:58:06 +0000. Importa chamar à atenção que deve ser sempre indicada a georreferencia da data/hora.

8 Quadro legislativo no âmbito da criminalidade informática

O presente capítulo não pretende ser um documento jurídico sobre a legislação portuguesa, no que esta tem a ver com a criminalidade informática.

O objetivo é dentro da medida do possível não recorrer a uma linguagem estritamente jurídica, procurando apresentar uma visão prática e direcionada para técnicos de informática, mas abarcando todos os condicionalismos legais com que estes têm de lidar no seu dia-a-dia.

Será apresentada a legislação mais importante que rege os crimes informáticos, onde os sistemas podem ser vítimas de crimes, utilizados na sua execução ou como armazenamento de prova de crimes, mesmo que não informáticos.

8.1 O Conceito de Crime Informático

A conceptualização do normalmente denominado crime informático, apresenta como primeira questão a de saber qual a denominação jurídica a adotar para os crimes que ofendam interesses e bens jurídicos, relativos ao uso, à propriedade, à segurança, à funcionalidade dos computadores e conjunto de equipamentos periféricos, à funcionalidade das redes e sistemas de telecomunicações, e dos programas que neles são executados.

Referências a crimes computacionais, crimes informáticos, crimes de computador, crimes eletrónicos, crimes telemáticos e cibercrimes, são designações que vulgarmente são utilizadas e que tem na base a utilização de um computador, ligado, ou não, em rede e sendo desprezível para o efeito que o mesmo seja alvo ou instrumento do crime.

De entre as diversas designações, as mais utilizada são sem dúvida a de *"crimes informáticos"* ou a de "*criminalidade informática*", para identificar as infrações que atingem os computadores, isolados ou em rede, as redes de comunicações, ou as que sejam praticadas com recurso a essas vias.

A particularidade e novidade em termos criminais é o facto de estarmos perante a prática de crimes cometidos à distância, sem ser necessário haver contacto físico entre o criminoso e a vítima e onde não há qualquer tipo de fronteiras, o que levanta problemas jurisdicionais em termos de competências territoriais.

Certo é, que a criminalidade informática como preocupação mundial, exige uma fixação do conceito que só será possível pela uniformização internacional das legislações nacionais. Está em causa afinal, o combate eficaz a novas realidades criminais, ou práticas criminais tradicionais que se servem das novas tecnologias de informação e comunicação.

A OCDE define a criminalidade informática como sendo, *"qualquer comportamento ilegal, não ético ou não autorizado, que envolva processamento automático de dados e/ou transmissão de dados", que consubstancia:*

- Uma preocupação em não excluir do espectro penal, um conjunto de práticas criminais já tipificadas, que pela adoção das novas tecnologias, vieram criar dificuldades de qualificação penal e de abordagem na sua investigação e
- Assumpção de que existem comportamentos que pela sua especificidade e novidade, devem motivar e impelir os Estados a legislar sobre crimes estritamente ligados à informática e às comunicações.

Assim, há um conjunto de realidades e atividades, que envolvem a informática e que criam problemas de aplicação ao Direito, algo que por isso vem motivando, por parte do poder legislativo, uma tomada de posição.

A produção de legislação que nesta área tem ocorrido, permite identificar pelo menos, quatro fases:

1. Criação de legislação relativa à proteção da vida privada, decorrente dos problemas causados pelas novas possibilidades de recolha, armazenamento, transferência e interconexão de dados pessoais;

2. Criação de legislação sobre combate à delinquência económica específica da informática, destinada a proteger uma realidade imaterial e não tangível, como são os casos de manipulação de computadores e adulteração dos seus programas;

3. Iniciativas legislativas relacionadas com a proteção da propriedade intelectual, direcionada aos programas de computador e em reação à cópia ilegal;

4. Legislação para o campo do Direito Processual Penal, tendente ao aperfeiçoamento de medidas de combate à nova criminalidade. É neste quadro, que se insere a nova Lei do Cibercrime, a Lei 109/2009 de 15 de Setembro, acolhendo grande parte destas tendências de neocriminalização e assumindo como principal preocupação a imposição de medidas processuais que facilitem a investigação e recolha de prova. No campo substantivo a tónica é colocada na imposição de procedimentos de segurança informática ou proibição da simples detenção de programas informáticos mal-intencionados, como sejam as limitações à criptografia e a programas geradores de Malware, bem como na necessidade de perseguição dos conteúdos imorais e perigosos na Internet, como por exemplo os de pedofilia ou ciberterrorismo. De notar ainda, que a legislação portuguesa, com a revisão do Código Penal de 2007, já tinha imposto medidas importantes relativas a conteúdos imorais, nomeadamente a denominada pornografia infantil na Internet.

8.2 Classificação dos Crimes Informáticos

A classificação mais aceite é a que relaciona a criminalidade informática com a função que o computador desempenha na execução do crime:

- Crimes em que o computador serve de instrumento ou meio, para atingir um objetivo criminoso e
- Crimes em que o computador é o alvo do ato criminoso.

Diga-se que se trata da perspetiva que mais se coaduna com a investigação criminal, permitindo logo numa fase inicial da investigação, que se possa estar na posse de elementos que permitam saber se o computador foi objetivo do crime, ou foi utilizado porque se trata de uma facilidade.

8.3 Os Crimes Informáticos na Legislação Portuguesa

No ordenamento jurídico português, a legislação penal referente á criminalidade informática não está concentrada num único diploma, tendo sido opção do legislador:

- A criação de uma lei específica para o tratamento da criminalidade informática propriamente dita, a denominada Lei do cibercrime (Lei 109/2009 de 15 de Setembro);

- Ter uma lei para a Proteção dos Dados Pessoais (a Lei 67/98, de 26 de Outubro) e

- Manter no Código Penal um conjunto de previsões criminais directamente relacionadas com a informática e telecomunicações nomeadamente a "Burla informática e nas comunicações" – art.º 221º.

Nos pontos seguintes será feita uma resenha sobre os elementos constitutivos do tipo, nos interesses ou bens jurídicos que protegem e eventuais questões de interpretação que se levantam na sua aplicação, em particular sobre a lei do cibercrime e no que esta também encerra ao nível de medidas processuais.

8.4 Lei do Cibercrime - Lei nº 109/2009 de 15 de Setembro

Esta Lei veio fornecer um novo instrumento, adequando as normas substantivas e processuais a uma nova realidade digital, liderada pelas tecnologias de informação e comunicação.

As alterações verificadas nas redes de comunicação, em particular o aparecimento da Internet, trouxeram uma nova vivência em sociedade, imprimindo na atividade das pessoas, das empresas e das instituições, um novo conceito associado ao mundo digital.

A realidade vem demonstrando a inevitabilidade da sociedade ser acompanhada e suportada pelas constantes evoluções das novas tecnologias, as quais, com enormes índices de penetração, já são o suporte indispensável nas mais distintas áreas de trabalho, liderando mesmo, as grandes mutações que aí ocorrem.

Por consequência, a informática passou a ser também um fator primordial na própria atividade individual privada, no relacionamento entre as pessoas e na interação familiar, estejamos ou não, a falar de atividades directamente com ela relacionadas.

É neste sentido que se entende não ser possível extrair, excecionar, ou eliminar da sua influência, as atividades da Justiça e do Direito, bem sabendo que estas, sendo obrigações do Estado, têm no seu íntimo as funções de previsão, aplicação e alteração de regras em sociedade, de relações entre pessoas e de criação de padrões de comportamento.

As atividades ilegais não são exceção e aparecem numa primeira linha no aproveitamento destas mutações. De facto, às alterações ocorridas nas tecnologias, corresponde um aumento de oportunidades de crime e no mundo criminal surgiram de imediato um conjunto vasto de novos "modus operandi" do chamado cibercrime, cujo termo, a nova lei adotou.

Como já referido, o enfoque que a atividade criminal colocou no uso da informática e nas novas tecnologias não se pode reduzir aos denominados crimes informáticos, uma vez que um vasto conjunto de crimes, aparecem agora a ser cometidos com recurso a meios informáticos, com a ajuda de plataformas de comunicação, ou, em que a informática é mero instrumento para a sua prática.

Esta realidade exponenciada pelo uso das tecnologias não foi no entanto descurada pela nova lei do cibercrime, a qual veio alargar o âmbito de aplicação das normas processuais e destinadas á recolha de prova, não só aos crimes informáticos, mas também aos cometidos por meio de um sistema informático, ou, em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico.

A Lei 109/2009 de 15 de Setembro, transpõe para a ordem jurídica interna a Decisão quadro n.º 2005/222/JAI, do Conselho Europeu, relativa a ataques contra sistemas de informação e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

Como fonte de direito interno e face á escassez de jurisprudência, esta convenção sobre cibercrime é o principal instrumento de interpretação da lei, constituindo-se como o suporte para a elaboração de legislação. Teve na sua base propostas de grupos de especialistas de vários países, que se debruçaram sobre os problemas dos crimes no ciberespaço e embora seja uma iniciativa do espaço comunitário europeu, engloba na sua elaboração outros países, como os USA, Canadá e Japão. É considerado um verdadeiro instrumento legislativo para as generalidades dos países mundiais.

Genericamente, a Lei 109/2009 de 15 de Setembro espelha os propósitos da Ciberconvenção, espelhados em 3 objetivos:

1. Redefinição e atualização das normas penais aplicáveis na área do cibercrime;
2. Criação de medidas processuais que viabilizem a obtenção e recolha de dados para fins de investigação criminal e
3. Implementação de normas específicas relativas à cooperação internacional em matéria penal.

O conceito de "sistema informático" surge na Lei do cibercrime com uma descrição mais abrangente em relação á legislação anterior, consumindo e aglutinando o anterior conceito de "rede informática", englobando num só conceito todo e qualquer dispositivo composto por hardware e software que tenha por função o tratamento automatizado de dados informáticos.

Por sua vez, também o conceito de "dados informáticos" passa a ter uma formulação mais abrangente, para possibilitar a inclusão de qualquer representação de factos.

Particularmente importante na área de aplicação do direito sobre crime informático, é o conceito de "dados de tráfego", cuja interpretação tem consequências importantes sobre quem pode solicitar e obter estes dados que são gerados nos operadores de comunicações.

Em termos jurídicos e tendo em conta o significado que eles possuem para a investigação, os dados de tráfego indicam a origem e o destino de uma comunicação, bem como se, durante o seu processamento, houve algum reencaminhamento.

Sendo gerados pela própria comunicação, esta informação é neutra, só ganhando conteúdo identificativo concreto quando relacionada com elementos a ela exteriores e prévios ao estabelecimento da comunicação, os chamados dados de base ou dados conexos, sendo este o caminho apontado pelo artº14 nº 4 da Lei nº 109/2009 de 15 de Setembro.

Artigo 14.º
Injunção para apresentação ou concessão do acesso a dados

…/…

4. *O disposto no presente artigo é aplicável a fornecedores de serviço, a quem pode ser ordenado que comuniquem ao processo dados relativos aos seus clientes ou assinantes, neles se incluindo qualquer informação diferente dos dados relativos ao tráfego ou ao conteúdo, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida pelo fornecedor de serviços, e que permita determinar:*
    a) *O tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço;*

b) A identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à faturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços; ou

c) Qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços.

…/…

Tendo presente que a Lei nº 109/2009 de 15 de Setembro não se pode dissociar do disposto na Lei nº 32/2008 de 17 de Julho, que veio regular a conservação e a transmissão de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, a individualização dos "dados de tráfego" na formulação da Lei nº 109/2009, constitui uma verdadeira exceção àquele regime.

Um outro novo conceito introduzido pela lei é o de "fornecedor de serviços", no sentido de clarificar quais podem ser os intervenientes no processo de comunicação.

Numa formulação abrangente que parece incluir todos os fornecedores de suporte de comunicações e/ou fornecedores de acessos a este tipo de plataformas, como por exemplo um cibercafé, biblioteca ou qualquer outro espaço público de acesso á internet, o certo é que, este conceito só pode de facto ser aplicado aos denominados ISP, porque só estes estão abrangidos pelas obrigações de preservação de dados imposta pela Lei 32/2008 de 17 de Julho.

As disposições penais materiais

De uma maneira simplista pode afirmar-se que as previsões penais enquadram comportamentos cujo resultado provocado ou espectável é punido como uma determinada pena.

Estes comportamentos podem ser punidos mesmo nos casos em que não foram consumados, o que quer dizer que a mera tentativa de os praticar é punida.

Outro dos aspetos importantes é o denominado dolo, que não é mais do que a intenção que o individuo tinha quando praticou determinado ato. Este pode ser intencional, caso em que se diz que houve dolo ou negligente, quando não houve intenção de cometer o crime. Este aspeto é importante porque existem crimes que se denominam dolosos, o que quer dizer que para essa conduta ser punida, teve de haver intenção de o praticar.

Finalmente, os crimes podem ser públicos, semipúblicos ou particulares. No primeiro caso, não é necessária a formalização de uma queixa, para que o Ministério Público dê inicio à investigação. No segundo, é necessário que a vítima do crime formalize uma queixa para que seja iniciada a investigação e esta termina caso a vítima desista da mesma. No último caso, é necessário que seja apresentada uma queixa, mas recai também sobre o queixoso grande parte do ónus de produzir a prova necessária para a investigação e mais tarde para a própria acusação e julgamento. Neste último caso estão por exemplo os crimes de difamação e injúrias.

Excluindo a previsão do art.º 8º cuja epígrafe é "Reprodução ilegítima de programa protegido", que se insere no campo das infrações relativas á proteção dos direitos de autor e direitos conexos, todos os outros tipos criminais, previstos na lei nº 109/2009 de 15 de Setembro, "Falsidade informática", (art.º 3º), "Dano relativo a programas ou outros dados informáticos", (art.º 4º), "Sabotagem informática", (art.º 5º), "Acesso ilegítimo" (art.º 6º) e "Interceção ilegítima" (art.º 7º), encaixam nas chamadas

infrações relativas á confidencialidade, integridade e disponibilidade de sistemas e dados informáticos.

De seguida e em relação a cada um dos crimes previstos na lei, apresenta-se uma análise mais detalhada, procurando dar uma visão mais enfocada para quem vem de uma área técnica e que não domina obrigatoriamente a linguagem e lógicas do direito.

Analisemos então com mais detalhe, as condutas que são criminalizadas na Lei.

A "Falsidade informática"

Artigo 3.º

Falsidade informática

1. *Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem, é punido com pena de prisão até 5 anos ou multa de 120 a 600 dias.*
2. *Quando as ações descritas no número anterior incidirem sobre os dados registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, a pena é de 1 a 5 anos de prisão.*
3. *Quem, atuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, usar documento produzido a partir de dados informáticos que foram objeto dos atos referidos no n.º 1 ou cartão ou outro dispositivo no qual se encontrem registados ou incorporados os dados objeto dos atos referidos no número anterior, é punido com as penas previstas num e noutro número, respetivamente.*
4. *Quem importar, distribuir, vender ou detiver para fins comerciais qualquer dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, sobre o qual tenha sido praticada qualquer das ações prevista no n.º 2, é punido com pena de prisão de 1 a 5 anos.*
5. *Se os factos referidos nos números anteriores forem praticados por funcionário no exercício das suas funções, a pena é de prisão de 2 a 5 anos.*

Numa clara colagem aos crimes tradicionais de falsificação de documentos, este tipo penal da falsidade informática possibilita a adaptação dos chamados dados informáticos ao conceito geral de documento, revelando-se mais abrangente quer quanto ao meio utilizado para o seu cometimento, quer quanto ao seu elemento subjetivo, o "*engano nas relações jurídicas*".

A principal novidade do crime de falsidade informática está contida no nº2 do artº.3, quando se refere á "falsificação" que incida sobre os "…*dados registados ou incorporados em cartão bancário de pagamento*…", algo que transporta para esta previsão a criminalidade normalmente associada á chamada "clonagem ou duplicação de cartões bancários". A consequência sobre a realidade recente, que tipifica estas situações como crime de burla informática, notar-se-á principalmente na medida da pena, a qual passará a ser substancialmente inferior.

Refira-se ainda que este nº2 prevê a punição para a "falsificação" que incida "…*sobre os dados registados ou incorporados em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado…*", onde se incluem por exemplo a fraudes com acessos pagos a serviços de disponibilização de conteúdos de media ou a zonas de acesso condicionado dentro de uma empresa, como por exemplo um *data center*.

Quanto ao nº4 do art.º 3, a previsão criminal constitui uma verdadeira antecipação da tutela penal, punindo autonomamente, "*quem importar, distribuir, vender ou detiver para fins comerciais qualquer dispositivo*…", para o cometimento do crime de falsidade informática do nº2 do mesmo artigo.

A tipificação deste crime visa proteger a segurança das relações jurídicas, enquanto interesse público essencial que ao próprio Estado de Direito compete assegurar. Nessa medida a lei não prevê a necessidade de queixa-crime para o prosseguimento do procedimento criminal, pelo que estamos assim perante um crime público.

O "Dano relativo a programas ou outros dados informáticos"

Artigo 4.º

Dano relativo a programas ou outros dados informáticos

1. *Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos alheios ou por qualquer forma lhes afetar a capacidade de uso, é punido com pena de prisão até 3 anos ou pena de multa.*
2. *A tentativa é punível.*
3. *Incorre na mesma pena do n.º 1 quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as ações não autorizadas descritas nesse número.*
4. *Se o dano causado for de valor elevado, a pena é de prisão até 5 anos ou de multa até 600 dias.*
5. *Se o dano causado for de valor consideravelmente elevado, a pena é de prisão de 1 a 10 anos.*
6. *Nos casos previstos nos nº. 1, 2 e 4 o procedimento penal depende de queixa.*

O interesse jurídico protegido, com o tipo de danos relativos a dados ou programas informáticos, é a integridade dos dados, o seu bom uso e o seu bom funcionamento.

Tal como no crime de "Falsidade Informática", no nº 3 também se verifica a tal antecipação da tutela penal, com punição autónoma para …*quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as ações não autorizadas.*…para o cometimento do crime principal (Dano informático) previsto no nº1 do art.º 4º.

Neste caso o bem jurídico protegido é o património do lesado. Nessa medida este crime dependerá de queixa, sendo um crime semipúblico. Exceto no caso de o dano ser de «valor consideravelmente elevado», caso em que se dispensa a necessidade de queixa-crime para o procedimento criminal, sendo então um crime público (n.º 4 e 5). Neste caso, considera-se que, se o dano atingir determinados valores há um risco de perturbação da paz social e da confiança das pessoas na segurança jurídica e, no caso, na fiabilidade dos meios eletrónicos, motivo pelo qual se considera haver um interesse público essencial em agir criminalmente.

A "Sabotagem informática"

Artigo 5.º

Sabotagem informática

1. *Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, entravar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático, através da introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento do acesso ou supressão de programas ou outros dados informáticos ou de qualquer outra forma de interferência em sistema informático, é punido com pena de prisão até 5 anos ou com pena de multa até 600 dias.*
2. *Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as ações não autorizadas descritas no número anterior.*
3. *Nos casos previstos no número anterior, a tentativa não é punível.*
4. *A pena é de prisão de 1 a 5 anos se o dano emergente da perturbação for de valor elevado.*
5. *A pena é de prisão de 1 a 10 anos se:*
   a) *O dano emergente da perturbação for de valor consideravelmente elevado;*
   b) *A perturbação causada atingir de forma grave ou duradoura um sistema informático que apoie uma atividade destinada a assegurar funções sociais críticas, nomeadamente as cadeias de abastecimento, a saúde, a segurança e o bem-estar económico das pessoas, ou o funcionamento regular dos serviços públicos.*

O crime de sabotagem informática constitui uma agravação do crime de dano, uma vez que, com o mesmo tipo de ações o seu autor pretende agora "*entravar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático*.

O legislador com a sua autonomização, não só prevê os danos a dados, mas também, atende aos prejuízos que possam advir da interferência no funcionamento de um conjunto de equipamentos interligados, quase sempre destinados a assegurar o normal funcionamento de serviços e bens públicos.

Prevê-se ainda um agravamento quando estão em causa sistemas informáticos de apoio aos serviços de emergência médica, sistemas automatizados de regulação de trânsito ou sistemas de comunicação bancária.

No caso, o bem jurídico protegido é a segurança dos sistemas e comunicações eletrónicas, havendo por isso, um interesse essencial do Estado em agir criminalmente. Razão pela qual este crime não depende de queixa para o prosseguimento do procedimento criminal, sendo um crime público.

Entre o tipo legal previsto neste artigo 5º e o previsto no artigo 4º subsistem duas distinções essenciais:

Por um lado, o elemento objetivo do "Dano relativo a dados ou programas informáticos" é mais restrito que o protegido pela "Sabotagem informática" que para além da proteção de "dados e programa informáticos" visa proteger o «funcionamento de um sistema informático ou de comunicação de dados à distância».

Por outro lado, o elemento subjetivo do artigo 5º exige que o agente atue «com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo para si ou para terceiros», enquanto no crime de "Sabotagem informática" para a tipificação legal basta que agente atue «com intenção de entravar ou

perturbar o funcionamento», não se exigindo a específica intenção de prejuízo ou benefício ilegítimos. Sendo por isso mais abrangente.

O "Acesso ilegítimo"

Artigo 6.º

Acesso ilegítimo

1. *Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.*
2. *Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as ações não autorizadas descritas no número anterior.*
3. *A pena é de prisão até 3 anos ou multa se o acesso for conseguido através de violação de regras de segurança.*
4. *A pena é de prisão de 1 a 5 anos quando:*
    a) *Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei; ou*
    b) *O benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado.*
5. *A tentativa é punível, salvo nos casos previstos no n.º 2.*
6. *Nos casos previstos nos n.os 1, 3 e 5 o procedimento penal depende de queixa.*

No crime de acesso ilegítimo, faz-se alusão ao "domicílio informático" e pretende-se com isto, identificar e individualizar a " *segurança dos sistemas informáticas*", como o bem jurídico a proteger.

O crime de acesso ilegítimo, vulgarmente designado de intrusão informática, é uma previsão complementar ao crime de sabotagem informática, na medida em que antecipa a proteção dos sistemas informáticos, antes mesmo de se verificarem alterações no seu normal funcionamento ou nos dados que nele se encontrem armazenados. O âmbito da previsão contida neste artº6 é pois "*a proteção da segurança e o impedimento de ataques aos sistemas e redes informáticas*".

Ao contrário da anterior lei que impunha a " *intenção do agente em alcançar, para si ou para outrem, um benefício ou vantagem ilegítimos"* para punir a conduta, a atual lei pune o acesso seja qual for a intenção ou mesmo que não haja qualquer intenção. Enquadram-se nestes casos, aqueles em que o seu autor apenas queria "testar" os seus conhecimentos de hacking ou reclamar os louros de ter quebrado as proteções de determinado sistema.

À semelhança dos artigos anteriores também o crime de acesso ilegítimo contém uma norma de antecipação de tutela penal e que encontra previsão no nº2 do art.º 6º, punindo autonomamente, *…quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as ações não autorizadas….*

O termo "acesso ilegítimo" abrange basicamente a infração relativa às ameaças à segurança (confidencialidade, integridade e disponibilidade) dos sistemas informáticos. O meio mais viável de prevenção do acesso não autorizado é, indubitavelmente, a introdução e o desenvolvimento de medidas de segurança eficazes.

Neste caso, o bem jurídico protegido é o património do lesado e a segurança dos sistemas informáticos. Nessa medida este crime dependerá de queixa, sendo um crime semipúblico.

Exceto nos casos em que através do acesso ilegítimo, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei ou «o benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado», em que se dispensa a necessidade de queixa-crime para o procedimento criminal, sendo então um crime público. Nestes casos, outros valores públicos se levantam que justificam o interesse do Estado em agir criminalmente: a defesa da "concorrência" e da liberdade de comércio, a proteção um "Direito, Liberdade e Garantia", ou ainda a proteção da segurança jurídica quando estão em causa valores elevados.

A "Interceção ilegítima"

Artigo 7.º

Interceção ilegítima

1. *Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, e através de meios técnicos, intercetar transmissões de dados informáticos que se processam no interior de um sistema informático, a ele destinadas ou dele provenientes, é punido com pena de prisão até 3 anos ou com pena de multa.*
2. *A tentativa é punível.*
3. *Incorre na mesma pena prevista no n.º 1 quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as ações não autorizadas descritas no mesmo número.*

Este artigo procura enquadrar aquelas condutas a que normalmente se designam por espionagem informática. Visa proteger o direito à privacidade, o direito à exclusividade na comunicação de dados, e num segundo patamar almeja a segurança dos sistemas informáticos e de comunicações.

O nº2 do art.º 7, contém também, a antecipação da tutela penal aplicado a dispositivos, programas ou outros dados informáticos que tenham por finalidade o favorecimento do crime.

A interceção ilegítima tem o intuito de proteger o direito à privacidade na comunicação de dados. Esta infração é aplicada a todas as formas de transferência eletrónica de dados, quer se trate de uma transferência por telefone, fax, correio eletrónico ou ficheiro. A infração aplica-se a transmissões "não-públicas" de dados informatizados. O termo "não-públicas" delimita a natureza da comunicação e não a natureza dos dados transmitidos. Os dados comunicados poderão constituir informação disponível ao público, mas as partes desejarem comunicar confidencialmente. Ou os dados poderão ser mantidos em sigilo, para fins comerciais, até que o serviço seja remunerado.

Desta forma, o termo "não-públicas" não exclui as redes públicas.

Aqui o bem jurídico protegido é a segurança e privacidade das comunicações eletrónicas, havendo por isso, um interesse essencial do Estado em agir criminalmente. Por isso, este crime não depende de queixa para o prosseguimento do procedimento criminal, sendo um crime público.

A "Reprodução ilegítima de programa protegido"

Artigo 8.º

Reprodução ilegítima de programa protegido

1. *Quem ilegitimamente reproduzir, divulgar ou comunicar ao público um programa informático protegido por lei é punido com pena de prisão até 3 anos ou com pena de multa.*
2. *Na mesma pena incorre quem ilegitimamente reproduzir topografia de um produto semicondutor ou a explorar comercialmente ou importar, para estes fins, uma topografia ou um produto semicondutor fabricado a partir dessa topografia.*
3. *A tentativa é punível.*

Para a análise do presente artigo, dever-se-á ter presente o DL-252/94, de 20 de Outubro[36], exclusivamente dedicado à proteção jurídica dos programas de computador e que transpõe para a ordem jurídica interna a Diretiva n.º 91/250/CEE, do Conselho, de 14 de Maio, sendo importante neste contexto o expressado no seu artigo 14º que diz que, "um programa de computador é penalmente protegido contra a reprodução não autorizada".

Uma segunda questão prende-se com a análise das ações necessárias para o cometimento do crime, "…*reproduzir, divulgar ou comunicar ao público*", cujo entendimento maioritário vai pela aplicação não cumulativa das ações.

Quanto aos interesses protegidos, estes estão directamente ligados à propriedade intelectual, garantindo-se direitos de criação de programas e do seu uso, algo que naturalmente implica direitos patrimoniais.

Um dos aspetos a ter sempre em conta em empresas produtoras de *software* é a propriedade intelectual dos programas desenvolvidos e de como a sua proteção está devidamente comtemplada nos contratos de trabalho dos seus colaboradores, sob pena de estes poderem vir a desenvolver os mesmos programas, módulos ou rotinas numa empresa concorrente.

Este aspeto é muito importante e deve ser mitigado também com políticas adequadas de segurança do código desenvolvido, uma vez que é muito difícil fazer prova em sede de processo-crime ou outro, de cópia ou plágio de *software*.

O artigo 14º do Decreto-lei nº 252/94, de 20/10[37], que regula a proteção jurídica de programas de computador, dispõe expressamente que quanto à tutela penal dos programas de computador lhes é aplicável o disposto no n.º 1 do presente artigo.

Embora o bem protegido seja um direito privado, entendeu-se que existe um interesse essencial do Estado em proteger os criadores intelectuais e se justificava o interesse do Estado em agir criminalmente contra a violação de direitos desta natureza. Assim, este crime não depende de queixa, sendo um crime público.

As disposições processuais

As normas processuais penais definem as regras de funcionamento do sistema penal, desde a investigação criminal até aos recursos dos julgamentos.

É nestas normas que vamos encontrar as regras para a recolha, apreensão e produção de prova para que estas sejam admissíveis em sede de julgamento. Este aspeto é muito importante para saber como agir dentro da lei, quando se recolhe e preserva prova digital, bem como para saber como agir quando se é alvo de uma busca judiciária, realidade a que um responsável por um sistema informático pode estar sujeito, no âmbito das suas responsabilidades.

Os artigos constantes do capítulo III da Lei 109/2009 de 15 de Setembro, enumeram um conjunto de medidas processuais, que tendo em conta as características do ambiente digital, inovam em relação ao Código de Processo Penal e trazem alterações importantes para os regimes de apreensão e meios de obtenção de prova.

Assim, temos:

1. Criação de regimes próprios de preservação e meios de obtenção de prova relacionados com dados informáticos, (art.º12º a 15º);
2. Criação de especificidades quanto á apreensão de dados informáticos, correio eletrónico e registos de comunicações de natureza semelhante, (art.º15º a 17º);
3. Alargamento dos regimes jurídicos de interceções de comunicações e de ações encobertas, (art.º15º e 16º)

A evolução tecnológica abriu novas áreas de ação para a atividade criminal e esta realidade é transversal às diversas formas de cometimento de crime que envolvem a informática, seja ela, instrumento, alvo ou suporte.

Os maiores desafios nesta área criminal, são:

1. A necessidade e dificuldade de identificação dos autores dos crimes praticados nas redes de comunicação e/ou sistemas informáticos,
2. A prova é extremamente volátil;
3. A rapidez de intervenção é um fator essencial para o êxito da investigação;

Estas medidas constituem um avanço significativo na adaptação das leis processuais penais á nova realidade criminal, dotando a investigação de meios capazes ao seu combate.

O capítulo das disposições processuais começa com uma norma de âmbito geral, que define o âmbito de aplicação das disposições processuais.

Trata-se de uma norma de extrema importância, que permite pela primeira vez a investigação de determinados crimes, completamente dependentes de dados informáticos, e que são:

1. *Os crimes informáticos e previstos nesta lei 109/2009*
2. *Os crimes cometidos por meio de um sistema informático, ou*
3. *Em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico.*

Com a entrada em vigor da Lei nº 32/2008 de 17 de Julho, os prestadores do serviço de acesso à Internet passaram a guardar os dados informáticos, mas a sua utilização estava reservada á

investigação dos chamados "crimes graves", em cuja formulação e catálogo não cabia nenhum crime informático ou de natureza informática.

Esta realidade veio a ser colmatada pela entrada em vigor da Lei 109/2009, ficando definido no seu artigo 11º:

Artigo 11.º

Âmbito de aplicação das disposições processuais

1. *Com exceção do disposto nos artigos 18.º e 19.º, as disposições processuais previstas no presente capítulo aplicam-se a processos relativos a crimes:*
    a) *Previstos na presente lei;*
    b) *Cometidos por meio de um sistema informático; ou*
    c) *Em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico.*
2. *As disposições processuais previstas no presente capítulo não prejudicam o regime da Lei n.º 32/2008, de 17 de Julho.*

É importante assinalar que ao prever a preservação dos dados de tráfego em termos criminais, estão excluídas todas as situações que caiem no âmbito de matéria cível, de trabalho ou de regulação do poder paternal, para dar alguns exemplos.

Analisemos agora, algumas particularidades das medidas processuais previstas na lei do Cibercrime.

A "Preservação expedita de dados"

Artigo 12.º

Preservação expedita de dados

1. *Se no decurso do processo for necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos armazenados num sistema informático, incluindo dados de tráfego, em relação aos quais haja receio de que possam perder-se, alterar-se ou deixar de estar disponíveis, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que preserve os dados em causa.*
2. *A preservação pode também ser ordenada pelo órgão de polícia criminal mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora, devendo aquele, neste último caso, dar notícia imediata do facto à autoridade judiciária e transmitir-lhe o relatório previsto no artigo 253.º do Código de Processo Penal.*
3. *A ordem de preservação discrimina, sob pena de nulidade:*
    a) *A natureza dos dados;*
    b) *A sua origem e destino, se forem conhecidos; e*
    c) *O período de tempo pelo qual deverão ser preservados, até um máximo de três meses.*
4. *Em cumprimento de ordem de preservação que lhe seja dirigida, quem tenha disponibilidade ou controlo sobre esses dados, designadamente o fornecedor de serviço, preserva de imediato os dados em causa, protegendo e conservando a sua integridade pelo tempo fixado, de modo a permitir à autoridade judiciária competente a sua obtenção, e fica obrigado a assegurar a confidencialidade da aplicação da medida processual.*
5. *A autoridade judiciária competente pode ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea c) do n.º 3, desde que se verifiquem os respetivos requisitos de admissibilidade, até ao limite máximo de um ano.*

A preservação expedita de dados só pode ter uma leitura correta, se integrada e harmonizada com o regime da Lei 32/2008 de 17 de Julho, que transpõe para a ordem jurídica interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados

gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações.

A medida da preservação expedita apenas é aplicável aos dados que por força desta lei 32/2008, já estejam armazenados pelos fornecedores de serviços e cujo prazo máximo de armazenamento está fixado num ano.

Desta forma e com recurso a esta medida, encontra-se excluída a possibilidade de recolha de dados em tempo real ou relativos a comunicações futuras, cujo regime é equiparado á interceção de comunicações e tratado no artº18.

Mas a interpretação do conceito de dados utilizado na epigrafe do presente artigo remete também para as definições constantes pelo art.º 2 al. b) e c), parecendo não haver dúvidas que para efeitos de aplicação desta Lei do cibercrime, as definições a ter em conta são as de «dados informáticos» e «dados de tráfego», na formulação daquele artigo.

Esta questão assume maior relevância a propósito da determinação da autoridade competente para a preservação ou obtenção dos dados, a qual contém especificidades.

Ao abrigo do nº1 do art.º12, a preservação dos dados informáticos pode ser ordenada pela autoridade judiciária competente em cada fase do processo, querendo isto dizer, que o Ministério Público o será em fase de inquérito e o Juiz de Instrução na fase de instrução e julgamento.

Sempre que haja autorização da autoridade judiciária, urgência ou perigo na demora, pode também a Policia Judiciária, como órgão de polícia criminal competente para a investigação, no âmbito das medidas cautelares, ordenar a preservação de dados, seguindo-se-lhe a transmissão previsto no art.º253 do CPP.

Quanto ao nº4 deste art.º 12, a norma reforça a responsabilidade que impende sobre quem tem a disponibilidade ou controlo dos dados em assegurar a sua integridade pelo tempo fixado, aplicando-lhe também a obrigação de confidencialidade. Esta preocupação na manutenção da integridade dos dados, assenta na forte possibilidade dos mesmo poderem constituir uma prova inequívoca de um crime, não devendo estar expostos a manuseamentos ou armazenamentos descuidados.

De salientar ainda que de acordo com a redação utilizada e dada a utilização da expressão "…designadamente o fornecedor de serviço" se estende o âmbito de aplicação a qualquer entidade que pelas suas características e atividade, possa ter este tipo de dados sobre o seu domínio.

Tratando-se de uma medida de acautelamento de prova, a preservação prevista é feita por períodos renováveis de três meses, e até ao limite máximo de um ano, (nº 5).

A "Revelação expedita de dados de tráfego"

Artigo 13.º

Revelação expedita de dados de tráfego

Tendo em vista assegurar a preservação dos dados de tráfego relativos a uma determinada comunicação, independentemente do número de fornecedores de serviço que nela participaram, o fornecedor de serviço a quem essa preservação tenha sido ordenada nos termos do artigo anterior indica à autoridade judiciária ou ao órgão de polícia criminal, logo que o souber, outros fornecedores de serviço através dos quais aquela comunicação tenha sido efetuada, tendo em vista permitir identificar todos os fornecedores de serviço e a via através da qual aquela comunicação foi efetuada.

Para garantir que todos os dados de tráfego são preservados e que os mesmos são fiáveis na determinação da origem e destino de uma comunicação, sobre os fornecedores de serviços, impende o dever de identificar eventuais outros operadores que tenham intervindo na comunicação. Uma vez identificado um dos operadores que tenha intervindo na comunicação, a este compete identificar todos os outros que nela tenham participado.

Neste clausulado estão enquadradas as situações de subalugueres de *ranges* de endereços IP.

A "Injunção para apresentação ou concessão do acesso a dados"

Artigo 14.º

Injunção para apresentação ou concessão do acesso a dados

1. *Se no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados que os comunique ao processo ou que permita o acesso aos mesmos, sob pena de punição por desobediência.*
2. *A ordem referida no número anterior identifica os dados em causa.*
3. *Em cumprimento da ordem descrita nos nºs 1 e 2, quem tenha disponibilidade ou controlo desses dados comunica esses dados à autoridade judiciária competente ou permite, sob pena de punição por desobediência, o acesso ao sistema informático onde os mesmos estão armazenados.*
4. *O disposto no presente artigo é aplicável a fornecedores de serviço, a quem pode ser ordenado que comuniquem ao processo dados relativos aos seus clientes ou assinantes, neles se incluindo qualquer informação diferente dos dados relativos ao tráfego ou ao conteúdo, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida pelo fornecedor de serviços, e que permita determinar:*
    a) *O tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço;*
    b) *A identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à faturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços; ou*
    c) *Qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços.*
5. *A injunção prevista no presente artigo não pode ser dirigida a suspeito ou arguido nesse processo.*

6. *Não pode igualmente fazer-se uso da injunção prevista neste artigo quanto a sistemas informáticos utilizados para o exercício da advocacia, das atividades médica e bancária e da profissão de jornalista.*
7. *O regime de segredo profissional ou de funcionário e de segredo de Estado previsto no artigo 182.º do Código de Processo Penal é aplicável com as necessárias adaptações.*

O presente artigo estabelece o regime de obtenção dos dados para efeitos de investigação criminal com aplicação exclusiva em sede de inquérito, sendo, por isso, afastada, qualquer possibilidade da sua utilização para efeitos de prevenção criminal.

À semelhança do regime da preservação expedita de dados do art.º12, o regime da obtenção desses dados previsto no art.º 14, sob a epígrafe (Injunção para apresentação ou concessão do acesso a dados), é um meio de obtenção de prova direcionado a entidades que pela sua natureza, salvo raras exceções, exercem funções no sector das comunicações eletrónicas, e integrados no conceito de "fornecedores de serviços".

A obtenção dos dados de acordo com o disposto nos nºs 1 e 3 pode ocorrer de duas formas:

a) Entrega voluntária por parte de quem tenha a sua disponibilidade, ou;

b) Permissão de acesso ao sistema informático onde os mesmos estão armazenados.

Pressupõe-se a colaboração efetiva de quem tem a disponibilidade ou o controlo desses dados, e em caso de incumprimento, é-lhe cominada a prática do crime de desobediência. Quer isto dizer que na falta de colaboração por parte de uma destas entidades, que o caminho a seguir seriam as buscas e pesquisas.

Sobre quem seja a autoridade judiciária competente para ordenar a entrega dos dados, e tendo presente o conceito de "dados de tráfego" fornecida pelo art.º2 al. c), " …*os dados informáticos relacionados com uma comunicação efetuada por meio de um sistema informático, gerados por este sistema como elemento de uma comunicação, indicando a origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo de serviço subjacente."*, o nº 4 do art.º14, define que estes dados de tráfego e os dados de conteúdo, só podem ser solicitados pelo juiz, em qualquer fase do processo.

Quer isto dizer á contrário, que todos os outros tipos de dados informáticos em que se incluem os das alíneas a), b) e c), do nº 4 do art.º 4, e que sejam necessários para a investigação, produção de prova e tendo em vista a descoberta da verdade, podem e devem ser solicitados por ordem do Ministério Publico, como autoridade judiciária competente na fase de inquérito, designadamente os que permitam determinar:

> *a) O tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço;*
>
> *b) A identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à faturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços; ou*
>
> *c) Qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços.*

A Lei 41/2004 de 18/08 e a Lei 32/2008 de 17/08, sofrem aqui derrogações e exceções importantes, atento o carácter excecional das medidas processuais implementadas pela Lei 109/2009 de 15 de Setembro.

Quanto às disposições contidas nos nºs 5, 6 do art.º14, as mesmas constituem limitações de aplicação da injunção, determinando que a solicitação para obtenção de dados, não pode ser dirigida a suspeito ou arguido nesse processo, nem em caso algum, a sistemas informáticos utilizados no exercício da advocacia, medicina, atividade bancária, ou jornalismo.

Com as necessárias adaptações, é também aplicável o regime de segredo profissional, de funcionário e de Estado, previsto no art.º182 do CPP.

A "Pesquisa de dados informáticos"

Artigo 15.º

Pesquisa de dados informáticos

1. *Quando no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente autoriza ou ordena por despacho que se proceda a uma pesquisa nesse sistema informático, devendo, sempre que possível, presidir à diligência.*
2. *O despacho previsto no número anterior tem um prazo de validade máximo de 30 dias, sob pena de nulidade.*
3. *O órgão de polícia criminal pode proceder à pesquisa, sem prévia autorização da autoridade judiciária, quando:*
    a. *A mesma for voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado fique, por qualquer forma, documentado;*
    b. *Nos casos de terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa.*
4. *Quando o órgão de polícia criminal proceder à pesquisa nos termos do número anterior:*
    a) *No caso previsto na alínea b), a realização da diligência é, sob pena de nulidade, imediatamente comunicada à autoridade judiciária competente e por esta apreciada em ordem à sua validação;*
    b) *Em qualquer caso, é elaborado e remetido à autoridade judiciária competente o relatório previsto no artigo 253.º do Código de Processo Penal.*
5. *Quando, no decurso de pesquisa, surgirem razões para crer que os dados procurados se encontram noutro sistema informático, ou numa parte diferente do sistema pesquisado, mas que tais dados são legitimamente acessíveis a partir do sistema inicial, a pesquisa pode ser estendida mediante autorização ou ordem da autoridade competente, nos termos dos n.os 1 e 2.*
6. *À pesquisa a que se refere este artigo são aplicáveis, com as necessárias adaptações, as regras de execução das buscas previstas no Código de Processo*
7. *Penal e no Estatuto do Jornalista.*

A pesquisa de dados informáticos também poderia chamar-se de "*busca de dados informáticos*" uma vez que esta medida processual é de facto um meio de obtenção de prova em tudo equiparável ao regime das buscas existente no CPP.

À partida, o regime das buscas abrange por si só a possibilidade de apreensão de meios e dados informáticos conferindo ao OPC que os apreende o poder de tomar conta e conhecimento do seu conteúdo.

Por se tratar de uma especificidade em relação ao regime das buscas merece destaque a possibilidade de pesquisa em sistemas remotos, que se encontra prevista no n.º5 do art.º15 e que pretende contemplar desde as situações de sistemas de armazenamento em "cloud" até ao caso de uma simples *drive* remota.

Devido à interconexão dos sistemas informáticos é cada vez mais frequente que os dados possam estar armazenados em locais diferentes do buscado, mas acessíveis a partir do sistema informático.

A lei prevê e alarga a pesquisa ao sistema no qual os dados efetivamente se encontram armazenados ou da extração dos dados para o sistema que está a ser alvo de pesquisa. Em todo o caso esta pesquisa adicional tem sempre que ser autorizada pela autoridade judiciária competente.

Este aspeto é importante ter sempre em conta nas situações em que a organização também é alvo de busca e há que acautelar que todos os preceitos legais estão a ser cumpridos.

A "Apreensão de dados informáticos"

Artigo 16.º

Apreensão de dados informáticos

1. *Quando, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem encontrados dados ou documentos informáticos necessários à produção de prova, tendo em vista a descoberta da verdade, a autoridade judiciária competente autoriza ou ordena por despacho a apreensão dos mesmos.*
2. *O órgão de polícia criminal pode efetuar apreensões, sem prévia autorização da autoridade judiciária, no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo anterior, bem como quando haja urgência ou perigo na demora.*
3. *Caso sejam apreendidos dados ou documentos informáticos cujo conteúdo seja suscetível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respetivo titular ou de terceiro, sob pena de nulidade esses dados ou documentos são apresentados ao juiz, que ponderará a sua junção aos autos tendo em conta os interesses do caso concreto.*
4. *As apreensões efetuadas por órgão de polícia criminal são sempre sujeitas a validação pela autoridade judiciária, no prazo máximo de 72 horas.*
5. *As apreensões relativas a sistemas informáticos utilizados para o exercício da advocacia e das atividades médicas e bancária estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas no Código de Processo Penal e as relativas a sistemas informáticos utilizados para o exercício da profissão de jornalista estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas no Estatuto do Jornalista.*
6. *O regime de segredo profissional ou de funcionário e de segredo de Estado previsto no artigo 182.º do Código de Processo Penal é aplicável com as necessárias adaptações.*
7. *A apreensão de dados informáticos, consoante seja mais adequado e proporcional, tendo em conta os interesses do caso concreto, pode, nomeadamente, revestir as formas seguintes:*
    a) *Apreensão do suporte onde está instalado o sistema ou apreensão do suporte onde estão armazenados os dados informáticos, bem como dos dispositivos necessários à respetiva leitura;*
    b) *Realização de uma cópia dos dados, em suporte autónomo, que será junto ao processo;*
    c) *Preservação, por meios tecnológicos, da integridade dos dados, sem realização de cópia nem remoção dos mesmos; ou*

d) Eliminação não reversível ou bloqueio do acesso aos dados.

8. *No caso da apreensão efetuada nos termos da alínea b) do número anterior, a cópia é efetuada em duplicado, sendo uma das cópias selada e confiada ao secretário judicial dos serviços onde o processo correr os seus termos e, se tal for tecnicamente possível, os dados apreendidos são certificados por meio de assinatura digital.*

Seguindo o regime das apreensões do Código de Processo Penal, o presente artigo contém um conjunto de disposições procedimentais importantes para a apreensão de dados informáticos, destacando-se:

- A limitação ao conhecimento dos dados, prevista no nº3, sempre que em causa possam estar dados pessoais ou íntimos e que possam pôr em causa a privacidade do respetivo titular ou de terceiro, obrigando a que seja o juiz a primeira pessoa a ter conhecimento dos mesmos e a decidir do seu interesse para os autos;
- Os regimes especiais consagrados no nº5 (advocacia, atividades médicas e bancária e jornalistas);
- Dadas as modalidades de apreensões previstas no nº7 e tratando-se de uma opção a aplicar ao caso concreto, dever-se-á ter sempre em conta o tipo de exame ou perícia que sobre os mesmo dados irá recair.
- E finalmente uma chamada de atenção para os procedimento contidos no nº8 do art.º, sempre que se opta pela apreensão de uma cópia de dados.

A "Apreensão de correio eletrónico e registos de comunicações de natureza semelhante"

Artigo 17.º

Apreensão de correio eletrónico e registos de comunicações de natureza semelhante

Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio eletrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal.

O presente regime é em tudo idêntico ao da apreensão de correspondência previsto no art.º 179 do CPP e para o qual nos remete.

As principais questões colocam-se ao nível da execução de apreensão, sabendo-se que, normalmente, além de correio eletrónico são também apreendidos outros tipos de dados informáticos. Nestas situações, durante a apreensão, deverá desde logo proceder-se á individualização de dados que constituam comunicações e que permita que possa ser o Juiz a primeira pessoa a tomar conta do seu conteúdo e avaliar do seu interesse para os autos.

Se esta individualização não for possível durante a apreensão, casos por exemplo em que se procede á apreensão de suportes informáticos, o procedimento em relação ao correio eletrónico, deverá ser

tido em conta aquando da realização do exame ou perícia ao material informático, sob pena de se incorrer num crime de violação de correspondência.

A "Interceção de comunicações"

Artigo 18.º

Interceção de comunicações

1. *É admissível o recurso à interceção de comunicações em processos relativos a crimes:*
   a) *Previstos na presente lei; ou*
   b) *Cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico, quando tais crimes se encontrem previstos no artigo 187.º do Código de Processo Penal.*
2. *A interceção e o registo de transmissões de dados informáticos só podem ser autorizados durante o inquérito, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público.*
3. *A interceção pode destinar-se ao registo de dados relativos ao conteúdo das comunicações ou visar apenas a recolha e registo de dados de tráfego, devendo o despacho referido no número anterior especificar o respetivo âmbito, de acordo com as necessidades concretas da investigação.*
4. *Em tudo o que não for contrariado pelo presente artigo, à interceção e registo de transmissões de dados informáticos é aplicável o regime da interceção e gravação de conversações ou comunicações telefónicas constante dos artigos 187.º, 188.º e 190.º do Código de Processo Penal.*

Sem a abrangência das outras medidas processuais que antecederam, o regime das interceções de comunicações aqui previsto, constitui-se como um novo instrumento e avanço significativo nas possibilidades de investigação, possibilitando que se aplique não só aos crimes previstos no art.º 187 do CPP, mas também aos crimes "ditos informáticos" e previstos nesta lei 109/2009: (Falsidade informática); (Dano relativo a programas ou outros dados informáticos); (Sabotagem informática); (Acesso ilegítimo); (Interceção ilegítima); (Reprodução ilegítima de programa protegido).

De salientar, que o crime de burla informática e nas comunicações, p e p pelo art.º221 do C. Penal, tratando-se de um crime informático, se encontra excluído desta possibilidade.

A interceção aqui prevista está direcionada para a recolha de dados informáticos em tempo real. Estes dados podem ser "dados de tráfego" ou também "dados de conteúdo", associados a comunicações específicas e transmitidos num determinado sistema informático. Consoante as necessidades da investigação, devem ser especificados o tipo de dados que se pretendem intercetar.

As "Ações encobertas"

Artigo 19.º

Ações encobertas

1. *É admissível o recurso às ações encobertas previstas na Lei n.º 101/2001, de 25 de Agosto, nos termos aí previstos, no decurso de inquérito relativo aos seguintes crimes:*
   a) *Os previstos na presente lei;*

b) Os cometidos por meio de um sistema informático, quando lhes corresponda, em abstrato, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, a discriminação racial, religiosa ou sexual, as infrações económico-financeiras, bem como os crimes consagrados no título IV do Código do Direito de Autor e dos Direitos Conexos.

2. Sendo necessário o recurso a meios e dispositivos informáticos observam-se, naquilo que for aplicável, as regras previstas para a interceção de comunicações.

A presente disposição constitui também, um alargamento do regime jurídico das ações encobertas previstas na Lei n.º 101/2001, de 25 de Agosto, as quais passam a ser permitidas como meio de obtenção de prova para a investigação dos seguintes crimes:

- Falsidade informática;
- Dano relativo a programas ou outros dados informáticos;
- Sabotagem informática;
- Acesso ilegítimo;
- Interceção ilegítima;
- Reprodução ilegítima de programa protegido;
- Os cometidos por meio de um sistema informático, quando lhes corresponda, em abstrato, pena de prisão de máximo superior a 5 anos;
- E ainda, sendo dolosos:
  - Os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes;
  - A burla qualificada;
  - A burla informática e nas comunicações;
  - A discriminação racial, religiosa ou sexual;
  - As infrações económico-financeiras, e
  - Os crimes consagrados no título IV do Código do Direito de Autor e dos Direitos Conexos.

Cooperação Internacional ao abrigo da lei nº 109/2009

Faz-se aqui uma breve abordagem a este aspeto da Lei, apenas para assinalar a existência de mecanismos de cooperação internacional, que permitem a investigação de crimes que não olham a fronteiras administrativas.

Em matéria de cooperação internacional e dada a necessidade de intervenção urgente na recolha de prova digital, a lei 109/2009 de 15 de Setembro, constituiu-se como um instrumento próprio de cooperação, relativo a crimes relacionados com sistemas ou dados informáticos, e cujo objetivo principal é "*Propiciar e facilitar, um regime mais eficaz de cooperação internacional*"

As disposições principais são:

1. Criação de um ponto de contacto permanente «Rede 24/7» (24 horas 7 dias por semana), (art.º 21º);

Tem na base a organização e centralização de outros centros de contacto, com o objetivo operacional de combate ao crime informático, nomeadamente quanto à obtenção dos dados de tráfego e é assegurado pela Polícia Judiciária em Portugal.

8.5 Código Penal - Lei n.º 59/2007 de 4 de Setembro

A "Devassa por meio de informática"

Artigo 193.º

Devassa por meio de informática

1. *Quem criar, mantiver ou utilizar ficheiro automatizado de dados individualmente identificáveis e referentes a convicções políticas, religiosas ou filosóficas, à filiação partidária ou sindical, à vida privada, ou a origem étnica, é punido com pena de prisão até dois anos ou com pena de multa até 240 dias.*
2. *A tentativa é punível.*

A criminalização destas práticas é decorrente do disposto no artigo 35º n.º 3 da Constituição da República Portuguesa, e visa proteger a reserva da vida privada contra possíveis atos de discriminação que a utilização de meios informáticos torna exponencialmente perigosos.

Artigo 35.º

(Utilização da informática)

1. *Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.*
2. *A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente.*
3. *A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.*
4. *É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei.*
5. *É proibida a atribuição de um número nacional único aos cidadãos.*
6. *A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.*
7. *Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei.*

Razão pela qual o procedimento criminal relativamente ao crime previsto neste artigo 193ºnão depende de queixa. É assim, um crime público, sobre o qual o Estado terá sempre interesse e dever de agir.

No tipo legal da "devassa por meio de informática" encontramos não só os atos de criação de ficheiros violadores do "Bem" protegido, mas também os meros atos de conservação e utilização desse ficheiro, ainda que sem qualquer comparticipação na sua criação. O tipo legal é assim bastante

abrangente quanto às condutas penalizadas, o que pretende ser um facto dissuasor face à dificuldade de prova do "autor" material do ficheiro. No mesmo sentido se penaliza a mera tentativa.

A "Violação de correspondência ou de telecomunicações"

Artigo 194.º

Violação de correspondência ou de telecomunicações

1. Quem, sem consentimento, abrir encomenda, carta ou qualquer outro escrito que se encontre fechado e lhe não seja dirigido, ou tomar conhecimento, por processos técnicos, do seu conteúdo, ou impedir, por qualquer modo, que seja recebido pelo destinatário, é punido com pena de prisão até um ano ou com pena de multa até 240 dias.
2. Na mesma pena incorre quem, sem consentimento, se intrometer no conteúdo de telecomunicação ou dele tomar conhecimento.
3. Quem, sem consentimento, divulgar o conteúdo de cartas, encomendas, escritos fechados, ou telecomunicações a que se referem os números anteriores, é punido com pena de prisão até um ano ou com pena de multa até240 dias.

Este artigo é directamente aplicável à correspondência eletrónica - via e-mail -, que é modernamente perfeitamente equiparável à correspondência postal fechada. O bem que se protege é aqui não só a privacidade mas também a confiança da comunidade na integridade dos meios de comunicação, nomeadamente das telecomunicações.

Coloca-se a questão de saber se este crime não se encontra absorvido pelo crime de "interceção ilegítima", previsto pelo artigo 7º da Lei 109/2009. Embora possa existir sobreposição quando a interceção da mensagem se dá durante a sua transmissão, já não haverá quando o acesso à mensagem se dá depois de esta ter sido já rececionada pelo seu destinatário, encontrando-se guardada na sua caixa de correio eletrónico. Embora, neste último caso, também se pudesse afirmar que estamos perante um crime de "acesso ilegítimo" previsto pelo artigo 6º da Lei 109/91, entendemos não sero caso, desde logo porque este crime exige uma especial intenção: "e com a intenção de alcançar, para si ou para outrem, um benefício ou vantagem ilegítimos", que o crime de "violação de correspondência ou de telecomunicações" não exige. Não se justificaria, assim, que uma correspondência fechada eletrónica, depois de rececionada, ficasse menos protegida que a correspondência em papel.

A "Burla Informática e nas Comunicações"

Artigo 221.º

Burla informática e nas comunicações

1. *Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo patrimonial, interferindo no resultado de tratamento de dados ou mediante estruturação incorreta de programa informático, utilização incorreta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento, é punido com pena de prisão até três anos ou com pena de multa.*
2. *A mesma pena é aplicável a quem, com intenção de obter para si ou para terceiro um benefício ilegítimo, causar a outrem prejuízo patrimonial, usando programas, dispositivos eletrónicos ou outros meios que, separadamente ou em conjunto, se destinem a diminuir, alterar ou impedir, total ou parcialmente, o normal funcionamento ou exploração de serviços de telecomunicações.*
3. *A tentativa é punível.*
4. *O procedimento criminal depende de queixa.*
5. *Se o prejuízo for:*
    a) *De valor elevado, o agente é punido com pena de prisão até cinco anos ou com pena de multa até 600 dias;*
    b) *De valor consideravelmente elevado, o agente é punido com pena de prisão de dois a oito anos.*
6. *É correspondentemente aplicável o disposto no artigo 206.º*

Relativamente à caracterização do crime de burla informática e nas comunicações, em termos de ação, estamos perante um ilícito de execução vinculada, quer isto dizer, que só terá aplicação, uma vez satisfeitas, uma de várias, das seguintes ações:

7. Interferência no resultado de tratamento de dados;
8. Estruturação incorreta de programa informático;
9. Utilização incorreta ou incompleta de dados;
10. Utilização de dados sem autorização ou
11. Intervenção por qualquer outro modo não autorizado no processamento de dados.

Num afastamento claro ao crime de burla, pretende-se restringir a aplicação do artº221, àquelas situações em que o bem jurídico tutelado seja ofendido por ações ou utilizações de meios informáticos.

Este afastamento é também evidente no que concerne à imputação objetiva, porquanto, a burla informática se concretiza numa lesão direta ao património, enquanto no crime de burla do artº217, a afetação do património pressupõe a criação, pelo autor, de um estado de erro sobre a vitima, (artificio fraudulento).

Ou seja, ao contrário do crime de burla, o crime de burla informática não pressupõe a intervenção de uma outra pessoa (vitima ou não), e concretiza-se com a afetação direta do património, pela utilização da informática ou dos seus meios.

O preceito, de natureza exemplificativa, tem na base a ofensa ao património, e está condicionado à utilização de meios que possam interferir com as telecomunicações.

Resta dizer, que o crime do art.º. 221 do Código Penal, é um crime de natureza semipública, um crime doloso, punível na forma tentada e cujas agravações estão condicionadas à clássica escala de valores;

«elevado» e «consideravelmente elevado», algo aliás, que acarreta a alteração da sua natureza para crime público, e o não faz depender de queixa, como na formulação base do crime.

8.6 Lei da Proteção de Dados Pessoais - Lei n.º 67/98, de 26 de Out.

O tema da proteção dos dados pessoais, está indissociavelmente ligado ao artº35 da Constituição da República Portuguesa, mas cuja regulamentação e desenvolvimento é remetido, para legislação específica.

Artigo 35.º

(Utilização da informática)

1. *Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.*
2. *A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente.*
3. *A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.*
4. *É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei.*
5. *É proibida a atribuição de um número nacional único aos cidadãos.*
6. *A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.*
7. *Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei.*

A parte relativa aos crimes está prevista na secção III e compreende os artº43º a 49º.

No art.º 43º, sob a epígrafe "*não cumprimento de obrigações relativas a proteção de dados*" são várias as condutas passíveis de configurar o crime, a saber:

- Omissão da notificação ou do pedido de autorização, nº1 alínea - a);
- Falsas informações, nº1 alínea - b);
- Utilização ilegal de dados; nº1 alínea - c);
- Interconexão ilegal, nº1 alínea - d);
- Não cumprimento das obrigações previstas por lei e dentro do prazo fixado pela CNPD, nº1 alínea – e);
- Manutenção do acesso a redes abertas de transmissão de dados, a responsáveis pelo tratamento de dados pessoais que não cumpram as disposições da presente lei. (pressupõe a violação da notificação feita pela CNPD).

O art.º 44º, prevê o crime de "*acesso indevido*", normalmente associado, mas também confundido, com o crime de Acesso ilegítimo, p. e p. no art.º 7º da Lei da Criminalidade Informática, parecendo no entanto claro, que o que o legislador quis, ao dar-lhes epígrafes diferentes, foi não só individualizar o acesso a dados pessoais, bem como configurar a hipótese de um concurso real de normas, ou seja: o acesso indevido não é uma ação contra o sistema, mas sim contra os dados que ali se encontrem,

podendo-se configurar que o acesso indevido aos dados ocorra como consequência e em concurso com um acesso ilegítimo ao sistema.

O art.º 45 versa sobre a "*viciação ou destruição de dados* " o qual prevê e pune as condutas de "apagar", "destruir", "suprimir", "apagar" e "modificar", dados; não se levantam questões relevantes de interpretação, remete-se contudo para o esclarecimento dos termos, "apagar" e "suprimir", feito acerca do crime falsidade informática a pag-32.

Consideramos que este crime é passível também de concurso real com o crime de acesso ilegítimo do art.º 7 da Lei da Criminalidade Informática.

Quanto aos art.º 46 (Desobediência qualificada), art.º 47 (Violação do dever de sigilo), art.º 48.º (Punição da tentativa), e art.º 49.º (Pena acessória), merece uma referência a disposição do art.º 47, a qual deve ser encarada como norma especial em relação ao art.º 195º do Código Penal, (Violação de segredo).

9 Conclusões e discussão

Foi constatada pelo autor ao longo de vários anos de experiencia profissional, que a preparação, quer de responsáveis e operacionais de sistemas informáticos, quer de juristas que têm de lidar com a prova digital, apresenta insuficiências, o que tem levado muitas vezes à anulação de provas em tribunal por inadmissibilidade legal, no caso dos primeiros ou à não verificação da integridade legal da prova por desconhecimento das suas nuances técnicas, no caso dos segundos.

Têm-se verificado inúmeras situações, em que a não preservação de indícios ou prova digital, tais como logs de acessos a sistemas, leva inevitavelmente ao arquivamento de processos.

O presente documento dá um contributo na mitigação desta lacuna, ajudando uns e outros, através da sistematização de diversos procedimentos na identificação, recolha e preservação da prova digital e detalhando situações como a entrevista ao suspeito, a recolha de cabeçalhos técnicos de correio eletrónico ou a identificação de quem registou determinada página na Internet, para dar apenas alguns exemplos.

Estes procedimentos resultam do levantamento das boas práticas recomendadas por diversos organismos internacionais que lidam com esta temática, tais como o G8, a Comissão Europeia ou a IACIS e tendo em conta a recentemente publicada norma ISO/IEC FDIS 27037:2012, adaptando-as ao ordenamento jurídico português.

9.1 Trabalho futuro

O presente trabalho pretendeu dar resposta às duas primeiras questões da informática forense, a identificação e recolha da prova digital e a sua preservação de forma legalmente admissível. Por outro lado, pretendeu também fazer a sempre difícil ponte entre o mundo técnico e o jurídico, e em particular no enquadramento jurídico-legal português.

A evolução natural para o presente trabalho e tomando-o como ponto de partida, será o levantamento, tratamento e sistematização das boas práticas e normas que regem os dois pontos seguintes da informática forense, a análise e investigação das provas e a apresentação de relatórios ou resultados. Ou seja, depois de ser ter apreendido e preservado a prova digital, há que proceder ao exame forense da mesma e posteriormente à elaboração dos respetivos relatórios forenses, de forma a apresentar os resultados obtidos, de uma forma clara e percetível por técnicos, juristas e todos os demais envolvidos no respetivo processo.

Outra vertente de possível desenvolvimento seria o aprofundamento de alguns dos temas tratados, nomeadamente o desenvolvimento de guias adicionais, à semelhança dos apresentados nos anexos, mas direcionados para outros públicos-alvo. Por exemplo, um guia direcionado para juristas, focado na verificação legal dos procedimentos técnicos no tratamento da prova digital.

Tal como referido na introdução, esta é uma área onde a formação dos técnicos e a dos juristas que têm de lidar com a prova digital é fundamental. Assim sendo, um dos desenvolvimentos possíveis para este trabalho seria a estruturação de módulos de formação adaptados às necessidades de cada um dos grupos alvo.

Anexos

O objetivo foi incluir nos anexos, guias que podem ser facilmente adaptados a manuais de bolso de consulta rápida.

O primeiro é direcionado para primeira resposta. Ou seja, destina-se a ser transformado em guia de consulta rápida com os principais princípios e passos a atender na identificação e recolha da prova digital e é direcionado para qualquer pessoa independentemente dos seus conhecimentos técnicos ou jurídicos, incluindo-se por essa razão um glossário com imagens para fácil identificação de objetos e compreensão de conceitos.

Serão ainda apresentados três fluxogramas que podem ser facilmente adaptados a guias de consulta rápida, para ilustrar de uma forma simples as melhores práticas na recolha de equipamentos eletrónicos.

Anexo I - Guia de primeira resposta

O presente capítulo tem como objetivo fornecer a todos aqueles que têm a responsabilidade de em primeira mão lidar com a preservação de prova digital, um guia auxiliar na aplicação das melhores práticas, na linha das recomendações elaboradas pelos principais organismos que lidam com esta problemática, tais como a IACIS[38], a Interpol, a Europol e de acordo com a ISO 27037.

Este capítulo ao contrário de outros deste documento, está direcionado para qualquer nível de conhecimentos técnicos, atendendo a que nem sempre será um técnico o primeiro a lidar com a prova digital, ainda que não seja esta a situação mais recomendada.

Com este objetivo em mente, o capítulo está organizado de forma a poder ser facilmente adaptado a um guia consulta ou a um *checklist* de tarefas a realizar. No final do capítulo existem também um glossário gráfico para uma consulta mais fácil.

Toda a informação com valor probatório para a investigação criminal, armazenada ou transportada em dispositivos eletrónicos é denominada prova digital e tem em comum as seguintes características:

- É frágil e pode ser facilmente alterada ou destruída. Deve portanto ser tratada com muito cuidado;
- É tão latente como os vestígios de ADN ou as impressões digitais;
- Pode ser facilmente transferida de local, física ou virtualmente, não respeitando nenhum tipo de fronteira;
- É muitas vezes dependente do tempo, isto é da hora e local exato onde foi produzida;

A informação produzida pelos sistemas de informação não é tangível, como a era a produzida antes de estas tecnologias estarem amplamente divulgadas.

As grandes dificuldades que se deparam a quem tem de lidar com a prova digital e a necessidade de a preservar, são:

- A existência de grandes quantidades de informação digital que pode ser criada, modificada, apagada ou removida em poucos segundos e
- Os sistemas de informação têm uma grande variedade, estão em constante evolução e nem sempre têm um especto físico que se assemelha ao que os investigadores reconhecem como dispositivos de armazenamento digital. Podem ser tão diversos como telefones, pagers, agendas, faxes, atendedores de chamadas, consolas de jogos, gravadores de DVD de sala, descodificadores de sinal de televisão/satélite, PENs USB com os mais variados feitios e dissimuladas nos mais diversos aparelhos ou objetos e podem ainda estar armazenadas em drives remotas acessíveis através de redes corporativas ou da Internet.

Este capítulo destina-se essencialmente ao técnico de primeira resposta (*first responder*), ou seja àquele que tem o primeiro contacto com os equipamentos e que pode não ser perito nesta matéria. Destina-se a ajudá-lo a reconhecer, recolher e preservar a prova digital quando não está disponível no local nenhum perito.

Nem sempre o *first responder* tem à sua disposição a assistência de um perito. Tornasse assim necessária a sua formação na correta recolha e preservação da prova digital. A adoção de técnicas e boas práticas, pode minimizar o risco de se perder ou danificar provas essenciais à investigação. O

objetivo é recomendar essas boas práticas, na identificação, recolha, documentação e preservação da prova digital.

Vão ser apresentados os princípios gerais que devem ser seguidos na manipulação da prova digital, a definição dos tipos básicos de recolha e as fases principais do processo de recolha.

Serão ainda enumerados detalhes específicos, quanto ao manuseamento dos vários tipos de equipamentos.

A explicação dos termos utilizados neste capítulo pode ser encontrada no glossário, com fotografias ilustrativas dos diversos tipos de equipamentos que se podem encontrar.

Princípios Gerais

Quando se manuseiam objetos contendo prova digital, importa seguir os seguintes princípios gerais:

- Presença múltipla no cenário;
- Integridade dos dados;
- Registo da cadeia da prova;
- Suporte técnico;
- Formação dos Técnicos;
- Conformidade com as normas legais em vigor.

Presença Múltipla no cenário

Princípio: O técnico que manuseia a prova nunca deve estar sozinho.

Pelo menos, dois técnicos devem estar envolvidos na interação com cada um dos objetos a recolher. Por um lado, vai permitir uma maior proteção jurídico-legal dos técnicos e por outro permitirá uma maior eficácia da recolha, seguindo aqui os princípios gerais das buscas policiais, que determinam que a busca a um determinado local deve ser efetuada por pelo menos duas vezes, por mais do que uma pessoa e em sentido inverso um do outro.

Finalmente e uma vez que "duas cabeças pensam melhor que uma", qualquer dificuldade técnica poderá mais facilmente ser ultrapassada.

Integridade dos Dados

Princípio: Nenhuma ação ou omissão deverá alterar os dispositivos eletrónicos ou o seu conteúdo, garantindo a sua integridade probatória em sede de inquérito criminal ou cível.

Quando se manipulam os dispositivos eletrónicos e os dados, nada deve ser alterado, nem o *hardware* nem o software.
O técnico é responsável pela integridade probatória dos meios de prova recolhidos e este constitui o primeiro passo na cadeia da prova, que a lavará a ter ou não, validade em sede de inquérito criminal ou cível.

Registo da Cadeia da Prova

Princípio: Registar todos os procedimentos executados na interação com os dispositivos eletrónicos.

Uma entidade externa deve poder chegar aos mesmos resultados executando os mesmos procedimentos. Não respeitar esta regra pode comprometer irremediavelmente a validade da prova.
Todas as atividades relacionadas com a recolha, acesso, armazenamento ou transferência da prova digital, devem ser documentada e armazenada para posterior análise.

Caso seja possível, estas informações devem inclusivamente ser registadas no respetivo documento de suporte da ação.
Este registo ajudará ainda o técnico na descrição dos passos tomados aquando da produção da prova em sede de julgamento, que normalmente tem lugar vários anos depois da recolha dos objetos.

Suporte Técnico

Princípio: Se é previsível a recolha de prova digital, no âmbito de uma operação dentro da empresa, deve ser garantida atempadamente a presença de um perito.

Em investigações que envolvam a busca e recolha de prova digital, pode ser necessária a consulta de peritos. Todos os peritos, mesmo aqueles não directamente envolvidos com o sistema de justiça, devem estar familiarizados com este documento ou outros similares.
Um perito deve possuir as seguintes características:

- Os conhecimentos e a experiência adequados, na área específica;
- Conhecimentos legais e de investigação criminal (basicamente no âmbito do Código de Processo Penal, Lei n.º 32/2008 de 17 de Julho e Lei n.º 109/2009 de 15 de Setembro;
- A idoneidade e a reserva necessária quando se lida com processos-crime;
- Características de comunicação oral e escrita.

Formação dos Técnicos

Princípio: Todos os *first responders* devem ter formação adequada.

Antes de irem para o terreno, os técnicos devem ter uma formação mínima, que lhes permita buscar e recolher elementos de prova digital, se não houver peritos disponíveis.
Nos casos excecionais, quando se torna necessário que um não perito lide com dispositivos de prova digital, este deve ser capaz de o fazer de acordo com as normas e deverá ainda ser capaz de explicar a relevância e as implicações das suas ações.

Conformidade com as normas legais em vigor

Princípio: O técnico e a entidade que representa, são responsáveis pela garantia de que a Lei e todos os procedimentos e boas práticas são estritamente cumpridos.
O mesmo se aplica à garantia da boa manutenção da cadeia da prova.
Independentemente de outras normas em vigor em Portugal, o técnico no local deve ter presente o estatuído:
Na Lei n.º 32/2008, de 17 de Junho, que transpõe para a ordem jurídica interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações e;
Na Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime), que transpõe para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa, nomeadamente nos seus Art.^{os} 15.º, 16.º e 17.º.
Ainda, como decorre do próprio ordenamento jurídico nacional devem ser observadas as normas quanto aos meios de prova e a sua obtenção previstas no Código Processo Penal.

Tipos de Recolha

Existem 4 tipos gerais de recolha de prova digital:

- Recolha dos equipamentos e dos meios de armazenamento;
- Cópia por imagem de conteúdos de memória;
- Recolha dos meios contendo as cópias de segurança existentes e
- Cópia seletiva de dados.

Os diferentes tipos são discutidos nas secções seguintes. Nestas temáticas não há compartimentos estanques, podendo uma mesma operação combinar diversos tipos de recolha consoante as circunstâncias.

Recolha dos equipamentos e dos meios de armazenamento

Este tipo de recolha pode ser adequado nas seguintes situações:

- Não existe muito equipamento para recolher. Por exemplo, um PC isolado ou uma pequena rede departamental;
- Não existe risco de graves prejuízos financeiros ou outros, em virtude da recolha dos equipamentos;
- É necessário interromper a atividade suportada pelos equipamentos, uma vez que a atividade é em si ilícita.

As vantagens deste tipo de recolha são as seguintes:

- Pode ser executada com alguma facilidade por Técnicos não peritos (na maioria das situações);
- Permite operações mais rápidas, o que pode ser vantajoso em ambientes hostis;
- A prova digital fica integralmente preservada;
- Permite uma análise forense mais cuidada, em ambiente próprio e com as ferramentas adequadas;
- Não carece de prévio despacho judicial adequado, uma vez que não se vai pesquisar dados (Art.º 15º e seg. da Lei n.º 109/2009 de 15/09)

As desvantagens são:

- Existe o risco de danificar os equipamentos e a própria prova;
- Existe o risco de danos colaterais, prejudicando terceiros que nada tenham a ver com os factos em investigação e que se vêm privados dos equipamentos ou dos serviços por estes disponibilizados;
- Existe o risco de prejuízo de outras atividades não relacionadas com os factos em investigação.

Os procedimentos deste tipo de recolha são descritos mais à frente.

Cópia por imagem de conteúdos de memória

Para este tipo de recolha, normalmente identificada como imagem são utilizados equipamentos e ferramentas informáticas forenses especiais para o efeito e que criam uma cópia exata, bit a bit, do conteúdo alvo para um dispositivo externo de armazenamento.
Estes dispositivos e ferramentas criam um resumo digital (código *Hash*), que permite certificar que a cópia não é posteriormente alterada e possa ser validada em sede de julgamento, caso seja levantada essa questão.

Este tipo de recolha é adequado nas seguintes situações:

- Existe uma grande quantidade de equipamentos para recolher (normalmente em empresa médias ou grandes);
- Não é possível nem viável a recolha dos equipamentos (ex: Sistemas informáticos de empresas);
- A recolha dos equipamentos causaria graves prejuízos para o funcionamento da empresa;
- Seja entendido que em função dos factos em apreço, não se torna necessário recolher o equipamento;

As vantagens são:

- Risco reduzido de danificação dos equipamentos;
- Não prejuízo de terceiros, que partilhem os equipamentos ou serviços;
- Não prejuízo da atividade económica da empresa;
- Menor pressão para a conclusão dos exames forenses, atendendo a que o equipamento continua ao dispor do suspeito;
- Menor necessidade de espaço para armazenamento de equipamento.

Desvantagens:

- É necessário equipamento especial no cenário da recolha;
- É necessária a presença de um perito ou de alguém familiarizado com os equipamentos forenses;
- É normalmente necessária a colaboração do alvo ou do seu administrador de sistemas, na identificação dos locais exatos dos dispositivos de prova;
- A recolha é muito mais morosa, podendo demorar várias dezenas de horas, não sendo por vezes possível conclui-la num só dia de trabalho;
- Corre-se o risco de "passar ao lado" da prova;

Recolha dos meios contendo os backups existentes

Este tipo de recolha é adequada para as mesmas situações daquelas adequadas para as de cópias integrais dos conteúdos de memória especialmente se existe uma grande quantidade de equipamentos e dados a recolher (grandes redes ou ambientes de Mainframe).

As vantagens são semelhantes as da realização das imagens, acrescidas de:

- Não é necessário equipamento especial e
- Não se perde tempo no local.

As desvantagens são:

- É necessária a presença de um perito;
- É necessária a colaboração do alvo ou do seu administrador de sistemas;
- Corre-se o risco de "passar ao lado" da prova, caso os *backups* estejam danificados, mal efetuados ou não tenham armazenado os dados pretendidos;
- É necessário replicar o ambiente do sistema informático do alvo, para que o *restore* tenha sucesso, nomeadamente com motores da base de dados, programas de gestão documental ou sistemas *Enterprise resource planning* (*ERP*) o que se pode revelar demasiado dispendioso.

Pelos motivos acima apresentados é um tipo de recolha a usar só em último recurso.

Cópia seletiva de dados

Este tipo de recolha deve apenas ser utilizado em circunstâncias especiais e se nenhum dos métodos anteriores for viável.
Neste método copia-se para um suporte apenas aqueles dados que se seleciona no momento.

As vantagens são semelhantes às dos *backups*.

Desvantagens:

- É necessária a presença de um perito;
- É necessário o uso de programas informáticos forenses para triagem, recolha e certificação dos dados;
- É necessário ter no local um suporte de armazenamento suficientemente grande para gravar todos os dados;
- Tem de se preparar a recolha previamente com a elaboração de palavras ou termos que facilitem a pesquisa e o uso do programa de triagem;
- Não vai ser possível pesquisar em ficheiros escondidos ou arquivados noutros locais ou em locais não autorizados pelos privilégios do utilizador que se está a usar, em partições não acessíveis, em ficheiros encriptados e em zonas dos discos não alocadas ou no *slack space* (espaço de alocação distribuído por vários sectores do disco, deixado "livre" por gravação o eliminação de ficheiros);
- Não é possível estabelecer um histórico da atividade do sistema;
- Não se regista a existência e configurações ou não de antivírus/firewall ou da existência de Malware no sistema e que poderá levantar a dúvida em sede de julgamento, sobre a consciência do titular do sistema da autoria dos factos em investigação.

Procedimentos de recolha de prova digital

Tal como foi mencionado na introdução, este documento focaliza-se nos procedimentos de recolha que envolvem a busca, a identificação, a recolha e a documentação dos dispositivos eletrónicos.

Os procedimentos têm cinco fases que serão desenvolvidas nas secções seguintes e que são:

- Preparação para a recolha;
- Criação do perímetro de segurança no cenário na recolha;
- Documentação do cenário;
- Recolha da prova;
- Acondicionamento, transporte e armazenamento.

No Anexo III é disponibilizado um Fluxograma/Guia de bolso que descreve os paços principais.

Preparação para a recolha

No decorrer das investigações preliminares e da recolha de informação, que por norma são feitas antes da operação de recolha, deve tanto quanto possível determinar-se se é previsível vir-se a encontrar prova digital relevante para os autos.

Neste caso, deverá ser de imediato informado o departamento de informática forense, caso exista. Em concertação com este e em função das informações previamente recolhidas, deverá em primeiro lugar ser decidido que tipo de recolha se vai realizar. Assim, os técnicos que se desloquem ao local, estarão melhor preparados, quer em termos de equipamentos quer em termos de conhecimentos em áreas

específicas que seja necessário estudar primeiro. Deverá ser recolhida o máximo de informação possível sobre os sistemas que se vão encontrar.

A título de exemplo e sempre que possível deverá ser recolhida informação sobre:

- Computadores, Sistemas Operativos, Programas e dispositivos de armazenamento;
- Redes de comunicações e informáticas (ISP, telefones, faxes, modems, LAN, equipamento de rede, etc.);
- Quem é responsável pelos sistemas ou rede (tem um Administrador local ou é administrada por uma empresa externa? Qual?);
- Que quantidade de equipamento é expectável recolher (relevante para o tipo de recolha a empreender);
- Que quantidade de dados se prevê copiar (relevante para o tipo de recolha a empreender);
- Existência ou não de um sistema de *backup* (relevante para o tipo de recolha a empreender).

As fases de preparação incluem os seguintes passos:

- Assegurar-se que as devidas autorizações estão passadas e nos termos do Código Processo Penal, Lei n.º 109/2009 de 15/09 e eventualmente nos termos da Lei n.º 32/2008 de 17/07;
- Obter o máximo de informação possível sobre o sistema a buscar (ver tópicos acima);
- Escolha da equipa (incluindo peritos se necessário);
- Atribuir tarefas individuais a cada elemento da equipa;
- Efetuar um briefing com toda a equipa;
- Fornecer os documentos e equipamentos e programas necessários para a operação.

Equipa de recolha

Se for previsível vir-se a recolher dispositivos eletrónicos, a equipa deve integrar um técnico treinado na recolha deste tipo de prova. Pode inclusivamente ser necessário consultar um perito externo.

Por exemplo, se a administração do parque informático for feita por uma empresa externa, poderá ser aconselhável envolve-la como perita ou testemunha. Este procedimento deverá ser aplicado com os maiores cuidados, sob pena do alvo vir a tomar conhecimento da operação que vai ser realizada.

No mínimo, deverá estar presente na equipa em técnico com treino básico de recolha da prova digital.

Todos os membros da equipa devem ser igualmente informados dos mesmos princípios na manipulação de dispositivos eletrónicos, e de quando deverão seguir procedimentos específicos (por exemplo, não deve ser usado pó de alumínio na recolha de vestígios lofoscópicos em equipamentos eletrónicos).

Equipamento e ferramentas

Equipamentos e ferramentas específicos podem ser necessários para recolher prova digital. As constantes evoluções da tecnologia fazem com que as ferramentas estejam em constante evolução e mutação. O equipamento descriminado na seguinte listagem poderá ser de grande importância numa recolha e deverá estar disponível para qualquer operação:

- Ferramentas de desmontagem:
- Chaves de parafusos várias (planas ou tipo Phillips e especificas de fabricante tais como Compaq ou Macintosh);
- Chaves de porcas (tipo Allen, sextavadas e de estrela);
- Alicates (normais e de pontas);
- Alicates de corte (para braçadeiras);
- Pinça pequena para circuitos integrados;
- Documentação:
- Folhas quadriculadas para elaboração de croquis do local;
- Etiquetas de várias cores e fita;
- Identificadores de cabos;
- Marcadores de tinta, normais e de escrita em superfícies plásticas;
- Encaixotamento e transporte:
    - Sacos antiestáticos (para circuitos impressos);
    - Braçadeiras para cabos;
    - Sacos e fita de prova;
    - Pequenas caixas para disquetes, disquetes JAZ/ZIP, DVDs e CDs;
    - Packs de caixas montáveis. Podem ser de cartão;
    - Sempre que possível, recorrer às caixas e esferovites originais do equipamento;
- Equipamentos de telecomunicações:
    - Telefones móveis ou rádios de comunicações não devem ser usados na proximidade dos equipamentos;
    - Contactos telefónicos dos peritos e do responsável pela operação, caso não estejam presentes.
- Outros:
    - Máquina de fotografar/filmar;
    - Pequena lanterna com pulseira;
    - Luvas de latex;
    - Carrinho de transporte;
    - Bandas de borracha;
    - Lupa;
    - Papel para impressora;
    - Discos óticos virgens (CD/DVD);
    - Clipes;
- Equipamentos e ferramentas forenses recomendadas (ver capitulo sobre a recolha da prova):
    - Disco ótico de arranque CD-R ou outro disco “Boot” forense, tal como o ”SPADA” ou o “Paladin” (caso se esteja treinado para usá-los);
    - Uma ou mais licenças de uma ferramenta de triagem tal como a da *ADF solutions* “Triage-G2” ou o “AD Triage” da AccessData com respetivos dispositivos externos de suporte.
    - Uma ou mais “PEN’s” com a versão “light” do “FTK Imager” da *AccessData*.

- Um ou mais kit's completos para efetuar cópias forenses, tais como o da *LogiCube*, "Portable Forensic Lab" com o dispositivo copiador "Talon".
- Um "RAID" externo de discos, com ligação multiformato (USB 2.0, FireWire 800, exata, etc.) com grande capacidade de armazenamento e com características forenses (capacidade de "wipe").

Criação do perímetro de segurança no cenário na recolha

Embora não caiba no âmbito da presente dissertação o estudo das buscas policiais, podemos das suas boas práticas retirar ensinamentos importantes, uma vez que a segurança deve ser sempre prioritária.

Normalmente não se associa o crime tecnológico com o crime violento, mas cabe aqui desmistificar este conceito, uma vez que o perfil do agente do crime é muito variado nos tipos de crimes que envolvem a alta tecnologia. Há situações reportadas de reações violentas em crimes tais como acessos ilegítimos, reprodução ilegítima de software ou divulgação de material de abusos sexuais de menores, assim que os suspeitos se apercebem que vão ficar privados dos seus equipamentos informáticos ou que foi descoberta a sua atividade. Por vezes esta reação violenta pode também ter em vista a destruição dos dispositivos de prova, existindo situações onde chegaram a ser usadas armas brancas e armas de fogo.

Assim sendo, assinalam-se apenas sobre as medidas que têm a ver exclusivamente com os dispositivos eletrónicos.

Os passos a seguir são:

- Afastar todas as pessoas dos equipamentos informáticos, incluído das ligações elétricas e quadros elétricos;
- Proteger todos os dispositivos que contêm dados voláteis, física e eletronicamente;
- Identificar, proteger, documentar a fotografar todos os dispositivos que contenham dados a recolher;
- Elaborar reportagem fotográfica do local onde se encontram os dispositivos a recolher, bem como de outros locais que se entenda poderem vir a ser relevantes para a prova (ex: nos casos de abusos sexuais de menores, importa fotografar os locais, para posterior comparação com fotografias de abusos, para consubstanciação da prova);
- Durante a diligência, controlar constantemente todas as pessoas presentes no local, para evitar que estas possam interferir com os elementos de prova;
- Manter sempre os dispositivos a recolher debaixo da vigilância atenta de pelo menos um dos elementos da equipa;
- Identificar e documentar todas as redes a que os dispositivos estavam ligados (dados, voz, wireless, etc...);
- Antes de interagir com os dispositivos a recolher ter o cuidado de triar se será relevante a recolha de outros tipos de vestígios, tais como biológicos, lofoscópicos, drogas, aceleradores ou outros. Em caso afirmativo:
  - Proceder de acordo com as regras para estes tipos de situações;
  - Adiar técnicas destrutivas até que seja salvaguardada a prova digital:
    - Recolher impressões digitais de teclados, ratos, disquetes, discos óticos ou outros componentes, depois de salvaguardada a prova digital;
    - Não usar pó de alumínio na recolha de vestígios lofoscópicos no local do crime até que se protejam os dispositivos eletrónicos.

- Buscar a cena do crime por outros objetos não eletrónicos, mas com eles relacionados, tais como (ver capitulo da recolha da prova para mais detalhes):
  - Palavras-chave escritas em post-it, papéis, cadernos ou diários;
  - Blocos de apontamentos com marcas manuscritas latentes;
  - Calendários e manuais de software;
  - Fotografias;
  - Folhas impressas;
  - Informações de interesses pessoais (matriculas, filhos, números de telefone, hobbies, nomes dos animais de estimação, etc...), que poderão ajudar na elaboração de dicionários para quebra de passwords.
- Efetuar entrevistas preliminares:
  - Separar e identificar as pessoas, identificando os locais onde estavam quando se entrou na cena da recolha (importante nas situações em empresas);
  - Tentar recolher as seguintes informações:
    - Finalidade do dispositivo em apreço;
    - Proprietários e utilizadores dos dispositivos, bem como *usernames* e *Internet Service Provider* que usa;
    - Todas as *passwords* necessárias para aceder ao sistema, programas e dados (BIOS, disco, sistema operativo, rede, ISP, bases de dados, sistemas de encriptação, correio eletrónico, etc...);
    - Quais os sistemas/dispositivos de segurança e destruição usados;
    - Todos os locais externos de armazenamento de dados;
    - Documentação explicativa de hardware e software instalados no sistema.
  - Ter sempre presente que as declarações prestadas em sede de recolha poderão ser as únicas que vamos ter dos suspeitos, uma vez que estes ainda em estado de surpresa, não tiveram muito tempo para pensar e ainda não foram aconselhados a não prestar declarações.

Documentação da cena

A documentação não é um momento da diligência, é antes um processo que decorre durante toda a recolha.

Tem de se ter sempre presente que vai ser a única vez que se vai perante o local original e que muito provavelmente vai ser necessário replicar o cenário e sustentar em sede de tribunal, sem margem para dúvidas, como é que o sistema estava a funcionar, onde e por quem.

É de importância crucial registar as localizações e estado de conservação dos computadores, dos dispositivos de armazenamento, de outros dispositivos eletrónicos e não eletrónicos.

Mais à frente são apresentadas instruções mais detalhadas sobre o que deve ser documentado. Esta secção apresenta apenas um sumário dessas instruções. Em termos gerais, deve ser documentado o seguinte:

- Cenário físico:
  - Desenhar croquis do sistema, com localização exata de todos os periféricos;
  - Desenhar croquis do local, com localização de todos os equipamentos a recolher, bem como indicações precisas sobre os seus utilizadores, passwords, etc.;
  - Reportagem fotográfica/vídeo do cenário se possível em 360º;
- Sistemas informáticos e dispositivos eletrónicos:

- Detalhes de todos os equipamentos (marca, modelo e número de série);
- Estado geral, localização no cenário e se estava ligado ou não;
- Todas as ligações (físicas ou wireless) de e para o computador ou outros dispositivos (ver figura 1):
  - Etiquetar todos os cabos (incluindo os periféricos), para posterior remontagem;
  - Etiquetar todas as portas não usadas, como não usadas;
  - Identificar dock stations, para posterior identificação de outros dispositivos.
- Detalhes do monitor na altura da intervenção:
  - Fotografar o computador e o ecrã do monitor;
  - Documentar por escrito o que estava no ecrã;
  - Ver capítulo dedicado ao registo de sistemas ligados (live systems).
- Documentar dispositivos eletrónicos relevantes que não vão ser apreendidos.

➢ Pessoas presentes no local:
- Entrevistar as pessoas presentes no local (ver ponto anterior);
- Documentar os seguintes aspetos:
  - Identificação pessoal;
  - Que dispositivos utilizava;
  - Comentários fornecidos por testemunhas sobre os equipamentos/pessoas no local.

➢ Todas as ações no local:
- Criar um registos, com todos os passos tomados em, relação a cada elementos de prova, com registo da hora exata de cada ação.

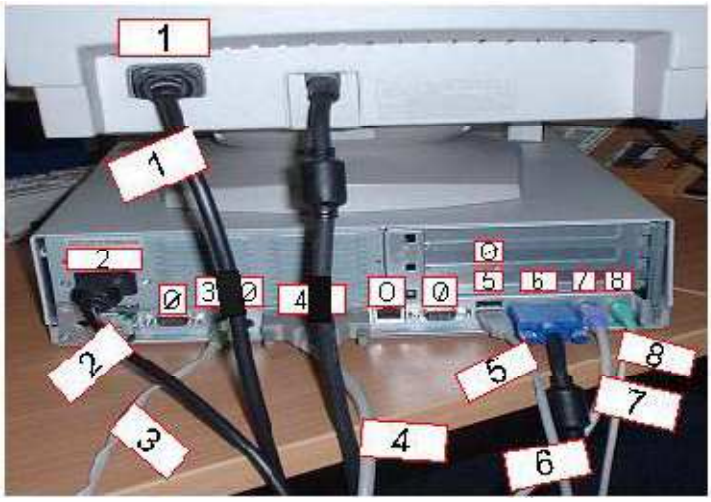


Figura 1: Etiquetar todos os cabos para posterior reembalagem

Recolha da prova

Um dispositivo não deve de ser apreendido só porque se encontra no local da recolha. A seleção deve ser adequada ao crime em causa e a decisão de recolher determinado objeto deve ser da responsabilidade do chefe de equipa ou de quem coordena a operação.

A prova digital, tal como os outros tipos de provas, deve ser manipulada de maneira a preservar o seu valor probatório. Isto não tem apenas a ver com a sua integridade física, mas sobretudo com os dados

que ela contém. Dependendo do tipo de dispositivo, medidas especiais de recolha, empacotamento e transporte. Prova que seja suscetível a campos eletromagnéticos fortes ou eletricidade estática, provocada por magnetos ou transmissores de rádio entre outros, devem de ser devidamente protegidos.

No capítulo seguinte serão discutidos os seguintes tipos de dispositivos:

- Computadores;
- Outros dispositivos eletrónicos;
- Dispositivos de armazenamento;
- Informação relacionada com redes.

Acondicionamento, transporte e armazenamento

Os dispositivos eletrónicos são frágeis, sendo sensíveis à temperatura, à humidade, a choques, à eletricidade estática, a campos magnéticos e até a algumas ações humanas tais como ligá-los ou desligá-los.

Assim, devem de ser tomadas medidas especiais quando se acondicionam, transportam e armazenam estes dispositivos. De igual modo e para que se mantenha a custódia da prova, há que registar todos os procedimentos que foram levados a cabo.

Em termos gerais, os seguintes concelhos devem de ser seguidos:

- Acondicionamento:
  - Todos os objetos devem de ser documentados e etiquetados antes de serem encaixotados;
  - Sempre que possível, utilizar as caixas e esferovites originais dos equipamentos;
  - Caso não estejam disponíveis, utilizar material antiestático (papel ou sacos de plásticos antiestáticos);
  - Não utilizar sacos de plásticos normais, porque provocam eletividade estática;
  - Não dobrar, torcer ou arranhar dispositivos de armazenamento tais como disquetes, discos óticos e cassetes (parece um concelho obvio, mas …);
  - Não colar etiquetas nas superfícies desses mesmos dispositivos. Utilizar caixas ou envelopes;
  - Certificar-se que todos os pacotes que contêm provas estão etiquetados;
  - Certificar-se que as etiquetas identificam inequivocamente o dispositivo.
- Transporte:
  - Manter os objetos afastados de fontes eletromagnéticas tais como transmissores rádio, altifalantes, amplificadores ou subwoofers de automóvel ou bancos de viaturas com sistemas de aquecimento;
  - Acondicionar os caixotes de maneira a que não tombem, nem saltitem;
  - Afastar de fontes de calor e humidade;
  - Amarrar os dispositivos que não estão encaixotados e colocá-los no chão da viatura ou seguros com os cintos de segurança;
  - Não colocar os objetos mais pesados em cima dos mais frágeis;
  - Manter os dispositivos o mais curto espaço de tempo possível dentro das viaturas e especialmente nunca longas horas ao sol.
- Armazenamento:
  - Certificar-se que os objetos estão corretamente inventariados;

- Caso exista um departamento da organização com as condições de armazenagem adequados, depositar o material o quanto antes;
- Os mesmos concelhos para o transporte são também aqui válidos, quanto à exposição dos equipamentos aos elementos, nomeadamente o pó;
- Utilizar uma sala de armazenamento com as condições apropriadas, nomeadamente:
  - Controle de acessos;
  - Segurança física contra catástrofes (incêndio, inundação, etc...);
  - Meio ambiente controlado em termos de temperatura, humidade e campos magnéticos.
- Esta sala não deve de estar nas imediações de outras com materiais inflamáveis tais como produtos de limpeza ou papéis;
- Evitar que esta sala tenha canalização, especialmente de teto e fora da parede;
- Ter atenção e agir em conformidade, nos casos de dispositivos que necessitem de manutenção constante das baterias para preservarem as suas memórias.

Tipos de prova digital: Instruções de Manuseamento

Computadores

Existem muitos tipos de computadores, tais como portáteis, desktops, torres, sistemas modulares em *rack*, mini e *mainframes*, entre outros

Potencialmente a prova relevante encontra-se em ficheiros armazenados em memória interna e externa ao computador.

O técnico no local da recolha deve sempre que possível recorrer a um perito, especialmente se o equipamento não for apreendido.

Aquilo a que normalmente se chama computador, tipicamente consiste em diversos equipamentos, cuja recolha deve ser levada em conta.

Os dispositivos normalmente são:

- A unidade principal, que contém a motherboard, o CPU, a memória e as placas de expansão;
- O monitor;
- O teclado;
- O rato;
- Os cabos;
- As fontes de alimentação;
- Os periféricos, tais como modems, impressoras, scanners, *docking stations*, leitores de cartões, *dongles*, *smart cards* ou dispositivos externos de armazenamento;
- Dispositivos de rede.

Note-se que outros dispositivos que não a unidade principal, podem conter memória interna, sem que tal seja visível do exterior.

É necessário igualmente ter atenção, que as unidades principais podem estar dissimuladas noutros tipos de objetos, tais como arcas, bidões, aquecedores, etc...

Finalmente, nunca é de mais alertar para dispositivos que possam não estar fisicamente ligados à unidade principal, mas que fazem parte do sistema. Caso a unidade principal tenha uma antena wireless, têm necessariamente de existir dispositivos que a utilizassem.

Os sistemas operativos normalmente encontrados em computadores pessoais são as variadas versões do *Microsoft Windows*, as de *Unix* e *Linux* ou o *Mac OS*. Estes podem estar sozinhos (*stand alone*) ou ligados a uma rede.

Neste caso é necessário ter atenção a outro tipo de dispositivos, tais como routers, hubs, switches, que podem ser de ligação por cabo ou wireless.

Os seguintes objetos de suporte também devem de ser considerados:

- Manuais do hardware e do software (incluindo os discos óticos originais);
- Notas, diários, calendários, ou outros suportes manuscritos onde possam estar passwords;
- Blocos não escritos mas com marcas de apontamentos de outras folhas;
- Livros técnicos sobre computadores;
- Folhas impressas da impressora;
- Fotografias relevantes.

Recolha do computador e dispositivos eletrónicos

Esta secção descreve os passos necessários a dar na recolha de um computador. Tal como já foi referido, toda a diligência deve de ser documentada, desde o que se passa no monitor do computador sem a intervenção da equipa até todos os pormenores das ações levadas a cabo e que interagiram com os equipamentos.

Nunca se deve seguir os concelhos ou as dicas do suspeito.

- Tornar o cenário seguro e afastar todas as pessoas dos equipamentos e dos quadros elétricos;
    - Procure os seguintes componentes:
        - Os computadores e seus componentes;
        - Dispositivos de armazenamento;
        - Outros dispositivos eletrónicos;
        - Outros objetos não eletrónicos
    - Se existir uma rede informática, deve-se contactar um perito da forense ou alguém por ele indicado, para auxiliar na operação:
        - Ter atenção que alguns dispositivos podem estar ligados a uma rede wireless (Bluetooth ou infravermelhos);
        - Ter muita atenção que se existe uma rede, esta poderá estar a ser manipulada durante a operação.
    - Conduzir entrevistas preliminares;
- Observar o computador e avaliar se este está ligado ou não (Ver secção seguinte);
- Documentar todas as ligações e componentes e colocar etiquetas tal como já descrito;
    - Fotografar ou elaborar um diagrama de todas as ligações e dos cabos;
    - Registar os objetos no relatório da operação.
- Remover o equipamento e registe os seus elementos técnicos. Esperar que os equipamentos arrefeçam antes de os encaixotar;
- Se for necessário transportar os equipamentos, deve-se acondicioná-los tal como descrito na respetiva secção.

Os guias de bolso do Anexo IV têm um resumo das melhores práticas para a recolha de computadores e PDAs.

Verificar se está ligado ou não (on/off)

Observar atentamente o computador e avaliar se este está ou não ligado:

- A maior parte dos computadores têm uma luz de status, estando acesa quando este está ligado.
- Se a ventoinha faz barulho é porque está ligado;
- Se o sistema está quente, pode ser uma indicação de que está ligado ou que esteve recentemente;
- Alguns portáteis ligam-se automaticamente ao levantar a tampa:
    - Considerar sempre a remoção das baterias.
- Um computador que aparente estar desligado pode simplesmente estar adormecido, podendo estar acessível remotamente, permitindo a alteração e a remoção de ficheiros;
- Alguns screen savers dão a impressão de que o computador está desligado.
- Observar o monitor e tentar determinar se o computador está ligado, desligado ou em sleep. O resultado da observação deve ser a seguinte:
    - Situação 1: Monitor ligado e o desktop está visível:
        - Documentar e fotografar os detalhes do que se vê no monitor;
        - Prosseguir para a situação B descrita abaixo.
    - Situação 2: Monitor ligado mas o ecrã está sem imagem (sleep) ou está um screen saver em execução (fotos ou imagens):
        - Mover o rato ligeiramente (sem tocar nos botões). O ecrã deve mudar e mostrar um desktop ou um pedido de password.
        - Se o movimento do rato não alterar nada, não fazer mais nada;
        - Documentar o que vê e o que fez registando a hora;
        - Prossiguir para a situação B descrita abaixo.
    - Situação 3: O monitor está desligado:
        - Tomar nota deste estado;
        - Ligar o monitor no botão e proceder como na situação 2.

O resultado da observação de se o computador está ligado ou não deve ter o seguinte resultado:

- Situação A: determinou-se que o Computador está desligado. Não o ligar:
    - Remover a ligação à corrente elétrica da unidade principal e registar a hora. (não desligar pela tomada da parede);
    - Se for um portátil, remover também as baterias.

Nunca ligar um computador, porque só o processo de startup vai alterar os dados contidos no computador, podendo alterar elementos de prova.

- Situação B: O computador está ligado. Não o desligar:
    - Deve-se contactar um perito. Caso este esteja disponível, seguir os seus concelhos, se não,
    - Não tocar no teclado ou noutros dispositivos de input;
    - Remover o cabo elétrico da unidade principal (não o da parede porque pode haver uma UPS, pelo meio) e registar a hora a que o fez;
        - Ter consciência de que isto pode fazê-lo perder elementos de prova
    - Retirar os dispositivos de armazenamento das respetivas *drives* e coloca-las nas respetivas caixas devidamente etiquetadas. Insirir uma disquete ou um CD-R forense ou vazios, nas respetivas *drives*;
    - Não remover discos óticos, nem tocar em nenhum botão dessas drives;

- Desligar a ficha do modem caso exista. Apenas a ação de o desligar, pode não ser suficiente;

Remover a corrente de um computador ligado, vai afetar todos os programas que estejam a ser executados, vai limpar toda a memória RAM e vai quebrar as ligações à Internet, a impressoras, a drives remotas e a drives encriptadas. Mais à frente faz-se referência às situações que envolvem os sistemas *live*.

- Situação C: não se consegue perceber se o computador está ligado ou não:
  - Assumir que está ligado e proceder como tal.

Redes de Computadores

Assumir sempre que existe uma rede de computadores.

Sempre que se confirme a existência de uma rede, contactar um perito em redes. Se não existir nenhum, a informação que se segue poderá ajudar.

Indicadores da existência de uma rede:

- A presença de vários computadores;
- A existência de componentes no computador, tais como:
  - Placas de rede, de cabo ou wireless e ou cabos de rede;
  - Dispositivos de redes Wireless (i.e., wireless access point);
  - Routers, hubs, e switches;
  - Servidores;
  - Cabos de rede ligados entre computadores ou *modems* e *hubs* ou outros ativos de rede.
- Informação fornecida por informadores ou outros funcionários no local da recolha.

Caso não exista nenhum perito por perto, deve-se seguir as instruções sugeridas.

Elementos potencialmente relevantes para recolha e recolha de elementos, no caso de existência de redes:

- *Internet Service Provider* (ISP) ou Prestador do serviço de acesso à Internet;
- Internet Protocolo (IP) ou endereços TCP/IP em utilização;
- Data e hora incluindo o fuso horário (time zone) (elemento fundamental);
- Configuração da rede;
- Servidores Domain Name Service (DNS);
- Contas e servidor de E-Mail;
- Segurança e encriptação;
- *Newsgroups*;
- *Chatrooms* ou salas de chat;
- Online shops / service providers (caso esteja em causa a informação sobre pagamentos online);
- Endereços IP e nomes de servidores de outros serviços eventualmente utilizados tais como ftp, telnet ou WWW.

Componentes adicionais

Tal como já mencionado, um computador pode incluir alguns dispositivos adicionais, tal como:

- Dispositivos externos de armazenamento, ligados por cabo ou outros interfaces:
  - Discos externos;
  - Blocos de memória USB (vulgo PEN's);
  - Leitores/Gravadores externos de CD-RW ou CD-ROM;
  - Leitores/Gravadores externos de DVD-ROM ou DVD-RW;
  - Drives de disquetes;
  - Drives JAZ;
  - Drives ZIP;
  - Drives de tapes magnéticas;
  - Drives ORB.
- Duplicadores;
- Leitores MP3;
- Dongles (i.e., Dongles USB, paralelos ou série);
- Smart cards e leitores de smart cards;
- Impressoras;
- Scanners;
- Docking stations;
- Replicadores de portas;
- PC cards e leitores de PC cards;
- Web câmaras (ver câmaras digitais);
- Modems (internos ou externos, dialup/analógicos ou por cabo, DSL, ISDN ou wireless);
- Dispositivos Wireless:
  - Adaptadores de infravermelho (USB, serie, mainboard);
  - Dispositivos Infrared-enabled (wireless LANs, ligações entre portáteis e PC, modems sem fios, detetores de movimento);
  - Dispositivos Bluetooth-enabling (Dongles Bluetooth USB para PDAs e PCs, PCcards para portáteis);
  - Dispositivos Bluetooth-enabled (headsets ou auriculares, PDAs, portáteis, telefones, receptores de GPS).

Ter atenção aos diversos formatos que estes dispositivos podem ter (Ver exemplos no glossário).

Dispositivos de armazenamento Digital

Os seguintes dispositivos não são normalmente armazenados junto dos computadores, mas sim numa sala próxima ou noutro edifício, nalguns casos fechados em cofres:

- Disquetes;
- Backups (i.e., tapes ou DATs);
- Disquetes JAZ, ZIP e ORB;
- CDs e DVDs;
- Discos rígidos não ligados ao computador;
- Placas para PCs;
- Cartões de fita magnética;
- Cartões de memória;
- Pens/keys/sticks USB;
- Dongles;
- Discos Solid State;
- PDA.

Ter atenção aos diversos formatos que estes dispositivos podem ter (Ver exemplos no glossário).

Sistemas ligados ou Live Systems

Por vezes pode ser fundamental para a produção da prova, registar tudo o que estava a acontecer naquele momento no sistema que se pretende recolher.

Para o fazer há ferramentas próprias, cuja utilização deve ser reservada para técnicos treinados para o fazer.

Sempre que se verificar a necessidade de preservar o conteúdo da memória de um sistema ou o conteúdo de um disco encriptado ou de uma drive remota, que naquele momento estão "abertos", deve ser sempre contactado um perito, para que este se desloque ao local.

Entre as diversas ferramentas que este terá ao seu dispor para preservar este tipo de prova encontra-se o X-Ways Forensics, o FTK Imager ou o ADF solutions AD-Triage.

Outros dispositivos eletrónicos

- Personal digital assistants (PDAs ou computadores portáteis), ver secção referente a:
  - Agendas eletrónicas;
  - Communicators;
  - Smart phone.
- Equipamentos vídeo (câmara vídeo, gravador de vídeo (VCR) ou leitor);
- Gravadores Áudio;
- Chips;
- Circuit boards;
- Placas de expansão;
- Câmaras digitais;
- Tokens de acesso (para identificação/autenticação do cartão e do utilizador, níveis de acesso, configurações, permissões, etc…):
  - Smart cards;
  - Dongles (security dongle);
  - Scanners Biométricos.
- Telefones ;
- Atendedores automáticos;
- Máquinas de Fax;
- Gravadores de voz (ver atendedores automáticos);
- Pagers;
- Playstations com cartões de memória ou discos, gameboys com cartridges, Xboxes, gamecubes ou outras consolas de jogos;
- Dispositivos de GPS;
- Relógios Digitais;
- Credit card skimmers (ou leitores de bandas magnéticas);
- fotocopiadoras.

Ter atenção aos diversos formatos que estes dispositivos podem ter (Ver exemplos no glossário).

Regras gerais para recolha de dispositivos eletrónicos

Os seguintes princípios devem de ser atendidos, quando se apreendem dispositivos eletrónicos:

- Se este está ligado, não desliga-lo porque pode ativar algum mecanismo de bloqueamento
  - Fotografar o ecrã (caso exista) e registar o que está visível;
  - Retirar todos os cabos de ligação à corrente elétrica (a partir do dispositivo e não da parede);
  - Nunca tentar aceder à memória do dispositivo;
- Se estiver desligado, não liga-lo, porque irá modificar o seu conteúdo, destruindo dessa forma a validade da prova;
- Desligar cada uma das ligações do telefone a partir da tomada da parede e colocar-lhes uma etiqueta;
- Recolher informações adicionais;
- Acondicionar e transportar os equipamentos conforme instruções fornecidas:
  - Como as baterias têm um tempo de vida limitado, mesmo com o dispositivo desligado, pode haver perda de dados. Por esta razão deve-se informar a pessoa que vai armazenar o equipamento, de tal facto, para que esta providencie que as baterias não se descarreguem;
  - No caso de telefones e PDAs, devem ser examinados por um perito, o mais rapidamente possível.

Personal digital assistants

Também denominados computadores de mão, agendas eletrónicas ou PDA e podem ter as normais funcionalidades de um computador e as de telefone/fax, pager, ligações a redes wireless, UMTS ou bluetooth, GPS e capacidade de fazer fotografia e filme.

É normalmente utilizado como agenda pessoal, pelo que conterá muita informação pessoal, incluindo históricos de email, sms, mms, contactos e compromissos.

Hoje em dia estes dispositivos aproximam-se muito das capacidades de um computador desktop. Alguns possuem discos rígidos, memórias internas de grande capacidade e cartões de memória em slots.

Normalmente possuem uns mecanismos de sincronização com um computador, usualmente através de um cradle.

Se existir um cradle, tentar localizar o dispositivo que o usa. Tratar o PDA como se de um normal computador se tratasse, com a agravante que pode ser facilmente escondido, ou mantido dentro do bolso do suspeito.

A memória do PDA é mantida pelas baterias e nalguns modelos mais antigos, se estas acabarem, toda a informação é perdida.

Nestes existiam duas baterias:

- Uma principal, que está encarregue de manter o ecrã e o teclado quando o PDA estiver ligado;
- Uma de backup que mantém as informações em memória quando a principal falha.

Alguns PDAs têm uma única bateria recarregável, que se recarrega quando o dispositivo está ligado no respetivo cradle e ligado ao computador.

Estas baterias tendem a descarregar-se num espaço de dias, quando não recarregadas.

Têm de ser adotadas medidas especiais, para preservar este tipo de prova.

A maioria dos sistemas operativos que podem ser encontrados atualmente nos PDA são o iOS, o Android, o WebOS, o Windows Mobile ou Phone, o BlackBerry, o Symbian, entre outros.

Quando se apreende PDAs como prova digital, deve-se considerar o seguinte:

- Recolha:
  - Se for encontrada uma rede, proceder tal como se sugeriu para as redes de computadores:
    - Tenha atenção que alguns PDAs podem estar ligados a uma rede wireless Bluetooth ou infravermelhos;
    - Nestes casos, ter atenção que o dispositivo pode ser acedido remotamente (desde que ligado e no raio de ação da rede).
  - Se o PDA estiver ligado, não pressionar a tecla de reset e não remover a bateria, porque pode apagar-se todos os dados;
  - Não ligar ou abrir nenhum PDA, caso este seja de tampa;
  - Recolher os respetivos cabos e periféricos, tais como extensões de memória e o cradle;
  - Os PDAs normalmente têm uma funcionalidade de bloqueio automático, semelhante ao screen saver com password dos computadores e que pode ter a funcionalidade de encriptação. Este mecanismo também pode ser ativado, quando este é desligado:
    - Evitar que este entre em modo de bloqueio, clicando numa zona vazia do ecrã até que esteja disponível um perito que saiba lidar com a situação;
- Acondicionamento, transporte e armazenagem:
  - Colocar o PDA no cradle até que seja examinado;
  - Consultar as instruções do Capítulo especifico.

Telefones

O telefone é um dispositivo que pode ser encontrado nas seguintes variantes:

- Por si só ser um telefone, como o são os telemóveis;
- Com uma estação remota, como são os portáteis sem fios;
- Ligados directamente à linha telefónica.

Atualmente, os telemóveis têm funcionalidades em tudo semelhantes aos PDAs e devem de ser tratados como tal.

Os telefones podem ser autoalimentados por uma bateria, estar ligados à corrente elétrica ou receber energia directamente da rede telefónica.

Consultar as instruções gerais sobre a sua recolha

Smart cards e cartões de banda magnética

Um smart card é um cartão que possui um circuito eletrónico (chip) com um processador, dai também ser denominado de chip card, e pode ter diversas informações ai armazenadas, tais como um valor monetário, uma chave de encriptação, passwords, certificados digitais, ou outros.

Alguns cartões por possuírem um pequeno sistema operativo podem até ser considerados como pequenos computadores.

Por estas razões, estes cartões são de grande importância porque podem possuir importantes provas, tal como um computador ou um PDA.

Os cartões podem ter uma grande variedade de aplicações, tais como:

- Acesso físico a áreas protegidas tais como edifícios ou salas;
- Acesso a máquinas, computadores, programas ou algumas das suas funções;
- Utilização do sistema bancário em ATM;
- porta-moedas eletrónico;
- cartão de crédito;
- cartão de cidadão;
- Certificador de assinatura digital;
- Payphone card ou pré-pago de telecomunicações;
- Suporte de armazenamento de dados pessoais, moradas, contactos, códigos, etc.

As dimensões dos cartões estão estandardizadas como 85.6 x 54 x 0.76mm (i.e., formato ID-1 normalmente denominado “cartão multibanco ou ATM") e tem uma placa de contactos elétricos na parte frontal e normalmente também possuem uma banda magnética.

Também existem cartões denominados ID-0, com tamanho de 25x15x0.76mm, que normalmente são utilizados nos telemóveis tendo a denominação corrente de SIM cards.

Existem ainda os USB tokens, que incluem o chip e o respetivo leitor, tudo num só dispositivo.

Os cartões de leitura sem contacto, são idênticos aos cartões de crédito ou aos smart cards normais.

Finalmente, os denominados “Super Smart Cards”, têm um pequeno display e um teclado numérico e possui um nível de segurança acrescido.

Normalmente o acesso à informação do chip está protegido por *password* ou PIN.

As regras para recolha destes cartões são:

- Não dobrá-lo;
- Não o expor a temperaturas elevadas;
- Não tocar nos contactos elétricos;
- Proteja-lo de riscos, líquidos e fontes magnéticas;
- Tentar apurar qual é o seu PIN;
- Não tentar aceder à informação contida no chip, mesmo que se esteja convencido que está a usar o PIN correto, porque se não estiver pode bloquear-se o acesso ao chip**;**
- Identificar no relatório, o cartão com os dizeres que este possui impressos;
- Sempre que possível, apreender também os respetivos leitores.

Atendedores automáticos

Um atendedor automático é um dispositivo que normalmente, ou faz parte do próprio telefone ou está entre este e a tomada da rede telefónica.

Podem ser de gravação em cassetes de fita magnética ou em memória digital.

Normalmente gravam voz e registam a data e hora das mensagens recebidas.

Potencialmente podem conter:

- Identificação dos números chamadores;
- Mensagens apagadas;
- Ultimo número marcado;
- Memos
- Números de telefone e nomes;
- Cassetes.

Consultar a secção sobre as regras de recolha.

Máquinas fotográficas

As máquinas fotográficas digitais podem ter memória interna e ou através de cartões de memória. Normalmente possuem capacidade de transferir essas imagens para os computadores através de leitores de cartões ou de cabos USB.

As provas potenciais destes dispositivos são:

- A máquina em si;
- Imagens;
- Cartões de memória;
- Som;
- Data e hora;
- Vídeo.

Consultar a secção sobre as regras de recolha.

Máquinas de Fax ou Facsimile

São dispositivos que permitem digitalizar texto e imagens enviando-os através da linha telefónica.

Os computadores também possuem esta funcionalidade, desde que providos de um scanner.

As provas potenciais destes dispositivos são:

- Cartão de memória;
- Números de telefone pré-programados;
- Histórico de documentos enviados e recebidos;
- Memória interna que armazena documentos para posterior envio ou documentos recebidos para posterior impressão;
- Logs ou histórico das transmissões;
- Cabeçalho pré-programado;
- Data e hora.

Consultar a secção sobre as regras de recolha.

Impressoras

As provas potenciais destes dispositivos (quando este detêm capacidade de armazenamento de informação, que em geral é raro) são:

- Logs de utilização;

- Data e hora;
- Identificação de rede, quando a esta ligadas;
- Documentos,
- Disco rígido;
- Imagens indeléveis nos rolos.

Consultar a secção sobre as regras de recolha.

Scanners

Estes dispositivos permitem digitalizar texto e imagens, criando documentos digitais.

O próprio dispositivo pode constituir prova, uma vez que ter a capacidade de digitalizar documentos pode ser relevante em casos de pornografia infantil, burlas, contrafação d moeda ou usurpação de identidade.

Acresce ainda que imperfeições tais como marcas no vidro do aparelho, podem ajudar a provar a origem da digitalização de determinado documento.

Consultar a secção sobre as regras de recolha.

Fotocopiadoras

Algumas fotocopiadoras mantêm registos de utilização quer de utilizadores quer de cópias realizadas. Podem também conter documentos em memória.

As provas potenciais destes dispositivos são:

- Documentos;
- Data e Hora;
- Logs.

Consultar a secção sobre scanners e a secção para as regras de recolha.

Multifunções ou Allinone

Os dispositivos acima referidos podem ser combinados num só. Esta combinação pode ser física ou lógica no caso de ser utilizada uma rede.

Pagers

Um pager é um dispositivo que caiu em desuso, mas era muito utilizado para enviar e receber mensagens de texto. Nestes casos deve-se seguir as instruções gerais.

Dispositivos de GPS

Estes dispositivos permitem a localização geográfica através da utilização de satélites e podem conter diversas informações sobre percursos efetuados e waypoints. Alguns registam automaticamente estas informações e outros logs.

As provas potenciais destes dispositivos são:

- Home ou destino de origem por defeito;
- Destinos anteriores;
- Logs de viagens;
- Informação de Trace/route;
- Coordenadas e nomes de Waypoints.

Consultar a secção sobre as regras de recolha.

Relógios Digitais

Existem muitos tipos de relógios digitais que podem igualmente funcionar como pagers, agendas, conter contactos, mensagens de correio eletrónico, podendo ter capacidades de sincronização com computadores.

As provas potenciais destes dispositivos são:

- Agenda de moradas;
- Agenda de compromissos;
- Mensagens de correio eletrónico;
- Notas;
- Números de telefone.

Podem ainda conter um token USB ou até uma câmara digital.

Consultar a secção sobre as regras de recolha.

Leitores de bandas magnéticas

Também designados por skimmers, são utilizados para ler as informações contidas nas bandas magnéticas dos cartões que as possuam.

As provas potenciais que podem ser lidas nestas bandas são:

- Informação sobre o titular do cartão, tais como:
  - Data de expiração do cartão
  - Número do cartão;
  - Informação de segurança.

Consultar a secção sobre as regras de recolha.

Anexo II - Glossário gráfico

Neste Glossário, pretende-se não só ilustrar os diversos equipamentos a que se fez referência durante o Anexo anterior, bem como mostrar as diversas variantes que estes podem apresentar.

Em algumas situações é fornecida a denominação em Inglês, uma vez que muitas vezes no meio informático são utilizadas estas denominações em vez das portuguesas.

O objectivo deste glossário gráfico é a de permitir de uma forma fácil, a criação de um guia de bolso para primeira resposta a funcionários com menos formação técnica, mas que tenham de atuar numa primeira resposta a incidentes técnicos, onde é necessário lidar com prova digital e executar os procedimentos especificados no Anexo I, onde muitos destes objectos são referidos.

Atendedor de Chamadas	Dispositivo eletrónico que faz parte do telefone ou está ligado entre este e o ponto de entrada da ligação da empresa prestadora do serviço.  
Argos	Sistema de geolocalização que armazena históricos. 
Arquivo	Um arquivo é um conjunto de ficheiros informáticos que foram compactados num só ficheiro. Esta compactação é feita por programas, que podem ser do próprio sistema operativo. No caso do Windows os mais populares são o Winzip e o 7-Zip. Estes compactadores permitem a colocação de palavras-chave para aceder aos ficheiros que contêm.  

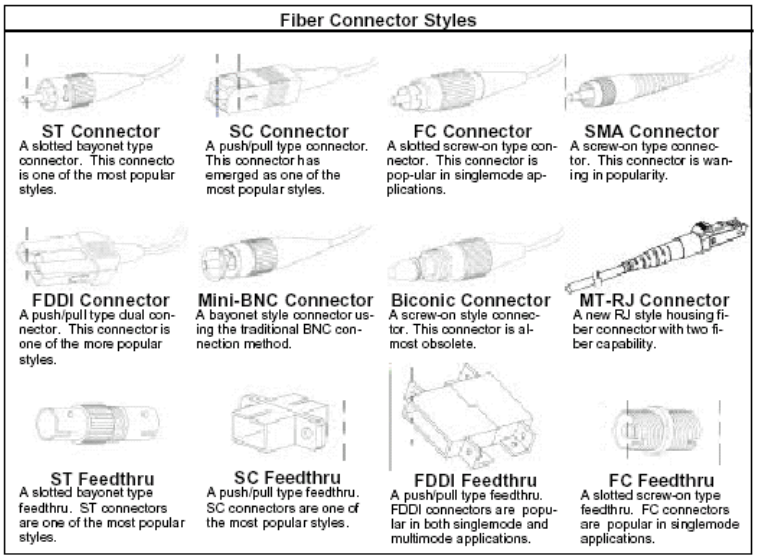
ATM	Automatic Teller Machine. A vulgarmente denominada caixa Multibanco.  
Backup	Uma cópia da informação de um determinado sistema informático.
Scanner Biométrico	Dispositivo que ligado a um sistema informático, reconhece características físicas do interlocutor, tais como impressões digitais, voz, retina e peso.   
BIOS	É o acrónimo de Basic Input Output System. É um conjunto de retinas armazenadas em memória ROM e que permite ao computador arrancar com o sistema operativo e que este comunique com todos os periféricos do sistema, tais como disco rígidos, teclado, rato, monitor e portos de comunicação.  

Bluetooth	É uma especificação da indústria para a comunicação sem fios de curta distância (Wireless), entre telefones, PDAs, teclados, ratos e o computador. Esta tecnologia requer que o dispositivo tenha um chip transceiver Bluetooth. 
Carrinho de transporte	
Card-Reader	Ver Smart Card Reader ou PC Card Reader 
CD-ROM CD-R CD-RW	Compact disk-read only memory: Disco ótico com dados para serem lidos.  Compact disk-recordable: Disco ótico, que permite a gravação uma única vez de dados e posterior leitura.

	 Compact disk-rewritable: Disco ótico no qual pode ser escrita e rescrita informação. 
Circuito Impresso	Uma placa em plástico contendo circuito e dispositivos eletrónicos. 
CMOS	Acrónimo de Complementary metal-oxide semiconductor. Define a tecnologia utilizada nos transístores presentes no microchip. Normalmente armazena as preferências e opções da BIOS e é alimentado por uma bateria.  

Utilizados para ligar os diversos periféricos à unidade principal do computador.

Podem ter diversas cores, grossuras e formas e apresentarem diversos tipos de fichas, dependendo dos componentes.



Cabos de Computador

Fichas dos Cabos

Various cables for computer and net


Various cables for computer and net


Various cables for computer and net


Cabo PS2

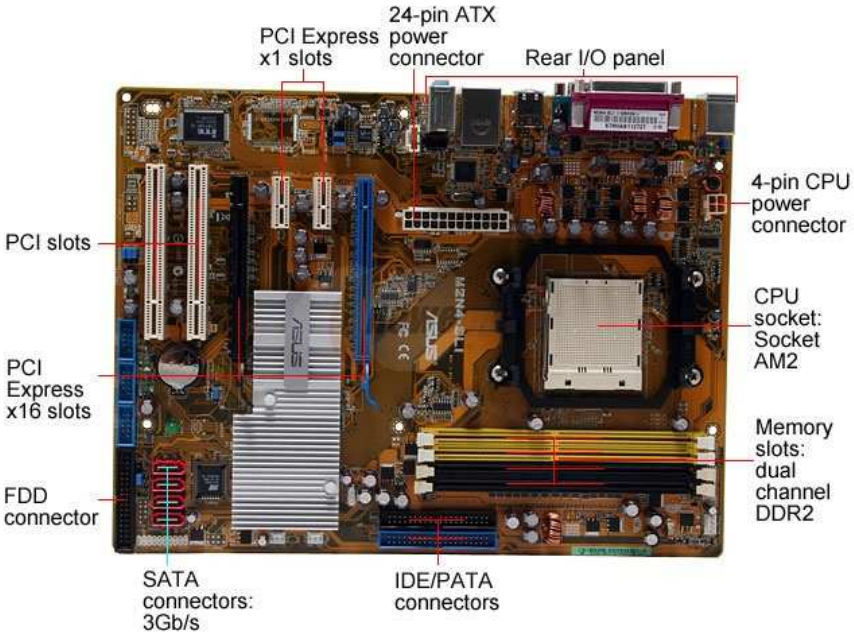
	 Cabo SCSI  Cabo Paralelo  Cabo série  Cabo USB

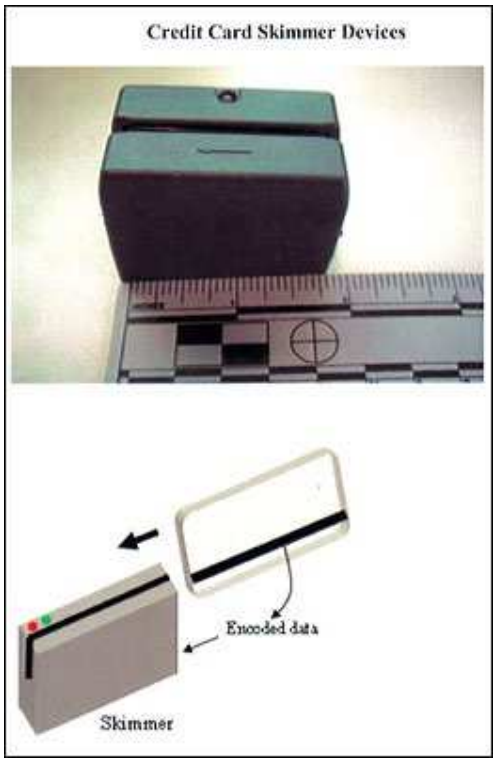
<table>
<tr>
<td></td>
<td>

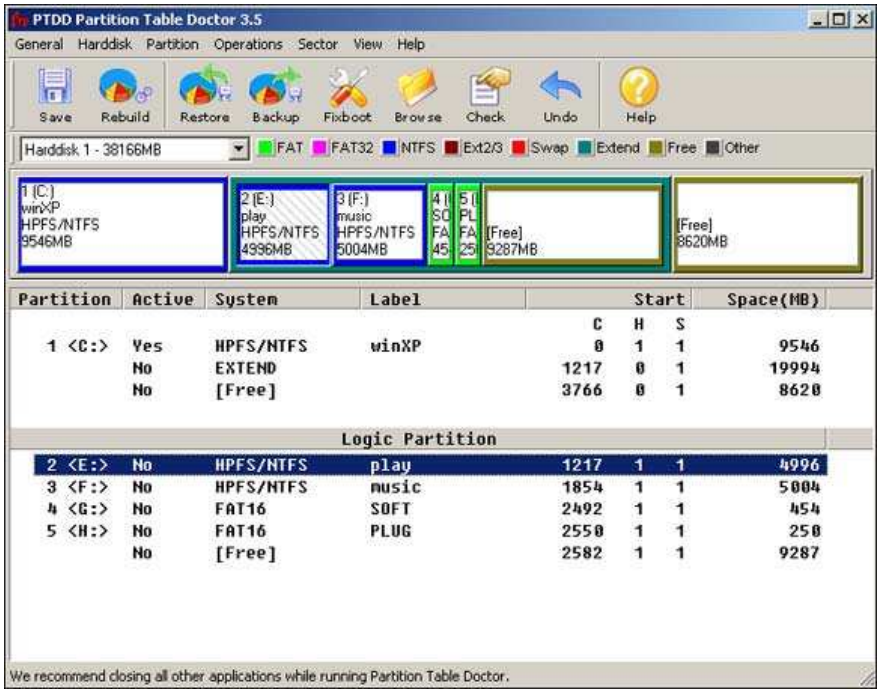

Fichas USB

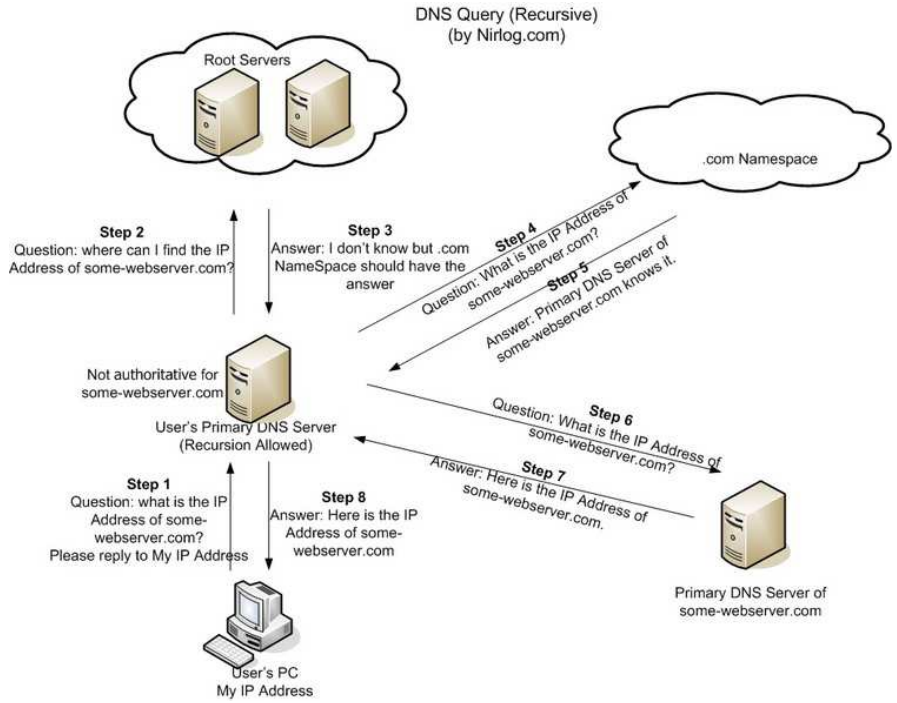
Cabo vídeo e áudio</td>
</tr>
<tr>
<td>Smart Card de proximidade</td>
<td>São smart Cards que permitem a leitura do chip por proximidade ao leitor.

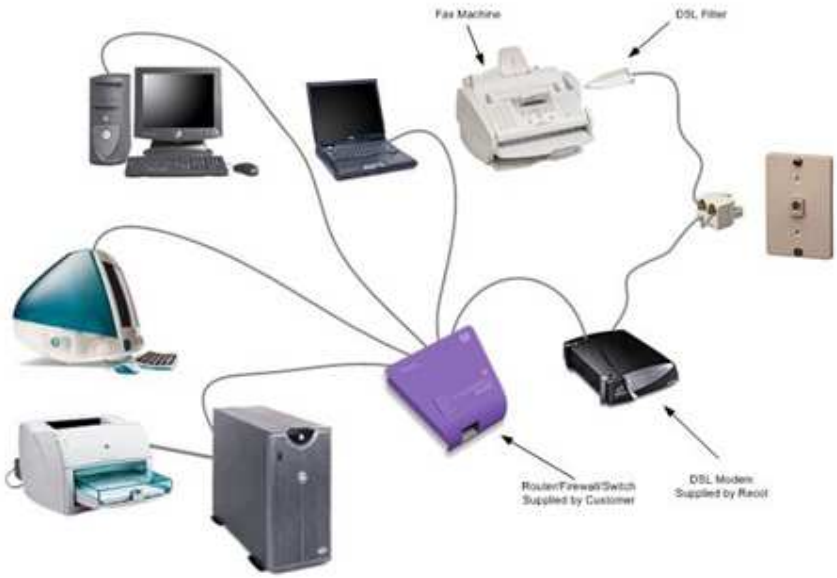
 </td>
</tr>
<tr>
<td>Máquina de cópias</td>
<td>Ver fotocopiadora</td>
</tr>
</table>

CPU	Acrónimo de Central Processing Unit. É o microchip que controla todo o computador. Localizado no interior do computador, mais concretamente no circuito impresso denominado MotherBoard é o "cérebro" que executa todos os cálculos aritméticos e lógicos e que controla todo o computador.   
Cradle	Dispositivo que permite a sincronização entre o PDA ou smartphone e o computador. 

Skimmer de cartão magnético	Leitor de banda magnética de cartões de crédito ou débito. 
Criptografia	Aplicação de algoritmos matemáticos que permitem tornar a informação ilegível para quem não conheça a chave secreta.
Gravador de voz	Dispositivo portátil que permite gravar som na sua memória interna. 
Câmara digital	Dispositivo que permite gravar fotografias e filmes em formato digital. As WebCams permitem a realização de vídeo-conferência. 

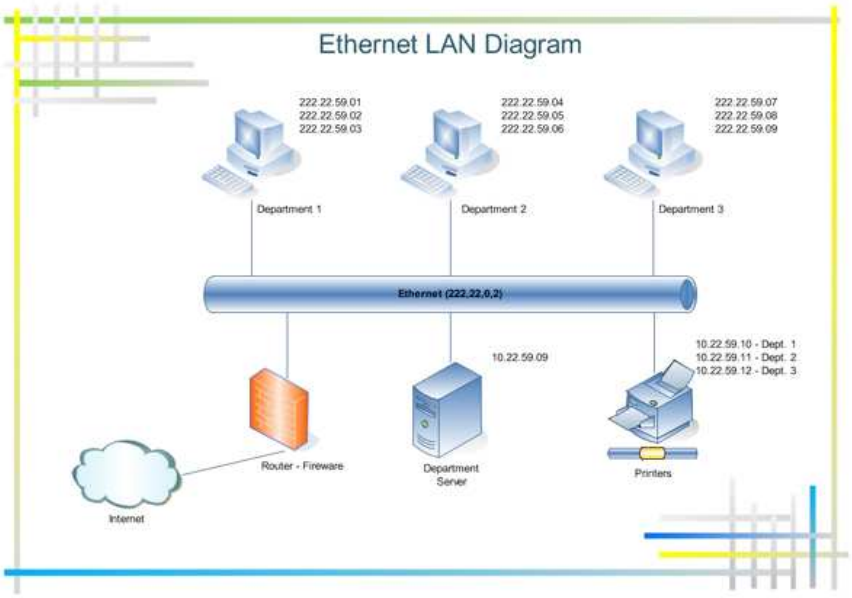
Certificado Digital Digital ID	Código digital, que permite a identificação inequívoca de uma pessoa (ver certificado de chave pública)
Assinatura Digital	Código digital que permite ao recetor de uma mensagem verificar da autenticidade e da identificação do remetente.
Relógio Digital	Relógio digital convencional, mas que pode conter funções de pager e guardar dados na sua memoria, tal como um qualquer PDA. 
Partição do Disco Rígido	Nos PCs, uma partição é uma divisão lógica do seu disco rígido, que permite ter diversos sistemas operativos simultaneamente e aparentar a existência de diversos discos físicos. Normalmente a cada partição está associada uma letra do alfabeto (“C:”, “A:”, “D:”). 

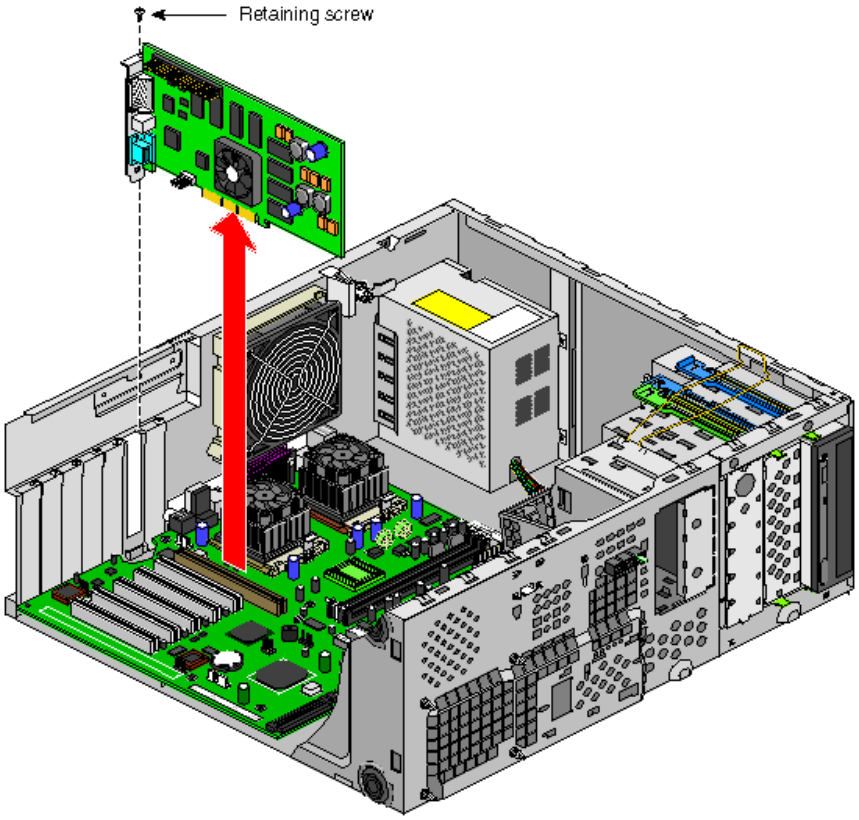
DNS	Acrónimo de Domain Name Service. É um serviço de rede de computadores que permite assignar nomes de máquinas a endereços IP e vice-versa. É uma espécie de páginas amarelas das máquinas de uma rede de computadores. Por exemplo se for perguntado a um servidor DNS qual o host name do endereço 74.125.77.99, este responderá que é www.google.com. 
Docking station	Dispositivo de acoplamento de um computador portátil, que permite utilizar periféricos tais como monitor, teclado e rato tal como se fosse um desktop. 

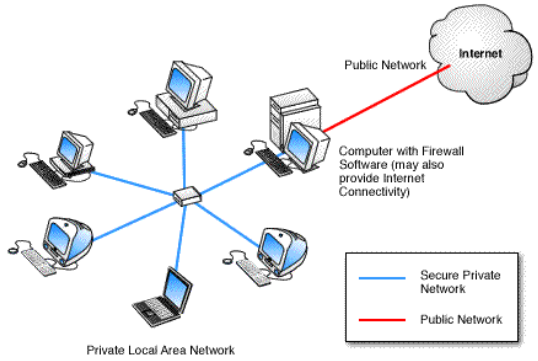
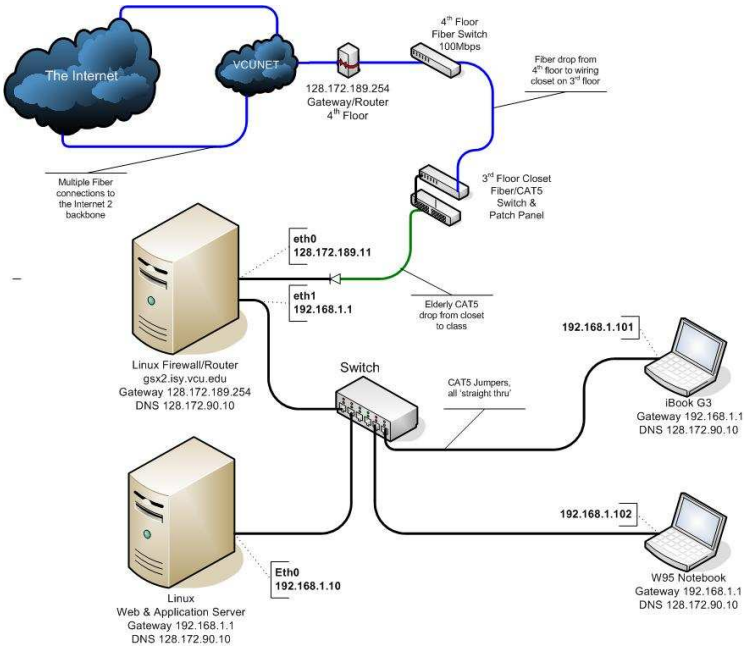
Dongle	Dispositivo, que pode ser USB ou de porta paralela e que cotem informação idêntica àquela contida num smart card. Normalmente é utilizado para armazenar chaves de determinado software sem o qual este não funciona. 
Duplicador de Discos	Dispositivo para cópia rápida de dispositivos de armazenamento tais como discos rígidos ou discos óticos. 
DSL	Acrónimo de Digital Subscriber Line. É um conjunto de protocolos que permite uma ligação de grande débito, através de uma normal linha de telefone. Necessita sempre de um modem adequado. 

DVD	Acrónimo de Digital Versatile Disk. Disco ótico de similar aparência a um Compact Disk, mas que tem uma capacidade muito superior (4.3 GB para os normais) 
Prova Digital	Ver prova eletrónica
E-mail	A troca de mensagens entre computadores, com aplicações que simulam a utilização do correio tradicional.
E-mail header ou cabeçalho	As mensagens de correio eletrónico são compostas por duas partes: O corpo e o cabeçalho (Header). O cabeçalho normal tem detalhes da mensagem, tais como hora e data de envio, remetente e assunto. Todas as mensagens também têm um cabeçalho estendido, que vai sendo escrita pelos diversos servidores de correio por onde vai passando a mensagem e que permite na maioria das situações identificar a máquina que esteve na origem da mensagem. Exemplo: *X-Message-Delivery: Vj0xLjE7dXM9MDtsPTA7YT0xO0Q9MTtTQ0w9MA==* *X-Message-Status: n:0* *X-SID-PRA: mail@dukevideo.com* *X-SID-Result: Pass* *X-Message-Info: JGTYoYF78jEDRA/wagTiWVIzaCVWmX2zAIeuTqjgxW+h6XdOHl1g7Q9QXPJF0//uj97oPzsEyVNp3M8Rk5scw6f3Xj8Je9dw* *Received: from clark.dukevideo.com ([89.107.1.19]) by bay0-mc8-f4.bay0.hotmail.com with Microsoft SMTPSVC(6.0.3790.2668);* *Tue, 26 May 2009 00:16:26 -0700* *Received: from mcrae ([192.168.10.12]) by clark.dukevideo.com with Microsoft SMTPSVC(6.0.3790.3959);* *Tue, 26 May 2009 08:15:50 +0100*

	MIME-Version: 1.0 *From: mail@dukevideo.com* *To: caixadeteste@hotmail.com* *Date: 26 May 2009 08:15:50 +0100* *Subject: dukevideo.com Despatch notification* *Content-Type: text/plain; charset=us-ascii* *Content-Transfer-Encoding: quoted-printable* *Return-Path: mail@dukevideo.com* *Message-ID: <CLARKDjpA4pbSmqZGUT0009889c@clark.dukevideo.com>* *X-OriginalArrivalTime: 26 May 2009 07:15:50.0219 (UTC) FILETIME=[CC4BC1B0:01C9DDD1]*
Prova Eletrónica	Dados com interesse para a investigação e que estão armazenados num dispositivo eletrónico ou foram transmitidos por um dispositivo eletrónico.
Assinatura eletrónica	Ver assinatura digital.
Encriptação	Método de codificar dados, para transformar texto corrente em texto cifrado, através de uma chave criptográfica de forma a evitar que mais ninguém a não ser o legítimo proprietário leia o seu conteúdo.

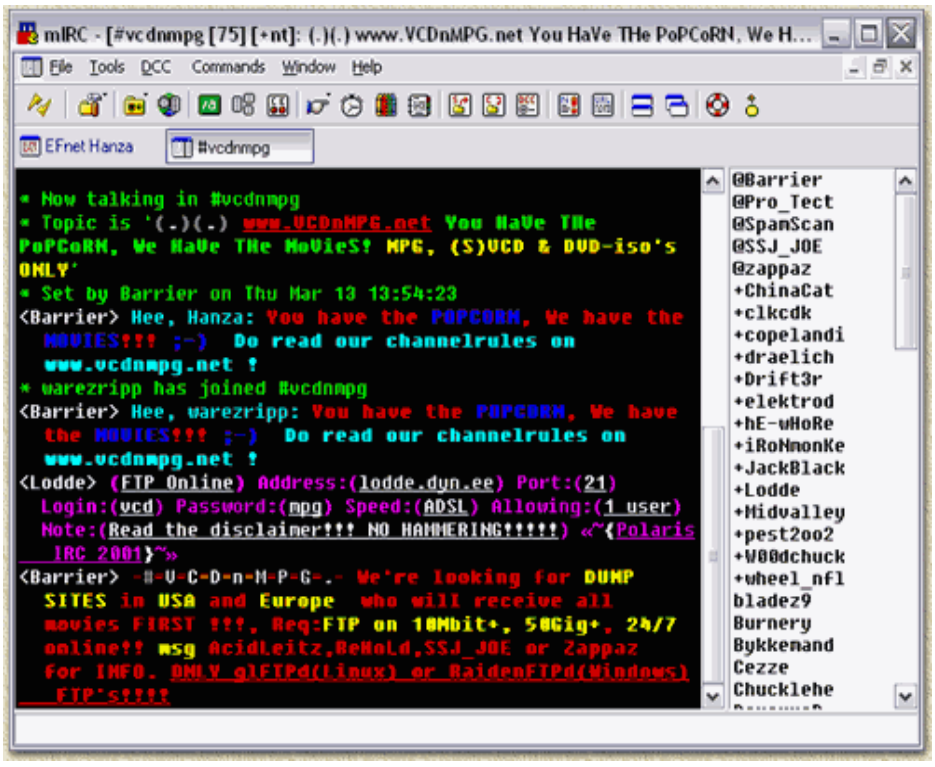
Ethernet	Tecnologia de rede mais utilizada. É especificada pelo standard IEEE 802.3, inicialmente desenvolvida pela Xerox e mais tarde por um consórcio formado pela própria Xerox, a DEC e a Intel. Este tipo de rede pode funcionar através de vários tipos de cabos, tais como coaxial, par entrançado ou fibra ótica e utiliza endereços MAC do tipo 01-23-45-67-89-ab.  

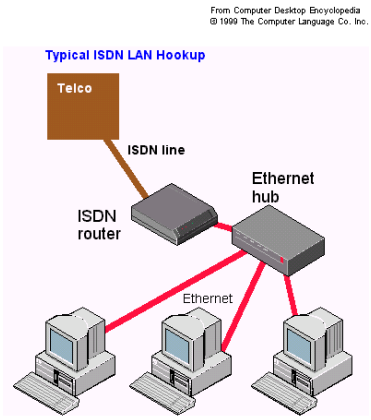
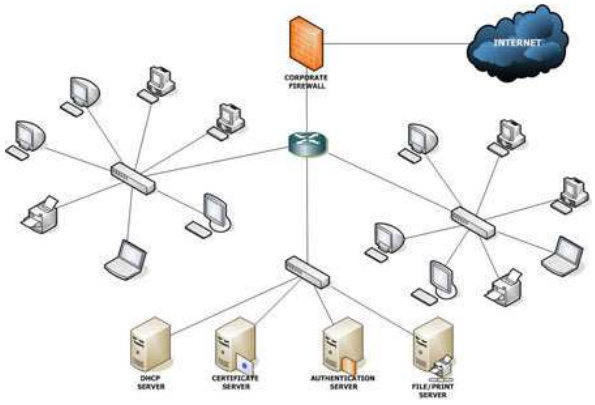
Placa de expansão	Circuito impresso que inserido num computador, lhe adiciona capacidades, tais como vídeo, rede, etc. 
Fac-simile ou Fax	Dispositivo que digitaliza imagens ou documentos e que os envia através de uma linha telefónica. Os mais modernos possuem memória interna para documentos e registam as origens e os destinos dos documentos trocados. 
File system ou sistema de ficheiros	Define a maneira como os ficheiros são nomeados e como são armazenados no disco do computador. O MS-DOS, Windows, OS/2, Macintosh, e sistemas baseados em UNIX, tal como o Linux, todos têm um sistema próprio de hierarquização dos ficheiros.

Firewall	Um conjunto de programas, que podem estar a ser executados numa máquina de rede, que pode ser um router, um servidor de rede denominado gateway, ou um normal computador pessoal e que tem como função a proteção dos recursos de uma rede privada de utilizadores externos não autorizados.   

First responder	O agente que em primeiro lugar chega ao local do crime ou incidente.
Cartão de memória Flash	Ver cartão de memória. A memória flash (por vezes denominada flash RAM) é um tipo de memória não volátil que pode ser apagada e reescrita. 
Floppy disk, Diskette ou Disquete	Disco flexível que armazena informação de forma magnética. Caiu um pouco em desuso e há diversos tipos: 3½ e 5-¼ polegadas. 
FTP	Acrónimo de File Transfer Protocol e que define um protocolo que permite a transferência de ficheiros entre computadores da mesma rede ou através da Internet.
Gameboy	Consola portátil de jogos, que se introduzem por cassetes (cartridges). 
Gamecube	Consola de Jogos. 

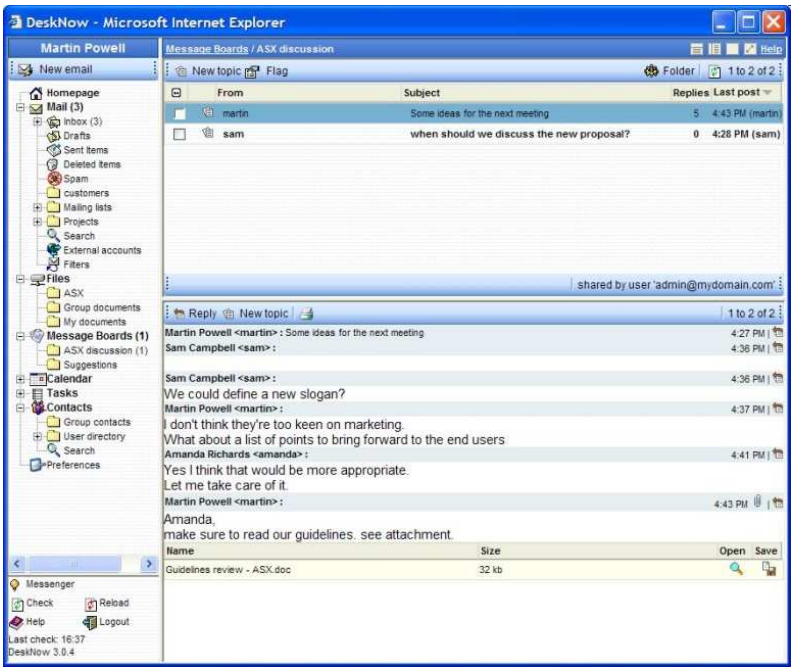
Dispositivo de GPS	Acrónimo de Global Positioning System e que utiliza uma constelação de entre 24 e 32 satélite geoestacionários que emite sinais por rádio frequência, que permitem a aparelhos de uso pessoal determinar com precisam a sua posição no planeta. A precisão varia entre os 100 e os 10 metros, estando as distâncias inferiores aos 10 metros reservadas para aplicações militares. Muitos destes aparelhos guardam um histórico dos locais por onde passaram, com datas e horas entre outros dados. 
Disco rígido ou *Hard Drive*	É uma caixa selada, que contem os discos magnéticos que armazenam dados. Podem ser internos ou externos ao Computador. 
Ficheiros escondidos ou *Hidden Files*	É um ficheiro que não aparece numa normal listagem ou pesquisa do sistema operativo. Em alguns sistemas operativos esta propriedade pode ser alterada pelo utilizador que criou o ficheiro.
Hub	Dispositivo de convergência numa rede local, onde os dados de um computador são distribuídos pelas restantes portas. 
Imaging, imagem ou duplicação	Criar uma cópia exata (bit a bit) do conteúdo digital de determinada memória.
IMAP	Acrónimo de Internet Message Access Protocol. É um protocolo de comunicações que permite receber ou consultar mensagens de correio eletrónico do respetivo servidor.

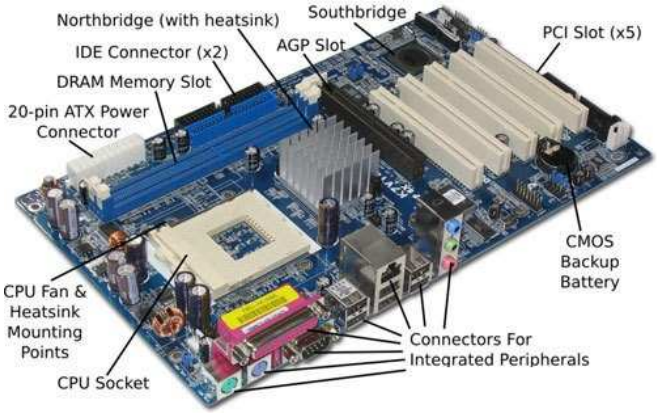
Infrared ou infravermelho	É uma tecnologia de transmissão de dados sem fios, com raios de alcance reduzido e com utilizações que vão desde redes locais wireless, ligações entre portáteis e PCs ou PDAs ou impressoras, entre outros. Infravermelho refere-se aos comprimentos de onda utilizados.  
IP	Acrónimo de Internet Protocol. É o protocolo mais utilizado hoje em dia nas comunicações entre computadores. A mais usada é a versão 4, e é composta por uma sequência de 4 bytes, sendo apresentada na sua notação decimal, tendo o aspeto do tipo, 192.67.198.7.
IRC	Acrónimo de Internet Relay Chat. É um serviço que disponibiliza uma interface de conversação online e de troca de ficheiros através do DCC (Direct Computer Connect) . 

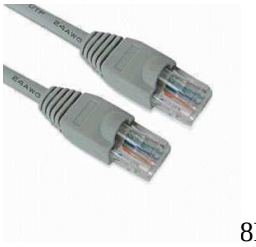
ISDN	Acrónimo de Integrated Services Digital Network. É uma linha de telefone de alto débito, em português identificada por RDIS. 
ISP	Acrónimo de Internet service provider e que corresponde às organizações que disponibilizam serviços de acesso à Internet, seja através da linha telefónica, cabo, satélite ou outros.
JAZ®	É um tipo de disco portátil ou disquete de grande capacidade que teve grande uso no passado. Era vendida pela Iomega Corporation, a mesma que desenvolveu a ZIP drive. Ambas eram comercializadas em dois tamanhos, de 1 GB e 2 GB. 
LAN	Acrónimo de Local Area Network. Nome comum, para as tecnologias de rede estandardizadas pelo IEEE (Institute of Electrical and Electronics Engineers) e que corresponde a uma rede local de uma habitação ou empresa. 

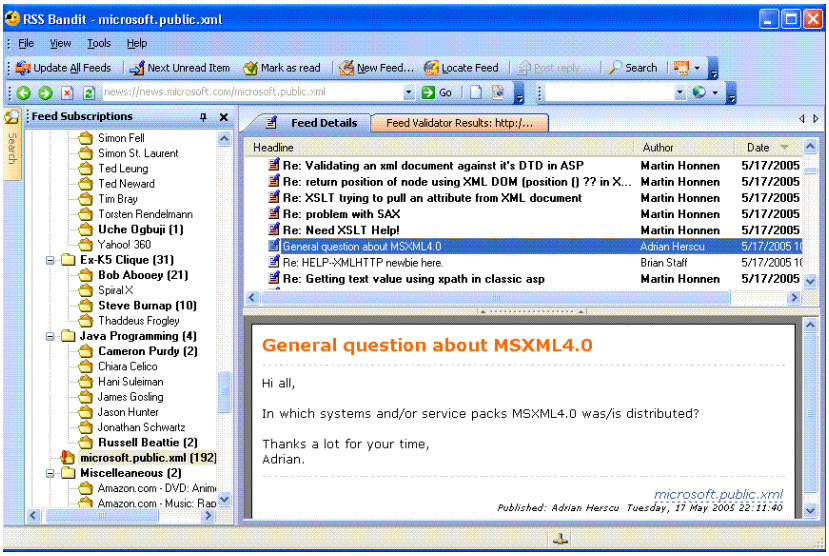
LAN configuration ou configuração de rede	É a tecnologia de rede que é utilizada, de que são exemplo a Ethernet e a Token Ring.
LDAP	Acrónimo de Lightweight Directory Access Protocol. É um conjunto de protocolos que permite aceder a directorias ou bases de dados remotas, algures na Internet.
Cartão de Banda Magnética	Cartão de plástico, vulgarmente identificado com o cartão multibanco e que possui uma banda magnética que permite gravar dados tais como informação bancária ou dados pessoais.  
Leitor de banda magnética	Dispositivo que permite ler a banda magnética de cartões. 
Cassete de fita magnética	É uma cassete parecida com as cassetes de vídeo 8mm, mas de grande capacidade (8GB ou 24GB), denominadas DAT, normalmente utilizadas para armazenar backups de sistemas informáticos. 

Mainframe	É um termo que se vulgarizou para denominar os grandes computadores dos anos 70 e 80. 
Main Unit ou unidade Principal	É normalmente a maior peça de um computador. É a caixa que contém a Motherboard com o processador. Pode ter várias configurações, que correspondem à denominação que assumem. Tower na vertical ou desktop na horizontal, para colocar em cima da secretária. 
Memory card ou cartão de memória	Também denominado por cartão Flash e é um pequeno cartão de armazenamento de dados. Existem muitos formatos e de muitas capacidades no mercado, sendo as mais populares as denominações SD card(Secure Digital), CF card (CompactFlash da SanDisk), SmartMedia (da Toshiba), Memory Stick (da Sony), e o MultiMediaCard (MMC da SanDisk e da Siemens AG/Infineon Technologies AG). A maioria tem memória não volátil (não se apaga e não necessita de estar ligada a uma fonte de energia. Pode ser usada em diversos tipos de aparelhos, desde computadores a máquinas fotográficas até PDA ou smart phones. 

Código *HASH*	É um número calculado com base no conteúdo de um ficheiro informático e que é único para cada ficheiro. Isto permite garantir que determinado ficheiro não foi alterado, desde que o código *hash* se mantenha inalterado.
Endereço MAC	É o número único que identifica a placa de rede de determinado dispositivo.
Message board	É um serviço online que disponibiliza um local onde as pessoas podem trocar mensagens e ficheiros e que pode ser público ou privado, onde só se entra com convite dos administradores do board. Também denominado BBS de bulletin board e têm normalmente temas ou áreas de interesse definidos. 
Smart Phone	Telefone portátil, normalmente com capacidade de processamento de programas e com câmara de fotografar/filmar. 

Modem	Acrónimo de MOdulator/DEModulator. É um dispositivo utilizado por computadores para comunicar através de um meio que não é o seu, tal como a linha de telefone ou o cabo de sinal de televisão. 
Motherboard	É o circuito impresso principal de um computador e que contém os seus principais componentes, tais como o processador e as controladoras dos discos e outros periféricos. 
Mouse ou Rato	É um periférico de entrada (input), que permite a deslocação do curso no ecrã do computador. Pode apresentar diversos tipos de fichas, tais como,  PS/2  serial  USB e PS/2  cordless/infrared Exemplos de ratos:  

MP3	Corresponde a MPEG-1 Audio Layer-3, que é um standard de tecnologia e de formato de compressão para um ficheiro de som e que corresponde a cerca de 1/12 do tamanho original do ficheiro de som, sem que seja perdido o nível de qualidade de som.
Rede ou Network	Um grupo de computadores ligados entre si e que partilham recursos se dados. Pode ser uma pequena rede local ou uma grande rede como a Internet. A ilustração mostra um bastidor de uma LAN, onde estão ligados diversos computadores. 
Cabo de rede e ficha	É através deles que são ligados os diversos componentes de uma rede de computadores. Há de diversos tipos, cores e espessuras, sendo as mais comuns as seguintes:  8P8C (normalmente denominado RJ 45), para par entrançado  BNC, para cabo coaxial  conectores SC e ST, para Cabo fibra ótica

NIC ou placa de rede	Acrónimo de Network interface Card e é o circuito que permite a ligação de um dispositivo a uma rede informática. Pode ser de cabo ou wireless e pode ser uma placa de expansão ou uma placa 
Newsgroup	É um service para redes que permite a discussão de um determinado tema, através de notas que os seus utilizadores vão ai colocando. Está normalmente alojado num servidor na Internet configurado para o efeito e é distribuído através da Usenet. Cada utilizador necessita de um programa cliente para aceder a essa rede: 
Prova não eletrónica	Objetos relevantes para a prova de um processo-crime, relacionados com a prova digital que foi apreendida, mas que estão num suporte não eletrónico. Exemplos são post-its com passwords ou outras notas escritas, manuais dos equipamentos, calendários, literatura e impressões de documentos.
Sistema Operativo	São os programas que são carregados para a memória do computador logo a seguir à BIOS e encarrega-se da comunicação dos programas do utilizador com os componentes do computador. Exemplos para computadores pessoais são o MSDOS, o Microsoft Windows XP ou Vista, o Unix, o Linux ou o Mac OS. Para PDAs, pode ter-se o Palm OS, o Psion EPOC ou o Windows CE.

ORB	É um disco rígido amovível d grande capacidade. As drives ORB utilizam tecnologia magnetoresistive (MR) para as cabeças de leitura e escrita. 
Pager	Dispositivo portátil, que caiu em desuso e que contém, elementos voláteis de números de telefone, voice-mail e email. 
Dongle de porta paralela	Idêntico ao dongle USB mas para ligar à porta paralela do computador. 
Password ou palavra-chave	É uma sequência alfanumérica de caracteres e que permite limitar o acesso a recursos sejam eles hardware ou software. Pode também ser referida como *Pass Phrase* ou PIN (*Personal Identification Number*).

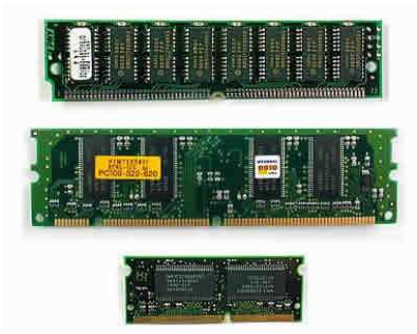
PC	Acrónimo de *Personal Computer*. Foi um termo inicialmente designado pela IBM, para identificar os computadores que lançou no Mercado e de uso individual. Normalmente são constituídos por uma unidade central, um monitor, um teclado e um rato.    
Placa de PC	Ver placa PCMCIA.
Leitor de placa de PC	ver leitor de placas PCMCIA.
PCMCIA	Acrónimo de *Personal Computer Memory Card International Association*. Cerca de 500 empresas definiram um standard para placas de pequena dimensão para computadores pessoais. Originalmente concebida para dar maior memória aos PCs portáteis, rapidamente foram expandidas as suas aplicações. Ver placa PC.

Placa PCMCIA	São placas baseadas nos standards PCMCIA e que são inseridas em slots de um computador portátil. Podem ter várias funcionalidades, tais como memoria, input/output, como sejam modems ou adaptadores ou até discos rígidos. Existem três tipos de placas, todas retangulares (85.6mm por 54 mm). Ver cartão de memória. 
Leitor de placas PCMCIA	É um dispositivo que permite ler várias placas PCMCIA e que pode ter interfaces USB ou porta paralela. 
Agenda Digital ou Personal digital assistant (PDA)	É um pequeno dispositivo com capacidade de computação, telefone/fax, acesso à Internet, GPS, máquina fotográfica, etc. 

PEN Drive	Dispositivo de memória com interface USB e que pode ter os mais variados feitios. 
PGP	Acrónimo de *Pretty Good Privacy*. É um software de criptografia de livre utilização. Pode ser utilizado para encriptar e assinar digitalmente mensagens de correio eletrónico ou ficheiros num computador, utilizando um sistema de chave assimétrica.

Fotocopiadora	Dispositivo que permite copiar documentos. Alguns modelos guardam em memória e por utilizador, cópias dos documentos digitalizados. 
Playstation	É uma consola de jogos com grande capacidade computacional e nalguns modelos com disco interno. 
POP POP3	Acrónimo de *Post Office Protocol*. É um protocolo que permite o acesso e a cópia/leitura de mensagens de correio eletrónico que estejam alojados num servidor.
Port, porta ou porto	É um termo que pode ter dois significados: • Um conector num dispositivo. (ex:Porta USB ou porta Paralela); • Um endereço da pilha TCP/IP, que conjuntamente com um endereço IP, identifica um serviço. (Port 21 é uma porta ftp ou port 80 que é a porta http, para o serviço de acesso à Internet)
Replicador de portas	É um dispositivo que pode ter uma interface USB e que permite a ligação de diversos dispositivos série, paralelos ou de rede. 

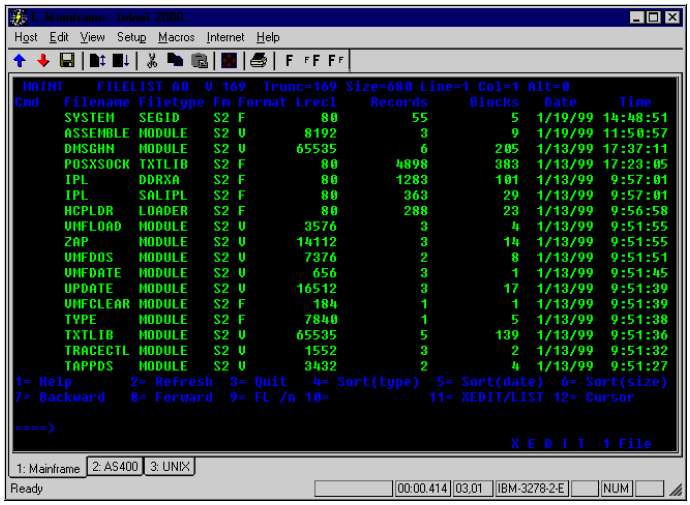
Computador portátil	É um PC na forma portátil. Também designado por notebook ou laptop. 
impressora	Dispositivo de impressão de documentos. Alguns modelos possuem memória de impressão.  
Public key Certificate ou Centro de Certificado Digital	É uma entidade emissora de certificados digitais (digital ID) e que tem de ser idónea. Em Portugal a entidade oficial é o ICP (infra-estrutura de Chave Pública) do ITIJ Este certificado atesta que determinada chave público é de determinada pessoa ou organização. As chaves públicas são usadas para verificar assinaturas digitais, que por sua vez são criadas com a correspondente chave privada, que deve ser mantida secreta pelo seu proprietário, por exemplo num cartão smart card protegido por PIN.
Sistemas modulares montados em Racks	Descreve um equipamento eletrónico modular e que está montado numa estrutura metálica denominada rack. 

RAM	Acrónimo de *Random Access Memory*. É o local onde o computador quando ligado coloca o sistema operativo, os programas que está a executar e os dados com que está a trabalhar. É a memória de acesso mais rápido no entanto é volátil, isto é, uma vez desligado o computador esta perda toda a informação. 
Router ou encaminhador	É um dispositivo ou em alguns casos um programa num computador, que determina para que ponto da rede, determinado pacote de informação deverá ser enviado para que chegue ao seu destino. Está ligado entre duas redes distintas e normalmente entre a rede privada e de uma empresa e a rede pública. 
Scanner	Dispositivo ótico que ligado a um computador permite criar uma cópia digital de um documento em papel. 
Screen saver	É um utilitário do sistema operativo e que permite salvaguardar o monitor de ficar muito tempo com a mesma imagem parada, danificando-o. Pode estar configurado para ser desativado unicamente através de palavra-chave, o que o torna num meio de restringir o acesso a uma máquina.

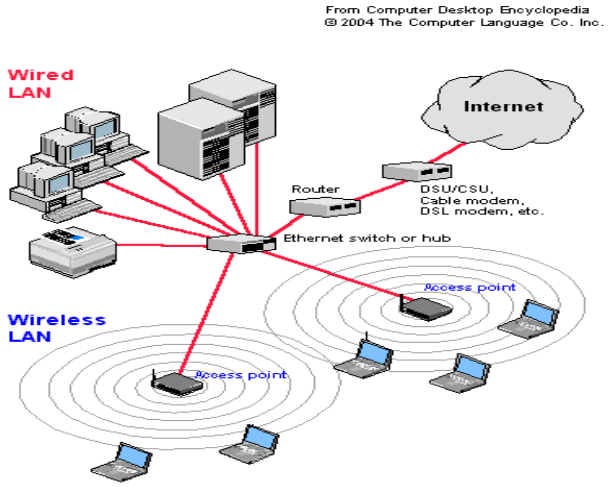
Dongle de segurança	Dispositivo idêntico aos dongles que contém programas de restrição de acessos à máquina ao qual está ligado.
Disquete forense	Disquete especialmente preparada para arranque do sistema operativo e que evite que o sistema se inicie com o sistema operativo dos disco internos.
Dongle de porta série	Dispositivo para ligar à porta série e que pode disponibilizar memória programada, updates remotos ou contadores. 
Cartão SIM	Acrónimo de *Subscriber Identity Module Card*. É um tipo especial de smart card destinado a telefones móveis. 
Sleep mode	Estado de conservação de energia, que desliga o disco e o monitor de um computador e que dá a ilusão de que o mesmo está desligado.
Smart card	É um cartão semelhante a um cartão de crédito, mas contendo um microchip com capacidade de computação e de armazenar informação, tal como informação bancária, chaves de encriptação ou certificados digitais. Normalmente esta informação está protegida por PIN. 

Leitor de Smart Cards	Dispositivo que permite ler a informação contida no chip de um smart card. Leitores de Smart Card  Leitores de Smart Card com Pin Pad 
S/MIME	Acrónimo de *Secure/Multipurpose Internet Mail Extensions*. Constitui um método seguro de enviar mensagens de correio eletrónico.
SMS/MMS	Acrónimo de *Short Message Service/Multimedia Message Service*. São formatos de mensagens escritas ou de multimédia de telefones móveis.
SMTP	Acrónimo de *Simple Mail Transfer Protocol*. É um protocolo que permite o envio de mensagens de correio eletrónico para um servidor (SMTP server).
Disco Solid State	É um dispositivo de memória tal como um normal disco rígido magnético, no entanto armazena os dados em DRAM (dynamic random access memory), ou seja do mesmo tipo da memória interna do computador, logo muito mais rápida, cerca de 200 vezes. 
Cartão de armazenamento	Ver cartão de memória

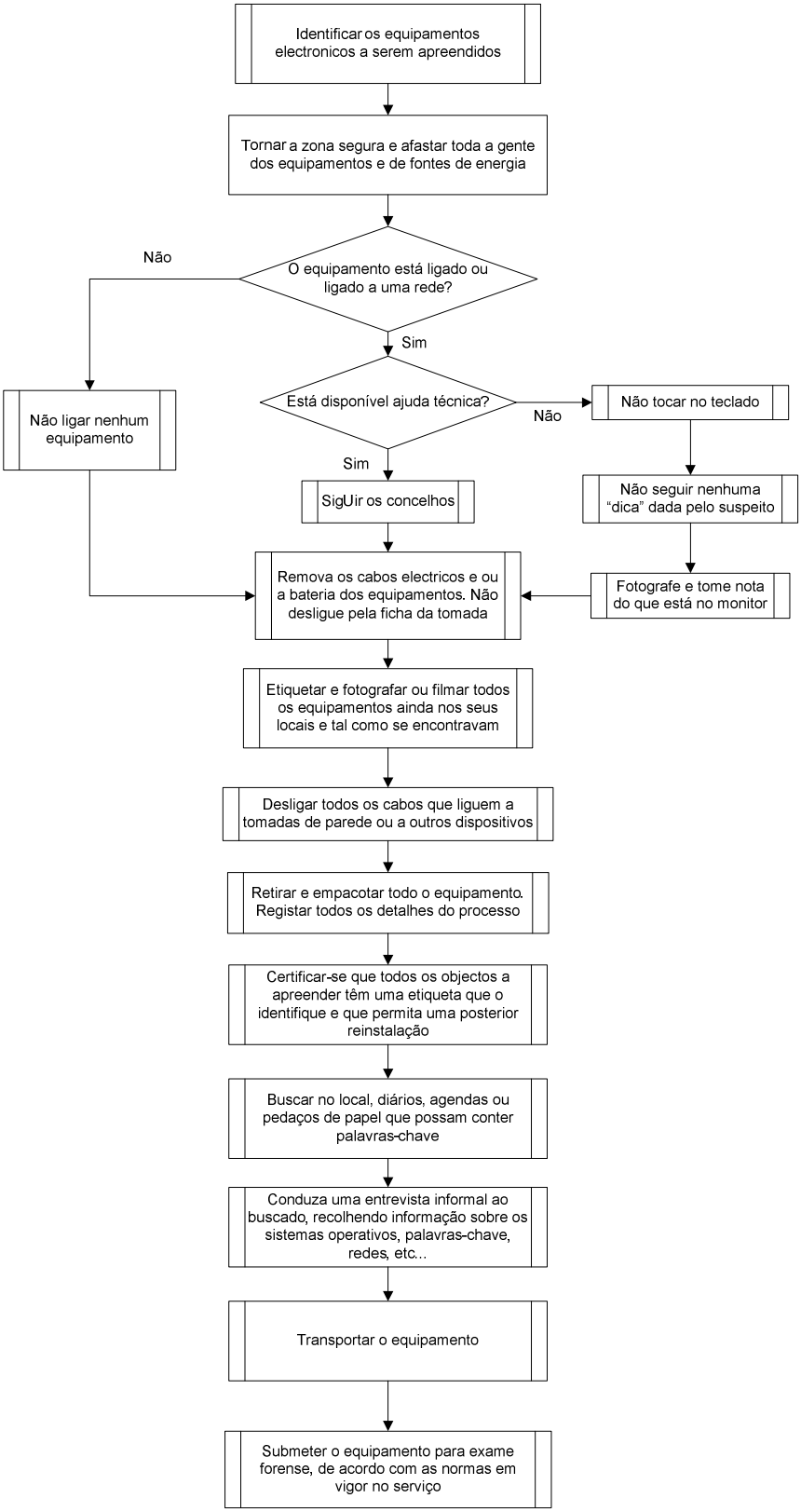
Super smart card	É um smart card comum pequeno display e um teclado numérico.  
Switch	É um dispositivo ativo de rede que canalize a informação originária de uma qualquer porta para a porta de destino onde está o destinatário da informação, diminuindo assim o tráfego na rede e evitando colisões desnecessárias, possibilitando maiores débitos. Numa rede Ethernet o Switch determina a placa de rede de destino com base nos endereços físicos MAC (Media Access Control ou MAC) que vêm na mensagem. 
Administrador do Sistema	É o indivíduo que detém os privilégios na rede que lhe permitem efetuar qualquer operação. Também conhecido como sysop, sysadmin ou system operator.
Tape Drive	Dispositivo de leitura e escrita em tapes ou DATs. 

Telnet	É um protocolo de comunicações entre dispositivos de rede e que normalmente está associado a operações de configuração e manutenção de equipamentos. 
UPS	Acrónimo de *Uninterruptbile Power Supply*. É um dispositivo que permite durante algum tempo, graças às suas baterias internas, manter em funcionamento um sistema informático que lhe esteja ligado, mesmo que a corrente elétrica seja interrompida. 
URL	Acrónimo de *Uniform Resource Locator* e corresponde ao endereço de um ficheiro acessível através da Internet (ex: “http://www.interpol.int”). O tipo de ficheiro depende do protocolo http(Hypertext Transfer Protocol).
USB	Acrónimo de *Universal Serial Bus.* É um interface para Hardware, para periféricos de baixa velocidade, tais como teclados, ratos scanners, impressoras, entre outros. Ver USB Dongle.

Dongle USB	É um pequeno dispositivo com uma porta USB e que possui as mesmas características do Dongle por porta paralela.  Dongle USB  Chave de memória USB  PEN USB
Vírus	É um programa ou um script, normalmente disfarçado como legítimo e que uma vez executado, despoleta uma ação indesejada no sistema informático. Pode ser transmitido como attachs de uma mensagem de correio, num download ou através de uma disquete ou PEN.
Endereço de uma página Web	Um URL ou um endereço IP.
Wireless access Point ou ponto de acesso	Um Hub que permite o acesso wireless a uma determinada rede. 

Wireless LAN ou rede	Wireless Local Area Network. Nome comum para definir as redes estandardizadas pela norma 802.11 do IEEE (Institute of Electrical and Electronics Engineers) e sem fios a ligar os seus componentes. 
World Wide Web (WWW)	Nome porque é conhecida a rede universal de documentos acessível através do protocolo Hypertext TransferProtocol (HTTP).
Xbox	Consola de Jogos da Microsoft. 
ZIP®	É uma evolução da disquete, com maior capacidade e é fabricada pela Iomega. 

Anexo III - Fluxograma/Guia rápido: Dispositivos eletrónicos



Transporte

- Tratar os objectos com cuidado, uma vez que se trata de equipamento frágil
- Mantenha todo o equipamento afastado de fortes campos magnéticos, tais como altifalantes, janelas ou bancos aquecidos ou rádios de comunicações
- Colocar os discos rígidos e as placas de circuitos impressos em sacos anti estáticos
- Não dobrar as disquetes nem lhes colocar estiquetas
- Transportar os monitores de ecrân para baixo, no banco de trás dos veículos e com o cinto e segurança colocado
- Colocar os PDA e agendas electronicas em sacos ou envelopes de papel
- Colocar os teclados, ratos, cabos e modems em sacos arejados e não os armazenar debaixo de pesos.

O que deve ser apreendido

Computadores:

- Unidade Principal. Normalmente a caixa à qual está ligado o teclado e o monitor;
- Monitor;
- Teclado e rato;
- Todos os cabos, incluindo os de corrente;
- Fontes de alimentação;
- Discos rígidos não instalados dentro do computador.

Componentes adicionais:

- Dongles;
- Modems;
- Impressoras e scanners;
- Componentes de rede

Dispositivos de armazenamento portátil:

- Disquetes, Discos opticos, cassetes DAT;
- Disquetes Jaz e Zip;
- Placas PCMCIA;
- Discos rígidos externos;
- Cartões de memória.

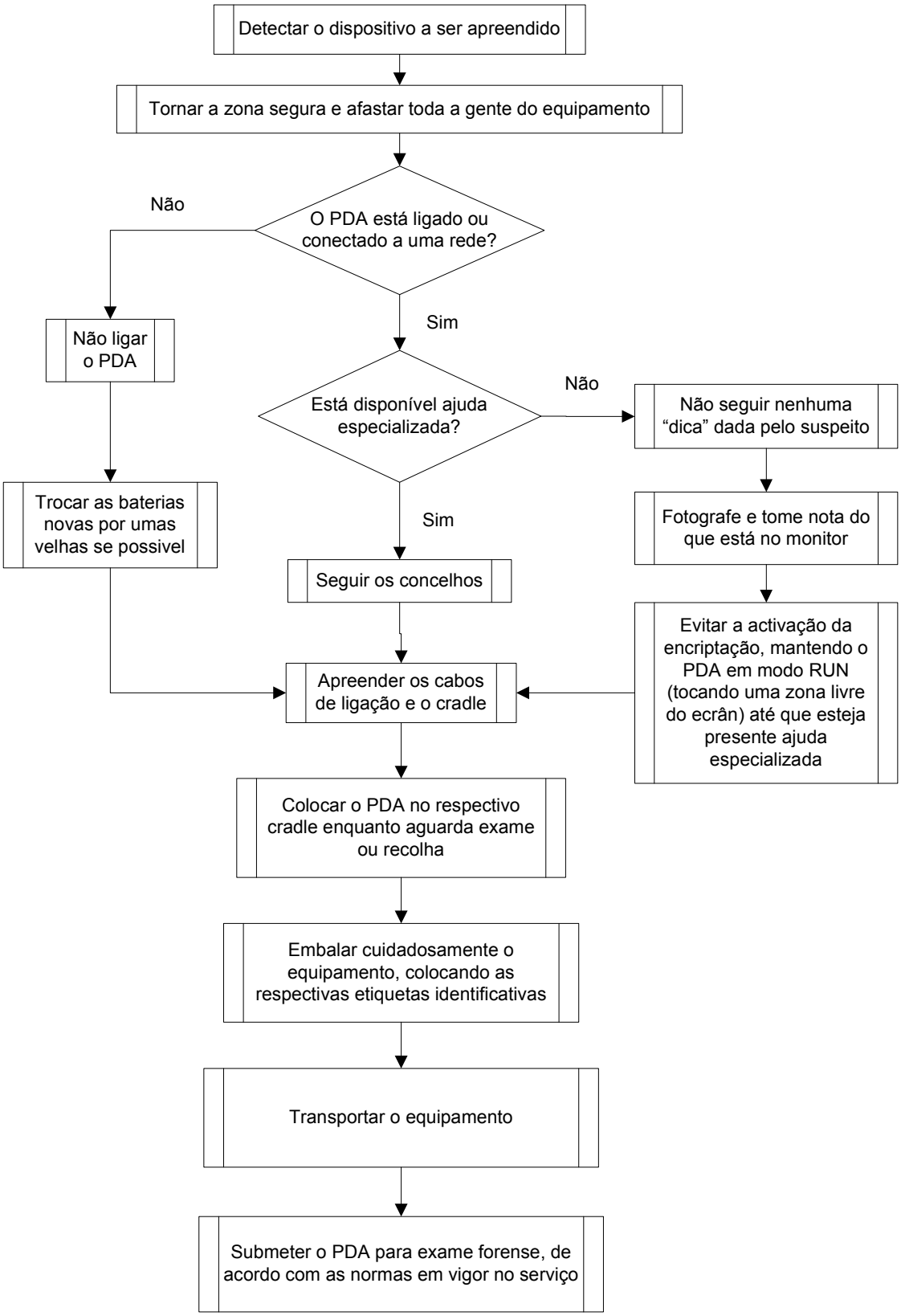
Outros dispositivos electrónicos:

- PDAs(Agendas electrónicas) e smart phones;
- Máquinas fotográficas e de filmar digitais

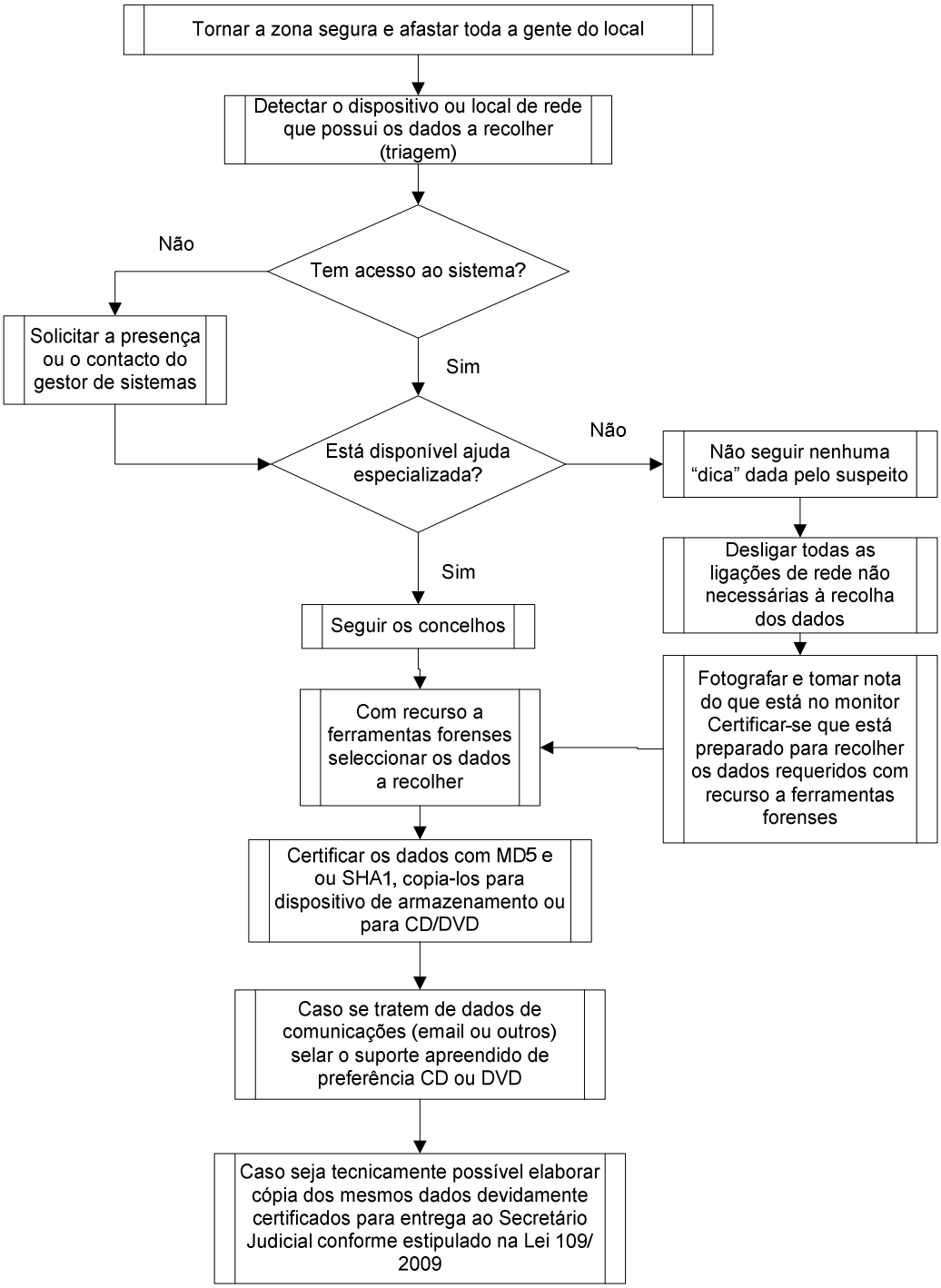
Material não electrónico:

- Software e manuais dos computadores;
- Papeis com palavras-chave;
- Chaves dos computadores

Anexo IV - Fluxograma/Guia rápido: Agendas eletrónicas (PDAs)



Anexo V - Fluxograma/Guia rápido: Recolha seletiva de dados



Atenção

Este tipo de recolha de dados só deve ser efetuada:

- Por técnicos com formação na área;
- Quando exista competente despacho ou autorização para efetuar pesquisas, no caso de autoridades judiciárias;

Glossário, siglas e acrónimos

Antiforensic – Termo utilizado para definir técnicas ou ferramentas utilizadas como contramedidas para evitar a eficácia das ferramentas forenses.

Batch files – Designação dada a ficheiros script, contendo texto com comandos que serão executados pelo sistema operativo no caso do MS-DOS, OS/2 e das diversas versões do Windows.

BIOS - Acrónimo de "Basic Input Output System". A BIOS de um computador é um pequeno segmento de código, normalmente armazenado numa memória ROM. Embora possa variar d fabricante para fabricante, mantém no entanto uma base comum de dados. Normalmente inclui a informação necessária para que o computador possa interagir com os dispositivos de entrada e saída (input/output ou IO), tais como teclados, CPU, placa de vídeo, recursos da motherboard ou placas de expansão ISA/PCI/AGP.

brute force - Termo normalmente utilizado no método de descoberta de palavra-chave através de tentativa e erro, percorrendo uma lista de palavras até se descobrir a correta

Checksum - Valor calculado que é utilizado para confirmar a integridade de dados. Entre as aplicações mais populares estão o Cyclic Redundancy Check (CRC) e o MD5.

CNPD – Comissão Nacional de Proteção de Dados.

CPP - Acrónimo de Código do Processo Penal.

File Slack - Área entre o último byte de um ficheiro e o fim do *cluster* assignado a esse ficheiro.

File slack - A área entre o último byte do ficheiro e o fim do *cluster* que está assignado a esse ficheiro

Host Protected Area (HPA) - Área reservada num disco, que não é "vista" pelo sistema operativo.

Honeypot - Designação anglo-saxónica que pode ser traduzida para "Pote de Mel" e é uma ferramenta que tem a função de criar uma armadilha ao atacante para registar os seus dados, através da colocação na rede de recursos inócuos e propositadamente vulneráveis.

Hashing - O termo mais usual que se encontra na literatura é a denominação anglo-saxónica, que pode ser traduzida por escrutínio ou resumo digital

Hash set - Denominação anglo-saxónica para uma coleção ou conjunto de códigos *hash*, normalmente com alguma relação que identifique esta coleção. Por exemplo, pode ser construído o "*hash* set" de todos os ficheiros identificados pela Interpol como contendo imagens de abusos sexuais de crianças.

HPA - Alguns discos estão equipados com um chip programável que permite aos programas definirem uma área no disco que é reservada e escondida do próprio sistema operativo. Esta área tem a denominação de "host protected area".

IETF - é uma comunidade internacional formada por técnicos, fabricantes e investigadores, que tem como missão melhorar o funcionamento da Internet. A IETF identifica e propõe soluções para problemas relacionados com a utilização e funcionamento da Internet, além de padronizar as tecnologias e protocolos envolvidos. A IETF publica documentos em forma de *drafts*, RFC (*Request for Comments*), STD (*Standards*) e BCP (*Best Current Practices*).

IDS - Acrónimo “Intrusion detection system”, que em português pode ser denominado por “Sistema de deteção de intrusões” e refere-se a meios técnicos para identificar numa rede quando nesta existe tráfego que podem indiciar ações maliciosas.

IOCE - Acrónimo de International Organization for Cooperation in Evaluation .

IPS - Acrónimo “Intrusion prevention system”, que em português pode ser denominado por “Sistema de prevenção de intrusões”. Trata-se de sistemas que evoluíram a partir de IDS com características de firewall para controlar os acessos na rede e que atualmente implementam formas inteligentes de bloqueio de tráfego na rede.

ISP - Normalmente designados pelas inicias anglo saxónicas ISP de *Internet Service Provider*, identifica os prestadores do serviço de acesso à Internet.

IACIS - Acrónimo de *International Association of Computer Investigative Specialists*, é uma organização internacional acreditada como certificadora pela *Forensic Specialties Accreditation Board* (FSAB).

Malware - Termo proveniente das palavras inglesas “malicious software” e identifica programas que se destinam a infiltrar um sistema informático de forma ilícita, com o intuito de causar dano, alteração no seu funcionamento ou retirada de informações. Vírus, worms, trojan horses e spywares são considerados malware.

Message Digest - O termo mais usual que se encontra na literatura é a denominação anglo-saxónica, que pode ser traduzida por resumo digital.

Multicast - Entrega de uma mensagem a um grupo de vários destinatários em simultâneo.

MTA - O Mail Transfer Agent é uma aplicação responsável pelo envio/receção de e-mail. Exemplos são o Postfix, o Exim ou o Qmail.

MUA - O Mail User Agent é um cliente de e-mail, isto é, onde as mensagens são escritas e lidas.

OCDE - Organization for Economic Cooperation and Developement.

OPC - Acrónimo de Órgão de Polícia Criminal.

Partition table - É uma tabela localizada no “Master Boot Record” de um disco que define com o este está particionado e inclui informação sobre o seu tamanho e localização, sistema de ficheiros utilizado por cada partição e que partições são bootable.

PDA - Acrónimo de Portable Digital Assistant, que pode ser traduzido para assistente pessoal digital ou *palmtop* e é um computador de dimensões reduzidas, dotado de grande capacidade computacional, cumprindo as funções de agenda e sistema informático de escritório elementar, com possibilidade de interconexão com um computador pessoal e uma rede informática sem fios.

Phishing - Derivado da designação anglo-saxónica *fishing* que quer dizer pesca e está relacionada com fraudes eletrônicas, caracterizadas por tentativas de adquirir dados pessoais de diversos tipos. Podem ser senhas, dados financeiros como número de cartões de crédito e outros dados pessoais. È normalmente executado através do envio de mensagens de correio eletrónico, mensagem instantânea ou SMS, levando o destinatário a crer na idoneidade do emissor e a fornecer os seus dados pessoais.

POP - O Post Office Protocol, ou POP3, é um protocolo utilizado no acesso remoto a uma caixa de correio eletrônico e permite a transferência de mensagens contidas numa caixa de correio eletrônico para um computador local, permitindo a sua leitura.

RAM Slack - O file slack é preenchido com dados da RAM. Isto só acontece nas versões Windows 95A e anteriores.

Ransomware - Denominação dada a um tipo de Malware que impede o normal funcionamento de um sistema informático, através do seu bloqueio ou da cifragem de informação, até que determinada quantia seja paga aos autores do Malware.

Sterile Media ou suportes esterilizados - Suportes onde cada byte foi reescrito com um valor hexadecimal conhecido ou aleatório, de forma a elimina os dados anteriores. Ao processo de reescrita chamasse "wiping" ou "esterilização".

SPADA - Acrónimo de *System Preview And Data Acquisition.*

SMTP - O Simple Mail Transfer Protocol permite a comunicação e entrega de mensagens entre duas entidades, também conhecidas como MTAs ou MUAs.

TSR - é um acrónimo que significa em inglês “terminate and stays residente”.

UPS - Acrónimo de “Uninterruptible Power Supply” e é um dispositivo que permite através da baterias, manter a energia de um sistema informático quando a energia elétrica falha.

Volume Boot Record - O primeiro sector de uma partição formatada num sistema de gestão de ficheiros do tipo FAT e que define a partição.

Wipe - Reescrita dos sectores do disco com dados aleatórios ou com 00h.

Recursos Digitais Adicionais

- Association of Chief Police Officers (United Kingdom) (2003). “Good Practice Guide for Computer Based Evidence,” V2.0: June 1999, V3.0: August 2003;
- Attallah, Mikhail (1999). CRC Press Algorithms and Theory of Computation Handbook;
- Centre for National High Tech Crime Training (UK) (2002). “Probationer training: High-tech crime overview,” V1.1;
- Como quebrar o MD5 e outras funções de *Hash*, disponível em http://www.infosec.sdu.edu.cn/uploadfile/papers/How to Break MD5 and other *Hash* Functions.pdf (consultado em 27/5/2013) e nos boletins do NIST em http://csrc.nist.gov/publications/PubsITLSB.html (consultado em 27/5/2013);
- "Classification and Generation of Disturbance Vectors for Collision Attacks against SHA-1" (PDF) publicado em 8 de Novembro de 2011 e consultado em http://eprint.iacr.org/2008/469.pdf (consultado a 6 de Abril de 2013);
- Council of Europe (2001). “Convention on Cybercrime,” European Treaty Series No. 185, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (consultado em 27/5/2013);
- Cryptographic *Hash* Workshop, 2007, http://csrc.nist.gov/groups/ST/*hash*/documents/Rivest_Bio.pdf (consultado a 6 de Abril de 2013);
- "Crypto++ 5.6.0 Benchmarks"., publicado em 27 de Fevereiro de 2011 e consultado em http://www.cryptopp.com/benchmarks.html (consultado a 6 de Abril de 2013);
- European Committee on Crime Problems (CDPC), http://www.coe.int/t/dghl/cooperation/economiccrime/default_en.asp. (consultado a 6 de Abril de 2013);
- Europol (2003). “Manual on Police Techniques and Practices within the European Law Enforcement Agencies”;
- FCCN (2011),http://www.cert.pt/images/docs/RecolhaArmazenamentoDadosProva.pdf. (consultado a 6 de Abril de 2013);
- Federal Ministry of the Interior (Austria) (2001). “Guide for Seizure and Evaluation of ElectronicEvidence,” (in German), Version 1.0, November 2001;
- http://www.cert.pt/index.php/recomendacoes/1616-recolha-e-armazenamento-de-dados-de-prova. (consultado a 6 de Abril de 2013);
- http://www.g8.fr/evian/english/navigation/the_g8/background_to_the_g8.html. (consultado a 6 de Abril de 2013);
- http://www.internetworldstats.com/stats.htm, (consultado em 6 de Abril de 2013)
- http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2012.pdf, (consultado em 6 de Abril de 2013);
- http://www.mcafee.com/us/resources/reports/rp-unsecured-economies-report.pdf, (consultado em 6 de Abril de 2013);
- http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_final_050912.pdf, (consultado em 6 de Abril de 2013);
- http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf. (consultado a 6 de Abril de 2013);
- http://www.enfsi.eu/sites/default/files/documents/forensic_it_best_practice_guide_v6_0.pdf. (consultado a 6 de Abril de 2013);
- http://www.nij.gov/nij/topics/forensics/evidence/digital/welcome.htm. (consultado a 6 de Abril de 2013);

- http://www.ncjrs.gov/pdffiles1/nij/199408.pdf. (consultado a 6 de Abril de 2013);
- https://www.swgde.org/documents Current Documents/2006-07-19 SWGDE Best Practices for Computer Forensics v2.1. (consultado a 6 de Abril de 2013);
- http://www.ioce.org/fileadmin/user_upload/2002/ioce_bp_exam_digit_tech.html. (consultado a 6 de Abril de 2013);
- http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Default_en.asp. (consultado a 6 de Abril de 2013);
- http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm. (consultado a 6 de Abril de 2013);
- http://www.infosec.sdu.edu.cn/uploadfile/papers/How to Break MD5 and Other *Hash* Functions.pdf (consultado a 6 de Abril de 2013);
- http://www.spada-cd.info/, (consultado a 6 de Abril de 2013);
- http://www.karenware.com/Dowertools/pt*hash*er.asp, (consultado a 6 de Abril de 2013);
- http://sourceforge.net/projects/jacksum/files/, (consultado a 6 de Abril de 2013);
- http://sourceforge.net/projects/cyo*hash*/, (consultado a 6 de Abril de 2013);
- http://www.rogeriopvl.com/*hash*r/, (consultado a 6 de Abril de 2013);
- http://www.fileformat.info/tool/*hash*.htm, (consultado a 6 de Abril de 2013);
- ISO/IEC FDIS 27037:2012: Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence. 60.60 (2012-10-15). http://www.iso.org/iso/catalogue_detail?csnumber=44381 (consultado em 27/5/2013);
- International Organization on Computer Evidence (2000). “First responders good practice guide template,” Proc. OCE 2000 Conference, Rosny sous Bois, France, December 2000;
- International Organization for Cooperation in Evaluation - http://www.ioce.net/. (consultado a 6 de Abril de 2013);
- Interpol (2002). “Cyber Crime Fighting,” Internet video material;
- Marques, Garcia e Martins, Lourenço (2006). “Direito da Informática”, Almedina;
- Martins, Lourenço (2003). “Criminalidade Informática”, artigo publicado em Direito da Sociedade da Informação, Volume IV, APDI, Coimbra Editora;
- M. E. Kabay "A Brief History of Computer Crime: A". Norwich University. Consultado em http://www.mekabay.com/overviews/history.pdf (consultado a 22 de Abril de 2013).
- New Technologies, Inc., URL: http://www.secure-data.com/ms.html, (consultado a 6 de Abril de 2013);
- Pieprzyk, Josef e Sadeghiyan, Babak (2007). Springer-Verlag Lecture Notes in Computer Science: Designs of *Hash*ing Algorithms;
- Police Cooperation Working Party (Council of the European Union) (2001). “Information Technology and Good Practice for Search & Seizure”;
- RFC 1321 - Definição do algoritmo MD5, disponível em http://tools.ietf.org/html/rfc1321 (consultado em 27/5/2013);
- Secure *Hash* Algorithm, publicado em 6 de Novembro de 2007e consultado em http:www.irnis.net/gloss/sha-1-checksum.shtml Secure *Hash* Algorithm. (consultado a 6 de Abril de 2013);
- SHA1 (Secure *Hash* Algorithm) – definição do algoritmo consultado em http://www.ietf.org/rfc/rfc3174.txt e http://www.irnis.net/gloss/sha-1-checksum.shtml (consultado em 27/5/2013);
- Technical Working Group for Electronic Crime Scene Investigation (2001). “Electronic Crime Scene Investigation: A Guide for First Responders” ;http://www.ncjrs.gov/pdffiles1/nij/219941.pdf (consultado em 27/5/2013);

- The guide to the TechTarget network, http://searchtechtarget.techtarget.com (consultado em 27/5/2013);
- Verdelho, Pedro, Bravo, Rogério, e Lopes Rocha, Manuel (2003). " Leis do Cibercrime", Centro Atlântico;
- Verdelho, Pedro, "Cibercrime" (2003). Artigo publicado em Direito da Sociedade da Informação, Volume IV, APDI, Coimbra Editora;

Referências

[1] http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2012.pdf, [disponível em 6 de Abril de 2013];

[2] http://www.mcafee.com/us/resources/reports/rp-unsecured-economies-report.pdf, [disponível em 6 de Abril de 2013];

[3] http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_

Cybercrime_Report_Master_final_050912.pdf, [disponível em 6 de Abril de 2013];

[4] http://www.internetworldstats.com/stats.htm, [disponível em 6 de Abril de 2013];

5 M. E. Kabay "A Brief History of Computer Crime: A". Norwich University, disponível em http://www.mekabay.com/overviews/history.pdf a 22 de Abril de 2013;

[6] http://www.cert.pt/index.php/recomendacoes/1616-recolha-e-armazenamento-de-dados-de-prova. [acedido em 6 de Abril de 2013];

[7] FCCN (2011). Disponível em http://www.cert.pt/images/docs/RecolhaArmazenamentoDadosProva.pdf. [acedido em 6 de Abril de 2013];

[8] http://www.g8.fr/evian/english/navigation/the_g8/background_to_the_g8.html. [acedido em 6 de Abril de 2013];

[9] IOCE - International Organization for Cooperation in Evaluation - http://www.ioce.net/. [acedido em 6 de Abril de 2013];

[10] http://www.acpo.police.uk/. [acedido em 6 de Abril de 2013];

[11] http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf. [acedido em 6 de Abril de 2013];

[12] Serious Organised Crime Agency. http://www.soca.gov.uk/. [acedido em 6 de Abril de 2013];

[13] http://www.enfsi.org/. [acedido em 6 de Abril de 2013];

[14] http://www.enfsi.eu/sites/default/files/documents/forensic_it_best_practice_guide_v6_0.pdf. [acedido em 6 de Abril de 2013];

[15] http://www.nij.gov/nij/topics/forensics/evidence/digital/welcome.htm. [acedido em 6 de Abril de 2013];

[16] http://www.ncjrs.gov/pdffiles1/nij/199408.pdf. [acedido em 6 de Abril de 2013];

[17] https://www.swgde.org/documents Current Documents/2006-07-19 SWGDE Best Practices for Computer Forensics v2.1. [acedido em 6 de Abril de 2013];

[18] http://www.ioce.org/fileadmin/user_upload/2002/ioce_bp_exam_digit_tech.html. [acedido em 6 de Abril de 2013];

[19]CDPC - European Committee on Crime Problems, http://www.coe.int/t/dghl/cooperation/economiccrime/default_en.asp. [acedido em 6 de Abril de 2013];

[20] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Default_en.asp. [acedido em 6 de Abril de 2013];

[21] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm. [acedido em 6 de Abril de 2013];

[22]Cryptographic Hash Workshop November 1, 2007 consultado a 6 de Novembro de 2007, de http://csrc.nist.gov/groups/ST/hash/documents/Rivest_Bio.pdf [disponível em 6 de Abril de 2013];

[23] Secure Hash Algorithm, publicado em 6 de Novembro de 2007 e disponível em http:www.irnis.net/gloss/sha-1-checksum.shtml Secure Hash Algorithm [disponível em 6 de Abril de 2013];

[24] "Crypto++ 5.6.0 Benchmarks"., publicado em 27 de Fevereiro de 2011 e disponível em http://www.cryptopp.com/benchmarks.html [disponível em 6 de Abril de 2013];

[25] "Classification and Generation of Disturbance Vectors for Collision Attacks against SHA-1" (PDF) publicado em 8 de Novembro de 2011 e disponível em http://eprint.iacr.org/2008/469.pdf [disponível em 6 de Abril de 2013];

[26] Toda a informação sobre este ponto pode ser consultada em “http://www.justice.gov/contact-us.html” [disponível em 6 de Abril de 2013];

[27] Toda a informação sobre este ponto pode ser consultada em “http://www.nsrl.nist.gov/index.html” [disponível em 6 de Abril de 2013];

[28] O documento encontra-se disponível para consulta em “http://www.infosec.sdu.edu.cn/uploadfile/papers/How to Break MD5 and Other Hash Functions.pdf” [disponível em 6 de Abril de 2013];

[29] Toda a informação sobre o produto pode ser consultada em http://www.spada-cd.info/ [disponível em 6 de Abril de 2013];

[30] Toda a informação sobre o produto pode ser consultada em “http://www.karenware.com/Dowertools/pthasher.asp” [disponível em 6 de Abril de 2013];

[31] Toda a informação sobre o produto pode ser consultada em http://sourceforge.net/projects/jacksum/files/ [disponível em 6 de Abril de 2013];

[32] Toda a informação sobre o produto pode ser consultada em http://sourceforge.net/projects/cyohash/ [disponível em 6 de Abril de 2013];

[33] Toda a informação sobre o produto pode ser consultada em http://www.rogeriopvl.com/hashr/ [disponível em 6 de Abril de 2013];

[34] Toda a informação sobre o produto pode ser consultada em "http://www.fileformat.info/tool/hash.htm" [disponível em 6 de Abril de 2013];

[35] New Technologies, Inc., URL: http://www.secure-data.com/ms.html[disponível em 6 de Abril de 2013];

[36] Transpõe para a ordem jurídica interna a Diretiva n.º 91/250/CEE, do Conselho, de 14 de Maio, relativa ao regime de proteção jurídica dos programas de computador;

[37] Transpõe para a ordem jurídica interna a Diretiva n.º 91/250/CEE, do Conselho, de 14 de Maio, relativa ao regime de proteção jurídica dos programas de computador;

[38] Acrónimo de International Association of Computer Investigative Specialists, é uma organização internacional acreditada como certificadora pela Forensic Specialties Accreditation Board (FSAB).